

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU BİLİM DALI

İDARENİN FAALİYETLERİNDE ELDE EDİLEN
KİŞİSEL VERİLERİN İŞLENMESİ

DOKTORA TEZİ

EMRE KILIÇ

İSTANBUL, 2025

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU BİLİM DALI

İDARENİN FAALİYETLERİNDE ELDE EDİLEN
KİŞİSEL VERİLERİN İŞLENMESİ

DOKTORA TEZİ
EMRE KILIÇ

Tez Savunma Jürisi

- | | |
|------------------|-------------------------------------|
| 1. Tez Danışmanı | : Prof. Dr. Gül ÜSTÜN |
| 2. Üye | : Prof. Dr. Zehreddin ASLAN |
| 3. Üye | : Prof. Dr. Nur Zeliha KAMAN |
| 4. Üye | : Dr. Öğr. Üyesi Ebru ZEYBEK CEBECİ |
| 5. Üye | : Dr. Öğr. Üyesi Nuray SÜMER |

İSTANBUL, 2025

İÇİNDEKİLER

KISALTMALAR.....	iv
ÖZET.....	vi
ABSTRACT	vii

GİRİŞ

1. KİŞİSEL VERİ KAVRAMI.....	2
1.1. Kişisel Veri.....	2
1.2. İlgili Kişi	5
1.2.1. Hayatta Olmayan Kişilere Ait Verilerin Durumu	10
1.2.2. Kimliği Belirli veya Belirlenebilir Olma	13
2. ÖZEL NİTELİKLİ (HASSAS) KİŞİSEL VERİ KAVRAMI	14
3. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ.....	16
4. KİŞİSEL VERİNİN HUKUKİ NİTELİĞİNE İLİŞKİN YAKLAŞIMLAR.....	22

1. BÖLÜM:

İDARENİN FAALİYETLERİNDE KİŞİSEL VERİ İŞLEMENİN HUKUKİ TEMELLERİ

1. İDARENİN KİŞİSEL VERİ İŞLEME SEBEPLERİ.....	29
2. İDARENİN KİŞİSEL VERİ İŞLEME SÜREÇLERİNDE UYMASI GEREKEN İLKELER.....	33
3. İSTİSNA HÜKÜMLERİ NEDENİYLE 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU’NUN KAPSAMI DIŞINDA BIRAKILAN HALLER	42
3.1. Tamamen Kanun Kapsamı Dışında Tutulan Haller	43
3.2. Kısmen Kanun Kapsamı Dışında Tutulan Haller.....	62
4. KANUNİ ŞARTLARA UYUM: 6698 SAYILI KANUNA GÖRE VERİ İŞLEMENİN ŞARTLARI VE İDARENİN YÜKÜMLÜLÜKLERİ.....	70
4.1. İdarenin Veri Sorumluları Siciline Kayıt Yükümlülüğü	70
4.2. İdarenin Veri Güvenliği Uygulamaları	75
4.3. Veri Sahipleriyle İletişimde İdarenin Aydınlatma Yükümlülüğü	79
4.4. Kanuni Gerekliliklere Uygun Veri İşlemenin Esasları	83
4.4.1. Genel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Şartlar	83
4.4.1.1. Kişisel Verinin İşlenebilmesinin Genel Şartı Olarak “Açık Rıza”	84
4.4.1.2. Açık Rıza Şartının İstisnaları	95
4.4.1.2.1. Kanunlarda Açıkça Öngörülmesi	97

4.4.1.2.2. Kişinin Hayatının veya Beden Bütünlüğünün Korunması.....	102
4.4.1.2.3. Sözleşme İlişkisi Bağlamında Kişisel Verilerin İşlenmesi	103
4.4.1.2.4. Veri Sorumlusunun Hukuki Yükümlülükleri Gereği Kişisel Veri İşlenmesi.....	105
4.4.1.2.5. Kişisel Verilerin İlgili Kişi Tarafından Alenileştirilmesi.....	112
4.4.1.2.6. Bir Hakkın Tesisi, Kullanılması veya Korunması Amacıyla Veri İşleme	114
4.4.1.2.7. Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlemesi: İdari Faaliyetlerde Meşru Menfaatin Yeri	114
4.4.2. Özel Nitelikli (Hassas) Verilerin İşlenmesine İlişkin Şartlar.....	117
4.4.2.1. 2 Mart 2024 Tarihli 7499 Sayılı Kanun Değişikliği Öncesi Durum	118
4.4.2.2. Yeni Düzenleme ve Genişleyen Veri İşleme Şartları.....	119
4.4.2.3. Özel Nitelikli Verilerin İşlenmesinde Aranılan Genel Şart Olarak KVK Kurulu Tarafından Belirlenen Yeterli Önlemlerin Alınması.....	126
4.4.3. İdarenin Veri Aktarımı veya Veriyi Koruması: Mahremiyet ve Güvenlik Ekseninde Bir Değerlendirme	129
4.4.3.1. İdarenin Kişisel Verileri Yurt İçinde Başka Bir İdareye Aktarması ile Aynı İdarenin Farklı Birimleri Arasındaki Veri Paylaşımı	129
4.4.3.2. İdarenin Kişisel Verileri Yurt İçinde Gerçek Kişilere Aktarması.....	133
4.4.3.3. İdarenin Kişisel Verileri Yurt Dışına Aktarması.....	140

2. BÖLÜM:

İDARENİN FAALİYETLERİNDE İŞLENEN KİŞİSEL VERİLER

1. KAMU HİZMETİ VE KOLLUK FAALİYETLERİNDE ELDE EDİLEN KİŞİSEL VERİLERİN İŞLENMESİ BAKIMINDAN AYRI BİR HUKUKİ REJİMİN UYGULANMASI GEREKLİ VE/VEYA MÜMKÜN MÜ?.....

2. İDARENİN FAALİYETLERİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN İŞLENMESİ.....

2.1. Kamu Hizmetlerinin Sunumunda Kişisel Verilerin İşlenmesi.....	149
2.1.1. Eğitim Hizmetlerinde Dijitalleşme ve Kişisel Veri Güvenliği.....	149
2.1.1.1. Genel Olarak	149
2.1.1.2. Dijital Eğitim Araçları ve Veri Güvenliği.....	154
2.1.2. Sağlık Hizmetlerinde Kişisel Sağlık Verilerinin İşlenmesi.....	162
2.1.3. Akıllı Ulaşım Sistemleri ile Sunulan Ulaşım Hizmetlerinde Kişisel Veri İşleme	168
2.2. Kolluk Faaliyetlerinde Kişisel Verilerin İşlenmesi.....	175
2.2.1. Genel Sağlığın Korunmasında Veri İşleme.....	175
2.2.1.1. Genel Olarak	175
2.2.1.2. Salgın Hastalık Dönemlerinde Kişisel Sağlık Verilerinin İşlenmesi	178

2.2.2. Kamu Güvenliği Kapsamında Elektronik Gözetim Sistemleriyle Kişisel Veri İşleme	187
2.2.3. Dirlik ve Esenlik Unsuru Kapsamında Toplantı ve Gösteri Yürüyüşlerinde Kişisel Verilerin İşlenmesi	191
2.3. Kamu Görevlilerine Ait Kişisel Verilerin İşlenmesi	198
2.3.1. Kamu Görevine Girişte Veri İşleme: Güvenlik Soruşturması ve Arşiv Araştırması	200
2.3.2. Kamu Görevi Süresince Veri İşleme.....	203
2.3.2.1. Özlük Dosyalarında İşlenen Kişisel Veriler	203
2.3.2.2. Disiplin İşlemleri Sürecinde İşlenen Kişisel Veriler	207
3. İDARENİN KİŞİSEL VERİ İŞLEMESİNDEN DOĞAN HUKUKİ SORUMLULUĞU	211
4. KİŞİSEL VERİLERİN İDAREYE KARŞI KORUNMASINA İLİŞKİN DENETİM MEKANİZMALARI.....	217
4.1. İdari Denetim.....	217
4.1.1. Veri Sorumlusu İdareye Başvuru	218
4.1.2. KVK Kurulunca Denetim.....	225
4.1.2.1. İlgili Kişi Tarafından Kurula Yapılan Şikâyet	225
4.1.2.2. KVK Kurulunun Resen Harekete Geçmesi.....	229
4.2.Yargısal Denetim.....	230
4.2.1. KVK Kurulu Kararlarına Karşı Yargı Yolu	230
4.2.2. Veri Sorumlusu İdarenin Yargısal Denetimi.....	231
4.2.2.1. İptal Davası	231
4.2.2.2. Tam Yargı Davası	233
SONUÇ	235
KAYNAKÇA	244

KISALTMALAR

AB	:	Avrupa Birliđi
ABAD	:	Avrupa Birliđi Adalet Divanı
AIHM	:	Avrupa İnsan Hakları Mahkemesi
AIHS	:	Avrupa İnsan Hakları Sözleşmesi
AYM	:	Anayasa Mahkemesi
BDEK	:	Bilgi Edinme ve Deđerlendirme Kurulu
bkz.	:	Bakınız
C.	:	Cilt
CBK	:	Cumhurbaşkanlığı Kararnamesi
CD.	:	Ceza Dairesi
CETS	:	Council of Europe Treaty Series
D.	:	Danıştay
DD.	:	Dava Dairesi
DMK	:	Devlet Memurları Kanunu
E.	:	Esas sayısı
E.T.	:	Erişim tarihi
GDPR	:	General Data Protection Regulation
İDDK	:	İdari Dava Daireleri Kurulu
İYUK	:	İdari Yargılama Usulü Kanunu
K.	:	Karar sayısı
KVKK	:	Kişisel Verileri Koruma Kanunu
KVK Kurulu	:	Kişisel Verileri Koruma Kurulu

OJ, L	:	Official Journal of the European Union, Legislation Series
par.	:	Paragraf
RG	:	Resmî Gazete
S.	:	Sayı
s.	:	Sayfa
T.	:	Tarih
TCK	:	Türk Ceza Kanunu
vb.	:	ve benzeri
vd.	:	ve diğerleri



ÖZET

İDARENİN FAALİYETLERİNDE ELDE EDİLEN KİŞİSEL VERİLERİN İŞLENMESİ

Bu tez, İdarenin faaliyetlerinde elde edilen kişisel verilerin işlenmesini, kamu hizmetleri ile bireysel mahremiyet hakları arasındaki denge üzerine odaklanarak incelemektedir. Çalışma, AB'nin Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'nin 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) da dahil olmak üzere çeşitli ulusal yasaları içeren yasal çerçeveleri analiz etmekte ve bunların kamu hizmeti ile kolluk faaliyetlerinde uygulanmasını ele almaktadır. Araştırma eğitim, sağlık ve ulaşım hizmetlerinde kişisel verilerin işlenmesi, kamu düzeninin korunması amacıyla kişisel veri işlemenin sınırları ve kamu görevlilerinin kişisel bilgilerinin korunması gibi temel konuları incelemektedir. Denetim mekanizmalarını, idari sorumlulukları ve veri ihlallerinin olası sonuçlarını karşılaştırmalı bir perspektiften araştırarak hem akademik söyleme hem de pratik politika oluşturmaya katkıda bulunmayı amaçlamaktadır. Tez, giderek küreselleşen ve dijitalleşen bir yönetim ortamında şeffaflık ile mahremiyet arasında dinamik bir denge ihtiyacını vurgulamaktadır.

Anahtar kelimeler: Kişisel verilerin korunması, Kamu yönetimi, Veri gizliliği, 6698 sayılı Kanun, İdari hesap verebilirlik, Dijital yönetim

ABSTRACT

**PROCESSING OF PERSONAL DATA OBTAINED IN THE ACTIVITIES OF THE
ADMINISTRATION**

This thesis examines the processing of personal data obtained in the activities of the Administration, focusing on the balance between public services and individual privacy rights. The study analyzes legal frameworks including various national laws, including the EU's General Data Protection Regulation (GDPR) and Turkey's Law No. 6698 on the Protection of Personal Data (KVKK), and considers their application in public service and law enforcement activities. The research examines key issues such as the processing of personal data in education, health and transportation services, the limits of personal data processing for the protection of public order and the protection of personal data of public officials. It aims to contribute to both academic discourse and practical policy-making by exploring control mechanisms, administrative responsibilities and the possible consequences of data breaches from a comparative perspective. The thesis emphasizes the need for a dynamic balance between transparency and privacy in an increasingly globalized and digitalized governance environment.

Keywords: personal data protection, public administration, data privacy, Law No. 6698, administrative accountability, digital governance

GİRİŞ

Dijital çağın hızla gelişen dinamikleri içerisinde, kişisel verilerin işlenmesi konusu, modern toplumların en kritik gündem maddelerinden biri haline gelmiştir. Özellikle idarenin faaliyetleri bağlamında, kişisel verilerin işlenmesi ve korunması, kamu hizmetlerinin etkinliği ile bireylerin temel hak ve özgürlükleri arasındaki hassas dengenin korunması açısından büyük önem taşımaktadır.

Günümüzde idare, vatandaşlara daha iyi hizmet sunabilmek, kamu politikalarını daha etkin şekilde oluşturabilmek ve toplumsal ihtiyaçlara daha hızlı cevap verebilmek adına giderek artan oranda kişisel veri işlemektedir. Ancak bu durum, veri güvenliği, mahremiyet hakkı ve kişisel özerklik gibi temel haklar açısından ciddi endişeleri de beraberinde getirmektedir. İşte tam da bu noktada, idarenin veri işleme ihtiyacı ile bireylerin kişisel verilerinin korunmasını isteme hakkı arasında nasıl bir denge kurulacağı sorusu, hukuki boyutuyla tartışılması gereken çetrefilli bir mesele olarak karşımıza çıkmaktadır.

Tezin giriş kısmında, kişisel veri kavramı, özel nitelikli (hassas) kişisel veri kavramı, kişisel verilerin korunmasının tarihsel gelişimi ve kişisel verinin hukuki niteliğine ilişkin yaklaşımlar ele alınacaktır. Bu kısım, konunun kavramsal çerçevesini oluşturacaktır.

İlk bölümde, idarenin kişisel veri işleme faaliyetlerinin tâbi olduğu kurallar derinlemesine incelenecektir. Bu kapsamda, idarenin veri işleme ihtiyacının arkasındaki motivasyonlar, bu faaliyetlerin hukuki dayanakları ve sınırları, özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun getirdiği yükümlülükler eleştirel bir bakış açısıyla değerlendirilecektir.

Tezimizin ikinci bölümü, kişisel verilerin işlenmesinin kamu hizmeti ve kolluk faaliyetlerindeki uygulamalarına ayrılacaktır. Bu kapsamda, eğitim, sağlık, ulaşım ve kamu görevlilerinin verilerinin işlenmesi gibi kritik alanlarda idarenin kişisel veri işleme faaliyetlerini derinlemesine inceleyeceğiz. Örneğin, eğitim sektöründe dijital platformların yaygınlaşmasıyla birlikte öğrenci verilerinin nasıl işlendiği; sağlık hizmetlerinde kişisel sağlık verilerinin yönetimi ve mahremiyetin korunması; akıllı ulaşım sistemlerinde toplanan verilerin işlenmesi ve güvenliği ele alınacaktır. Ayrıca, kamu düzeninin korunması bağlamında salgın hastalıklarda sağlık verilerinin işlenmesi, kamu güvenliğinin korunması amacıyla elektronik gözetim sistemleriyle kişisel veri işleme, dirlik-esenliğin sağlanmasında toplantı ve gösteri yürüyüşleri sırasında kişisel veri işleme ve kamu görevlilerinin özlük dosyaları, güvenlik soruşturmaları gibi hassas konularda kişisel verilerin işlenmesi ve korunması konuları incelenecektir. İdari faaliyetler bağlamında farklı örnekler üzerinden yapılan analizler, idarenin farklı alanlardaki veri işleme pratiklerini, karşılaşılan zorlukları ve geliştirilen çözümleri ortaya koyarken, aynı zamanda geleceğe dönük politika önerileri için de zemin hazırlayacaktır.

Ayrıca, idarenin kişisel veri işleme faaliyetlerinden kaynaklanan hukuki sorumluluğunun kapsamı ve bu faaliyetlerin denetim mekanizmaları incelenecektir. Bu bağlamda, KVK Kurulu'nun idari denetim rolü ve veri sorumlusu İdarenin yargısal denetim süreçleri değerlendirilecektir.

Bu çalışma, idarenin faaliyetlerinde elde edilen kişisel verilerin işlenmesi konusundaki durumu analiz etmeyi, karşılaşılan zorlukları tespit etmeyi ve olası çözüm önerileri sunmayı hedeflemektedir. Teknolojik gelişmeler ve değişen toplumsal ihtiyaçlar karşısında, idarenin kişisel verileri koruma yükümlülüğü ile idari faaliyetlerini etkin bir şekilde yürütme görevi arasındaki dengenin nasıl kurulacağı sorusu, tezimizin temel odak noktalarından birini oluşturacaktır.

Sonuç olarak, bu tez çalışması, idarenin faaliyetlerinde elde edilen kişisel verilerin işlenmesi konusunda kapsamlı bir inceleme sunarak hem akademik literatüre katkı sağlamayı hem de uygulayıcılara yol gösterici olmayı amaçlamaktadır.

1. KİŞİSEL VERİ KAVRAMI

1.1. Kişisel Veri

Kişisel veri kavramının tanımı çeşitli uluslararası metinlerde benzer şekilde yapılmıştır. Örneğin, Avrupa Konseyi tarafından çıkarılan 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nde (108 sayılı Sözleşme)¹ ve Ekonomik İş Birliği Örgütü (OECD) tarafından yayımlanan “Mahremiyetin ve Kişisel Verilerin Sınır Ötesi Akışını Düzenleyen Rehber İlkeler” adlı metinde² kişisel veri “*kimliği belirli veya belirlenebilir kişiye ilişkin her türlü bilgi*” şeklinde tanımlanırken, Avrupa Birliği tarafından çıkarılan 95/46/EC sayılı Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif'te³ ve bu Direktif'in yerini alan 2016/679 sayılı Genel Veri Koruma Tüzüğü'nde⁴ kişisel veri “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır. Görüldüğü üzere, ilk tanımda gerçek ya da tüzel kişi ayrımı yapılmazken, ikinci tanımda sadece gerçek kişiye ilişkin verilerin kişisel veri olabileceği kabul edilmiştir.

Ülkemizde 24 Mart 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda⁵ (KVKK) kişisel veri “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*”

¹ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 (1981).

² Organisation for Economic Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (1980).

³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281/31

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(2016) OJ L 119/1.

⁵ RG, 7.4.2016/29677.

şeklinde tanımlanmıştır. Dolayısıyla tüzel kişilere ilişkin veriler 6698 sayılı Kanun kapsamında yer almamaktadır⁶.

Anayasa Mahkemesi ise kişisel veri kavramını çeşitli örnekler vererek şu şekilde tanımlamaktadır:

“Kişisel veri – belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmişi, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır”.⁷

Danıştay kararlarına bakıldığında, farklı bir tanımlama yapılmak yerine AYM’nin yukarıdaki tanımına atıfta bulunulduğu görülmektedir⁸. Öte yandan Yargıtay’a göre kişisel veri “*kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri... kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilgi*”dir⁹.

Yapılan tanımlara bakıldığında, kişiye ait her türlü bilginin kişisel veri kavramı içerisine dahil olduğu görülmektedir. Nitekim kanuni tanım da “kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgi” şeklindedir. Kişinin medeni hali, etnik kökeni, dini ve siyasi görüşü, cinsel ve ahlaki eğilimi, sendikal bağlantıları, DNA’sı, saç, tükürük örnekleri¹⁰, hatta kişinin yürüyüş biçimi ve vücut kokusu gibi bilgiler de biyometrik bir veri olması sebebiyle kişisel verilere dahildir¹¹. Parmak izi, yüz, el geometrisi, iris, imza ve ses gibi klasik biyometrik verilerin dışında kulak biçimi, vücut ısı, derinin yansıtıcılığı, retina, klavye tuşlamaları ve dudak hareketleri gibi diğer biyometrik kimlik yöntemleri de kullanılarak kişilerin kimlikleri tespit edilebildiğinden¹² bu veriler de birer kişisel veri olarak kabul edilebilir.

⁶ Bu konudaki değerlendirmemiz için **1.2. İlgili Kişi** başlığına bakılabilir.

⁷ AYM, E.2013/122, K.2014/74, T.9.4.2014; AYM, E.2014/74, K.2014/201, T.25.12.2014; AYM, E.2014/180, K.2015/30, T.19.3.2015; AYM, B.n.: 2018/24439, T.15.6.2021.

⁸ Danıştay 12.D. E.2020/1676, K.2021/1304, T.15.3.2021 (Lexpera); Danıştay İDDK, E.2019/2278, K.2020/2460, T.19.11.2020 (Lexpera)

⁹ Yargıtay 12. CD., E.2013/9669, K.2014/3760, T.17.2.2014 (Lexpera).

¹⁰ Yargıtay 12. CD., E.2013/9669, K.2014/3760, T.17.2.2014 (Lexpera).

¹¹ Aydın AKGÜL, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması Hukuku**, Beta Yayınevi, 2. Baskı, 2016, s.9.

¹² Çeşitli biyometrik yöntemlere ilişkin ayrıntılı bilgi için bkz.: Cüneyd ER, **Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Yetkin Yayınları**, Ankara, 2007, s. 21 vd.

Bununla birlikte, her türlü kişisel verinin 6698 sayılı Kanunun koruması altında olmadığı da ifade edilmelidir. Nitekim, Kanunun “Kapsam” başlıklı ikinci maddesinde “*Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.*” kuralına yer verilmiştir. Buna göre, Kanunun yalnızca verileri tamamen ya da kısmen otomatik olan veya herhangi bir veri kayıt sisteminin parçası haline getirmek kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağını, dolayısıyla bir sisteme dayalı olmaksızın ya da sonradan herhangi bir sisteme dahil edilmeksizin veri işleyen kişilerin ve işlenen verilerin bu Kanun kapsamında sayılmadığı kabul edilmiştir. Kanundaki tanımına göre “*Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi(n)*” varlığı halinde bir veri kayıt sisteminden bahsedilebileceğine göre veri kaydının bilgisayar ya da fiziki olarak tutulması fark etmez. İsim, tarih, yer gibi çeşitli kriterler esas alınarak sınıflandırılan ve kayda alınan, başka bir deyişle geliş güzel olmayıp sistematik bir düzende işlenen veriler ve bunu işleyenler 6698 sayılı Kanun kapsamındadır¹³. İdarelerin işleyiş biçimi düşünüldüğünde, sahip olunan verileri belli bir sistematik içinde kayıt altında tuttukları, dolayısıyla işledikleri kişisel verilerin 6698 sayılı Kanun kapsamında olacağı kabul edilmelidir. Bununla birlikte, Kanunun 28. maddesinde yer verilen “İstisna” hükümleri hatırd tutulmalıdır. Aşağıda ayrıntısıyla yer verileceği üzere, özellikle İdarelerin bazı amaçlarla işledikleri veriler için 6698 sayılı Kanunun uygulanmayacağı kabul edilmiş ve geniş sayılabilecek bir alan Kanun kapsamı dışında bırakılmıştır¹⁴.

Öte yandan, Kanunun 2. maddesi bağlamında kapsam dışında bırakılan kişisel verilerin işlenmesinin tümünden hukuka uygun olduğu söylenemez. İlgili maddenin gerekçesinde de vurgulandığı üzere, bu şekilde işlenen kişisel veriler 6698 sayılı Kanunun korumasında değilse de hâlâ kişisel veri olarak kabul edildiğinden başta Anayasa olmak üzere ilgili diğer mevzuat hükümlerine uygun olarak işlenmesi gerekmekte olup, örneğin bu tür verilere ilişkin veri işleme faaliyetlerinin 5237 sayılı Türk Ceza Kanunu’nun ilgili maddeleri uyarınca suç teşkil edebileceği unutulmamalıdır¹⁵.

¹³ Çağla TANSUĞ, **İdari Faaliyetlerde İşlenen Kişisel Verilerin İdare Tarafından Korunması**, On İki Levha Yayıncılık, 2023, s. 59.

¹⁴ 6698 sayılı Kanunun 28. maddesine ilişkin inceleme için bkz.: “**3. 6698 SAYILI KVKK’NİN İSTİSNALARI**” başlığı.

¹⁵ Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s.7, <https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf> (E.T. 3.9.2023).

Türk Ceza Kanunu’nun 135. maddesinde “kişisel verilerin kaydedilmesi suçu”, 136. maddesinde “verileri hukuka aykırı olarak verme veya ele geçirme” ve 138. maddesinde “verileri yok etmeme” suçları düzenlenmiştir. Konuya ilişkin bazı eserler şöyledir: Şeyma SERT, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin, 2. Baskı, Mayıs 2023; Zeynel T. KANGAL, **Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması**, On İki Levha Yayıncılık, Eylül 2019; Hasan SINAR, **Kişisel Verilerin Ceza Normlarıyla Korunması**, Der Yayınevi, Haziran 2023; Melike KÖSE AYSUN, **Kişisel Verilerin Kaydedilmesi Suçu**, Seçkin, 2. Baskı, Ekim 2021; Mahmut KOCA, “Ceza Hukuku Açısından Kişisel Verilerin Korunması Ve Verilerin İmha Edilmemesinin Sonuçları” içinde **Kişisel Verilerin İmhası**, Seçkin, 2. Baskı, Ekim 2022, s. 381 vd.

1.2. İlgili Kişi

6698 sayılı Kişisel Verilerin Korunması Kanunu, gerçek kişilerin kişisel verilerini korumakta, tüzel kişileri ise kapsam dışında tutmaktadır. Kanunun 3. maddesinin (d) fıkrasına göre kişisel veri *kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi* ifade eder. Bu sebeple, tüzel kişilerin de kişisel verilerinin korunup korunmayacağı hususu tartışma konusu olmuştur. Adalet Bakanlığınca hazırlanan ve 22.4.2008 yılında Bakanlar Kurulunca kabul edilen Kişisel Verilerin Korunması Kanunu Tasarısı'nda ilgili kişi tanımına Avrupa Birliği'nin son direktifleri doğrultusunda tüzel kişilerin de dahil edildiği madde gerekçesinde ifade edilmişken¹⁶, yeniden hazırlanan ve 18.1.2016 tarihinde meclise gönderilen tasarıda tüzel kişilere Kanun kapsamında yer verilmemiş ve Kanun bu şekliyle yürürlüğe konulmuştur. Dolayısıyla, tüzel kişilerin kanun kapsamına dahil edilmesi fikrinin en azından başlangıçta kabul gördüğü ancak yaklaşık sekiz yıl sonra yasalaşan Kanunda bu fikrin kabul edilmediği söylenebilir.

AB'nin 95/46/EC sayılı Direktifi'ne ve 2016/679 sayılı Genel Veri Koruma Tüzüğü'ne bakıldığında tüzel kişilerin koruma kapsamına alınmadığı görülmektedir. 108 sayılı Avrupa Konseyi Sözleşmesi ise tüzel kişileri kapsamı dışında bırakmamıştır. Sözleşmenin 2. Maddesinin (a) fıkrasında kişisel veri kimliği belirli ya da belirlenebilir kişi (individual) hakkındaki her türlü bilgi olarak tanımlanmıştır. Bu sebeple Sözleşmeyi imzalayacak ülkeler tüzel kişileri mevzuatlarına dahil edip etmemekte serbesttir. Örneğin, İsviçre ve Avusturya gibi bazı ülke kanunlarında tüzel kişiler de gerçek kişiler gibi veri koruma yasalarının koruması kapsamına dahil edilmiştir¹⁷.

5237 sayılı Türk Ceza Kanunu'nun 135. maddesi bağlamında değerlendirildiğinde bu konunun tartışmalı olduğu görülmektedir. 135. madde uyarınca “(1) *Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*” ŞEN'e göre, bu hükümde suçun mağduru olarak gerçek kişi-tüzel kişi ayrımı yapılmadığından TCK bakımından “kişisel verilerin kaydedilmesi” suçunun mağduru bir tüzel kişi de olabilir¹⁸. Bununla birlikte, söz konusu hükmün gerekçesinde suçun mağdurunun gerçek kişiler olabileceği belirtilmişse de ŞEN bunun madde metninin amacını sınırlayan hatalı bir ifade olduğunu kabul etmektedir.

Öte yandan, KOCA/ÜZÜLMEZ' e göre tüzel kişilere ait veriler bu suçun konusunu oluşturamayacağı için bu suçun mağduru ancak gerçek kişiler olabilir¹⁹. Buna göre, ticari veya sınai bir

¹⁶ Kişisel Verilerin Korunması Kanunu Tasarısı, 18.1.2016, <https://www2.tbmm.gov.tr/d23/1/1-0576.pdf> (E.T. 26.8.2021).

¹⁷ Ayrıntılı bilgi için bkz.: Cemal BAŞAR, “Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması”, **Dokuz Eylül Üniversitesi SBE**, Doktora Tezi, 2019, s.17 vd.

¹⁸ Ersan ŞEN, “Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi”, **İstanbul Barosu Dergisi**, C.83, S.3, Mayıs 2009, s.1201. Aynı yönde görüş için bkz.: Yılmaz SACİT, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Adalet Yayınları, Nisan 2016, s.257.

¹⁹ Mahmut KOCA/ İlhan ÜZÜLMEZ, “Kişisel Verilerin Kaydedilmesi Suçu (m.135)”, **D.E.Ü. Hukuk Fakültesi Dergisi**, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, s.75.

işletmeye ait ticari sır, bankacılık sırrı yahut müşteri sırrı niteliğindeki bilgi ve belgelerin hukuka aykırı şekilde açıklanması ancak TCK'nin 239. maddesinde tanımlanan suç oluşturacaktır²⁰.

Bilindiği üzere, 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK'nin 135. maddesi ile kişisel verilerin hukuka aykırı olarak kaydedilmesi, 136. maddesi ile başkalarına verilmesi veya ele geçirilmesi ve 138. maddesi ile kişisel verilerin yok edilmemesi fiilleri suç olarak kabul edilmiş ve bu düzenleme kişisel verilerin korunmasına yönelik olarak yapılan ilk özel düzenleme olmuştur. Bu hükümlerin, Türkiye'nin 28 Ocak 1981 tarihinde imzalayarak taraf olduğu 108 sayılı Sözleşme hükümlerine geçerlilik tanımak amacıyla getirildiği madde gerekçelerinde belirtilmiştir²¹. 108 sayılı Sözleşmenin onaylanması ve kişisel verilere ilişkin özel bir kanunun çıkarılması için 2016 yılına dek beklenilmesinin 5237 sayılı TCK'deki düzenlemelerin kapsamı konusunda tereddüt yaşanmasına sebebiyet verdiği söylenebilir²².

Anayasa Mahkemesi tarafından verilen bir kararda ise tüzel kişilere ait kişisel verilerin de Anayasanın 20. maddesi uyarınca koruma altında olduğu ifade edilmiştir²³. Karara konu hüküm, 6475 sayılı Posta Hizmetleri Kanununun 3/1 maddesinin (a) bendinde yer verilen “ilgili mevzuatı saklı kalmak kaydıyla” ibaresinden sonra gelen “gerçek” ibaresidir. Madde hükmüne göre PTT bünyesinde bir “adres bilgi kayıt sistemi” oluşturularak gerçek ve tüzel kişilere ait fiziki ve elektronik adresler bu sisteme kaydedilecek, sisteme kayıtlı bilgiler reklam ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığı kullandırılacaktır. Hükümün tartışmalı kısmı, ticari amaçlarla veri tabanı oluşturulurken gerçek kişilerin rızası alınma zorunluluğu getirilmesi; ancak aynı zorunluluğun tüzel kişiler bakımından geçerli olmamasıdır.

Anayasa Mahkemesi yaptığı değerlendirmede, Anayasa'nın 20. maddesinde kişisel verilerin kişi bakımından korunma alanı ile ilgili herhangi bir açıklığa sahip olmadığını, maddenin gerekçesinde de buna ilişkin bir belirleme yapılmadığını, ayrıca madde metninde “herkes” tabirinin kullanılması dikkate alındığında tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerektiğini ifade etmiştir²⁴.

²⁰ Madde 239 (1): “Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikâyet üzerine, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi halinde de bu fıkra göre cezaya hükmolunur.”

²¹ Aktaran: KOCA/ÜZÜLMEZ, s.72. Sözleşme bu tarihte imzalanmışsa da ülkemizde onaylandığına ilişkin Bakanlar Kurulu kararı ve metnin Türkçe çevirisi 17.3.2016 tarih ve 29656 sayılı RG’de yayımlanmıştır.

²² KOCA/ÜZÜLMEZ, s.72.

²³ AYM, E.2013/84, K.2014/183, T. 4.12.2014.

²⁴ Anayasanın 20. maddesinin 3. fıkrası şu şekildedir: “(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

Kişisel verilerin korunması hakkının temelde neyi ya da kimi koruduğuna ilişkin yapılacak bir değerlendirmeye bu hususta daha doğru bir sonuca varılabilir. Kişisel verilerin korunması hakkı temel haklardan olup, özünde insanın kişiliği ile onun özel alanını korumayı amaçlamaktadır²⁵. Nitekim, gerek 2010 yılındaki değişikliğe kadar Anayasamızda gerekse de Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) kişisel verilerin korunması hakkı açıkça belirtilmemişse de AYM ve AİHM tarafından genişletici yorum yapılarak kişisel verilerin korunması “özel hayatın gizliliği” ve “maddi ve manevi varlığı geliştirme” hakları altında korunmuştur²⁶.

Ayrıca, yukarıda söz ettiğimiz AYM kararının “Karşı Oy” yazısında ifade edildiği üzere AİHM, kişisel verilerin korunmasına yönelik kararlarında Sözleşmenin 8. maddesi bağlamında değerlendirme yapmakta ve bu maddede de “herkes” kavramına yer vermekte, bununla birlikte maddenin temel amacının bireyi korumak olduğu ve “herkes” teriminin yaş, temyiz kudreti, vatandaşlık veya cinsiyet ayrımı gözetilmeksizin her bireyin bu haktan yararlanabileceği bağlamında anlaşıldığı ifade edilmektedir²⁷. Dolayısıyla, kişisel verilerin korunması hakkı esasen “gerçek kişinin” korunmasını amaçlayan bir hak olarak görülmektedir. Bu açıdan bakıldığında, tüzel kişilerin kişisel verilerin korunması kapsamında kabul edilmesinin hakkın amacıyla uyumlu olmadığı söylenebilecektir²⁸.

Öte yandan, tüzel kişiye ait bir verinin gerçek bir kişiyi belirlemesi ya da belirlenebilir kılması halinde bu verilerin de koruma kapsamında olacağı Kişisel Verileri Koruma Kurumunca ifade edilmiştir. Tabii olarak bu durumda korunan menfaat tüzel kişiye değil gerçek kişiye ait olacaktır²⁹. Örneğin, 6102 sayılı Türk Ticaret Kanunu'nun 40. maddesine göre her gerçek kişi ya da tüzel kişi tacirin ticari işletmesini ve ticari unvanını işletme merkezinin bulunduğu yer ticaret siciline tescil ve ilan ettirmek zorundadır. Kayıtlar Ticaret Bakanlığı tarafından oluşturulan Merkezi Sicil Kayıt Sistemi (MERSİS) üzerinde elektronik olarak da tutulmaktadır. Ticaret siciline yapılan kayıtlarda işin doğası gereği tacirin

²⁵ Berat DUMAN, “Anayasa Hukukunda Kişisel Verilerin Korunması”, **Selçuk Üniversitesi SBE**, Yayınlanmamış Doktora Tezi, 2020, s. 56.

²⁶ DUMAN, s. 142. Örneğin, AYM tarafından verilen bir kararda, 5429 sayılı Türkiye İstatistik Kanunu'nun 8. maddesiyle, vatandaşlara hiçbir sınırlama öngörmeksizin istatistiki birimlere istenilen bilgilerin verilmesi yükümlülüğü yükleyen kanun hükmü Anayasa'nın “Özel hayatın gizliliği” başlıklı 20. maddesi ile “Düşünce ve kanaat hürriyeti” başlıklı 25. maddelerine aykırı bulunarak iptal edilmiştir: AYM, E.2006/167, K.2008/86, K.t.: 20.3.2008. AİHM tarafından verilen bir kararda da ilgilinin rızası alınmaksızın açık ev adresinin ülke genelinde yayımlanan bir gazetede yer verilmesinin toplum menfaatleri için gerekliliğini ortaya koyabilecek haklı bir gerekçemim bulunmaması nedeniyle başvuranın özel hayata saygı hakkını ihlal niteliği taşıdığına karar verilmiştir: AİHM, Alkaya / Türkiye, B.n. 42811/06, T. 9.11.2012.

²⁷ AYM, E.2013/84, K.2014/183, T. 4.12.2014.

²⁸ Tüzel kişilerin verilerinin kişisel veri olarak kabul edilmesinin KVKK'nın ruhuna aykırı olacağı yönündeki görüş için bkz.: Onur BASKIN, **Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2021, s. 24. Hukuk düzeninin tüzel kişilere yönelik düzenlemeler yaparak haklarını koruması nedeniyle bunlara ait kişisel verilerin de koruma kapsamında olması gerektiği yönünde görüş için bkz.: AKGÜL, s.16. 6698 sayılı Kanun'da bulunmasa da tüzel kişilere ait kişisel verilerine mevzuatta dağınık olarak yer verildiğine ve özellikle İdarenin kamu hizmetleri bağlamında tüzel kişilerin verilerini korumakla sorumlu olduğuna ilişkin görüş için bkz.: Ceren KÜPELİ, **Tüzel Kişi Verilerinin Korunmasında İdarenin Sorumluluğu**, Adalet Yayınevi, Ankara, 2020, s.65 vd.

²⁹ Kuruma ait “İlgili Kişi Kimdir?” başlıklı yazı için bkz.: <https://www.kvkk.gov.tr/Icerik/2034/Ilgili-Kisi-Kimdir> (E.T. 27.8.2021). Aynı yönde görüş için bkz.: Oğuz ŞİMŞEK, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınevi, Şubat 2008, s.123.

kişisel bilgileri de kayıt altına alınmaktadır. Burada aslen ticari işletmenin sahibi ya da ortakları gibi bilgiler kaydedilmekle birlikte nihayetinde ortakların adı soyadı, kimlik numarası gibi nüfus bilgileri ile imzası gibi gerçek kişiye ait kişisel verilerin de kayıt altına alınarak işlenmesi söz konusudur.

6102 sayılı TTK'nın 24. maddesine 2012 yılında eklenen 5. fıkrasına göre "*Ticaret sicili kayıt işlemlerinin elektronik ortamda yapılması için toplanması ve işlenmesi gerekli olan kişisel veriler, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin mevzuata uygun bir şekilde korunur*" hükmüne yer verilmiştir. Veri güvenliğine ilişkin ayrıntılı düzenleme ise 27 Ocak 2013 tarihli Resmî Gazete'de yayımlanan Ticaret Sicil Yönetmeliği'nin 14. maddesiyle yapılmıştır. Burada veri güvenliğinin sağlanabilmesi için bazı teknik önlemlerin alınması öngörülmüştür. Öte yandan, gerek 6102 sayılı Kanunun 35. maddesinde gerekse de Ticaret Sicil Yönetmeliğinin 15. maddesinde "açıklık" ilkesi benimsenerek herkesin ticaret sicillerinde saklanan tüm senet ve belgeleri inceleyebileceği ve isterse ücreti mukabilinde bu belgelerin onaylı suretlerini alabileceği düzenlenmiştir. 6698 sayılı KVKK'nın 8. maddesinde kişisel verilerin aktarılması konusu düzenlenmiştir. Buna göre kural olarak kişisel veriler ilgisinin açık rızası olmaksızın aktarılamaz. Ancak, maddenin ikinci fıkrasının (a) bendinde "*5 inci maddenin ikinci fıkrasında belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir*" ifadesine yer verilmiştir. Kanunun bu atfı takip edildiğinde³⁰ madde 5/2(a) uyarınca TTK'da açıkça öngörüldüğü için ticaret sicillerinde bulunan belgelerin gerçek kişilere ait kişisel veri içermesi halinde dahi isteyen herkese aktarılabilmesi söylenebilir. Ancak, TTK'nın 24/5 maddesi göz önünde bulundurulduğunda, söz konusu evraklarda bulunan kişisel verilerin, özellikle kimlik numaralarının karartılarak paylaşılması gerektiği söylenebilir.

Ticaret Sicil Yönetmeliğinin 15. maddesinde ise herkesin sicil içeriğini ve saklanan tüm senet ve belgeleri inceleyebileceği ifade edildikten sonra sicil defterlerinin sicil dairesinden dışarıya çıkarılması yasaklanmış, ayrıca sicil müdürünün defterlerin incelenmesi sırasında kişisel verilerin korunmasına yönelik gerekli önlemleri alması zorunlu kılınmıştır. Görüldüğü üzere, Yönetmelikte kabul edilen önlemlerden birisi sicil defterlerinin daire dışına çıkarılmasının önlenmesidir. Bunun dışında gerekli önlemlerin sicil müdürü tarafından alınması öngörülmüştür. Bu bağlamda evraklar üzerindeki

³⁰ **MADDE 5-** (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

T.C. kimlik numaraları, imzalar, ortaklara ait iletişim numaraları gibi kişisel bilgilerin karartılarak paylaşılması alınabilecek önlemlerdendir.

Benzer durum, ticaret sicilindeki bilgilere elektronik ortamda erişilmesi hali için de mevcuttur. Ticaret ve sanayi odaları ile ticaret odaları binalarında bulunan bilgisayarlardan sicildeki belge ve dokümanlara erişim mümkün idi. Ticaret Sicili Yönetmeliği'nin 15. maddesinin 3. fıkrasında elektronik ortamlarda yapılacak incelemelerde de kişisel verilerin korunması ve bilgi güvenliğini sağlayacak tedbirlerin alınması öngörülmüştür. Bununla birlikte, uygulamada bazı odalar sicildeki dosyalara erişim için ilgisinden alınmış yetki ya da izin belgesi talep etmektedir³¹. Ancak, 6102 sayılı Kanunun 35. maddesinin ikinci fıkrasında *“Herkes ticaret sicilinin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebileceği gibi giderini ödeyerek bunların onaylı suretlerini de alabilir”* denilmekte ve herhangi bir istisna öngörülmemektedir. Ticaret Sicil Yönetmeliği'nde kişisel verilerin korunmasına ilişkin gerekli tedbirler alınacağı belirtilmişse de bu tedbirlerin ne olduğu açıkça belirlenmemiştir. İlgilinin yazılı açık rızasının aranması ise gerek KVKK'ye gerek TTK'ye uygun değildir. Nitekim, KVKK kişisel verilerin kanunlarda öngörülmesi halinde ilgisinin açık rızası olmaksızın paylaşılabilmesini öngörmekte, TTK ise ticaret sicillerinin herkese açık olduğunu kabul etmektedir. TTK'de kişisel verilerin korunmasına ilişkin mevzuata uygun önlemler alınabileceği düzenlenmişse de alınacak önlemler kanuna aykırı olamaz. Bu sebeple, ticaret sicillerinde bulunan dosyalara erişim için ilgisinden alınmış yetki ya da izin belgesi aranması uygulaması hukuka uygun değildir. Kaldı ki, KVKK dahi ilgisinden alınan açık rızasının yazılı olmasını şart koşmamaktadır. İleride açıklanacağı üzere, açık rızanın yazılı olması zorunluluğu bulunmamaktadır.

Bu konuda değinilmesi gereken diğer bir husus, ticaret odalarına ait web sitelerinden erişilebilen bilgilerdir. Bazı odalara ait web sitelerinde kendilerine kayıtlı ticari işletmeler hakkında herhangi bir bilgi yer almazken, bazılarındaysa üyelerinin sadece ticari unvanı ya da bu unvanla birlikte şirkete ait telefon numaraları bilgisi bulunmaktadır. KVKK kapsamında sadece gerçek kişilere ilişkin bilgilerin kişisel veri olarak kabul edildiği düşünüldüğünde şirketlere ait telefon numaraları ve adres bilgilerinin erişilebilir olması bu kanun kapsamında sorun teşkil etmemektedir. Ancak, bazı ticaret odalarına ait web sitelerinde yer alan “Bilgi Bankası” sekmesinden ticari şirketlerin isimleriyle birlikte sahiplerinin ve ortaklarının da adı ve soyadı bilgilerine erişim imkânı verilmektedir. İlgili web sitesinde bulunan arama motoruna ismi ve kimlik numarası bilgileri girilen gerçek kişi hakkında, ortağı, yönetim kurulu üyeliği veya yetkilisi bulunduğu bir ticari işletme olup olmadığı bilgisine erişmek mümkündür. Ayrıca, meslek grubuna göre arama yapıldığında herhangi bir semtte ve herhangi bir firma türünde arama yapılarak

³¹ 6102 sayılı Türk Ticaret Kanunu'nun 24. maddesi uyarınca Ticaret Bakanlığı tarafından il merkezlerindeki ticaret ve sanayi odaları ile ticaret odalarında faaliyet gösterecek ticaret sicil müdürlükleri kurulmuştur. Bu sebeple, sicillerdeki belge ve dokümanlara erişmek isteyenler odalarda bulunan bu müdürlüklere başvurmaktadır.

erişilen ticari işletmeye ait firma unvanı, iş adresi ve oda sicil numarası gibi bilgilerin yanında işletmenin yetkili ve/veya ortaklarının adı ve soyadı bilgilerine ulaşılabilmektedir.

Tüzel kişiye ait bir verinin gerçek bir kişiyi belirlemesi ya da belirlenebilir kılması halinde bu verilerin de KVKK kapsamında korunması gerektiği Kişisel Verileri Koruma Kurumunca da ifade edilmiştir. O halde, şirket ortakları ve yetkililerinin ad soyad bilgilerine Odaların web sitelerinde yer verilmesinin KVKK kapsamında bir sorun teşkil edip etmediği sorusu gündeme gelmektedir. 6102 sayılı Ticaret Kanunu'nda ya da 5174 sayılı Türkiye Odalar ve Borsalar Birliği ile Odalar ve Borsalar Kanunu'nda bu bilgilerin internet ortamında Odalar tarafından yayımlanmasına ilişkin açık bir hüküm bulunmamaktadır. Bununla birlikte Kurul tarafından verilen bir kararda Odaların kanunla kendilerine yüklenen hukuki yükümlülükleri gereği ticaret siciline işlenen bilgileri web sitelerinde yayımlayabilmelerinde hukuka aykırılık görmemiştir³².

1.2.1. Hayatta Olmayan Kişilere Ait Verilerin Durumu

Kişisel verilerin korunması hukuku bağlamında irdelenmesi gereken önemli meselelerden biri, hayatta olmayan kişilere ait verilerin koruma kapsamında değerlendirilip değerlendirilemeyeceğidir. Ölüler için kişisel veri korumasının kural olarak bulunmadığı; ancak ölüye ait verinin hayatta olan bir kişiyle bağlantılı olması sebebiyle yaşayan bu kişinin belirlenebilir duruma gelmesi halinde bunun da kişisel veri olacağı ifade edilmektedir³³. Örneğin ölünün kalıtsal bir hastalığı olduğuna dair sağlık verisi hayatta olan aile bireylerine etki edebilecektir.

Türk Medeni Kanunu'nun 28. maddesine göre kişilik ölümle sona ermektedir. Ölen kişinin hak ve borçlara sahip olma imkânı ortadan kalkmaktadır³⁴. Ölen kişinin kişi varlığı hakları sona ererken malvarlığı hakları da mirasçılara geçmektedir³⁵. Dolayısıyla ölen kişiye ait kişisel verilerin koruma altında olmadığı söylenebilir. Bununla birlikte mevzuatımızda sağlık verilerine ilişkin bazı

³² 6102 sayılı Türk Ticaret Kanunu'nun 24. maddesi gereği ticaret sicillerinin ticaret odaları içerisinde bulunduğu, dolayısıyla ticaret siciline kaydedilen bilgilerin halihazırda ticaret odası bünyesinde mevcut olduğu ifade edildikten sonra "Ayrıca, ticaret sicil gazetesinde yer alan bir bilginin ticaret odasının sayfasında bulunmasındaki amacın yine ticaret sicil işlemlerine ilişkin bilginin daha kolay ulaşılabilir olmasını sağlamak adına gerçekleştirildiği, bununla birlikte söz konusu bilgiye yalnızca ilgilileri tarafından ticaret odasının sayfasındaki bilgi bankası platformundan firma bilgileri girilmek suretiyle erişildiği, söz konusu bilginin ticaret sicil gazetesinde yayınlanma amacından farklı bir amaçla yayınlandığına ilişkin herhangi bir emare bulunmadığı dikkate alındığında söz konusu kişisel veri işleme faaliyetinin Kanun'un Genel İlkeler başlıklı 4 üncü maddesinde yer alan "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine de aykırılık teşkil etmediği, diğer yandan söz konusu bilginin ilgili kişi tarafından da belirtildiği üzere doğru olduğu ve yayınlanmasında amaca aykırılık bulunmadığı" sonucuna ulaşılmıştır KVK Kurulu, 6.1.2022 tarih ve 2022/6 sayılı kararı, <https://www.kvkkarar.com/2022-6/> (E.T. 1.9.2022).

³³ Mesut Serdar ÇEKİN, **Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, 3. Baskı, İstanbul, Temmuz 2020, s. 44. Hayatta olmayan kişiler için kişisel veri korumasının Avrupa Birliği Veri Koruma Tüzüğü (GDPR) bakımından da geçerli olmadığına dair bkz.: BYGRAVE, Lee A./ TOSONI, Luca, "Article 4(1). Personal Data", **The EU General Data Protection Regulation (GDPR) A Commentary**, Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY (Eds.), Oxford University Press, 2020, s.113.

³⁴ Mehmet AYAN, / Nurşen AYAN, **Kişiler Hukuku**, 8. Baskı, Seçkin, Ankara, Ekim 2016, s.171.

³⁵ BASKIN, s.27.

düzenlemelere yer verilmiştir. Örneğin, Hasta Hakları Yönetmeliği'nin³⁶ 21. maddesinin 3. fıkrasına göre “Ölüm olayı, mahremiyetin bozulması hakkını vermez.” Ayrıca, Kişisel Sağlık Verileri Hakkında Yönetmelik'in³⁷ 11. maddesine göre ise ölen kimsenin sağlık verileri yalnızca murisin yasal mirasçılarınca alınabilirken, bu veriler en az yirmi yıl süreyle saklanacaktır.

Hal böyleyken, ölen kişiye ait bazı bilgilerin, örneğin sosyal medya hesapları ya da sağlık verileri gibi, kişisel veri korumasına dahil edilip edilmemesi hususu tartışmalıdır. Sosyal medya hesaplarının dijital bir miras olarak kabul edilmesi ve bu sebeple ölenin mirasçılarına bu hesaplara erişim imkânı verilmesi gerektiğine yönelik bazı yargı kararları mevcuttur. Amerikalı bir askerin Irak'ta görev yaparken ölmesi üzerine e-posta hesabına erişmek isteyen ailesini haklı bulan yargı kararı, Almanya'da ölen kişinin sosyal medya hesabına ailesi tarafından erişim sağlanması gerektiğine külli halefiyet prensibi uyarınca kabul eden yargı kararı ve murisin mailinin, sosyal medya hesaplarının ve dijital cüzdanlarının mirasçılara intikal etmesi gerektiğine karar veren Antalya Bölge Adliye Mahkemesi 6. Hukuk Dairesi'nin E.2020/1149, K.2020/905 sayılı kararları bunlara örnek olarak verilebilir³⁸.

Ölen kişinin sağlık verilerinin kullanılması hususu da sorundur. Nitekim, ölen kişiden açık rıza alınması mümkün olmadığına göre bunların sadece anonimleştirilmek suretiyle kullanılabileceği söylenebilir³⁹. Öte yandan, sağlık verilerinin öldükten sonra kullanılmasına dair kişinin hayattayken izin vermesini teşvik etmenin yararlı olacağı da ifade edilmektedir⁴⁰.

Belirtmek gerekir ki, ölen kişiye ait bazı verilerin korunmaması o kişinin anısına zarar verebilecek niteliktedir. Örneğin, kişinin sosyal medya hesaplarındaki özel yazışmaları, e-posta adreslerindeki yazışmalar ya da ölen kişinin hayattayken kimsenin bilmesini istemediği bir hastalığının olduğuna dair sağlık verisinin kişinin öldükten sonraki anısına zarar verebileceği, dolayısıyla, tıpkı hayatta olduğunda bu bilgilerin korunduğu gibi öldükten sonra da korunmasını isteyebileceği fikri göz ardı edilmemelidir. Bu sebeple, parasal değeri olan sosyal medya ve çeşitli bulut hesaplarının miras olarak kabul edilerek mirasçılara verilmesi ile kişinin yaşadığı dönemdeki özel hayatının gizliliğinin öldükten sonra da korunması gibi iki önemli hususun çatışmasından doğacak sorunlara mevzuatta çözüm bulunması gerekmektedir.

Ölen kişiyi ölümünden sonra da korumaya yönelik iki teori bulunmaktadır. Bunlardan ilki “hatıranın korunması teorisi” olarak ifade edilmektedir. Bu teoriye göre ölen kişinin kişiliğine yapılan saldırı, örneğin hakkında yapılan yalan haberler yahut doğru olmakla birlikte kamu yararı bulunmayan

³⁶ RG, 1.8.1988/23420.

³⁷ RG, 21.6.2019/30808.

³⁸ Bu kararlara ilişkin ayrıntılı bilgi için bkz.: Yasemin MARAŞLI DİNÇ, “Ölümden Sonra Sosyal Medya Hesaplarının Hukuki Akıbeti: Dijital Miras”, **TBB Dergisi**, 2019 (142), s. 273-287.

³⁹ BASKIN, s.28.

⁴⁰ David M. SHAW/Juliane V. GROSS/Thomas C. ERREN, “Data Donation After Death”, **Embo Reports**, Vol.: 17, Issue: 1, January 2016, <https://doi.org/10.15252/embr.201541802> (E.T. 1.9.2021).

haberler, ölenin yakınlarını zedeleyebilir; çünkü ölenin hatırası ardında bıraktığı yakınları için devam etmektedir⁴¹. Bu sebeple, ölenin yakınları bu saldırıların durmasını talep edebileceği gibi maddi ve manevi tazminat talebinde de bulunabilir. Görüldüğü üzere, bu teoride korunan ölenin kişilik hakkı değil; yakınlarının kişilik hakkı olmaktadır⁴². TMK m.28 uyarınca ölenin kişiliği ve hak ehliyeti sona ereceğinden, hatıranın korunması teorisi Türk hukuk sistemi için de uygun görünmektedir. Ayrıca, 5237 sayılı Türk Ceza Kanunu'nun 130. maddesinde kişinin hatırasına hakaret suç olarak kabul edilmiştir⁴³. Burada da korunan değer, kişinin şeref ve haysiyeti değil, hatırası olduğu ifade edilmektedir⁴⁴.

Ölen kişinin kişiliğinin sona ermediği ve dolayısıyla korunması gereken bir değer olarak varlığını sürdürdüğüne yönelik ikinci teori ise “uzatılmış kişilik hakkı teorisi” olarak ifade edilmektedir. Alman hukuk doktrininde savunulan bu görüş uyarınca, kişi hayatını kaybetse de kişilik hakkına yönelik bazı değerlerin korunması gerekeceğinden bu kişiliğin korunması için ölenin yakınlarının ölene yapılan saldırılardan zarar görmesine yahut kişiliğin korunması için yakınlarının iradesine ihtiyaç yoktur⁴⁵. Bunun için ölümünden önce kişi, ölümüyle birlikte devam edecek kişilik değerlerinin korunması, yapılan saldırıların durdurulması için talepte bulunabilecek bir kişi yahut bir kurum tayin edebilir.

Yukarıda ifade ettiğimiz üzere, bazı kişisel verilerin kişinin ölümünden sonra ortaya çıkması, bilinmesi kişinin toplumdaki anısına zarar verebilecek nitelikte olabilir. Ancak, burada kastettiğimiz hatıranın korunması teorisinde olduğu gibi sadece yakınlarının psikolojisini etkileyecek, onların kişilik haklarını zedeleyecek türde bilgilerin ortaya çıkması değildir. Bunun da ötesinde bazı kişisel verilerin ilgisince ölümünden sonra dahi hiçbir zaman bilinmesini istemeyeceği türden verilerin olabileceğini ifade etmek istiyoruz. Bu veriler ölen kişinin hayattayken sahip olduğu bazı kötü alışkanlıklara ilişkin yazışmaları veya cinsel yollarla bulaşan bir hastalığı olduğuna ilişkin sağlık bilgileri olabilir. Bu bilgilerin her zaman ölenin yakınlarına zarar verebileceği, onların psikolojilerini bozacağı söylenemese de ölenin ardında bıraktığı izlenimi, anıyı olumsuz etkileyebilecek türden olabilir. İşte bu sebeplerle, ilgiliye ait söz konusu kişisel verilerin ilgilinin ölümünden sonra dahi korunması gerektiği kabul edilmelidir⁴⁶. Bu koruma, uzatılmış kişilik hakkı teorisinde olduğu gibi ilgili kişinin ölümünden önce bu tarz verilerinin korunması için bir kişi tayin etmesi yoluyla sağlanabileceği gibi kişinin kişisel verilerinin

⁴¹ Gamze TURAN BAŞARA, “Kişiliğin Korunması Kapsamında Ölümünden Sonra Hatıranın Korunması Teorisi”, **ÇÜHFD**, C.5, S.1, Nisan, 2020, s. 343.

⁴² TURAN BAŞARA, s. 342.

⁴³ Madde 130: (1) Bir kimsenin öldükten sonra hatırasına en az üç kişiyle ihtilat ederek hakaret eden kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Ceza, hakaretin alenen işlenmesi halinde, altıda biri oranında artırılır. (2) Bir ölünün kısmen veya tamamen ceset veya kemiklerini alan veya ceset veya kemikler hakkında tahkir edici fiillerde bulunan kişi, üç aydan iki yıla kadar hapis cezası ile cezalandırılır.

⁴⁴ Ayrıntılı bilgi için bkz.: Ezgi CANKURT, “Kişinin Hatırasına Hakaret Suçu (TCK m.130)”, **Beykent Üniversitesi Hukuk Fakültesi Dergisi**, C.1, S.1, 2015, s. 147-176.

⁴⁵ TURAN BAŞARA, s. 344.

⁴⁶ ŞİMŞEK, aksi yöndeki görüşünde, kişisel verilerin korunması hakkının bireyin kişisel verileri üzerindeki belirleme hakkını koruması nedeniyle hak sahibinin yaşayan gerçek bir kişi olması gerektiğini, dolayısıyla ölmüş kimsenin kişisel verilerinin korunması hakkının doğrudan muhatabı olamayacağını ifade etmektedir: ŞİMŞEK, s.123.

ölümünden sonra kimlere iletilebileceğini çeşitli veri türleri için ayrı ayrı değerlendirmek suretiyle seçmesi yoluyla da sağlanabilir⁴⁷.

Öte yandan henüz doğmamış olan ceninlerin kişisel verilerinin koruma altında olup olmadığına ilişkin de iki farklı görüş mevcuttur. Bir görüş kişisel veri korumasının mümkün olmadığını veri koruma hukukunun kişiye sunduğu bilgilendirme, aydınlatma, silme talepleri gibi imkânların doğmamışlar için işlevsel olmayacağı gerekçesiyle savunmaktayken⁴⁸, diğer görüş kişinin hak ehliyetini sağ ve tam doğmak şartıyla ana rahmine düştüğü an itibarıyla kazanıyor olmasından hareketle cenine ait bilgilerin de kişisel veri kabul edilmesi gerektiği yönündedir⁴⁹.

Hak ehliyeti, kişinin hak sahibi olabilmesi ve borç altına girebilmesi anlamına gelmektedir⁵⁰. Kişi, hak ehliyetine sağ doğmak şartıyla ana rahmine düştüğü an itibarıyla sahip olmaktadır. Böylelikle, henüz doğmamış da olsa cenin diğer insanların sahip olduğu tüm haklara sahip olabilme ehliyetini haizdir. Kişisel verilerin korunması hakkı da bu haklardan biridir. Örneğin, ceninin anne karnındayken kayıt altına alınan sağlık verilerinin sağ doğmak şartıyla ilgisine ait kişisel veri olarak kabul edilmesi gerekir. Bu bağlamda, kişisel verilerin korunması hakkı gereği ilgisine tanınan hakların onun velisi/vasisi tarafından kullanılması gerekecektir.

1.2.2. Kimliği Belirli veya Belirlenebilir Olma

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgi olarak tanımlanmaktadır. Kimliği belirli kişi, var olan bilgiler dışında başkaca bir işleme yahut bir bilgiye ihtiyaç duyulmaksızın ilgili kişiyle bağlantı kurmayı sağlayan veriler, şeklinde ifade edilebilir. Örneğin, ilgili kişiye ait kimlik numarası, doğum tarihi, adresi ile adı ve soyadı bilgilerinin başkaca bir bilgiye ihtiyaç duyulmaksızın kimi işaret ettiği söylenebilir⁵¹.

Bununla birlikte, bazı bilgiler mevcut olmakla birlikte, kişinin tespit edilebilmesi için başka bilgilere ihtiyaç duyuluyorsa, eklenen yeni bilgiler ile ilgili kişi tespit edilebilir hale geliyorsa, bu halde de kimliği belirlenebilir gerçek kişiye ait kişisel veriler söz konusudur⁵². Örneğin, internete bağlanan her bilgisayar için atanan IP adresleri (internet protocol) bilgisayar kullanıcısının belirlenmesi için yeterli değildir çünkü kullanıcısının kimliğine ilişkin bilgi içermemektedir. Ancak IP adresleri internet sağlayıcıları tarafından kişiye özel atandığından, bu sağlayıcıların sistemleri sayesinde IP adresinin kime

⁴⁷ Çeşitli sosyal medya hesapları hesap sahiplerine ölümünden sonra nasıl bir yol izlenmesi gerektiğine yönelik tercih hakkı sunmaktadır: Necdet ÇALIŞKAN, “Öldükten sonra sosyal medya hesaplarınız ne oluyor?”, **Habertürk**, 19.12.2020, <https://www.haberturk.com/oldukten-sonra-sosyal-medya-hesaplari-ne-oluyor-haberler-2907289-teknoloji> (E.T. 2.9.2021)

⁴⁸ ÇEKİN, s. 44.

⁴⁹ Yasin AYDOĞDU, “Kamu İdaresinde Kişisel Verilerin Korunması”, **SÜHFD.**, C.29, S.1, 2021, s. 267, dn.: 6; BASKIN, s.27.

⁵⁰ O. Gökhan ANTALYA / Murat TOPUZ, **Medeni Hukuk**, Cilt 1, Seçkin Yayıncılık, 4. Baskı, 2021, Ankara, s. 121.

⁵¹ AKGÜL, s. 17.

⁵² Firdevs YÜZBAŞI TOBAZ, “Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması”, **Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü**, Doktora Tezi, 2021, s. 50.

ait olduğu belirlenebilir. Dolayısıyla, IP adresi de tek başına “kimliği belirlenebilir kişi”ye ait olduğundan bir kişisel veri olarak kabul edilmektedir⁵³.

2. ÖZEL NİTELİKLİ (HASSAS) KİŞİSEL VERİ KAVRAMI

Özel nitelikli kişisel veriler, yukarıda tanımladığımız kişisel verilerin bir alt kategorisini oluşturmakta olup genel olarak bilinmesi halinde ilgisinin toplumda bir ayrımcılığa uğraması ihtimalini doğurma potansiyelini taşıyan ve bu sebeple daha fazla koruma altına alınan verilerdir⁵⁴. Bu veriler 6698 sayılı KVKK’de tahdidi olarak sayılmıştır. Başka bir ifadeyle sınırlı sayıda belirlenen bu hassas verilerin kıyas yoluyla genişletilmesi mümkün değildir. Söz gelimi, veri sahibi kişi gelir kaynaklarının ve bunları nereye harcadığına ilişkin bilgilerin kendisi için oldukça hassas bilgiler olduğunu savunarak özel nitelikli veriler için belirlenen kurallara tabi olarak korunmasını talep edemeyecektir⁵⁵.

Kanunun 6. maddesine göre, “*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir*”.

Türk Hukukunda böyle olmakla birlikte, ihtiyaca göre bazı ülkelerde farklı tür veriler özel nitelikli kişisel veri kapsamında kabul edilebilmektedir. Örneğin, destek ve sosyal refah yardımları, internet üzerinden yapılan satın almalar ile alkol ve uyuşturucu kullanımı gibi veriler çeşitli ülkelerde hassas kişisel veri olarak kabul edilmektedir⁵⁶. Ayrıca, gerek 95 sayılı Direktif gerekse de bunun yerini alan AB Veri Koruma Tüzüğü’nde (GDPR) özel nitelikli kişisel veriler arasında sayılmamasına karşın mali veriler Danimarka, Finlandiya, Yunanistan, Hollanda, Portekiz ve Fransa veri koruma kanunlarında hassas nitelikli veri olarak kabul edilmiştir⁵⁷.

Özel nitelikli veriler, kişiler için daha ciddi sonuçlar doğurabilir. Bu nedenle, bu verilerin daha sıkı kurallarla korunması gerekir. Hangi verilerin bu özel korumadan yararlanacağını net bir şekilde belirlemek için, özel nitelikli verilerin türlerinin sınırlı sayıda ve açıkça listelenmesi önemlidir. Bu

⁵³ KVK Kurulu, 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar, s. 19.

<https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVA%20PLAR.pdf> (E.T. 8.9.2021); YÜZBAŞI TOBAZ, s.51; ÇEKİN, s.47.

⁵⁴ Metin BULUT, “Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler”, **Ankara Barosu Dergisi**, 2020/3, s.109; AKGÜL, s.19. Özel nitelikli kişisel verilerin ortaya çıkışının özellikle İkinci Dünya Savaşı’nda yaşanan olaylara dayandığına dair bkz.: Sevgi TÜRKMEN, “Özel Nitelikli Kişisel Veri Kavramının Ortaya Çıkışı, Gerekliliği ve Özel Nitelikli Kişisel Veri Tanım ve Kapsamları”, **Lexpera Blog**, 18.10.2019, <https://blog.lexpera.com.tr/ozel-nitelikli/> (E.T. 27.8.2021).

⁵⁵ Halil ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, Adalet Yayınevi, Ankara, 2021, s.25.

⁵⁶ BULUT, s.111.

⁵⁷ AKGÜL, s.23.

yaklaşım, kuralların hangi verilere uygulanacağını kesin olarak ortaya koyar. Farklı kuralların öngörüldüğü hallerin gerek veri sahipleri tarafından gerekse de veri sorumlularınca öngörülebilebilir olması karmaşık bir durumu basitleştirmesi bakımından faydalıdır. Bununla birlikte, bu çözüm yönteminin eksik yanlarının bulunduğu da ifade edilmelidir. Örneğin, Avrupa Veri Koruma Tüzüğü uyarınca fotoğraf özel nitelikli bir veri olarak kabul edilmemektedir. Bu durum 51 no’lu gerekçede şu şekilde ifade edilmektedir:

“Fotoğrafların işlenmesi sistematik olarak özel kategorilerdeki kişisel verilerin işlenmesi olarak değerlendirilmemelidir, çünkü bunlar yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya kimlik doğrulamasına izin veren belirli bir teknik araçla işlendiğinde biyometrik veri tanımı kapsamına girmektedir.”⁵⁸

6698 sayılı Kanunun 6. maddesinde de fotoğraf, özel nitelikli veriler arasında sayılmamıştır. Yalnızca biyometrik olması halinde fotoğrafın hassas veri olarak kabul edilmesi söz konusudur. Ancak bazı durumlarda bir fotoğraf verisinin işlenmesi, en az diğer hassas veriler kadar ilgisine zarar verebilir. Örneğin, dini kıyafetler giyen, belirli saç stili, bıyığı, gözlüğü bulunan kişi hakkında bir fotoğrafı üzerinden ırkı, dini ve siyasi görüşü ile sağlığı hakkında kolayca çıkarımda bulunulabilecektir. Öte yandan, bir kişinin yüz ya da boy fotoğrafından madde bağımlısı olup olmadığı anlaşılabilmekte ya da sosyal medya platformlarına yükledikleri fotoğraflardan ilgisinin depresyonda olup olmadığı tespit edilebilmektedir⁵⁹. Amerika’da yüz fotoğrafları üzerinden ilgililerin Demokrat ya da Cumhuriyetçilerden oldukları yüksek oranda doğru şekilde tespit edilebilmiştir⁶⁰.

Öte yandan, bir dini grup lideri ile herhangi bir vatandaşın dini görüşlerine ilişkin verisinin işlenmesi aynı sonucu doğurmayacaktır. Belki de dini grup lideri, bu bilginin paylaşılmasını daha olumlu bir durum olarak görmektedir. Özel nitelikli veriler tahdidi olarak sayılırken ilgisinin ayrımcılığa uğraması ya da maddi manevi kayıplarının daha fazla olması kriteri gözetilecekse, örneğin bir kişi, ailesi ve yakınları tarafından sigara ve alkol kullandığına dair verinin paylaşılmasındansa kolunun kırıldığına dair sağlık verisinin işlenmesini yeğleyebilecektir. Çünkü alkol ve sigara tüketimine dair bilginin yayılması, dindar bir çevresi bulunan kişi için çok daha ağır sonuçlara yol açabilir.

Hassas kişisel verilerin sınırlı sayıda (numerus clausus) belirlenmesine yönelik eleştirel yaklaşımlar literatürde mevcuttur. Bu bağlamda iki temel görüş öne çıkmaktadır: Birinci yaklaşım, 'bağlamsal görüş' olarak adlandırılmakta olup, bir verinin hassas nitelikte olup olmadığının değerlendirilmesinde, verinin işlenme koşulları ve mevcut şartların bütüncül olarak ele alınması gerektiğini savunmaktadır. Bu görüş, veri sahiplerinin menfaatleri, verinin alıcıları ve toplanma amacı

⁵⁸ <https://gdpr-info.eu/recitals/no-51/>.

⁵⁹ Daniel J. SOLOVE, “Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data”, **118 Northwestern University Law Review**, 1081 (2024), GWU Legal Studies Research Paper No. 2023-22, 21.1.2024, s. 1123, <http://dx.doi.org/10.2139/ssrn.4322198> (E.T. 3.7.2024).

⁶⁰ SOLOVE, “Data Is What Data Does...”, s.1124.

gibi çoklu faktörlerin göz önünde bulundurulmasını öngörmektedir⁶¹. İkinci yaklaşım ise 'amaçsal görüş' olarak tanımlanmakta ve bir verinin hassas niteliğinin, işleme amacına göre belirlenmesi gerektiğini ileri sürmektedir. Bununla birlikte, her iki görüş de belirli eleştirilere maruz kalmaktadır. Bağlamsal görüş, uygulamada sektörel düzenlemelerin gerekliliği ve bunun getireceği yüksek maliyetler nedeniyle eleştirilmektedir. Amaçsal görüş ise, somut olaylarda verinin hassas niteliğini belirleyecek otoritenin belirsizliği sebebiyle eleştirilere konu olmaktadır⁶². Bu tartışmaların, yukarıdaki örnekler de düşünüldüğünde, kişisel verilerin korunması hukukunda hassas veri kavramının sınırlarının belirlenmesi ve uygulanması konusundaki zorlukları yansıttığı söylenebilir.

SOLOVE'a göre, neredeyse her türlü veri bir şekilde hassas sayılabilecek bilgiler içerebildiğinden veri türüne dayalı basit ayrımlar günümüz çıkarım (inference) çağında yetersiz kalmaktadır. Bunun yerine, yasal düzenlemeleri verilerin kullanımından kaynaklanan zarar ve risklere orantılı bir şekilde uyarlayacak "risk-zarar" yaklaşımı benimsenmelidir. Nitekim modern teknoloji çağında veri analitiği ve algoritmaların yardımıyla bunu sağlamak mümkündür⁶³.

Hassas verilerin belirlenmesine ilişkin tartışmaların devamı bireylerin özel hayatın gizliliği hakkını daha üst düzeyde korunmasını sağlamak bakımından önemlidir. Ancak, mevcut şartlar üzerinden düşünüldüğünde, örneğin fotoğraf verisinin, ilgisi hakkında farklı özel nitelikli veri çıkarımı yapılabilir nitelikte olsa bile, doğrudan özel veri olarak kabul edilmesi mümkün görünmemektedir. Bununla birlikte, fotoğrafın hangi amaçla işlendiğine bakılarak farklı bir sonuca varılabilir. Söz gelimi, kişilerin dini ve siyasi görüşlerine ilişkin bilgilerin tutulduğu dosyada bu bilgileri doğrulamak amacıyla ilgisinin fotoğraflarına yer verilmiş olması halinde fotoğraf özel nitelikli veri olarak kabul edilebilmelidir. Ancak, ilgisinin kişisel yaşam alanında daha büyük önem arz ettiğini ileri sürerek özel nitelikli veriler arasında sayılmayan bilgilerinin de bu kapsamda işlenmesine yönelik talebi kabul edilmeyecektir. Yukarıda verilen alkol ve sigara kullanımına ilişkin bilginin paylaşımı, bu duruma örnektir.

3. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ

Bugünkü anlamıyla olmasa da "kişisel veriler" İdare için her zaman önemliydi. İdare eden, idare ettiği topluluk hakkındaki bilgileri kayıt altına alarak bunları düzeni sağlamak, ihtiyaçları karşılamak yahut idare eden konumunda kalmak için gereken eylemleri planlamakta kullanmaktaydı. Bu sebeple, idarenin veri kaydetmesini insanlık tarihi kadar eskiye dayandırmak mümkündür⁶⁴.

⁶¹ AKGÜL, s.22.

⁶² AKGÜL, s.22-23.

⁶³ SOLOVE, "Data Is What Data Does...", s.1136.

⁶⁴ Michael P. ROCH, "Filling the Void of Data Protection in the United States: Following the European Example", **Santa Clara High Technology Law Journal**, V.12, Issue:1, January, 1996, s.72. <https://digitalcommons.law.scu.edu/chtlj/vol12/iss1/3/> (E.T. 15.7.2021).

Kişisel verilerin korunmasına ilişkin tartışmalar özellikle İkinci Dünya Savaşı sonrasındaki teknolojik gelişmelerin artmasıyla başlamıştır. Bilgisayarın icadıyla birlikte idare topladığı verileri birbiriyle ilişkilendirmeyi sağlamış ve bu dönemde en büyük veri tekeli haline gelmiştir⁶⁵. Her ne kadar bütün idareler verileri kayıt altına alsa da elindeki verileri ilişkilendirerek devasa bir bilgi birikimi elde eden idarelerin bu gücü elde etmesinin teknolojiyi kullanabilme imkânıyla doğru orantılı olduğunu kabul etmek gerekir. Örneğin Amerika’da bilgisayarın icadıyla bilgi toplamacılığı büyük bir değişime uğramış, 1950’lerde verilerin toplanması, paylaşılması ve kullanılması önemli ölçüde artmış ve 1960’tan sonra mahremiyet / özel hayat (privacy) konusu tartışılır hale gelmiştir.⁶⁶

İdareler tarafından verinin toplanma ve kullanılma boyutu teknolojiyle doğrudan ilgili olsa da bu verilerin “kişisel veri” olarak belirli kanuni düzenlemelerle koruma altına alınması aynı tarihi doğrultuda seyretmemiştir. Örneğin, kişisel verilerin korunmasına yönelik ilk düzenleme Almanya’nın Hessen Eyaleti’nde 1970 yılında çıkarılmışken Amerika’da kişisel verilere ilişkin doğrudan yapılan ilk düzenleme olan “Özel Hayatın Gizliliği Kanunu” (The Privacy Act of 1974) bundan dört yıl sonra yürürlüğe konulmuştur⁶⁷.

Öte yandan, kişisel bilgilerin paylaşılmasının önüne geçilmesini hedefleyen kurallardan ilkinde Hipokrat Yemininde rastlanmaktadır. Bu metinde hekimlerin tedavi sürecinde yahut bunun dışında gördükleri ve işittikleri bilgiler hakkında sessiz kalacaklarına, bunları konuşmayacaklarına dair yemin etmeleri istenmektedir⁶⁸. Böylelikle günümüzde “hassas veri” olarak kabul edilen kişilerin sağlık verilerinin milattan önceki tarihten bu yana korunmaya çalışıldığı görülmektedir.

Özel hayatın korunması bağlamında kişisel bilgilerin korunmasına yönelik bazı kuralların ihtiyaç duyuldukça getirildiği görülmektedir. Amerika’da postaların başkalarının okunması 1825 yılında bir suç olarak kabul edilmiş, 1877 yılında ise Amerikan Temyiz Mahkemesi (The Supreme Court) kamu görevlilerinin bir postayı kanuni izinleri olmadıkça açmalarının yasak olduğuna karar vermiştir⁶⁹. Başka bir örnek, nüfus sayımına ilişkindir. Amerika’da, vatandaşlar hakkında daha ayrıntılı bilgileri toplama amacına yönelik olarak gerçekleştirilmeye başlanan nüfus sayımlarında toplanan bilgilerin gizliliği tartışma konusu edilmiştir. 1790 yılında yapılan sayımda yalnızca 4 soru sorulmaktayken, 1860 yılında soru sayısı, ekonomik durum, engelli çocuk, hastalık gibi çoğunluğu kişisel bilgilere yönelik olarak, 142’ye yükselmiştir. Toplumda bu bilgilerin güvenliği konusunda ortaya

⁶⁵ BAŞAR, s.134.

⁶⁶ Daniel J. SOLOVE, “A Brief History of Information Privacy Law”, **PROSKAUER ON PRIVACY**, PLI, 2006, s.24, https://scholarship.law.gwu.edu/faculty_publications/923/ (E.T. 15.7.2021).

⁶⁷ KÜZECİ, **Kişisel Verilerin Korunması**, s.103. The Privacy Act of 1974, United States Congress, 1974, 5 U.S.C. §552a.

⁶⁸ Hipokrat Andı’nda sır saklamaya ilişkin kısım şöyledir: “Gerek sanatımın icrası sırasında gerekse insanlarla gündelik ilişkideyken edindiğim bilgileri ortalığa saçmayacağım, bir sır olarak saklayacağım ve kimseye açmayacağım.” https://tr.wikipedia.org/wiki/Hipokrat_Yemini (E.T. 16.7.2021)

⁶⁹ SOLOVE, “A Brief History of Information Privacy Law”, s.7.

çıkan itirazlar üzerine 1919 yılında bu vesileyle edinilen bilgilerin kanuna aykırı şekilde kamuya açıklanması suç olarak kabul edilmiştir⁷⁰.

1960'lı yıllara gelindiğinde ise Amerika'da kişisel verilere ilişkin farklı bir sorun ortaya çıkmıştı: Kredi raporu. Başlangıçta küçük topluluklar halinde yaşayan insanların kazançları, harcamaları ya da borçlarını ödeyip ödemeyecekleri ayrıntılı bir araştırma yapılmadan bilinebilir durumdaydı. Ancak, kalabalıklar arttıkça güvenilir bilgilere erişmek zorlaştı. Bu sebeple ilki 1899 yılında olmak üzere Tüketici Raporlama Ajansları (Consumer Reporting Agencies -CRAs) kuruldu. Bu ajanslar kişiler hakkında topladıkları bilgilere istinaden özellikle bankalara, müşterilerinin borcunu ödeyebilecek potansiyele sahip olup olmadığına yönelik raporlar sunuyordu. Bilgisayarın icadı toplanan bilgilerin içeriğinin artmasını ve bu bilgilerin otomatik bir sistemle sınıflandırılarak kişiye özel kredi notu oluşturulmasını sağladı⁷¹. Ancak, değerlendirmeye alınan bilgilerin güncelliğini yitirmiş olması, kişilere ilişkin cinsel yönelim, alışveriş alışkanlıkları, sağlık harcamaları gibi bilgilerin de toplanması, daha da önemlisi toplanan bilgilere kişilerin erişim sağlayamaması 1960'lı yılların başında Ajansları tartışılır hale getirdi. Ajanslarca toplanan bilgilere bankalar rahatça erişebiliyorken, bu bilgilerin kimler tarafından toplanacağı, hangi amaçla kullanılacağı ve bilgilerin güvenliği konularındaki belirsizlik halkın tepkisine neden oldu⁷². İşte bu sebeple 1970 yılında "Adil Kredi Raporlama Yasası" (The Fair Credit Reporting Act - FCRA) çıkarıldı. Bu yasa uyarınca vatandaşlara kendileri hakkında toplanan bilgilerin bulunduğu dosyaya erişme, belirlenen rapor sonucuna ve toplanmış bilgilerin yanlış olduğuna ilişkin itirazda bulunma hakkı tanınmıştır⁷³.

1974 yılında çıkarılan Özel Hayatın Gizliliği Kanunu (The Privacy Act of 1974) ise soğuk savaş dönemine denk gelmektedir. Bu dönemde Amerikan Devletinin komünist komplolarına karşı korunmak amacıyla bireyler hakkındaki kişisel bilgileri fazlaca kayıt altına almaya başlaması Devletin sınırlandırılması ihtiyacını doğurmuştur⁷⁴. Bu kanunda, ajanslar tarafından tutulan kayıtların açığa çıkmasını sınırlamak, bireylere bu bilgilere daha fazla erişim imkânı tanımak, bireylerin bu kayıtlardaki eksiklik ve yanlışlıklar için düzeltme ile değişiklik talep etme hakkı vermek ve ajansların yasal normlara uymasını sağlamak adına "adil bilgi uygulamaları" kodu oluşturmak şeklinde dört temel amaç belirlenmiştir⁷⁵.

Avrupa'da Amerika'ya benzer şekilde teknolojinin gelişmesiyle özel hayatın gizliliğine yönelik tehlikeler artınca çeşitli düzenlemeler yapılmaya başlanmıştır. Doğrudan kişisel verilerin korunmasına

⁷⁰ SOLOVE, "A Brief History of Information Privacy Law", s.6.

⁷¹ DUMAN, s.10.

⁷² DUMAN, s.10.

⁷³ SOLOVE, "A Brief History of Information Privacy Law", s.28. Bu düzenleme, Ajansların kişisel verileri toplayabilmesini de garanti altına aldığından düzenlemenin finansal mahremiyetin azaltılmasına sebep olduğu sonucuna da varılabilir.

⁷⁴ Ayhan BOZLAK, **ABD Hukukunda Özel Hayatın Gizliliği Hakkının Korunması**, Beta, Ocak 2015, s.162, dn. 31.

⁷⁵ "Overview Of The Privacy Act Of 1974", **The United States Department Of Justice Archives**, <https://www.justice.gov/archives/opcl/policy-objectives> (E.T. 29.7.2021).

ilişkin çıkarılan ilk kanun olma özelliğini de taşıyan veri koruma kanunu Almanya'nın Hessen Eyaleti'nde 1970 yılında yürürlüğe konulmuştur. Bu kanun alanında ilk olmakla birlikte sadece çıkarıldığı eyalette uygulanması sebebiyle bölgesel bir düzenlemedir. Hessen Eyaleti'nde kabul edilen bölgesel yasadaki sonradan ulusal düzeyde uygulanan Federal Almanya Veri Koruma Kanunu ise 1977 yılında kabul edilmiştir.

Öte yandan Hessen Eyaleti'ndeki gibi bölgesel olmayıp, ulusal boyutta uygulanan ilk kanun ise İsveç'te 1973 yılında çıkarılmıştır⁷⁶. İsveç Veri Bankası Yasası özellikle devletin izni olmadan kişilere ait veri toplanmasını yasaklamıştır. Ayrıca, bu yasanın uygulanmasını sağlamak amacıyla "Veri İnceleme Kurulu" kurulmuştur. Buna göre Kurul, veri toplamak için lisans verilmesi ve veri bankalarının yasaya uygun şekilde çalışıp çalışmadığını kontrol etme yetkisini haizdir⁷⁷. 1973 tarihli İsveç'te çıkarılan yasayı, 1974'te ABD, 1977'de Federal Almanya ve 1978 yılında Fransa takip etmiştir. Diğer birçok Avrupa ülkesi ise kişisel verilerin korunmasına ilişkin düzenlemelerini Avrupa Birliği Konseyi ve Avrupa Parlamentosu tarafından çıkarılan kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/EC sayı ve 24.10.1995 tarihli Direktif'ten sonra yürürlüğe koymuştur⁷⁸.

Avrupa Birliği uygulamasıyla Amerika karşılaştırıldığında, AB'de kişi güvenliği bağlamında veri güvenliğine önem verilirken Amerika'da kişi güvenliğine ilişkin düzenlemelerde daha yavaş hareket edildiği ve açıkça gizlilik hakkı olarak veri gizliliğine yönelik düzenlemelerin yapılmadığı görülmektedir⁷⁹. Halbuki, mahremiyet/gizlilik hakkı ilk olarak 1890 yılında iki Amerikalı hukukçu Brandeis ve Warren tarafından ortaya konulmuştur. "The Right to Privacy" (Gizlilik Hakkı) adlı makalede gizlilik hakkı "kişiyi devlet ve diğer kişilerin hayatına zorla girmesinden koruyan yalnız kalma hakkı" olarak tanımlanmıştır⁸⁰. Makalede, taşınabilir kamera ve magazin haberciliğinin ortaya çıkması üzerine ileriye dönük olarak tahminlerde bulunulmuş, kişilerin kendi başına bırakılma hakkının (the right to be let alone) kanunlarla koruma altına alınması gerektiği anlatılmıştır. "*Son buluşlar ve iş yöntemleri, kişinin korunması ve bireye ... 'kendi başına bırakılma' hakkının güvence altına alınması için atılması gereken bir sonraki adıma dikkat çekiyor. Sayısız mekanik aygıt, 'dolapta fısıldanan şey, evin üstlerinden de söylenecektir' öngörüsünü doğrulamakla tehdit ediyor.*"⁸¹

⁷⁶ TURAN BAŞARA, s.130.

⁷⁷ ROCH, s.77.

⁷⁸ AKGÜL, s.185. İrlanda 1988; Belçika, İsveç ve Macaristan 1992; Estonya 1996; Yunanistan ve Polonya 1997; İngiltere, İsveç ve Portekiz 1998; Arnavutluk, Slovenya ve Finlandiya 1999; Hollanda ve Litvanya 2000; Bosna Hersek ve Bulgaristan 2001; Slovakya 2002 ve son olarak Türkiye 2016 yılında kişisel verilerin korunması bağlamında genel bir kanuni düzenleme yapan ülkeler arasındadır: YÜZBAŞI TOBAZ, s.121-122.

⁷⁹ ROSCH, s.88.

⁸⁰ Samuel D. WARREN/Louis D. BRANDEIS, "The Right to Privacy", **Harvard Law Review**, Vol: IV, December 15, 1890, No.5. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (E.T. 28.7.2021).

⁸¹ WARREN/BRANDEIS, §4.

Kişisel verilerin korunmasına ilişkin ilk uluslararası metin Ekonomik İş Birliği Örgütü (OECD) tarafından yayımlanmıştır. 1980 yılında “Mahremiyetin ve Kişisel Verilerin Sınır Ötesi Akışını Düzenleyen Rehber İlkeler”⁸² başlığı ile çıkarılan metin bağlayıcılığı bulunmayan, bir tavsiye kararı niteliğindedir. Örgütün yayımladığı tavsiye kararların farklı devletlerin karşılıklı irdelemesi ile ortaya çıkması ve üye devletlerin dünya ekonomisinin önemli bir kısmını oluşturması nedeniyle kendine özgü bir güce sahip olduğu kabul edilmelidir⁸³. Bu bağlamda, 1980 yılında yayımlanan kararın başta o tarihte kişisel verilere ilişkin herhangi bir düzenlemesi bulunmayan ülkeler olmak üzere tüm ülkeler için yol gösterici bir işlev üstlendiği söylenebilir⁸⁴. Belirtmek gerekir ki, OECD’nin yayınladığı bu ilkeler kişi güvenliğinin sağlanması yerine öncelikli olarak uluslararası veri akışının önündeki engelleri kaldırmayı amaçlamıştır. Nitekim, veri akışının kesilmesi bankacılık ve sigortacılık gibi çeşitli ticari işlerin sekteye uğramasına sebebiyet verebilecektir. Bu sebeple Örgüt kuruluş amacına da uygun olarak, ulusal mevzuatlardaki farklılıklardan doğan veri akışının kesilmesinin önüne geçmeyi hedeflemiştir⁸⁵.

İmzalayan ülkeler bakımından bağlayıcılığı bulunan ilk uluslararası metin ise Avrupa Konseyince oluşturulan 1981 tarihli "108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması” adlı sözleşme olmuştur. Türkiye, 28 Ocak 1981 tarihinde bu sözleşmeyi imzalamıştır. Bununla birlikte, sözleşmenin uygun bulunmasına ve onaylanmasına ilişkin kararın 17 Mart 2016 tarihli Resmî Gazete’de yayımlanmasıyla sözleşme iç hukuka dahil edilmiştir⁸⁶. Bu sözleşmenin amacı, her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkının korunmasını sağlamaktır (m.1). Öte yandan, Sözleşmenin “Giriş” kısmında özel hayata saygı hakkı ile uluslararası serbest bilgi akışının birbirleriyle uzlaştırılması gerekliliğine de vurgu yapılmıştır. Görüldüğü üzere, gerek OECD tarafından sunulan rehber ilkeler gerekse de Avrupa Konseyi’nce ortaya konulan sözleşme kişisel verilerin işlenmesini genel bir kural olarak yasaklamamakta, verilerin işlenmesi faaliyetini belirli kurallara bağlamaktadır. Ayrıca her iki metin de verilerin uluslararası paylaşımını engelleyecek ulusal aksaklıkları ortadan kaldırmayı amaçlamaktadır⁸⁷.

⁸² OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>.

⁸³ Ayrıntılı bilgi için bkz.: Aynur BAYRAKTAR, “Ekonomik İş birliği ve Kalkınma Örgütü (Organisation For Economic Cooperation and Development – OECD) ve Çevre”, **Biyoloji Bilimleri Araştırma Dergisi**, S. 3 (2), 2010, s. 6.

⁸⁴ DUMAN, s.17.

⁸⁵ YÜZBAŞI TOBAZ, s.133.

⁸⁶ Sözleşmenin Türkçe metni için bkz.: RG, 17.3.2016/29656. Anayasanın 90. maddesinin 5. fıkrasına göre usulüne göre yürürlüğe konulmuş uluslararası anlaşmalar kanun hükmündedir. Uluslararası anlaşmaların normlar hiyerarşisindeki yeri ve Türk hukukundaki etkisine ilişkin tartışmalar için bkz.: Rona AYBAY, “Uluslararası Antlaşmaların Türk Hukukundaki Yeri”, **TBB Dergisi**, S. 70, 2007; Esra ÖZGÜN TEKİN, “1982 Anayasası’nın 90. Maddesi Uyarınca Uluslararası Andlaşmaların Türk Hukukundaki Yeri Sorunu”, **Journal Of Social, Humanities and Administrative Sciences**, Vol: 5, Issue: 14, 2019, s. 137-149.

⁸⁷ Bireylerin özel hayat gizliliğinin korunması ve kişisel verileri kontrol edenler ile ülkeler arasındaki veri akışının devamının sağlanması kişisel verilerin korunması hukukunun iki temel amacını oluşturur: AKGÜL, s.183.

Latin Amerika ülkelerinde ise kişisel verilerin korunması “Habeas Data” kavramının Anayasalarında yer verilmesiyle başlamıştır. “Veriye sahip olmalısın” anlamına gelen bu kavram Latin Amerika ülkelerinin Avrupa Konseyi tarafından imzaya sunulan 108 sayılı Sözleşmeden etkilenmesinin bir sonucudur⁸⁸ ve ilk olarak 1988 tarihli Brezilya Anayasasında düzenlenmiştir. Brezilya örneğinden sonra 1992’de Paraguay, 1993’te Peru, 1994’te Arjantin, 1996’da Ekvator ve 1997’de Kolombiya anayasalarında da bu kavrama yer verilmiştir⁸⁹. Her bir ülkenin uygulaması kendi içerisinde farklılıklar taşısa da genel anlamda *habeas data* hakkı sayesinde kişi mahkemeye başvurarak kendisi hakkında düzenlenen dosyayı görmek, bilgileri öğrenmek, yanlış olanların düzeltilmesi ya da silinmesi için itirazda bulunmak haklarına sahiptir⁹⁰.

Türk hukukunda ise kişisel verilerin korunmasına ilişkin düzenlemeler aşamalı bir gelişim göstermiştir. İlk olarak Türkiye, 28 Ocak 1981 tarihinde "108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması” adlı uluslararası sözleşmeyi imzalamasına karşın sözleşmenin uygun bulunması ve onaylanarak iç hukuka dahil edilmesi için 17 Mart 2016 tarihine kadar beklenilmiştir. Ulusal mevzuatta ise çeşitli kanunlarda dağınık hükümler şeklinde kendini gösteren kişisel verilerin korunması kavramı, zamanla müstakil bir kanuni düzenlemeye kavuşmuştur. Kişisel verilerin korunmasına ilişkin ilk hükümler, 26 Eylül 2004 tarihinde kabul edilen 5237 sayılı Türk Ceza Kanunu'nun 135-140. maddelerinde yer almıştır. Bu düzenlemeler, kişisel verilerin hukuka aykırı olarak kaydedilmesi, ele geçirilmesi ve yayılması gibi fiilleri suç olarak düzenlemiştir. Bunun dışında, Türk Medeni Kanunu⁹¹, Fikir ve Sanat Eserleri Kanunu⁹², Ceza Muhakemesi Kanunu⁹³, İş Kanunu⁹⁴ ve Bilgi Edinme Kanunu⁹⁵ gibi farklı düzenlemelerde kişisel verilerin korunmasına yönelik bazı hükümlere yer verilmiştir⁹⁶.

Kişisel verilerin korunması hakkının anayasal düzeyde açıkça tanınması ise 7 Mayıs 2010 yılında yapılan Anayasa değişikliği ile gerçekleşmiştir. Bu değişiklikte, Anayasa'nın 20. maddesine eklenen fıkra ile herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu açıkça düzenlenmiştir. Bu fıkra, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğini hüküm altına almıştır. Kişisel verilerin korunmasına ilişkin müstakil kanuni

⁸⁸ YÜZBAŞI TOBAZ, s.124.

⁸⁹ Andres GUADAMUZ, “Habeas Data vs the European Data Protection Directive”, **The Journal of Information, Law and Technology (JILT)**, 2001, Issue: 3, s. 3. <http://elj.warwick.ac.uk/jilt/01-3/guadamuz.html> (E.T. 28.7.2021).

⁹⁰ YÜZBAŞI TOBAZ, s.125. Habeas Data kavramı hakkında ayrıntılı bilgi için bkz: GUADAMUZ, s.4 vd.

⁹¹ No: 4721, Kabul T. 22.11.2001, R.G. 24607, T. 08.12.2001.

⁹² No: 5846, Kabul T. 05.12.1951, R.G. 7981, T. 13.12.1951.

⁹³ No: 5271, Kabul T. 04.12.2004, R.G. 25673, T. 17.12.2004.

⁹⁴ No: 4857, Kabul T. 22.05.2003, R.G. 25134, T. 10.06.2003.

⁹⁵ No: 4982, Kabul T. 09.10.2003, R.G. 25269, T. 24.10.2003.

⁹⁶ Ayrıntılı bilgi için bkz.: A. Çiğdem AYÖZGER ÖNGÜN, **Kişisel Verilerin Korunması Hukuku**, Beta, 2. Baskı, Ocak 2019, s. 96 vd.

düzenleme olan 6698 sayılı Kişisel Verilerin Korunması Kanunu ise 7 Nisan 2016 tarihinde yürürlüğe girmiştir.

4. KİŞİSEL VERİNİN HUKUKİ NİTELİĞİNE İLİŞKİN YAKLAŞIMLAR

Kişisel veri kavramı “kişiyeye ait her türlü bilgi” şeklinde tanımlandığından çok geniş bir içeriğe sahip olduğu görülmektedir. Bu geniş içerik karşısında kişisel verilerin layıkıyla korunabilmesi için bu kavramın hukuki niteliğinin belirlenmesi büyük önem arz etmektedir. Nitekim, kavramın niteliği belirlendiğinde, verilerin hangi çerçeveden bakılarak ve hangi hukuki enstrümanlar kullanılarak korunacağına dair önemli ipuçları elde edilebilecektir.

Genel olarak, kişisel veri kavramına iki farklı yaklaşımın var olduğu görülmektedir. Bunlardan ilki, Anglo-Amerikan hukukunda baskın olan ve kişisel verileri mülkiyet hakkı ya da fikri mülkiyet hakkı bağlamında değerlendiren yaklaşımdır; diğeri Kıta Avrupası’nda hâkim olan ve kişisel verileri temel bir insan hakkı yahut kişilik hakları altında değerlendiren yaklaşımdır⁹⁷.

Mülkiyet hakkı görüşü kişisel veriyi kişinin bir ürünü veya mülkü olarak kabul etmektedir. Bu sebeple, kişi kendisine ait verilerden kullanma, yararlanma ve her türlü tasarrufta bulunma haklarına sahiptir. Başka bir deyişle, kişisel veri eşya hukukundaki “şey” kavramıyla ifade edilmelidir⁹⁸. Bu sayede, kişi mülkiyet hakkına tanınan geniş korumadan yararlanarak kişisel verileri üzerinde tam bir denetimi elinde bulundurmuş olur⁹⁹. Bu görüşün kişilere yansıyan başka bir kazanımıysa verilerin ivazlı ya da ivazsız satım ya da kira akdine konu edilebilmesidir¹⁰⁰. Kişisel verilerin kullanımı sayesinde büyük gelir elde eden şirketlerin veri sahiplerine bir ödeme yapması gerekliliği ortaya çıkacak, bu sayede hem veri sahiplerinin gelire ortak olması sağlanacak hem de kullanılan veri için ücret ödenmek istenmemesi halinde kişisel verilerin işleme oranında düşüş sağlanabilecektir. Ancak bu görüş, bireylerin güçlü şirketler karşısında sözleşmenin tarafı olarak çok güçsüz durumda kalacağı ve ticari hayatın kıt kaynaklarının herkese paylaştırılmasının imkân dahilinde olamayacağı gerekçeleriyle eleştirilmektedir¹⁰¹.

Amerika’da savunulan **başka bir görüş** ise kişisel verilerin **fikri mülkiyet hakkı** bağlamında korunması yönündedir. Kişinin ürettiği bir kitap, sanat eseri yahut teknolojik ürün gibi kişisel veri de

⁹⁷ Sinan Sami AKKURT, “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, *Kişisel Verileri Koruma Dergisi*, C. 2, S.1, 2020, s. 21.

⁹⁸ Corien PRINS, “When Personal Data, Behavior And Virtual Identities Become A Commodity: Would A Property Rights Approach Matter?”, *Script-ed*, C. 3, S. 4, 2006, s. 274-275; AKKURT, s.22.

⁹⁹ Elif KÜZECİ, *Kişisel Verilerin Korunması*, Turhan Kitabevi, 3. Baskı, Ankara, 2019, s.60.

¹⁰⁰ Pamela SAMUELSON, “Privacy As Intellectual Property?” *Stanford Law Review*, Vol. 52, No: 5, 2000, s.1130; Murat Volkan DÜLGER, “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, C. 5, S.1, 2018, s. 76.

¹⁰¹ KÜZECİ, *Kişisel Verilerin Korunması*, s.61; AKKURT, s.23.

kişiyeye ait bir ürün olduđu için bu kapsamda korunması gerektiđi savunulmaktadır¹⁰². Ancak fikri mülkiyet hakkının genel olarak kişiyeye ait fikri eserlerin ekonomik anlamda korunmasıyla ilgiliyken kişisel verilerin korunmasında amacın kişiyeye ait bilgilerin koruma altına alarak ekonomik kaygılardan ziyade kişisel değlerlerin korunmasını sağlamak olduđu eleştirisi yapılmaktadır. Ayrıca, fikri mülkiyet hakkı kişiyeye ait fikri ürünleri korumaktayken kişisel verilerin her zaman kişisel irade ile ortaya çıkmayan, kişiyeye ait isim, hastalık, yara izi, genetik bilgiler gibi kişinin bir parçası olmakla birlikte onun fikri bir ürünü olarak kabul edilemeyecek bilgilerden oluştuđu, bu sebeple fikri bir ürüne benzetilerek bu bağlamda korunmaya çalışılmasının doğru bir yaklaşım olmadığı da ifade edilmektedir¹⁰³.

Kıta Avrupası'nda hâkim olan görüşlerden biri ise kişisel veriyi **kişilik hakkı içerisinde değerlendirilen görüştür**. Kişilik hakkı kamu hukukunda ortaya konulan insan haklarına paralel olarak özel hukukta yerini bulan, yine insanın sırf insan olmasından doğan hakları şeklinde ifade edilebilir¹⁰⁴. Temel bir farklılık olarak, kişilik hakkı söz konusu olduğunda özel hukukta bireyin diğer bireylere karşı korunması söz konusuyken; kamu hukuku alanında genel olarak insanın devlet gücüne karşı temel haklarının korunması konu edilmektedir¹⁰⁵.

Kişilik hakkının koruduđu değler hukuk düzeninin koruduđu tüm kişisel değleri kapsamaktadır. Bu sebeple ki, kişilik hakkının konusunun tahdidi olarak belirlenemeyeceđi, zaman içerisinde meydana gelen değışimler ve teknolojik gelişmeler neticesinde yeni değlerin kişilik hakkının koruduđu değlere eklenmeye devam ettiđi ifade edilmektedir¹⁰⁶. Türk Medeni Kanunu'nun 23. ve 24. maddelerinde yer verilen kişilik hakkına ilişkin düzenlemelerde de bu hakkın içeriđine yönelik herhangi bir belirleme yapılmamış olması hukukumuz için de benzer bir kabulün geçerli olduğunu göstermektedir¹⁰⁷. Kişilik hakkının koruduđu değlere ilişkin Yargıtay'ın bir kararında yaptığı değerlendirme ise şu şekildedir:

¹⁰² Jonathan ZITTRAIN, "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication", *Stanford Law Review*, Vol. 52, No: 5, 2000, s. 1203; DÜLGER, s.77.

¹⁰³ AKKURT, s.24.

¹⁰⁴ "İnsan hakları, devletten önce gelen, insanın insan olmasından kaynaklanan haklardır.": Kemal GÖZLER, **İnsan Hakları Hukuku**, Ekin Yayınevi, 2. Baskı, Ekim 2018, s. 84.

¹⁰⁵ Mümin Serdar GÜNTÜRK, **Özel Hayatın Gizliliđinin Korunması**, Seçkin Yayıncılık, 2012, s. 28; BASKIN, s.52. Kişilik hakkının özel hukukun da ötesinde Anayasanın 17. maddesiyle anayasal bir teminat altında bulunduđu, bu maddede ifade edilen yaşama, maddi ve manevi varlığını geliştirme hakkını geliştirmeyi amaçladığı ifade edilmektedir: AYAN/AYAN, **Kişiler Hukuku**, s. 89.

¹⁰⁶ AYAN/AYAN, **Kişiler Hukuku**, s.90; GÜNTÜRK, s.31. Bu yeni gelişmelere "çevre ve gürültü kirliliđi, organ ticareti, gen teknolojisi ile insan denekleri üzerinde yapılan deneyler, gizli izleme teknolojisindeki gelişmeler ve kişisel verilerin işlenmesi" gibi örnekler verilebilir. Aktaran: İhsan ERDOĞAN / A. Dilşad KESKİN, **Türk Medeni Hukuku (Başlangıç Hükümleri – Kişiler Hukuku)**, Gazi Kitabevi, 2. Baskı, 2019, s. 277, dn.: 665.

¹⁰⁷ ERDOĞAN/KESKİN' e göre TMK'deki ilgili hükümlerin çerçeve hüküm şeklinde düzenlenmesi zamana göre yeni değlerin kişilik hakkının korumasına dahil edilmesine imkân tanımaktadır: ERDOĞAN/KESKİN, s.277. TMK'nin 23. ve 24. maddeleri şu şekildedir: **Madde 23:** Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. / Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlandırmaz. / Yazılı rıza üzerine insan kökenli biyolojik maddelerin alınması, aşılması ve nakli mümkündür. Ancak, biyolojik Madde verme borcu altına girmiş olandan edimini yerine getirmesi istenemez; maddi ve manevi tazminat isteminde bulunulamaz.

“Kişilik değerleri, kişinin haklarını oluşturup, bu hakların, yazılı hukukta bir tanıma yapılmamış olmakla birlikte, teori ve yargısal kararlardaki tanıma göre, kişinin yaşamı, sağlığı, vücut ve ruh bütünlüğü ile toplum içindeki yerini sağlayan ve koruyan haklar olduğu söylenebilir. Yine bu haklar fiziki, duygusal ve sosyal kişilik değerlerinden oluşurlar. İşte kişi, bu değerlerin oluşumu ve korunmasının var olduğu durumlarda yaşamı bir anlam ve değer kazanabilir.”¹⁰⁸

Kişilik hakkının koruduğu değerlere ilişkin öğretide farklı sınıflandırmaların yapıldığı görülmektedir. Ancak daha önce de ifade edildiği üzere, bu sınıflandırma korunan değerlerin sınırlandırılması anlamına gelmemektedir. Bu bakımdan, kişinin maddi değerleri (hayat, beden tamlığı ve sağlık değerleri), manevi değerleri (ehliyetler, özgürlük, şeref ve haysiyet, ad, resim, özel hayat alanı) ve iktisadi bütünlüğe ilişkin değerleri (iktisadi hürriyet ve varlık, mesleki şeref ve haysiyet ile mesleki ve ticari hayata ilişkin sır çevresi) kişilik hakkı çerçevesinde korunan değerler olarak sayılabilir.¹⁰⁹ Görüldüğü üzere, özel hayatın gizliliği hakkı da kişilik hakkının koruduğu değerler arasında yer almaktadır.

“Özel hayat” sözlükte *“kişinin kendine özgü yaşayışı, yaşama tarzı, kendisini ilgilendiren tutum ve davranışı, öz yaşam, özel yaşam”* şeklinde tanımlanmaktadır¹¹⁰. Bununla birlikte özel hayat kavramının da değişmez, yeknesak bir tanımının yapılamayacağı ifade edilmektedir. Bu bakımdan isim, öğrenim, sağlık ve kişisel tercihler gibi insanı tanımlayan tüm nitelikler özel yaşamın içeriğini oluşturmaktadır¹¹¹. Özel hayatın gizliliği hakkı içerisinde konut dokunulmazlığı, sebepsiz arama, haberleşmeye müdahale, doğum kontrolü, giyim tarzı ve cinsel yönelim gibi pek çok farklı konu tartışılmaktadır¹¹².

Kişinin mahremiyetinin sağlanması amacından hareketle, kişilik hakkı içerisinde yer alan özel hayatın gizliliği hakkının kişisel verilerin korunması hakkını da içerdiği savunulmaktadır. Buna göre, kişinin ismi, sağlık bilgileri, cinsel tercihleri, görüşmeleri, giyim tarzı gibi kişisel verileri aynı zamanda

Madde 24: *Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. / Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.*

¹⁰⁸ Yargıtay 4. HD. E. 2000/ 10596, K. 2001/1501, T.15.2.2001, aktaran: GÜNTÜRK, s. 26.

¹⁰⁹ AYAN/AYAN, s.90 vd. Yaşam hakkı, vücut bütünlüğü ve sağlık hakkı, özgürlükler, onur ve saygınlık, resim üzerindeki hak, kişinin haberleşme hakkı, ad üzerindeki hak ve özel hayatın gizliliği hakkı önemli kişilik hakları arasında sayılmaktadır: GÜNTÜRK, s.33 vd.; ERDOĞAN/KESKİN, s.278 vd.

¹¹⁰ Türk Dil Kurumu Sözlükleri, <https://sozluk.gov.tr> (E.T. 22.10.2021).

¹¹¹ GÜNTÜRK, s.45.

¹¹² Sultan ÜZELTÜRK, **Özel Hayatın Gizliliği Hakkı**, Beta, 2004, İstanbul, s.5. Bu geniş içerik nedeniyle öğretide fikir birliğine varılan husus bu hakkın tek bir tanımının yapılamayacağı yönündedir: ER, s.78. Özel hayatın gizliliği hakkı bakımından yapılacak tanımlamaların bu hakka yöneltilen bakış açısına göre değişeceğine dair bkz. KÜZECİ, **Kişisel Verilerin Korunması**, s.71.

özel hayat hakkı bağlamında mahremiyetinin sağlanması gereken bilgiler olduğundan kişisel verilerin korunmasını isteme hakkı da özel hayatın gizliliği hakkının alt başlığı olarak değerlendirilmelidir¹¹³.

Bu görüşe karşı yapılan eleştiriler ise genel olarak kişisel verilerin bireyin sadece gizli kalmasını istediği özel alanına ilişkin bilgiler olmadığı, bundan daha geniş bir alanı kapsadığı, bu sebeple de özel hayatın gizliliği hakkı bağlamında yeterli korumanın sağlanamayacağı yönündedir¹¹⁴. Öte yandan, kişisel verilerin korunması hakkının kişilik hakkı olarak değerlendirilmesi halinde bu hakkın kamu hukuku boyutunun göz ardı edilmiş olacağı yapılan eleştiriler arasındadır¹¹⁵.

Özellikle Avrupa kıtasında etkili olan **bir diğer görüş**, kişisel verilerin **temel bir insan hakkı olduğunu** kabul etmektedir¹¹⁶. Kişisel verilerin korunması ihtiyacının genel itibariyle mahremiyet ve özel hayatın korunması ihtiyacından doğduğunu söylemek yanlış olmayacaktır. Nitekim, tarihsel gelişimine bakıldığında başlangıçta idarelerin, sonrasında özel kuruluşların bireyler hakkında topladığı bilgilerin artması, bunların sistematik bir şekilde kaydedilerek saklanması, bireylerin özel hayatlarına ve mahremiyetlerine dair endişelerini arttırmış, bu durum kişisel verileri koruma altına alan yeni hukuksal düzenlemeleri doğurmuştur¹¹⁷.

AİHM de kişisel verilerin korunması gerektiğine yönelik verdiği kararlarda AİHS'in 8. maddesinde temel bir insan hakkı olarak düzenlenen özel yaşamın gizliliği hakkına dayanmaktadır¹¹⁸. Ayrıca Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi (m.12), Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme (m.17) gibi diğer bazı uluslararası metinlerde özel hayat hakkı temel bir insan hakkı olarak tanınmıştır. Avrupa Birliği Temel Haklar Şartı ve diğer bazı AB düzenlemeleri ile yine muhtelif anayasal düzenlemelerde ise kişisel verilerin özel hayatın gizliliği hakkından bağımsız temel bir hak olarak düzenlendiği görülmektedir¹¹⁹.

Anayasamızda ise kişisel verilerin korunmasını isteme hakkı “özel hayatın gizliliği” başlıklı 20. maddeye 2010 yılında eklenen bir fıkra ile düzenlenmiştir. İlgili fıkra şu şekildedir: “*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*” Kişisel verilerin korunması hakkının Anayasamızdaki yeri

¹¹³ AKKURT, s.26.

¹¹⁴ AKKURT, s.26.

¹¹⁵ BASKIN, s.54.

¹¹⁶ DÜLGER, s.77.

¹¹⁷ Ayrıntılı bilgi için bkz.: “**3. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ**” başlığı.

¹¹⁸ AİHM, Marina / Romanya, B.n. 504669/14, T. 26.5.2020; AİHM, M.N ve diğerleri / San Marino, B.n. 28005/12, T.7.7.2015;

AİHM, Panteleyenکو / Ukrayna, B.n. 11901/02, T. 29.6.2006.

¹¹⁹ KÜZECİ, **Kişisel Verilerin Korunması**, s.65.

gözetildiğinde, bu hakkın özel hayatın gizliliği hakkının içerisinde bir alt başlık olarak düşünüldüğü anlaşılmaktadır.

Kişisel verilerin korunması hakkının niteliğine yönelik değerlendirmelerin temelinde bir değer olarak kişisel verinin niteliğinin ne olduğu sorusuna verilen cevap etkili olmaktadır. Kişisel veri Eşya Hukuku bağlamında bir “şey” midir yoksa bireyin kendisinden doğan ya da bireyin özüne ait bir değer midir?

Kişisel verinin bir “şey” olduğu görüşü onu mülkiyet hakkı yahut fikri mülkiyet hakkı çerçevesinde korunması gerektiğini savunmaktadır¹²⁰. Mülkiyet hakkı, kişinin sahip olduğu şeylerden kullanma, yararlanma ya da onu üçüncü kişilere devredebilme haklarını içermektedir. Ayrıca, ticari hayatın ayrılmaz bir parçası haline gelen, hatta “geleceğin petrolü” olarak kabul gören¹²¹ kişisel veriler sayesinde çok büyük miktarda kazanç elde eden şirketlerin esasında bireye ait olan şeyler için bir bedel ödemesi gerekir. Bu bedelin çoğunlukla ödemeye yanaşılmayacağı için de kişisel veri kaydının azalacağı ifade edilmektedir¹²².

Kişisel verileri kullanılarak kazanç elde eden birçok şirket veri toplamayı aslında sunduğu bir tür hizmet karşılığında sağlamaktadır. Teknolojinin geliştiği ve internetin bu denli yaygınlaştığı günümüzde özellikle telefonlar için üretilen uygulamalar kişilere çoğu zaman ücretsiz şekilde sunulmakta, karşılığında ise bu uygulamaları kullananlardan kişisel verilerinin kayıt altına alınmasına izin vermeleri istenmektedir. Bu bakış açısıyla yaklaşıldığında, çoğu zaman şirketlerin kişisel veriler için aslında ödeme yapmak yerine sunulan uygulamaları ücretsiz şekilde kullandırdıkları söylenebilir. Bu eleştirinin tüm kişisel veriler bakımından geçerli olmadığı aşıkardır; ancak işlenen her bir kişisel veri için bedel ödenmese de azımsanmayacak bir boyutu için bireylerin de fayda elde ettiğini söylemek yanlış olmayacaktır.

Öte yandan kişisel verinin eşya hukukuna konu edilen bir şey olduğu görüşüne de katılmak güçtür. Çünkü, kişisel verilerin mülkiyet hakkı bağlamında sözleşmelere konu edilmesi mümkün görünmemektedir. Nitekim, kişinin ismi, biyolojik verileri, dini inancı veya siyasi görüşüne ilişkin bilgileri tüm haklarıyla üçüncü bir kişiye devrederek bir daha kullanmaması hukuk mantığıyla çelişir¹²³.

Kişisel verinin korunmasının amacı insan onuru ve mahremiyet gibi temel değerlerle yakından ilgilidir. Kişisel verinin korunmasına yönelik düzenlemelerin kişilerin eşyalarının karşılıksız kullanılmasının önlenmesini sağlamak amacından değil; mahremiyetinin korunması amacından hasıl olduğu görülmektedir. Ayrıca, kişisel verilerin korunmasının kişilerin kendileri hakkında özgürce karar

¹²⁰ PRINS, s. 274-275.

¹²¹ “The world’s most valuable resource is no longer oil, but data”, **The Economist**, 6.5.2017, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (E.T.: 24.10.2021).

¹²² SAMUELSON, s.1132.

¹²³ AKKURT, s.23.

verebilme ve kendilerini bu özgür kararlar çerçevesinde geliştirebilme haklarıyla da doğrudan bağlantılıdır.

Almanya Anayasa Mahkemesince 1983 yılında verilen “nüfus sayımı” kararında ilk kez ortaya konulan enformasyonel self-determinasyon hakkı (the right to informational self-determination) herkesin kendilerine ait kişisel verilerinden hangilerinin, kimler tarafından ve hangi sebeplerle işleyebileceğine karar verme hakkı olarak tanımlanmaktadır¹²⁴. Mahkeme bu hakkı insan onuru ve kendi kaderini tayin etme hakkına dayandırmıştır¹²⁵.

Kendi kaderini tayin etme hakkı kişinin kendisi hakkında özgürce seçimler yapabilmesini ifade etmektedir. Mahkemeye göre, bir birey kendisi hakkındaki bilgilerin sosyal çevresinde kimler tarafından ne kadarının bilindiğinden emin olamıyorsa planlama ve özgürce karar verebilme özgürlüğü sınırlanmış olur. Ayrıca bir kişi çevresince bilinen davranışlarından farklı bir davranışa, yönelime sahipse ve bunun kaydedilip kaydedilmediğine, ya da bunların paylaşılıp paylaşılmadığına emin olamıyorsa, bu davranışını sergilemekten geri duracak ve toplumda dikkat çekmemeye çalışacaktır. Dahası, Mahkeme, kişinin bir meclise ya da siyasi bir aktiviteye katılmasının resmi şekilde kaydedileceğini ve bundan ileride zarar görebileceğini düşünüyorsa bu hakkını kullanmaktan vazgeçebileceği örneğini vermektedir¹²⁶. Özgürce karar verebilme yalnızca kişinin gelişimini etkilemekle kalmaz, bu aynı zamanda özgür demokratik bir toplumun temel kaynağını da oluşturur¹²⁷.

İletişim teknolojilerindeki gelişmeler, kişisel verilerin türlü amaçlarla ve kolayca sistematik olarak işlenebilmesine imkân vermektedir. Microsoft tarafından geliştirilen bir yazılım, bilgisayara yüklenen bir program ve kablosuz sensörler vasıtasıyla çalışanların vücut ateşini, kan basıncını, yüz ifadelerinden psikolojik durumunu tespit ederek çalışanların üretim, fiziksel sağlık ve verimliliğini ölçmeyi amaçlamaktadır¹²⁸. Bu ölçümlerin sürekli şekilde kayıt altına alınarak işverenlerce takip edileceği düşünüldüğünde, çalışanların bir sistem tarafından uzaktan ancak sürekli şekilde takip edilerek kaydedilen verilerden hareketle sistemin alacağı kararlara göre (çalışanın stresli ve verimsiz, çalışkan ya da hasta olduğu gibi) hareket etmek zorunda kalacağı aşıkardır¹²⁹. Bu durum, kişileri kendi özgür

¹²⁴ Aktaran: AKGÜL, s.77.

¹²⁵ Antoinette ROUVROY / Yves POULLET, “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy”, in Gutwirth S., Poulet Y., De Hert P., de Terwangne C., Nouwt S. (eds) **Reinventing Data Protection?**, Springer, Dordrecht, January 2009, s. 49.

¹²⁶ Aktaran, ROUVROY/POULLET, s.52-53. Mahkemeye göre, her tür veri başka verilerle ilişkilendirilerek kişiler hakkında yeni bilgiler elde edilebildiğinden önemsiz bir verinin olmadığını, dolayısıyla verilerin işlenmesinde özel nitelikli olan – olmayan ayrımının yapılmaması gerektiğini ifade etmektedir: AKGÜL, s.78-79.

¹²⁷ Aktaran: ROUVROY/POULLET, s.53.

¹²⁸ Alexi MOSTROUS/David BROWN, “Microsoft seek patent for Office ‘spy’ software”, **The Times**, 16.1.2008, <https://www.thetimes.co.uk/article/microsoft-seeks-patent-for-office-spy-software-h0dd5zmtfnt> (E.T. 28.10.2021). İşverenlerin çalışanlarını gözetim altında tutmasını sağlayan teknolojik gelişmelerin diğer bazı örnekleri için bkz.: Mike INGRAM, “Microsoft’s new ‘Productivity Score’ helps employers spy on workers”, **World Socialist Web Site**, 29.11.2020, <https://www.wsws.org/en/articles/2020/11/30/micr-n30.html> (E.T. 28.10.2021).

¹²⁹ ROUVROY/POULLET, s.47.

iradeleriyle karar vermelerine engelleyerek, bir sistem tarafından belirlenen “doğru” davranış kalıplarına uymaya zorlayacaktır.

Görüldüğü üzere, kişisel verilerin korunması kavramına ekonomik açıdan yaklaşmak meselenin sadece küçük bir boyutuyla ele alınmasına neden olacaktır. Kişisel verilerin hukuka aykırı şekilde işlenmesinden dolayı maddi ve manevi zararların oluşabileceği söylenebilirse de kişisel verilerin korunmasıyla kişilerin yalnızca ekonomik kayıplarının karşılanmasının amaçlanmadığı, bireyin kendi kaderini tayin etme hakkı ve insan onurunun korunmasının öncelikli amaç olduğunu kabul etmek gerekir.

Öte yandan, “*kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde geniş bir içeriğe sahip olan kişisel verilerin kamu hukuku ya da özel hukuk gibi tek bir boyutla ele alınması yeterli olmayacaktır. Nitekim günümüzde kişisel veriler hem devletler hem de özel şirketler tarafından işlenmektedir. Kişisel verilerin korunması hakkını temel bir insan hakkı olmaktan uzaklaştıran etmenler arasında kamu güvenliği amacıyla kişisel verilerin korunmasındaki esneme ve bu esnemenin daha fazla faydalanmak isteyen özel sektör lehine yapılan düzenlemeler sayılmaktadır¹³⁰. Dolayısıyla, kişisel verilerin bağımsız bir hak olarak kabul edilerek bütüncül bir bakış açısıyla koruma altına alınması kişisel verilerin korunmasının temelinde bulunan “bireyin korunması” amacına ulaşmayı kolaylaştıracaktır.

¹³⁰ DÜLGER, s.82.

1. BÖLÜM:

İDARENİN FAALİYETLERİNDE KİŞİSEL VERİ İŞLEMENİN HUKUKİ TEMELLERİ

Modern devlet anlayışında idare, kamu hizmetlerinin etkin ve verimli biçimde sunulması amacıyla geniş bir faaliyet alanına sahiptir. Bu faaliyetlerin icrasında, idarenin kişisel verilere erişimi ve bu verileri işlemesi kaçınılmaz hale gelmiştir. Bilgi toplumuna geçiş süreciyle birlikte, kişisel verilerin korunması hakkı, temel bir insan hakkı olarak anayasal güvence altına alınmış; idarenin veri işleme faaliyetlerinin hukuki çerçevesi ise özel kanunlar ve düzenleyici işlemlerle belirlenmiştir. Bu noktada, 6698 sayılı Kişisel Verilerin Korunması Kanunu, idarenin kişisel veri işleme faaliyetlerine ilişkin temel ilkeleri ve esasları ortaya koyan ana düzenleme niteliğindedir.

İdarenin kişisel veri işlemesi, bir yandan kamu hizmetlerinin sunumunda etkinliği ve verimliliği artırırken, diğer yandan bireylerin temel hak ve özgürlüklerine müdahale riski taşımaktadır. Bu ikilem, idarenin kişisel veri işlemesinde hukuki temellerin açık ve belirli olmasını, aynı zamanda hukuki güvenliği sağlayacak mekanizmaların oluşturulmasını zorunlu kılmaktadır. Zira idarenin kişisel veri işlemesi, hukuki dayanağını anayasanın 20. maddesinde bulan kişisel verilerin korunması hakkının sınırlandırılması niteliğindedir ve bu sınırlandırmanın da anayasanın 13. maddesinde düzenlenen temel hak ve özgürlüklerin sınırlandırılması rejimine tabi olması gerekir.

Bu bölümde, idarenin faaliyetlerinde elde edilen kişisel verilerin işlenmesinin hukuki temelleri, sistemli bir yaklaşımla ele alınacaktır. Öncelikle, idarenin veri işleme sebepleri incelenecek, ardından kişisel veri işleme süreçlerinde uyulması gereken temel ilkeler değerlendirilecektir. 6698 sayılı Kanun'un uygulama alanının sınırlarını çizen istisnalar, idarenin faaliyetleri bağlamında analiz edilecektir. Son olarak, kanuni şartlara uyum kapsamında idarenin yükümlülükleri ve veri işleme şartları detaylı biçimde incelenecektir. Bu inceleme, idarenin kişisel veri işlemesinin hukuki temellerinin anlaşılmasına ve uygulamada ortaya çıkabilecek sorunların çözümüne katkı sunmayı amaçlamaktadır.

1. İDARENİN KİŞİSEL VERİ İŞLEME SEBEPLERİ

İdare, kişiler hakkında kayıt tutmaya kişinin hayata gözlerini açmasıyla başlar. Bir sağlık kuruluşunda gerçekleşen doğum olayında, sağlık kuruluşu yeni doğanın sağlık durumu ve doğum saati gibi bilgilerine ilişkin rapor oluşturur ve bu rapor *e-rapor* sistemine yüklenir¹³¹. Böylelikle, kişi

¹³¹ “Hastanelerimizde gerçekleşen doğumlar için Doğum Raporu düzenlenmesi ve talep edildiği takdirde doğumu gerçekleştiren bebek/bebekler için “Kimlik Kartı” başvurularının Nüfus ve Vatandaşlık İşleri Genel Müdürlüğümüze iletimini hızlandıran,

hakkındaki ilk veriler İdare tarafından işlenmiş olur. Daha sonrasında kişinin yaşamı boyunca, İdare ile girdiği hemen hemen tüm etkileşimler birer veri olarak kayıt altına alınır. Toplanan veriler arasında mali faaliyetler, cezai suçlamalar, istihdam durumu, tıbbi tedavi ve bunların maliyetleri, sosyal yardımlardan yararlanma durumu gibi birçok kişisel veri çeşidi yer alır.

İdarenin, kendisiyle etkileşen her bir birey hakkındaki kişisel verileri kayıt altına almasının sosyal refah programlarının yönetilmesi, vergilerin doğru ve yeterli şekilde toplanması ve kanunların uygulanması faaliyetlerinin yönetilmesi gibi sebepleri olduğu ifade edilmektedir¹³². OECD tarafından hazırlanan bir rapora göre ise verilerin doğru şekilde kullanımı sayesinde, kamu hizmetlerinin planlanması ve sunumu, kanuni düzenlemelerin iyileştirilmesi ve ihtiyaca uygun yeni kurallar getirilmesi ile İdarenin işlem ve eylemlerinde performans yönetiminin sağlanması mümkündür¹³³. İlgili rapora şu sorularla başlanarak İdarenin kişisel verileri kullanmak suretiyle ne gibi kazanımlar elde edebileceğine dikkat çekilmektedir: *“Ya daha fazla yoksul aile ihtiyaç duydukları devlet yardımlarından yararlıysaydı? Ya daha fazla hastanın hayatı kurtarılabilirse? Ya daha fazla çocuk istismar durumlarından korunabilseydi? Ya daha fazla insan yaklaşan selden kurtarılabilirse? Peki ya daha fazla terör saldırısı önlenebilirse?”*¹³⁴.

İdare tarafından çeşitli vasıtalarla elde edilen, farklı türdeki yüksek hacimli verilerin (büyük verinin) çeşitli teknolojik araçlarla analiz edilerek anlamlı sonuçlar çıkartılmasıyla¹³⁵, toplumun ihtiyaç duyduğu hizmetler fark edilerek yeni hizmet çeşitleri oluşturulabilir, mevcut hizmetler ihtiyaç duyanlarca ya da herkesçe adil ve verimli şekilde kullanabilmesi amacıyla yeniden planlanabilir. Öte yandan, kamu düzeninin sağlanabilmesi, kanuni düzenlemelerin uygulanabilmesi (örneğin vergi kaçırmaların önlenmesi) ve toplumun ileriye dönük ihtiyaçlarının tespit edilerek gerekli önlemlerin gecikmeden hayata geçirilebilmesi için de İdarenin kişisel verileri kullanması mümkündür¹³⁶.

Nitekim Dünya’da kişisel verilerin İdare tarafından kullanılması ve toplumsal fayda sağlanmasına ilişkin örnekler mevcuttur. Örneğin, Avustralya İdaresinin uzun vadeli işsizlik ve refah

olumlu bulunması halinde kimliğin belirtilen adrese gönderimini sağlayan uygulamadır.”, <https://erapor.saglik.gov.tr/portal/detay/dogum-raporlari-0> (E.T. 9.6.2024).

¹³² Priscilla M. REGAN, “Privacy, Government Information, and Technology.” **Public Administration Review**, vol. 46, no. 6, 1986, p.629, <https://doi.org/10.2307/976229> (E.T. 7.6.2024).

¹³³ Charlotte VAN OOIJEN, Barbara UBALDI, Benjamin WELBY, “A data driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance”, **OECD Working Papers on Public Governance No.33**, 2019, s.4, <https://dx.doi.org/10.1787/09ab162c-en> (E.T. 7.6.2024).

¹³⁴ VAN OOIJEN ve diğerleri, s.6.

¹³⁵ Ayşe Nur AKINCI, “Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti”, **T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı**, Uzmanlık Tezi, 2019, s.5.

¹³⁶ MACIEJEWSKI’ye göre İdare tarafından büyük veri üç farklı yaklaşımla kullanılabilir: İdarenin geçmişten bilgileri analiz ederek kararlar aldığı *tarihsel* yaklaşım, verilerin mevcut durumunu inceleyerek birkaç dakika ya da birkaç saatlik gecikmeyle anlık sonuçlar elde ettiği ve buna göre kararlar aldığı *gerçek zamanlı* yaklaşım ve gelecekte ne olacağını görmek amacıyla, İdarenin geleceğe yönelik tahminlere dayalı kararlar aldığı *tahmine dayalı* yaklaşım: Mariusz MACIEJEWSKI, “To do more, better, faster and more cheaply: using big data in public administration”, **International Review of Administrative Sciences**, 83(1_suppl), 2017, s.123, <https://doi.org/10.1177/0020852316640058> (E.T. 8.6.2024).

bağımlılığı riski altında bulunan kişileri tespit etmek ve gerekli önlemleri almak için büyük veri kullandığı ifade edilmektedir¹³⁷. Yeni Zelanda İdaresi ise tahmine dayalı analizler yardımıyla sosyal bakım, vergilendirme, sağlık, adalet ve sosyal destek yönetimi alanlarında kişisel verilerden yararlanmaktadır¹³⁸. Singapur’da ise günlük 6,3 milyon yolculuk için toplu taşımanın işleyişini iyileştiren bir sistem oluşturmak amacıyla büyük veriden faydalanılmış, bu amaçla başlatılan projede 12 milyondan fazla toplu taşıma işlemi hakkındaki veriler incelenerek yolcunun başlangıçtan bitiş noktasına kadar yaptığı her yolculuk kayıt altına alınmıştır¹³⁹.

Ülkemizde de farklı kurum ve kuruluşlar tarafından büyük veri kullanılarak çeşitli projeler ve faaliyetler yürütülmektedir. Vatandaşların tüm kişisel verilerin ortak bir merkezde toplandığı ve ilgililerin de bu verilere belli ölçülerde erişebildiği e-devlet sisteminin yanı sıra, örneğin, Sosyal Güvenlik Kurumu tarafından yürütülen *e-bildirge sistemi* ile sigorta ve işyeri tescil kayıtlarının takibi gerçekleştirilmekte; Millî Eğitim Bakanlığı tarafından çıkarılan *e-Okul* projesi ile okul kaydından mezuniyetine kadar bir öğrenci ait tüm veriler kayıt altına alınarak öğrenim süreci takip edilmekte; Sağlık Bakanlığı’nca yürütülen *e-Nabız*, *MHRS* ve *Aşı Takip Sistemi* gibi projelerle sağlık verileri kayıt altına alınmaktadır¹⁴⁰.

İdarenin, işlemiş olduğu kişisel verilerle gerek ülke genelinde gerekse yerel yönetimlerde birçok faydalı kazanımlar elde edebilme imkanına sahip olmasının yanında, bireylerin özel hayatına müdahale ve kişisel verilerin hukuka aykırı işlenmesi gibi olumsuz sonuçlar da doğurabileceği unutulmamalıdır. İdarenin birden çok iç içe geçmiş yapıdan oluştuğu göz önünde alındığında, yeterli sistem gereksinimlerinin oluşturulmaması halinde her seferinde verilerin tekrar işlenmesi, bu verilerin kontrolsüz şekilde İdari birimler arasında paylaşılması, veriler arasında tutarsızlıkların oluşması mümkündür¹⁴¹. Ayrıca, verilerin genel ölçekte kullanılarak suç oranlarının düşürülmesi veya kanser hastalıklarının önlenmesi sağlanabilirken, bunun aksine kötü amaçlı bir kullanımla, analizlerin bireyler üzerine odaklanarak özel hayatın gizliliği ilkesi tümenden ihlal edilebilir¹⁴². Yine, kişisel verilerin suçun önlenmesi amacıyla kullanıldığı ve profileme yapılarak suçların işlenmeden önce önüne geçilmeye

¹³⁷ Joanna REDDEN, “Democratic governance in an age of datafication: Lessons from mapping government discourses and practices” **Big Data & Society**, Vol. 5(2), 2018, s. 2, <https://doi.org/10.1177/2053951718809145> (E.T. 7.6.2024).

¹³⁸ REDDEN, s.2.

¹³⁹ MACIEJEWSKI, s.128.

¹⁴⁰ Ayrıntılı bilgi için bkz.: Özer KÖSEOĞLU/Yılmaz DEMİRCİ, “Türkiye’de Büyük Veri ve Veri Madenciliğine İlişkin Politika ve Stratejiler: Ulusal Politika Belgelerinin İçerik Analizi”, **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Y.2017, C.22, Kayfor15 Özel Sayısı, s.2223-2239; Deniz Boz ERAVCI, “Kurumların Dijital Dönüşümü: Büyük Veri”, **Çalışma İlişkileri Dergisi**, Ocak 2020, C.11, S.1, s. 90-112.

¹⁴¹ Raf BUYLE ve diğerleri, “Streamlining Governmental Processes by Putting Citizens in Control of Their Personal Data”, İçinde: Chugunov, A., Khodachek, I., Misnikov, Y., Trutnev, D. (Eds.) **Electronic Governance and Open Society: Challenges in Eurasia**. EGOSE 2019, Springer, ss. 346-359, s. 347, https://doi.org/10.1007/978-3-030-39296-3_26 (E.T. 7.6.2024).

¹⁴² REDDEN, s.9.

çalışıldığı durumlarda, hatalı profillemeye nedeniyle birçok kişi İdarenin ayrımcılık ve diğer olumsuz uygulamalarına maruz kalabilecektir¹⁴³.

Öte yandan, kişisel verilerin İdarenin faaliyetlerinde etkin şekilde kullanılmasının demokrasi uygulamasına katkı sağladığı söylenebilir. Nitekim, idari faaliyetlerin vatandaşların katılımıyla şekillendirilmesi mümkün olmaktadır. İdare vatandaşın verilerini analiz ederek kamunun ihtiyaçlarını tespit etmekte, hizmetlerini yenilemekte ve gerektiğinde yeni hizmet modelleri geliştirebilmektedir. Bununla birlikte, kişisel verilerin bu demokratik kullanımının, teknolojik gelişmeler neticesinde aksi yönde sonuçlar doğurma potansiyeli de göz ardı edilmemelidir. Buna göre İdare elindeki verileri, vatandaşların fikirlerine yer bırakmayan yukarıdan aşağıya bir kontrol mekanizması uygulayarak, vatandaşın talep ve ihtiyaçlarına göre karar almaktan ziyade aldığı kararlara uygun bir yaşam biçimini vatandaşa dikte edebilir¹⁴⁴.

Kişisel verilerin İdarenin elinde iyi yönetim amaçları yerine kötü amaçlarla kullanılması ya da yetersiz teknoloji ve yetersiz önlemler neticesinde yukarıda ifade edilen sorunlar ortaya çıkabilir, kişilerin özel hayatın gizliliği ve kişisel verilerin korunması hakları başta olmak üzere birçok hakkı İdare tarafından ihlal edilebilir. Ancak, kişisel verilerin hukuka uygun şekilde kullanılması halinde bile, İdarenin düşünsel biçiminde olumsuz etkiler meydana getirebileceği ifade edilmelidir. Bu etkiler,

- Vatandaşların birer insan olarak görülmesinden ziyade sadece birer “veri öznesi” olarak görülmeye başlanması;
- Kişilere ilişkin çok daha fazla verinin işlenmesinin İdare eliyle teşvik edilmesi;
- Daha somut ve ayrıntılı sonuçlara varabilmek amacıyla hükümetlerin ellerindeki veri kümelerini başka hükümet ya da özel sektör aktörlerinin elinde bulunan veri kümeleriyle birleştirme isteğinin artması, böylece veri güvenliği risklerinin büyümesi;
- Kişisel verilerle eğitilen yapay zekâ sistemleriyle daha fazla idari işlemin otomatikleştirilmesi ve böylece idari karar süreçlerinin karmaşılaştırılarak belirsiz hale gelmesi;
- Neredeyse sonsuz derecede bilinebilir hale gelmesine karşın vatandaşların kişisel verilerinin toplanma ve kullanılma süreçleri hakkındaki sorgulama yapma konusunda yeteri kadar aktif olmaması ve idarenin de bu bilincin oluşması konusunda teşvik edici olmaması, şeklinde özetlenebilir¹⁴⁵.

İdarenin kişisel verileri kullanması sonucu ortaya çıkan olumsuz durumların en aza indirilmesi için sunulan çözüm önerileri ise şeffaflık, hesap verilebilirlik ve bireysel mahremiyetin sağlanması

¹⁴³ MACIEJEWSKI, s.131.

¹⁴⁴ Heather BROOMFIELD / Lise REUTTER, “In search of the citizen in the datafication of public administration”, **Big Data & Society**, 9(1), 2022, s.3, <https://doi.org/10.1177/20539517221089302> (E.T. 7.6.2024).

¹⁴⁵ REDDEN, s.3.

ilkelerinde birleşmektedir. Buna göre, kişisel verilerin kullanımı ile zikredilen bu ilkeler arasında bir denge kurulması gerekir¹⁴⁶. Örneğin, dolandırıcılık suçlarının tespiti için kullanılan yöntemlerin İdare tarafından tümünden ifşa edilmesi o yöntemi tamamen etkisiz kılabilirken, sistemin işleyişi hakkında hiçbir bilginin sunulmaması kişi haklarının ihlali konusunda şüphe uyandıracaktır.

Ayrıca, demokratik yönetimlerde sağlıklı bir devlet-vatandaş ilişkisi vatandaşın İdari karar alma süreçlerini inceleyebilme ve bunları değiştirme, iptal ettirme veya yeni kararlar aldırma gibi taleplerde bulunabilmesine, Broomfield ve Reutter'in ifadesiyle “*bunlara meydan okuyabilme becerisine*” bağlıdır¹⁴⁷. Dolayısıyla, İdarenin kişisel verileri kullanarak politika üretilmesi süreçlerinde yeterli düzeyde şeffaf davranmasının yanı sıra, bu sürece ilgisiz olsalar bile vatandaşları alınan kararlara dahil etmesi ve gerektiğinde bu kararlara karşı çıkma konusunda onları cesaretlendirmesi gerekir.

Öte yandan, İdareler kişisel veriye sahip olmanın ve bu verileri teknolojiyle harmanlayarak elde edebileceği kazanımların cazibesine kapılmadan önce şu soruları da değerlendirmelidir¹⁴⁸: Büyük veri ve benzeri teknolojik araçların kullanımı her türlü hizmetin sağlanmasında gerekli midir? Yoksa bazı hizmetlerde alternatif, veriye ihtiyaç duymayan ya da daha az veriyle işleyen sistemler aracılığıyla benzer sonuçlara ulaşılabilir mi? Ya da güvenilir ve geçerli bir sistem kurmak, bu sistemi sürdürmek ve bunu İdari faaliyetlere entegre etmek için yapılan mali ve bilgi yatırımları bu sistemlerden beklenen getirilerden daha yüksek olabilir mi? Başka bir deyişle, verimlilik amacıyla yakıtı kişisel veriler olan bu sistemler aslında bazı durumlarda kamu zararına neden olabilir mi? İdarenin bu sorulara vereceği cevaplara göre hareket ederek, daha az verinin işlenmesi, güvenlik risklerinin azaltılması ve kamu zararlarının önüne geçilmesi sağlanabilecektir.

2. İDARENİN KİŞİSEL VERİ İŞLEME SÜREÇLERİNDE UYMASI GEREKEN İLKELER

24 Mart 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ülkemizde kişisel veri hukukuna ilişkin temel kanuni düzenleme niteliğindedir. Kanunda kişisel verilerin işlenmesine ilişkin olarak beş ilke belirlenmiştir. Kanunun 4. maddesine göre kişisel veriler işlenirken hukuka ve dürüstlük kurallarına uygun hareket edilmeli; doğru ve gerektiğinde güncel olmalı; veriler belirli, açık ve meşru amaçlar için işlenmeli; işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmalı; ve

¹⁴⁶ REGAN, s.629.

¹⁴⁷ BROOMFIELD/REUTTER, s.3. Aynı yönde bkz.: Thomas OLSEN/Tobias MAHLER, “Identity management and data protection law: Risk, responsibility and compliance in ‘Circles of Trust’ – Part II”, **Computer Law & Security Review**, Vol. 23, Issue 5, 2007, s. 415-426, <https://doi.org/10.1016/j.clsr.2007.07.001> (E.T. 7.6.2024).

¹⁴⁸ Liesbet VAN ZOONEN. “Data Governance and Citizen Participation in the Digital Welfare State.” **Data & Policy**, Vol. 2 2020: e10, s.13, [doi:10.1017/dap.2020.10](https://doi.org/10.1017/dap.2020.10) (E.T. 7.6.2024).

mevzuatta öngörülen süre kadar veya işlendikleri amaç için gerektiği kadar saklanmalıdır. Bu ilkeler, 95/46/EC sayılı Avrupa Birliği Direktifi'nin 6. maddesine paralel şekilde kaleme alınmıştır.

Ayrıca, Direktifi ilga eden GDPR ile KVKK arasında da veri işleme ilkeleri bakımından önemli benzerlikler bulunmaktadır. KVKK'nın 4. maddesinde sayılan ilkeler, GDPR'ın 5. maddesindeki ilkelerle büyük ölçüde örtüşmektedir. Her iki düzenlemede de hukuka uygunluk, doğruluk, belirli amaçlarla işleme, amaçla bağlantılı ve sınırlı olma ile saklama süresi sınırlaması gibi temel ilkeler yer almaktadır. Bununla birlikte, GDPR'da açıkça yer alan şeffaflık, veri bütünlüğü ve gizliliği ile hesap verebilirlik ilkeleri, KVKK'da ayrı birer ilke olarak sayılmamıştır. Ancak, KVKK'nin uygulanmasında ve KVK Kurulu kararlarında, bu ilkelere uygun bir yaklaşım benimsendiği söylenebilir.

6698 sayılı Kanunda kişisel verilerin işlenmesi *“kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”* şeklinde tanımlanmıştır (m.3/1-e). Görüldüğü üzere, kişisel verilerin işlenmesi ifadesinden kasıt bir verinin elde edilmesinden başlayarak o veri üzerinde gerçekleştirilecek her türlü eylemdir¹⁴⁹. Bu sebeple kişisel verilerin işlenmesine ilişkin genel ilkeler veri koruma hukukunun sac ayaklarıdır, denilebilir ve bu ilkelere herhangi birine aykırı şekilde veri işleme faaliyetinde bulunulması verinin korumasız kaldığı anlamına gelecektir. 95/46/EC sayılı Direktif'ten hareketle¹⁵⁰, sayılan ilkeler kaliteli verinin temel prensiplerini oluşturmaktadır.

- Hukuka ve Dürüstlük Kurallarına Uygun Olma: Kişisel verilerin işlenmesi sürecinde hukuka uygun şekilde hareket edilmelidir. Hukuka uygunluk, ilgili kanun ve yönetmelik ile mevzuatta yer alan diğer kurallara uygun davranılmasının yanında evrensel hukuk kurallarına uygunluğu da kapsayacak şekilde geniş kapsamlı anlaşılması gerektiği ifade edilmektedir¹⁵¹. Hukuk devleti olmanın bir gereği, kamu makamlarının da koydukları kurallarla bağlı olması gerekecektir. Başka bir deyişle, en başta kişisel veri işleyen İdari makamlar ilgili kanun ve mevzuatta yer alan diğer kurallara uymakla yükümlüdür. Hukuka uygun davranma ilkesi, aslında diğer tüm uygulanabilir yasa kurallarına uymayı

¹⁴⁹ Veri işleme faaliyeti içerisinde kabul edilen her bir eylemin ayrıntılı tanımı için bkz.: Sevgi ERARSLAN, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, On İki Levha, 2. Baskı, İstanbul, Aralık 2020, s.93 vd.

¹⁵⁰ Direktifin 6. maddesinin yer aldığı bölümün başlığı “Principles Relating to Data Quality / Veri Kalitesine İlişkin İlkeler” şeklindedir.

¹⁵¹ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s.2, <https://kvkk.gov.tr/Icerik/2030/Rehberler?&page=2> (E.T. 11.11.2021).

işaret eder¹⁵². Kişisel veri işlenirken sayılan diğer dört ilkeye yahut 6698 sayılı Kanunda belirlenen kurallara uyulmaması halinde hukuka aykırı davranılmış olacaktır.

Öte yandan, TMK'nın 2. maddesinde “*herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır*” şeklindeki düzenleme ile mevzuatımızda yer bulan dürüstlük kuralının tanımına Kanunda yer verilmemiştir. Sözlükte “doğruluk” şeklinde tanımlanan dürüstlük, hukuki bağlamda, kişinin haklarını kullanırken ya da borçlarını yerine getirirken ahlaka, örf ve âdet kurallarına uygun davranması ve doğruluktan ayrılmaması şeklinde ifade edilebilir¹⁵³. Bir kararında Kurul, hizmetin ifası için gerekli olmamasına rağmen kişisel verilerin işlenebilmesi için açık rıza talebinde bulunulmasının, bu rızanın verilmemesi nedeniyle de hizmetin sunulmamasının dürüstlük kuralına aykırı olduğuna karar vermiştir¹⁵⁴. Başka bir kararında ise Kurul, bir varlık yönetim şirketi tarafından ilgili kişinin telefonuna aynı içeriğe sahip mesajların farklı tarihlerde birden çok kez gönderilmesini veri sorumlusunun sahip olduğu hakkın kötüye kullanılması şeklinde değerlendirerek bu durumun hukuka ve dürüstlük kurallarına uygun olmadığına karar vermiştir¹⁵⁵.

Dürüstlük kuralı gereği, karşısındakiyle hukuki bir ilişki kuran kişinin onun güvenini sarsacak, beklenmedik eylem ve işlemlerden uzak durması beklenir¹⁵⁶. Bu bağlamda dürüstlük kuralı gereği kişinin muhatabına karşı şeffaf olması gerektiği de vurgulanmaktadır¹⁵⁷.

95/46/EC sayılı Direktif'in ilgili hükmünde ve 6698 sayılı Kanunda “şeffaflık” ilkesine yer verilmemekle birlikte dürüstlük kuralının bu ilkeyi barındırdığı ifade edilmişken, 27 Nisan 2016 tarihli Tüzüğün (GDPR) 5. maddesinde hukuka ve dürüstlük kuralına uygun davranmanın yanında veri öznesiyle kurulan ilişkide şeffaf şekilde davranılması gerektiği açıkça vurgulanmıştır¹⁵⁸.

Bu ilkedен hareketle, kişisel veri işleyen kamu kurumları, bu faaliyeti sürecinde gerek mevzuatla belirlenen kurallara gerekse de evrensel hukuk kurallarına uygun hareket etmekle yükümlü olup, bu süreçte ilgili veri öznesine karşı şeffaflık ilkesine uygun davranmalıdır. Bu bağlamda 6698 sayılı Kanunun 10. ve 11. maddelerinde veri sorumlusunun aydınlatma yükümlülüğü ile ilgili kişinin

¹⁵² Cecile de TERWANGNE, “Article 5: Principles relating to processing of personal data”, in **The EU General Data Protection Regulation (GDPR) A Commentary**, Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY (Eds.), Oxford University Press, 2020, s.314.

¹⁵³ Şaban KAYIHAN / Mustafa ÜNLÜTEPE, **Medeni Hukuk Bilgisi**, Seçkin Yayıncılık, 4. Baskı, Eylül 2017, Ankara, s. 122. Dürüstlük kuralının başka bir tanımı ise şu şekildedir: “Dürüstlük kuralı, *herkesin, haklarını kullanırken ve borçlarını yerine getirirken, ortalama zeka seviyesine sahip, makul, dürüst ve güvenilir bir kişiden aynı hal ve şartlar altında beklenebilecek davranış tarzına uygun şekilde davranma zorunluluğu(dur)*”: ANTALYA / TOPUZ, s.494.

¹⁵⁴ KVK Kurulu, 5.5.2020 tarih ve 2020/335 sayılı kararı: <https://www.kvkk.gov.tr/Icerik/6909/2020-335> (E.T. 28.12.2020).

¹⁵⁵ KVK Kurulu, 31.5.2019 tarih ve 2019/159 sayılı kararı: <https://kvkk.gov.tr/Icerik/5494/2019-159> (E.T. 3.1.2022).

¹⁵⁶ KAYIHAN / ÜNLÜTEPE, s.122.

¹⁵⁷ Berrak YILMAZ, “Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması”, **Hacettepe Üniversitesi SBE**, Doktora Tezi, 2019, s.98; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2.

¹⁵⁸ Direktif’te şeffaflık (transparency) kavramına yer verilmese de bunun dürüstlük kavramı içerisinde yer aldığı kabul edilmiş, bununla birlikte açıklık sağlamak adına verilerin yasal ve adil şekilde işlenmesi ihtiyacını gidermek amacıyla Tüzükte şeffaflık kavramına açıkça yer verildiği ifade edilmektedir: de TERWANGNE, s.314.

hakları düzenlenmiş olup, ilgili kişiye, kişisel verilerinin kim tarafından, hangi amaçla, ne kadarlık bir süre için işleneceğine ilişkin bilgi alma, eksik ya da yanlış işlenen verilerin değiştirilmesini, şartların sağlanması halinde verilerin silinmesini isteme gibi haklar tanınmıştır. Ayrıca, işlenen verilerin kanuna aykırı şekilde ele geçirilmesi halinde bu durumun hem ilgisine hem de Kurula bildirilmesi zorunluluğu şeffaflık ilkesine ilişkin bir düzenlemedir (m. 12/5).

- Doğru ve Gerekliğinde Güncel Olma: Kişisel verilerin işlenmesindeki genel ilkelerden biri de verilerin doğru ve gerektiğinde güncel olmasıdır. Bilgilerin doğru ve güncel olması genel anlamda veri sorumlusunun yükümlülüğüdür. Bununla birlikte bilgilerin güncelliği veri öznesinin temel haklarının korunması bakımından da önem arz ettiğinden ilgili kişinin de bilgilerinin güncelliğini takip etmesi fayda sağlayacaktır. Nitekim veri sorumlusu İdarenin, bilgilerin değişip değişmediğini sürekli kontrol etmesi, bu konuda ilgili kişiden sık sık bilgi talep etmesi hem İdarenin iş yükü göz önünde bulundurulduğunda verimli sonuçlar doğurmaz hem de ilgili kişinin gereksiz yere meşgul edilmesine de sebep olur. Bilgilerin güncel kalması bakımından belirli aralıklarla matbu hatırlatma metinleri hazırlanarak ilgililerin bunları görmesi sağlanabilir. Ayrıca, internet üzerinden verilen hizmetlerde bilgilerin kolayca güncellenmesini sağlayacak sekmeler oluşturulabilir.

Bilgilerin doğru ve güncel olması bazen kişiye bir hakka ulaşması bakımından fayda sağlayabilirken bazen de kişinin temel haklarına müdahale edilmesinin önüne geçebilir. Örneğin, evli olan çiftten biri çalışmıyor ya da işinden ayrılmışsa bu bilginin İdareye bildirilmesi ve talep edilmesi halinde belirlenen asgari geçim indiriminde (AGİ) değişiklik sağlanmış olacaktır. Normal şartlarda, kişinin işinden ayrılmış olduğu yahut çocuk sahibi olduğuna yönelik bilgiler farklı kamu kurumları aracılığıyla İdarenin bilgisi dahilindedir. Ancak, mevcut bilginin güncellenmesi ve ilgili kişi tarafından Sosyal Sigortalar Kurumuna başvurulması halinde gerekli değişiklik yapılmaktadır.

Öte yandan, çoğu zaman bilginin güncel tutulması veri sorumlusu olan İdareden beklenir. Örneğin, aracı Eskişehir’de çalınan ve daha sonra Bursa’da bulunan kişi aracını bulunduğu ilden almış fakat geri dönerken çalıntı kaydının sistemden düşülmemesi nedeniyle MOBESE kaydına takılınca yolda tekrar çevrilmiştir. Durumun sonradan anlaşılması üzerine çalıntı kaydı sistemden düşülmesiyle araç sahibi yoluna devam edebilmiştir¹⁵⁹. Ancak, durum her zaman bu kadarla sınırlı kalmayabilir. Araç sahibinin haksız yere gözüaltına alınarak özgürlüğünün kısıtlanması da mümkündür. Nitekim, ruhsatsız silah bulundurmaktan dolayı ceza alan kişi, mahkeme kararının infaz edilmesine rağmen bu bilginin Genel Bilgi Toplama (GBT) sisteminde güncellenmemesi nedeniyle belli aralıklarla tekraren gözüaltına alınmıştır. Danıştay, idarenin hizmet kusuru bulunduğuna ve kişinin uğradığı manevi zararın tazminine

¹⁵⁹ “Otomobilin çalıntı kaydı sistemden düşülmeyince” 21.2.2013, <https://www.sondakika.com/yerel/haber-otomobilin-calinti-kaydi-sistemden-dusulmeyince-4353662/> (E.T. 13.11.2021).

karar vermiştir¹⁶⁰. Bu örneklerin yaşanmaması adına İdarece işlenen verilerin doğru ve güncel olması önem arz etmektedir.

- Belirli, Açık ve Meşru Amaçlar İçin İşlenme: Bu ilke, kişisel verilerin işlenmesine ilişkin gerek açık rıza metni gerekse de Veri Sorumluları Siciline kayıt işlemi sunulan metinlerin içeriğinde belirsiz ifadelerden kaçınmayı gerektirmektedir. Kişisel verileri işlenecek kişiler, bu işlemin hangi amaca yönelik yapıldığını yeterli açıklıkta ve kesinlikte öğrenebilmelidir. Muğlak ifadelerle, kişileri bilgilendirmekten kaçınan tavırlar bu ilkeye aykırılık teşkil edecektir.

Amacın belirli ve açık olması, olası kullanım amacıyla veri toplamanın da önüne geçmektedir. İleride herhangi bir amaç için kullanılmak üzere kişisel verilerin toplanması, kayıt altına alınması bu ilke gereği Kanuna aykırı kabul edilecektir. Bu hususun ilgili kişilere yönelik katkısı ise daha büyüktür. Şöyle ki, verinin işlenme amacını bilmeyen, daha sonra nerede kullanılacağından emin olmayan kişinin özgürce kendisini ifade etmesi kolay olmayacaktır. Dolayısıyla bu ilke kişinin maddi ve manevi varlığını geliştirmesi ve bireysel özerklik gibi demokratik hakların korunması bakımından da önem arz etmektedir.¹⁶¹

Amacın meşru olmasından kasıt, öncelikle yasalara uygun bir amaç belirlenmesidir. Ayrıca, *“amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.”*¹⁶² Başka bir deyişle belirlenen amaç ile toplanan veri arasında mantıklı bir bağ olması gerekir. Söz gelimi, bir nüfus müdürlüğü çalışanının MERNİS sisteminde kayıtlı telefon numarası bilgisini kullanarak ilgili kişiyle özel amaçları için iletişime geçmesi, ilgili kişinin telefon verisinin meşru amaçlar dışında işlenmesi anlamına gelecektir. Bu durumda Kanun gereği kamu kurumlarına idari para cezası verilemediğinden sorumlular hakkında disiplin hükümlerinin işletilmesi gerekecektir¹⁶³. Başka bir örnekte, bir doktorun hastalarının verilerini seyahat acentesi işleten eşiyle paylaşarak, sağlık turizmi bağlamında özel fırsatlar sunulmak üzere işlemesi halinde de meşru bir amacın güdülmediği söylenebilecektir¹⁶⁴.

- İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme: Veri sorumlusunca işlenen kişisel veriler, eğer mevzuatta belirlenen bir süre varsa bu süre boyunca; yoksa verinin işlenmesi amacının gerçekleşmesi için gereken süre kadar kayıtlı tutulabilir. Bu bağlamda, 6698 sayılı Kanunun 7. maddesinde ifade edildiği üzere verinin daha fazla kullanılması gerekmiyorsa veri sorumlusu veriyi silecek, yok edecek ya da anonimleştirecektir. İleride kullanılmak

¹⁶⁰ Danıştay 10.D., E. 2007/1376, K. 2007/4756, T.17.10.2007 (Kazancı).

¹⁶¹ KÜZECİ, **Kişisel Verilerin Korunması**, s.203.

¹⁶² KVK Kurulu, 3.3.2020 tarih ve 2020/191, 2020/192, 2020/193, 2020/194 sayılı kararları: <https://www.kvkkarar.com/2020-191-2020-192-2020-193-2020-194/> (E.T. 4.5.2023).

¹⁶³ Bu durumda kamu görevlisinin kişisel verileri hukuka aykırı şekilde ele geçirmesi sebebiyle 5237 sayılı Türk Ceza Kanunu’nun 136. maddesi uyarınca ceza sorumluluğu da bulunmaktadır.

¹⁶⁴ ERARSLAN, s.111.

üzere verinin saklanması hukuka aykırılık teşkil edecektir. Nitekim, “*kişisel verilerin korunması hakkı, herhangi bir kişinin kendisiyle ilgili olarak toplanan kişisel verilerin toplanma amacına ulaşıldıktan sonra bilgisi dışında muhafaza edilmeyeceği veya başka bir amaç için kullanılmayacağı güvencesine sahip olması hâlinde söz konusu olabilir. Kişinin kişisel verilerinin hayatı boyunca bir yerlerde kayıtlı tutulacağını ve başka bir amaçla kullanılabileceğini düşünmesi kişisel verilerin korunması hakkını zedeler.*”¹⁶⁵

Mevzuatta belirlenen bir sürenin varlığı halinde kişisel verinin kayıt altında tutulma süresi bakımından bir kesinlik mevcutken, “işlendikleri amaç için gerekli olan süre” kısmı için aynı kesinliğin bulunmadığını söylemek mümkündür. Nitekim, Kanunun 4. maddesinin 2. fıkrasının (d) bendinden yer alan “veya işlendikleri amaç için gerekli olan” şeklindeki kuralın belirsiz, sübjektif ve geniş yorumlamaya müsait olması sebebiyle belirlilik ilkesine aykırı olduğu gerekçesiyle Anayasa Mahkemesi’ne başvurulmuştur.

AYM kararında¹⁶⁶, kişisel veri kavramının çok geniş bir kapsamı bulunduğunu, bu sebeple her bir veri için mevzuatta azami sürelerin belirlenmesinin mümkün olamayabileceğini, öte yandan kanunda öngörülen “işlendikleri amaç için gerekli olan süre” kuralı ile mevzuatta azami süresi belirlenmeyen kişisel veriler için de kişilere bir güvence sağlanmaya çalışıldığı ifade edilmiştir. Kanunda belirtilen düzenlemenin yanında, 11. maddeyle ilgililerin, kişisel verilerin amacına uygun kullanıp kullanılmadığını öğrenebilme ve 7. maddeyle öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini yahut anonim hale getirilmesini isteme hakkının tanındığı hatırlatılmıştır. Son olarak, veri sorumlularının kamuoyuna açık olan Sicile kaydolurken azami veri işleme sürelerini de belirtme zorunluluğunun bulunması karşısında iptali istenen düzenlemenin belirsiz ve sübjektif olmadığı sonucuna varılmıştır.

Veri sorumlularının söz konusu kurala dayanarak kişisel verileri belirlenen amacın gerçekleşmesi için gerektiğinden veya mevzuatta belirlenenden daha uzun bir süre kayıt altında tutması halinde, Kanunun 13. maddesine göre ilgili kişilerin veri sorumlularına başvurması, başvurularının reddi ya da yetersiz bir cevap verilmesi halinde bu kez Kanunun 14. maddesi uyarınca Kurula şikâyetle bulunması mümkündür. Böylelikle, verilerin gerekenden fazla süreyle kayıt altında tutulmasının önüne geçilebilecektir.

- İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma: İşlenmek amacıyla toplanan kişisel verilerin belirlenen amaçla bağlantılı, bu amaçla sınırlı ve ölçülü olması gereklidir. Bu ilke uyarınca, toplanacak verilerin en aza indirilmesi de amaçlanmaktadır. Örneğin, bir belediyeye iş başvurusunda bulunan kişinin başvurduğu pozisyon gereği araç kullanması gerekmiyorsa burada başvuranın ehliyet bilgilerinin

¹⁶⁵ AYM, E.2016/125, K.2017/143, T.28/09/2017, par. 15, RG, 23.1.2018/30310.

¹⁶⁶ AYM, E.2016/125, K.2017/143, T.28/09/2017, par. 16-17, RG, 23.1.2018/30310.

istenmesi halinde amacın sınırlarını aşan bir veri işleme faaliyeti gerçekleştirilmiş olur¹⁶⁷. Bu sebeple, belirlenen amaç için gereken bilgilerin iyi şekilde tahlil edilmesi, bu amacın dışına taşan verilerin ilgililerden talep edilmemesi yerinde olacaktır. Başka bir örnek, bir suç şüphesinin araştırılmasına ilişkin olarak mahkeme aracılığıyla bankadan istenen verilerin suçla hiçbir ilgisi olmayan üçüncü kişilerin verilerini de içermesi durumudur. AİHM kararına konu olayda, İtalya’da soruşturulan ve birkaç şüphelisi bulunan kara para aklama suçuyla ilgili olarak yetkili mahkeme istinabe yoluyla San Marino’dan, iki ülke arasındaki anlaşmalar uyarınca, suçla ilgisi olabileceği düşünülen bankalarda ve diğer kurumlarda bulunan ve İtalya vatandaşlarına ait hesap bilgilerini, e-posta, banka beyannameleri ve çekleri talep etmesi üzerine bu bilgilerin kopyası İtalya mahkemesine verilmiştir. Olaydan bir yıl sonra bilgilerinin paylaşıldığına dair haberdar edilen başvuran, soruşturulan suçlara ilişkin şüpheli ya da sanık olmamasına karşın banka bilgilerinin işlenmesinden şikayetçi olmuştur. AİHM, başvuranın, şüpheli ya da sanık olmaması nedeniyle özel hayatına ve yazışmalarına ilişkin bilgilerin talep edilmesine itiraz etme imkânı olmadığını, San Marino yasalarında başvuranın “özel hayatına” ve “yazışmalarına” yapılan müdahaleye itiraz etmek için usuli güvencelerin eksik olduğunu, maruz kaldığı tedbire itiraz etmek için ulusal hukuk kapsamında kendisine hiçbir yol sunulmadığını, dolayısıyla ulusal hukukun etkin korumasından yararlandırılmadığını belirlemiştir. Bu nedenle, demokratik toplumda gerekli olan “etkili denetim hakkından” mahrum bırakılan başvuranın özel hayata saygı hakkının ihlal edildiği sonucuna varılmıştır¹⁶⁸.

Ölçülülük ilkesi kamu hukukunda özellikle temel hak ve özgürlüklerin sınırlanması konusunda sıkça başvurulmuş ve elverişlilik, gereklilik ile orantılılık alt ilkelerini içeren bir kavramdır. Toplanan kişisel verilerin belirlenen amacı gerçekleştirmeye elverişli olması, bu amacın gerçekleşmesi için söz konusu verilerin muhakkak işlenmesinin gerekli olması ve veri işlemeyle gerçekleştirilmek istenen amaç arasında makul bir dengenin kurulması gerekir¹⁶⁹. Dolayısıyla, İdarenin meşru amacına ulaşmada en hafif şiddetteki önlem aracı olarak ilgili veriyi işlediği sonucuna varılabiliyorsa, o veri işlemenin ölçülü olduğu söylenebilir¹⁷⁰.

Danıştay’a göre, bir kamu idaresine ait binaların giriş ve çıkışları, binaları çevreleyen alanları, koridorları, otoparkları kamu düzeninin ve güvenliğin sağlanması amacıyla güvenlik kameralarıyla izlenerek görüntü kayıtları toplanabilirken, bunun dışında çalışanların çalışma odaları ve servisleri de

¹⁶⁷ Peter CAREY, “Data Protection Principles”, **Data Protection**, Peter Carey (Ed.), Oxford University Press, Fifth Edition, 2018, s.36.

¹⁶⁸ AİHM, M.N ve diğerleri / San Marino, B.n. 28005/12, T.7.7.2015, <https://hudoc.echr.coe.int/eng?i=001-155819>.

¹⁶⁹ Ergun ÖZBUDUN, **Türk Anayasa Hukuku**, Yetkin Yayınları, 19. Basım, Aralık, 2019, s. 114.

¹⁷⁰ İlkenin yalnızca orantılılık ilkesi göz önüne alınarak yapılan bir tanıma göre, Ölçülülük, “İdari makamın meşru hedefe ulaşmada mümkün olan en hafif şiddetteki önleme başvurusudur.” Yücel OĞURLU, **Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi**, Seçkin Yayıncılık, 2002, s.21.

görsüntüleyecek şekilde kamera yerleştirilmesi ve kişilerin görsüntü kayıtlarının toplanması kamu düzeni ve güvenlik amacını aşan bir uygulama olduğundan ölçölülük ilkesine aykırıdır¹⁷¹.

Başka bir kararda ise Danıştay İdari Dava Dairleri Kurulu, icra dairelerinin ve icra müdürü masasının bulunduğu alanların kamera sistemiyle izlenmesi hususunda, icra dairelerine ve icra müdürü masasının bulunduğu alanlara ilgili olan herkesin giriş çıkış yapabilmesi nedeniyle “özel hayatın gizliliğine makul saygı hakkı beklentisinin” yüksek olmayacağı, icra dairelerindeki rüşvet iddialarının ve yaşanan şiddet olaylarının faillerinin tespiti amacıyla kamera sistemiyle takip edilmesinin 6698 sayılı Kanunun 5. Maddesi uyarınca veri sorumlusunun meşru menfaatleri için gerekli olduğu ve bu sebeple kayda alınan kişilerin açık rızasına ihtiyaç duyulmayacağı, söz konusu görsüntü kayıtlarının da sadece kaydı alan idare tarafından saklanarak paylaşılmayacağı hususunda şüphe bulunmaması nedeniyle bu şekilde yapılan veri işleme faaliyetinin hukuka uygun olduğuna karar vermiştir¹⁷².

İdari yargı makamlarının kamu binalarındaki görsüntü kayıt sistemlerine ilişkin verdiği yukarıdaki iki karar, hukuki değerlendirme açısından dikkat çekici farklılıklar içermektedir. Danıştay'ın ilk kararında çalışma odaları ve servislerin görsüntülenmesi ölçölülük ilkesine aykırı bulunurken, Danıştay İDDK'nın kararında icra dairelerindeki servislerin ve icra müdürü masasının görsüntülenmesi ölçölülük ilkesine uygun kabul edilmiştir. Bu farklılığın temelinde, izlenen mekânın niteliği ve kamera kullanım amacı yatmaktadır. Buna göre, nüfus, tapu ve icra müdürlükleri gibi kamu personeli servislerinin bulunduğu ortamların genel olarak izlenmesi, güvenliğin sağlanması ve rüşvetin önlenmesi gibi meşru amaçlar taşıdığından ve bu amaçların gerçekleştirilebilmesinde kamera ile izlemenin gerekliliği bulunduğundan, ölçülü kabul edilmelidir. Ancak, her servis masasının ya da kamu personeli odalarının münferiden izlenmesi, çalışanların performansını denetleme amacını aşarak özel hayata müdahale riski taşıdığından, ölçölülük ilkesiyle bağdaşmayacaktır. Zira çalışanların mesai saatlerine riayeti ve görev performansı gibi hususlar, özel hayata daha az müdahale eden alternatif yöntemlerle denetlenebilir. Bu bağlamda, kamu hizmetinin etkin yürütülmesi ile çalışanların özel hayat hakları arasında hassas bir denge kurulması, her somut durumun kendi özellikleri çerçevesinde değerlendirilmesi ve ölçölülük ilkesinin gözetilmesi gerekmektedir.

Bu başlık altında değinilmesi gereken başka bir husus, toplanan verilerin aydınlatma metninde belirtilen amaç dışında ya da sonradan ortaya çıkan bir ihtiyaca dayalı başka bir amaçla işlenip işlenemeyeceğidir. 95/46 sayılı Direktif'te veri işleme faaliyetinin başlangıcında belirlenen amaçtan farklı yeni bir amaçla kişisel verinin işlenebilmesi mümkündür. Ancak sonradan ortaya çıkan amacın önceki amaçla uyumsuz (incompatible) olmaması gerektiği belirtilmiştir¹⁷³. Genel Veri Koruma

¹⁷¹ Danıştay 10.D., E. 2019/12230, K. 2021/41 (Lexpera).

¹⁷² Danıştay İDDK, E. 2021/1603, K. 2021/2631, (danistay.gov.tr).

¹⁷³ Madde 6(1)(b): *Member States shall provide that personal data must be: collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.*

Tüzüğü'nde ise halihazırda belirli bir amaçla toplanmış kişisel verilerin sonradan ortaya çıkan başka bir amaçla işlenebilmesi için başlangıçta belirlenen amaçla yeni amacın “uyumlu” olması gerektiği söylendikten sonra bu tespitin yapılmasında dikkate alınması gereken çeşitli kriterler belirlenmiştir. Tüzüğün 6. maddesinin 4. fıkrasına göre, sonradan ortaya çıkan amacın başta belirlenen amaçla uyumlu olup olmadığı tespit edilirken, iki amaç arasındaki bağlantı, verinin toplandığı bağlam özelinde veri sorumlusu ve ilgili kişi arasındaki ilişki, kişisel verilerin niteliği (örneğin hassas veri olup olmadığı), sonraki işlemenin ilgili kişi için muhtemel sonuçları ve yeterli koruma önlemi alınıp alınmadığı hususlarına dikkat edilmesi gerekir¹⁷⁴.

Öte yandan, 95/46 sayılı Direktif'in 6/1(b) maddesinde toplanan verilerin farklı amaçla işlenebilmesi için ilk amaçla sonraki amacın uyumlu olması gerektiği belirtildikten sonra, düzenlemenin ikinci cümlesinde üye Devletlerin uygun önlemleri sağlaması şartıyla, verilerin tarihsel, istatistiksel ve bilimsel amaçlarla daha fazla işlenmesinin uyumsuzluk olarak kabul edilmeyeceği ifade edilmiştir. Başka bir deyişle, belirli bir amaç için toplanan verilerin daha sonra tarihsel, istatistiksel ve bilimsel amaçlarla işlenmesi halinde, iki amacın “uyumlu” olduğu kabul edilecektir. Genel Veri Koruma Tüzüğü'nün 5/1(b) maddesinde göre ise, kamu yararına arşivleme amaçları, bilimsel ve tarihi araştırma amaçları veya istatistiksel amaçlar için kişisel verilerin tekraren işlenmesi ilk amaçlarla uyumsuz kabul edilmeyecektir. Öte yandan, 6698 sayılı Kanunun 28/1. maddesinin (b) bendi uyarınca “*kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi*” ve aynı fıkranın (c) bendi uyarınca “*kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliğini, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi*” hallerinde ilgili Kanun hükümlerinin uygulanmayacağı kabul edilmiştir. Görüldüğü üzere, Direktif ve Tüzük hükümleri uyarınca bazı hallerde ikincil veri işlemenin mümkün olduğu kabul edilirken bu ikinci işleme faaliyetine diğer Direktif ve Tüzük hükümleri uygulanmaya devam edecektir. Ancak 6698 sayılı Kanunda yer alan düzenleme gereği ilgili hususlar Kanunun tamamen kapsamı dışında bırakılmıştır.

95/46 sayılı Direktif ve Tüzük için halihazırda işlenmiş verilerin yeni bir amaçla işlenmesine çeşitli şartların karşılanması halinde imkân tanınmışken, 6698 sayılı Kanunumuzda buna ilişkin açık bir düzenleme bulunmadığı görülmektedir. Daha önce ifade edildiği üzere, sonradan ortaya çıkabilecek

Sonradan ortaya çıkan amacın başta belirlenen amaçla “ilgili” kabul edilebilmesi için her somut olayda, “*verilerin toplanma amaçlarıyla sonraki işleme amaçları arasındaki ilişki, verilerin toplandığı bağlam ve veri sahiplerinin daha sonraki kullanımlarına ilişkin makul beklentileri, verilerin niteliği ve sonraki işlemenin veri sahipleri üzerindeki etkisi ve adil işlemeyi sağlamak ve veri sahipleri üzerinde herhangi bir uygunsuz etkiyi önlemek için kontrolör tarafından uygulanan önlemleri*” göz önünde bulundurmak gerektiği 29. madde Çalışma Grubu raporunda ifade edilmiştir: Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, s. 23 vd, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (E.T. 6.1.2022).

¹⁷⁴ Ayrıntılı bilgi için bkz.: Cenk KONUKPAY/Uğur TABAK, “Kişisel Verilerin İşleme Amacının Sonradan Değişmesi: Uyumluluk Kriterlerinin Uygulanması Sorunu”, **Kişisel Verileri Koruma Dergisi**, C. 3, S.2, s. 19 vd.

muhtemel ihtiyaçların giderilmesine yönelik geniş kapsamlı genel bir amaçla ya da başlangıçta açıkça belirlenen bir amaç olmaksızın kişisel verilerin işlenmesi mümkün değildir. Kanunun 4/2. maddesinin (c) fıkrasında kişisel verilerin *belirli, açık ve meşru amaçlar için işlenmesi* ve (ç) fıkrasında *işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması* gerektiği ifade edilmiştir. Başlangıçta belirlenen amacın değişmesi halinde, belirlenen yeni amaç için de hukuka uygunluk koşullarının sağlanması gerekir. Bu hukuki dayanak 6698 sayılı Kanunun 5. maddesinde belirlenen kişisel verilerin işlenme şartlarından veya 6. maddesinde belirlenen özel nitelikli verilerin işlenme şartlarından birinin sağlanması olabileceği gibi yine çeşitli kanunlarda veri işlenmesine açıkça izin veren farklı bir hüküm de olabilir¹⁷⁵. Örneğin, 6698 sayılı Kanunun 5. maddesinde sayılan ve açık rıza alınmasına gerek bulunmayan durumlarda, söz gelimi yeni amacın veri sorumlusunun hukuki sorumluluğunu yerine getirebilmesi zorunluluğundan doğması ya da bu amaç doğrultusunda veri işlenebileceğinin kanunlarda açıkça öngörülmüş olması gibi hallerde ilgili kişiden açık rıza alınmaksızın daha önce toplanmış verilerin bu yeni amaçla işlenmesi, ilgili kişilere bu yeni amaca ilişkin aydınlatma yapılması şartıyla, mümkün olacaktır. Fakat ortaya çıkan yeni veri işleme amacı Kanunun 5. veya 6. maddelerindeki açık rıza alınması şartının istisnalarından birisi olarak kabul edilemezse, bu halde ortaya çıkan yeni amaç doğrultusunda veri işlemenin hukuka uygun olması için ilgisinden açık rıza almak gerekecektir¹⁷⁶.

3. İSTİSNA HÜKÜMLERİ NEDENİYLE 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU’NUN KAPSAMI DIŞINDA BIRAKILAN HALLER

Kanun koyucu 6698 sayılı Kanun’da yer alan üç farklı hükümle, ilgili Kanunun uygulanmayacağı halleri belirlemiştir. İlk olarak, “Tanımlar” başlıklı 3. maddesinde “kişisel veri” tanımı yapılırken “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” diyerek tüzel kişilere ait verileri kişisel veri olarak kabul etmemiştir. Böylelikle tüzel kişi verileri hakkında bu Kanun uygulanmamaktadır¹⁷⁷.

İkinci olarak Kanunun “Kapsam” başlıklı 2. maddesinde, verileri tamamen ya da kısmen otomatik olan veya herhangi bir veri kayıt sisteminin parçası haline getirmek kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında 6698 sayılı Kanun hükümlerinin uygulanacağı kabul edilerek, bir sisteme dayalı olmaksızın ya da sonradan herhangi bir sisteme dahil edilmeksizin veri işleyen kişiler ve işlenen veriler hakkında bu Kanun hükümlerinin uygulanmayacağı kabul edilmiştir.

¹⁷⁵ Konuya ilişkin örnek bir karar olarak KVK Kurulu’nun 25.3.2019 tarih ve 2019/78 sayılı kararına bakılabilir: <https://www.kvkk.gov.tr/Icerik/5434/2019-78> (E.T.10.1.2022).

¹⁷⁶ KONUKPAY/TABAK, s.28.

¹⁷⁷ Ayrıntılı bilgi için bkz.: “1.2. İlgili Kişi” başlığı.

Son olarak, Kanunun “İstisnalar” başlıklı 28. madde hükmünün 1. fıkrasıyla Kanunun uygulanmayacağı veri işleme halleri, 2. fıkrasıyla da Kanunun 10., 11. ve 16. hükümlerinin uygulanmayacağı veri işleme halleri düzenlenmiştir.

Kanunun kapsamı dışında bırakılan ilk iki hususa çalışmanın birinci bölümünde “Kişisel Veri Kavramı” başlığı altında değinildiğinden, burada Kanunun 28. madde düzenlemesi ele alınacaktır.

3.1. Tamamen Kanun Kapsamı Dışında Tutulan Haller

Kanunun 28. maddesinin ilk fıkrasında “Bu Kanun hükümleri aşağıdaki hallerde uygulanmaz” kuralına yer verilerek beş ayrı bent ile sayılan hallerde 6698 sayılı Kanunun uygulanmayacağı kabul edilmiştir. Belirlenen kişisel veri işleme halleri şu şekildedir:

“a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.”

Hükmün “a” bendi İdare Hukuku kapsamında bulunmadığından diğer istisna halleriyle ilgili açıklamalara yer verilecek olmakla birlikte, bu ilk bent hakkında da kısaca şunlar söylenebilir. Kanun koyucu, gerçek kişilerin kendisiyle ya da aynı konutta yaşadığı aile fertleriyle ilgili işleyeceği kişisel verileri Kanun kapsamı dışında bırakmak istemiştir. Böylelikle gerçek kişilerin belirli sınırlar içerisinde gereğinden fazla zorlukla karşı karşıya kalınması istenmemiştir¹⁷⁸. Bu halde, örneğin kişinin ailesiyle birlikte yaptığı bir doğum günü kutlamasına ilişkin anları kayıt altına alması, fotoğraflaması eylemine Kanun hükümleri uygulanmayacaktır. Kişi bu video kayıtlarını ya da fotoğrafları kendi bilgisayarında saklayabilecektir. Bununla birlikte, eylemin tamamen kendisiyle ilgili ya da aynı konutta yaşadığı aile fertleriyle ilgili olması, başka bir deyişle “ailevi kullanım faaliyetleri” amacıyla işlenmesi gerekir.

¹⁷⁸ ÇEKİN, s. 31.

Doğum gününe ait görüntülerin çeşitli şekillerde alenileştirilmesi, farklı kişilerle paylaşılması halinde istisna hükmünden bahsedilemeyecektir¹⁷⁹. Ayrıca, veri işlemenin mesleki ya da iktisadi bir amaç taşıması halinde de istisnai hüküm geçerli olmaz¹⁸⁰.

- Kişisel Verilerin Resmi İstatistik ile Anonim Hâle Getirilmek Suretiyle Araştırma, Planlama ve İstatistik Gibi Amaçlarla İşlenmesi: İdarenin elindeki sınırlı maddi güç ve insan kaynağı sebebiyle vatandaşlara sunulacak kamu hizmetlerinin verimli ve sürdürülebilir olması şarttır. Bu bağlamda İdare elde ettiği verileri araştırma, planlama ve istatistiki sonuçlar üretmek amacıyla kullanır ki böylece kamuya sunulacak hizmetler ihtiyaca göre belirlenebilsin ve kaynak israfına engel olunabilsin. İşte, İdarenin resmi istatistik ve anonim hale getirilmek şartıyla araştırma, planlama ve istatistik gibi amaçlarla kişisel veri işlemesi 6698 sayılı Kanun kapsamında çıkarılmıştır.

Söz konusu bendin bir istisna hükmü olduğu ve dolayısıyla dar yorumlanması gerektiği düşünüldüğünde, “araştırma, planlama, istatistik gibi amaçlarla işlenmesi” denilmek suretiyle sayılanların sadece bir örnekleme olduğu ve artırılabilmesi izlenimi olduğundan, eleştiriye açık bir düzenleme olduğu söylenebilir. Bununla birlikte, cümlelerin “resmi istatistik” ile “anonim hale getirilmek suretiyle araştırma, planlama, istatistik gibi” amaçlarla işlenmesi şeklinde iki parçadan oluşması önemlidir. Nitekim, ikinci parçanın “anonim hale getirme” şartını içermesi, tabiri yerindeyse bu “arızın” sonuçlarını ortadan kaldıracı niteliktedir. Çünkü, 6698 sayılı Kanunun “Tanımlar” başlıklı ikinci maddesinde anonim hale getirme “*Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi*” şeklinde tanımlanmıştır. Dolayısıyla, anonim hale getirilmiş bir verinin kime ait olduğunun belli olmadığı, ya da farklı verilerle ilişkilendirilerek dahi kime ait olacağının belirlenemeyeceği düşünüldüğünde, bu şekilde anonimleştirilen verilerin artık Kanuni tanım bağlamında kişisel veri olmayacağı ortadır. Bu sayede, ilgili bent düzenlemesindeki “gibi amaçlarla” şeklindeki ifadenin lafzi anlamda doğru bir düzenleme olmadığı söylenebilirse de olumsuz sonuçlar doğurmayacağı düşünülmektedir. Öte yandan, anonimleştirilmiş verinin Kanun bağlamında kişisel veri kabul edilmediği de düşünüldüğünde, bu verilerin Kanun kapsamı dışında tutulduğu yönündeki düzenlemenin “malumun ilamı” niteliğinde olduğu ifade edilmelidir.

Öte yandan, ilgili hükmün ilk parçasına, yani “resmi istatistik amacıyla işlenmesi” kısmına gelince, resmi istatistik ifadesinin mevzuattaki karşılığı bulunmakla Kanun dışında bırakılan ve istatistik

¹⁷⁹ “6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı”, Kişisel Verileri Koruma Kurumu, s.8: <https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami> (E.T. 17.9.2023).

¹⁸⁰ ÇEKİN, s.31. Günümüzde çok sık karşılaştığımız, sosyal medyada “influencer” olarak bilinen ve çocuklarının, diğer aile bireylerinin görüntülerini paylaşarak kazanç elde eden kişilerin yapmış olduğu tüm bu veri işleme faaliyetlerinde 6698 sayılı Kanunun uygulanacağı muhakkaktır.

amacıyla tutulan bu verilerin hangileri olduđu ortaya ıkacaktır. 5429 sayılı Trkiye İstatistik Kanunu’nun 2/1/g maddesinde “resmi istatistik” ifadesi tanımlanmıştır. Buna gre resmi istatistik “Trkiye İstatistik Kurumu veya (Resmi İstatistik) Program(ın)da yer alan konularda istatistik retecek kurum ve kuruluşlar tarafından derlenen verilerin, kitle zelliklerini ortaya koymak amacıyla işlenmesi ile elde edilen bilgi” anlamına gelmektedir. Bu tanımda geen “kurum ve kuruluşlar” ifadesinin ieriğine bakıldığında ise resmi istatistik amacıyla işlenebilecek verilerin byklđ ortaya ıkmaktadır. 5429 sayılı Kanunun yine 2/1/e maddesinde yapılan tanıma gre Trk İdari Teşkilatının tamamı ve hatta fazlası resmi istatistik ifadesinin tanımında bahsedilen kurum ve kuruluşlardan sayılmıştır¹⁸¹. İfade etmek gerekir ki, burada sayılan İdarelerin yapmış olduđu tm veri işleme faaliyetleri deđil, sadece kitle zelliklerini ortaya koymak amacıyla işlenerek elde edilen bilgiler 6698 sayılı Kanun kapsamı dışında bırakılmaktadır.

İlgili veriler 6698 sayılı Kanun kapsamı dışında bırakılmakla birlikte bunların korunmasına ilişkin 5429 sayılı Kanun’da eşitli hkmlere yer verilmiş ve yine Trkiye İstatistik Kurumu tarafından Resmî İstatistiklerde Veri Gizliliđi Ve Gizli Veri Gvenliđine İlişkin Usul Ve Esaslar Hakkında Ynetmelik ıkarılmıştır¹⁸². 5429 sayılı Kanunda ilgilinin dođrudan ya da dolaylı şekilde tanınabilmesini ve bylece kişisel bilgilerinin aıđa ıkarılmasına imkân sađlayan, bireysel ya da tablo halinde saklı tutulan veriler “gizli veri” olarak kabul edilmiş (madde 2/1/s) ve bu gizli verileri işleyen kurum ve kuruluşlar iin eşitli ykmllđler ngrlmştr. Nitekim, Kanunun 13. maddesinde gizli verilere erişimin yalnızca resmi istatistik retiminde grev alanlarla sınırlanması gerektiđi; resmi istatistik amacıyla işlenen verilerin idari, adli ve askeri hibir organ, makam, merci veya kişiyeye verilemeyeceđi, istatistik amacı dışında kullanılamayacađı, bunların ispat aracı olamayacađı; bu bilgileri derleyen ve deđerlendiren memurların grevlerinden ayrılmalardan sonra da devam edecek şekilde ilgili yasalara uyması gerektiđi belirtilmiştir. te yandan aynı madde hkmnde herkes tarafından erişilebilen kaynaklardan elde edilen bilgilerin gizli veri olarak kabul edilmeyeceđi ve ilgilisinin kendisine ait kişisel verilerin aıklanmasına yazılı onay vermesi halindeyse veri gizliliđinin ortadan kalkacađı kabul edilmiştir.

Yine, 5429 sayılı Kanunun 15. maddesinde istatistikî birimlerin (ilgililerin) haklarına yer verilmiştir. Buna gre kişisel verileri resmi istatistik amacıyla işlenen ilgililer, sayımın veya araştırmının amacını, kapsamını ve veri gizliliđinin sađlanması iin alınan nlemleri đrenme, 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamında bilgi edinme haklarını kullanma ve kendilerine ait gizli

¹⁸¹ **5429 sayılı Kanun, madde 2/1/e :** “Kurum ve kuruluşlar: Cumhurbaşkanlıđı ve bakanlıklar ile bunların bađlı, ilgili ve ilişkili kuruluşlarını, mahallî idareler ve bunların bađlı ve ilgili kuruluşları ile birlik ve şirketlerini, Trkiye Cumhuriyet Merkez Bankası, İstanbul Menkul Kıymetler Borsası ve niversiteler de dâhil olmak zere, tzel kişiliđi haiz enstit, teşebbs, teşekkl, birlik, dner sermaye, fon ve sair adlarla kurulmuş olan diđer kurum ve kuruluşlar ile kamu kurumu niteliđindeki meslek kuruluşlarını, ifade eder.”

¹⁸² RG, 20.06.2006/26204.

verinin izinsiz açıklanması durumunda da maddi ve manevi her türlü zararının tazmin edilmesini isteme haklarına sahiptir.

- Kişisel Verilerin Sanat, Tarih, Edebiyat veya Bilimsel Amaçlarla ya da İfade Özgürlüğü Kapsamında İşlenmesi: 6698 sayılı Kanunun 28/1/c maddesine göre kişisel verilerin sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi halinde bu veri işleme faaliyetine ilgili Kanun hükümleri uygulanmayacaktır. Ancak, kuralın geçerli olabilmesi için bu veri işlemenin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemesi şartlarını karşılaması gerekir. Veri işleme faaliyetinin söz konusu şartları ihlal edip etmediği somut olay bağlamında her seferinde incelenmesi gerekecektir. Öte yandan, düzenlemenin özellikle ifade özgürlüğü kapsamında işlenip işlenmediği değerlendirilirken menfaat dengesinin kurulması gerektiğini işaret ettiği ifade edilmektedir¹⁸³.

Düzenlemenin en fazla dikkat çeken kısmının kişisel verilerin ifade özgürlüğü kapsamında işlenmesi hâli olduğu söylenebilir. Anayasa'nın 26. maddesinde düzenlenen 'düşünceyi açıklama ve yayma hürriyeti' ile bununla bağlantılı ve yine Anayasanın 28. maddesinde düzenlenen 'basın hürriyeti' nin kişisel verilerin korunması hürriyeti ile çatıştığı durumlar sık sık yaşanmakta, bu durum Kurul kararlarına da yansımaktadır¹⁸⁴. Bu kapsamda Kurul, ifade özgürlüğü ile özel hayatın gizliliği gibi kişilik haklarının çatıştığı durumlarda denge testinin yapılarak çatışan hakların durumuna göre karar verilmesi gerektiğini ifade etmektedir. Buna göre *"basın özgürlüğü söz konusu iken ilgili kişi açısından da kişisel verilerin korunmasını isteme hakkının söz konusu olduğu, dolayısıyla basın özgürlüğü ile kişisel verilerin korunmasını isteme hakkının karşı karşıya olduğu, haberdan beklenen yarar ile ilgili kişinin kişisel verilerinin korunmasını isteme hakkından beklediği meşru çıkarın karşılaştırılması gerektiği ve bunun için temel ölçütün ise kamu yararı olduğu, gerek yazılı ve gerek görsel basın tarafından bu işlev yerine getirilirken, yayının kamu ilgi ve yararının bulunması ile gerçek ve güncel olmasının sağlanmasının ve haberi verirken özle biçim arasındaki dengenin korunmasının gerektiği"* ifade edilmiştir¹⁸⁵. Örneğin, Türkiye'de tanınmış bir kişi olan ilgilinin evinde gerçekleşen hırsızlık olayının üç dört gün sonrasında olayı haberleştiren gazete tarafından olaya ilişkin detaylarla birlikte ilgilinin açık ev adresine de yer vermesi hakkında karar veren AİHM, bazı özel koşullarda, ünlü kişilerin özel hayatı hakkında yapılan yayınların toplumun genel menfaatine aykırı olmayabileceğini hatırlatmakla birlikte, somut olayda, ilgilinin rızası alınmaksızın açık ev adresinin ülke genelinde yayımlanan bir gazetede ifşa edilmesinin toplum menfaatleri için gerekli olduğunu ortaya koyacak haklı bir gerekçe bulunmadığına,

¹⁸³ ÇEKİN, s.32; TANSUĞ, s. 65; KÜZECİ, **Kişisel Verilerin Korunması**, s. 379.

¹⁸⁴ KVK Kurulu, 6.1.2022 tarih ve 2022/13 sayılı; 2.12.2021 tarih ve 2021/1217 sayılı; 30.9.2021 tarih ve 2021/989 sayılı; 22.5.2020 tarih ve 2020/414 sayılı kararları.

¹⁸⁵ KVK Kurulu, 6.1.2022 tarih ve 2022/13 sayılı kararı.

bu nedenle ilgili haberin sunuluş biçiminin başvuranın özel hayata saygı hakkını ihlal niteliği taşıdığı sonucuna varmıştır¹⁸⁶.

KVK Kurulu tarafında, veri işleme faaliyetinin belirlenen şartlara uygun olmadığının tespiti halindeyse bu kez işlenen verinin niteliğine göre Kanunun 5. ve 6. maddeleri ile diğer ilgili maddelerine göre inceleme yapılmakta ve şikâyet konusu veri işleme faaliyetinin 6698 sayılı Kanuna uygun olup olmadığı değerlendirilmektedir. Örneğin, üniversiteyi kazanan adayların sevincini haberleştiren bir yayında T.C. kimlik numarası kısmı gizlenerek ilgiye ait sonuç belgesine yer verilmiştir. Bu belgede ise ilgilinin adı soyadı, fotoğrafı, yerleştiği üniversite adı ve puan bilgisi yer almaktadır. İlgili tarafından yapılan şikâyet hakkındaki değerlendirmesinde Kurul “*biçim ve öz arasındaki denge açısından haberlerde kullanılan dil ve ifadenin gerektirdiği ölçüde olduğu ve haberlerin verilişinde gerekli, ilgili ve yararlı olmayan beyan ve değerlendirmelerde bulunulmadığı sonucuna varılması sebebiyle habere konu kişisel veriler açısından öz ile biçim arasındaki denge kriterine muhalefet edilmediği anlaşılmakla beraber, söz konusu haberin ilgili kişinin yüksek bir başarısı olduğundan bahisle yapılmadığı, yalnızca üniversiteyi kazanan gençlerden birinin örneğinin verildiğinin görüldüğü, bu sebeple haberin toplumda sık rastlanan bir olay olduğu ve haberdeki olayın toplumu konu üzerinde düşünmeye sevk etmediği ve dolayısıyla bir kamu yararı bulunmadığı kanaatine varılmış olup söz konusu haberde gerçekleştirilen kişisel veri işleme faaliyetinin Kanunun 28 inci maddesinin (1) numaralı fıkrasında düzenlenen ifade özgürlüğü kapsamında değerlendirilemeyeceği ve söz konusu kişisel veri işleme faaliyetinin istisna kapsamında olmadığı*” sonucuna varmış, ardından şikâyetle ilişkin veri işleme faaliyetinde 6698 sayılı Kanunun 5. ve 6. maddelerinde sayılan kişisel verilerin işleme şartlarından birinin bulunmaması nedeniyle veri işleme faaliyetinin Kanuna aykırı olduğuna ve veri sorumlusu hakkında idari para cezası uygulanmasına karar vermiştir¹⁸⁷.

Yukarıdaki kararlardan da görüleceği üzere Kurul, basın yoluyla kişisel verilerin işlenmesi halinde bu veri işleme faaliyetinin 28/1-c kapsamında kalıp kalmadığını irdelerken kamu yararının varlığı, haberin gerçek ve güncel olması ve haberde biçim ve öz arasındaki dengenin sağlanmış olması şartlarının birlikte gerçekleşmesini aramaktadır. Haberde kullanılan dil ve ifadenin gerektiği ölçüde kalması ve haberde yer verilen beyan ve değerlendirmelerin gerekli, haberle ilgili ve yararlı olması halinde haberde biçim ve öz arasındaki denge sağlanmış olacaktır. Ayrıca, haberin toplumda sıkça rastlanan bir olaydan ziyade “toplumu konu üzerinde düşünmeye sevk eden” türden olması halinde kamu yararının varlığı kabul edilecektir.

¹⁸⁶ AİHM, Alkaya / Türkiye, B.n. 42811/06, T. 9.11.2012, <https://hudoc.echr.coe.int/eng?i=001-125912>. Ayrıca bkz.: Bir radyo programında başvuranın kız kardeşinin inisiyatifıyla başvuranın ve eski eşinin kişisel verilerini içeren mektubun okunmasına ilişkin karar AİHM, Marina / Romanya, B.n. 504669/14, T. 26.5.2020; Taşıyıcı anne aradığına yönelik gazete ilanı vermesinin ardından, bir araştırmacı gazetecinin başvuran ile “taşıyıcı anne adayı” gibi iletişime geçerek, bilgisi olmaksızın fotoğraflarını çekmesi, aralarında geçen konuşmaları kayıt altına alması ve bunları “Doğmamış Çocukların Ticareti” başlıklı bir haber olarak yayımlaması üzerine verilen karar AİHM, Hájovský / Slovakya, b.n. 7796/16, T. 1.7.2021.

¹⁸⁷ KVK Kurulu, 6.1.2022 tarih ve 2022/13 sayılı kararı.

İdarenin ifade özgürlüğü kapsamında kişisel veri işleyip işleyemeyeceğine gelince, Anayasa’da yer alan temel hak ve özgürlüklerin birer insan hakkı olduğu, İdareninse bu hakların bireyler tarafından eşit şekilde kullanılmasını sağlamakla görevli olduğu, bu haklardan birinin kullanıcısı olamayacağı için 6698 sayılı Kanunun 28/1-c maddesi bağlamında ifade özgürlüğü kapsamında kişisel veri işleyemeyeceği söylenebilir de; İdarenin bazı temel hakların bireyler tarafından eşit şekilde kullanılmasını sağlamak için pozitif yönde hareket etmesi gerektiği, ifade özgürlüğü kapsamında bireylerin haber alma haklarını kullanabilmesine yardımcı olmak adına bir kamu tüzel kişisi olan Türkiye Radyo ve Televizyon Kurumu (TRT)’na bağlı olarak birçok radyo ve televizyon kanalında yapılan yayınlar aracılığıyla kendisine kanunla verilen görevleri yerine getirdiği¹⁸⁸, dolayısıyla bu amaçla işlenen kişisel verilerin de ifade özgürlüğü hakkının sahibi tarafından olmasa da bu hakkın kullanımının sağlanması amacıyla yine bu hak kapsamında işlendiği kabul edilmelidir. Nitekim, 6698 sayılı Kanunun ilgili hükmüne bakıldığında kişisel verilerin ‘ifade özgürlüğü kapsamında’ işlenmesinden bahsedilmektedir. Dolayısıyla, ifade özgürlüğünün kullanılmasının sağlanmasına yönelik eylemlerin de “ifade özgürlüğü kapsamı” içerisinde kabul edilebileceği söylenebilir. 6698 sayılı Kanunun 28/1-c maddesi uyarınca ifade özgürlüğü ve kişisel verilerin korunması hakkı kapsamında sağlanması gereken menfaat dengesi ise verisi işlenen kişinin kişisel verilerinin korunması hakkı ile diğer bireylerin haber alma hakkı arasında gözetilerek sağlanacaktır¹⁸⁹.

İtalya’da bulunan bir özel okulda öğretmenlik yapan başvuranın da dahil olduğu bir grup kişi hakkında İtalya savcılığınca okulun maddi yönetimindeki usulsüzlüklere ilişkin bir soruşturma başlatılmıştır. Soruşturma uyarınca toplanan dosyaya başvuranın parmak izleri ve görevliler tarafından tutuklama sırasında çekilen fotoğrafı da dahil edilmiştir. Suç soruşturması devam ederken polis tarafından bir basın toplantısı yapılmış ve soruşturmaya ilişkin basına bilgi verilmiştir. Olayı haberleştiren bir gazete, haber metninde başvurana ait tutuklama sırasında çekilen fotoğrafı kullanmıştır. Tutuklama sırasında resmi görevlilerce dosyaya konulmak üzere çekilen fotoğrafın basınla paylaşılmasının özel hayata saygı hakkını ihlal ettiği yönündeki şikâyeti inceleyen AİHM, başvuranın kamuya mal olmuş veya siyasetçi olmadığını, ilgili fotoğrafın yayımlanmasının özel hayatın gizliliği

¹⁸⁸ 2954 sayılı Türkiye Radyo ve Televizyon Kanunu’nun 5. maddesine göre “Haberlerin toplanması, seçilmesi ve yayınlanmasında tarafsızlık, doğruluk ve çabukluk ilkeleri ile çağdaş habercilik teknik ve metotlarına bağlı olmak”, “Haberler ile yorumları ayırmak ve yorumların kaynaklarını açıklamak” ve “Kamuoyunun sağlıklı ve serbestçe oluşabilmesi için kamuoyunu ilgilendirecek konularda yeterli yayın yapmak; tek yönlü, taraf tutan yayın yapmamak ve bir siyasi partinin, grubun, çıkar çevresinin, inanç veya düşüncenin menfaatlerine alet olmamak” TRT’nin genel yayın esasları arasında sayılmıştır.

¹⁸⁹ İfade özgürlüğü, birçok hak ve özgürlüğün merkezini oluşturmaktadır. AİHS’in 10. maddesinde “Herkes ifade özgürlüğüne sahiptir. Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü de kapsar” denilmek suretiyle ifade özgürlüğünün kaynaklık ettiği, bu hak kapsamında kabul edilen diğer hak ve özgürlükler gösterilmiştir. Benzer şekilde Anayasanın 26. maddesinin 1. fıkrasında da “Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet Resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar” şeklindeki hüküm yer almaktadır. Görüldüğü üzere ifade özgürlüğü, haber alma ve haber verme özgürlüklerini de kapsamaktadır.

kapsamına girdiğini, fotoğrafın resmi bir amaç için çekilmiş olup, İdare tarafından basına servis edildiğini tespit etmiştir. Hükümet yaptığı savunmada, kişinin özel hayatına saygı gösterilmesi hakkının, halkın bilgilendirme hakkı ve başka suçların önlenmesi amacı ile sınırlı olduğunu, mevcut başvuranın resmi makamlarca suçlu bulunduğunu ve mahkûm edildiğini, suçun bir okulun yönetimiyle ilgili olması nedeniyle de toplum çıkarlarını ilgilendirdiğini, dolayısıyla müdahalenin hukuka uygun olduğunu ileri sürmüştür. Mahkeme ise, özel hayatın gizliliği hakkına bir müdahale olduğunu teyit ettikten sonra, müdahalenin Mahkeme içtihatlarına uygun yasal bir dayanağının bulunmadığını, daha çok uygulamanın bu şekilde gerçekleştiğini tespit etmiş, bu sebeple, fotoğrafın paylaşılmasının hukuka uygun olmadığına, başvuranın özel hayatın gizliliği hakkına haksız müdahalede bulunulduğuna karar vermiştir¹⁹⁰.

28/1-c maddesinde düzenlenen bir başka konuya, bilimsel amaçlarla kişisel veri işlenmesi halidir. İlgili Kanunda “bilimsel amaç” ifadesinin tanımına yer verilmemiştir. İlk akla gelen sağlık verilerinin işlenmesi hususu olsa da bilimsel amaçlarla toplumsal, sosyolojik, ekonomik vb. birçok konuda çalışmalar yapılabileceği söylenebilir. Nitekim, soru soran, bu sorulara ampirik araştırma yöntemlerini kullanarak cevap arayan, sonuçları doğrulanabilir, ölçülebilir ve tekrar gözlemlenebilir olan araştırmalar bilimsel araştırma olarak kabul edilmektedir¹⁹¹. Dolayısıyla kişisel verilerin bilimsel amaçlarla işlenmesi halinde bu veri işlemenin Kanun kapsamı dışında kalacağına yönelik hüküm bir istisna hükmü olduğu da düşünüldüğünde geniş bir alanı Kanun kapsamı dışına çıkardığı için eleştiriye açıktır. Bununla birlikte, bilimsel araştırmalarla kamu yararına yönelik birçok alanda ilerleme ve gelişmeler sağlandığından, bu amaçla yapılan veri işleme faaliyetleri bakımından bireylerin kişisel verilerinin korunması hakkından kısmı bir fedakârlık yapması beklenebilir bir durumdur¹⁹². Nitekim, bilimsel amaçla kişisel verilerin işlenmesi Kanun kapsamı dışına çıkarılmışsa da tamamen serbest bir alan olduğu savunulamaz.

KVK Kurulu tarafından yayımlanan “Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”de bilimsel amaçla işlenecek olan genetik verilerinin Kanun kapsamı dışında da olsa öncelikle Kişisel Sağlık Verileri Hakkında Yönetmeliğin kişisel sağlık verilerinin bilimsel araştırmalarda kullanımına ilişkin koşulları düzenleyen 16. maddesine uygun şekilde işlenmesi, son çare olma ilkesi gereği bilimsel araştırmadan beklenen sonuca ulaşılabilmesi için verinin işlenmesinin zorunlu olması, hakkın korunması için gerekli tüm tedbirlerin alınması ve bu bağlamda ölçülülük ilkesine uygun hareket edilmesi ile kullanılan kişisel verilerin ihtiyaç süresinin doğru şekilde saptanarak

¹⁹⁰ AİHM, Sciacca / İtalya, B.n. 50774/99, T. 11.1.2005, <https://hudoc.echr.coe.int/eng?i=001-67930>.

¹⁹¹ Aydın USTA, “*Bilimsel Araştırmalarda Yapısal Etmenler ve Evreler*”, **İnönü Üniversitesi Uluslararası Sosyal Bilimler Dergisi**, C.1, S.1, 2012, s. 99 vd., <https://dergipark.org.tr/tr/pub/inijoss/issue/8624/415750> (E.T. 13.10.2023)

¹⁹² ŞİMŞEK, s.124. Nitekim Genel Veri Koruma Tüzüğü (GDPR) ile de veri koruma hakkının özüne saygı duymak ve veri sahibinin temel hak ve hürriyetlerini ve menfaatlerini korumak şartıyla bilimsel amaçlarla ve kamu yararına yönelik veri işlemenin ilgilinin açık rızası bulunmasa bile yasal olduğu düzenlenmiştir. Bilimsel araştırmaların kamu yararı taşıdığı da düşünüldüğünde kişisel verilerin işlenmesi faaliyetinin meşru kabul edildiği, yeterli korumanın sağlanmasıyla veri işlemenin hukuka uygun olacağı ifade edilmiştir: Sabire Sanem YILMAZ, “Bilimsel Amaçlı Kişisel Veri İşlenmesine Hukuki Bakış”, **kisiselveriilhali.com**, 8.12.2021 (E.T. 13.10.2023).

daha fazla ihtiyaç duyulmayan kişisel verilerin imha edilmesini sağlayacak mekanizmaların oluşturulması gerektiği ifade edilmiştir¹⁹³.

KVK Kurulu kararına yansıyan bir olayda, bir doktor daha önce çalıştığı Sağlık Bakanlığına bağlı bir hastanede kronik hastalıklara ilişkin bilimsel çalışmalar yapıldığını, bu amaçla hastalara ait kan, serum ve doku örneklerinin toplandığını, ancak bunların korunması için gereken önlemlerin alınmadığı için bozulması üzerine tamamının çöpe atıldığını, dolayısıyla 6698 sayılı Kanunun 12. maddesi uyarınca veri güvenliğine ilişkin yükümlülüklerin yerine getirilmediğinden bahisle Kurula şikâyetinde bulunmuştur.

Kurul tarafından yapılan incelemede, toplanan verilerin tasnif ediliş biçimleriyle kimlere ait olduğunun belirlenebilir olması nedeniyle ortada bir kişisel veri işleme faaliyeti bulunduğunu tespit etmiştir. Bununla birlikte Kurul *“Hastalardan alınan kan, serum ve doku örneklerinin bilimsel amaçlarla kaydedildiği Kanunun 28 inci maddesi kapsamında bu verilerin işlenmesinin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmediği ya da suç teşkil etmediği değerlendirildiğinden şikâyet hakkında bu aşamada yapılacak bir işlem olmadığı”* yönünde karar vermiştir.

- Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Kapsamında İşlenmesi: 6698 sayılı Kanunun 28/1-ç maddesine göre kanunla görev ve yetki verilmiş kamu kurum ve kuruluşlarının yürüttüğü önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenen kişisel veriler 6698 sayılı Kanun kapsamı dışında bırakılmıştır. Ancak kişisel veriler millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olarak işlenmesi gerekir. Aksi halde söz konusu kamu kurum ve kuruluşlarının işleyeceği veriler için yine 6698 sayılı Kanun hükümleri geçerli olacaktır.

Öğretide ilgili hükümde yer verilen önleyici, koruyucu ve istihbari faaliyet kavramlarının çok geniş kapsamlı olduğu ve bu kavramların sınırlarının çizilmesinin zor olduğu gerekçeleriyle eleştirilen düzenleme¹⁹⁴ aynı zamanda Kanunun çeşitli maddelerinin iptali için yapılan başvuruda Anayasa Mahkemesi tarafından da incelenmiştir¹⁹⁵. İptal talebinin başvuru gerekçesi, mezkûr kavramların genişliği ve belirsizliği nedeniyle İdarenin keyfi uygulamalarına sebebiyet verebilecek olması, kamu kurumlarının veri işleyebileceği hallerin sayma yoluyla belirlenmesi gerektiği aksi halde özel hayatın gizliliği hakkının özüne dokunulmuş olacağı, mevcut haliyle sınırları belirsiz olan hükmün ilgili hakka doğrudan müdahale niteliği taşıdığı yönündedir.

¹⁹³ Kişisel Verileri Koruma Kurumu, **KVKK Yayınları No: 43**, s.36-37, kvkk.gov.tr (E.T. 13.10.2023).

¹⁹⁴ TANSUĞ, s.71.

¹⁹⁵ AYM, E.2016/125, K.2017/143, T. 28.9.2017.

Yüksek Mahkeme tarafından yapılan incelemede öncelikle Anayasa’da özel sınırlama sebepleri öngörülme­yen özgürlükler için de o özgürlüklerin doğasından kaynaklanan bazı sınırları olabileceği, bu bağlamda Anayasa’da yer alan diğer özgürlüklere getirilen sınırlama sebepleri ile Devlete verilmiş ödevlerin özel sınırlama sebebi öngörülmemiş özgürlükler için de bir sınır kabul edilebileceği, dolayısıyla Devletin görevlerinden olan milli güvenliğin ve kamu güvenliğinin sağlanması ile suç işlenmesinin önlenmesi amaçlarıyla özgürlüklerin sınırlanabileceği tespiti yapılmıştır. Bununla birlikte, özgürlüklerin sınırlanmasının sınırını belirleyen Anayasanın 13. maddesi hatırlatılmıştır (§153-154). Buna göre *“Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”*

Kararda, söz konusu sınırlamanın devletin Anayasa’yla kendisine verilen görevleri yerine getirebilmek için, başka bir deyişle milli güvenliği, kamu düzenini ve suç işlenmesinin önlenmesini sağlayabilmek için getirilmiş olması sebebiyle demokratik toplum düzeninin gereklerine uygun olduğu ifade edilmiştir (§157).

Kuralda yer verilen kavramların soyut olduğu yönündeki şikâyetler içinse, bu durumun kanun yapma tekniğinden kaynaklandığı, kuralın genel ve soyut olmasının tüm çözümleri kuralın içerisine dahil etme ya da kuralın amaçla uyumlu herhangi bir çözümü kapsam dışında bırakmama çabasından kaynaklandığı vurgulanmıştır. Öte yandan, kural gereği veri işleyecek İdarelerin belirsiz olduğu, hangi hallerde veri işleyebileceğinin belirlenmesi gerektiği yönündeki itirazı ise Mahkeme şu gerekçelerle haksız bulmuştur:

“159. Öte yandan 2559 sayılı Polis Vazife ve Salahiyet Kanunu, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu gibi ilgili kuruluş kanunlarında görev ve yetki verilmiş polis teşkilatı ve MİT gibi veya 4208 sayılı Kanun’la kurulan, görev ve yetkileri 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile yeniden belirlenen Malî Suçları Araştırma Kurulu (MASAK) gibi kamu kurum ve kuruluşlarının dava konusu kuralda yer alan millî güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliğini sağlamaya yönelik olarak kanunla görev ve yetki verilen kamu kurum ve kuruluşları olduğu açıktır. Bu kanunlarda, söz konusu kamu kurum ve kuruluşlarının görev ve yetkileri ayrıntılı şekilde düzenlenmiş ve bu düzenlemelerde söz konusu görevlerin Türkiye Cumhuriyeti’nin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilecek mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını oluşturmak veya suç gelirlerinin aklanmasının önlenmesini sağlamaya yönelik olduğu belirtilerek bu kamu kurum ve kuruluşları tarafından yürütülecek önleyici, koruyucu ve istihbari faaliyetler de düzenlenmiştir. Bu bağlamda dava konusu kuralla düzenlenen “önleyici, koruyucu ve istihbari” faaliyetlerin ilgili

kuruluş kanunlarında veya diğer kanunlarda kapsam, sınır ve içeriklerinin ayrıntılı şekilde düzenlenmesi karşısında söz konusu faaliyetlerin kapsamının belirsiz olduğu söylenemez.”

Ayrıca kararda, kişisel verilerin amacı dışında kullanılmasını önlemeye yönelik 5237 sayılı Türk Ceza Kanunu’nda yer verilen düzenlemelerle özel hayata dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyen yasal güvencenin sağlandığı, ilgili İdarelerde görev alan kişiler için de bu düzenlemelerin geçerli olduğu düşünüldüğünde “*dava konusu kurallarla kişisel verilerin korunması hakkına getirilen sınırlamaların özel hayatın gizliliği ve kişisel verilerin korunması hakkının özünü zedelenmediği gibi bu haklar ile ülkede millî güvenliğin sağlanmasına yönelik önlemler arasındaki makul dengenin kurulduğu*” ve demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine aykırılığın da bulunmadığı sonucuna varılmıştır (§160).

Gerçekten de Mahkeme tarafından değinilen 2559, 2937 ve 4208 sayılı kanunlar gibi ilgili kamu kurumlarının kuruluş kanunlarında önleyici, koruyucu ve istihbari faaliyetler ve bunları yerine getirmekle görevli İdareler düzenlenmiş olmakla 6698 sayılı Kanunun 28/1-ç hükmünün sınır ve içeriklerinin belirlendiği söylenebilir. Bununla birlikte, 28/1-ç maddesinde yer alan kural ile aynı maddenin ikinci fıkrasında yer verilen 28/2-a hükmü karşısında ortaya çıkan belirsizlik gözden kaçırılmamalıdır. Nitekim, 28/1-ç kuralına göre millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak önleyici faaliyetler kapsamında işlenecek kişisel veriler bakımından bu Kanun hükümlerinin uygulanmayacağı kabul edilmişken; 28/2-a hükmüyle “suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması” nedeniyle işlenen kişisel veriler hakkında bu Kanunun 10., zararın giderilmesini talep etme hakkı hariç 11. ve 16. madde hükümlerinin uygulanmayacağı, başka bir deyişle sayılan maddeler haricinde Kanunun diğer hükümlerinin geçerli olduğu kabul edilmiştir.

Mevcut çelişkinin 28/1-ç bendinin düzenlenişindeki hatadan kaynaklandığı, düzenlemenin milli savunma, milli güvenlik ve ekonomik güvenlik amaçlarıyla sınırlı olarak düzenlenmek yerine kamu düzeni ve kamu güvenliği amaçlarının da eklenmiş olmasıyla 28/2-a bendiyle kesişerek belirsizliğin doğmasına sebebiyet verildiği ifade edilmektedir¹⁹⁶. Nitekim, kamu düzeni ve kamu güvenliği amacıyla gerçekleştirilen önleyici faaliyetler aslında kolluk faaliyetlerini işaret etmektedir.

Kolluk faaliyetleri, Devletin, kamu düzenini sağlamak amacıyla bireylerin toplum içindeki tutum ve davranışlarını gözetip düzenlemek suretiyle icra ettiği faaliyetlerdir¹⁹⁷. Kolluk faaliyetinin konusu olarak kamu düzeni, “düzensizliğin karşıtı olan maddi bir düzendir”¹⁹⁸. Kargaşa ve aksaklıkların kamu gücü kullanılarak önlenmesi ve bu suretle alışık olduğumuz “*sokak düzeni*”nin devam etmesi

¹⁹⁶ TANSUĞ, s.75.

¹⁹⁷ DURAN, s.248.

¹⁹⁸ OKAY TEKİNSOY, içinde **İdare Hukuku**, Turan YILDIRIM (ed.), s.610.

sağlanır. Bu sebeple kolluk, daha çok İdarenin bireylere dikte ettiği emir ve yasaklar ile bunlara uyulmaması halinde kullanılan kamu gücü şeklinde görülür.

Öte yandan, kolluk adli ve idari kolluk olarak ikiye ayrılmaktadır. Adli kolluk, kişilerin kamu düzenine aykırı olan ve kanunların suç saydığı eylemlerinin cezalandırılması amacıyla faillerin ve suça ilişkin kanıtların ortaya çıkarılmasına ilişkin yürütülen faaliyetlerdir¹⁹⁹. İdari kolluk ise kamu düzeninin korunmasına ve düzenin devam etmesine yönelik faaliyetlerdir. İdari kolluk kamu düzeninin bozulmasını önlemek amacıyla yürütülen faaliyetler olduğundan “önleyici kolluk” ya da “suç öncesi kolluk” şeklinde de ifade edilebilirken²⁰⁰, adli kolluk, “*kamu düzeni bozulduktan sonra faillerin tespiti, delillerin toplanması ve bunları adli makamlara teslim etmek suretiyle bozulan kamu düzenini yeniden tesis etmek için yapılan faaliyetler*”²⁰¹ olduğundan “suç kolluğu” olarak da isimlendirilmektedir. Bu iki kolluk faaliyetleri konu bakımından birbirinden ayrılmışken faaliyetler genelde aynı teşkilatlar tarafından yerine getirilmektedir. Söz gelimi, polis, jandarma ve mahalle bekçileri kamu düzeninin bozulmasını önlemek amacıyla idari kolluk görevlerini yerine getirirken aynı zamanda suçun işlenmesinden sonra kamu düzeninin onarılmasında da görev alırlar.

6698 sayılı Kanunun 28/1-ç maddesinde “kamu düzenini ve kamu güvenliğini sağlamaya yönelik... önleyici ...faaliyetler” ifadesine yer verilmiştir. Öyleyse buradan idari kolluk faaliyetlerinin anlaşılması gerekir. Çünkü idari kolluk da kamu düzeninin bozulmasını ve devamını sağlamaya ilişkin faaliyetlerdir. 28/2-a maddesine bakıldığında ise “suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması” ifadelerine yer verildiği görülmektedir. Başka bir deyişle madde, idari kolluk ve adli kolluk faaliyetlerini de içerecek şekilde düzenlenmiştir. Çünkü her suç tehlikesi kamu düzenini bozma potansiyeline sahiptir. Nitekim suç, “*Toplumsal düzenin devamı açısından korunması gereken hukuki değerlerin bilerek ve istenerek ihlalini (kast) veya bu değerleri korumaya yönelik kurallara karşı özensizliği (taksir) ifade eden insan davranışı*” şeklinde tanımlanabilir²⁰². Bir suçun önlenmesiyle kamu düzeninin devamı sağlanır. İşte bu sebeple mevcut haliyle Kanunun ilgili düzenlemeleri birbiriyle çelişmekte ve hukuki belirsizliğe sebep olmaktadır. Bu belirsizlik TANSUĞ’un da ifade ettiği gibi kamu düzeni ve kamu güvenliği ifadelerinin 28/1-ç hükmünden çıkarılması halinde giderilebilir görünmektedir.

Bununla birlikte, suç işlenmesini önlemeye yönelik faaliyetler sırasında işlenen kişisel verilerin bu faaliyetlerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlama amacı taşıması halinde 28/1-ç kapsamında sayılarak bunlar hakkında 6698 sayılı

¹⁹⁹ DURAN, s.251.

²⁰⁰ OKAY TEKİNSOY, içinde **İdare Hukuku**, Turan YILDIRIM (ed.), s.615.

²⁰¹ Bahtiyar AKYILMAZ/Murat SEZGİNER/Cemil KAYA, **Türk İdare Hukuku**, Savaş Yayınevi, 12. Baskı, Eylül 2020, s.586.

²⁰² T.C. Adalet Bakanlığı Mağdur Bilgilendirme, “Suç Nedir?”, <https://magdurbilgi.adalet.gov.tr/298/Suc-Nedir> (E.T. 6.11.2023).

Kanunun uygulanmaması, öte yandan bu gibi hallerin dışında kalan suç işlenmesini önleyici faaliyetlerinse 28/2-a hükmü kapsamında kabul edilmesi, söz konusu düzenlemenin bir istisna hükmü olduğu da dikkate alınarak herhangi bir şüphenin bulunması halinde ise ilgili veri işleme faaliyetinin 28/2-a kapsamında kabul edilmesi önerisi, düzenlemedeki belirsizliğe bir çözüm yolu olarak sunulmuştur²⁰³. Ancak, yukarıda da ifade edildiği gibi, bir suçun işlenmesini önlemek kamu düzeninin devamını sağlamak anlamına gelmektedir. Kanun koyucunun suç saydığı eylemlerden herhangi birisi için “işlenmesi halinde kamu düzeninin bozulmayacağı” söylenemez. Dolayısıyla böyle bir ayırım yapılarak iki hüküm arasındaki çelişki giderilemeyecektir.

28/1-ç hükmünün mevcut hali şu yönüyle de hukuki açıdan eleştirilebilir durumdadır. İlgili hüküm “kamu düzeni” ve “kamu güvenliği” amacıyla önleyici faaliyetlerin yerine getirilmesinde işlenecek kişisel verileri 6698 sayılı Kanunun kapsamı dışında bırakmaktadır. Yukarıda ifade edildiği üzere bu faaliyetler aslında idari kolluk faaliyetlerini işaret etmektedir. İdari kolluk faaliyetleri ise kamu düzeninin sağlanması ve korunması amacıyla İdare tarafında yürütülen faaliyetlerdir. Burada kamu düzeninin içeriğine kısaca değinmek idari kolluk faaliyetlerinin ne denli geniş olabileceğini ve dolayısıyla söz konusu hükmün ne kadar büyük bir alanı 6698 sayılı Kanun kapsamı dışında bıraktığını göstermek açısından önemlidir.

Kamu düzeni kısaca “*toplumun barış, güven ve gelişme içinde yaşamını sürdürmesi halidir*”²⁰⁴. Bu hâlin korunması bakımından kamu düzeninin üç temel unsuru olduğu kabul edilmektedir: dirlik, esenlik, genel güvenlik ve genel sağlık²⁰⁵. Dirlik ve esenlik bireylerin günlük yaşantısında gürültü, toz, duman ya da koku gibi farklı dış etkenlerden korunması, huzurlu bir yaşam sürmesi anlamına gelmektedir²⁰⁶. Örneğin mevzuatta belirlenen desibel aralığından fazla gürültü yapılması, çöplerin mahalle sakinleri tarafından sadece belirlenen saatlerde dışarı çıkarılmasına ilişkin kurallar kamu düzeninin dirlik ve esenlik unsuruyla ilgilidir. “*Bireylerin tehlike ve kazalara karşı korunmasını, can, ırz ve mal güvenlikleri bakımından huzur içinde bulunmalarını*” sağlamak²⁰⁷ için yapılan faaliyetler ise genel güvenlik unsuru içerisinde yer alır. Bu bakımdan, trafik düzenlemeleri, doğal afetler öncesi ve

²⁰³ Ali UZUNÖZ, “6698 sayılı Kişisel Verilerin Korunması Kanunu’nun kapsamı: İstisna hükümleri açısından bir değerlendirme”, **Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü**, Yüksek Lisans Tezi, 2022, s.75.

²⁰⁴ DURAN, s.249. “Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın önkoşulu kamu düzeninin tesisidir. Kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereği gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, kamu düzenini sağlama görevi de bulunmaktadır. Şiddetin ve suç işlenmesinin önlenmesi amacıyla çeşitli tedbirler almak, Anayasa’nın 5. maddesiyle Devlete yüklenen kamu düzenini koruma ödevinin bir gereğidir. Bu nedenle, özgürlüğün kullanımının kamu düzenini tehdit etmesi durumunda sınırlandırılması mümkündür.” AYM, E.2013/95, K. 2014/176, T. 13.11.2014.

²⁰⁵ Bazı eserlerde kamu düzeni unsurlarının genişlediği, genel ahlak, estetik, ekonomi ve ekoloji gibi konuların da kamu düzeni unsurlarından biri haline geldiği ifade edilmekteyse de bu görüş mezkûr konuların tamamının aslında üç temel unsur içerisinde yer alabileceği, kamu düzeninin sağlanması amacıyla bireylerin hak ve özgürlüklerinin kısıtlanması söz konusu olduğundan unsurların çoğaltılarak kamu düzeni kavramının belirsiz hale getirilmemesi gerektiği gerekçeleriyle eleştirilmektedir: OKAY TEKİNSOY, içinde **İdare Hukuku**, Turan YILDIRIM (ed.), s.614.

²⁰⁶ DURAN, s.255.

²⁰⁷ AKYILMAZ/SEZGİNER/KAYA, s.579.

sonrasında alınan tedbirler, sınır güvenliği, orman güvenliği, doğal hayat ve kültürel varlıkların korunması amacıyla gerçekleştirilen faaliyetler İdarenin güvenlik unsuru amacıyla yerine getirdiği kolluk faaliyetlerine örnek olarak verilmektedir²⁰⁸. Kamu düzeninin sağlık unsuru ise kişilerin tek tek hastalıklardan arınması, tedavi edilmesi değil, toplumun bulaşıcı ve salgın hastalıklardan korunması²⁰⁹, bu tür hastalık tehlikelerinin giderilmesi, genel itibarıyla sağlıklı bir ortamda yaşaması amacıyla yapılan faaliyetleri içermektedir. Aşı uygulamaları, hijyen şartlarının belirlenmesi, alkol satışının yasaklanması²¹⁰ gibi uygulamalar kamu düzeninin genel sağlık unsuru ile ilgilidir.

Dikkat edilirse kamu düzenini ilgilendiren hususlar sadece Türk Ceza Kanunu ve diğer kanunlarda yer verilen ve “suç” olarak kabul edilen eylemlerin engellenmesinden ibaret değildir. Kamu düzeni, suç olmayan bir eylemle de bozulabilmektedir. Söz gelimi gece vakti yüksek sesle müzik dinlemek ya da belirlenen saatler dışında sokağa çöp çıkarmak bilinen anlamıyla suç değil kabahattir ve karşılığında birey idari para cezasıyla cezalandırılabilir. İfade edilmek istenen şey, kamu düzeni amacıyla İdarenin gerçekleştirdiği önleyici faaliyetlerin alanının oldukça geniş olduğu ve 28/1-ç hükmüne göre bu faaliyetler sırasında işlenen kişisel verilerin 6698 sayılı Kanuna tabi olmaktan çıkarılmış olduğudur²¹¹.

Öte yandan önleyici, koruyucu ve istihbari faaliyetlere ilişkin, yukarıda yer verilen Anayasa Mahkemesi kararında da ifade edilen kanuni düzenlemelerde, bu faaliyetler yerine getirilirken işlenecek kişisel verilerin korunmasına ilişkin bazı kurallara yer verilmiştir. Örneğin, 2559 sayılı PVSK’nın “Parmak izi ve fotoğrafların kayda alınması” başlıklı 5. maddesinin ikinci fıkrasında, bireylerden alınan parmak izlerinin kimlik bilgileriyle birlikte bunlara özgü sisteme kaydedileceği ancak parmak izinin hangi sebeple alındığı bilgisinin kaydedilmeyeceği kuralına yer verilmiştir. Yine aynı maddenin sekizinci fıkrasına göre “*sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur*”. Dokuzuncu fıkradaysa,

²⁰⁸ AKYILMAZ/SEZGİNER/KAYA, s.579.

²⁰⁹ Nitekim, Kurul tarafından Covid-19 salgınıyla ilgili 27.3.2020 tarihinde yapılan kamuoyu duyurusunda, mevcut durumun kamu güvenliğini ve kamu düzenini tehdit etmesi nedeniyle salgının bertaraf edilmesine ilişkin yerine getirilecek faaliyetler sırasında 6698 sayılı Kanunun 28/1-ç maddesi gereği İdare tarafından özel nitelikli sağlık verileri dahil tüm kişisel verilerin işlenmesinde bir engel bulunmadığı belirtilmiştir. <https://kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-> (E.T.8.11.2023).

²¹⁰ AYM, E.2013/95, K. 2014/176, T. 13.11.2014: “4250 sayılı Kanun’un 6. maddesinin dava konusu kuralı da içeren son fıkrasında, kitlelerin yoğun olarak bir araya geldiği bazı ortamlarda alkol satışının yasaklandığı görülmektedir. Fıkra ile alkol satışı yasaklanan alanların niteliği göz önünde bulundurulduğunda, dava konusu kuralla amaçlanan hususun, gençlerin alkol bağımlılığından korunmasının yanında, kamu düzeninin tesis edilmesi olduğu da anlaşılmaktadır. Kanun koyucu, eğitim ve öğretim yapılan ortamlarda gençlerin alkole erişebilirliğini kısıtlamak suretiyle bir yandan alkol bağımlılığını diğer yandan da aşırı alkol tüketiminin etkisiyle suç işlenmesini ve bu suretle kamu düzeninin bozulmasını engellemeyi amaçlamaktadır.”

²¹¹ Bilindiği üzere ülkemizde bazı kolluk faaliyetleri özel kişiler tarafından da yerine getirilebilmektedir. Özel güvenlik, yapı denetim kuruluşları, fahri trafik müfettişleri, araç muayene istasyonları bu duruma verilebilecek çeşitli örneklerdir. 28/1-ç hükmü, kamu düzeni amacıyla önleyici faaliyetlerin “kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından” yürütülmesi ile sınırlandırıldığından özel kişilerce yürütülen önleyici kolluk faaliyetleri sırasında işlenen kişisel verilerin bu Kanun kapsamı dışına çıkarılmadığı kabul edilmelidir. Eğer bu faaliyetler, örneğin özel güvenlik faaliyetleri, özel kişilerce yürütülse de “suçun önlenmesi” amacını taşıyorsa bu halde 28/2-a hükmü kapsamında değerlendirilebilir.

parmak izi kayıtlarının gizliliğinin esas olduğu ve yalnızca bu maddede belirtilen “kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından” ve “kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak” amacıyla kolluk birimleri tarafından kullanılabilmesi belirtilmiştir. Yine aynı Kanunda “*Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayiş sağlamaya yönelik, ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar*” kuralına yer verilmiş ve bu faaliyetler sırasında elde edilen verilerin yukarıdaki amaçlar dışında kullanılamayacağı, kayıtların saklanması ve korunmasında gizlilik ilkesinin geçerli olduğu, buna aykırı hareket edenlerince Cumhuriyet savcılarınca doğrudan soruşturulacağı düzenlenmiştir²¹².

Sonuç olarak, 6698 sayılı Kanunun 28/1-ç maddesiyle çok geniş bir alanın Kanun kapsamı dışına çıkarıldığı kabul edilmekle birlikte, kapsam dışında bırakılan konulara ilişkin faaliyetleri yürütmekle görevli kamu kurum ve kuruluşlarına ilişkin kanunlarda kişisel verilerin işlenmesi konusunda çeşitli kurallara yer verildiği görülmektedir. Yine de bu kuralların 6698 sayılı Kanun düzenlemesi kadar kapsamlı ve koruyucu hükümler içermediği açıktır. Kanun koyucunun özellikle İdari faaliyetler sırasında işlenen kişisel verileri koruma altına almak bakımından yeteri kadar titiz davranmadığı ifade edilmelidir. Özellikle 28/1-ç hükmünde olduğu gibi İdarenin kamu gücünü kullanmak suretiyle çeşitli hak ve özgürlükleri kısıtlama yetkisini haiz olduğu ve bu yetkiyi kullanarak yürüttüğü faaliyetlerde 6698 sayılı Kanundan farklı ancak yine de mevcut halden daha koruyucu ve bütünüleyici başka bir düzenleme yapılması düşünülmelidir²¹³.

- Kişisel Verilerin Yargı Makamları veya İnfaz Mercileri Tarafından İşlenmesi: 6698 sayılı Kanunun 28/1-d maddesine göre “*kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz*

²¹² Ek madde 7/1 ve 7/7.

²¹³ Avrupa Birliği Hukuku düzenlemesi olan “Suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı ile ilgili, 2008/977/Aİİ sayılı Konsey Çerçeve Kararı yerine geçen 27 Nisan 2016 tarihli (AB) 2016/680 SAYILI AVRUPA PARLAMENTOSU ve KONSEY DİREKTİFİ” isimli direktif böyle bir düzenleme çeşidine örnek olarak verilebilir: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680> (E.T. 8.11.2023). Söz konusu direktif “*kişisel verilerin, kamu güvenliğine karşı tehditlerin önlenmesi ve kamu güvenliğinin bu tehditlere karşı korunması da dahil olmak üzere, yetkili makamlarca suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin kuralları düzenlemek*” amacıyla çıkarılmıştır. Direktif’in çeşitli konulardaki eksikleri nedeniyle eleştirilmesinin yanında, mevzuatımızda ihtiyaç duyulan bir alanı tek bir Direktif altında düzenlemiş olması bakımından önemlidir. Direktif’in Türkçe tercümesi için: İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü çevirisine bakılabilir: <https://www.mbkaya.com/hukuk/law-enforcement-directive-turkce.pdf> (E.T. 8.11.2023). Ayrıca bkz.: Gülşah BOSTANCI BOZBAYINDIR, “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, S.2018/2, s.51-103.

işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi” halinde bu veri işleme faaliyetine ilişkin olarak 6698 sayılı Kanun hükümleri uygulanmayacaktır. Görüldüğü üzere, kanun koyucu yalnızca yargı makamları ve infaz mercileri tarafından soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak işlenmesi şartıyla işlenen kişisel verileri kapsam dışına çıkarmıştır. Dolayısıyla söz gelimi tarafların yargılama sürecinde birbirlerine ait kişisel verileri işlemesi halinde 6698 sayılı Kanun geçerli olacaktır.

28/1-d maddesi, kapsam dışına çıkarılan veri işleme faaliyetini veriyi işleyenler bakımından “yargı makamları” ve “infaz mercileri” ile sınırlandırdığına göre, bu makam ve mercilerin tespiti önem arz eder. İlgili maddeye ilişkin Kanun gerekçesinde konuya ilişkin bir açıklamaya yer verilmediği görülmektedir. Anayasa’nın 9. maddesi uyarınca “*Yargı yetkisi, Türk Milleti adına bağımsız ve tarafsız mahkemelerce kullanılır*”. Dolayısıyla mahkemelerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin faaliyetlerinde işlenen kişisel veriler hakkında 6698 sayılı Kanun hükümleri uygulanmayacaktır²¹⁴.

Öte yandan infaz, kelime manası olarak “bir kararı, bir yargıyı yerine getirme, uygulama” anlamına gelmektedir²¹⁵. 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun’un 5. maddesinde “*mahkeme, kesinleşen ve yerine getirilmesini onayladığı cezaya ilişkin hükmü Cumhuriyet Başsavcılığına gönderir. Bu hükmü göre cezanın infazı Cumhuriyet savcısı tarafından izlenir ve denetlenir*” hükmüne yer verilmiştir. Böylece infaz sürecinde ana yetkinin Cumhuriyet başsavcılıklarında olduğu söylenebilir²¹⁶. Ayrıca, kararı veren mahkeme, Cumhuriyet başsavcılığı ve infaz hakimlerinin yanı sıra infazın icrası sürecinde verilen kararları uygulayan ceza infaz kurumları ve denetimli serbestlik müdürlükleri ile yakalamanın icrası ve bazı adli kontrol tedbirlerinin uygulanması bakımından adli kolluk birimleri de dahil olmaktadır²¹⁷. Bu sebeple, infaz mercileri olarak sayılan bu İdari birimler tarafından infaz işlemlerine ilişkin olarak işlenen verilerin de 6698 sayılı Kanun kapsamı dışına çıkarıldığı anlaşılmaktadır.

Bu noktada, bazı infaz mercilerinin aynı zamanda suçun önlenmesi ve suçların soruşturulması ile kovuşturulması gibi İdari ve yargısal faaliyetlerde de görevli olması dikkat çekmektedir. Kanunun 28/1-d kapsamında tam istisna tanınan veri işleme faaliyetleri infaz işlemlerine ilişkin olarak işlenmiş olanlardır. Söz gelimi, Cumhuriyet başsavcılığı tarafından bir suçun soruşturması kapsamında kişisel veri işlenmesi

²¹⁴ Söz konusu istisna yalnızca davanın taraflarına ilişkin işlenecek kişisel verilerle sınırlıdır. “*Yargısal organlara tanınan istisna, ancak uyumsuzluğun tarafları açısından geçerli olabilir. Anayasa’nın 20/3 maddesine göre aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkı, 6698 Sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılamaz*”: İstanbul BAM, 23. HD, E. 2017/596, K. 2017/527, T.31.3.2017, aktaran: UZUNÖZ, s.92.

²¹⁵ Güncel Türkçe Sözlük, Türk Dil Kurumu Sözlükleri, <https://sozluk.gov.tr/> (E.T. 15.11.2023).

²¹⁶ Bülent YILDIZ ve diğerleri, **İlamat ve İnfaz Eğitim Modülü**, T.C. Adalet Bakanlığı Eğitim Dairesi Başkanlığı Rize Personel Eğitim Merkezi, s.3. <https://rayp.adalet.gov.tr/resimler/591/dosya/ilamat-ve-infaz-egitim-modulu16-12-202110-01-pm.pdf> (E.T. 15.11.2023).

²¹⁷ YILDIZ ve diğerleri, s.2.

durumu Kanunun 28/2-a maddesi uyarınca²¹⁸ kısmi istisna kapsamında kabul edilecek, ancak kişisel veri işleme faaliyetinin cezanın infazına yönelik olması halinde bu veri işleme 28/1-d hükmü bağlamında tamamen Kanun kapsamı dışında kabul edilecektir.

Kanunun 28/1-d hükmüyle tamamen 6698 sayılı Kanunun kapsamı dışına çıkarılmış olmakla birlikte bu hüküm kapsamında sayılabilecek kişisel verilerin hiçbir sınırlama olmadan yargı makamları veya infaz mercilerince işlenebileceği söylenemez. Nitekim, kişisel verilerin korunmasını isteme hakkı Anayasanın 20/3 maddesinde düzenlenen bir hak olmakla, ancak Anayasanın 13. maddesinde belirlenen yöntemle sınırlanabilecektir. Dolayısıyla en başta söz konusu İdarelerin ölçülülük ilkesine uygun şekilde hareket etmesi, ilgili işlemin yahut yargılamanın gerçekleştirilebilmesi için zorunlu ise kişisel verileri işleme yoluna gitmesi gerekir. Aksi halde temelde özel hayatın gizliliği ilkesinin ihlali gündeme gelebilir. Nitekim, *Panteleyenکو v. Ukrayna* davasında AİHM, başvuruğun ruhsal durumuna ve ilgili tıbbi tedaviye ilişkin gizli bilgilerin bir ruh ve sinir hastalıkları hastanesinden elde edilmesini ve kamuya açık duruşmada açıklanmasını AİHS'in 8. maddesinde yer verilen "özel hayata saygı" hakkına müdahale niteliğinde olduğuna karar vermiştir. Kararda, söz konusu ayrıntıların davanın sonucunu etkilemesi mümkün olmadığından, yerel mahkemenin bilgi talebinin gereksiz olduğu, ayrıca yerel mevzuat bakımından yerel mahkemenin bilgi talebini ve bu bilgileri ifşasını haklı çıkaracak bir yasa bulunmadığı gerekçesine dayanılmıştır²¹⁹.

Ayrıca, kanun koyucu 28/1-d hükmüyle 6698 sayılı Kanunun kapsamı dışında bıraktığı kişisel veri işleme hallerine ilişkin mevzuatta bazı hükümlerle bu verilerin işlenmesine çeşitli sınırlamalar getirmiştir. Örneğin, Anayasa'nın 141. maddesine göre mahkemelerde duruşmaların herkese açık olduğu kural olarak belirlenmiş olmakla birlikte, genel ahlakın veya kamu güvenliğinin kesin olarak gerekli kıldığı durumlarda duruşmaların kapalı yapılmasına karar verilebileceği kabul edilmiştir. 6100 sayılı Hukuk Muhakemeleri Kanunu'nun "Aleniyet ilkesi" başlıklı 28.maddesinde ise "(1) Duruşma ve kararların bildirilmesi alenidir. (2) Duruşmaların bir kısmının veya tamamının gizli olarak yapılmasına ancak genel ahlâkın veya kamu güvenliğinin yahut yargılama ile ilgili kişilerin korunmaya değer üstün bir menfaatinin kesin olarak gerekli kıldığı hâllerde, ilgilinin talebi üzerine yahut resen mahkemece karar verilebilir. (3) Tarafların gizlilik talebi ön sorunlar hakkındaki hükümler çerçevesinde gizli duruşmada incelenir ve karara bağlanır. Hâkim, bu kararının gerekçelerini, esas hakkındaki kararı ile birlikte açıklar. (4) Hâkim, gizli yargılama işlemleri sırasında hazır bulunanları o yargılamayla ilgili edindikleri bilgileri açıklamamaları hususunda uyarır ve 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun gizliliğin ihlaline ilişkin hükmünün uygulanacağını ihtar ederek bu hususu tutanağa geçirir." kurallarına yer verilmiştir. 2577 sayılı İYUK'nun 18. maddesinde

²¹⁸ "(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması."

²¹⁹ AİHM, *Panteleyenکو / Ukrayna*, B.n. 11901/02, T. 29.6.2006, <https://hudoc.echr.coe.int/eng?i=002-3281>.

de duruşmaların açık olarak yapılacağı; ancak genel ahlakın ve kamu güvenliğinin gerektirdiği hallerde duruşmanın kısmen ya da tamamen gizli yapılabileceği düzenlenmiştir.

Yine 6100 sayılı Kanunun 153. maddesinin ilk fıkrasında duruşma sırasında hiçbir şekilde fotoğraf çekilemeyeceği ve video kaydı alınamayacağı belirlenmiştir. Fıkranın devamında, duruşma sırasında yalnızca mahkemeler tarafından, yargılamanın zorunlu kıldığı hallerde çekim ve kayıt yapılabileceği, yapılan çekim ve video kayıtları dahil olmak üzere kişilik haklarını ilgilendiren konuları içeren her türlü belge ve tutanakların mahkeme ve ilgisinin açık izni olmadıkça hiçbir yerde yayımlanamayacağı kabul edilmiştir. Maddenin üçüncü fıkrası uyarınca kayıt ve yayın yasağına aykırı davranılması halinde ilgili kişi hakkında TCK 286. maddesi²²⁰ uygulanacaktır.

Anayasa Mahkemesi, dava dosyasında ameliyatına ilişkin bel üstü fotoğrafları bulunan kadın davacının gizlilik talebinin reddedilmesi karşısında ilgilinin özel hayata saygı hakkının ihlal edildiğine karar vermiştir. Kararda, yargılama faaliyetinin şeffaflığını sağlamak amacıyla aleniyet ilkesinin geçerli olduğu, bununla birlikte kişisel verilerin korunmasını gerektiren durumlarda yargı makamlarının gerekli tedbirleri alma ödevinin bulunduğu, bu bağlamda mahkemelerin aleniyet ilkesinin sağladığı kamusal menfaat ile başvurucunun mahremiyetinin korunması menfaati arasında adil dengenin kurulması ve bu konuda varılan sonucun yeterli gerekçelerle açıklanması gerektiği ifade edilmiştir²²¹. Buradan hareketle, ilk derece mahkemesince gizlilik talebinin reddine yönelik kararda hiçbir gerekçe sunulmaması, yedi yılı aşan dava süreci boyunca başvurucunun korunmak istediği riskle yüz yüze bırakılması nedeniyle *“bireysel yarar ile kamu yararı arasında adil dengeyi sağlayacak bir önlem alınmadığı”*, bu nedenle başvurucunun özel hayatın gizliliği hakkının ihlal edildiğine karar verilmiştir²²².

Yargılama sürecinde yargı makamlarınca işlenen taraflara ait kişisel verilerin korunmasına yönelik bir başka hükme HMK’nun 161. maddesinde yer verilmiştir. Buna göre, taraflar veya fer’î müdahil zabıt katibinin gözetimi altında dava dosyasını inceleyebilirken, dava ile ilgili olduklarını ispatlayan diğer kişilerse hâkimin izin vermesi halinde dosyayı görebilecektir²²³.

Mevzuatta duruşmaların gizli yürütülmesi, dosya bilgilerinin paylaşımının kısıtlanması gibi önlemler, yargı makamlarınca yargılama sürecinde işlenen verileri özellikle üçüncü kişilere karşı korumaktadır. Ancak, bazı durumlarda mahkemelerin taraflardan ya da üçüncü kişilerden talep ederek

²²⁰ **Ses veya görüntülerin kayda alınması**

Madde 286- (1) Soruşturma ve kovuşturma işlemleri sırasındaki ses veya görüntüleri yetkisiz olarak kayda alan veya nakleden kişi, altı aya kadar hapis cezası ile cezalandırılır.

²²¹ AYM, B.n. 2014/14189, T.25.10.2017, § 61.

²²² AYM, B.n. 2014/14189, T.25.10.2017, § 68. Benzer şekilde, HIV enfeksiyonu rahatsızlığı bulunan ilgilinin işverene karşı açmış olduğu davada gizlilik talebinin reddedilmesi, ilk derece mahkemesi kararının muğlak ve somut gerekçeleri barındırmaması nedeniyle, özel hayatın gizliliği hakkının ihlali niteliğinde kabul edilmiştir: AYM, B.n.2014/19081, T. 1.2.2017.

²²³ Öte yandan, söz konusu hükme istinaden üçüncü kişilerin dava dosyasını sadece inceleyebileceği; fakat dosya içerisindeki bilgi ve belgelerden suret alamayacağı ifade edilmektedir: S. Hilal ÜÇÜNCÜ, **Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması**, On İki Levha Yayıncılık, Temmuz 2019, s. 211.

yargılama sürecine dahil ettiği kişisel verilerin tarafların ya da davadan bağımsız üçüncü kişilerin haklarını ihlal ettiği durumlar da yaşanabilir. Nitekim, 5271 sayılı Ceza Muhakemesi Kanunu'nun 161. maddesinde savcılık ve ceza mahkemelerinin adli kolluk ve diğer kamu görevlilerinden her türlü bilgiyi isteyebileceği, 332. maddesinde de ilgililerden her türlü bilgiyi yazılı olarak isteyebileceği düzenlenmiştir²²⁴. Yine 2577 sayılı İYUK'nun 20. maddesinde İdari yargı mahkemelerinin lüzum gördükleri evrakın gönderilmesini ve her türlü bilginin verilmesini taraflardan ve ilgililerden isteyebileceği düzenlenmiştir. Mahkemeler tarafından dosyanın incelenmesine dahil edilmek suretiyle işlenen kişisel veriler de 28/1-d hükmü uyarınca 6698 sayılı Kanun kapsamı dışındadır. Örneğin, Kurul kararına konu olayda, şikâyetçi iş sözleşmesinin feshi konulu davada işveren tarafından mahkemeye sunulan özlük dosyasında dava konusuyla ilgisi olmayan kişisel sağlık verilerinin de sunulmasından şikâyetçi olmuş, fakat ilgili davada mahkeme tarafından tüm özlük dosyasının istenmiş olması nedeniyle işverenin dosyada belge ayırımı yapmaksızın tamamını mahkemeye göndermiş olduğu, bu bağlamda 6698 sayılı Kanunun 28/1-d hükmü hatırlatılarak Kurul tarafından tesis edilecek bir işlem bulunmadığına karar verilmiştir²²⁵.

Son olarak, 28/1-d hükmünün geçerli olabilmesi işlenen kişisel verilerin söz konusu soruşturma, kovuşturma, yargılama ve infaz işlemlerinin tarafı olan kişilere ilişkin olması gerektiği ifade edilmelidir. Nitekim İzmir 8. Bölge Adliye Mahkemesi tarafından verilen bir kararda “*Aynı Yasanın 28/1-d maddesindeki yargısal organlara tanınan istisna, ancak uyumsuzluğun tarafları açısından geçerli olabilecektir. T.C. Anayasası'nın 20/3. maddesine göre aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkı, 6698 Sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılamaz*” denilerek hükmün yalnızca tarafların kişisel verilerinin işlenmesi halinde geçerli kabul edilmesi gerektiği ifade edilmiştir²²⁶.

²²⁴ “**Madde 161/1** - Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adli kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir; yukarıdaki maddede yazılı sonuçlara varmak için bütün kamu görevlilerinden her türlü bilgiyi isteyebilir.”

“**Madde 332/1** - Suçların soruşturma ve kovuşturması sırasında Cumhuriyet savcısı, hâkim veya mahkeme tarafından yazılı olarak istenilen bilgilere on gün içinde cevap verilmesi zorunludur. Eğer bu süre içinde istenen bilgilerin verilmesi imkânsız ise, sebebi ve en geç hangi tarihte cevap verilebileceği aynı süre içinde bildirilir.” Konuya ilişkin olarak bkz.: Bilal OSMANOĞLU, “Türk Ceza Muhakemesi Hukukunda Cumhuriyet Savcısı ve Mahkemelerin Bilgi ve Belge İsteme Yetkisi”, **TBB Dergisi**, 2020, S.151, Kasım-Aralık, s.103-138.

²²⁵ KVK Kurulu, 18.2.2020 tarih ve 2020/138 sayılı kararı. <https://www.kvkkarar.com/2020-138/> (E.T. 18.11.2023).

²²⁶ İzmir BAM, 8. HD., E. 2018/2146 K. 2019/655 T. 6.3.2019, (Lexpera). Karara konu olayda bir icra dosyasında alacaklı vekili, dosyadaki borçlulara ait aktif ve pasif tapu kayıtlarının tespiti ve taşınmazların kimlere hangi tarihlerde satıldığını, takyidatlı raporlarını ve devir resmi senet bilgilerinin ilgili tapu dairelerinden istenmesi talebini icra müdürlüğüne iletmış fakat icra müdürlüğü devir resmi senetler bilgisinin taşınmazı satın alan üçüncü kişilerin kişisel verilerinin işlenmesi anlamına geleceğinden talebi reddetmiştir. Benzer yönde verilen BAM kararları Yargıtay 12.HD. tarafından onaylanmıştır. Örneğin: Yargıtay 12. HD., E. 2022/13128 K. 2023/785 T.13.2.2023 ve Yargıtay 12. HD., E. 2022/9859 K. 2023/2649 T.13.4.2023, (Lexpera). Başka bir BAM kararına konu olayda yine alacaklı vekili, ölmüş olmaları halinde veraset ilamı çıkarmak suretiyle mirasa haciz konulmasını sağlamak amacıyla borçlunun anne baba kaydını gösterir nüfus kayıt örneği talep edilmiş ancak bu talep reddedilmiştir. Alacaklı avukatın icra müdürlüğü kararının iptalini talep etmesi üzerine ilk derece mahkemesi bu talebin reddine karar vermiş, dosya istinaf mahkemesine taşınmıştır. İstinaf mercii kararında şu ifadelere yer vermiştir: “*Öte yandan; borçlunun murisi olabilecek kişilerin nüfus kaydına erişilmesinin ve onların ölmüş olup olmadıklarının tespitinin alacağın tahsilinde alacaklı tarafa katkı sağlayacağı muhakkaktır. Hatta bu durum murisinden kendisine intikal eden malları adına*

AİHM kararına konu bir olayda, başvuran hakkında çalıştığı devlet okulundaki bir meslektaşı tarafından taciz suçlamasıyla İdareye şikâyetle bulunulmuş fakat İdare yaptığı soruşturmadan sonra başvuran hakkında herhangi bir disiplin cezası verilmesine gerek görmemiştir. Şikâyetle bulunan meslektaş daha sonra İdareye karşı tazminat davası açmış ve mahkeme İdareyi haksız bularak davacı lehine tazminata hükmetmiştir. Bu davada, davalı taraf İdare olmakla birlikte, dava sırasında başvuranın adı zikredilmiş ve mahkeme tarafından davaya konu eylemlerin taciz niteliği taşıdığı yönündeki görüşleri kayıtlara geçmiştir.

Başvuran, konu hakkında bir yargılama yapıldığını yerel bir gazetede konuya ilişkin haber yapıldığında öğrenmiştir. İlgili karar, gerekçesiyle birlikte ve başvuranın adı açık olarak yazılı şekilde kamuoyuyla paylaşılmıştır. Başvuruyu inceleyen AİHM, özel hayata saygı hakkı bağlamında, bu hakkın kişinin itibar ve onurunu da kapsadığını, birkaç yıl önce hakkındaki suçlamalar reddedilen başvuran hakkında yapılan bu yargılamadan başvuranın haberdar edilmediğini, dolayısıyla isminin gizli tutulması yönünde talepte bulunma fırsatının verilmediğini, ilgili davada kimliğinin belirlenebilir şekilde ifşa edilmesinin özel hayata saygı hakkına müdahale teşkil ettiğini tespit etmiştir. Mahkeme işlemlerinin şeffaflığının sağlanmasında kamu yararı bulunduğu düşünülebilirse de kararın bu şekilde yayınlanmasıyla başvuranın mesleki itibarı ve onuru üzerinde önemli bir etki yarattığı düşünüldüğünde, mahkemenin başvuranın ismini çıkarmak ya da sadece baş harflerini kullanmak yönündeki takdir yetkisini kullanmamasını haklı çıkaracak ikna edici gerekçelerin bulunmadığı, bu sebeple özel hayatın gizliliği hakkına haksız bir müdahalede bulunulduğu tespit edilmiştir²²⁷.

Karara konu olay 6698 sayılı Kanun bağlamında düşünüldüğünde, başvuranın davanın bir tarafı olmadığından hareketle, dava dosyasında isminin açıkça zikredilmesinin 28/1-d maddesine tabi olmadığı

tescil ettirmeyen borçluların bu şekilde davranmalarının önüne geçmek sonucunu da doğurabilir. Ancak kişisel verilerin bu şekilde işlenmesi ile elde edilmesi muhtemel yararların yanı sıra doğabilecek zararlar da birlikte değerlendirilmelidir. Anayasa Mahkemesinin 09/04/2014 tarih ve 2013/122-2014/74 EK sayılı kararında kişisel verilerin niçin gizli tutulması gerektiği ayrıntılı olarak açıklanmıştır. “Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa’nın 20. Maddesinin üçüncü fıkrasının son cümlesinde, “Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır.” Bu durumda, yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmasının yaratması muhtemel olan zararlarının, sağlaması muhtemel olan yararlarına göre daha fazla ve daha mühim olduğu anlaşılmaktadır.

Açıklanan sebeplerle; ilk derece mahkemesi kararının usul ve yasaya uygun olduğu, davacının istinaf başvuru nedenlerinin yerinde olmadığı, kararda kamu düzenine aykırılık da bulunmadığı anlaşılmakla HMK’nın 353/1-b-1 maddesi gereğince başvurunun esastan reddine karar verilmesi gerekmektedir.” Samsun BAM, 4. HD., E. 2018/3158 K. 2019/845 T. 18.3.2019, (Lexpera). Öte yandan, borçlunun pasif tapu kayıtlarının getirilmesi talebinin, kime satılmış olduğu bilgisini içermeyecek olması şartıyla, üçüncü kişilerin kişisel verilerinin işlenmesi anlamı taşımayacağından 6698 sayılı Kanuna aykırı bir yanı bulunmamaktadır. Aynı yönde bkz. İzmir BAM, 12. HD., E. 2016/59, K. 2016/68, T. 13.10.2016, (Kazancı).

²²⁷ AİHM, Vincent Del Campo / İspanya, B.n. 25527/13, T. 6.10.2018, <https://hudoc.echr.coe.int/eng?i=001-187509>.

kabul edilmelidir. Öte yandan, kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenmesi gerektiğinden, mahkeme işlerinin şeffaflığı gerekçe gösterilerek başvuran adının kamuoyuyla paylaşılması Kanuna aykırı kabul edilmelidir. Nitekim, olaya ilişkin daha önce ilgilinin lehine kesinleşmiş bir idari kararın bulunmasının yanı sıra, davada ilgili kişiye aksi yönde savunma yapma fırsatı da sunulmamıştır. Bu şartlar altında, olayın oluş şekli ve verilen kararın öğrenilmesinde bir kamu yararı bulunduğu söylenebilirse de ilgilinin açık adının gerekçeli kararda zikredilmek suretiyle kişisel verisinin işlenmesinin ve böylece itibarına zarar verilmesinin, bu yararın gerçekleşmesi bakımından gerekli olduğu söylenemeyecektir.

3.2. Kısmen Kanun Kapsamı Dışında Tutulan Haller

Kanun koyucu, 6698 sayılı Kanunun 28. maddesinin ilk fıkrasında, yukarıda izah edilmeye çalışılan hallerde bu Kanunun uygulanmayacağı kuralına yer verdikten sonra, aynı maddenin ikinci fıkrasında bu kez Kanunun kısmen uygulanmayacağı halleri belirlemiştir. Buna göre, ikinci fıkrada sayılan dört farklı veri işleme hallerinde Kanunun “*veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri*” uygulanmayacaktır. Bununla birlikte, bu dört veri işleme halinin, herhalde Kanunun amacı ve temel ilkelerine uygun ve orantılı bir şekilde gerçekleştirilmesi gerektiği ikinci fıkrada ifade edilmiştir. Buna göre, aşağıda açıklanan hâllerde işlenen kişisel veriler için kısmi bir istisna durumu söz konusu olsa da Kanunun kişisel verilerin işlenmesinde öncelikle özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini koruma amacına uygun şekilde veri işlenmeli ve Kanunun 4/2. maddesinde sayılan kişisel verilerin işlenmesinde uyulması gereken genel ilkelere aykırı bir veri işleme faaliyetinden kaçınılmalıdır²²⁸.

28. maddenin ikinci fıkrasında sayılan veri işleme halleri şunlardır: “*a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması, b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi, c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması, ç)*

²²⁸ AİHM tarafından verilen bir kararda, dini bir kuruluş olan Yehova Şahitleri’nin Rusya’da bulunan merkezinin üyesi olan başvuranlar, özellikle kamu hastanelerinde tedavi oldukları sırada, kan nakli yapılmasını reddettikleri anda tıbbi dosyalarının Rus savcılık makamlarına gönderilmesinden şikayetçi olmuşlardır. Savcılık makamı, örgütün faaliyetlerinin hukuka uygunluğuyla ilgili bir soruşturma kapsamında tüm kamu hastanelerine kan naklini reddedenlerin bilgilerinin istendiğini bildirmiştir. Mahkeme yaptığı incelemede, başvuranların gizli tıbbi bilgilerinin ifşa edilmesine yönelik acil bir sosyal ihtiyacın bulunmadığını, savcılığın soruşturmayı yürütürken kullandığı gizli bilgilerin önceden bilgi verilmeksizin veya itiraz fırsatı olmaksızın ifşa edilmesini içeren bu baskıcı yöntemin “gerekli” olmadığını, bu sebeplerle, savcılığın başvuranların özel hayata saygı haklarıyla, savcının kamu sağlığını koruma amacı arasında “adil bir denge” kurulamadığını ifade ederek AİHS’nin 8. maddesinin ihlal edildiğine karar vermiştir. AİHM, Avilkina ve diğerleri / Rusya, B.n. 1585/09, T. 6.6.2013, <https://hudoc.echr.coe.int/eng?i=001-120071>.

Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.”

- **Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması:** 6698 sayılı Kanunun 28/2-a maddesi uyarınca, suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması halinde işlenen kişisel verilere ilişkin veri sorumlusunun aydınlatma yükümlülüğü ve Veri Sorumluları Siciline kayıt yükümlülüğü bulunmamakta, verisi işlenen kişininse zararın giderilmesini talep etme hakkı hariç Kanunun 11. maddesinde düzenlenen haklarını kullanma imkânı bulunmamaktadır. Suç işlenmesinin önlenmesi amacıyla gerçekleştirilen faaliyetler idari kolluk faaliyetleri olarak adlandırılırken; suçun işlenmesinden sonra, suçun soruşturulması amacıyla gerçekleştirilen faaliyetler adli kolluk olarak adlandırılmakta ve bu kapsam içerisinde incelenmektedir. Yukarıda da izah edildiği üzere, 28/2-a hükmündeki “suç işlenmesinin önlenmesi için kişisel veri işlenmesi” haline aslında tam istisna kapsamının belirlendiği birinci fıkranın “ç” bendinde de yer verilmiştir. Nitekim, ilgili hükme göre *“kişisel verilerin ... kamu güvenliğini, kamu düzenini...sağlamaya yönelik olarak...önleyici...faaliyetler kapsamında işlenmesi”* halinde 6698 sayılı Kanun uygulanmayacaktır. Hukuki belirsizliğe yol açan düzenlemeye ilişkin görüşlerimize yukarıda yer verilmiş olduğundan²²⁹ burada sadece iki hüküm arasındaki farka değinmek yerinde olacaktır.

28/1-ç hükmü “kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından” işlenmesi halinde geçerli olacaktır, başka bir deyişle kanunla görev ve yetki verilmiş bir kamu kurum ve kuruluşu olmayanlar için tam istisna kuralı geçerli olmayacaktır. İşte 28/2-a hükmünde kişisel veriyi işleyen kişiler bakımından bir sınırlama öngörülmediğinden, kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları dışında kalan kişilerce suçun önlenmesi için gerekli olduğundan kişisel veri işlenirse, bu veri işleme hali için 28/2-a hükmü geçerli olacak, dolayısıyla 6698 sayılı Kanun kısmen uygulanmayacaktır. Örneğin, Kamu güvenliğini tamamlayıcı nitelikteki²³⁰ özel güvenlik hizmetlerini yerine getiren özel güvenlik şirketleri ve özel güvenlik görevlileri tarafından suçun önlenmesi için gerekli olması nedeniyle işlenen kişisel veriler 28/2-a hükmü kapsamında kabul edilmelidir²³¹. Yine, 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine

²²⁹ Konuya ilişkin açıklamalarımız için bkz.: “3.1. Tamamen Kanun Kapsamı Dışında Tutulan Haller” başlığı.

²³⁰ 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun, “Madde 1- Bu Kanunun amacı, kamu güvenliğini tamamlayıcı mahiyetteki özel güvenlik hizmetlerinin yerine getirilmesine ilişkin esas ve usulleri belirlemektir.”

²³¹ 5188 sayılı Kanun’un 7. maddesine göre özel güvenlik görevlilerine tanınan yetkilerden bazıları şunlardır:

“b) Toplantı, konser, spor müsabakası, sahne gösterileri ve benzeri etkinlikler ile cenaze ve düğün törenlerinde kimlik sorma, duyarlı kapıdan geçirme, bu kişilerin üstlerini detektörle arama, eşyaları X-ray cihazından veya benzeri güvenlik sistemlerinden geçirme.

d) (Değişik: 23/1/2008 – 5728/544 md.) Görev alanında, haklarında yakalama emri veya mahkûmiyet kararı bulunan kişileri yakalama ve arama.

f) Hava meydanı, liman, gar, istasyon ve terminal gibi toplu ulaşım tesislerinde kimlik sorma, duyarlı kapıdan geçirme, bu kişilerin üstlerini detektörle arama, eşyaları X-ray cihazından veya benzeri güvenlik sistemlerinden geçirme.

g) Genel kolluk kuvvetlerine derhal bildirmek şartıyla, aramalar sırasında suç teşkil eden veya delil olabilecek ya da suç teşkil etmemekle birlikte tehlike doğurabilecek eşyayı emanete alma.

h) Terk edilmiş ve bulunmuş eşyayı emanete alma.

Dair Kanun uyarınca spor federasyonların tarafından işlenen bazı kişisel verilerin 28/2-a kapsamında olduğu söylenebilir²³². Nitekim, ilgili Kanunun düzenleniş amacı müsabakaların yapılacağı yere gidiş dönüş güzergahlarında şiddet ve düzensizliğin önlenmesidir. Kanunun 5/11-a maddesinde yer verilen “*Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisi federasyonlara ait olup federasyonlar bu amaçla bünyelerinde merkezi kontrol sistemi oluşturur. Elektronik kart oluşturulmak amacıyla alınacak kişisel bilgiler federasyon bünyesinde oluşturulan merkezi veri tabanında tutulur. Bu veri tabanı Hazine ve Maliye Bakanlığı ve İçişleri Bakanlığı erişimine açıktır*” şeklindeki düzenleme gereği işlenen kişisel veriler 6698 sayılı Kanunun 28/2-a kapsamında olacaktır.

Öte yandan maddenin “suç soruşturması için kişisel veri işlenmesi” kısmının, yine aynı maddenin ilk fıkrasının “d” bendi²³³ ile birlikte okunması gerektiği, buradan hareketle, 28/1-d hükmü uyarınca kişisel verilerin soruşturma işlemlerine ilişkin olarak yargı makamları ve infaz mercileri tarafından işlenmesi halinin Kanunun tamamen kapsamı dışında tutulduğu, bununla birlikte aynı amaçla adli kolluk makamlarınca kişisel veri işlenmesi halinde 28. maddenin ikinci fıkrası uyarınca Kanunun kısmen uygulanmayacağı sonucuna varılmaktadır.

- İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi: 6698 sayılı Kanunun 28/2-b maddesi uyarınca “ilgilinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi” halinde Kanunun aydınlatma yükümlülüğüne ilişkin 10. maddesi, zararın giderilmesini talep etme hakkı dışında kişinin haklarını düzenleyen 11. maddesi ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. maddesi uygulanmayacaktır. İlgilisince aleni hale getirilen kişisel veriler idari faaliyetlerin gerçekleştirilmesinde İdareler tarafından da kullanılabilir.

Kanun koyucu, benzer bir düzenlemeye veri işleme şartları arasında da yer vermiştir. Kanunun 5/2-d maddesine göre ilgisinin kendisi tarafından alenileştirilmesi halinde genel nitelikli verisinin işlenebileceği kabul edilmiş; 6/3-ç maddesine göreyse, ilgisinin alenileştirildiği özel nitelikli kişisel verilerin alenileştirme iradesine uygun olarak işlenmesine imkân tanınmıştır. Esasında, bu iki fıkra arasındaki ‘alenileştirme amacına uygun olma’ farkı pratikte bir değişikliğe yol açmayacaktır. Çünkü, bir kişisel verinin ilgisince alenileştirildiğinin kabulü için bu eylemin açık şekilde ve bizzat gerçekleştirilmesi gereklidir. Alenileştirilen

j) (Değişik: 23/1/2008 – 5728/544 md.) Olay yerini ve delilleri koruma, bu amaçla Ceza Muhakemesi Kanununun 168 inci maddesine göre yakalama.”

²³² Esasında spor federasyonlarının tüzel kişiliğinin niteliği öğretide tartışmalıdır. Spor federasyonlarının kamu tüzel kişisi olduğu, özel hukuk tüzel kişisi olduğu ve karma nitelikte/sui generis tüzel kişiler olduğu şeklinde üç farklı görüş bulunmaktadır. Çalışmamızın kapsamı dışında kalması nedeniyle burada yalnızca konuya ilişkin bazı eserlere yer verilmekle yetinilecektir: Zehreddin ASLAN / Halil ALTINDAĞ, “Bağımsız Spor Federasyonlarının Kamu Tüzel Kişiliği Sorunu”, **İstanbul Spor Hukuku Dergisi**, Y. 2019, Ay: 1 C.1, S.1, s. 181-196; Taner AYANOĞLU: “Türkiye Futbol Federasyonu’nun Özel Hukuk Tüzel Kişiliği Görüşü Hakkında Düşünceler ve Eleştiriler”, **Legal Hukuk Dergisi**, Y.2017, S.174, s. 2839-2858; Şeref ERTAŞ/ Hasan PETEK, **Spor Hukuku**, Yetkin Yayınları, Ankara, 2011; Sait GÜRAN, “Türkiye Futbol Federasyonu’nun İdare Hukuku ile İlişkisi”, **Prof. Dr. Rona Serozan’a Armağan**, Cilt II, 1. Baskı, On İki Levha Yayınları, İstanbul, 2010, s. 1913-1919.

²³³ “Madde 28 – (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.”

bu verilerin işlenmesinde ise Kanunun 4. maddesinin ikinci fıkrasında yer verilen genel ilkeler geçerli olduğundan, her halde bu kişisel verilerin alenileştirilme amacıyla bağlı, sınırlı ve ölçülü şekilde işlenmiş olması aranır.

Kanunun 28/2-b fıkrası, 5. ve 6. maddelerde yer verilen hükümlerle birlikte okunduğunda, kişisel verilerin ilgilisince alenileştirilmiş olması halinde, bu verilerin işlenmesinde ilgisinin açık rızasının aranmayacağı gibi, veri sorumlusunun aydınlatma yükümlülüğünün ile sicile kayıt yükümlülüğünün bulunmayacağı ve ilgilinin varsa zararlarının giderilmesini isteme hakkı dışında Kanunun 11. maddesinde sayılan haklarını talep edemeyeceği söylenebilecektir. Ancak, işleme faaliyeti alenileştirme amacıyla uygun olmadığı takdirde, bu veri işleme hukuka aykırı olacaktır.

- Kişisel Verilerin Denetleme veya Düzenleme Görevlerinin Yürütülmesi ile Disiplin Soruşturma veya Kovuşturması İşlemleri Sırasında İşlenmesi: 6698 sayılı Kanunun 28/2-c hükmü uyarınca kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının, kanunun verdiği yetkiye dayanarak yerine getirdikleri denetleme veya düzenleme görevlerinin yürütülmesi ve disiplin soruşturması veya kovuşturması için gerekli olduğu hallerde işlenen kişisel veriler hakkında, veri sorumlusunun aydınlatma ile sicile kayıt yükümlülüklerine ve zararın giderilmesini talep etme hakkı haricinde 11. maddede düzenlenen ilgili kişilerin haklarına ilişkin hükümler uygulanmayacaktır.

İlgili istisna hükmünün görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları tarafından işlenen veriler bakımından geçerli olduğu görülmektedir. Kanun koyucu 6698 sayılı Kanunda “kamu kurum ve kuruluşları” kalıbını farklı maddelerde kullanmıştır²³⁴. Söz konusu hükümlerin uygulanışı ve KVK Kurulu kararları²³⁵ göz önüne alındığında, öğretilerdeki görüşten farklı olarak²³⁶, bu kullanımın genel anlamda kamu tüzel kişiliğine sahip merkezden ve yerinden yönetim

²³⁴ **Madde 9/5:** Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

Madde 18/3: Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

Madde 20/1: Kurumun görevleri şunlardır: b) İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak.

Madde 28/1: Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

²³⁵ Örneğin, bir Valilik çalışanı hakkında başlatılan disiplin soruşturmasına dayanak olarak kullanılan kişisel verilere ilişkin yapılan başvuruda Kurul 28/2-c maddesi uyarınca 6698 sayılı Kanun kapsamında yapılacak bir işlem bulunmadığına karar vermiştir. Halbuki Valilikler merkezden yönetim İdaresi içerisinde yer alan Kamu idarelerinden olup kamu kurum ve kuruluşu olarak ifade edilen kamu tüzel kişiliklerinden değildir. KVK Kurulu 19.3.2020 tarih ve 2020/26 sayılı kararı. <https://www.kvkk.gov.tr/Icerik/6893/2020-226> (E.T. 3.12.2023).

²³⁶ Öğretilerde kamu kurumu ve kamu idaresi kavramlarının farklı anlamlara geldiği ifade edilmektedir. “*Hizmet bakımından yerinden yönetim, özel bilgi ve uzmanlık gerektiren teknik nitelikteki bazı kamu hizmetlerinin merkez teşkilatından ayrı ve kamu tüzel kişiliğine sahip kuruluşlar eliyle yürütülmesidir... Bu özelliğe haiz kuruluşlara ise kamu kurumları adı verilir.*”: AKYILMAZ/SEZGİNER/KAYA, s.304. Öte yandan Özay, kamu kuruluşu teriminin hukuksal bir tanımının bulunmadığını,

İdarelerinin tümünü kapsar şekilde anlaşılması gerektiği sonucuna varılmaktadır²³⁷. Dolayısıyla, söz gelimi bir kamu kurumu olan üniversitelerde öğrenciler ya da kamu görevlileri hakkında yürütülen disiplin soruşturması ya da kovuşturması süreci için bu kısmi istisna hükmü geçerli olduğu gibi, yer bakımından yerinden yönetim İdaresi olan belediyelerde yürütülen disiplin soruşturma ve kovuşturma süreçlerinde de bu hüküm uygulanacaktır.

Öte yandan, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun 3. maddesi uyarınca yine bu Kanunun ekli (III) sayılı cetvelinde yer alan kurumlar “düzenleyici ve denetleyici kurumlar” olarak belirlenmiştir²³⁸. Kişisel Verileri Koruma Kurumu da burada sayılan kamu kurumları arasındadır. Bu kuruluşların kanunlarla kendilerine verilen alanlarda yürüttükleri düzenleme ve denetleme faaliyetlerinde işledikleri kişisel veriler hakkında 28/2-c hükmünün uygulama alanı bulacağı muhakkaktır. Kamu kurumu niteliğindeki meslek kuruluşları (ve aynı hukuki rejime tabi olan üst kuruluşları)²³⁹ ise Anayasa'nın 135. maddesinde düzenlenmiş ve “*belli bir mesleğe mensup olanların müşterek ihtiyaçlarını karşılamak, mesleki faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, meslek mensuplarının birbirleri ile ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hakim kılmak üzere meslek disiplini ve ahlakını korumak maksadı ile kanunla kurulan ve organları kendi üyeleri tarafından kanunda gösterilen usullere göre yargı gözetimi altında, gizli oyla seçilen kamu tüzelkişilikleri*” şeklinde tanımlanmıştır. Bu nitelikteki meslek kuruluşlarının da mahsus oldukları meslek kurallarının düzenlenmesi ve üyelerinin denetlenmesi süreçlerinde işledikleri kişisel veriler hakkında veri sorumlusunun aydınlatma ile sicile kayıt yükümlülüklerine ve zararın giderilmesini talep etme hakkı haricinde 11. maddede düzenlenen ilgili kişilerin haklarına ilişkin hükümler uygulanmayacaktır.

Soyut, objektif, sürekli uygulanabilir niteliğini haiz idari işlemler tesis etme yetkisi bulunan, başka bir deyişle düzenleyici işlemler çıkarabilen İdareler, bu işlemlerin çıkarılması sürecindeki hazırlık aşamasında ihtiyaç duyulan araştırmalar, hukuki sorunların tespiti ve ihtiyaçların belirlenmesi gibi kamu

ancak terimin tüzelkişiliği bulunmayan örgütleri anlatmak için kullanılabileceğini ifade etmektedir: İl Han ÖZAY, **Günüşğinde Yönetim**, Filiz Kitabevi, 2017, s. 130-131. Kamu idareleri ise Anayasanın “merkezi idare” başlıklı 126. maddesi ile “mahalli idareler” başlıklı 127. maddesinde sınırlı sayıda/numerus clausus belirlendiği, bu bağlamda Devlet, il, belediye (ve büyükşehir belediyeleri) ile köy idarelerinden ibaret olduğu ifade edilmektedir. ÖZAY, **Günüşğinde Yönetim**, s.127.

²³⁷ Aynı yönde bkz. TANSUĞ, s. 90.

²³⁸ İlgili Kanunun (III) sayılı cetvelinde yer alan kurumlar şunlardır:

- 1) Radyo ve Televizyon Üst Kurulu
- 2) Bilgi Teknolojileri ve İletişim Kurumu
- 3) Sermaye Piyasası Kurulu
- 4) Bankacılık Düzenleme ve Denetleme Kurumu
- 5) Enerji Piyasası Düzenleme Kurumu
- 6) Kamu İhale Kurumu
- 7) Rekabet Kurumu
- 8) Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu
- 9) Kişisel Verileri Koruma Kurumu
- 10) Nükleer Düzenleme Kurumu
- 11) Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu

²³⁹ Hüseyin Melih ÇAKIR, “Yerinden Yönetim”, içinde **İdare Hukuku**, Turan Yıldırım (Ed.), s. 228.

hizmetinin en iyi şekilde icra edilebilmesi adına koyulacak kuralların belirlenmesinde kişisel veri işleyebilmektedir. 28/2-c maddesi işte bu süreçte İdareler tarafından işlenen kişisel verileri de kapsamı içerisinde barındırmaktadır.

Yukarıda ifade edildiği üzere, aydınlatma yükümlülüğü ve Veri Sorumluları Siciline kayıt yükümlülüğü ile zararın giderilmesini talep etme hakkı hariç ilgili kişinin haklarının kullanılamayacağı düzenlenmiş olmakla beraber, Kanunun 28/2 bağlamında işlenecek kişisel verilerin her zaman Kanunun amacına ve temel ilkelerine uygun ve orantılı olması gerekmektedir. Dolayısıyla, kanunun verdiği yetkiye dayanarak yürütülen bir disiplin soruşturmasında işlenecek kişisel verilerin 28/2-c hükmü kapsamındaki kısmi istisnalara tabi olabilmesi için, söz gelimi kayıt altına alınan kişisel verinin hangi meşru amaca dayandığı İdare tarafından açıklanabilmelidir. Yine işlenen kişisel verilerin doğru ve güncel olmasına dikkat edilmeli, disiplin soruşturmasının kapsamını aşacak şekilde, soruşturma konusunu aşacak şekilde geliş güzel bir veri işleme faaliyetine imkân verilmemelidir. Nitekim, 6698 sayılı Kanunun ilk amacı özel hayatın gizliliği başta olmak üzere temel hak ve özgürlüklerin korunmasıdır. Öyleyse yürütülen soruşturma ya da kovuşturma mevzuatın belirlediği gizlilikte ilerlemeli, konuyla ilgisiz kişilerin soruşturma dosyasına erişmesini, dosyadaki bilgilerin üçüncü kişilerle paylaşılmasını engelleyecek mekanizmaların oluşturulması gerekecektir. Kanunun 28/2-c maddesi, bu kapsamda işlenen kişisel veriler için bir takım istisna durumları getirmiş olsa bile işlenen veri 6698 sayılı Kanun kapsamında kişisel veri niteliğini korumakta ve belirlenen istisna hükümleri dışındaki hükümlere tâbi olmayı sürdürmektedir.

Örneğin, üniversitede yapılan sınav esnasında telefonu ile kopya çektiği ve masasının altında not kağıtları olduğu sınav gözetmenince tespit edilen öğrenciden, kopya çekme eyleminin tespiti için sınav kağıdıyla birlikte telefonu ve not kağıtları istendiğinde, öğrencinin, bu talep karşısında telefondaki bilgilerin ve notlarının kişisel veri olduğu yönündeki itirazını yukarıdaki istisna hükmünü de göz önünde bulundurmak suretiyle KVKK kuralları bağlamında değerlendirmek gerekir.

Bu bağlamda, öncelikle KVKK m. 28/2-c maddesi gereği, belirli hükümleri hariç, KVKK uygulanacaktır. Öyleyse, İdarenin, öğrencinin telefonu ve masanın altında bulunan not kağıtlarının içeriklerini incelenmek için KVKK'nun 5. maddesinde belirlenen veri işleme şartlarından birine dayanması gerekir. Bu bağlamda İdarenin hukuki yükümlülüklerini yerine getirebilmesi için zorunlu olması (m.5/2(ç)) şartına dayanarak ilgili verileri işleyebileceği kabul edilmelidir. Nitekim 2547 sayılı Kanun'da yükseköğretimin amaçlarını ve ilkelerini belirleyen 4. ve 5. maddelerinden hareketle Yükseköğretim Kurumu'nun eğitim ve öğretimin kalitesini ve güvenilirliğini sağlama yükümlülüğü bulunduğu kabul edilmelidir. Yine Kanunun 54/1(a) maddesinin 5. alt bendine göre sınav esnasında kopya çekmeye teşebbüs etmek disiplin suçudur ve öğrenci kınama cezasıyla cezalandırılır. Dolayısıyla, kopya çekme teşebbüsünün görüldüğü anda üniversite tarafından görevlendirilmiş olan gözetmen, bu teşebbüsü tespiti yarayan ve kişisel veri içeren belge ve materyalleri talep edebilir ve bu bilgiler soruşturmacı tarafından işlenebilir.

Bununla birlikte, soruşturma sırasında veri koruma ilkelerine özen gösterilmeli, veri minimizasyonu ilkesi gereği sadece kopya teşebbüsüyle ilgili kişisel verilere erişim sağlanmalıdır. Örneğin, sınavın başlangıç saati esas alınarak kopya teşebbüsünü tespit amacıyla öğrencinin cep telefonundaki, söz gelimi son 1 saatlik internet gezinmesi, son çektiği fotoğraflar ve son 1 saat içindeki mesajlaşma dökümleri incelenmelidir. Ayrıca, soruşturma sona erdikten sonra, kişisel verileri içeren soruşturma evrakları da ilgili mevzuatta belirlenen süre geçtikten hemen sonra imha edilmelidir.

- Kişisel Verilerin Bütçe, Vergi ve Mali Konulara İlişkin Olarak Devletin Ekonomik ve Mali Çıkarlarının Korunması Amacıyla İşlenmesi: 6698 sayılı Kanunun 28/2. maddesinin “ç” bendinde yer verilen hükme göre “*kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması*” halinde Kanunun aydınlatma yükümlülüğüne ilişkin 10. maddesi, zararın giderilmesini talep etme hakkı dışında kişinin haklarını düzenleyen 11. maddesi ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. maddesi uygulanmayacaktır.

İlgili maddede içeriği duruma göre değişebilen, soyut ifadelerin kullanıldığı dikkati çekmektedir. “Mali konulara ilişkin”, “Devletin ekonomik (çıkarları)” ve “(Devletin) mali çıkarları” gibi ifadelerin içeriğinin tespit edilmesi güçtür. İçeriğinde para olan ya da parasal anlamda etki gücüne sahip bulunan politik, siyasi her türlü mesele bu kavramların içine dahil edilebilir görünmektedir²⁴⁰. Üstelik Devletin ekonomik ve mali çıkarları, içinde bulunulan ekonomik durum, kriz, vergi politikası gibi hususlara göre değişkenlik gösterebilecektir²⁴¹. Rekabetin sağlanması adına yapılan çalışmaların, ithalat ve ihracat kurallarına ilişkin düzenlemelerin veya idarenin kamu hizmetlerinin gördürülmesi bağlamında akdettiği sözleşmelerin Devletin mali çıkarlarına ilişkin kabul edilmesinin önünde de bir engel olduğu söylenemez. Ayrıca, bu geniş kapsamına rağmen ilgili hükümde istisna kapsamında kabul edilen veri işleme faaliyetini gerçekleştirecek kişi ya da kurumlara ilişkin bir sınırlamaya yer verilmediği görülmektedir. Örneğin, 28/1-ç maddesinde “kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları”, yine 28/1-d maddesinde “yargı makamları veya infaz mercileri” gibi veri sorumlusu bakımından getirilen bir sınırlama 28/2-ç fıkrasında bulunmamaktadır.

²⁴⁰ Mimarlar Odası Ankara Şubesi tarafından Toplu Konut İdaresi Başkanlığı’na yapılan ve Atatürk Orman Çiftliği arazisi üzerine inşa edilen Cumhurbaşkanlığı sarayının maliyeti hakkında bilgi verilmesine yönelik bilgi edinme başvurusu talebi, 4982 sayılı Bilgi Edinme Hakkı Kanunu’nun 17. maddesinde yer verilen “*Açıklanması ya da zamanından önce açıklanması hâlinde, ülkenin ekonomik çıkarlarına zarar verecek veya haksız rekabet ve kazanca sebep olacak bilgi veya belgeler, bu Kanun kapsamı dışındadır*” hükmü gerekçe gösterilerek reddedilmiş, bu husus medyaya “Maliyeti Açıklanırsa Ülke Ekonomisi Çıkarları Zarar Görür” başlıklı haber metinleriyle yansımıştır. “Maliyeti açıklanırsa ülke ekonomisi çıkarları zarar görür”, **Dünya**, 2.12.2014, <https://www.dunya.com/gundem/039maliyeti-aciklanirsa-ulke-ekonomisi-cikarlari-zarar-haberi-264593>; “TOKİ, Cumhurbaşkanlığı Sarayı’nın maliyetini mahkemeye de açıklamadı”, **CNN Türk**, 28.1.2015, <https://www.cnnturk.com/turkiye/toki-cumhurbaskanligi-sarayinin-maliyetini-mahkemeye-de-aciklamadi> (E.T. 7.12.2023).

²⁴¹ Neslihan KARATAŞ DURMUŞ, “Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti”, **TAAD**, Y. 8, S. 31 (Temmuz 2017), s. 399; Arzu KALYON, “Türk Vergi Hukukunda Kişisel Verilerin Korunması”, **Marmara Üniversitesi SBE**, Doktora Tezi, 2021, s.75.

Öte yandan, 28/1-ç maddesinde yer verilen “...ekonomik güvenliği sağlamaya yönelik olarak...önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi” halinde 6698 sayılı Kanunun uygulanmayacağına yönelik kural ile 28/2-ç hükmünde Devletin ekonomik çıkarlarının korunması amacıyla işlenen kişisel veriler için kısmi istisna uygulanacağı hükmünün çeliştiği ifade edilmektedir²⁴². Nitekim, “bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik çıkarlarının korunması” amacıyla yapılacak işlemlerin genel anlamda ekonomik güvenliğin sağlanması amacını taşıyacağı söylenebilecektir. Bu sebeple, hangi hükmün ne zaman uygulanacağı sorunu ortaya çıkmaktadır. Bir görüş, 28/2-ç maddesinde yer verilen “bütçe, vergi ve mali konular” ifadelerinden hareketle vergi konusunda öncelikle bu bendin uygulanması gerektiğini, bu hükmü aşan hususlarda ise 28/1-ç maddesinin uygulama imkânının olup olmadığının değerlendirilebileceğini savunmaktadır²⁴³. Böylece, ilgililere daha geniş bir hukuki korunma sağlanmış olacaktır. Bir diğer görüşse, AYM’nin 28/1-ç hükmünü de incelediği E.2016/125, K.2017/143 sayılı kararındaki, ilgili hüküm bağlamında kişisel veri işleyen kurumların 2559 sayılı PVSK, 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun’da gösterildiğine ilişkin ifadelerinden hareketle, bu kanunlarda gösterilen kamu kurum ve kuruluşlarının yetkisi dahilinde bulunmamakla birlikte Devletin ekonomik ve mali çıkarlarına ilişkin olan hususlarda 28/2-ç hükmünün uygulanması gerektiğini savunmaktadır²⁴⁴.

6698 sayılı Kanun gerekçesinde ilgili hükümlere ilişkin herhangi bir açıklamaya yer verilmemiş olup hükümlerin tekrarıyla yetinildiğinden, bu noktadan hareketle bir yorumda bulunulamamaktadır. Öte yandan, Kurul tarafından 28/2-ç hükmünün anıldığı yalnızca bir karara rastlandığı, bu kararda vergi incelemesine tabi tutulan mükellefin yanı sıra mükellefle ilgili kimselerden olan şikâyetçi kişiye ait kişisel verilerin işlenmesinin 28/2-ç kapsamında değerlendirildiği görülmektedir²⁴⁵.

28/2-ç maddesinde bütçe ve vergi kavramlarının en azından açıkça zikredilmiş olması sebebiyle bunlara ilişkin yapılacak olan kişisel veri işleme faaliyetlerinde bu hüküm uygulanmalıdır. Bununla birlikte, somut olaya göre değerlendirildiğinde bütçe veya vergiye ilişkin bir hususta işlenen kişisel verilerin ekonomik güvenliği ilgilendirdiği gerekçesiyle 28/1-ç hükmü bağlamında değerlendirilmesi de mümkündür. İlgili veri işleme faaliyetinin hangi kapsamda kaldığına ilişkin nihai kararı görevli yargı yeri vermelidir. Öte yandan, kısmi istisnanın öngörüldüğü hallerde kişisel veri işlemenin bu Kanunun amacına ve temel ilkelerine uygun ve orantılı şekilde yapılması gerektiği unutulmamalıdır.

Bir AİHM kararına konu olayda, Macaristan hükümeti tarafından 2006 yılında borçlu vergi mükelleflerinin kişisel verilerin yayınlanması yönünde mevzuat değişikliğine gidilmiş ve vergi

²⁴² TANSUĞ, s. 92.

²⁴³ UZUNÖZ, s.121.

²⁴⁴ TANSUĞ, s.93-94.

²⁴⁵ KVK Kurulu, 13.2.2020 tarih ve K.2020/120 sayılı kararı, <https://www.kvkkarar.com/2020-120/> (E.T. 7.12.2023).

makamlarının internet sitesinde “büyük vergi borçluları” adı altında yüksek oranda vergi borcu olan kişilerin ad ve soyadlarıyla birlikte ev adreslerinin de yazılı olduğu listeler yayımlanmaya başlanmıştır. Yapılan başvuruyu inceleyen Mahkeme, söz konusu yayımların vergi disiplinini sağlamasında kişinin mahremiyet hakkına karşı kamu yararının tartışılmadan sistematik olarak yapıldığını, hükümet tarafından değişiklik ile elde edilecek yararın hesaplanmadığını, ayrıca vergi borçlusunun ev adresinin internette yayınlanarak kötü niyetli kişilerce de ulaşılabilir olmasının oluşturduğu riskin yetkililerce değerlendirilmediğini, bu gerekçelerle, hükümetin bu tür konularda karar verme noktasında geniş takdir yetkisi bulunmasına karşın, söz konusu yayınların yapılma gerekçelerinin, başvuranın haklarına yapılan müdahalenin gerekli olduğunu göstermek için yeterli olmadığı sonucuna varmış ve özel hayata saygı hakkının ihlal edildiğine karar vermiştir²⁴⁶.

4. KANUNİ ŞARTLARA UYUM: 6698 SAYILI KANUNA GÖRE VERİ İŞLEMENİN ŞARTLARI VE İDARENİN YÜKÜMLÜLÜKLERİ

İdare kendisine kanunla verilen görevleri yerine getirirken birçok durumda kişisel veri işleme faaliyetinde bulunmaktadır. 6698 sayılı Kanun, 28 inci maddesinde sayılan durumlar haricinde, İdareyi bu Kanunda belirlenen kurallardan bağışık tutmadığı için kişisel veri işleme faaliyetinde bulunan İdarenin de Kanunda düzenlenen yükümlülükler uygun şekilde hareket etmesi gerekmektedir.

Bu bakımdan, aşağıda kişisel veri işleme faaliyetinde bulunan bir İdarenin yerine getirmesi gereken Veri Sorumluları Sicili’ne (VERBİS) kayıt yükümlülüğü, veri güvenliğinin sağlanması yükümlülüğü, aydınlatma yükümlülüğü ve kişisel verileri Kanunda belirlenen şartlara uygun şekilde işleme yükümlülüğü konularına yer verilecektir.

4.1. İdarenin Veri Sorumluları Siciline Kayıt Yükümlülüğü

6698 sayılı Kanunun 16. maddesinin ilk fıkrasında KVK Kurulunun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulacağı belirtilmiş, ikinci fıkrasında ise kişisel verileri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce bu sicile kaydolmak zorunda oldukları ifade edilmiştir. Dolayısıyla kural olarak bir veri sorumlusu VERBİS’e kaydolmadan veri işleyemez.

Bununla birlikte, kanun koyucu sicile kayıt zorunluluğunun istisnalarını belirleme yetkisini Kurul’a vermiştir (m.16/2). Buna göre Kurul, “işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu” gibi yine Kurul tarafından belirlenecek objektif kriterleri göz önüne alarak Sicile kayıt zorunluluğuna istisna getirebilecektir.

²⁴⁶ AİHM, L.B. / Macaristan, B.n. 36345/16, T. 9.3.2023.

Kanun hükmünde örnekleme yoluyla bazı objektif kriterlere yer verilmiş olmakla beraber Kurul bu kriterleri kullanmakla sınırlanmamıştır.

19.07.2018 tarih ve 2018/88 sayılı Kurul kararı uyarınca VERBİS'e kaydolmakla yükümlü olanlar belirlenmiştir. Karara göre kayıt yükümlülüğünün belirlenmesinde çalışan sayısı ve yıllık mali bilanço kriterlerinin dikkate alındığı görülmüştür. Buna göre, yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları sicile kaydolmak zorundadır. Bununla birlikte çalışan sayısı veya mali bilanço kriterini taşımasa da ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişilerin de sicile kaydolması zorunludur. Ayrıca, yurt dışında yerleşik olan gerçek ve tüzel kişiler de sicile kaydolmakla yükümlüdür.

Kurul tarafından daha sonra alınan kararlar uyarınca VERBİS'e kayıt yükümlülüğü bulunmayanlar listesi genişlemiştir. Buna göre, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler, noterler, ilgili Kanunlarına uygun olarak kurulmuş olan dernek, vakıf ve sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler, siyasi partiler, avukatlar, serbest muhasebeci mali müşavirler ve yeminli mali müşavirler²⁴⁷; gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirleri²⁴⁸ ve arabulucular²⁴⁹ sicile kaydolmakla yükümlü değildir. Ayrıca, 22.4.2020 tarih ve 2020/315 sayılı Kurul kararı ile dernek, vakıf ve sendikalara ilişkin “yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler” şeklindeki 2018/32 sayılı kararda yer alan hüküm “yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalardan kendisine herhangi bir iktisadi işletmesi bulunmayanlar” şeklinde değiştirilmiş, ardından Türkiye’de yerleşik olup da kendisine bağlı herhangi bir iktisadi işletmesi bulunanların, yalnızca bu işletme faaliyetlerine ilişkin bilgileri vermek suretiyle VERBİS'e kayıt yaptırmalarına karar verilmiştir²⁵⁰.

Öte yandan, 2018/32 sayılı Kurul kararında kamu kurum ve kuruluşları bakımından kural olarak herhangi bir istisnaya yer verilmemiş ve kişisel veri işleme faaliyetinde bulunan tüm kamu kurum ve kuruluşlarının sicile kaydolması zorunlu tutulmuştur. Kural bu olmakla birlikte, İdarelerin her türlü kişisel veri işleme faaliyeti için sicile kaydolma yükümlülüğü bulunduğunu söylemek güçtür. Nitekim, 6698 sayılı Kanunun “İstisnalar” başlıklı 28 inci maddesinin ilk fıkrasında sayılan konulara ilişkin yapılacak veri işleme faaliyetleri bu Kanun kapsamında bulunmadığından; ikinci fıkrasında sayılan veri işleme faaliyetleri içinse aydınlatma yükümlülüğünün yanı sıra VERBİS'e kayıt yükümlülüğünün de

²⁴⁷ KVK Kurulu, 2.4.2018 tarih ve 2018/32 sayılı kararı.

²⁴⁸ KVK Kurulu, 28.6.2018 tarih ve 2018/68 sayılı kararı.

²⁴⁹ KVK Kurulu, 5.7.2018 tarih ve 2018/75 sayılı kararı.

²⁵⁰ KVK Kurulu, 9.6.2021 tarih ve 2021/571 sayılı kararı.

uygulanmayacağı düzenlendiğinden, İdarelerin Kanunun 28 inci maddesinde sayılan konularda yapacağı kişisel veri işleme faaliyetleri bakımından sicile kayıt zorunluluğu bulunmamaktadır.

6698 sayılı Kanunun 16. maddesinin 3. fıkrasında sicile kayıt başvurusunda hangi bilgilere yer verilmesi gerektiği düzenlenmiştir. Buna göre, sicile kayıt başvurusu amacıyla Kuruma yapılacak bildiride “*veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri, kişisel verilerin hangi amaçla işleneceği, veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar, kişisel verilerin aktarılabilmesi için alıcı veya alıcı grupları, yabancı ülkelere aktarımı öngörülen kişisel veriler, kişisel veri güvenliğine ilişkin alınan tedbirler ve kişisel verilerin işlendikleri amaç için gerekli olan azami süre*” hususlarındaki bilgilere yer verilmelidir.

Veri Sorumluları Siciline ilişkin diğer usul ve esasların yönetmelikle düzenleneceğine yönelik Kanun hükmü (m.16/5) uyarınca Veri Sorumluları Sicili Hakkında Yönetmelik 30.12.2017 tarihinde Resmî Gazete’de yayımlanmıştır²⁵¹. Yönetmeliğin 5. maddesine göre sicile kayıtlı yükümlü olan veri sorumluları Kişisel Veri İşleme Envanteri hazırlamakla yükümlü tutulmuş, Sicil başvurularında Sicile açıklanacak bilgilerin bu envantere dayalı olarak hazırlanacağı belirlenmiştir. Kişisel veri işleme envanteri Yönetmelikte “*veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter*” şeklinde tanımlanmıştır (m.4/1(h)).

Envanterin doğru, güncel, hukuka uygun ve eksiksiz şekilde tutulması önem arz etmekte olup envanterin bu kurallara uygun şekilde tutulmasında sorumluluk veri sorumlusu olan İdarededir (Yönetmelik, m.5/e). Nitekim, Kanunda öngörülen aydınlatma yükümlülüğü, ilgili kişilerin Kanunun 13. maddesi uyarınca veri sorumlusuna yapacağı başvuruların yanıtlanması ve ilgili kişilerin vereceği açık rızaların kapsamlarının belirlenmesi hususlarındaki incelemelerde bu envantere dayalı olarak Sicile sunulan bilgiler esas alınacaktır (Yönetmelik, m.5/d).

Bu noktada, Kanuni tanımdan hareketle, tüzel kişilerde kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan veri sorumlusu tüzel kişiliğin kendisi olduğu, yoksa tüzel kişi içerisinde çalışan kişiler olmadığı ifade edilmelidir. Nitekim, Türkiye’de yerleşik olan tüzel kişilerin veri sorumlusu yükümlülüklerinin, ilgili mevzuat hükümlerine göre tüzel kişiliği temsile yetkili organ yahut kişi veya kişiler aracılığıyla yerine getirileceği, bu organların Kanuni yükümlülüklerin yerine getirilmesi için bir veya birden fazla kişiyi görevlendirebileceği, ancak bu görevlendirmenin tüzel kişiliğin sorumluluğunu ortadan kaldırmayacağı

²⁵¹ RG, 30.12.2017/30286.

Yönetmeliğin 11. maddesinin ilk fıkrasında düzenlenmiştir. Öte yandan, veri sorumluları adına belirlenen veri sorumlusu temsilcilerinin, Sicile kayıt sırasında irtibat kişisi belirleyerek bu kişinin bilgilerini Sicile işleyeceği, ancak irtibat kişilerinin veri sorumlusunu temsile yetkili olmadığı kuralına da yer verilmiştir (Yönetmelik, m.11/4).

Tüm kamu kurum ve kuruluşları birer tüzel kişilik olduklarından bu tüzel kişilikler de kanuni tanıma uymak şartıyla birer veri sorumlusudur. Özel hukuk tüzel kişisinden farklı olarak 6698 sayılı Kanunda İdareler için bir “üst düzey yönetici” belirlenmesinden söz edilmiştir. Gerçekten, Kanunun 1. geçici maddesinin beşinci fıkrasında “*Bu Kanunun yayımı tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında bu Kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenerek Başkanlığa bildirilir.*” düzenlemesine yer verilmiştir. Yönetmelikte Kişisel Verileri Koruma Kurumu ile İdare arasındaki iletişimi sağlamak amacıyla Sicile kaydı yapılan ve daire başkanı veya üstü yöneticiler arasından seçilen irtibat kişisinin, Kanunda belirtilen “üst düzey yönetici” tarafından belirleneceği kabul edilmiştir (Yönetmelik, m.11/5).

Veri Sorumluları Siciline kayıt başvurusunda veri sorumluları tarafından “Kişisel verilerin işlendikleri amaç için gerekli olan azami süre” bilgisine de yer verilmesi gerektiği ifade edilmiştir (Kanun, m.16/3(f)). Yönetmelik hükmüne göre de Sicile sunulan verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi, Kanunun 7. maddesinde yeri verilen veri sorumlularının silme, yok etme veya anonim hale getirme yükümlülüklerinin yerine getirilmesinde dikkate alınacaktır (m.5/ğ)²⁵².

Veri sorumlularının belirli veri kategorilerinin işlenmesine ilişkin Sicile bildireceği azami muhafaza edilme sürelerine ilişkin olarak mevzuatta farklı bir süre belirlenmiş olması halinde ilgili mevzuat hükmü uygulanacaktır. Mevzuatta belirlenen azami muhafaza sürelerine örnek olarak, özellikle disiplin cezalarının özlük dosyasından silinmesi için öngörülen sürelerle ilişkin kanuni düzenlemeler²⁵³

²⁵² Ayrıca yine Yönetmeliğe göre “*kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin belirlenmesi, bu sürelerin kişisel veri işleme envanterinde belirtilen bilgilerle uyumu ve azami sürenin aşılmamasının takibi için kişisel veri saklama ve imha politikası hazırlayarak, bu politikanın uygulanmasını temin*” etmek veri sorumlularının görevlerindendir (m.9/5). Bu politikanın kapsamı ise Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’te düzenlenmiştir (RG,28.10.2017/30224).

²⁵³ 657 sayılı Devlet Memurları Kanunu’nun 133/1. maddesi uyarınca uyarma ve kınama cezalarının uygulanmasından itibaren beş yıl, Devlet memurluğundan çıkarma cezası dışındaki diğer cezaların uygulanmasından itibaren on yıl sonra silinmelerinin talep edilebileceğine ilişkin düzenleme; 2547 sayılı Yükseköğretim Kanunu’nun 53/G maddesinin ikinci fıkrası uyarınca, uyarma ve kınama cezalarının uygulanmasından itibaren beş yıl, aylıktan veya ücretten kesme ve kademe ilerlemesinin durdurulması veya birden fazla ücretten kesme cezalarının uygulanmasından itibaren on yıl sonra özlük dosyasından silinmelerinin talep edilebileceğine ilişkin düzenleme ve yine 2802 sayılı Hakimler ve Savcılar Kanunu’nun 75/1. maddesinde yer verilen kurala göre uyarma, aylıktan kesme ve kınama cezalarının kesinleşmesinden itibaren dört yıl, kademe ilerlemesi ve derece yükselmesini durdurma cezalarının kesinleşmesinden itibaren altı yıl geçtikten sonra sicillerinden silinmesini isteyebileceklerine ilişkin düzenlemeler örnek olarak verilebilir.

ve 5352 sayılı Adli Sicil Kanunu'nda adli sicil ve arşiv bilgilerinin silinmesine ilişkin 12. madde hükmü²⁵⁴ gösterilmektedir²⁵⁵.

Dolayısıyla, veri sorumlusu İdarelerin kişisel verilerin işlendikleri amaç için gerekli azami muhafaza sürelerini belirlerken öncelikle mevzuattaki düzenlemelere göre hareket etmesi gerekecektir. Ancak, mevzuatta İdarenin işlediği kişisel veri kategorisine ilişkin olarak herhangi bir süre belirlenmemişse o halde bu süreyi veri sorumlusu İdare Yönetmelikte belirlenen ölçütleri dikkate alarak kendisi belirleyecektir²⁵⁶.

6698 sayılı Kanun'un 16. maddesi ve Veri Sorumluları Sicili Hakkında Yönetmelik hükümleri bu yönde olmakla birlikte, 16.7.2018 tarih ve 30480 sayılı RG'de yayımlanan 11 No'lu Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi veri sorumlusu İdareler için farklı bir durum yaratmıştır. Devlet Arşivleri Başkanlığı'nın kuruluş, görev ve yetkilerini ilişkin usul ve esasları düzenlemek için çıkarılan 11 No'lu CBK'da devlet arşivlerine ilişkin esasları belirlemek, arşiv belgelerinin tahribini önleyici tedbirler almak, arşivlerden yararlanma usul ve esasları belirlemek gibi hususlar Başkanlığın görevleri arasında sayılmıştır. Devlet arşivleri kişisel verilerle sınırlı bilgilerden ibaret olmamakla beraber elbette kişisel verileri de barındıran nitelikteki belgelerdir. Bu düzenlemeye tabi kılınan İdarelerin genişliği de düşünüldüğünde²⁵⁷ ilgili CBK'nın kişisel veriler içerebilecek

²⁵⁴ Adli Sicil Kanunu'nun 12. maddesi şu şekildedir: (1) (Değişik: 5/4/2012-6290/2 md.) Arşiv bilgileri; a) İlgilinin ölümü üzerine, b) Anayasanın 76 ncı maddesi ile Türk Ceza Kanunu dışındaki kanunlarda bir hak yoksunluğuna neden olan mahkûmiyetler bakımından kaydın arşive alınma koşullarının olduğu tarihten itibaren; 1. Yasaklanmış hakların geri verilmesi kararı alınması koşuluyla onbeş yıl geçmesiyle, 2. Yasaklanmış hakların geri verilmesi kararı alınması koşulu aranmaksızın otuz yıl geçmesiyle, c) Diğer mahkûmiyetler bakımından kaydın arşive alınma koşullarının olduğu tarihten itibaren beş yıl geçmesiyle, tamamen silinir. (2) Fiilin kanunla suç olmaktan çıkarılması halinde, bu suçtan mahkûmiyete ilişkin adli sicil ve arşiv kayıtları, talep aranmaksızın tamamen silinir. (3) Kanun yararına bozma veya yargılamanın yenilenmesi sonucunda verilen beraat veya ceza verilmesine yer olmadığı kararının kesinleşmesi halinde, önceki mahkûmiyet kararına ilişkin adli sicil ve arşiv kaydı tamamen silinir. (4) (Ek: 24/11/2016-6763/40 md.) Akıl hastalığı nedeniyle hükmedilen güvenlik tedbirlerine ilişkin kayıtlar, infazının tamamlanmasıyla tamamen silinir.

²⁵⁵ ÇAĞLAYAN, Ramazan, "İdare Hukuku Açısından Kişisel Verilerin İmhası ve Denetim", içinde **Avrupa Birliği Hukuku İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası**, SAKA, Rıza/ÇAĞLAYAN, Ramazan/KOCA Mahmut, Seçkin Yayıncılık, 2. Baskı, 2022, Ankara, s. 262-263; TANSUĞ, s.114-115.

²⁵⁶ Veri Sorumluları Sicili Hakkında Yönetmelik'in 9/4. maddesinde kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme sürelerinin belirlenmesinde şu hususların dikkate alınması gerektiği ifade edilmiştir: "a) İlgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre, b) İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre, c) İlgili veri kategorisinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre, ç) İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre, d) Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı, e) Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre, f) Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi."

²⁵⁷ 11 No'lu CBK'nın "Kapsam" başlıklı 2. maddesi şu şekildedir: "(1) Bu Cumhurbaşkanlığı Kararnamesi, Türkiye Büyük Millet Meclisi ve Milli İstihbarat Teşkilatı Başkanlığı hariç olmak üzere 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununa ekli cetvellerde yer alan kamu idarelerini, Genelkurmay Başkanlığını, Kuvvet Komutanlıklarını, mahalli idareler (köyler hariç) ve bunların bağlı kuruluşlarını, kamu tüzel kişiliğini haiz diğer kurum, kuruluş, enstitü, teşebbüs, teşekkül, birlik, fon gibi adlarla kurulmuş olan bütün kamu kurum ve kuruluşlarını, kamu kurumu niteliğindeki meslek kuruluşlarını, vergi muafiyeti tanınan vakıfları ve kamu yararına çalışan dernekleri kapsar."

belgelerin imha süreçlerine ilişkin usul ve esasları düzenlemesinin hukuka uygun olup olmadığı değerlendirilmelidir.

Aşağıda daha ayrıntılı şekilde değinilmekle birlikte²⁵⁸ şu kadarı ifade edilmelidir ki, Anayasa'nın İkinci Kısımının İkinci Bölümünde, 20/3. maddesinde düzenlenen kişisel verilerin korunması hakkına ilişkin bir düzenlemenin Kanunla yapılması gerekir. Nitekim, bu durum Anayasanın 20/3. maddesinin son cümlesinde “*Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*” denilmek suretiyle açıkça ifade edilmiştir. Kişisel verilerin saklanması ve imhası hususları da kişisel verilerin korunması hakkı kapsamındadır. Olağan dönem CBK'ların düzenleme yapabileceği alanların Anayasa'nın 104. maddesiyle sınırlandığı da düşünüldüğünde, Devlet arşivlerinde bulunan belgelerin saklanması ve imhasına ilişkin Kanuni bir düzenleme yapılması ve bu Kanuna dayalı olarak çıkarılacak Yönetmeliklerle ayrıntıların belirlenmesi hukuka uygun olacaktır²⁵⁹. Bu yönde yapılacak bir mevzuat çalışmasına kadar ise 6698 sayılı Kanun'un 7. maddesi ile buna dayanılarak çıkarılan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine göre hareket edilmesi gerekir.

4.2. İdarenin Veri Güvenliği Uygulamaları

6698 sayılı Kanunun 12. maddesinde veri sorumlularının veri güvenliğine ilişkin yükümlülükleri konusuna yer verilmiştir. Buna göre veri sorumluları a) kişisel verilerin hukuka aykırı işlenmesini ve b) kişisel verilere hukuka aykırı erişilmesini önlemek ile c) kişisel verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kanun hükmüne bakıldığında verilerin kanuna uygun işlenmesi, kanuna aykırı şekilde erişilmemesi ve yine ikincisine benzer olarak, verilerin muhafazasının sağlanması amacıyla güvenlik tedbirleri alınması gerektiğinin düzenlendiği görülmektedir. Kişisel verilere kanuna aykırı şekilde erişilmesini önlemek ile muhafazasını sağlamak ifadelerinin benzer anlamlar taşıdığı göze çarpmaktaysa da “hukuka aykırı şekilde erişilmesini önlemek” ifadesindeki anlamın yetkisiz kişilerin verilerin bulunduğu fiziksel yahut elektronik ortama sızmasını engellemek olduğu, “verilerin muhafazasının sağlanması” ifadesinden ise verilerin doğru şekilde muhafaza edilmek suretiyle deprem, su baskını ve hırsızlık gibi olaylara karşı gerekli tedbirlerin alınması şeklinde okunması gerektiği ifade edilmektedir²⁶⁰.

Öte yandan “kişisel verilerin hukuka aykırı olarak işlenmesini önlemek” amacıyla gerekli tedbirleri almanın geniş bir anlamı ifade ettiği görülmektedir. Bu bağlamda, kişisel verilerin 6698 sayılı Kanunun 4. maddesinde sayılan genel ilkelere, 5. maddesinde sayılan genel nitelikli verilerin işlenme şartlarına ve 6. maddesinde sayılan özel nitelikli verilerin işlenme şartlarına aykırı şekilde işlenmesini

²⁵⁸ Bkz. “4.4.1.2.1. Kanunlarda Açıkça Öngörülmesi” başlığı.

²⁵⁹ Aynı yönde görüş için bkz. TANSUĞ, s.190.

²⁶⁰ ALTINDAĞ, *Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları*, s.79; ÇEKİN, s.197.

engellemek için lazım gelen tedbirlerin alınması gerekecek, bu kurallara aykırı şekilde veri işlenmesi halinde veri sorumlusunun “veri güvenliğine ilişkin yükümlülükleri yerine getirmemesi” kabahatini işlemesi anlamına gelebilecek ve bu durum idari para cezasının belirlenmesinde etkili olacaktır (m.18/b). Dolayısıyla, veri güvenliğinin sağlanmasının sadece fiziki veya elektronik önlemlerin alınmasından ibaret olmadığı, alınacak her türlü teknik ve idari tedbirlerle kişisel verilerin kanunda sayılan ilke ve şartlara aykırı şekilde işlenmesinin de önüne geçilmesi gerektiği ifade edilmelidir²⁶¹.

Veri güvenliğine ilişkin alınan önlemler, veri sorumlusunun kusurunun belirlenmesi bakımından önem arz etmektedir. Bu bağlamda veri sorumlusunun makul teknik ve idari tedbirleri almış olmasına rağmen kişisel verileri hukuka aykırı şekilde işlenmesine ya da elinde bulundurduğu verilere erişilmesine engel olamazsa yine de bundan sorumlu tutulacak mıdır? Kanunun 12/1. maddesi hükmünde “*uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak*” zorunda olduğu kuralına yer verilmiştir. Dolayısıyla, veri sorumlusu veri güvenliğine ilişkin mevcut olan, piyasada yeterli kabul edilecek düzeyde ve Kurul kararlarını da gözeterek veri güvenliğini sağlayan teknik ve idari tedbirleri aldıktan sonra yine de verilerin hukuka aykırı işlenmesine, verilere hukuka aykırı şekilde erişilmesine engel olamaz ya da verilerin muhafazasını sağlayamazsa, bu halde veri sorumlusu 6698 sayılı Kanunun 18/1. maddesinin (b) fıkrasında düzenlenen “veri güvenliğine ilişkin yükümlülüklerini yerine getirmeme” kabahatinden dolayı cezalandırılmamalıdır. Nitekim, 6698 sayılı Kanunda veri sorumlusunun kusursuz sorumluluğunun da açıkça düzenlenmediği düşünüldüğünde, 5326 sayılı Kabahatler Kanunu’nun 9. maddesi gereği veri güvenliğine ilişkin yükümlülüklerini yerine getirmeme kabahatinin kasti ya da taksirli bir davranışla işlenmesi gerekir^{262,263}.

KVK Kurulu Kanunun 12. maddesi uyarınca alınabilecek idari tedbir ve önlemler hakkında aldığı tavsiye niteliğindeki kararını kamuoyuyla paylaşmıştır²⁶⁴. Çift kademeli kimlik doğrulama imkânı sunulması, kullanıcıların uzun ve farklı karakterle oluşturulmuş güçlü bir parola belirlemesi konusunda teşvik edilmesi, IP adresinden yapılacak başarısız giriş denemelerinin sınırlandırılması gibi tedbirleri içeren duyuruda her veri sorumlusunun kendi risk değerlendirmelerine göre tavsiye edilen tedbirlerden kendileri için uygun olanları almasını tavsiye etmiştir²⁶⁵. Alınabilecek teknik ve idari tedbirler elbette

²⁶¹ ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, s.78.

²⁶² ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, s.136. Kabahatler Kanunu Madde 9 – “Kabahatler, kanunda açıkça hüküm bulunmayan hallerde hem kasten hem de taksirle işlenebilir.”

²⁶³ Bununla birlikte, kusurun aranması konusunda varılan sonucun kabahatin işlenmesine ilişkin olduğu ifade edilmelidir. 6698 sayılı Kanunun 14/3. maddesi uyarınca kişilik hakları zarar gören kişilerin genel hükümlere göre tazminat hakkı saklı tutulduğundan, veri sorumlusunun kusuru yoksa bile kişisel verinin hukuka aykırı işlenmesinden, verilere hukuka aykırı erişilmesinden ya da verilerin muhafaza edilememesinden doğan zararların, şartları oluşmuşsa, kusursuz sorumluluk hallerinden hareketle veri sorumlusundan tazmini yoluna gidilebilir.

²⁶⁴ Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu, <https://www.kvkk.gov.tr/Icerik/7177/Kullanici-Guvenligine-Iliskin-Veri-Sorumlulari-Tarafindan-Alinmasi-Tavsiye-Edilen-Teknik-ve-Idari-Tedbirlere-Iliskin-Kamuoyu-Duyurusu> (E.T. 15.08.2023).

²⁶⁵ İlgili kamuoyu duyurusunda Kurul tarafından veri sorumlularına almaları tavsiye edilen teknik ve idari tedbirler şunlardır: “Çift kademeli kimlik doğrulama (two-factor authentication) sistemlerini kurmaları ve kullanıcılarına üyelik başvurusu

bunlarla sınırlı değildir²⁶⁶. Veri sorumlusu İdare gerektiğinde sunduğu hizmetin içeriğine, kişisel verilerin nitelik ve niceliğine göre veri güvenliğini sağlayacağı farklı tedbirleri de almakla yükümlü olacaktır. Bu bakımdan her veri sorumlusu için geçerli ve yeterli olabilecek önlemler listesi hazırlamak oldukça güçtür. Bununla birlikte, Kurul tarafından verilen kararlar dikkate alınmak suretiyle veri güvenliğine ilişkin alınan teknik ve idari tedbirler çeşitlendirilerek veri güvenliği daha güçlü hale getirilmelidir.

Örneğin, Kurul tarafından verilen bir kararda, 657 sayılı Devlet Memurları Kanunu'na tabi olarak çalışan ve kişisel veri işleyen personelin 6698 sayılı Kanun ve buna ilişkin çıkarılan diğer mevzuata uygun hareket etmekle yükümlü olmalarının 657 sayılı Kanun gereği olduğu, bu sebeple söz konusu çalışanlara bir gizlilik sözleşmesi imzalatılmasına gerek olmadığı; bununla beraber, ilgili personele kişisel verilerin korunması hakkının korunması için uyulması gereken usul ve esasları içeren bilgilendirici metinlerin tebliğ edilmesi ve bu konuda düzenli şekilde eğitimler verilmesi gerektiği ifade edilmiştir²⁶⁷.

Yine Kurul tarafından alınan banko, gişe, masa gibi hizmet alanlarında kişisel verilerin korunmasına yönelik ilke kararında *“Bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesi uyarınca kişisel verilerin*

aşamasından itibaren alternatif güvenlik önlemi olarak sunmaları; kullanıcıların hesaplarına sık erişim sağlayan cihazlar haricinde farklı cihazlar üzerinden giriş yapılması durumunda, giriş bilgilerinin e-posta/sms vb. yöntemlerle ilgili kişilerin iletişim adreslerine iletilmesinin sağlanması; uygulamaların HTTPS (Hypertext Transfer Protocol Secure - Hiper Metin Aktarma Güvenli İletişim Kuralı) ile veya aynı güvenlik seviyesini sağlayacak bir şekilde koruma altına alınması; kullanıcı parolalarının, siber saldırı yöntemlerine karşı korunmasını teminen, güvenli ve güncel karma (hashing) algoritmaların kullanılması; IP (Internet Protocol Address) adresinden yapılacak başarısız giriş denemesi sayısının sınırlandırılması; ilgili kişilerin en az son 5 adet başarılı ve başarısız giriş denemeleri ile ilgili bilgilerini görüntüleyebilmelerinin sağlanması; ilgili kişilere aynı parolanın birden fazla platformda kullanılmaması gerektiğinin hatırlatılması; veri sorumluları tarafından parola politikasının oluşturulması ve kullanıcılara ait parolaların belirli aralıklarla değiştirilmesinin sağlanması veya bu hususun ilgili kişilere hatırlatılması; yeni oluşturulan parolaların, eski parolalarla (en az son üç parolayla) aynı olmasının engellenmesi, kullanıcı hesaplarına girişlerde bilgisayar ile insan davranışlarını ayırt edici güvenlik kodu gibi teknolojilerin (CAPTCHA, dört işlem vb.) kullanılması, erişime izin verilen IP adreslerinin sınırlandırılması; veri sorumlularının sistemlerine giriş yapılan parolaların uzunluğunun asgari 10 karakter olması, büyük-küçük harf, rakam ve özel karakterlerin bir arada kullanılmasına yönelik güçlü parola oluşturulmasının sağlanması; veri sorumlularının sistemlerine giriş için üçüncü parti yazılımlar veya servisler kullanılıyorsa bu yazılımların ve servislerin güvenlik güncelleştirmelerinin düzenli olarak gerçekleştirilmesi ve gerekli kontrollerin yapılması.”

²⁶⁶ Örneğin, Kurul kararına konu olan bir olayda, veri sorumlusu hastane çalışanı doktor, hastasının burun estetiği operasyonu sırasında baygın haldeyken fotoğraflarını çekmiş ve bunu kendi sosyal medya hesabında paylaşmıştır. Hastanenin Kurula yaptığı savunmada ilgili kişinin açık rıza beyanının bulunduğu ifade edilse de Kurul, ilgili rıza beyanının veri sorumlusu hastaneye verildiği, bu nedenle hastane çalışanı olan doktorun kişisel sosyal medya hesabında fotoğrafları paylaşmasına yönelik bir rıza beyanı bulunmadığı, öte yandan ilgili sosyal medya paylaşımından veri sorumlusu hastanenin haberi olmasına karşın bunun engellenmesine yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle özel hastane hakkında idari para cezası uygulanmasına karar verilmiştir: KVK Kurulu, 29.6.2022 tarih ve 2022/630 sayılı kararı. <https://www.kvkk.gov.tr/Icerik/7567/2022-630> (E.T. 15.8.2023).

²⁶⁷ KVK Kurulu, 26.12.2019 tarih ve 2019/393 sayılı kararı. <https://www.kvkk.gov.tr/Icerik/6868/2019-393> (E.T. 15.8.2023).

korunması ile ilgili olarak; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri almasına” karar verilmiştir²⁶⁸.

Yine Kişisel Verileri Koruma Kurumu tarafından yayımlanan “Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)” isimli kitapçıkta veri güvenliğine ilişkin önlemler hakkında bilgi verilmektedir²⁶⁹. İlgili Rehberde yetki matrisi, yetki kontrolü, erişim logları, kullanıcı hesap yönetimi, ağ güvenliği, uygulama güvenliği, şifreleme, sızma testi, saldırı tespit ve önleme sistemleri, log kayıtları, veri maskeleyme, veri kaybı önleme yazılımları, yedekleme, güvenlik duvarları, güncel anti-virüs sistemleri, silme, yok etme veya anonim hale getirme işlemleri ve anahtar yönetimi konularının alınabilecek teknik tedbirler olarak ifade edilmektedir. İdari tedbirler bakımından ise kişisel veri işleme envanteri hazırlanması, kurumsal politikalar (erişim, bilgi güvenliği, kullanım, saklama ve imha vb.), sözleşmeler (veri sorumlusu - veri sorumlusu, veri sorumlusu - veri işleyen arasında), gizlilik taahhütnameleri, kurum içi periyodik ve/veya rastgele denetimler, risk analizleri, iş sözleşmesi, disiplin yönetmeliği (kanuna uygun hükümler ilave edilmesi), kurumsal iletişim (kriz yönetimi, kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.), eğitim ve farkındalık faaliyetleri (bilgi güvenliği ve kanun) ve veri sorumluları sicil bilgi sistemine (verbis) bildirim şeklindeki tedbirlerin alınabileceği belirtilmektedir²⁷⁰.

Öte yandan, 6698 sayılı Kanunun 12. maddesinde, veri güvenliğinin sağlanması ve kanun hükümlerinin uygulanması amacıyla veri sorumlusu tarafından denetimler yapılması veya yaptırılması öngörülmüş (m.12/3), veri sorumluları ve veri işleyenlerin, öğrendikleri kişisel verileri Kanun hükümlerine aykırı şekilde açıklayamayacakları ve verinin işleme amacı dışında kullanamayacakları, bu yükümlülüklerinin işten ayrıldıktan sonra da devam edeceği düzenlenmiştir (m.12/4). Öte yandan, veri ihlalinin ortaya çıkması halinde, durumun veri sorumlusu tarafından en kısa sürede ilgisine ve Kurula bildirmesi gerektiği belirtilmiştir²⁷¹ (m.12/5). Ayrıca, 12. maddenin ilk fıkrasında belirtilen

²⁶⁸ Banko, Gişe, Masa gibi Hizmet Alanlarında Kişisel Verilerin Korunmasına Yönelik KVK Kurulu’nun 21/12/2017 tarih ve 2017/62 sayılı ilke kararı.

²⁶⁹ Kişisel Verileri Koruma Kurumu, “Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)”, KVKK Yayınları, Ocak 2018, Ankara. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (E.T. 15.8.2023).

²⁷⁰ İlgili eserde tavsiye edilen her türlü tedbire ilişkin ayrıntılı bilgiye yer verilmiştir.

²⁷¹ Bir kararında Kurul “İhlalin tespit edilmesinden 25 gün sonra Kuruma bildirildiği, İlgili kişilerden hastaneye gelen bir kişi dışında, hiç birine ihlalin bildirilmemiş olduğu hususları dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası hükmü ve Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin KVK Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan ‘en kısa sürede’ ifadesinin 72 saat olarak yorumlanmasına yönelik ifadeleri çerçevesinde bildirim yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 150.000 TL ... idari para cezası uygulanmasına” karar vermiştir. KVK Kurulu, 20.5.2020 tarih ve 2020/407 sayılı kararı. <https://www.kvkk.gov.tr/Icerik/6914/2020-407> (E.T. 15.8.2023).

teknik ve idari tedbirlerin alınması konusunda veri sorumlusu ve onun nam ve hesabına kişisel verileri işleyen kişi (veri işleyen) müştereken sorumlu kabul edilmiştir (m.12/2).

6698 sayılı Kanunun 12. maddesiyle genel anlamda veri güvenliğine ilişkin bir hüküm düzenlenmişse de özel nitelikli verilerin işleme şartlarının belirlendiği 6. maddesinin dördüncü fıkrasında “*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır*” şeklinde bir kurala daha yer verilmiştir. Söz konusu düzenlemeye istinaden Kurul tarafından 2018/10 sayılı ve “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*” başlıklı karar alınmış ve bu karar Resmî Gazete’de yayımlanmıştır²⁷². Dolayısıyla, veri sorumlusu İdare özel nitelikli verileri işlerken Kurul tarafından alınan bu kararda yer verilen veri güvenliğine ilişkin önlemleri de almakla yükümlüdür. Böylelikle kanun koyucu, hukuka aykırı şekilde işlenmesi halinde ilgilisi için daha büyük olumsuzluklara ve zararlara neden olması muhtemel hassas nitelikli verilerin güvenliğinin sağlanması bakımından daha detaylı ve ciddi önlemlerin alınmasını sağlamak istemiştir. Konu bütünlüğünün sağlanması ve tekrara düşülmemesi adına konuya ilişkin ayrıntılı açıklamalara aşağıda “5.4.2.1. Özel Nitelikli Verilerin İşlenmesinde Aranılan Genel Şart Olarak KVK Kurulu tarafından Belirlenen Yeterli Önlemlerin Alınması” başlığında yer verilmiş olup bilgi için bu başlığa bakılabilir.

4.3. Veri Sahipleriyle İletişimde İdarenin Aydınlatma Yükümlülüğü

6698 sayılı Kanunun 10. maddesinde “Veri Sorumlusunun Aydınlatma Yükümlülüğü” düzenlenmiştir. İlgili maddede veri sorumlusu ya da yetkilendirdiği kişilerin ilgili kişilere veri işleme faaliyeti konusunda vermesi gereken asgari bilgilere yer verilmiştir. Buna göre veri sorumlusu İdarenin aydınlatma yükümlülüğünü yerine getirmiş sayılabilmesi için en az 10. maddede belirtilen bilgileri içerecek şekilde ilgili kişileri bilgilendirmiş olması gerekmektedir²⁷³. 10. maddenin ilk fıkrasına göre bu bilgilendirme kişisel verilerin elde edilmesi sırasında gerçekleştirilmelidir.

İlgili maddeye göre aydınlatma metni de diyebileceğimiz bu bilgilendirme içerisinde “1- veri sorumlusunun ve varsa temsilcisinin kimliği; 2- kişisel verilerin hangi amaçla işleneceği; 3- işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilmesi; 4- kişisel veri toplamanın yöntemi ve hukuki sebebi ile 5- Kanunun 11. maddesinde sayılan ve ilgili kişiye tanınan hakları” konularında bilgi verilmelidir.

Kişisel Verileri Koruma Kurumu tarafından hazırlanan ve aydınlatma yükümlülüğü konusunda uyulacak usul ve esasların belirleyen Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ 10 Mart 2018 tarihli Resmi Gazete’de yayımlanmıştır. Bu Tebliğ’de

²⁷² RG, 7.3.2018/30353.

²⁷³ ALTINDAĞ, *Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları*, s.57.

aydınlatma yükümlülüğünde uyulacak usul ve esasların yanı sıra kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğünün ne zaman gerçekleştirileceği konusu da düzenlenmiştir.

Yukarıda ifade edildiği üzere Kanunun 10. maddesinde aydınlatmanın ilgili kişinin kişisel verisinin elde edildiği sırada gerçekleştirilmesi gerektiği düzenlenmiştir. İlgili kişinin açık rıza beyanı da alınacaksa söz konusu aydınlatma yükümlülüğü en geç bu rızanın alınmasından önce yerine getirilmeli, böylece aydınlatma yükümlülüğü ile ilgilinin kişisel verilerinin akıbeti hakkında geniş bir şekilde bilgilendirilerek neye rıza gösterdiğini ya da göstermediğini bilmesine yardımcı olunmalıdır²⁷⁴.

Öte yandan veri sorumlusu İdare kişisel verileri ilgisinden elde edebileceği gibi 3. kişiler aracılığıyla da kişisel veri edinebilir. İşte bu durumlarda veri sorumlusunun aydınlatma yükümlülüğü devam etmekte ve bu yükümlülüğün en geç ne zaman yerine getirilmesi gerektiği sorusu önem kazanmaktadır. Tebliğin 6. maddesinde bu hususa yer verilmiştir. Buna göre “*Kişisel verilerin ilgili kişilerden elde edilmemesi halinde; a) Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, b) Kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, c) Kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada, ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerekir.*”

Kanunun 10. maddesinde aydınlatma yükümlülüğünün içermesi gereken asgari bilgilere yer verilmekle yetinilmiş, bu yükümlülüğün yerine getirilmesinde uyulacak usul ve esaslar ise Kurum tarafından çıkarılan Tebliğ’de düzenlenmiştir. Dolayısıyla, veri sorumlusu İdarenin bu yükümlülüğü yerine getirirken Tebliğ hükümlerine de uygun hareket etmesi gerekir.

Öncelikle kişisel veri ister açık rızaya dayalı olarak işlensin isterse Kanunun diğer veri işleme şartlarına dayanılsın, her durumda aydınlatma yükümlülüğünün yerine getirilmesi gereklidir (Tebliğ m.5/1/a). Ancak ifade edilmelidir ki eğer ilgili kişiden açık rıza beyanı da alınması gerekliyse aydınlatma yükümlülüğü ve açık rıza beyanının alınması işlemi ayrı ayrı yerine getirilmelidir (Tebliğ m.5/1/f)²⁷⁵. Yukarıda kişisel verilerin işlenmesine ilişkin genel ilkelerde değinildiği üzere kişisel verileri işleme amacı sonradan değiştirilebilir ancak veri işleme amacı değiştiğinde veri işleme faaliyetine geçmeden önce değişen veri işleme amacı için ilgili kişiye ayrı bir aydınlatma yapılması gerekir (Tebliğ

²⁷⁴ TANSUĞ, s.133.

²⁷⁵ “Online platformda iş başvurusunda bulunurken üyelik kaydı yapılmasının zorunlu olduğu, üyelik kaydı yapılması sırasında ise, aynı kutucuğun işaretlenmesi yoluyla hem aydınlatma metninin okunduğuna hem de kişisel verilerin işlenmesi hususunda açık rıza verildiğine ilişkin onay alınması yoluna gidildiği tespit edilmiştir. Söz konusu uygulamanın 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) amacına ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinin (1) numaralı fıkrasının (f) bendinde yer alan hükme uygun olmadığı, bu itibarla aydınlatma metninin okunduğuna ilişkin geri bildirim alınması ile ilgili kişilerin kişisel verilerinin işlenmesi hususunda gerekli seçimlik haklarının da tanındığı açık rıza metninin onaylandığının ispatını sağlayacak mekanizmaların ayrıştırılması hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.” KVK Kurulu, 26.7.2018 tarih ve 2018/90 sayılı kararı, <https://www.kvkkarar.com/2018-90/> (E.T. 25.8.2023).

m.5/1/b)²⁷⁶. Dolayısıyla ilgili kişiye veri işleme amacı açık ve belirli şekilde sunulmalı, muğlak ifadelerden kaçınılmalı ve “*gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır*” (Tebliğ m.5/1/g). Ayrıca aydınlatma yapılırken ilgili kişilere eksik, yanıltıcı ya da yanlış bilgiler verilmemelidir (Tebliğ m.5/1/j). Bu bağlamda aydınlatma açık, anlaşılır ve sade bir dil kullanılarak yerine getirilmelidir (Tebliğ m.5/1/ğ).

Öte yandan, aydınlatma yükümlülüğünün yerine getirilmesi ilgili kişinin talebine bağlı olmadığı gibi bu yükümlülüğünün yerine getirildiğinin ispatı da veri sorumlusuna aittir (Tebliğ m.5/1/d ve e). Tebliğ’in 5. maddesinin ilk fıkrasında aydınlatma yükümlülüğünün veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortamlar kullanılmak suretiyle yerine getirilebileceği düzenlenmiştir. Veri sorumlusu ispat yükünün kendisinde olduğu kuralını dikkate alarak kendisi için en uygun yöntemi tercih etmelidir²⁷⁷. Ancak, uygulamada genellikle uzun ve teknik terimlerle dolu aydınlatma metnlerinin hazırlandığı göze çarpmaktadır. Bu durumsa çoğu zaman ilgilinin aydınlatma metnini okumaktan imtina etmesine sebebiyet vermektedir. Bu sebeple, asıl metnin yanı sıra muhatabına göre bunların kısa özetlerinin de hazırlanarak en azından bu özetlerin okunması sağlanmalıdır. Ayrıca, özellikle telefon aracılığıyla yapılan bilgilendirmelerde katmanlı aydınlatma yapılarak ‘size daha iyi hizmet verebilmek amacıyla bazı kişisel verileriniz işlenmektedir’ denildikten sonra ayrıntılı bilgi için web sitelerine yönlendirildiği durumlarda, KVK Kurulu’na göre ilk aşamada veri sorumlusunun kimliği ve veri işleme amacı gibi temel bilgilerin verilmesi gerekmektedir²⁷⁸. Bu temel bilgiler arasında, işlenen bazı kişisel verilerin de zikredilmesi yerinde olacaktır. Böylece, ilgilinin dikkati cezbedilerek aydınlatma metninin tamamını okuması sağlanabilir.

Kanuna göre aydınlatma bildirimi içerisinde yer alması gereken bilgilerden biri de veri işleme faaliyetinin hukuki sebebidir (m.10/1/ç). İşte bu hukuki sebeplerse yine Kanunun 5. ve 6. maddelerinde sayılan kişisel verilerin işleme şartlarından ibarettir. Tebliğ’e göre, veri sorumlusu aydınlatma

²⁷⁶ 5. maddenin “c” fıkrasına göre eğer veri sorumlusunun farklı birimlerinde kişisel verilerin farklı amaçlarla işlenmesi söz konusu ise bu halde her bir birimde ayrı aydınlatma yapılması gerekir.

²⁷⁷ Kişisel Verileri Koruma Kurumu tarafından kamuoyunu bilgilendirme amacıyla hazırlanan “*Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*” adlı kitapçıkta veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmesi yöntemleri konusunda şu örneklerle yer verilmiştir: “*Bu yöntemlere örnek olarak; veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü (yüz yüze yapılan, şifahi aydınlatma gibi), yazılı (web sayfasında yer alan metin, bina girişinde duvara asılı levha, bir kameranın altında duvara monte edilmiş bilgi panosu gibi), ses kaydı (ilgili kişiye ses kaydı dinletilmesi gibi), çağrı merkezi (operatörle görüşmeden önce bir ses dosyası dinletilmesi) gibi fiziksel veya elektronik ortam (web sayfasında yer alan bir belgede katmanlı aydınlatma yapılması, açılan pencere [pop-up pencere] çıkması, mobil uygulamalar gibi) kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesi verilebilir. / Ayrıca, görme engellilerin söz konusu aydınlatmaya erişebilmesi için ilgili mevzuatta (5378 sayılı Engelliler Hakkında Kanun, Erişilebilirlik İzleme ve Denetleme Yönetmeliği vb.) öngörülen uygulamaların yapılması önem arz etmektedir.*” s.14, <https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi> (E.T. 23.08.2023).

²⁷⁸ KVK Kurulu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu**, 26.6.2020, <https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU> (E.T. 25.8.2023)

metninde “6698 sayılı Kanunun 5. ve 6. maddesinde belirlenen işleme şartlarına dayanılarak kişisel verileriniz işlenecektir” gibi belirsiz bilgilendirme geçerli olmayacaktır. Nitekim “Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir.” (Tebliğ m.5/1/h). Dolayısıyla veri işlemenin 5. ve 6. maddelerde düzenlenen hangi hukuki sebebe dayandırıldığı açıkça ifade edilmelidir²⁷⁹.

Son olarak, aydınlatma yükümlülüğü bildiriminde kişisel veriler 6698 sayılı Kanuna uygun şekilde aktarılacaksa verilerin aktarılma amacı ve aktarılacak kişiler ile tamamen veya kısmen otomatik yollarla ya da otomatik olmayan yollarla gibi veri işleme yöntemlerinden hangisinin kullanılacağı bilgilerine yer verilmesi gerekmektedir (Tebliğ m.5/1/ı ve i).

Yukarıda, kişisel verilerin açık rıza ile yahut diğer veri işleme şartlarına dayalı olarak işlenmesine bakılmaksızın her halde aydınlatma yükümlülüğünün yerine getirilmesi gerektiği ifade edilmiştir. Bununla birlikte, 6698 sayılı Kanunda aydınlatma yükümlülüğünün geçerli olmadığı, başka bir deyişle ilgili kişilere aydınlatma bildiriminin yapılmayacağı haller de düzenlenmiştir. Kanunun 28. maddesinin ilk fıkrasında belirtilen hallerde bu Kanun hükümlerinin uygulanmayacağı düzenlendiğinden bu durumlarda ilgililere aydınlatma bildirimi de yapılmayacaktır²⁸⁰. Yine 28.

²⁷⁹ “İhbara konu web adresi üzerinden erişim sağlanan “GİZLİLİK ve KVK Politikamız” başlıklı metin, söz konusu mevzuat düzenlemeleri çerçevesinde incelendiğinde; Web sitesinin ilgili kişiler hakkında işlediği ad, soyadı, doğum tarihi, cep telefonu numarası, e-posta, cinsiyet, adres, sosyal medya hesaplarıyla bağlanması durumunda üyenin o kanallar aracılığıyla paylaşılmasına onay verdiği bilgilerin, üyenin tüm alışveriş bilgilerinin, yani hangi üye işyeri, alışveriş noktası ve zamanı, ne kadar ödeme yaptığı, hangi kampanyadan faydalandığı, aldığı indirim tutarı, alışverişindeki ürün bilgileri, uygulama üzerindeki gezinme ve tıklama bilgilerinin, uygulamayı açtığı lokasyon bilgilerinin, “ilgili mevzuat”tan kaynaklanan yasal yükümlülük çerçevesinde mi yoksa ilgili kişilerin açık rızalarına istinaden mi işlendiğinin ya da söz konusu kişisel verilerin hangilerinin “ilgili mevzuat”tan kaynaklanan yasal yükümlülük çerçevesinde hangilerinin ise ilgili kişilerin açık rızalarına istinaden işlendiğinin açıkça belirtmemiş olduğu, İlgili kişilerin kişisel verilerin işlenmesinin hukuki sebebi olarak “ilgili mevzuattan kaynaklanan yasal yükümlülük”ten bahsedildikten sonra, aydınlatma metninin devamında, “... söz konusu amaç ve yasal yükümlülüklerini yerine getirebilmeyi sağlayacak kişisel verilerinizi ... sizlerden talep etmektedir. Bu kişisel veriler veri sorumlusunun sunmuş olduğu hizmetlerden yararlanabilmeniz adına, **açık rızanıza istinaden**, ... işlenecek ve saklanacaktır.” şeklinde bir bilgilendirmede bulunularak, kişisel veri işleme faaliyetinin asıl olarak ve yalnızca ilgili kişilerin açık rızalarına dayanarak gerçekleştirildiği izlenimine neden olunduğu, Oysa kişisel veri işleme faaliyetinin, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı; nitekim ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesinin hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına geleceği, dikkate alındığında, bahse konu web adresi üzerinden erişim sağlanan “GİZLİLİK ve KVK Politikamız” başlıklı metnin, “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”e uygun düzenlenmediği, bu kapsamda söz konusu metnin Tebliğde yer verilen hükümler dikkate alınmak suretiyle güncellenmesi, ayrıca aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği yönünde Şirketin talimatlandırılmasına karar verilmiştir.” KVK Kurulu 8.7.2019 tarih ve 2019/206 sayılı kararı. <https://www.kvkkarar.com/2019-206/> (E.T. 25.8.2023).

²⁸⁰ “**MADDE 28-** (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

- a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.
- b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

maddenin ikinci fıkrasına göre bu fıkarda düzenlenen hallerde, zikredilen diğer maddelerle birlikte aydınlatma yükümlülüğünün düzenlendiği Kanunun 10. maddesinin de uygulanmayacağı kabul edilmiştir²⁸¹.

4.4. Kanuni Gerekliliklere Uygun Veri İşlemenin Esasları

Anayasanın 20. maddesinin 3. fıkrasına göre kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla, Türk hukukunda kural olarak kişisel veriler işlenemez. Kişisel verilerin korunmasına ilişkin olarak çıkarılan 6698 sayılı Kanunda ise açık rıza verilmesinin yanı sıra diğer bazı şartların bulunması halinde kişisel verilerin işlenebileceği durumlar düzenlenmiştir. Kanunun 5 inci maddesinde genel nitelikli kişisel verilerin işlenmesine ilişkin şartlara yer verilmiş, 6 ncı maddesinde ise özel nitelikli kişisel verilerin işlenmesine ilişkin şartlar düzenlenmiştir.

4.4.1. Genel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Şartlar

6698 sayılı Kanunun 5. maddesinin ilk fıkrasında kişinin açık rızası olmaksızın kişisel verisinin işlenemeyeceği belirtildikten sonra, ikinci fıkrasında belirlenen yedi farklı durumdan birinin bulunması halinde ilgilinin açık rızası alınmaksızın kişisel verisinin işlenebileceği düzenlenmiştir. Buna göre, aşağıda sayılan hallerde ilgisinin açık rızası alınmaksızın kişisel verisi işlenebilecektir:

“a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.”

²⁸¹ “**MADDE 28-** (2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.”

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”²⁸²

Belirtmek gerekir ki, bu şartların varlığı halinde yalnızca açık rıza alınma zorunluluğu ortadan kalkmakta, kanunun diğer hükümleri geçerliliğini devam ettirmektedir. Bu bakımdan İdare diğer şartlardan birinin bulunması sebebiyle açık rıza almadan kişisel verileri işleyebilmesi halinde dahi özellikle, Kanunun 4. maddesinde sayılan veri işlemenin genel ilkelerine uygun şekilde işleme faaliyetini yerine getirmelidir.

Aşağıda öncelikle veri işlemenin genel şartı olan açık rıza alınması kuralının kapsam ve çerçevesine yer verilecek, ardından genel nitelikli verilerin işlenmesine ilişkin Kanunun 5. maddesinde yer verilen ve açık rıza şartını ortadan kaldıran durumlar anlatılacaktır.

4.4.1.1. Kişisel Verinin İşlenebilmesinin Genel Şartı Olarak “Açık Rıza”

Türk hukukunda kişisel verilerin işlenebilmesi için ilgili kişinin açık rızasının alınması şarttır. 6698 sayılı Kanunda özel nitelikli (hassas) veriler için de “açık rıza” alınması öngörülmüştür. Ayrıca, 8/1. madde ve 9/1. madde uyarınca kişisel verilerin üçüncü kişilere ya da yurt dışına aktarımı da ilgilinin açık rızası halinde mümkündür. Kanunun 3/1 maddesinin (a) bendinde açık rıza “belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlanmıştır.

Öte yandan, gerek 95/46 sayılı Direktif gerekse de Tüzük düzenlemelerinde genel nitelikli kişisel verinin işlenmesi bakımından ilgiliden “rıza” (consent) alınması yeterliyken, özel nitelikli veriler için “açık rıza” (explicit consent) alınması öngörülmüştür. 95/46 sayılı Direktif’te veri öznesinin rızası “kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rıza” şeklinde tanımlanmıştır²⁸³. Tüzükte ise “ilgili kişinin

²⁸² Genel nitelikli verilerin işlenmesi bağlamında 95/46 sayılı Direktif (7. madde) ile 2016/579 sayılı Tüzük (6. madde) düzenlemelerine bakıldığında hükümlerin birbirlerine benzer olduğu görülmektedir. Bununla birlikte, 6698 sayılı Kanunun 5. maddesinde yer verilen kişisel verilerin işleme şartlarının mehzaz Direktiften farklı birkaç şarta yer vermesi göze çarpmaktadır. Kanuna göre açık rıza alınmaksızın veri işlenebileceği öngörülen hallerden *kanunda açıkça öngörülmesi; verinin ilgilinin kendisince alenileştirilmesi ve bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması* halleri Direktifte yer almamıştır. Bu bakımdan, Kanunun Direktife göre daha geniş alanda veri işlemeye imkân tanıdığı, veri işleme imkânlarını genişlettiği söylenebilir.

²⁸³ Madde 2/(h): 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. İnsan Hakları Ortak Platformu tarafından yapılan çeviri için bkz.: <https://ihop.org.tr/kiisel-verilerin-ilenmesi-ve-serbest-dolamna-dair-ab-konseyi-ve-avrupa-parlamentosu-direktifi/> (E.T. 12.1.2022).

rızası”nın²⁸⁴ “*ilgili kişinin isteklerinin özgür, somut, bilgilendirmeye dayalı ve kesin olan her türlü göstergesini ifade eder ki kişi, bir ifade ya da olumlu eylem sayesinde kendisiyle ilgili kişisel verinin işlenmesini kabul ettiğini bu sayede belirtsin*”²⁸⁵ anlamına geldiği ifade edilmiştir.

Genel nitelikli kişisel verilerin işlenmesinde de açık rızanın varlığını arayan 6698 sayılı Kanunun mehzaz Direktif ile sonrasında çıkarılan Tüzükten daha ağır koşullar içerdiği söylenebilir. Peki rıza (consent) ile açık rıza (explicit consent) kavramları arasında nasıl bir fark bulunmaktadır? Tüzük’te açık rızaya ilişkin bir tanıma yer verilmemiştir. Elbette bu düzenlemelerde özel nitelikli veriler için nitelikli bir açık rıza aranıp da diğer kişisel veriler için basit bir rıza anlayışının benimsendiği söylenemez. İster rıza beyanı olsun isterse açık rıza beyanı olsun, her ikisi de ilgili kişinin belirli bir konuya ilişkin, bilgilendirilmeye dayalı ve farklı bir yoruma açık olmayacak şekilde ortaya koyduğu irade beyanı olmalıdır. Buradaki önemli nokta, “açık” rızanın daha net bir beyanla teyit edilmesi gerekliliğidir²⁸⁶. Açık rıza beyanı da sözlü ya da yazılı olabilir. İlgili kişinin aktif hareketinden verilerinin işlenmesine rıza gösterdiği yorumu yapılarak, rızanın diğer şartlarını sağlaması halinde, kabul edilebilir bir “rıza” (consent) beyanı elde edilebilir. Ancak, “açık rıza” açıkça ifade edilmelidir. Bir kişinin, şüpheyi yer bırakmayacak şekilde de olsa, örtülü rıza beyanı geçerli bir “açık rıza” beyanı olmayacaktır.

Örneğin, bir kamu kurumunda düzenlenen sosyal etkinlik devam ederken, görevli tarafından fotoğraf çekileceği ve bu fotoğrafların çeşitli mecralarda yayınlanacağı içeride bulunanlara duyurulduğunda, buna rağmen fotoğraf karesinde yer alan kişilerin, kişisel verilerinin bu şekilde işlenmesine “rıza” gösterdiği kabul edilmelidir. Elbette, bu örnekte fotoğrafların sadece duyuruda belirtilen amaçla sınırlı olarak işlenmesi faaliyetine verilen bir rıza söz konusudur. Öte yandan, aynı örnekte ilgililerden “açık rıza” alınması gerekiyorsa, 6698 sayılı Kanunda olduğu gibi, kişilerden “Etkinlik boyunca çekilen fotoğrafların belirtilen amaçlar kapsamında (bu amaçlar açıkça gösterilmelidir) işlenmesine rıza gösteriyorum” şeklinde bir metnin altına imza atması istenebilir. Yahut bu cümlemin yanına konulacak bir onay kutucuğunu işaretlemesi de yeterli olacaktır. Açık rızanın yazılı olma şartı bulunmamakla birlikte, rıza gösterildiğini kanıtlama yükümlülüğünün veri sorumlusu üzerinde olduğu düşünüldüğünde, yazılı şekilde beyan alınması hem şüpheyi hem de ileride ortaya çıkabilecek aksaklıkları ortadan kaldıracak bir yöntem olacaktır. Ayrıca, söz gelimi sosyal etkinlik davetiyesinde “Etkinliğe katılanların etkinlik boyunca çekilecek fotoğraflarının sosyal medyada paylaşılmasına rıza göstereceği kabul edilecektir.” gibi bir ibareye yer verilmesi üzerine katılımcıların

²⁸⁴ Madde 4/11: ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

²⁸⁵ ÇEKİN, s.83-84.

²⁸⁶ The UK’s Information Commissioner’s Office (ICO), “What is explicit consent?”, **Guide to the GDPR**, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/> (E.T. 17.1.2022).

bu veri işleme faaliyetine “rıza” gösterdiği kabul edilebilirse de “açık rıza” beyanında bulundukları söylenemez.

“Başka bir yoruma yer bırakmayacak” ya da “şüpheye yer bırakmayacak” (unambiguous) şekilde rıza beyanında bulunulabilmesi, örtülü rıza beyanında bulunulabileceği sonucunu doğurmakla birlikte, sırf hareketsiz kalmak ya da sessiz kalmak tek başına rıza gösterildiği anlamına gelmemektedir. Rıza beyanı aktif bir hareket içermelidir. Öyle ki ilgili kişi, kasıtlı olarak, aktif şekilde rıza göstermeyi tercih etmelidir²⁸⁷.

6698 sayılı Kanunda her türlü kişisel verinin işlenmesi için açık rızanın aranmış olması nedeniyle yukarıda yer verilen farklılıklar bakımından Kanunun daha ağır koşullar barındırdığı söylenebilir. Bu durumun bir tür “rıza yorgunluğuna” sebep olacağı, her türlü veri işleme için ilgisinden açık rıza talep edilmesi halinde ilgililerin genel nitelikli veri- hassas veri ayrımı yapmaksızın açık rıza vermekten kaçınabileceği ya da açık rızaya ilişkin metni okumaksızın buna onay verebileceği eleştirisi yapılmaktadır²⁸⁸. Bu eleştirinin çok da haksız olmadığını ifade etmek gerekir. Buna ek olarak, her türlü veri işleme faaliyeti için gerektiğinde alınacak rızanın “açık rıza” beyanı olması bazı durumlarda ek iş yükü ve prosedür anlamına da gelecektir. Ayrıca internet ortamında önüne gelen sayfadaki metni okumaksızın “Okudum, onayladım.” seçeneğini aktifleştirerek istenilen sayfaya erişimi bir an önce sağlama alışkanlığı üzerine kişisel verilerin işlenmesi konusundaki farkındalığın az olması eklendiğinde her türlü veri için açık rıza alınmasının verimli bir yöntem olmadığı söylenebilir. Bu bakımdan Avrupa Birliği düzenlemelerinde olduğu gibi basit kişisel verilerin işlenmesinde açık rıza yerine sadece “rıza” verilmesinin aranması ve böylece örtülü rıza beyanının da yeterli kabul edilmesi yöntemi benimsenmelidir²⁸⁹. Ancak mevcut kanuni düzenlemenin buna imkân vermediği açıktır. Nitekim, Kurul tarafından verilen bir kararda zımni irade beyanı ile açık rıza alınmasının mevzuata uygun olmadığı ifade edilmiştir²⁹⁰.

Kanunda açık rıza beyanı alınması herhangi bir şekil şartına tabi tutulmadığından, elektronik ortamlar dahil, yazılı ya da sözlü şekilde veya internet ortamında kişinin önüne gelen ve belirtildiği

²⁸⁷ The UK’s Information Commissioner’s Office (ICO), “What is an unambiguous indication (by statement or clear affirmative action)?”, **Guide to the GDPR**, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/> (E.T. 17.1.2022).

²⁸⁸ ÇEKİN, s.85.

²⁸⁹ Ayrıntılı bilgi için bkz.: BAŞALP, Nilgün, **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayınları, 2004, s.24; KÜZECİ, **Kişisel Verilerin Korunması**, s.232 vd.; BAŞAR, s. 46, vd.

²⁹⁰ “Veri sorumlusundan alınan yazıda hali hazırda mevzuata uygun olarak yurtdışına veri aktarım faaliyeti yapıldığı belirtilmiş olsa da “Amazon Hesabınızı Oluşturun” sekmesine tıklayarak “Gizlilik Bildirimi”nin de kabul edildiği (“Hesap oluşturularak işbu Gizlilik Bildirimi’nde belirtilen uygulamaları kabul etmekteyiz.”); aynı şekilde kayıtlı bir müşteri, site üzerinden sipariş verdiğinde kendisine “Gizlilik Bildirimi”nin kabul edildiğine dair tekrar hatırlatma yapıldığı (“Sipariş verdiğinizde Amazon.com.tr’nin Gizlilik Bildirimini, Kullanım ve Satış Koşullarını ve Çerez Bildirimini kabul etmiş olursunuz”) belirtilerek ilgili kişilerin rızasının alındığı veri sorumlusunca iddia edilmekle birlikte, zımni irade beyanı ile onay alınmasının mevzuata uygun kabul edilemeyeceği değerlendirilmektedir. Kanun çerçevesinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır.” KVK Kurulu, 27.2.2020 tarih ve 2020/173 sayılı kararı: <https://www.kvkk.gov.tr/Icerik/6739/2020-173> (E.T. 12.1.2022).

şekilde kişisel verilerinin işlenmesine onay verdiğini gösteren kutucuğu işaretlemesiyle açık rızanın alınması mümkündür²⁹¹. Öte yandan, otomatik olarak kutunun işaretlenmiş olduğu ya da kişisel verinin işlenmemesi için aktif bir hareketi gerektiren durumlarda kişinin açık rızasının alındığı kabul edilmemektedir²⁹².

6698 sayılı Kanunun tanımında açık rızanın “belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle” yapılan bir irade beyanı şeklinde ifade edilmesi karşısında, açık rıza kavramının belirli bir konuya ilişkin olma, bilgilendirmeye dayanma ve özgür iradeyle açıklanma gibi üç unsurdan oluştuğu söylenebilir.

Açık rızanın **belirli bir konuya ilişkin olarak verilmesi**, konusu sınırlandırılmış bir veri işleme faaliyeti için rıza talebinde bulunulmasını ifade etmektedir. “Her türlü veri işleme faaliyeti” gibi bir ifadeyle sınırları belirlenmemiş veri işleme faaliyetleri için alınacak genel nitelikteki rıza “battaniye rıza” olarak kabul edilmekte ve geçersiz sayılmaktadır²⁹³. Örneğin, bir medya şirketi tarafından yapılan ankette “Firmalardan ürünler hakkında bilgi ve tanıtımlarını SMS yoluyla almak ister misiniz?” şeklindeki sorunun belli bir şirketi işaret eder şekilde olmadığı için, konusu sınırlanmamış, genel nitelikte bir soru olduğu ve anket kapsamında kişilerden alınan “evet” cevabının açık rıza olarak değerlendirilemeyeceği ifade edilmiştir²⁹⁴. Ayrıca amaçları birbirinden farklı birden fazla kişisel veri işleme faaliyetinin bulunduğu durumlarda da “belirli bir konu” bulunmadığından, birden fazla veri işleme faaliyeti için alınacak tek bir açık rıza beyanının geçerli olmayacağı kabul edilmelidir. Örneğin, tanıtım, reklam, satış ve pazarlama amaçlarıyla ad soyad ve telefon numaralarının işlenmesi ile birlikte özel nitelikli kişisel verilerin iş gereği ve sağlık hizmeti verilebilmesi ve bu hizmetlerin planlaması amacıyla işlenmesi faaliyetlerine tek bir metin ile açık rıza talep edilmesi halinde verilen rıza beyanı geçerli olmayacaktır²⁹⁵. Bunun yerine reklam, pazarlama, tanıtım amacıyla işlenecek basit kişisel veriler için ayrı; özel nitelikli kişisel verilerin işlenmesi için ayrı şekilde açık rıza alınmalıdır.

Açık rıza beyanının belirli bir konuya ilişkin olarak verilmesi hususuna AİHM’nin şu kararı örnek olarak verilebilir²⁹⁶. Rusya’da bir belediyenin Psikolojik, Tıbbi ve Sosyal Hizmetler Merkezi tarafından hazırlanan bir kitapçığın kapağında başvuranın küçük çocuğunun fotoğrafı yayımlanmıştır. “Çocukların bir aileye ihtiyacı var” başlıklı kitapçık, Merkez’in hem yetimleri koruma hem de evlat edinmek isteyen ailelere yardımcı olma rolü hakkında bilgilendirme amacını taşımaktadır. Bir okulda öğretmenlik yapan

²⁹¹ Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar – 2 Kitapçığı**, s. 22.

²⁹² Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar – 2 Kitapçığı**, s. 19.

²⁹³ Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar – 2 Kitapçığı**, s. 15.

²⁹⁴ KVK Kurulu, 11.3.2021 tarih ve 2021/227 sayılı kararı: <https://www.kvkk.gov.tr/Icerik/7115/2021-227> (E.T. 12.1.2022).

²⁹⁵ Söz konusu örneğe, arama motorunda çıkan sonuçlardan birinde rastlanılmıştır. Bu metin bir eğitim kurumuna ait açık rıza metnidir.

²⁹⁶ AİHM, Bogomolova / Rusya, B.n. 13812/09, T. 20.6.2017, <https://hudoc.echr.coe.int/?i=001-174420>.

başvuran, fotoğrafın kullanılmasının oğlunu terk ettiği izlenimi verdiği, bu durumun bir anne ve bir öğretmen olarak itibarını zedelediği iddiasıyla tazminat talebinde bulunmuştur. Ancak yerel mahkemeler, fotoğrafın çekilmesine başvuranın onay verdiği gerekçesiyle talebi reddetmiştir. AİHM, konuya ilişkin verdiği kararında, bir kişinin imajının kişisel özelliklerinden biri olması nedeniyle AİHS'nin 8. maddesi bağlamında fotoğrafın yayınlanmasını reddetme hakkı dahil olmak üzere, fotoğrafının kullanımını kontrol etme hakkının kendisinde olduğunu, bu nedenle çocuğun özel hayat hakkının ihlal edildiğini, yerel mahkemelerce fotoğrafın çekilmesinde başvuranın onayının bulunması gerekçe olarak gösterilmesine karşın, ilgili fotoğrafın yayımlanmasına ilişkin rızasının olup olmadığının araştırılmadığını, ayrıca fotoğrafın böyle bir derginin baş sayfasında yayımlanmasının çocuğun yetim olduğu, asıl ailesinin ona sahip çıkmadığı, mevcut ailesinin ise koruyucu aile olduğu izlenimini yaratabileceğini ifade ederek ihlal kararı vermiştir. Buradan hareketle, kişinin bir fotoğrafın çekilmesine ses çıkarmaması yeterli olmayıp, ilgilinin fotoğrafın hangi amaçla kullanılacağına ilişkin bilgilendirilmesi ve bu amaca uygun olarak işlenmesine rıza göstermesi gerektiği ifade edilmelidir.

İlgilinin açık rızasını konuya ilişkin **yeterli bilgilendirme** yapıldıktan sonra vermesinin gerekli olması, açık rızanın veri işlenmeye başlamadan önce alınmasını zorunlu kılar. Dolayısıyla, sonradan alınacak rıza beyanı veri işleme faaliyetini hukuka uygun hale getirmeyecektir. Bununla birlikte bilgilendirmenin, yani açık rıza metninin içeriğine ilişkin mevzuatımızda herhangi bir düzenleme yer almamaktadır. Kanun gerekçesinde kişinin konuyla ilgili yeterli bilgi sahibi olması gerektiği ifade edilmiştir. Tüzüğün 7. maddesinin 2. fıkrasında ise veri sahibinin rızasının başka hususları da içeren yazılı bir beyan ile verilmiş olması durumunda, muvafakat talebinin diğer hususlardan açıkça ayırt edilebilir şekilde, anlaşılır ve kolay erişilebilir bir biçimde, açık ve sade ifadeler kullanılarak sunulması gerektiği ifade edilmiştir.

Madde 29 Çalışma Grubunun (The Working Party) hazırladığı kılavuzda açık rıza metninin içeriğine ilişkin önerilere yer verilmiştir. Buna göre açık rıza metninde,

- i. veri sorumlusunun kimliği,
- ii. rızası talep edilen her bir işleme faaliyetinin amacı,
- iii. ne çeşit kişisel verinin toplanacağı ve kullanılacağı,
- iv. rızanın geri alınabileceği,
- v. verinin otomatik karar verme sistemleriyle işlenmesi söz konusu ise bu konu hakkında, ve
- vi. (yeterli düzeyde veri güvenliğine sahip ülkeler hakkında verilen) yeterlilik kararı (adequacy decision) ve uygun garantilerin bulunmadığı durumlarda yurt dışına aktarılan verilere dair riskler hakkında

ilgili kişiye bilgi verilmesi gerekir²⁹⁷. Bununla birlikte, sayılan hususlar hakkında verilecek bilgilerin Tüzüğün 7/2. maddesinde ifade edildiği gibi, açıkça anlaşılır ve sade ifadeler kullanılarak verilmesi gerektiği düşünüldüğünde, açık rıza metninin uzunca yazılmış, dikkat dağıtıcı ve muhatabına uygun olmayan bir dille kaleme alınmaması önemlidir. Çünkü ilgili kişinin ne için açıkça rıza beyanında bulunduğunu bilmesi o beyanın geçerli olmasını sağlamaktadır.

AB mevzuatında kabul edildiği gibi açık rıza beyanının yalnızca özel nitelikli veriler için aranmasının daha yararlı bir yöntem olduğu ancak Türk hukukunda bunun geçerli olmadığı yukarıda ifade edilmiştir. Bu bağlamda, özellikle hassas nitelikli verilerin işlenmesine ilişkin açık rıza beyanının alınması konusunda ilgilinin açık rıza metnini okumasını teşvik edecek yöntemlere başvurulması gerektiği değerlendirilmektedir. Örneğin, yüz yüze olunan ortamlarda ilgilinin rıza metnini okumasını sağlamak için söz konusu işleme devam edilmesine kısa bir ara verilmesi ve kişiden imzasının üzerine “Yukarıda açıklanan şartlar altında kişisel verilerimin işlenmesine rıza gösteriyorum” şeklindeki bir cümleyi el yazısıyla yazması istenebilir. Öte yandan, çevrimiçi olarak alınan açık rıza beyanları için açık rıza metni penceresinin otomatik olarak açılması ve makul bir süre (15-20 saniye kadar) sayfanın kapatılmaması yöntemleri kullanılabilir. Telefonda ise kişiye en azından hangi verilerinin işleneceği açıkça belirtilerek ilgilide açık rıza metnini okuması yönünde bir ilgi uyandırması sağlanmalıdır.

Son olarak, ilgili kişinin açık rıza beyanı **özgür iradesinin bir ürünü** olmalıdır. Kişinin iradesini sakatlayan cebir, tehdit, hata ve hile hallerinin bulunması durumunda kişinin ortaya koyduğu açık rıza geçerli kabul edilmeyecektir. Ayrıca, açık rızanın verilmediği hallerde olumsuz sonuçların doğması ihtimali varsa, örneğin hizmetin sunumu için kişisel veri işlenmesinin mecburiyeti bulunmadığı halde hizmetin sunumu açık rızaya bağlanmışsa bu halde verilen rıza geçerli olmayacaktır.

Belirtmek gerekir ki, özellikle taraflar arasında güç dengesinin bulunmadığı durumlarda, örneğin veri sorumlusu ile ilgili kişi arasında kamu kurumu – vatandaş ya da işveren – işçi ilişkisi bulunması hallerinde kişisel verinin işlenmesi için verilen açık rızanın özgür iradeye dayanıp dayanmadığı daha dikkatli incelenmeli ve somut olaya göre karar verilmelidir. Tüzüğün 43 numaralı gerekçe kısmında, ilgili kişi ile veri sorumlusu arasında açık bir güç dengesizliğinin bulunduğu durumlarda, özellikle veri sorumlusunun kamu kurumu olduğu hallerde, veri işleme için alınan rızanın her zaman geçerli bir hukuka uygunluk sebebi olarak kabul edilmemesi gerektiği ifade edilmiştir.

Örneğin, bir kamu binasında giriş çıkışların ve ortak alanların güvenlik amacıyla kamerayla izlenmesinin dışında kamu görevlilerinin çalışma masalarını görebilecek şekilde, görevlinin diğer insanlarla olan iletişimlerini sesli ve sürekli kayıt altına alan bir kamera sistemiyle izlenmesinin kamu görevlilerinden alınan açık rıza beyanına dayandırılması durumunda, alınan açık rıza beyanlarının özgür

²⁹⁷ Article 29 Working Party, **Guidelines on consent under Regulation 2016/679**, 10.4.2018, s. 13, <https://ec.europa.eu/newsroom/article29/items/topic/6936> (E.T. 15.1.2022).

iradeyle verildiği iddiasına şüpheyile yaklaşılmalıdır. Nitekim, kişisel alanlarına ve mahremiyetlerine müdahalede bulunulmasına kamu dairesinde çalışan herkesin istisnasız rıza göstermesi düşük bir olasılıktır. Öte yandan, kamera sistemiyle masalarının izlenmesini istemeyen görevliler için gözetlemenin yapılmadığı ve diğer çalışma alanlarından fiziksel olarak herhangi bir farklılık taşımayan başka alanlarda çalışma imkânı getirilmiş olması, rıza göstermeyenler için hiçbir negatif ayrımcılığın yapılmayacağının garanti edilmiş olması durumunda açık rızanın özgür iradeyle verilmiş olduğu kabul edilebilir.

Başka bir örnekte, belediyenin düzenlemiş olduğu yardım kampanyasına katkıda bulunan kişilerden, yapılan yardımlar hakkında genel bilgilendirme maili gönderilmek üzere e-posta adreslerinin işlenmesi amacıyla açık rıza beyanının istenmesi durumunda ilgili kişinin rızasını özgür iradeyle verdiği kabul edilebilir. Ancak burada, bağışta bulunmak için e-posta adresinin işlenmesine açık rıza vermek zorunda olmadığı ve yardımlar konusunda belediyenin web sitesinden de bilgi edinilebileceği konusu kişiye açıkça anlatılmalıdır.

Bir eğitim kurumunca düzenlenen sosyal etkinliğe dair kurumun web sitesinde yayımlanacak fotoğraflarda yer alan ilgililerden istenen açık rızanın özgür iradeyle verildiğinin kabulü için, öğretmen, çalışan ya da öğrencinin rıza vermemesi halinde söz gelimi eğitim kurumunca düzenlenen diğer etkinliklere katılamama, işten çıkarılma, ders notunun düşürülmesi gibi hiçbir olumsuz durum yaşamayacağı garanti edilmelidir. Aksi halde alınan rızanın özgür iradeye dayandığını söylemek mümkün olmayacaktır²⁹⁸.

Öte yandan, geçerli bir açık rıza beyanının ilgisince her zaman geri alınabileceği kabul edilmektedir. Rızanın geri alınması Kanunda düzenlenmemiş olmakla birlikte özgür iradenin bir sonucu olduğundan geri alınabilecektir²⁹⁹. Bununla birlikte, açık rızanın geri alınması ileriye yönelik sonuç doğuracağından geçmişte gerçekleştirilen veri işleme faaliyetinin hukuka uygunluğunu etkilemeyecektir. Ancak, açık rızanın geri alınmasından itibaren devam eden veri işleme faaliyetine son verilmesi gerekir.

Örneğin, ilgili kişinin fotoğrafının açık rızası olmadan öğrencisi bulunduğu okul tarafından internet sitesinde yayımlanmak ve broşürde kullanılmak suretiyle işlenmesi üzerine yapılan şikâyetle ilişkin olarak Kurul, ilgili kişinin velisi tarafından daha önce açık rıza beyanında bulunulduğunu tespit etmiş, öğrencinin ilgili kurumdan ayrılmasından sonra fotoğrafın kullanılmasının şikâyet edilmesini açık rızanın geri alınması olarak değerlendirmiştir. Bu sebeple, eğitim kurumundan şikâyet konusu

²⁹⁸ Article 29 Working Party, **Guidelines on consent under Regulation 2016/679**, 10.4.2018, s. 7.

²⁹⁹ Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar – 2 Kitapçığı**, s. 17.

fotoğraftaki ilgili kişi görüntüsünün fotoğraftan ayrılabilir olup olmadığının değerlendirilerek ilgili kişi görüntüsünün buzlanması ya da görüntünün imha edilmesi istenmiştir³⁰⁰.

- Çocukun Kişisel Verilerinin İşlenmesine Yönelik Rızası

Açık rızanın kabul edilebilmesi için rıza gösterinin iradesinin hukuki olarak kabul görmesi de gerekir. Başka bir anlatımla, kişi iradesini ortaya koyabilecek bir ehliyete sahip olmalıdır. Bu durum da özellikle çocukların gösterdiği açık rızanın kabul edilebilirliği hususu önem kazanmaktadır. 6698 sayılı Kanunda çocuklara ait kişisel verilerin işlenmesine yönelik bir düzenlemeye yer verilmemiştir. Bununla birlikte, kişisel verilerin korunması bakımından ilgili kişiyi “kişisel verisi işlenen gerçek kişi” şeklinde tanımlayan hükümden hareketle elbette çocukların Kanunun koruma kapsamı dışında kaldığı söylenemez. Öte yandan, veri işleyebilmek için gereken “açık rızanın” çocuklar tarafından beyan edilmesi halinde bu beyanın hukuki geçerliliğinin incelenmesi de gerekir.

6698 sayılı Kanunda çocukların rıza beyanında bulunup bulunamayacağına ilişkin bir hüküm bulunmadığı gibi 95/46 sayılı Direktifte de buna ilişkin bir düzenlemeye yer verilmemiştir. Öte yandan, Tüzükte çocukların rıza beyanına ilişkin bir hükme yer verilmiştir. 8. maddeye göre, kişisel verilerin işlenmesinin açık rızaya dayalı olduğu durumda, “bilgi toplumu hizmetlerinin” çocuğa doğrudan sunulduğu hallerde, verilen rızanın geçerli kabul edilebilmesi için çocuğun 16 yaşından büyük olması gerekmektedir. 16 yaşından küçük olması halinde çocuğun velisi ya da vasisinin veri işlenmesine rıza göstermesi aranmaktadır. Tüzükte, 16 yaş sınırının üye devletlerde değişiklik gösterebileceği ancak bu belirlemenin 13 yaşın altında olamayacağı belirtilmiştir. Söz konusu kural, bilgi toplumu hizmetlerinin³⁰¹ çocuğa doğrudan sunulduğu ve veri işlemenin rızaya dayalı olduğu hallerde uygulanacaktır. Tüzükte, çocukların riskleri, sonuçları ve güvenceleri ile kişisel verilerin işlenmesine ilişkin hakları konusunda daha az farkındalık içerisinde olduklarından dolayı böyle bir koruma sağlanması gerektiği ifade edilmiş, öte yandan, çocuğa sunulan önleyici veya bilgilendirici hizmetler söz konusu olduğunda veli ya da vasisinin rızasının aranmasının gerekli olmadığı belirtilmiştir³⁰².

³⁰⁰ KVK Kurulu, 9.6.2021 tarih ve 2021/572 sayılı kararı: <https://www.kvkk.gov.tr/Icerik/7118/2021-572> (E.T. 14.1.2022).

³⁰¹ Bilgi toplumu hizmetleri (information society services), Tüzükte, “normalde ücret karşılığı, uzaktan, elektronik araçlarla ve hizmet alıcısının bireysel talebi üzerine sağlanan herhangi bir hizmet” şeklinde tanımlanmıştır. Bu tanımda geçen “uzaktan” kelimesi hizmetin taraflar aynı anda mevcut olmadan sağlanması; “elektronik araçlarla” ifadesi hizmetin, verilerin işlenmesi (dijital sıkıştırma dahil) ve depolanması amacıyla ve tamamen kablo, radyo, optik veya diğer elektromanyetik ekipmanlarla iletilmesi ve hedefinde alınması; “hizmet alıcısının bireysel talebi üzerine” ifadesi ise hizmetin bireysel talep üzerine verilerin iletilmesi yoluyla sağlanması anlamlarına gelmektedir (Avrupa Birliği, 2015/1535 sayılı Direktifi, madde 1/1(b)). Bu tanıma göre, çoğu çevrimiçi hizmet “bilgi toplumu hizmeti” olarak kabul edilebilecektir. Örneğin, son kullanıcıya ücretsiz olarak sunulan ancak reklamlar aracılığıyla finansa edilen çevrimiçi oyun uygulaması veya arama motoru bunlardandır. Ayrıntılı açıklama için bkz.: The UK’s Information Commissioner’s Office (ICO), “What are the rules about an ISS and consent?”, **Guide to the GDPR**, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/> (E.T. 20.1.2022).

³⁰² GDPR, 38 no’lu gerekçe.

6698 sayılı KVKK’da konuya ilişkin bir hüküm yer almadığından, çocuğun rızasının geçerliliğine ilişkin olarak hukuki işlem yapma ehliyetinin düzenlendiği Türk Medeni Kanunu’na bakmamız gerekir. 4721 sayılı Türk Medeni Kanunu’na göre, kişi kendi eylemleriyle hak edinebilmesi ve borç altına girebilmesi için fiil ehliyetine sahip olmalıdır (md.9). Başka bir deyişle, “*fiil ehliyeti, kişinin, kendi fiiliyle borç altına girebilme ve haklar kazanabilme yeteneğidir.*”³⁰³.

Kişilerin sahip olduğu fiil ehliyeti çeşitli ayrımlara tabidir. Ayırt etme gücüne sahip, kısıtlı olmayan ve erginliğe erişmiş kişinin tam fiil ehliyeti bulunduğu kabul edilir. Buna göre bu kişinin yukarıda ifade edilen şartlara uygun şekilde göstereceği rıza beyanı geçerli bir beyan olacaktır. Ancak, ayırt etme gücüne sahip olmakla birlikte ergin olmayanlar ve kısıtlılar sınırlı ehliyetsiz olarak kabul edilmektedir. Bu kişilerde ehliyetsizlik asıldır, istisnai olarak Kanunda sayılan bazı hallerde ehliyetli oldukları kabul edilir³⁰⁴. TMK’nın 16. maddesine göre, sınırlı ehliyetsizlerin yasal temsilcilerinin rızası olmadıkça, kendi işlemleriyle borç altına girmesi mümkün değildir. Bununla birlikte, karşılıksız kazanma ve kişiye sıkı sıkıya bağlı hakları kullanmada bu rıza aranmaz. Kişiye sıkı sıkıya bağlı haklar, hak sahibinin kişiliğini yakından ilgilendirdiğinden, bunların bizzat hak sahiplerince kullanılması gerekir. Ayrıca bu hakların devredilemez ve miras bırakılamaz haklardan olduğu kabul edilmektedir³⁰⁵. Sınırlı ehliyetsizler, kişiye sıkı sıkıya bağlı haklara ilişkin işlemler yaparken kanuni temsilcilerinin iznini veya onayını almak zorunda değildir³⁰⁶. Ancak, kanunda bazı istisnalar öngörülmüştür. Buna göre, ergin kılınma, nişanlanma, evlenme ve evlat edinilmede ayırt etme gücüne sahip küçüğün kanuni temsilcisinin izni gereklidir³⁰⁷.

Kişisel verilerin korunması hakkına, Anayasamızda “özel hayatın gizliliği” hakkının düzenlendiği 20. maddede, ayrı bir fıkra olarak yer verilmiştir. Benzer şekilde AİHM, kişisel verilerin korunmasını AİHS’nin 8. maddesinde düzenlenen özel hayatın gizliliği hakkı içerisinde incelemektedir. Dolayısıyla, özellikle Amerikan Hukukunda mülkiyet hakkı bağlamında incelenirse de Avrupa Hukukunda ve Türk Hukukunda kişisel verilerin korunması hakkı³⁰⁸ bir kişilik hakkı olarak kabul edilmektedir. Bu bağlamda “*kişisel verilerin işlenmesine rıza gösterme hakkı*”nın da kişilik hakkı bağlamında kişiye sıkı sıkıya bağlı haklardan biri olduğu söylenebilir³⁰⁹.

TMK’nun 16. maddesinden hareketle, ayırt etme gücüne sahip küçüğün kendisine sıkı sıkıya bağlı haklarını kullanırken kanuni temsilcisinin iznine ihtiyacının olmadığı, bu sebeple, kişisel verilerin işlenmesine rıza gösteren ayırt etme gücüne sahip küçüğün rızasının hukuken geçerli bir rıza olarak

³⁰³ ANTALYA/TOPUZ, s.210.

³⁰⁴ ANTALYA/TOPUZ, s.216.

³⁰⁵ AYAN/AYAN, **Medeni Hukuka Giriş**, Seçkin Yayıncılık, 12. Baskı, 2016, s.109 vd.

³⁰⁶ AYAN/AYAN, **Kişiler Hukuku**, s.69.

³⁰⁷ Türk Medeni Kanunu, m.12, m.118/2, m.126 ve m.309.

³⁰⁸ Kişisel verinin hukuki niteliği hakkında bilgi için bkz.: “**4. Kişisel Verinin Hukuki Niteliğine İlişkin Yaklaşımlar**” başlığı.

³⁰⁹ Hüseyin Can AKSOY, “Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu”, **Haluk Konuralp Anısına Armağan**, Cilt 3, Yetkin Yayınları, Ankara 2009, s. 57; ÖZKAN, s.100.

kabul edilmesi gerektiği söylenebilir. Nitekim kanunda nişanlanma, evlenme ya da evlat edinmede olduğu gibi aksi yönde bir düzenleme mevcut değildir³¹⁰. Bununla birlikte, küçüğün ayırt etme gücünün varlığı konusunda her somut olaya göre ayrı değerlendirme yapılmalı, kişisel verilerinin işlenmesine gösterdiği rızanın hukuki sonuçlarını öngörüp öngöremediği dikkatle irdelenmelidir³¹¹.

Öte yandan, akla uygun şekilde hareket etme kabiliyetine, hareketlerinin sebep ve sonuçlarını anlayabilme kapasitesine sahip olmayanlar, başka bir deyişle ayırt etme gücü bulunmayanlar tam ehliyetsiz olarak kabul edilmektedir³¹². Yaş küçüklüğünün ayırt etme gücünü etkilediği söylenebilirse de Türk Medeni Kanunu'nda belirli bir yaştan altında olan küçüklerin ayırt etme gücüne sahip olmadığına yönelik bir kurala yer verilmemiştir. Dolayısıyla, küçüğün tam ehliyetsiz olup olmadığı somut olay bazında incelenmesi gerekir. Kişisel verilerinin işlenmesi halinde doğabilecek sonuçları öngöremeyen, bu işleme faaliyeti karşısında fayda ve zarar dengesini kuramayan küçüğün söz konusu veri işleme faaliyeti bakımından ayırt etme gücünün bulunmadığı söylenebilir³¹³. Peki böyle bir durumda nasıl hareket edilmelidir?

Yukarıda, kişisel verilerin kullanılmasına rıza gösterme hakkının kişiye sıkı sıkıya bağlı haklardan olduğunu ifade etmiştik. Kişiye sıkı sıkıya bağlı haklar, hak sahibinin kişiliğini yakından ilgilendirdiğinden bizzat kendilerince kullanılması gerekir. Ancak ayırt etme gücü bulunmayanlar bu haklarını da kullanamayacaklarından bazı hallerde kişilerin tamamen korunmasız kalacağı durumlar ortaya çıkabilir. Bu sebeple, öğretide yasal temsilcilerin tam ehliyetsizler adına bazı kişiye sıkı sıkıya bağlı haklarını kullanabilmeleri gerektiği ifade edilmiştir³¹⁴. Buna göre, evlenme, boşanma ve soy bağının reddi gibi hakların mutlak kişiye sıkı sıkıya bağlı haklar olarak kabul edilmesi ve yasal temsilcilerin tam ehliyetsizler adına bu hakları kullanamaması gerektiği; öte yandan, kişiliğin korunmasına ilişkin dava açma ve ergin kılınma gibi haklarınsa nisbi kişiye sıkı sıkıya bağlı haklar olduğu ve tam ehliyetsizler adına yasal temsilcilerinin bu hakları kullanabileceği kabul edilmektedir³¹⁵.

Konuya bu açıdan yaklaşıldığında, kişilik hakkına yapılan saldırı karşısında dava açma hakkını kullanabilen yasal temsilcinin, tam ehliyetsiz kişinin kişisel verileri işlenmesi halinde kişilik hakkına zarar gelip gelmeyeceğini değerlendirerek bu konuda açık rıza verme yetkisine de evleviyetle sahip

³¹⁰ Kanunda belirlenen sınırlamaların, sınırlı ehliyetsizlerin korunması amacıyla getirildiği, kişisel verilerin işlenmesi halinde de sınırlı ehliyetsizlerin zarar görme ihtimallerinin bulunduğu, Kanunda “kişisel verilerin işlenmesine rıza gösterilmesi” hususunda sınırlı ehliyetsizler için bir düzenleme bulunmaması da bunun bir “örtülü boşluk” olarak kabul edilmesi ve sınırlı ehliyetsizlerin kişisel verilerinin işlenmesinden önce kanuni temsilcilerin izinlerinin alınması gerektiği yönünde görüş için bkz.: AKSOY, s.57 vd.

³¹¹ ÇEKİN, s.100.

³¹² Başka bir tanıma göre ayırt etme gücü “kişinin iyiyi kötünden, doğruyu yanlıştan ayırabilmesi için yeterli ruhi olgunluğa erişmesi”dir: ERDOĞAN/KESKİN, s.234.

³¹³ Murat UÇAK, “Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası”. **Kişisel Verileri Koruma Dergisi**, 2021, S.3, s.57. <https://dergipark.org.tr/tr/pub/kvkd/issue/62960/826099> (E.T. 14.3.2022).

³¹⁴ Emine AKYÜZ, **Çocuk Hukuku**, Pegem Akademi Yayıncılık, 7. Baskı, 2020, s. 113.

³¹⁵ ERDOĞAN/KESKİN, s.249.

olması gerektiği ifade edilmektedir³¹⁶. Yasal temsilcinin göstereceği bu rızanın küçüğün üstün yararı ilkesine uygun düşecek yönde olması gerektiği muhakkaktır³¹⁷. Nitekim, TMK'nın 346. maddesinde çocuğun menfaatinin tehlikeye düşmesi halinde ana babanın bu duruma çare bulamazsa hâkimin çocuğu korumaya yönelik uygun önlemler alacağı düzenlenmiştir. Bir boşanma davasında hâkim, babanın “anne tarafından çocuklarının sosyal medya hesabında sürekli paylaşılması” konusunda şikâyetçi olması üzerine verdiği ara kararında çocukların velayetinin dava bitene kadar babada kalmasına, fotoğrafların sosyal medyada paylaşılmasının da yasaklanmasına karar vermiştir³¹⁸.

Öte yandan, ayırt etme gücüne sahip olan çocuğun kişisel verilerinin işlenmesine yönelik iradesi ile velisinin iradesinin çatışması halinde çocuğun iradesinin geçerli olması gerektiği kabul edilmelidir³¹⁹. Çünkü, kişisel verilerin korunması hakkı çocuğun kişiliğini yakından ilgilendiren kişiye sıkı sıkıya bağlı bir haktır ve bu tür hakların, TMK'nda sayılan evlenme, evlat edinilme gibi istisnalar haricinde, bizzat hakkın sahibi tarafından kullanılması esastır. Söz gelimi, bir belediyeye ait kütüphanenin tanıtımı için kütüphaneyi kullanan çocukların fotoğraflarının çekilerek belediyeye ait sosyal medya hesaplarında paylaşılması olayında, çocuklardan bazılarının velileri bu fotoğrafların kaldırılmasını talep ederse, belediye tarafından çocukların fotoğrafları çekilirken fotoğrafların hangi amaçla çekildiğini ve sosyal medya hesaplarında paylaşılacağını bildikleri, ayırt etme gücüne sahip oldukları, bu amaçla poz verdikleri ve açık rıza beyanında bulundukları yönünde yapılan savunmanın geçerli bir savunma olacağı kabul edilmelidir. Elbette, çocukların somut olaya ilişkin ayırt etme gücünün bulunup bulunmadığı

³¹⁶ UÇAK, s.51. KVK Kurulu da kendisine yapılan bir başvuruya ilişkin yaptığı değerlendirmede, çocuğun üstün yararı da düşünülerek kişisel verilerin korunması hakkının somut olay bazında nisbi kişiye sıkı sıkıya bağlı hak olarak kabul edilmesi gerektiğine karar vermiştir. Karara konu olayda, baba çocuğunun sağlık verisinin silinmesi için veri sorumlusuna başvurmasına rağmen cevap alamayınca 18 yaşın altında olan çocuk Kuruma bizzat şikâyet başvurusunda bulunmuştur. Kararda Kurul, 18 yaşın altında bulunan çocuğun bizzat Kuruma başvurup başvuramayacağı ve veri sorumlusuna başvuruyla Kuruma başvuran kişilerin farklı olmasının mevzuata uygun olup olmadığı hususlarını incelemiştir. Buna göre, kişisel verilerin korunması hakkının kişiye sıkı sıkıya bağlı haklardan olduğu, dolayısıyla ayırt etme gücüne sahip küçük tarafından bizzat kullanılabileceği belirtilmiştir. Ayrıca, TMK'nın 16. maddesinde ayırt etme gücüne sahip küçüklerin ve kısıtlıların kişiye sıkı sıkıya bağlı hakları kullanırken yasal temsilcilerinin rızasına ihtiyacı olmadıklarına yönelik kuralın hakkın sahibi bakımından bir yetki kuralı olduğu, öte yandan yasal temsilci için bir yasak getirmediği, dolayısıyla velinin çocuk adına nisbi kişiye sıkı sıkıya bağlı hakları kullanabileceği ifade edilmiştir: KVK Kurulu, 11.8.2020 tarih ve 2020/622 sayılı karar, <https://www.kvkk.gov.tr/Icerik/6816/2020-622> (E.T. 14.3.2022).

³¹⁷ “Çocuğun üstün yararı” ilkesi, çocukları ilgilendiren tüm karar verme süreçlerinde, sürecin her aşamasında çocuk için en iyi seçeneklerin değerlendirilmesini ve çocuğun ihtiyaçlarının merkeze alınmasını gerektiren bir yaklaşımdır. Bu ilke, farklı yorumlamalara açık olsa da temel olarak çocuk odaklı bir karar verme sürecini hedefler ve çocuğun refahını, gelişimini ve haklarını önceliklendirir. Ayrıntılı bilgi için bkz.: Zeynep HAZAR, “İnsan Hakları Çatışmalarının Çözümlemesinde Çocuğun Üstün Yararı İlkesinin İşlevi: Türk Anayasa Mahkemesi Kararları Çerçevesinde Bir Değerlendirme”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C.XXVI, Y. 2022, S.2, s.647-684.

³¹⁸ “Mahkeme çocuklarını reklam malzemesi yapan blogger annenin iki çocuğunu babaya verdi” **NTV**, 30.6.2017. <https://www.ntv.com.tr/turkiye/mahkeme-cocuklarini-reklam-malzemesi-yapan-blogger-annenin-iki-cocugunubabaya-verdi,qS8Pj79Zc0SNNhjagnJu8A> (E.T. 14.3.2022).

³¹⁹ Örneğin, İtalya’da görülen bir davada 16 yaşındaki çocuk, rızası olmaksızın fotoğraflarını sosyal medyada paylaşan annesine karşı açtığı davada, çocuğun kişilik haklarının korunması gerektiği gerekçesiyle haklı bulunmuştur: ÖVGÜ Pınar, “Oğlunun fotoğraflarını izinsiz sosyal medyada paylaşan anne suçlu bulundu”, **BBC News Türkçe**, 8.1.2018. <https://www.bbc.com/turkce/haberler-dunya-42604622> (E.T. 15.3.2022).

dikkatle irdelenmelidir. Ayrıca çocuğun anlayabileceği şekilde aydınlatma yapıldığı ve açık rıza beyanlarının alındığı belediye tarafından ispat edilmelidir.

Konuya ilişkin olarak mevzuatımızda yeni sayılabilir bir düzenleme örneği de mevcuttur. 21 Haziran 2019 tarihli Resmî Gazete’de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmeliğin 8. maddesinde “çocukların sağlık verilerine erişimi” başlıklı düzenlemeye göre ebeveynlerin herhangi bir izne ihtiyaç duymaksızın çocuklarının sağlık verilerine e-nabız sistemi üzerinden erişebilecekleri kabul edilmiştir. Bununla birlikte, ayırt etme gücüne sahip olan çocuklar ebeveynlerinin sağlık geçmişlerine erişimini e-nabız sistemi üzerinden izne tabi tutabilecektir³²⁰. Dolayısıyla, ayırt etme gücüne sahip olan çocuk sağlık verilerinin ailesi tarafından bilinmesini istemezse ebeveynin hilafına söz konusu verilere erişimi engelleyebilir.

Öte yandan, ayırt etme gücüne sahip olmayan çocuklar hakkında veli, vasi ya da yargı makamlarınca karar verilirken çocuğun iradesinin de göz önünde bulundurulması gerektiği ifade edilmektedir³²¹. Buna göre, çocuğun iradesinin belirlenmesinde onun duygu ve düşünceleri ve konuya yönelik istekleri değerlendirilmelidir. 1989 BM Çocuk Hakları Sözleşmesi’nin 12. maddesi, taraf devletlerin, görüşlerini oluşturma yeteneğine sahip çocuğun kendini ilgilendiren her konuda görüşlerini serbestçe ifade etme hakkını, bu görüşlere çocuğun yaşı ve olgunluk derecesine uygun olarak gereken özen gösterilmek suretiyle tanınması gerektiğini belirtmektedir. Yine, Çocuk Haklarının Kullanılmasına İlişkin Avrupa Sözleşmesi’nin 3. maddesi, iç hukuk tarafından yeterli idrake sahip olduğu kabul edilen bir çocuğa, kendisini ilgilendiren adli davalarda bazı haklar tanımaktadır. Bu haklar arasında ilgili tüm bilgileri alma, kendisine danışılma ve kendi görüşünü ifade etme, ayrıca görüşlerinin uygulanmasının ve alınacak her tür kararın olası sonuçları hakkında bilgilendirilme hakları yer almaktadır. Dolayısıyla, konumuz özelinde, kişisel verilerinin korunmasına yönelik verilecek bir rıza beyanı noktasında, yeterli derecede ayırt etme gücüne sahip olmadığı düşünülen çocukların dahi konuya ilişkin duygu ve düşünceleri ve istekleri dinlenilmeli, alınacak kararda bu hususlar göz ardı edilmemelidir. Elbette, nihai kararın çocuğun iradesiyle aynı yönde olma zorunluluğu bulunmamakta; ancak çocuğun üstün yararı ilkesiyle bağdaşır yönde olması gerekmektedir³²².

4.4.1.2. Açık Rıza Şartının İstisnaları

6698 sayılı Kanunun 5. maddesinin ilk fıkrasında ilgilinin açık rızası bulunmaksızın kişisel verilerin işlenemeyeceği belirtildikten sonra maddenin ikinci fıkrasında sayılan hallerden birinin bulunması halinde açık rıza alınmaksızın kişisel veri işlenmesinin mümkün olduğu belirtilmiştir. İlk

³²⁰ RG, 21.6.2019/30808.

³²¹ Özge YÜCEL, “Çocuğun Yüksek (Üstün) Yararı Bağlamında Çocuğun İradesi”, **Ufuk Üniversitesi Hukuk Fakültesi Dergisi**, C.1, S.2, Aralık 2013, s.134.

³²² YÜCEL, s.135.

bakışta, burada sayılan istisnai hallerin varlığı halinde veri sorumlusuna açık rıza alıp almama konusunda bir seçim şansı tanınmış gibi görünse de istisnai hallerden biri nedeniyle veri işleme yapılmasına rağmen yine de ilgiliden açık rıza alınması, ilgili kişinin yanıltılması ve yanlış yönlendirilmesi anlamına geleceğinden, bu durumda veri sorumlusunun Kanunun 4. maddesinde sayılan “hukuka ve dürüstlük kurallarına uygun şekilde” veri işleme kuralına aykırı hareket ettiği kabul edilmektedir³²³. Nitekim, açık rızası alınan ilgili kişi, bu rızasını her zaman geri alabileceğini ve hakkındaki verilerin işlenmesine son verebileceğini düşünecektir.

Kanunun 5. maddesinin ikinci fıkrasına göre *kanunlarda açıkça öngörülmesi fiili imkânsızlık nedeniyle rızasını açıklayamayan ya da rızasına geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunluluk bulunması, bir sözleşmenin kurulması veya ifasıyla doğrudan ilgili olmak kaydıyla, sözleşmenin taraflarına ait verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için kişisel veri kaydının zorunlu olması, kişisel verinin ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek şartıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması* durumlardan birinin varlığı halinde kişisel veriler ilgilinin açık rızası alınmadan işlenebilir. Bununla birlikte, bu şartlardan herhangi biri sebebiyle yapılan veri işleme faaliyeti için 6698 sayılı Kanunda düzenlenen diğer tüm kurallar geçerliliğini korumaktadır.

95/46 sayılı Direktifin 7. maddesinde de kişisel verilerin işleme şartları düzenlenmiştir. Buna göre, ilgili kişinin şüpheye yer bırakmayacak şekilde rıza beyanında bulunmuş olması, ilgili kişinin taraf olduğu bir sözleşmenin ifası için veya bir sözleşmeye girmeden önce ilgili kişinin talebi üzerine adımlar atmak için veri işlemenin gerekli olması, veri sorumlusunun hukuki bir yükümlülüğünü yerine getirebilmesi için veri işlemenin gerekli olması, ilgili kişinin hayati menfaatlerini korumak için veri işlemenin gerekli olması, kamu yararına yürütülen bir görevin yerine getirilmesi veya veri sorumlusuna ya da üçüncü bir tarafa verilen resmi yetkinin kullanılması için işlemenin gerekli olması ve ilgili kişinin temel hak ve özgürlüklerine ilişkin menfaatlerini geçersiz kılmamak şartıyla veri sorumlusu ya da

³²³ Kişisel Verileri Koruma Kurumu, “Hizmetin Açık Rıza Şartına Bağlanması”, <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanın-Hizmet-Sartina-Baglanmasi> (E.T. 26.1.2022); KVK Kurulu, 8.7.2019 tarih ve 2019/206 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6709/2019-206> (E.T. 27.1.2022). AB hukukunda mevcut olan başka bir görüş, kişisel verilerin işleme şartları arasında herhangi bir hiyerarşik sıralama bulunmadığından, veri sorumlusunun diğer şartlar bulunsu dahi ilgilinin açık rızasına dayanarak veri işlemeyi tercih edebileceğini savunmaktadır. Ancak, ilgili kişiden alınan açık rıza sonradan geri alınırsa bu halde veri sorumlusunun diğer veri işleme şartlarından birine dayalı olarak işleme faaliyetine devam etmesi dürüstlük kuralına aykırılık teşkil edecektir. Özellikle, açık rıza alınması dışındaki şartlardan birinin varlığının açık şekilde belirgin olmadığı hallerde veri sorumlusunun açık rızaya dayalı veri işleyebilmesi gerektiği, açık rızanın geri alınması halinde veri sorumlusunun bu kez diğer şartlardan birine dayalı olarak veri işlemeye devam etmek istemesinin dürüstlük kuralına aykırılık teşkil edeceği ifade edilmektedir. Bu bağlamda, söz konusu Kurul kararı, maddi olgu oluşmadan yaptırım kararı uygulamak anlamını taşıdığı gerekçesiyle eleştirilmektedir: ÇEKİN, s.103 vd.

üçüncü kişilerin meşru menfaatlerini korumak için veri işlemenin gerekli olması şartlarından birinin varlığı halinde veri işleme faaliyetinin meşru olduğu kabul edilmiştir.

Benzer bir düzenlemeye 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün 6. maddesinde yer verilmiştir. İlgili kişinin, kişisel verilerinin bir veya daha fazla belirli bir amaç için işlenmesine izin vermesi, ilgili kişinin taraf olduğu sözleşmenin ifası için veya bir sözleşmeye girmeden önce ilgili kişinin talebi üzerine adımlar atmak için işlemenin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için işlemenin gerekli olması, ilgili kişinin ya da başka gerçek bir kişinin hayati menfaatlerini korumak için işlemenin gerekli olması, kamu yararına yürütülen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için işlemenin gerekli olması ya da ilgili kişinin özellikle çocuk olduğu durumlarda, kişisel verileri korumayı gerektiren temel hak ve özgürlüklerine ilişkin menfaatlerini geçersiz kılmamak şartıyla, veri sorumlusu ya da üçüncü kişilerin meşru menfaatlerini korumak için veri işlemenin gerekli olması hallerinden en az birinin geçerli olduğu durumlarda veri işleme faaliyeti hukuka uygun gerçekleştirilmiş olmaktadır. Bununla birlikte, son şartın kamu makamları tarafından görevlerini yerine getirirken gerçekleştirilen işlemlere uygulanmayacağı belirtilmiştir (m.6/1 (son cümle)).

95/46 sayılı Direktif ile 2016/579 sayılı Tüzük düzenlemelerine bakıldığında hükümlerin birbirlerine benzer olduğu görülmektedir. Bununla birlikte, 6698 sayılı Kanunun 5. maddesinde yer verilen kişisel verilerin işleme şartlarının mehzaz Direktiften farklı birkaç şarta yer vermesi göze çarpmaktadır. Kanuna göre açık rıza alınmaksızın veri işlenebileceği öngörülen hallerden *kanunda açıkça öngörülmesi; verinin ilgilinin kendisince alenileştirilmesi ve bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması* halleri Direktifte yer almamıştır. Bu bakımdan, Kanunun Direktife göre daha geniş alanda veri işlemeye imkân tanıdığı, veri işleme imkânlarını genişlettiği söylenebilir³²⁴.

4.4.1.2.1. Kanunlarda Açıkça Öngörülmesi

Kanunun 5. maddesinin ilk fıkrasında “kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.” denildikten sonra ikinci fıkrada kanunlarda açıkça öngörülmesi halinde açık rıza olmaksızın işlenmesinin mümkün olduğu düzenlenmiştir. Öyleyse, kanunda “Açık rıza olmaksızın ilgili veriler işlenebilir. / İlgilisinin açık rızasının olması aranmaz.” benzerinde bir ifadenin bulunması gerekir mi? Yoksa kişisel veri olarak kabul edilen bir verinin veri işleme faaliyeti kapsamındaki bir eyleme imkân veren bir ifadenin bulunması yeterli olacak mıdır?

³²⁴ BAŞAR, s.70.

Türkçe sözlükte “açıkça” kelimesi “*gizli bir yönü kalmaksızın, kolay anlaşılır bir biçimde, alenen, aşikare*” şeklinde tanımlanmaktadır³²⁵. Dolayısıyla, “kanunda açıkça öngörülmesi” ifadesinden muğlaklık içermeyecek, şüpheye yer bırakmayacak kesinlikte bir düzenleme anlaşılmalıdır. Bu yönde hüküm içeren kanuni düzenlemenin içeriğinin nasıl olması gerektiği sorusuna ise 6698 sayılı Kanunun gerekçesi ışık tutmaktadır. Kanunun gerekçesinde 2559 sayılı PVSİ’nın 5. maddesinde bir suç soruşturması sebebiyle kolluk tarafından şüphelilerin parmak izlerinin alınması ile 5352 sayılı Adli Sicil Kanunu’nun 2. maddesi ve diğer ilgili hükümleri uyarınca kişilerin ceza mahkumiyetlerine ilişkin verilerinin Adalet Bakanlığınca işlenmesi bu duruma örnek olarak verilmiştir³²⁶. Bu hükümlerde bir takım kişisel verilerin çeşitli araçlar vasıtasıyla kaydedileceği/saklanacağı ifade edilmektedir. Dolayısıyla, kanunda açıkça öngörüldüğünün kabulü için “açık rıza alınmaksızın veri işlenebileceği” şeklindeki bir ibarenin yer aldığı bir düzenlemeden ziyade, sadece kişisel verilere ilişkin veri işleme faaliyeti sayılan işlemlere imkân veren ifadelerle yer verilmesinin yeterli olacağı anlaşılmaktadır. Aksi yönde bir düşünüşün, yani açık rıza olmaksızın veri işlenebileceğinin öngörülmesi gerektiğini savunmak, 6698 sayılı Kanundaki ilgili hükmün amacını aşacak şekilde yorumlanması anlamına gelecektir. Nitekim, mevzuatımızda kişisel verilerin işlenebilmesine olanak veren kanun hükümlerinde bazı veri işleme faaliyetleri için ilgisinden açık rıza alınması öngörülmüşken, ilgisinden alınmış açık rıza aranmaksızın belirli veri işleme faaliyetlerinin gerçekleştirilebileceğine yönelik bir düzenlemeye rastlanılmamaktadır. Başka bir deyişle, kanun koyucu ilgisinden açık rıza alınmasını öngörmüyorsa bunu dile getirmemekte, sadece açık rızanın alınması gerekiyorsa bunu açıkça ifade etmektedir³²⁷.

5411 sayılı Bankacılık Kanununa 13.2.2011 tarihinde eklenen “Ek Madde 1” hükmü uyarınca, Türkiye Bankalar Birliği nezdinde, finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ya da tüzel kişilerle veya onay vermeleri halinde diğer kişilerle paylaşılmasını sağlamak üzere Risk Merkezi kurulmuştur. Buna göre, tüm kredi kuruluşlarının ve

³²⁵ Türk Dil Kurumu Sözlükleri, **Güncel Türkçe Sözlük**, <https://sozluk.gov.tr/> (E.T. 4.2.2021).

³²⁶ Söz konusu örneklerin parmak izi ve mahkûmiyet kararı gibi özel nitelikli kişisel verilerin işlenmesine yönelik hükümler olması ilginçtir. **2559 sayılı Kanunun 5. maddesi:** Polis; a) Gönüllü, b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, ç) Türk vatandaşlığına başvuruda bulunan, d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, e) Gözaltına alınan, kişilerin parmak izini alır. / Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez.

5352 sayılı Kanunun 2. maddesi: Hakkında Türk mahkemeleri veya yabancı ülke mahkemeleri tarafından kesinleşmiş ve Türk Hukukuna göre tanınan mahkûmiyet kararı bulunan Türk vatandaşları ile Türkiye’de suç işlemiş olan yabancıların kayıtları da dahil tüm adli sicil bilgileri; mahallinde bilgisayar ortamına aktarılmasını takiben, Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğündeki Merkezi Adli Sicilde tutulur.

³²⁷ Bunun bir istisnasına **5809 sayılı Elektronik Haberleşme Kanununda** rastlanılmaktadır. Madde 51: (8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların **açık rızası aranmaksızın** konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

öngörülen bazı finansal kuruluşların Risk Merkezine üye olması zorunlu tutulmuş, bu kuruluşların Risk Merkezince istenen, müşterileri ile ilgili tüm bilgileri merkeze vermesi zorunlu kılınmıştır. Düzenlemede kredi kuruluşlarının müşterilerine ait bilgileri Risk Merkezine vermesi şeklindeki veri işleme faaliyetine yönelik olarak ilgili kişilerin açık rızasına başvurulmayacağından bahsedilmemiştir. Öte yandan aynı maddenin 9. fıkrasında sır sahibinin bilgilerinin açıklanması yönünde açık rızasının bulunması halinde belirlediği kişiye risk bilgilerinin verilebileceği ifade edilmiştir. Dolayısıyla, sır sahibine ilişkin verinin kendi isteğiyle paylaşılacak suretiyle işlenebilmesi konusunda ilgisinin açık rızasının alınması kanunda açıkça düzenlenmiştir³²⁸.

-Olağan Dönemde Çıkarılan CBK'lar ile Kişisel Verilerin İşlenmesine İlişkin Düzenleme Yapılması: “Kanunda açıkça öngörülmesi” şeklindeki ifadede yer alan “kanun” ibaresinin neyi ifade ettiği de değerlendirilmelidir. Anayasanın 7. maddesi uyarınca Kanun çıkarma yetkisi Türkiye Büyük Millet Meclisine aittir ve bu yetki devredilemez. Dolayısıyla, “kanun” ibaresinden ilk olarak TBMM tarafından “kanun” adı altında yapılan düzenlemeler anlaşılabilmektedir³²⁹. Öte yandan, Anayasanın 90. maddesinin 5. fıkrasına göre usulüne uygun olarak yürürlüğe konulmuş Milletlerarası andlaşmalar da kanun hükmündedir. Öyleyse, bir konuda kişisel verilerin işlenebileceğine ilişkin bir hükmün kanunlarımızda bulunmamakla birlikte, Milletlerarası bir andlaşmada yer alıyor olması halinde bu konuda düzenleme sınırları çerçevesinde veri işlenebileceği söylenebilir³³⁰.

2017 yılında 6771 sayılı Kanunla yapılan Anayasa değişikliği sonrası Cumhurbaşkanlığı hükümet sistemine geçilmiş ve Cumhurbaşkanına yürütme yetkisine ilişkin konularda Cumhurbaşkanlığı kararnamesi çıkarabilme yetkisi tanınmıştır (Anayasa m.104/17). Ayrıca, Anayasanın 119. maddesinin 6. fıkrasına göre “*Olağanüstü hallerde Cumhurbaşkanı, olağanüstü halin gerekli kıldığı konularda ... Cumhurbaşkanlığı kararnamesi çıkarabilir. Kanun hükmündeki bu kararnameler Resmî Gazetede yayımlanır, aynı gün Meclis onayına sunulur.*” Dolayısıyla, OHAL döneminde çıkarılan Cumhurbaşkanlığı Kararnameleri kanun hükmündedir ve bu düzenlemeyle açıkça veri işlemeye imkân veren bir husus öngörülmüşse ilgili kişiden açık rıza alınmaksızın veri işlenebilir. Bununla birlikte, OHAL CBK'larının uygulanma süresi olağanüstü hâl süresi ile; uygulanacağı yer ise

³²⁸ Benzer düzenleme örnekleri olarak: **5809 sayılı Elektronik Haberleşme Kanunu, Madde 51:** (3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir. / (6) Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verileri ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilir.

5684 sayılı Sigortacılık Kanunu, Madde 31/B: (5) Sigorta Bilgi ve Gözetim Merkezinin bütün işlem ve kayıtları gizlidir. Sigorta Bilgi ve Gözetim Merkezi topladığı her türlü bilgiyi, Müsteşarlığa istenen biçim ve sürede vermekle yükümlüdür. Söz konusu bilgiler, sahibinin açık rızasının bulunması durumunda belirlediği kişiye belli bir ücret karşılığında verilir.

³²⁹ ÖZBUDUN, s. 208 vd.

³³⁰ “Anayasamıza göre usulüne uygun olarak onaylanıp yürürlüğe konulan sözleşmeler kanun hükmündedir. Başka bir deyişle aynı zamanda iç hukukumuzun kuralı haline gelmiş olur.”: Ömer ANAYURT, **Anayasa Hukuku**, Seçkin Yayıncılık, 3. Baskı, 2020, s. 284.

olağanüstü halin ilan edildiği yerlerle sınırlı olması nedeniyle³³¹, böyle bir düzenlemeyle veri işlemeye imkân verilmişse, veri işleme faaliyetinin de OHAL ilan edilen coğrafi bölge ve OHAL süresiyle sınırlı olacak şekilde yapılması gerekir. Anayasanın 119. maddesinin 7. fıkrası uyarınca *savaş ve mücbir sebeplerle TBMM'nin toplanamaması hali hariç olmak üzere, olağanüstü hâl sırasında çıkarılan Cumhurbaşkanlığı kararnameleri üç ay içinde TBMM'de görüşülüp karara bağlanacağı* kabul edildiğinden, Mecliste kabul edilerek kanuna dönüşen OHAL CBK'sı³³² için artık yukarıda kanunlara ilişkin anlatılan kuralların geçerli olacağı söylenebilir. Ancak, kuralın olağanüstü hâlin ilanına sebep olan tehdit veya tehlikelerin bertaraf edilmesine yönelik ve olağanüstü hâl süresiyle sınırlı olarak uygulanması şartlarını taşıması halinde Anayasa'ya uygunluk denetimi bakımından Anayasa'nın olağanüstü hallerde temel hak ve özgürlüklerin kullanılmasının sınırlandırılması ve durdurulması hususunu düzenleyen 15. maddesinin esas alınacağı; aksi halde kurala ilişkin incelemenin sınırlamaya konu hakkın düzenlendiği Anayasa maddesi, Anayasa'nın diğer hükümleri ve olağan dönemde hak ve özgürlüklerin sınırlandırılması konusunun düzenlendiği 13. maddesine göre inceleme yapılacağı unutulmamalıdır³³³.

Olağanüstü hâl Cumhurbaşkanlığı kararnamesinden farklı olarak, olağan dönemde çıkarılan Cumhurbaşkanlığı kararnamelerinin hukuki niteliğine ilişkin öğretide farklı görüşler yer almaktadır³³⁴. Ancak bu tartışmalar inceleme konumuz dışında kaldığından, sadece olağan dönemde çıkarılan Cumhurbaşkanlığı kararnameleriyle kişisel verilere ilişkin düzenleme yapılıp yapılamayacağına ilişkin bilgi vermekle yetinmek yerinde olacaktır. Anayasanın 104. maddesinin 17. fıkrasında³³⁵ hangi konularda CBK çıkarılamayacağına ilişkin çizilen sınırlardan biri de “Anayasada münhasıran kanunla düzenlenmesi öngörülen konular”dır. Anayasada hangi hususların münhasıran kanunla düzenleneceğine ilişkin özel bir hüküm bulunmamakla birlikte, Anayasa Mahkemesi kararlarında anayasa koyucunun kanunla düzenlenmesini öngördüğü konuların bu kapsamda kabul edilmesi gerektiği ifade

³³¹ Kemal GÖZLER, *Türk Anayasa Hukuku Dersleri*, Ekin Yayınevi, 22. Baskı, Eylül, 2018, s. 383.

³³² Yavuz ATAR, *Türk Anayasa Hukuku*, Seçkin Yayıncılık, 14. Baskı, 2021, s. 284.

³³³ AYM, E. 2018/91, K. 2020/10, § 15-17.

³³⁴ Yavuz Atar, olağan dönem CBK'larının da kanunla eşdeğer norm niteliğinde olduğunu savunmaktadır: ATAR, s.275 vd.; Söyler ise Anayasada CBK'larla düzenlenmesi öngörülen münhasır alanlarda çıkarılacak CBK'ların kanunla eş değer olduğunu savunmaktadır: Yasin SÖYLER, *Yeni Başkanlık Sisteminde Cumhurbaşkanlığı Kararnamesi*, Seçkin Yayıncılık, 2018, s. 164. Öte yandan çoğunluk olarak kabul edilebilecek görüş ise normlar hiyerarşisinde olağan dönem CBK'ların kanunun altında yer aldığını ifade etmektedir.; Turan YILDIRIM, “İdarenin Kanuniliği İlkesi Bağlamında Cumhurbaşkanlığı Kararnamelerinin Anayasal Sınırı”, *Anayasa Yargısı Dergisi*, Cilt: 36, S. 1, 2019, s. 293-314; Abdurrahman EREN, “Anayasa Mahkemesinin Kanun Hükmünde Kararnamelere İlişkin İçtihadı Doğrultusunda Cumhurbaşkanlığı Kararnamelerinin Değerlendirilmesi”, *Anayasa Yargısı Dergisi*, Cilt: 36, S. 1, 2019, s. 1-72; Artuk ARDIÇOĞLU, “Cumhurbaşkanlığı Kararnamesi”, *Ankara Barosu Dergisi*, S. 3, 2017, s. 20-51.

³³⁵ Anayasa, m.104/17: “Cumhurbaşkanı, yürütme yetkisine ilişkin konularda Cumhurbaşkanlığı kararnamesi çıkarabilir. Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle dördüncü bölümde yer alan siyasi haklar ve ödevler Cumhurbaşkanlığı kararnamesiyle düzenlenemez. Anayasada münhasıran kanunla düzenlenmesi öngörülen konularda Cumhurbaşkanlığı kararnamesi çıkarılamaz. Kanunda açıkça düzenlenen konularda Cumhurbaşkanlığı kararnamesi çıkarılamaz. Cumhurbaşkanlığı kararnamesi ile kanunlarda farklı hükümler bulunması halinde, kanun hükümleri uygulanır. Türkiye Büyük Millet Meclisinin aynı konuda kanun çıkarması durumunda, Cumhurbaşkanlığı kararnamesi hükümsüz hale gelir.”

edilmektedir³³⁶. Öte yandan Anayasanın kişisel verileri düzenleyen 20. maddesine bakıldığında kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Bu sebeple, anayasa koyucunun kanunla yapılmasını öngördüğü kişisel verilerin korunmasına ilişkin düzenlemelerin CBK ile yapılmasının mümkün olmadığı kabul edilmelidir.

Anayasanın 104. maddesinin 17. fıkrasına göre olağan dönem CBK'larının konu bakımından sınırlarından bir diğeri de Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleridir. Anayasa koyucu, bu konulara ilişkin düzenlemelerin CBK ile yapılmasına imkân vermemiştir. Anayasanın ikinci kısmının ikinci bölümünde düzenlenen haklardan biri de özel hayatın gizliliğidir. Kişisel verilerin korunmasını isteme hakkının özel hayatın gizliliği hakkının düzenlendiği 20. maddenin 3. fıkrasında yer alması sebebiyle de bu hususta CBK ile bir düzenleme yapılması Anayasaya aykırı olacaktır. Son olarak, kişisel verilerin işlenebileceğinin öngörülmesi, aslında kişisel verilerin korunması hakkına getirilen bir sınırlama niteliği taşıyacaktır. Nitekim Anayasanın 20/3 maddesinin sondan ikinci cümlesinde kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasının bulunması halinde işlenebileceği ifade edilmiştir. Anayasanın 13. maddesi uyarınca temel hak ve özgürlüklere getirilecek sınırlamalar ancak kanunla yapılabileceğinden, yine bu alanda yapılacak bir CBK düzenlemesinin Anayasaya aykırı olacağı sonucuna ulaşılabilecektir³³⁷.

Son dönemde yayımlanan bir Anayasa Mahkemesi kararında da CBK'lar ile ilgili aynı sonuca ulaşılmış ve kişisel verilerin işlenmesini öngören düzenleme maddeleri iptal edilmiştir. 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin incelendiği kararda, Cumhurbaşkanlığı İdari İşler Başkanlığının birimlerinden biri olan Personel ve Prensipier Genel Müdürlüğünün görevlerinin düzenlendiği ilgili CBK'nın 8. maddesinin (1) numaralı fıkrasının "*Devletin sevk ve idaresinde görevli üst kademe yöneticileri hakkında bilgi toplamak, sicil özetlerini ve biyografilerini tutmak*" şeklindeki (f) bendinde yer alan "bilgi toplamak" ibaresine yönelik itiraz incelenmiştir. Yüksek Mahkeme, Anayasanın 104. maddesinin 17. fıkrasını ikinci cümlesi uyarınca Anayasa'nın İkinci Kısmı'nın Birinci ve İkinci Bölüm'lerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölümü'nde yer alan siyasi haklar ve ödevlerin CBK ile düzenlenemeyeceğini, bu bağlamda Anayasa'nın 20. maddesinde düzenlenen ve "*Kişinin Hakları ve Ödevleri*" başlıklı İkinci Bölüm'ünde yer alan kişisel verilerin korunması hakkına ilişkin olarak da CBK ile düzenleme yapılmasının mümkün olmayacağını ifade etmiştir. İtiraz konusu düzenleme gereği ilgili Müdürlük tarafından devletin sevk ve idaresinde görevli

³³⁶ AYM, E. 2018/133, K. 2021/70, T.13.10.2021, § 11; AYM, E. 2018/127, K. 2021/18, T.18.3.2021, § 11; AYM, E.2016/150, K.2017/179, T.28/12/2017, § 57; AYM, E.2016/180, K.2018/4, T.18/1/2018, § 17; AYM, E.2017/51, K.2017/163, T.29/11/2017, § 13.

³³⁷ Anayasada CBK'larla düzenlenmesi öngörülen alanlarda çıkarılacak kararnamelerde temel hak ve özgürlüklerin sınırlanamayacağına ilişkin bkz.: Melikşah YASİN, "Cumhurbaşkanlığı Kararnamelerinin Türk İdari Teşkilat Hukukuna Etkileri", **Anayasa Yargısı Dergisi**, Cilt: 36, S. 1, 2019, s. 323 vd.

üst kademe yöneticileri hakkında toplanacak bilgilerin önemli ölçüde anılan kişilerin mesleki ve özel durumlarını yansıtan sicil bilgileri, iş ve sosyal yaşamını içine alacak şekilde özgeçmişleri gibi kişisel veri niteliği taşıyan bilgilerden oluşacağı saptamasını yapan Mahkeme, bu nedenle kuralın kişisel verilere ilişkin olduğunu ve CBK ile düzenlenemeyecek yasak alan içerisinde kaldığını tespit ederek Anayasanın 104. maddesinin 17. fıkrasının ikinci cümlesine aykırı olduğundan ötürü iptaline karar vermiştir³³⁸.

4.4.1.2.2. Kişinin Hayatının veya Beden Bütünlüğünün Korunması

6698 sayılı Kanunun 5. maddesinin 2.b bendine göre fiili imkânsızlık nedeniyle rızasını açıklayamayan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin yahut bir başkasının hayatı ve beden bütünlüğünün korunması için zorunluluk bulunan hallerde ilgisine ait kişisel verilerin işlenmesinde açık rıza aranmayacaktır. Kanunun gerekçesinde ifade edildiği üzere, kişinin şuurunun yerinde olmadığı ya da akıl hastası olduğu durumda hayat veya beden bütünlüğünün korunması için yapılacak tıbbi müdahalede gerekli kişisel veriler ilgilinin açık rızası alınmaksızın işlenecektir. Böyle bir durumda, kişinin adı, soyadı, adresi ya da yakınlarına ulaşmak için telefon numarasının kullanılması gibi genel nitelikli kişisel verilerin işlenmesi söz konusu olabileceği gibi, kan grubu, genetik verileri veya diğer bazı sağlık bilgileri gibi kişinin özel nitelikli verilerinin işlenmesi de söz konusu olabilecektir.

Kanunun 5/2(b) maddesi hayat ve beden bütünlüğünün korunması söz konusu olduğunda açık rıza olmaksızın genel nitelikli verilerin işlenmesini sağlamaktadır. Bununla birlikte, benzer durumlarda işlenmesi gerekli olabilecek sağlık verileri içinse 6. maddenin 3. fıkrası göz önünde bulundurulmalıdır. Buna göre, sağlık ve cinsel hayata ilişkin özel nitelikli verilerin sır saklama yükümlülüğü bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgisinin açık rızası alınmaksızın işlenebilmesi belli amaçlar dahilinde mümkün olup, bunlardan biri de tıbbi teşhis, tedavi ve bakım hizmetlerinin yerine getirilmesidir. Dolayısıyla, kişinin hayat ve beden bütünlüğünün korunması amacıyla ve ilgisinin açık rızasının alınmadığı hallerde genel nitelikli verilerinin işlenmesi Kanunun 5/2(b) hükmünce hukuka uygunken, Kanunun 6. maddesinin 3. fıkrasıyla da benzer durumda kişinin sağlık verilerinin işlenmesi

³³⁸ AYM, E.2018/118, K.2023/180, T.26/10/2023, § 7-15. Söz konusu kararda, aynı CBK’da yer verilen, Politika Kurullarının kendi görev alanlarıyla ilgili olarak her türlü bilgi ve belgeyi ilgili bakanlıklar ile kamu kurum ve kuruluşlarından talep edebileceğini öngören 33. maddesinin 3. fıkrasının birinci cümlesinde yer alan “her türlü bilgi ve belgeyi” ibaresinin; kurulların bilgi toplama ve sır saklama yükümlülüğüne ilişkin usul ve esasların düzenlendiği ve kurulların, görevleri ile ilgili olarak gerekli olan bilgileri bütün kamu kurum ve kuruluşlarından istemeye yetkili olduklarını düzenleyen 36. maddenin 1. fıkrasının birinci cümlesinde yer alan “gerekli olan bilgileri” ibaresinin; ve kurulların başkan ve üyeleri ile personelinin, görevlerini yerine getirmeleri sırasında edindikleri, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, ticari sırları ve bunlara ait belgeleri, bu konuda mevzuat gereği yetkili kılınan mercilerden başkasına açıklayamayacaklarını, kendilerinin veya üçüncü kişilerin yararına kullanamayacaklarını düzenleyen 36. maddesinin 3. fıkrasının aynı gerekçeyle iptaline karar verilmiştir (§ 154-160). Bu kararda ayrıca, CBK’nın Sağlık Bakanlığının kişisel sağlık verilerini işlemesine imkân veren 378. maddesi de yukarıda açıklanan gerekçeyle iptal edilmiştir (§ 373-378).

hukuka uygun kabul edilecektir. Bununla birlikte, sađlık verileri bakımından veri işleyebilecek kişilerin sır saklama yükümlülüğü bulunan kişiler ile yetkili kurum ve kuruluşlarla sınırlı olduđu gözden kaçırılmamalıdır.

Kişinin hayatı ve beden bütünlüğünün tehlikeye girmesi yalnızca tıbbi tedavi ihtiyacının doğduđu anlarla sınırlı değildir. Örneğin, kişinin kaçırılması, hürriyetinin kısıtlanması gibi hallerde, kişinin kurtarılabilmesi amacıyla gerek hürriyeti kısıtlanan kişinin gerekse şüphelinin taşıdığı telefon, bilgisayar, banka kartları yahut diğler araçlarla yerinin belirlenmesini sağlayacak kişisel verilerin işlenmesi için de açık rıza beyanı aranmayacaktır³³⁹.

4.4.1.2.3. Sözleşme İlişkisi Bağlamında Kişisel Verilerin İşlenmesi

Kanunun 5/2(c) maddesine göre “bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” halinde, veri işleme faaliyeti açık rıza olmaksızın gerçekleştirilecektir. Bu noktada, kanun koyucunun sözleşmenin tarafları arasında menfaat dengesini sağlamaya çalıştığı söylenebilir. Genel olarak kişisel verinin işlenmesi için ilgisinden açık rıza alınmasını şart koşan kural, bir sözleşme söz konusu olduğunda iki tarafın da kanun gereği veri işleyebilmesi yönünde yumuşatılmıştır³⁴⁰.

Burada dikkat edilmesi gereken hususlardan biri, işlenen kişisel verilerin sözleşmenin kurulması ya da ifasıyla doğrudan doğruya ilgili olması gerekliliğidir. Örneğin bir satış sözleşmesinde satım konusu malın teslimi için alıcının adres bilgisinin işlenmesi sözleşmenin ifasıyla doğrudan ilgili ve gereklidir. Bununla birlikte, müşterinin satın aldığı şeylerin kaydedilmek suretiyle, örneğin ilgisine göre yeni ürünler sunmak için müşteri profili oluşturulması satış sözleşmesinin ifasıyla doğrudan ilgili değildir. Her ne kadar müşteri memnuniyeti ve daha fazla satış sözleşmesi için yararlı olsa da bu amaçla veri işlemek bir sözleşmenin kurulması ya da ifasıyla doğrudan doğruya ilgili bulunmadığı ve gerekli olmadığından ilgisinin açık rızası olmaksızın veri işlemek hukuka aykırı kabul edilecektir³⁴¹. Başka bir örnekte, KVK Kurulu, yolcuların şoförler tarafından puanlanması ve verilen puanların ortalamasının alınmak suretiyle işlenmesinin, sözleşmenin ifası bakımından ana kurucu öge olmadığı ve sözleşmenin ifasıyla doğrudan doğruya ilgili de bulunmadığına karar vermiştir³⁴².

Sözleşme, iki ya da daha fazla tarafın hukuki bir sonuç doğurmak amacıyla birbirleri arasında vardıkları anlaşmadır³⁴³. İdare ise çoğunlukla, “idare işlevine ilişkin, kamu gücü kullanarak yapılan tek

³³⁹ Kişisel Verileri Koruma Kurumu, **Madde ve Gerekeşesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, KVKK Yayınları, Mart 2019, Ankara, s. 19.

³⁴⁰ ÇEKİN, s.104.

³⁴¹ Information Commissioner’s Office (ICO), **Guide to the General Data Protection Regulation (GDPR)**, 2019, s. 67; ÇEKİN, s.108.

³⁴² KVK Kurulu 27.1.2020 tarih ve 2020/65 sayılı kararı: <https://www.kvkk.gov.tr/Icerik/6717/2020-65> (E.T. 10.2.2022).

³⁴³ Erol CANSEL / Çağlar ÖZEL, **Borçlar Hukuku Genel Hükümler**, Seçkin Yayıncılık, Cilt:1, 2. Baskı, 2017, s. 62.

yanlı irade açıklamaları”³⁴⁴ şeklinde tanımlanan idari işlemler tesis eder. İdarenin görevlerini yerine getirirken tek taraflı işlemler tesis etmesi esasken, bazı faaliyetleri yerine getirirken iki taraflı sözleşmeler de yapabilir. Hatta Kamu İhale Kanunu uyarınca mal veya hizmet alımları ile yapım işlerinde idarenin sözleşme yapması zorunludur.

İdarenin akdettiği sözleşmeler³⁴⁵, tabi oldukları hukuki rejim ve bu sözleşmelerden doğacak uyuşmazlıklarda görevli yargı yerinin belirlenmesi temelinde özel hukuk sözleşmeleri ve idari sözleşmeler olarak ikiye ayrılmaktadır³⁴⁶. Ancak, özellikle kamu hizmetlerinin gördürülmesine ilişkin yapılan sözleşmelerde, ister özel hukuka isterse de kamu hukukuna tabi olsun, idarenin kamu gücüne dayalı olarak faaliyet yürütmesinden kaynaklanan bazı yetki ve ayrıcalıklara sahip olduğu görülmektedir³⁴⁷. Bu durum özellikle idari sözleşmelerin bir sözleşme türü olmasından ziyade idarenin tesis ettiği “katılma işlem” olduğu eleştirisini doğurmuştur³⁴⁸. Nitekim, sözleşmenin ayrıntılarına ilişkin şartname idare tarafından tek taraflı olarak düzenlenmekte, karşı taraf ise sözleşmenin sadece mali konularına ilişkin kısmına katılmaktadır.

Gerek sözleşmenin şartlarının belirlenmesi süreci gerekse de idarenin çeşitli yetki ve ayrıcalıklarla donatılması bakımından idarenin sözleşmeleri, klasik anlamda tarafların eşit güçteki iradelerinin uyuşmasından doğan özel hukuk sözleşmelerinden farklıdır. Ancak, 6698 sayılı Kanunda “bir sözleşmenin kurulması ya da ifası” denilmek suretiyle idari sözleşme – özel hukuk sözleşmesi ayırımına gidilmemiştir. Ayrıca Kanunda İdare de veri sorumlusu olarak kabul edildiğinden 5/2(c) maddesinin İdarenin yapmış olduğu sözleşmeler için de geçerli olduğu sonucuna varılacaktır. Bu sebeple, kural olarak İdare tarafından akdedilen sözleşmelerde de açık rıza olmaksızın kişisel veri işlenebilmesi için sözleşmenin kurulmasıyla ya da ifasıyla doğrudan ilgili olmak ve gerekli olmak şartlarının bulunması gerekir. Bununla birlikte, Kamu İhale Kanunu’nda olduğu gibi özellikle sözleşmenin kurulma aşamasına ilişkin şartlar çoğunlukla kanunlar çerçevesinde belirlendiğinden, bu aşamada yapılan kişisel veri işleme faaliyetlerinin hukuki temeli 5/2(a) fıkrasına dayandırılabilir. Bu fıkra göre kanunlarda açıkça öngörülmesi halinde açık rıza olmaksızın kişisel verilerin işlenmesi kabul edilmiştir.

³⁴⁴ YILDIRIM, “İdari İşlemler”, içinde: **İdare Hukuku**, Turan Yıldırım (Ed.), On İki Levha Yayıncılık, 8. Baskı, s. 410.

³⁴⁵ YILDIRIM, “İdari İşlemler”, içinde: **İdare Hukuku**, s. 511 vd.; ÖZAY, **Günlük Yönetim**, s. 508 vd.; DURAN, s. 427 vd.; A. Şeref GÖZÜBÜYÜK / Turgut TAN, **İdare Hukuku**, Turhan Kitabevi, 12. Baskı, Ankara, 2018, s. 515 vd.; ULUSOY, **Yeni Türk İdare Hukuku**, s. 359 vd.; Onur KARAHANOGULLARI, **İdarenin Hukukla Kavranması: Yasallık ve İdari İşlemler**, Turhan Kitabevi, 4. Baskı, Ankara, 2018, s. 207 vd.; Zehra ODYAKMAZ, “Genel Olarak İdarenin Sözleşmeleri”, **GÜHFD**, 1998, Cilt: 2, S.:1-2, https://webftp.gazi.edu.tr/hukuk/dergi/2_12.pdf (E.T. 11.2.2022); Ebru ZEYBEK CEBECİ, **Kamu Hizmetlerinin Gördürülmesine İlişkin Sözleşmeler**, Seçkin Yayıncılık, 2021, s. 65 vd.

³⁴⁶ İdari sözleşmeler kamu hukuku rejimine tabi olmakta ve çıkan uyuşmazlıklar idari yargı yerlerinde görülmektedir. Özel hukuk sözleşmeleri ise özel hukuka tabi olup bu tür sözleşmelerden doğan uyuşmazlıklar adli yargıda çözümlenmektedir: ZEYBEK CEBECİ, s.69.

³⁴⁷ Sezin ÖZTOPRAK, “İdari Sözleşmelerde Kamu Gücü Ayrıcalıkları”, **Selçuk Üniversitesi SBE**, Doktora Tezi, 2019, s.54 vd.

³⁴⁸ ÖZAY, **Günlük Yönetim**, s. 511.

Benzer bir durum kamu görevlileri bakımından da mevcuttur³⁴⁹. 657 sayılı Devlet Memurları Kanunu'na göre kamu hizmetleri memurlar, sözleşmeli personel ve işçiler eliyle görülür. Kamuda memur olarak çalışan kişiler ile İdare arasında özel hukuktan aşına olduğumuz şekilde bir iş sözleşmesi bulunmamaktadır. Taraflar arasında sözleşme ilişkisi yerine bunların hak ve yükümlülüklerini belirleyen kanun hükümleri bulunmakta ve İdare tesis ettiği tek yanlı idari işlem ile istihdam oluşturmaktadır³⁵⁰. Dolayısıyla, İdarenin memurlarına ilişkin kişisel veri işlemesi 657 sayılı DMK çerçevesinde mümkündür.

Öte yandan, sözleşmeli personel ve işçiler ile İdare arasında bir sözleşme ilişkisi bulunmaktadır. İşçi statüsünde bulunanlara İş Kanunu hükümleri uygulanacağından bu başlık altında ifade edilen açıklamalar bunlar için de geçerlidir. Yine, İdare ile sözleşmeli personel arasında idari hizmet sözleşmesi imzalanmaktadır³⁵¹. Dolayısıyla, sözleşmedeki yükümlülüklerin yerine getirilmesiyle ilgili olan, eğitim, izin, disiplin gibi bilgilerin kaydedilmesi hukuka uygun kabul edilecektir³⁵².

4.4.1.2.4. Veri Sorumlusunun Hukuki Yükümlülükleri Gereği Kişisel Veri İşlenmesi

6698 sayılı Kanunun 5/2 maddesinin ç bendine göre “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” halinde açık rıza alınmaksızın kişisel veri işlenebilecektir. Kanun gerekçesinde, bir şirketin çalışanlarına maaş ödemelerini yapabilmeleri için banka hesapları, çalışanın medeni durumu, bakmakla yükümlü olduğu kişiler ve eşinin çalışıp çalışmadığına ilişkin bilgileri işlemesi bu duruma örnek olarak verilmiştir³⁵³.

Açık rıza olmaksızın veri işlemenin bu sebeple yapılabilmesi için bir zorunluluğun bulunması gerekir. Veri sorumlusunun ilgili veriyi işlemeksizin hukuki yükümlülüğünü yerine getirebilmesi mümkünse, veri işlemeyi gerektirmeyen bu yöntemi tercih etmelidir. Ayrıca, yükümlülüğü karşılayacak derece veri işlemekle yetinilmesi önemlidir. Örneğin, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 20. maddesinde “*Mahkemeler belirlenen süre içinde lüzum gördükleri evrakın gönderilmesini ve her türlü bilgilerin verilmesini taraflardan ve ilgili diğer yerlerden isteyebilirler. Bu husustaki kararların, ilgililerce, süresi içinde yerine getirilmesi mecburidir.*” düzenlemesine yer verilmiştir. Benzer bir

³⁴⁹ Geniş anlamda kamu görevlisi, istihdam sebebine bakılmaksızın kamuda çalışan herkesi kapsamaktadır. Dar anlamda kamu görevlisi ise, devletin siyasi kısmında bulunanlar ile İş Kanunu'na tabi olarak çalışanlar haricindeki kamu görevlilerini ifade eder. İdare hukukunun konusunu oluşturan bu dar anlamdaki kamu görevlileri kısmıdır: Nur KAMAN, “Kamu Görevlileri”, içinde: **İdare Hukuku**, Turan Yıldırım (Ed.), s. 262; Çınar Can EVREN/İsmail UÇAR, **Kamu Görevlileri Hukuku**, Seçkin Yayıncılık, 2. Baskı, 2020, s. 15 vd.

³⁵⁰ KAMAN, “Kamu Görevlileri”, içinde **İdare Hukuku**, Turan Yıldırım (Ed.), s. 266.

³⁵¹ ULUSOY, **Yeni Türk İdare Hukuku**, s. 603.

³⁵² BAŞAR, s.61.

³⁵³ Kişisel Verileri Koruma Kurumu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, KVKK Yayınları, Mart 2019, Ankara, s. 19.

düzenleme 6100 sayılı Hukuk Muhakemeleri Kanunu’nda da yer almaktadır. Kanunun 221. maddesine göre mahkeme taraflarca ileri sürülen hususların ispatında kullanılması zorunlu olan belgeleri elinde bulunduran üçüncü kişi ya da kurumlara bu bilgilerin ibrazını emreder. Bu emri alan herkes elindeki belgeleri ibraz etmek, edemiyorsa bunun gerekçesini delillendirmek zorundadır. Gerek idari yargı gerekse de adli yargı yerlerinden talep edilen bilgiler kişisel veri içeriyorsa, veri sorumlusunun bu bilgileri mahkemelerle paylaşması yukarıdaki hükümler gereği bir hukuki yükümlülüktür ve kişisel veri sahibinin açık rızasının alınması gerekmez. Bununla birlikte, talep edilen bilgidен fazlasının yargı mercii ile paylaşılması 6698 sayılı Kanuna aykırı olacaktır³⁵⁴.

Belirtmek gerekir ki, “hukuki yükümlülük” kavramının kapsamı Kanunda belirli değildir. Kişinin hukuki yükümlülükleri doğal olarak kanuni bir dayanaktan kaynaklanabileceği gibi bir sözleşmeye dayalı da olabilir. Ancak gerek Direktif’te gerekse de Tüzük’te yer verilen bu düzenlemenin sözleşmeden kaynaklanan yükümlülükleri içermediği ifade edilmektedir³⁵⁵. 6698 sayılı Kanun bakımından da hukuki yükümlülük ifadesinin sözleşmeden kaynaklanan yükümlülükleri kapsamadığı ifade edilmelidir³⁵⁶. Nitekim, Kanunun 5. maddesinin (c) bendinde³⁵⁷ sözleşmeden kaynaklanan kişisel verilerin işlenmesine ilişkin bir düzenleme zaten öngörülmüştür ki bu hükümde sadece sözleşmenin taraflarına ait kişisel verilerin işlenmesinin zorunlu olması halinde açık rızanın alınmasına gerek olmadığı ifade edilerek bilinçli bir sınırlama getirilmiştir. Bu bakımdan, “hukuki yükümlülük” kavramının sözleşmeden kaynaklanan yükümlülükleri de içerdiği kabul edilirse sözleşmenin tarafı olmayan üçüncü kişilerin de kişisel verisinin işlenebilmesi durumu ortaya çıkar ve (c) bendinin kapsamı genişlemiş olur; çünkü (ç) bendinde üçüncü kişilerin verilerinin işlenmesine yönelik bir sınırlama bulunmamaktadır. Ayrıca, sözleşme bağlamında tarafların yükümlülüğü sözleşmenin ifasıdır. Eğer sözleşmenin ifası (ç) bendi bağlamında “hukuki yükümlülük” kapsamında kabul edilirse kanun koyucunun aynı konuyu (c) ve (ç) bendinde tekraren düzenlemiş olduğu sonucu doğabilir. Bu durumun hukuk mantığıyla çelişeceği açıktır. Dolayısıyla, kural olarak veri sorumlusunun mevzuattan kaynaklanan hukuki yükümlülükleri nedeniyle açık rıza olmaksızın veri işleyebileceği söylenebilir.

³⁵⁴ Bu şekilde yapılacak veri paylaşımı Kanunun 4. maddesinin ç bendi belirlenen kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü şekilde işlenmesi ilkesine aykırılık teşkil edecektir: <https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik>- (E.T. 10.3.2022)

³⁵⁵ Waltraut KOTSCHY, “Article 6 Lawfulness of Processing”, **The EU General Data Protection Regulation (GDPR) A Commentary**, Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY (Eds.), Oxford University Press, 2020, s. 332. Öte yandan Direktif’in 7(c) maddesinin ilk halinin “ulusal veya AB yasalarından kaynaklanan yükümlülükler” şeklinde olmasına rağmen son halinin “hukuki yükümlülükler” olarak belirlendiği ifade edilmiştir. KOTSCHY, s.332, dn.35.

³⁵⁶ Aynı yönde görüş için bkz.: ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, s.83; Furkan Güven TAŞTAN, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, On İki Levha, 2. Baskı, 2017, s. 170, dn.56. Aksi yönde görüş için bkz.: ERARSLAN, s.285.

³⁵⁷ “(c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.”

Burada mevzuat ifadesinden, kanunlar, kanun hükmünde kararnameler, yönetmelikler ve idare tarafından çıkarılan diğer düzenleyici işlemler anlaşılmalıdır³⁵⁸.

Kişisel verilerin korunması hakkı Anayasa’da güvence altına alınan temel hak ve özgürlüklerden biridir. Dolayısıyla, bu verilerin işlenmesine yönelik bir yükümlülük Anayasanın 13. maddesi gereği kanunla getirilmelidir. Anayasa Mahkemesinin son kararları ışığında, temel hak ve özgürlüklerin kanunla sınırlandırılmasında ilgili kanuni düzenlemenin yeterince güvenceyi içermesi ve hakkın kapsamını açıkça belirlemesi gerektiği söylenebilir. Bu bağlamda Anayasa Mahkemesi, Anayasada kanunla düzenlenmesi öngörülen hususlara ilişkin kanuni düzenlemelerde temel esasların, ilkelerin belirlenmesini ve çerçevenin çizilmiş olmasını aramaktadır³⁵⁹.

“Yürütmenin türevselliği ilkesi gereğince, yürütme organının bir konuda düzenleme yapabilmesi için yasama organınca yetkilendirilmesi gerekmektedir. Kural olarak, kanun koyucunun genel ifadelerle yürütme organını yetkilendirmesi yeterli olmakla birlikte, Anayasa’da kanunla düzenlenmesi öngörülen konularda genel ifadelerle yürütme organına düzenleme yapma yetkisi verilmesi, yasama yetkisinin devredilmezliği ilkesine aykırılık oluşturabilmektedir. Bu nedenle, Anayasa’da temel hak ve özgürlüklerin sınırlandırılması, vergi ve benzeri mali yükümlülüklerin konması ve memurların atanmaları, özlük hakları gibi münhasıran kanunla düzenlenmesi öngörülen konularda, kanunun temel esasları, ilkeleri ve çerçeveyi belirlemiş olması gerekmektedir. Anayasa koyucunun açıkça kanunla düzenlenmesini öngördüğü konularda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamaz.”³⁶⁰

Bu sebeple, kararda belirlenen kriterlere uygun bir kanunla veya bu kanuna dayanarak çıkarılan düzenleyici işlemlerle kişisel verilerin işlenmesi yönünde hukuki yükümlülük öngörülmesi mümkündür.

³⁵⁸ “İlgili kişi ile hastane görevlileri arasında yaşanan tartışma neticesinde yaşanan olayla ilgili hastane görevlilerince tutanak tutulduğu, sonrasında hastane görevlilerince ilgili kişi hakkında Savcılığa suç duyurusunda bulunulduğu, bu kişilerce kamu gücü kullanılarak açık rızası olmaksızın ad, soyad ve T.C. kimlik numarası bilgilerinin hastane verilerinden alınarak olay yeri tutanağına 1 yıl 3 ay sonra işlendiği, bu şekilde temel hak ve özgürlüklerinin ihlal edildiği gerekçesiyle hastaneye başvurduğu; hastanenin vermiş olduğu cevapta ise, ilgili kişinin babasının tedavisinin eksiksiz planlanıp yapıldığı, olay ile ilgili tutanağın 1 yıl 3 ay sonra değil, olayla aynı gün tutulduğu, Sağlık Bakanlığı Hukuk Müşavirliği Hukuki Yardım ve Beyaz Kod Uygulamasına dair 2016/3 Genelgesine göre işlem başlatılarak Cumhuriyet Savcılığına bildirildiği; ayrıca Kanunun 6 ncı maddesi uyarınca kişisel verilerin, hastane kapsamında sır saklamakla yükümlü bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından paylaşıldığı yanıtları karşısında ilgili kişinin Kuruma yaptığı şikâyet başvurusunun, veri sorumlusundan alınan bilgi ve belgeler ve yukarıda belirtilen hukuki gerekçeler çerçevesinde incelenmesi sonucunda; söz konusu kişisel verilerin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendi uyarınca veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi kapsamında işlendiği kanaati olduğundan, söz konusu şikâyete ilişkin Kanun kapsamında yapılacak bir işlem olmadığına karar verilmiştir.” KVK Kurulu, 27.1.2020 tarih ve 2020/63 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6870/2020-63> (E.T. 10.3.2022).

³⁵⁹ Ayrıntılı bilgi için bkz.: SEVER, s.204 vd.

³⁶⁰ AYM, E.2013/50, K.2015/38, T.1.4.2015.

Anayasa Mahkemesi’nce verilen bir kararda, 663 sayılı KHK’nın 47. maddesinde Sağlık Bakanlığı ve bağlı kuruluşlarının “mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıta ile toplamaya, işlemeye ve paylaşmaya” yetkili olduklarına yönelik düzenlemeye ilişkin Mahkeme:

“... kişisel bilgilerin "her türlü vasıta ile" toplanmasına, işlenmesine ve paylaşılmasına izin verilmesi, sınırlamayı, öngörülme amacının ötesinde kişisel bilgilerin gizliliğinin keyfi şekilde ihlal edilmesi sonucunu doğurabilecek bir araca dönüştürmektedir. Bu ise sınırlama aracıyla sınırlama amacı arasında bulunması gereken makul dengeyi bozmakta, özel hayatın ve kişisel verilerin korunmasını isteme haklarına kuralda belirtilen sınırlama amacı dışında ölçüsüz bir şekilde müdahale edilebilmesine imkân tanımaktadır” gerekçesiyle hükmün Anayasanın 2., 13. ve 20. maddelerine aykırı olduğuna karar vermiştir³⁶¹.

Aynı maddenin 3. fıkrasında ise "Bakanlık ve bağlı kuruluşları mevzuatla kendilerine verilen görevleri yerine getirebilmek amacıyla gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye” yetkili kılınmış ve istenen bilgileri elinde bulunduranlar bu bilgileri vermekle yükümlü tutulmuştur. Bu hükme ilişkin olarak Mahkeme, bakanlık ve bağlı kuruluşlarına verilen görevlerin çok geniş olduğunu, bu görevlerin tamamının kişilerin özel hayatlarına müdahale edilmesini gerektirecek bir toplumsal zorunluluk barındırmadığını, bu sebeple, demokratik toplum düzeninin zorunlu kıldığı hallerle sınırlı tutulmayan bu düzenlemenin ölçülülük ilkesine aykırılık taşıdığını ifade ederek ilgili kanun hükmünün Anayasanın 2., 3. ve 20. maddelerine aykırı olduğuna karar vermiştir (§102).

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu’nun 78. maddesinin 2. fıkrasında, genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilere ait sağlık bilgilerinin ne şekilde korunacağı ve ulusal güvenlik nedeniyle sağlık bilgisi paylaşımına açılmayacak kişilerin tespitinin Çalışma ve Sosyal Güvenlik Bakanlığı tarafından yapılacağı ve yine bu kişi ve grupların sağlık bilgilerinin nasıl tutulacağının Bakanlıkça hazırlanan Yönetmelikle belirleneceği düzenlenmiştir. Bu düzenlemeye ilişkin verilen kararda AYM, yasama yetkisinin devredilmezliği ilkesi uyarınca Anayasa’da açıkça kanunla düzenlenmesi öngörülen konularda yürütme organına doğrudan ilk elden düzenleyici işlem yapma yetkisi verilemeyeceği, ancak söz konusu kanun hükmüyle Sosyal Güvenlik Kurumu’na elde edilen sağlık bilgilerinin korunması, paylaşılması ve tutulmasına yönelik usul ve esasları belirleme yetkisinin Bakanlığa bırakıldığını, bu durumun Anayasa’nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine

³⁶¹ AYM, E. 2013/114, K. 2014/184, T.4.12.2014, § 99.

ilişkin güvenceye aykırı olduğu gerekçesiyle ilgili kanun hükmünün Anayasaya uygun olmadığına karar vermiştir³⁶².

Kişisel verilerin işlenmesine yönelik hukuki yükümlülüklerin İdare tarafından çıkarılacak düzenleyici işlemlerle öngörülmesi de mümkündür. Ancak, elbette düzenleyici işlemlerin Kanunlara uygun olarak düzenlenmesi gerekir³⁶³. Örneğin, 5253 sayılı Dernekler Kanunu uyarınca çıkarılan ve 31.3.2005 tarihli Resmi Gazete’de yayımlanan Dernekler Yönetmeliği’nde dernek başkanının ad soyad bilgileriyle üyelerin gerçek ve tüzel kişi kadın ve erkek olarak sayıları beyan edilmesi öngörülmüşken, 1.10.2018 tarihinde yapılan bir değişiklikle derneklere, kişilerin dernek üyeliğine kabul edilme, üyelikten çıkma veya çıkarılma durumlarını ve gerçek kişi üyelerin ad, soyad, T.C. kimlik numarası, mesleği, öğrenim durumu bilgilerinin Dernek Beyannamesine kaydının yapılması zorunluluğu getirilmiştir. Değişikliğin yapıldığı tarihte Dernekler Kanunu’nun “Beyanname verme yükümlülüğü ve denetim” başlıklı 19. maddesinde “*Dernekler, yıl sonu itibarıyla faaliyetlerini, gelir ve gider işlemlerinin sonuçlarını düzenleyecekleri beyanname ile her yıl Nisan ayı sonuna kadar mülkî idare amirliğine vermekle yükümlüdürler. Beyannamenin düzenlenmesine ilişkin esas ve usuller yönetmelikte düzenlenir*” kuralı yer almaktadır. Söz konusu Yönetmelik değişikliğinin dava edilmesi üzerine yaptığı değerlendirmede Danıştay, kişilerin dernek üyeliği, ad-soyad, kimlik numarası, meslek ve öğrenim bilgilerinin kişisel veri niteliğinde olduğunu, bu bilgilerin işlenebilmesi için 6698 sayılı Kanun uyarınca kural olarak ilgililerden açık rıza alınması gerektiğini, aksi halde verilerin işlenemeyeceğini, değişikliğin yürürlüğe girdiği tarihte Yönetmeliğin de dayanağı olan Dernekler Kanunu’yla derneklere getirilen beyanname verme yükümlülüğünün kapsamının derneklerin yıllık faaliyetleri ile gelir ve gider işlemlerinin sonuçlarıyla sınırlandırıldığını, dolayısıyla İdareye tanınan düzenleme yetkisinin yalnızca belirlenen kapsamın esas ve usullerini düzenlemekle sınırlı olduğunu belirlemiştir. Dernek üyelerine ait kişisel veri ve özel nitelikli kişisel verilerin dernek faaliyetleri kapsamında değerlendirilmesinin mümkün olmadığını ifade eden Danıştay, söz konusu Yönetmelik hükmünün hukuka aykırı olduğuna karar vermiştir³⁶⁴.

³⁶² AYM, E. 2014/74, K. 2014/201, T.25.12.2014.

³⁶³ Bununla birlikte, idari işlemler hukuka uygunluk karanesinden yararlandığı için İdare tarafından kanuna uygun olmayan düzenleyici işlemler tesis edilmiş olsa da İdari yargı yerlerince iptal edilmedikçe bu düzenlemeler hukuken geçerli kabul edilecek ve bunlarda öngörülen yükümlülükler bağlamında açık rıza olmaksızın kişisel veriler işlenebilecektir. İdari işlemlerin hukuka uygunluk karanesinden yararlanmasına ilişkin bkz.: Esengül ALBAYRAK SEKBAN, “İdari İşlem: Hukuka Uygunluk Karanesi”, **İstanbul Barosu Dergisi**, C.92, S.3, Mayıs 2018, s. 354-369; İsmail UÇAR, “İdare Hukukunda Kamu Gücü Ayrıcalığı Kavramı ve Bir Kamu Gücü Ayrıcalığı Olarak Hukuka Uygunluk Karanesi”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XX, S.3, 2016, s. 331-373.

³⁶⁴ Danıştay 10.D., E. 2018/5213, K. 2021/1859, <https://karararama.danistay.gov.tr/>. Nitekim, söz konusu Yönetmelik değişikliğinin Danıştay’da incelenmesi devam ederken Dernekler Kanunu’nun 23. maddesi şu şekilde değiştirilmiştir: “*Dernekler, genel kurulu izleyen otuz gün içinde, yönetim kurulu ve denetim kurulu ile derneğin diğer organlarına seçilen asıl ve yedek üyeleri, üyeliğe kabul edilenler ile üyeliği sona erenlerin adını, soyadını, doğum tarihini ve kimlik numarasını kabul edilme ve sona erme tarihinden itibaren kırk beş gün içinde merkezinin bulunduğu dernekler birimine bildirmekle yükümlüdür. Dernek organlarında ve yerleşim yerinde meydana gelen değişiklikler de aynı usule tâbidir. Genel kurul sonuç bildirimi ile üyeliğe ilişkin bildirimlerin şekli, içeriği ve gerekli belgeler yönetmelikte düzenlenir.*” Dikkat edilirse yeni düzenlemede üyelere

- CBK'lar ile Kişisel Verilerin İşlenmesini Zorunlu Kılan Hukuki Yükümlülüklerin

Öngörülmesi: Kişisel verilerin işlenmesini gerektirecek bir hukuki yükümlülüğün doğrudan CBK ile öngörülmesinin mümkün olup olmadığı da irdelenmesi gereken konular arasındadır. 27.3.2018 tarih ve 14 no'lu İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 17. maddesinin 2. fıkrasında, Başkanlığın görevleriyle ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden isteyebileceği, kendisinden bilgi istenenlerin de bu bilgileri belirlenen süre içerisinde vermekle yükümlü olduğu belirlenmiştir. Bu maddenin “gerekli gördüğü bilgileri” ibaresinin iptalinin incelendiği kararda, Başkanlığa verilen görevlerin yerine getirilebilmesi için görevleriyle sınırlı olarak bilgi talep edebilmesinin zorunlu olduğu, itiraz konusu kuralın 6698 sayılı Kanunun uygulanmasını engelleyen, daraltan, genişleten ya da bu hükümlere temas eden bir yanının bulunmadığı, dolayısıyla Anayasanın 20. maddesiyle ilgisi bulunmayan bu düzenlemenin konu bakımından yetki yönünden Anayasaya aykırı olmadığına çoğunluk görüşüyle karar verilmiştir³⁶⁵.

Karar gerekçesinden anlaşılacağı üzere, AYM çoğunluk görüşü, CBK ile yapılan ve İletişim Başkanlığı'nın tüm kamu kurum ve kuruluşlarından, gerçek ve tüzel kişilerden görevleriyle ilgili gerekli gördüğü bilgileri isteyebilmesine ilişkin düzenlemenin “kişisel verilere ilişkin bir düzenleme içermediği” yönündedir. Ancak bu görüş eleştiriye açıktır. Nitekim, AYM'nin bir başka kararında ifade ettiği üzere “devletin yetkili temsilcileri tarafından ilgililer hakkında rızaları olmaksızın bilgi toplanmasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur”³⁶⁶

Bunun yanı sıra, AYM bir kararında kurumlar tarafından bilgi talep edilmesi hususunu Anayasanın 13. ve 20. maddeleri bağlamında incelemiştir³⁶⁷. Örneğin, 5809 sayılı Elektronik Haberleşme Kanunu'nun 60. maddesine eklenen 11 no'lu fıkra da yer verilen “(Bilgi Teknolojileri ve İletişim) Kurumu, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir... Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık,

ait meslek ve öğrenim bilgisi verilerinin işlenmesi öngörülmemiştir. Bu haliyle düzenlemenin amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine daha uygun olduğu söylenebilir.

³⁶⁵ AYM, E. 2018/134, K. 2021/13, T.3.3.2021, § 24-25.

³⁶⁶ AYM, E. 2014/87, K. 2015/112, T.8.12.2015, §170.

³⁶⁷ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 3. maddesinin (4) numaralı fıkrasında yer alan “Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verilir.” şeklindeki hükmün iptali için yapılan başvuruda Kuruma verilecek bilginin kişisel verileri de içereceği kararda şu şekilde ifade edilmiştir: “Dava konusu kuralda geçen trafik bilgisi, 5651 sayılı Kanun'un 2. maddesinin (j) bendinde, taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri şeklinde tanımlanmıştır. Dolayısıyla trafik bilgisi adı altında istenen bilgiler genel anlamda belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade eden kişisel veri kavramı içerisindedir.” AYM, E. 2014/149, K. 2014/151, T.2.10.2014.

kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir.” şeklindeki hükmün iptalinin incelendiği kararda AYM, dava konusu kuralların kişisel verileri içeren bir düzenleme olduğunu şu şekilde ifade etmektedir:

“Dava konusu kurallar, Kuruma, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilme ve bunların değerlendirmesini yapabilme; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilme, bunlarla irtibat kurabilme ve bu kapsamda diğer gerekli önlemleri alabilme veya aldırabilme konularında yetki tanımakta ve bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebinin ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilmesini öngörmektedir. Kurumun yetki ve talebine konu bilgiler genel anlamda belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade eden kişisel veri kavramı kapsamındadır.”³⁶⁸

Anayasanın 104/17. maddesinde Cumhurbaşkanına tanınan yürütmeye ilişkin kararname çıkarma yetkisinin yanında diğer maddelerinde bazı konuların da yine CBK ile düzenleneceği kabul edilmiştir. Buna göre, üst düzey kamu yöneticilerinin atanmalarına ilişkin usul ve esaslar (md. 104/9), bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatının kurulması (md. 106/11), Devlet Denetleme Kurulunun işleyişi, üyelerinin görev süresi ve diğer özlük işleri (md. 108/4) ve Milli Güvenlik Kurulu Genel Sekreterliği’nin teşkilatı ve görevleri (md.108/6) CBK’lar ile düzenlenecektir.

Bu hususta tartışma konusu olan kısım, CBK ile bir bakanlığa temel hak ve özgürlükleri sınırlandıran görev ve yetkilerin verilir verilemeyeceğidir. Bu konuda bizim de katıldığımız öğretideki çoğunluk görüşü, Anayasada CBK ile düzenlenmesi öngörülen dört farklı konuda çıkarılacak CBK’ların da Anayasanın 104/17. maddesine tabi olduğunu, Anayasanın 13. maddesine göre temel hak ve özgürlüklerin ancak kanunla sınırlandırabileceğini, 104/17 maddesinde münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılamayacağı kabul edildiğinden CBK’larla temel hak ve özgürlüklerin sınırlandırılmasını öngören bir düzenlemenin yapılamayacağını kabul etmektedir³⁶⁹.

Anayasanın 20/3. maddesinde “Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir” kuralına yer verilmiş, 13. maddesinde ise “Temel hak ve hürriyetler, ... ancak kanunla sınırlandırılabilir” kuralı kabul edilmiştir. Dikkat edilirse birinde “düzenlemek” diğerinde “sınırlamak” ifadeleri kullanılmıştır. Temel hak ve özgürlüklerin sınırlandırılması aynı zamanda düzenlenmesi anlamına da gelirken, yapılan her düzenlemenin sınırlama anlamına gelmeyeceği ifade edilmektedir. SAĞLAM’a göre sınırlamanın yapılıp yapılmadığı her düzenleme için ayrı ayrı tespit edilmelidir. Buna göre, bir

³⁶⁸ AYM, E. 2017/16, K. 2019/64, T.24.7.2019, §55.

³⁶⁹ YASİN, “Cumhurbaşkanlığı Kararnamelerinin Türk İdari Teşkilat Hukukuna Etkileri”, s.325; Osman CAN, “Cumhurbaşkanlığı Kararnamelerinin Hukuki Rejimi ve Anayasa Mahkemesi Yaklaşımı”, *Anayasa Yargısı*, C.37, S.1, 2020, s.156; Ali ULUSOY, “Cumhurbaşkanlığı Kararnameleri: Varoluşsal, Yapısal ve Hukuksal Bir Değerlendirme”, *Anayasa Yargısı*, C.37, S.2, 2020, s. 58 vd.

düzenleme belli bir hak veya özgürlüğün güvence altına aldığı yaşam alanını, başka bir deyişle norm alanını daraltıyorsa burada aynı zamanda bir sınırlama da söz konusuyken, hakkı güçlendiren, onun daha kolay ve etkin şekilde kullanılmasını sağlayan düzenleme sınırlayıcı olmaz³⁷⁰.

14 No’lu CBK düzenlemesi bu açıdan değerlendirildiğinde karşımıza çıkan sonuç şudur: CBK’nın 3. maddesinde İletişim Başkanlığı’na “basın-yayın kuruluşu mensuplarına basın kartı düzenlemek” ve “Türkiye Medya Veri Tabanını oluşturmak” gibi görevler verilmiştir. Düzenlemenin 17. maddesinin 2. fıkrasında ise Başkanlığın görevleriyle ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden isteyebileceği, kendisinden bilgi istenenlerin de bu bilgileri belirlenen süre içerisinde vermekle yükümlü olduğu belirlenmiştir. İletişim Başkanlığı’nın görevleri dikkate alındığında gerekli gördüğü bilgilerin kişisel veri içereceği kuşkusuzdur. Dolayısıyla, kişisel verileri elinde bulunduranlara Başkanlıkla paylaşma yükümlülüğü getirilmesinin kişisel verilerin korunması hakkına getirilen bir sınırlama niteliğini taşıdığı kabul edilmelidir. Sonuç olarak, 14 No’lu CBK’nın 17/2. maddesinde yer verilen düzenleme ile kişisel verilerin korunması hakkı sınırlanmış olduğundan bu hükmün Anayasanın 13. maddesine aykırı olduğu kabul edilmelidir.

4.4.1.2.5. Kişisel Verilerin İlgili Kişi Tarafından Alenileştirilmesi

Kanunun 5/2(d) maddesine göre kişinin kendisi hakkındaki kişisel verileri alenileştirmiş olması halinde söz konusu veriler ilgisinden açık rıza alınmaksızın işlenebilir. İlgili madde metninin gerekçesinde bu durum, ilgili kişi tarafından herkesçe bilinir hale getirilen verilerin işlenmesinde korunması gerekli hukuki yararın ortadan kalkması gerekçesine dayandırılmıştır.

Alenileştirme, kişinin kendisine ait kişisel verilerini kendi rızasıyla toplumda bilinir kılması şeklinde ifade edilebilir. Nitekim, özellikle sosyal medya kullanıcılığının önemli ölçüde arttığı günümüzde kişiler fotoğraflarını, çeşitli alışkanlıklarına ilişkin bilgilerini, siyasi görüşlerini kendi rızalarıyla sosyal medya platformlarında paylaşmaktadır. Peki kişisel veri olarak kabul edilen bu bilgiler insanların kendi rızalarıyla alenileştirilmesi nedeniyle koruma kapsamı dışında kalacak mıdır?

Kişinin kendi rızasıyla alenileştirdiği kişisel verilerin işlenmesi için ilgili kişiden açık rıza alınması gerekli değilse de bu veriler işlenirken Kanunun 4. maddesinde sayılan genel ilkelere riayet edilmesi gerektiği vurgulanmalıdır. Nitekim, kişinin kendisine ait verisini paylaşmış olması halinde yalnızca açık rıza beyanı gerekliliği ortadan kalkmakta, Kanunun diğer koruyucu hükümleri etkisini sürdürmektedir. Bu bağlamda, 4. maddede sayılanlardan biri olan “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesi gereğince ilgisince alenileştirilmiş kişisel verinin de alenileştirme sebebiyle

³⁷⁰ Fazıl SAĞLAM, **Temel Hakların Sınırlanması ve Özü**, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1982, Ankara, s. 21.

bağlı, bu sebeple sınırlı ve ölçülü şekilde işlenmesi gerekir³⁷¹. KVK Kurulu da aynı görüştedir. Kurul tarafından verilen bir karara³⁷² konu olayda mesleğine ilişkin danışılması amacıyla iletişim bilgilerini internet ortamında paylaşmış olan şikâyetçi, bir Sigorta Şirketi tarafından sigortacılık faaliyetleri kapsamında arandığı için kuruma şikâyet başvurusunda bulunmuştur. Sigorta şirketi, kişiye ait telefon numarasını herkese açık şekilde görülen bir web sitesinden aldığını ve bu bilginin ilgili kişinin kendi iradesiyle alenileştirildiğini, dolayısıyla bu bilgiyi kullanmasının hukuka uygun olduğu savunmasını yapmıştır. Ancak Kurul, kişisel verinin işlenmesindeki açık rıza zorunluluğunu ortadan kaldıran “alenileştirme” eyleminin amacı ile verinin işlenme amacının aynı olması gerektiği, bu sebeple kişinin profesyonel bilgisine başvurmak amacı dışında şirket faaliyetleri kapsamında randevu oluşturmak amacıyla, söz gelimi araç kaskosu sözleşmelerindeki kampanyalar hakkında aranmasının Kanunun 5/2(b) maddesi uyarınca hukuka aykırı olduğuna karar vermiştir.

Karardan anlaşılacağı üzere, örneğin bir web sitesinde avukat olduğu ve danışılmak istenmesi halinde kendisine ait irtibat numarası ve adres bilgilerini paylaşan kişiye bu amaç dışında bir faaliyet için ulaşılması, bu bilgilerin kayıt altına alınması, paylaşılması; kısaca bu kişisel bilgilerin işlenmesi hukuka aykırı kabul edilecektir³⁷³. Örneğin, bu kişinin sağlık merkezince genel sağlık bakımı hizmetlerinde yapılan indirimin reklamı için aranması hukuka aykırı olacağı gibi, aynı kişinin sağlık merkezince baro ile yapılan bir anlaşma gereği avukatlara yapılan indirim kampanyası hakkında aranması da hukuka aykırı kabul edilmelidir. Çünkü, kişinin adı soyadı, irtibat numarası ve mesleki bilgisi gibi kişisel verileri ilgisinin kendisi tarafından avukatlık mesleğine uygun şekilde, hukuki uyumsuzluklara ilişkin danışmanlık ihtiyacı duyulması halinde ulaşılır olmak için alenileştirilmiştir. Ancak, verilen örnekte sağlık merkezi bu amaçla bağlantısı olmayan başka bir amaçla, sağlık hizmetlerinde yapılan avukatlara özel bir kampanya hakkında reklam yapmak amacıyla söz konusu verileri işlemektedir. Dolayısıyla bu işleme faaliyeti Kanunun 5. maddesinin 2(d) fıkrası kapsamında kabul edilemeyeceği için hukuka aykırı olacaktır.

Öte yandan, ilgilinin hakkındaki kişisel veriyi alenileştirdiğinin kabulü için kişisel verinin ilgisinin iradesi ile kamuoyunda bilinir hale gelmesi gerekir. Onun isteği dışında kişisel verinin herkes tarafından bilinir hale gelmesi yahut topluma açık bir yerde olmakla birlikte ilgisinin kişisel verisini alenileştirme niyetini taşıması halinde o verinin “alenileştiği” gerekçesiyle ilgisinin açık rızası alınmaksızın işlenmesi mümkün değildir. Kurum tarafından yapılan kamuoyu duyurusunda da bu husus şu şekilde ifade edilmiştir: *“Bu çerçevede, kişisel verinin, aleni kabul edilebilmesi için öncelikle ait olduğu kişinin aleni olmasını istemesi, başka bir ifade ile bu yönde bir iradesinin var olması gerekir.*

³⁷¹ KÜZECİ, **Kişisel Verilerin Korunması**, s.346; ERARSLAN, s.288.

³⁷² KVK Kurulu, 7.11.2019 tarih ve 2019/331 sayılı kararı, <https://kvkk.gov.tr/Icerik/6623/2019-331> (E.T. 25.8.2021).

³⁷³ Tüzel kişilere ait kişisel verilerin ilgili kanunlar gereği yahut kendilerince alenileştirilmiş olmasının ya da açık sicillerde yer almış olmasının, söz konusu verilerin ticari amaçlarla üçüncü kişilere aktarımına rıza gösterdiği anlamına gelmeyeceği hususunda bkz.: AYM, E.2013/84, K.2014/183, T. 4.12.2014. Karara ilişkin değerlendirme için bkz.: “**1.2. İlgili Kişi**” başlığı.

Bu anlamda tek başına kişisel verinin kamuoyuna açık hale gelmesi, örneğin herkesin görebileceği bir yerde olması ya da herkesin erişimine açık durumda bulunması alenileştirilmiş olması bakımından yeterli olmamakta; eylemin, ilgili kişinin iradesi ile de desteklenmesi gerekmektedir. Kişinin iradesi dışında bir sebeple kişisel verinin kamuoyuna açıklandığı durumlarda Kanun kapsamında bir alenileştirmeden söz etmek mümkün olmayacaktır.”³⁷⁴

4.4.1.2.6. Bir Hakkın Tesisi, Kullanılması veya Korunması Amacıyla Veri İşleme

Kanunda açık rıza olmaksızın kişisel veri işlenebilmesinin istisnalarından biri de “*bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması*”dır. Kanunun gerekçesinde “*bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasiinin veya kayyımın, kısıtlının mali bilgilerini tutması*” halleri bu duruma örnek olarak verilmiştir³⁷⁵. Benzer şekilde, işverenin davalı olduğu eski işçisine ait verileri dava zamanaşımı boyunca saklaması, tapuda yapılacak tescil işlemlerinde kişisel verilerin kullanılması da bu kapsamda hukuka uygun sayılacaktır³⁷⁶. İdarenin kamu görevlisine ilişkin atama ve terfi işlemlerini gerçekleştirirken ilgiliye ilişkin kişisel verileri işlemesi de bir hakkın tesisini sağlamak bakımından hukuka uygundur.

Kanun hükmünde gözden kaçırılmaması gereken husus, veri işleme faaliyetinin hakkın tesisi, kullanılması ya da korunması bakımından bir zorunluluk teşkil etmesidir. Bu bakımdan, kişisel verinin paylaşımından başka bir seçeneğin bulunması durumunda bu seçenek tercih edilmelidir. Ayrıca, hakkın korunmasını sağlayacak derecede verinin işlenmesi hukuka uygun kabul edilirken gerekenden fazla kişisel verinin işlenmesi, Kanunun 4. maddesinde belirlenen kişisel verilerin “*işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma*” ilkesine aykırılık teşkil edecektir.

4.4.1.2.7. Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlemesi: İdari Faaliyetlerde Meşru Menfaatin Yeri

Kanunun 5/2(f) maddesine göre “*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*” halinde ilgisinden açık rıza alınmaksızın kişisel veri işlenebilecektir. Kanun gerekçesinde bu kurala ilişkin şu örneğe yer verilmiştir: “*Bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, çalışanların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesi gibi amaçlarla*

³⁷⁴ Kişisel Verileri Koruma Kurumu, “Alenileştirme” Hakkında Kamuoyu Duyurusu, <https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU> (E.T. 25.8.2021).

³⁷⁵ Kişisel Verileri Koruma Kurumu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, s. 20.

³⁷⁶ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, KVKK Yayınları, s. 4.

kişisel verileri işleyebilecektir. Bu durumda, kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi gerekmektedir.”

Kanunda meşru menfaat kavramının tanımına yer verilmemiştir. Ancak, Kurum tarafından hazırlanan terimler sözlüğünde meşru menfaat, “*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla gerçekleştirilecek işleme faaliyetinde, veri sorumlusunun elde edeceği faydanın meşru, etkin, belirli ve mevcut bir menfaatine ilişkin olması*” şeklinde tanımlanmıştır³⁷⁷. Meşru menfaat, hukuk düzeni içerisinde korunan, hukuka aykırı olmayan menfaat anlamına gelir. Örneğin, bir şirketin devralınmasında, şirketi devralacak kişinin, şirketin güncel durumuna ilişkin bilgi sahibi olmak amacıyla kişisel verileri de içeren bazı bilgileri incelemesi, ölçülü olması ve gerekli güvenlik önlemlerinin de alınması şartıyla meşru menfaat kapsamında kabul edilebilecektir³⁷⁸. Başka bir örnekte, veri sorumlusu şirket, hatalı akaryakıt dolumlarının önüne geçmek için “araç tanıma projesi” kapsamında ilgililere ait plaka ve akaryakıt tipi verilerini meşru menfaat kapsamında kullanma talebiyle Kuruma başvuruda bulunmuştur. Kurul, yanlış ürün ikmalinden kaynaklanan araç arızalarından dolayı 6502 sayılı Tüketicinin Korunması Hakkında Kanun uyarınca işletici ile birlikte dağıtıcı şirketin de sorumluluğunun bulunması, bu bağlamda ortaya çıkan zararın hem tüketicinin hem de dağıtıcının maddi kaybı ile şirketin marka değeri ve hizmet kalitesinde kayıplara neden olması dikkate alınarak, veri sorumlusu şirketin tüketicilere ait plaka ve ürün tipi bilgilerini işleminin “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” kapsamında olduğuna karar vermiştir³⁷⁹.

Yine aynı kararda Kurul, kişisel verinin meşru menfaat kapsamında işlenebilmesi için göz önünde bulundurulması gereken kriterlere de değinmiştir. Buna göre, kişisel verinin işlenmesiyle elde edilecek menfaat ilgili kişinin temel hak ve özgürlükleriyle yarışabilir düzeyde olmalıdır. Söz konusu menfaate erişilebilmesi için ilgilinin kişisel verilerinin işlenmesinin zorunlu olması da gereklidir. Başka bir yöntemle kişisel veri işlenmeksizin aynı yarar sağlanabiliyorsa bu yöntem tercih edilmelidir. Veri sorumlusunun gelecekte elde edeceği bir yarar amacıyla da veri işleme hukuka aykırı kabul edilecektir. Başka bir deyişle meşru menfaat kişisel verinin işleneceği anda mevcut, belirli ve açık olmalıdır. Ayrıca, meşru menfaatin sadece ekonomik yarara ilişkin olmasından ziyade çok sayıda kişiyi etkileyen, iş süreçlerini ya da bir işleyişi kolaylaştıracak tarzda, şeffaf ve hesap verilebilir nitelikte olması

³⁷⁷ Kişisel Verileri Koruma Kurumu, **Madde ve Gerekeşi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, s. 114. “Meşru menfaat” ifadesinin tanımında hem “meşru” hem de “menfaat” kavramlarına yer verilmesinin iyi bir tanımlama yöntemi olmadığı ifade edilmelidir. Öte yandan, meşru menfaat kavramı, İdari Yargılama Hukukunda da yer alan bir terimdir. 2577 sayılı İdari Yargılama Usulü Kanunu’nun 2.maddesinin (a) fıkrası uyarınca, tesis edilen bir idari işlemle menfaati ihlal edilen kişi, bu işleme karşı iptal davası açabilir. Burada bahsi geçen menfaat, “kişi ile idari işlem arasında bulunan meşru, güncel ve makul bir ilgi/bağ” şeklinde tanımlanmaktadır. Menfaat hukuk düzenine aykırı değilse meşru kabul edilmektedir. Konuya ilişkin ayrıntılı bilgi için bkz.: Turan YILDIRIM/Gül FİŞ ÜSTÜN, **Açıklamalı-Notlu İdari Yargılama Usulü Kanunu**, On İki Levha Yayıncılık, İstanbul, Ekim 2020, s. 24 vd.

³⁷⁸ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 13.

³⁷⁹ KVK Kurulu, 25.3.2019 tarih ve 2019/78 sayılı kararı.

aranmaktadır. Meşru bir menfaat gereği yapılan veri işleme faaliyetlerinde de kişisel verinin korunması için gereken her türlü önlem alınmalı ve Kanunda belirlenen genel ilkelere uyulmalıdır. Son olarak, ilgili kişinin temel hak ve özgürlükleri ile veri sorumlusunun meşru menfaatleri arasında makul bir denge kurulması gerekir.

İdarenin bir veri sorumlusu olarak, meşru menfaatinin korumak amacıyla kişisel veri işleyip işleyemeyeceği irdelenmesi gereken bir konudur. Kural olarak, 6698 sayılı Kanuna göre İdarenin 5/2(f) maddesi uyarınca açık rıza olmaksızın veri işleyebilmesi mümkündür. Nitekim, Kanuna göre kamu tüzel kişileri de veri sorumlusu olabilir ve bu maddeye ilişkin olarak kamu tüzel kişilerini kapsam dışı bırakan bir hükme Kanunda yer verilmemiştir.

Belirtmek gerekir ki Direktif ve Tüzük'te yer verilen düzenlemelerde, 6698 sayılı Kanunun aksine, veri sorumlusu ile birlikte üçüncü kişinin meşru menfaatlerinin gerektirdiği durumlarda da açık rıza olmaksızın veri işlenebileceği kabul edilmiştir. Bununla birlikte Tüzük düzenlemesinde, kamu makamlarının görevlerini yerine getirirken gerçekleştirdiği işlemlerde meşru menfaate dayalı olarak veri işleyemeyeceği kuralına yer verilmiştir (md. 6/1(son cümle). Düzenlemeye ilişkin 47 no'lu gerekçeta bu durum “*Kamu makamlarının kişisel verileri işlemesi için yasal dayanağı kanunla sağlamanın kanun koyucuya ait olduğu göz önüne alındığında, bu yasal dayanak, kamu makamlarının görevlerini yerine getirirken işlemleri için geçerli olmamalıdır*” şeklinde ifade edilmiştir. Başka bir deyişle, kamu kurumlarının görevleri kanun koyucu tarafından belirlendiğine göre, bu görevler sırasında kişisel verilerin işlenmesi gerekecekse bunun da kanun koyucu tarafından öngörülmesi gerektiği söylenebilir.

Kural olarak İdare kamu yararını gerçekleştirmeye yönelik eylemlerde bulunan ve idari işlemler tesis eden bir kurumdur. Kendisine tanınan üstünlük ve ayrıcalıkları kullanarak kamu yararını gerçekleştirmeyi amaçlar³⁸⁰. Bu bakımdan, yetki, şekil, sebep, konu ve amaç unsurlarından oluşan idari işlemlerin kamu yararı amacı ile tesis edilmesi gerekir³⁸¹. Kamu yararı kavramının üzerinde uzlaşılan temel bir tanımı olduğu söylenemez³⁸². Ancak, bireysel yarar ya da ayrıcalıklı bir topluluğun yararı yerine toplumun ortak yararının tercih edilmesi halinde kamu yararının uygun şekilde hareket edildiği söylenebilecektir. Burada vurgulanması gereken, İdarenin idari faaliyetleri yerine getirirken kamu yararı amacıyla hareket ettiği ya da en azından bu amaçla hareket etmesi gerektiğidir. Başka bir deyişle, İdarenin kendisine yasalarla verilen görevleri yerine getirdiği sırada toplumun ortak menfaatleri yerine kendi menfaatleri amacını gütmesi mümkün değildir. 6698 sayılı Kanunun ilgili maddesinde sadece veri sorumlusunun kendi meşru menfaatleri için kişisel veri işlemesine imkân tanındığı da düşünüldüğünde,

³⁸⁰ İdare kamu yararına hareket ettiği için kamu gücü ayrıcalıklarından faydalanmaktadır: ÖZAY, **Gümrükte Yönetim**, s. 29.

³⁸¹ İdari faaliyetlerin amacı kamu yararıdır: YILDIRIM, “İdari İşlem”, içinde: **İdare Hukuku**, s. 510. Ayrıca bkz.: Celaleddin KOÇ, “İdari İşlemin Amaç Unsuru”, **Bursa Uludağ Üniversitesi SBE**, Yayımlanmamış Yüksek Lisans Tezi, 2019, s. 5.

³⁸² DURAN, s. 25. Kamu yararı kavramı yerine genel yarar, toplum yararı, ortak iyilik gibi kavramların da kullanıldığı ifade edilmektedir. Tekin AKILLIOĞLU, “Kamu Yararı Kavramı Üzerine Düşünceler”, **İHİD**, C.9, S.1-3, 1988, s.15. <https://dergipark.org.tr/tr/download/article-file/13697> (E.T. 2.3.2022).

veri sorumlusu olarak kamu tüzel kişilerinin kamusal görevlerini yerine getirirken 6698 sayılı Kanunun 5/2(f) maddesine dayanarak açık rıza olmaksızın kişisel veri işleyemeyeceği söylenebilir. Bunun yerine, özellikle aynı maddenin (a) bendinde düzenlenen “kanunlarda açıkça öngörülmesi” yahut (ç) bendinde öngörülen “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartlarına dayanılabilir. Nitekim, idarenin kanuniliği ilkesi gereği kişisel verilerin işlenmesini gerektiren bir görevin kanunlarda ve alt düzenleyici işlemlerde düzenlenmesi gerekir.

Bununla birlikte, İdarenin işlemleri yalnızca idare işlevine yönelik, kamu gücüne dayalı ve tek yanlı işlemlerden ibaret değildir. İdare, özel hukuka dayalı hukuki işlemler de tesis etmektedir. İdarenin medeni veya ticari nitelikteki işlemleri, haksız fiilleri, mallarının idaresi, ekonomik faaliyetleri ve ticari nitelikteki sözleşmeleri özel hukuk alanında sonuç doğuran işlem ve eylemlerine örnek olarak verilebilir³⁸³. İşte İdarenin bu alanda gerçekleştirdiği eylem ve işlemler kamu hukuku kurallarına tabi olmadığından, kamu yararı amacını da taşımak mecburiyetinde değildir. Bu hallerde bir kamu tüzel kişinin tıpkı diğer tüzel kişiler gibi meşru menfaatleri doğrultusunda açık rıza olmaksızın kişisel veri işleminin mümkün olduğu kabul edilmelidir.

4.4.2. Özel Nitelikli (Hassas) Verilerin İşlenmesine İlişkin Şartlar

6698 sayılı Kanunun 6. maddesi uyarınca gerçek kişinin *ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri* özel nitelikli verilerdir. Bu veriler Kanunda sınırlı sayıda düzenlenmiş olduğundan kıyas yoluyla çoğaltılması mümkün değildir. Öte yandan, özel nitelikli verilerin bu şekilde tahdidi olarak belirlenmesine ilişkin literatürdeki tartışmalara yukarıda değinilmiştir³⁸⁴.

2 Mart 2024 tarihinde çıkarılan ve 1.6.2024 tarihinde yürürlüğe giren 7499 sayılı Kanun ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yapılan önemli değişiklikler arasında, özel nitelikli verilerin işlenmesine ilişkin şartların yeniden düzenlenmesi yer almaktadır. 6698 sayılı Kanun'un ilk halinin, 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifi esas alınarak formüle edildiği bilinmektedir. Bununla birlikte, 2016 yılında kabul edilen ve 25 Mayıs 2018 tarihinde yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğü (GDPR), veri koruma alanındaki güncel ihtiyaçlara daha kapsamlı bir yanıt niteliğindedir.

³⁸³ YILDIRIM, “İdari İşlem”, içinde: **İdare Hukuku**, s. 440. Belirtmek gerekir ki, idarenin özel hukuk sözleşmelerine özel hukuk kuralları uygulanmakla birlikte, bu sözleşmelerin imzalanmasından önce gerçekleştirilen hazırlık aşamasındaki işlemler kamu hukuku rejimine tabidir. ÖZAY, **Günışığında Yönetim**, s. 508 vd.

³⁸⁴ Bkz. “2. ÖZEL NİTELİKLİ (HASSAS) KİŞİSEL VERİ KAVRAMI” başlığı.

Bu bağlamda, 6698 sayılı Kanun'da gerçekleştirilen son değişiklikler ile Türk veri koruma mevzuatının, GDPR'da yer alan düzenlemelerle daha uyumlu hale getirildiği gözlemlenmektedir. Bu uyum süreci, özellikle özel nitelikli verilerin işlenmesine ilişkin şartların yeniden ele alınmasında belirgin bir şekilde tezahür etmektedir. Yapılan değişikliklerin Türk hukukundaki etkisini daha anlaşılır kılmak için aşağıda öncelikle değişiklik öncesi kurallara ve bunlara getirilen eleştirilere kısaca yer verilecek, ardından mevcut kurallara değinilecektir.

4.4.2.1. 2 Mart 2024 Tarihli 7499 Sayılı Kanun Değişikliği Öncesi Durum

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ilk fıkrasında özel nitelikli veriler tahdidi olarak sayılmış ve yapılan Kanun değişikliği sonrasında bu verilerde herhangi bir değişiklik olmamıştır. Değişiklikler, hassas verilerin işlenme şartlarına ilişkin kurallarda yapılmıştır. Değişiklik öncesinde Kanunun 6. maddesinin işlenme şartlarına ilişkin 2. ve 3. fıkraları şu şekildeydi:

“(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrafta sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.”

Görüldüğü üzere Kanun, özel nitelikli verilerin işlenmesi için kural olarak ilgili kişinin açık rızasını şart koşmaktaydı. Ancak, sağlık ve cinsel hayat dışındaki özel nitelikli veriler ile sağlık ve cinsel hayata ilişkin veriler için farklı istisnalar öngörmekteydi.

Sağlık ve cinsel hayat dışındaki özel nitelikli veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilmekteydi. Sağlık ve cinsel hayata ilişkin veriler ise, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilmekteydi.

Bu düzenleme, çeşitli açılardan eleştirilere maruz kalmıştı. Özellikle, sağlık ve cinsel hayata ilişkin verilerin işlenmesi için belirlenen amaçların Kanunda açıkça tanımlanmaması ve belirsizlik içermesi eleştiri konusu olmuştu. Nitekim, bu husus Anayasa Mahkemesi'ne yapılan iptal başvurusunda da incelenmişti³⁸⁵.

³⁸⁵ AYM, E. 2016/125, K. 2017/143, §62.

Anayasa Mahkemesi, ilgili düzenlemenin Anayasa'ya aykırı olmadığına karar vermişti. Mahkeme, sağlık ve cinsel hayata ilişkin kişisel verilerin açık rıza olmaksızın işlenebileceği hallerin kapsam, amaç ve sınırlarının ilgili fıkra da gösterildiğini, ayrıca Kurul tarafından belirlenen önlemlerin alınması kuralının getirildiğini ve bu verilerin sadece sır saklama yükümlülüğü bulunan kişiler ve yetkili kurumlarca işlenebileceğini vurgulamıştı (§75-80).

Bununla birlikte, düzenlemenin iki açıdan Anayasa'ya aykırılık taşıdığı öne sürülmekteydi. İlk olarak, sağlık ve cinsel hayata ilişkin kişisel verilerin Kanunda sayılan ve sınırlarının belirlenmesinde güçlük yaşanan amaçlar bağlamında işlenebilmesinin öngörülmesiyle İdareye geniş bir takdir yetkisi tanınmaktaydı. Bu durum, Anayasa'nın 13. maddesinde belirtilen temel hak ve özgürlüklerin ancak kanunla sınırlanabileceği ilkesine aykırılık oluşturabilmekteydi.

İkinci olarak, sağlık ve cinsel hayata ilişkin verilerin açık rıza olmaksızın işlenebilme şartı olarak yalnızca Kanunun 6/3. maddesinin 2. cümlesinde sayılan amaçlar doğrultusunda sır saklama yükümlülüğü altındaki kişi ve kurumlarca işlenebilmesinin öngörülmesi, ilginç bir sonuç doğurmaktaydı. Bu düzenleme, sağlık ve cinsel hayata ilişkin kişisel verilerin Kanunun 6/3. maddesinde sayılan amaçlardan birine dahil edilemeyecek bir amaçla işlenmesini öngören başka bir kanun çıkarılması halinde, bu kanuna istinaden kişisel veri işlenmesini imkânsız kılmaktaydı. Örneğin, 193 sayılı Gelir Vergisi Kanunu'nun 31. maddesine göre çalışma gücünün en az %40'ını kaybetmiş kişi, bu durumu sağlık raporuyla kanıtlayarak vergi indiriminden faydalanabilmektedir³⁸⁶. Ancak, 6698 sayılı Kanun'un 6/3. maddesinde sayılan amaçlar arasında "vergi indirimi" amacı yer almadığından, bu tür bir veri işleme faaliyetinin hukuka uygunluğu tartışmalı hale gelmekteydi. Bu çelişkili durum, Anayasa'nın 13. ve 20. maddelerine aykırı bir sonuç doğurmaktaydı. Anayasa'nın 20/3. maddesi ayırım yapmaksızın tüm kişisel verilerin kanunlarda öngörülmesi halinde işlenebileceğini düzenlerken, 6698 sayılı Kanun'un 6/3. maddesi bu imkânı sınırlandırmaktaydı.

Sonuç olarak, eski düzenleme, özel nitelikli verilerin korunması açısından önemli bir adım olmakla birlikte, uygulamada çeşitli sorunlara ve tartışmalara yol açmaktaydı. Bu nedenle, düzenlemenin yeniden ele alınarak, İdarenin takdir yetkisinin sınırlandırılması ve "kanunlarda açıkça öngörülmesi" halinin sağlık ve cinsel hayata ilişkin verilerin açık rıza olmaksızın işlenebilme şartları arasına eklenmesi gerekliydi³⁸⁷.

4.4.2.2. Yeni Düzenleme ve Genişleyen Veri İşleme Şartları

Yapılan kanun değişikliği sonrasında KVKK'nın 6. maddesinin ikinci fıkrası kaldırılmış, "açık rıza" ise özel nitelikli verilerin işlenmesine ilişkin hukuka uygunluk sebebi olarak üçüncü fıkraya

³⁸⁶ KALYON, s.102.

³⁸⁷ Aynı yönde görüş için bkz.: ALTINDAĞ, *Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları*, s. 91; ERARSLAN, s.157.

eklenmiştir. Mevcut haliyle düzenlemede, özel nitelikli verilerin işlenmesinin kural olarak yasak olduğu vurgulanmış, ardından bu kuralın istisnalarına yer verilmiştir. Sonuçta ortaya çıkan veri işleme şartları şu şekildedir:

“(3) Özel nitelikli kişisel verilerin işlenmesi yasaktır. Ancak bu verilerin işlenmesi;

a) İlgili kişinin açık rızasının olması,

b) Kanunlarda açıkça öngörülmesi,

c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,

d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,

e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,

f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,

g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde mümkündür.”

Kanun koyucu, kanun gerekçesinde 6. maddedeki değişikliklerin güncel ihtiyaçların ve Avrupa Birliği Genel Veri Koruma Tüzüğü’nün dikkate alınarak yapıldığını bildirmektedir. Önceki düzenlemede sağlık ve cinsel hayata ilişkin olanlar dışındaki özel nitelikli veriler sadece kişinin açık rızası ve kanunlarda öngörülmesi halinde işlenebiliyor; sağlık ve cinsel hayata ilişkin verilerse açık rıza dışında sadece sır saklama yükümlülüğü altındaki kişi ve kurumlarca kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetlerinin finansmanı, yönetimi ve planlanması amacıyla işlenebiliyordu. Yapılan değişikliklerle özel nitelikli verilerin işleme istisnaları epey artırılmış, 5. maddede genel nitelikli veriler için sayılan şartlarla benzer hale getirilmiştir.

3. fıkranın (a) bendinde ilgilinin açık rızası veri işleme şartlarından biri olarak kabul edilmiştir. Kanunumuz genel nitelikli veriler için de açık rıza aradığından, bu iki rıza bakımından herhangi bir fark

bulunmamaktadır. Oysaki Tüzük’te genel nitelikli veriler için ilgilinin rızasının alınması, özel nitelikli veriler içinse açık rızasının alınması gerektiği düzenlenmiştir.

Düzenlemenin (b) bendinde kanunlarda açıkça öngörülmesi eski düzenlemeden farklı olarak tüm özel nitelikli veriler için bir işleme şartı olarak kabul edilmiştir. Önceki düzenlemeden farklı olarak “açıkça” ibaresinin konulmasıyla 5. madde ile uyum sağlanmıştır³⁸⁸.

Özel nitelikli kişisel verilerin işlenmesi çeşitli kanunlarda öngörülmektedir. Örneğin 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu uyarınca yapılacak arşiv araştırmasında ilgili kişinin adli sicil kaydının, kişi hakkında herhangi bir tahdit olup olmadığının, hakkında kesinleşmiş mahkeme kararlarının, 5271 sayılı Ceza Muhakemesi Kanunu uyarınca kişi hakkında kamu davasının açılmasının ertelenmesi ya da hükmün açıklanmasının geri bırakılması kararlarının veriliş verilmemesi tespiti edilmektedir (m.4).

Yine 5490 sayılı Nüfus Hizmetleri Kanunu’nun 7. maddesine göre, kişinin kimlik numarası, doğum yeri ve tarihi, dini, medeni hali, fotoğrafı ve biyometrik verisi gibi kişisel verilerinin nüfus müdürlüklerince tutulacak aile kütüklerine işlenmesi öngörülmüştür. Ayrıca Kanunun 41. maddesi uyarınca Türkiye Cumhuriyeti Kimlik Kartı (TCKK) içerisinde yer alacak bilgileri belirlemeye de İçişleri Bakanlığı yetkilidir. Bilindiği gibi, TCKK projesi 2016 yılında denenmeye başlanmış, 2017 yılında ise tüm Türkiye’de yaygınlaştırılmıştır. Yeni kimlik kartlarında geçmişte çokça tartışılan “din bilgisi” ibaresinin ve kan grubu bilgisinin kimlik üzerinde yer alması uygulamasına son verilmiştir. Ancak, TCKK üzerinde yer alan çip içerisine din bilgisi de kaydedilebildiğinden, yeni kartlarda değişen tek hususun din bilgisine kart üzerinde yer verilmemesinden ibaret olduğu, kişilerin dini inançlarını açıklama zorunluluğunun devam ettiği yönündeki eleştiriler sona ermemiştir³⁸⁹. Ancak, 3.12.2019 tarihli Resmî Gazete’de yayımlanan Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliğinin bu eleştiriler dikkate alınarak hazırlandığı söylenebilir. Düzenlemenin 17. maddesinin 2. fıkrasına göre TCKK için başvuran kişinin kimlik bilgileri, biyometrik verisi, fotoğrafı, ıslak imzası, kart seri numarası ve elektronik sertifikaları ile talep edilmesi halinde din bilgisi ve kan grubu, kart üzerindeki çipe işlenmek suretiyle kartın kişiselleştirilmesi sağlanacaktır. Dikkat edilirse din bilgisi ve kan grubu bilgisinin “talep edilmesi” halinde kartta bulunan çip üzerine işleneceği belirtilmektedir. Dolayısıyla, bu iki bilgi vatandaş talep etmedikçe kaydedilemez. Ancak uygulamada nüfus müdürlüklerine TCKK için başvurulduğunda “Dini inancınıza ve kan grubunuza ilişkin bilgilerin de kaydedilmesini ister misiniz?”

³⁸⁸ Kanunun genel nitelikli kişisel verilerin işleme şartlarını düzenleyen 5. maddesinde, “kanunda açıkça öngörülmesi” açık rıza olmaksızın kişisel veri işlenebilme şartı olarak belirlenmesine karşın (f.2/a) değişiklik öncesinde özel nitelikli verilerin işleme şartlarını düzenleyen 6. maddede yalnızca “kanunlarda öngörülen hallerde” ifadesine yer verilmiş, açıkça düzenlenmesi aranmamıştı. Özel nitelikli verilerin diğer verilere kıyasla daha sıkı korunması gerektiği halde kanunlarda ‘açıkça’ öngörülmesinin aranmaması eleştiri konusu olmuştur. ERARSLAN, s.217; KÜZECİ, **Kişisel Verilerin Korunması**, s.351.

³⁸⁹ Berke ÖZENÇ, “İnancını Açıklamama Hakkı Açısından Türkiye Cumhuriyeti Kimlik Kartlarındaki Din Hanesi”, **TBB Dergisi**, S.141, s. 41.

sorusu sorulmamaktadır. Bunun yerine kişi bu bilgileri kaydetmek istemediğini beyan etmesi halinde sistemde “seçilmemiş” butonu işaretlenmektedir.

Ancak, Yönetmeliğin bu hali dahi ölçülülük ilkesi ile birlikte düşünüldüğünde eleştiriye açıktır. Mevcut durumda kişi talep etmesi halinde din hanesinde belirleme yapılabilmektedir. Ancak ülkemiz şartları düşünüldüğünde, bunun bir seçenek olarak sunulması halinde din hanesini boş bırakmayı düşünen kişi çevresinde baskı hissedebilir. Nitekim nüfus müdürlüklerinde “Din hanesini dilerseniz boş bırakabilirsiniz” şeklinde bilgi verilen vatandaşların “Ne demek, biz dinsiz miyiz?” benzerindeki itirazları duyulabilmektedir. İşte bu sebeple, kayıtlardan din hanesinin tamamen kaldırılmasının daha özgürlükçü bir yaklaşım olduğu savunulabilir.

Benzer şekilde, özürllülük bilgisinin nüfus cüzdanında yer almasına ilişkin yönetmelik hükümlerinin iptali konusunda Danıştay İdari Dava Daireleri Kurulu'nun verdiği karar da ölçülülük ilkesi açısından önem taşımaktadır. Kurul, nüfus cüzdanının Türk vatandaşlığını kanıtlayan ve çeşitli hukuki işlemlerde ibrazı gereken temel bir kimlik belgesi olduğunu hatırlatmış, bu bağlamda, özürllülük oranının nüfus cüzdanına yazılmasının, kimliğin her kullanımında kişinin özel durumunun başkaları tarafından öğrenilmesine yol açacağını belirtmiştir. Bu durum, özürllü vatandaşların günlük yaşamlarında sürekli olarak özel durumlarını açıklamak zorunda kalmalarına ve potansiyel olarak ayrımcılığa maruz kalmalarına neden olabilecektir. Sonuç olarak, Kurul, özürllü bireylerin sadece ihtiyaç duydukları durumlarda ibraz edebilecekleri ayrı bir kimlik kartı uygulamasının hem yasal çerçeveye uygun hem de kişi hak ve özgürlüklerini koruyucu nitelikte olacağını belirtmiştir³⁹⁰.

Ayrıca, özel nitelikli kişisel verilerin işlenmesine ilişkin yasal düzenlemelerin Anayasa'nın 13. ve 20. maddelerinde belirtilen kriterlere uygun olması gerektiği ifade edilmelidir³⁹¹. Anayasa Mahkemesi (AYM), bu konuda önemli kararlar vermiştir. Örneğin, güvenlik soruşturması ve arşiv araştırması hakkındaki bir kararında, kişisel verilerin işlenmesine yönelik temel ilkelerin kanunla

³⁹⁰ Danıştay İDDK, E. 2008/1763, K. 2012/2340, Danıştay Dergisi, Y.2013, S.133, s.128 vd.

³⁹¹ Kanunda yapılan değişikliklerin genel anlamda Avrupa Veri Koruma Tüzüğü'ne uyum sağlamak amacını taşıdığı kanun koyucu tarafından da ifade edilmekle birlikte Tüzük düzenlemesinin doğrudan uygulama bulmadığı ülkemizde, Anayasa'nın 13. maddesi hatırlatılmakta ve 6/3(b) maddesinde yer verilen “kanunda açıkça öngörülme” ibaresinin boşa söylenmiş bir şey olmadığı, dolayısıyla kanunla getirilecek sınırlamaların Anayasa Mahkemesi kararlarında belirlenen kanun kriterlerini taşıması gerektiği vurgulanmaktadır., Sezen KAMA ve diğerleri, “Reformun Sebebi, İçeriğinin Tanıtılması ve Müstakbel Değişiklikler” [Konferans 1. Oturumu], **KVKK Reformu Konferansı**, 8 Mayıs 2024, İstanbul, Türkiye.

belirlenmesi gerektiğini vurgulamıştır³⁹². Bu karar sonucunda, 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu çıkarılmıştır³⁹³.

AYM'nin bireysel başvuru kararları da bu konuda yol göstericidir. Bir belediyenin parmak izi ile mesai takibi uygulamasına ilişkin kararda, özel nitelikli kişisel verilerin işlenmesi için kanuni dayanak gerektiği belirtilmiştir. AYM, kanunlarda açıkça öngörülme ifadesinin, ilgili alanda özel nitelikli veri işlemenin ayrıca ve açıkça düzenlenmesi gerektiği şeklinde anlaşılması gerektiğini vurgulamıştır³⁹⁴. Kişisel verilerin işlenmesinde ölçülülük ilkesi de büyük önem taşımaktadır. Mesai takibi için parmak izi kullanılması örneğinde olduğu gibi, bu konuda bir kanun hükmü bulunduğu varsayımında dahi, bir uygulamanın amaca elverişli olması yeterli değildir; aynı zamanda gerekli ve orantılı olması da gerekmektedir. Daha az müdahaleci yöntemler varken özel nitelikli verilerin işlenmesi, ölçülülük ilkesine aykırı olabilir.

AYM kanun koyucu tarafından yapılacak düzenlemelerin Anayasanın 13. maddesi bağlamında sahip olması gereken özellikleri ise şöyle tarif etmektedir: *“Bununla birlikte kanunun çalışanın temel hak ve özgürlüklerinin sınırlandırılmasını içeren konuyla ilgili temel esasları ve ilkeleri belirleyecek nitelikte olması gerektiği de vurgulanmalıdır. Bu kapsamda kanun ve ilgili kanuna dayanan mevzuatın özellikle kişisel verilerin işlenmesinin kapsamına ve muhafazasına ilişkin esasları belirlemesi beklenir. Kanunun ayrıca tutulma süresi, üçüncü kişilerin erişimi ile verilerin kullanılması ve imhası konusundaki usullere ilişkin muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralları içermesi gerekmektedir. Bunun yanında kanunla sınırlamanın elbette meşru bir amaca dayanması, demokratik toplum gereklerine uygun ve ölçülü olması gerektiği hatırlatılmalıdır.”*³⁹⁵

³⁹² 657 sayılı Kanunun 48. maddesine eklenen düzenlemeyle “güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak” devlet memurluğuna girişte aranan özel şartlardan biri olarak kabul edilmiştir. Ancak, yapılan iptal başvurusunu değerlendiren AYM, Anayasanın 13. maddesinde temel hak ve özgürlüklerin yalnızca kanunla sınırlanabileceğini hatırlatmış, güvenlik soruşturması ve arşiv araştırmasıyla verilerin alınması, kaydedilmesi ve kullanılmasının özel hayata saygı hakkına getirilen bir sınırlama niteliğinde olduğunu ifade ettikten sonra şu değerlendirmede bulunmuştur: *“Kuralda güvenlik soruşturması ve/veya arşiv araştırması yapılması memurluğa alımlarda genel şartlar arasında sayılmasına karşın güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilen kullanılmasına ilişkin temel ilkeler belirlenmeksizin kuralla sadece güvenlik soruşturması ve arşiv araştırması yapılması devlet memurluğuna alımlarda aranacak şartlar arasında sayılmıştır. / Güvenlik soruşturması ve arşiv araştırması sonucunda devlet memurluğuna atanmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13., 20. ve 128. maddeleriyle bağdaşmamaktadır.”* AYM, E. 2018/73, K. 2019/65, T.24.7.2019, §171-72.

³⁹³ AYM'nin benzer yöndeki karar sayısının artması üzerine (AYM, E.2018/163, K.2020/13, T.19.02.2020, §16-17; AYM, E.2020/24, K.2021/39, T.03.06.2021, §48-49; AYM, E. 2020/41, K. 2021/91, T.16.12.2021, §18-19; AYM, Fatih Saraman, B.n. 2014/7256, §89, 90; AYM, Turgut Duman, B.n. 2014/15365, §88) güvenlik soruşturması ve arşiv araştırmasına ilişkin kanuni düzenleme çalışmaları başlatılmış ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu 17.4.2021 tarih ve 31457 sayılı RG'de yayımlanarak yürürlüğe konulmuştur.

³⁹⁴ AYM, B.n. 2018/11988, T.10.3.2022, §55-57.

³⁹⁵ AYM, B.n. 2018/11988, T.10.3.2022, § 55-57.

AYM, tutuklu bir başvuruçunun mektuplarının UYAP'a kaydedilmesi konusundaki kararında, kişisel verilerin korunması ve haberleşme hürriyeti bağlamında "kanunilik" ilkesini değerlendirmiştir. Mahkeme, ceza infaz kurumlarındaki yazışmaların denetimi için yasal düzenlemeler bulunduğunu belirtmiş, ancak bu düzenlemelerin içerik bakımından yetersiz olduğuna dikkat çekmiştir. AYM'ye göre, kanunlar yazışmaların tutulma süresi, erişim, kullanım, imha ve gizlilik konularında detaylı kuralları içermelidir. Mevcut uygulamanın dayanağı olan Genelge'nin, mahpusun sakıncalı bulunmayan, kişisel nitelikte bilgi içeren ve yargısal süreçle ilgisi olmayan yazışmalarının UYAP'a kaydedilmesini sağlayarak mevzuatın öngördüğü usulden ayrıldığı ve kişisel verilerin korunması konusunda yeterli güvence sağlamadığı tespit edilmiştir. Sonuç olarak, AYM bu uygulamanın kanuni dayanaktan yoksun olduğuna ve dolayısıyla özel hayata saygı hakkı ile haberleşme hürriyetine aykırı olduğuna karar vermiştir³⁹⁶.

Yapılan değişiklik sonrasında eklenen (c) bendi ile fiili imkânsızlık hallerinde kişinin ya da bir başkasının beden bütünlüğünün ya da hayatının korunması için zorunlu olması halinde özel nitelikli veriler de işlenebilecektir. Değişiklik öncesinde, söz gelimi trafik kazası nedeniyle bilinci kapalı olan kişinin kan grubu, sağlık durumu gibi bilgiler bunları paylaşan kişi sır saklama yükümlülüğü altındaki bir sağlık çalışanı değilse Kanuna göre hukuka aykırı olarak kabul edilmekteydi³⁹⁷. Mevcut düzenlemeyle bu aksaklık giderilmiştir. Ancak, fiili imkânsızlık durumunda sadece beden bütünlüğünün ya da hayati tehlikenin zorunlu kıldığı özel nitelikli verilerin işlenmesi gerektiği unutulmamalıdır. Kişinin sağlık durumuna etki edecek hastalık verilerinin işlenmesi akla ilk gelebilecek verilerdir. Bunun dışında, örneğin Yehova Şahitleri'nin kan naklini kabul etmemesi nedeniyle yapılacak müdahalenin imkanlar dahilinde buna göre belirlenmesi için de ilgilinin bu inanışa sahip olduğu bilgisi de işlenebilecektir.

Getirilen bir başka veri işleme şartı ise özel nitelikli verilerin ilgisince alenileştirilmesidir. Verilerin işlenmesi alenileştirme iradesine uygun şekilde olduğu müddetçe ilgisince alenileştirilen verilerin işlenmesi hukuka uygun olacaktır. Kanun gerekçesinde de ifade edildiği üzere, ilgisinin acil

³⁹⁶ Aynı konuya ilişkin olarak AİHM'e yapılan başvuruda Mahkeme, özel hayata saygı hakkına müdahale teşkil etmemesi için yapılan müdahalenin "kanunla öngörülmüş olması" ve meşru bir amaca hizmet etmesi gerektiğine, dahası bu amacın demokratik toplumda gerekli olmasına vurgu yapmış, 2016 tarihli söz konusu genelgenin idarenin iç yazışmalarında yer aldığını, dolayısıyla başvuranların bilgisi dahilinde olmadığını, bu bakımdan genelgenin "Sözleşme ile güvence altına alınan haklara kamu gücünün keyfi müdahalelerini önlemek için gerekli uygun koruma ve hukuki güvenlik sunamayacağı için Mahkeme'nin içtihatları anlamında yeterli "nitelikte" bir "kanun" olarak görülemeyeceği" ifade edilerek, yapılan müdahalenin "kanunla öngörülmüş olması" ilkesini karşılamadığı gerekçesiyle özel hayata saygı hakkının ihlal edildiğine karar verilmiştir: AİHM, Nuh Uzun ve diğerleri / Türkiye davası, B.n. 49341/18 ve diğer 13 başvuru, T.29.3.2022, <https://hudoc.echr.coe.int/eng?i=001-218188>.

³⁹⁷ ÇEKİN, bu durumu veciz bir şekilde makalesinin başlığında şöyle ifade etmektedir: "Rahmetlinin Hayatını Kurtaramadık Ama En Azından Kişisel Sağlık Verilerini Koruduk!!! Covid-19 Pandemisi Karşısında Kişisel Sağlık Verilerinin İşlenmesine Dair KVKK Hükümlerinin İş İlişkileri Kapsamında Değerlendirilmesi", **Lexpera Blog**, 6.4.2020, <https://blog.lexpera.com.tr/author/mesut-ekin/> (E.T. 1.7.2024).

durumlarda kullanılması için herkesin erişebileceği alanda kan grubu ve alerji bilgilerini paylaşması ve verilerin bu amaca uygun olarak üçüncü kişilerce kullanılması bu duruma örnek olarak verilebilir³⁹⁸.

Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması hali de 5. maddede olduğu gibi özel nitelikli veriler için de işleme şartlarından biri olarak kabul edilmiştir. Söz gelimi, engelli park kartı uygulamasını sunmak isteyen belediye, engelli vatandaşlara özel park alanları tahsis etmek ve park kartı vermek için, kişilerin engellilik durumlarına ilişkin sağlık verilerini işleyebilecektir. Öte yandan, kendisine karşı açılacak bir malpraktis davasına karşı savunma yapabilmek amacıyla hastasının bilgilerini davada delil olarak kullanması ya da dava zamanaşımı boyunca bu bilgileri saklaması hukuka uygun kabul edilecektir³⁹⁹.

Kanunda sır saklama yükümlülüğü altında bulunan kişi ya da yetkili kurum ve kuruluşlarca kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla veri işlenebilmesi şartı muhafaza edilmiştir. Değişiklik öncesinde, yalnızca sağlık ve cinsel hayata ilişkin verilerin işlenmesine ilişkin olarak kabul edilen bu hüküm için yeni düzenlemede böyle bir sınırlama öngörülmemiştir. Ancak, hükmün amaçsal yönden sınırlandırma şekli ve getiriliş amacı göz önünde bulundurulduğunda, bu işleme şartına dayanarak sadece sağlık ve cinsel hayata ilişkin verilerin işlenebileceği kabul edilmelidir⁴⁰⁰.

KVKK'nun 6. maddesinde bir başka veri işleme şartı (f) bendinde belirlenmiştir. Buna göre, istihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması halinde özel nitelikli verilerin işlenebileceği kabul edilmiştir. Gerekçede de ifade edildiği üzere, İş Kanunu'yla işverenlere verilen engelli veya hükümlü çalıştırma zorunluluğu nedeniyle işverenlerce ilgililerin sağlık veya ceza mahkûmiyetine ilişkin verilerinin işlenmesi, sağlık kuruluşlarınca diyaliz hastalarına sunulan taşıma hizmetlerinin yerine getirilebilmesi amacıyla ilgisinin sağlık raporunun işlenmesi bu kapsamda kabul edilecektir. Yine özellikle belediyeler tarafından sosyal hizmetler ve sosyal yardımların sunulması için gerekli olabilecek sağlık bilgilerinin işlenmesi de bu kapsamda kabul edilebilecektir. Doğal afetlerden etkilenenlere İdareler tarafından sunulabilecek çeşitli hizmetlerin ve yardımların gerçek ihtiyaç sahiplerine ulaşması bakımından bu verilerin işlenmesi hukuka uygun olacaktır.

Kanunun 5. maddesinde yer verilen ve veri sorumlusunun hukuki yükümlülüklerini yerine getirmesi amacıyla veri işlemesine imkân veren düzenleme ile 6. maddenin (f) bendindeki bu düzenleme arasında amacın sınırlandırılması bakımından fark bulunmaktadır. Nitekim, 6. maddede veri sorumlusunun

³⁹⁸ 6698 sayılı Kanunda yapılan değişikliklere ilişkin Kanun ve madde gerekçesi için bkz.: Mehmet Bedii KAYA, **KVKK Reformu: 2024 Değişiklikleri (Dijital Baskı 1.0)**, 2024, s.100, <https://mbkaya.com/hukuk/kvkk-reformu.pdf>.

³⁹⁹ Ömer EKMEKÇİ ve diğerleri, “Ceza Muhakemesi Kanunu ile Bazı Kanunlarda ve 659 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılmasına Dair Kanun Teklifi ile 6698 Sayılı Kanun’da Yapılan Değişiklikler”, **Lexpera Blog**, 02.03.2024, <https://blog.lexpera.com.tr/cmk-659-6698-degisiklikler/> (E.T. 5.7.2024).

⁴⁰⁰ KAYA, s.14.

yalnızca istihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülükleri nedeniyle zorunlu olması aranırken, 5. maddede böyle bir sınırlama öngörülmemiştir.

Özel nitelikli verilerin işlenmesi için öngörülen yeni istisnalardan biri de (g) bendinde düzenlenmiştir. Buna göre bazı özel kuruluşlar, faaliyetleri gereği özel nitelikli kişisel verileri işleyebilir. Bu kuruluşlar arasında siyasi partiler, dini cemiyetler, felsefi gruplar ve sendikalar gibi kâr amacı gütmeyen organizasyonlar yer alır. Bu tür kuruluşlar, belirli şartlar altında üyelerinin, eski üyelerinin veya düzenli iletişimde oldukları kişilerin hassas verilerini kullanabilir. Ancak bu kullanım, kuruluşun yasal çerçevesine ve amaçlarına uygun olmalı, faaliyet alanlarıyla sınırlı kalmalı ve üçüncü taraflarla paylaşılmamalıdır. Bu düzenlemeyle, özel nitelikli verilerin korunması ile sivil toplum kuruluşlarının faaliyetlerini sürdürebilmesi arasında bir denge kurulması amaçlanmaktadır. Örneğin, bir dini dernek üyelerinin inanç bilgilerini tutabilir veya bir sendika üyelerinin siyasi görüşlerine dair bilgileri saklayabilir. Ancak bu bilgilerin kullanımı, kesinlikle kuruluşun meşru faaliyetleriyle sınırlı olmalı ve gizlilik ilkelerine sıkı sıkıya bağlı kalınmalıdır.

4.4.2.3. Özel Nitelikli Verilerin İşlenmesinde Aranan Genel Şart Olarak KVK Kurulu Tarafından Belirlenen Yeterli Önlemlerin Alınması

6698 sayılı Kanunun 6. maddesinin ilk fıkrasında özel nitelikli kişisel veriler belirlenmiş, üçüncü fıkrasında bu verilerin kural olarak açık rıza alınmaksızın işlenmesinin yasak olduğu belirlendikten sonra devamında açık rıza olmaksızın işlenebilmesinin istisnalarına yer verilmiştir. Maddenin son fıkrasında ise bu tür verilerin işlenmesinde ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu belirtilmiştir. Kanunun 12. maddesinde yer alan ve tüm kişisel veriler için geçerli olan veri güvenliğine ilişkin hükmün⁴⁰¹ yanı sıra bu hükümle kanun koyucunun özel nitelikli verilerin korunması bakımından daha hassas ve yüksek güvenlik önlemleri alınmasını amaçladığı söylenebilir.

Kanunun 6/5. maddesine istinaden Kurul tarafından 2018/10 sayılı ve “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” başlıklı karar alınmış ve bu karar Resmî Gazete’de yayımlanmıştır⁴⁰². Kanun düzenlemesinden anlaşıldığı üzere, veri sorumlusu ister ilgilinin açık rızasına dayalı olsun isterse de 3. fıkrada sayılan istisnalara dayalı olsun özel nitelikli veri işlerken belirlenen bu önlemleri almak mecburiyetindedir. Aksi halde, diğer şartlar sağlansa dahi özel nitelikli verilerin işlenmesi hukuka aykırı olacaktır.

⁴⁰¹ Kanunun 12. maddesi hakkında bkz. “4.2. İdarenin Veri Güvenliği Uygulamaları” başlığı.

⁴⁰² RG, 7.3.2018 / 30353.

Kurul tarafından alınan kararda ilk olarak özel nitelikli verilerin güvenliğine ilişkin “*sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi*” gerektiği ifade edilmiştir. Dolayısıyla, eğer veri sorumlusu genel nitelikli kişisel verilerin yanı sıra özel nitelikli verileri işleyecekse buna özgü ayrı bir politikanın ve prosedürün belirlenmesi gerekir.

Kararda, bu tür verilerin işlenmesi süreçlerinde çalışacak kişilere yönelik alınması gereken çeşitli tedbirlere de yer verilmiştir. Çalışanlara mevzuat ve veri güvenliğine ilişkin düzenli olarak eğitim verilmesi; çalışanlarla gizlilik sözleşmesi yapılması; verilere erişim yetkisi olanların yetki ve sürelerinin kesin şekilde belirlenmesi; periyodik yetki kontrollerinin yapılması; görev değişikliği ya da işten ayrılma durumlarının gerçekleşmesi halinde derhal yetkilerin kaldırılması ve ilgiliye tahsis edilen envanterin kendisinden iade alınması bu hususta belirlenen tedbirlerdir.

Ayrıca, özel nitelikli kişisel verilerin işlendiği, erişildiği ya da muhafaza edildiği ortamların fiziksel ya da elektronik ortam olmasına bağlı olarak değişen çeşitli tedbirlere de yer verilmiştir. Eğer elektronik ortamda bulunuyorsa, verilerin kriptografik yöntemler kullanılarak saklanması, veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması, verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin kullanılması bu tedbirlerden bazılarıdır. Öte yandan fiziksel ortamda tutulan veriler için, ortamın şartlarına göre elektrik kaçağı, yangın, su baskını ya da hırsızlık gibi durumlara karşı yeterli güvenlik önlemlerinin alınması ve bu ortamlara yetkisiz giriş çıkışların engellenmesi yönünde tedbirlerin alınması gerektiği belirtilmiştir.

Özel nitelikli kişisel verilerin aktarılması hususundaysa, e-posta yoluyla aktarılması halinde şifreli kurumsal e-posta adresi ya da Kayıtlı Elektronik Posta (KEP) hesabının kullanılması, taşınabilir bellek, CD, DVD gibi ortamlarda aktarılabilecek bunların kriptografik yöntemlerle şifrenmesi, kâğıt ortamında aktarılan verilerin çalınma, kaybolma ya da yetkisiz kişilerce görülmesinin önlenmesine yönelik tedbirlerin alınması gerektiği ifade edilmiştir.

Kararda son olarak, veri sorumlusunun, yukarıda sayılan önlemlerin dışında Kurum tarafından internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirlenen uygun güvenlik düzeyini sağlamaya yönelik teknik ve idari tedbirleri de dikkate alması gerektiği ifade edilmektedir⁴⁰³. Belirtmek

⁴⁰³ Kişisel Verileri Koruma Kurumu, “Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), **KVKK Yayınları**, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf> (E.T. 20.4.2022). Rehberde belirlenen tedbirlere ilişkin ayrıntılı bilgi için bkz.: ERARSLAN, s.163 vd. Özel nitelikli verilerin önemine istinaden Kurul bu verilerin korunmasına ilişkin yeni tedbirlerin yer aldığı rehberler yayımlayabilmektedir: Örneğin, 16 Eylül 2021 tarihinde Kurumun web sitesinde özel nitelikli kişisel verilerden biri olan biyometrik verilerin işlenmesinde dikkat edilmesi gereken hususlara ilişkin rehber yayımlamıştır. Veri sorumlularının Kurul tarafından yayımlanan bu tür rehberlerde belirlenen tedbirlere uygun şekilde hareket etmesi gerekmektedir: Kişisel Verileri Koruma Kurumu, “Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”, **KVKK Yayınları**, s.15. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abel-d32dc18e2d7e.pdf> (E.T. 20.4.2022).

gerekir ki, söz konusu tedbirlere kamu kurum ve kuruluşlarının da dikkat etmesi ve buna ilişkin önlemleri alması zorunludur⁴⁰⁴.

Öte yandan 6 Temmuz 2019 tarihli Resmî Gazete’de Cumhurbaşkanlığı tarafından “Bilgi ve İletişim Güvenliği Tedbirleri” başlıklı genelge yayımlanmış, tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerin⁴⁰⁵ belirlenen tedbirlere uyması zorunlu kılınmıştır. Genelgede, nüfus, sağlık ve iletişim kayıtları, genetik ve biyometrik veriler gibi kritik bilgi ve verilerin yurtiçinde saklanması; kamu kurum ve kuruluşlarında bulunan verilerin kendi özel sistemlerinde ya da yerli bulut depolama hizmetlerinde saklanması; gizlilik dereceli veya kurumsal mahremiyet içeren bilgilerin kişisel cihazlarda bulundurulmaması; şahsi e-posta adreslerinden kurumsal iletişim kurulmaması; kamu e-posta sunucularının ülkemizde ve kurum kontrolünde bulundurularak iletişim şifreli olarak yapılması gibi çeşitli güvenlik tedbirlerine yer verilmiştir. Ayrıca, güvenlik risklerini en aza indirmek ve özellikle açığa çıkarıldığında milli güvenliği tehdit edebilecek kritik türdeki verilerin güvenliğinin sağlanması için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda “Bilgi ve İletişim Güvenliği Rehberi” hazırlanması öngörülmüştür. Söz konusu Rehberde yer verilen usul ve esaslara tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerin uyması zorunlu kılınmıştır.

Dijital Dönüşüm Ofisi söz konusu Genelgeye istinaden 10 Temmuz 2020 tarihinde Bilgi ve İletişim Güvenliği Rehberi yayımlamıştır. Rehberin temel amacı “*bilgi güvenliği risklerinin azaltılması*,

⁴⁰⁴ Kurul tarafından verilen bir kararda şikâyetçi, aralarında boşanma davası devam eden eşinin, müşterek çocuklarına taciz suçlamasıyla tutuklu olarak yargılandığını belirtmiş, yargılama sürecinde eşinin avukatı tarafından mahkemeye sunulan çocuğuna ait epikriz raporunun usulsüz şekilde elde edildiğini iddia etmiştir. Söz konusu epikriz raporunun Sağlık Bakanlığı’na bağlı bir Eğitim ve Araştırma Hastanesinden alındığı görülmektedir. Yapılan incelemede, Kurul tarafından belirlenen tedbirlerin Hastanede tam olarak uygulanmadığı saptanmıştır. Bu sebeple veri sorumlusu Sağlık Bakanlığının şu hususlarda talimatlandırılmasına karar verilmiştir: “*Veri sorumlusu Sağlık Bakanlığı bünyesindeki çalışanların tereddütte kalmadan takip edebilecekleri sistemli, kuralları net, yönetilebilir ve sürdürülebilir ayrı bir politika hazırlaması gerektiği; idari bir tedbir olarak ilgili Eğitim ve Araştırma Hastanesi çalışanlarının kişisel verilerin korunması uyum çalışmaları kapsamında eğitim alması, bu eğitimde özel nitelikli kişisel verilerle muhatap olan hastane personelinin kişisel verilerin işlenmesinde yetki kapsamına açıkça yer verilmesi ve alınan eğitim belgelerinin Kuruma sunulması; kişisel verilerin güvenliğinin sağlanması açısından teknik bir tedbir olarak hastane otomasyon sisteminin erişim loglarının görüntüleme işlemi de dâhil olmak üzere tutulmasını sağlamak için sistemin güncellenmesi ve Kuruma bilgi verilmesi; hastanedeki tüm doktor ve hasta kayıt personelinin tüm hasta kayıtlarına erişmesi yerine, yalnızca hastaların muayene ve tedavisi ile ilgili olarak çalışan personelin ve doktorların söz konusu verilere erişmesine dair yetki matrisinin net bir şekilde ortaya konulması; hastane otomasyon sisteminden hasta kayıt örneklerinin çıktı alınması konusunda belirli prosedürlerin ve yetkili personelin belirlenmesi, bu çerçevede kişisel verilerin korunması hususunda verilen tüm talimatlara ilişkin yapılan işlemlerin sonucundan Kurula bilgi verilmesi; veri sorumlusu bünyesinde çalışan kişinin, ilgili kişinin çocuğuna ait özel nitelikli kişisel verileri ilgili avukata 6698 sayılı Kanunun 8 inci maddesinde yer alan aktarım şartlarından herhangi birine dayanmadan aktardığı, bu çerçevede veri sorumlusu tarafından Kanunun 12 nci maddesi kapsamında gerekli idari ve teknik tedbirlerin alınmadığı kanaatine varıldığından, Kanunun 18 inci maddesinin (3) numaralı fıkrası uyarınca ilgili kamu kurum ve kuruluşundaki sorumlular hakkında disiplin hükümlerine göre işlem yapılmasına ve sonucundan Kurula bilgi verilmesi.*” KVK Kurulu, 6.8.2021 tarih ve 2021/761 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/7137/2021-761> (E.T. 20.4.2022).

⁴⁰⁵ Ulaştırma ve Altyapı Bakanlığı’nca hazırlanan 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı’nda kritik altyapı ifadesi “*işlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar*” şeklinde tanımlanmıştır. Buna göre elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi ve kritik kamu hizmetleri “kritik altyapı sektörleri” olarak kabul edilmektedir: http://www.sp.gov.tr/tr/temel-belge/s/202/Ulusal+Siber+Guvanlik+Stratejisi+ve+Eylem+Plani+_2020-2023, s. 9.

ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanması” şeklinde ifade edilmiştir⁴⁰⁶.

4.4.3. İdarenin Veri Aktarımı veya Veriyi Koruması: Mahremiyet ve Güvenlik Ekseninde Bir Değerlendirme

Kişisel verilerin paylaşımı ve korunması, kamu idarelerinin karşı karşıya kaldığı en önemli hukuki meselelerden biridir. Çünkü, kamu idareleri açısından veri paylaşımı, iki yönlü bir değerlendirmeyi zorunlu kılar. İlk olarak, kişisel verilerin gereğinden fazla veya hukuka aykırı şekilde paylaşılması, bireylerin özel hayatın gizliliği ve kişisel verilerin korunması haklarına ölçüsüz bir müdahale oluşturabilir. Öte yandan, bazı durumlarda kişisel verilerin paylaşılması, bireyin ve kamunun üstün menfaatlerinin korunması bakımından bir zorunluluk teşkil edebilir. Örneğin, bir kişinin sağlığı veya güvenliği tehlike altındaysa, durumun ilgili mercilere bildirilmesi hayati önem taşır. Keza, suç soruşturmaları, disiplin işlemleri, bilgi edinme başvuruları gibi alanlarda da kişisel verilerin işlenmesi ve paylaşılması gerekebilir. Burada önemli olan, veri paylaşımının kanuni bir dayanağının bulunması ve amacın gerektirdiği ölçüde sınırlı şekilde yapılmasıdır.

6698 sayılı Kanun, bu alanda temel düzenlemeleri içermekte, kişisel verilerin işlenmesi ve aktarılmasını belirli şartlara bağlamaktadır. Yurt içinde ve yurt dışında veri aktarımına ilişkin Kanunun sırasıyla 8. ve 9. maddeleri ihdas edilmiştir. Yurt içinde veri aktarımı kural olarak ilgili kişinin açık rızasıyla mümkündür. Açık rızanın bulunmadığı hallerde ise, KVKK m. 5 ve m. 6'da sayılan istisnai veri işleme şartlarından birinin varlığı gerekir. İdareler, veri paylaşımına ilişkin talepleri bu hükümler çerçevesinde değerlendirmeli, bireyin temel hakları ile kamusal yarar arasında adil bir denge kurmaya çalışmalıdır.

4.4.3.1. İdarenin Kişisel Verileri Yurt İçinde Başka Bir İdareye Aktarması ile Aynı İdarenin Farklı Birimleri Arasındaki Veri Paylaşımı

Kişisel verilerin aktarımı, veri sorumluları arasında gerçekleşen bir işlem olup, KVKK'nin 8. maddesinde düzenlenmiştir. Ancak, bu aktarımın kapsamı ve niteliği açısından önemli bir ayrım mevcuttur: Farklı tüzel kişilikler arasında yapılan veri aktarımı ile aynı tüzel kişiliğin farklı birimleri arasındaki veri paylaşımı teknik olarak aynı işlem olarak kabul edilmemektedir. Nitekim Kişisel Verileri Koruma Kurumu tarafından yayımlanan rehberde de bu husus açıkça ifade edilmiş, veri aktarımının iki

⁴⁰⁶ Bilgi ve İletişim Güvenliği Rehberi'nin tam metni için bkz.: <https://cbddo.gov.tr/bigrehber/> (E.T. 20.4.2022).

ayrı veri sorumlusu arasında yahut veri sorumlusu ile veri işleyen arasında gerçekleştirilebileceği belirtilmiştir⁴⁰⁷. Dolayısıyla, aynı tüzel kişilik içinde gerçekleşen veri paylaşımı, "veri aktarımı" olarak nitelendirilemez, zira burada verinin kontrolü ve sorumluluğu aynı tüzel kişilik bünyesinde kalmaktadır.

Buna karşılık, farklı idareler arasında kişisel veri aktarımı gerçekleştirilirken KVKK'nın 8. maddesi uyarınca kanuni şartlara uygun hareket edilmesi gereklidir. Kanun, yurt içi veri aktarımı için genel kural olarak ilgili kişinin açık rızasını aramakta, ancak Kanunun 5. maddesinin 2. fıkrasında ve yeterli önlemlerin alınması kaydıyla 6. maddenin üçüncü fıkrasında belirlenen şartlardan birinin bulunması hâlinde veri aktarımına olanak tanımaktadır. Örneğin, "bir hakkın tesisi, kullanılması veya korunması için zorunlu olması" (KVKK m. 5/2-e) ya da "hukuki yükümlülüğün yerine getirilmesi" (KVKK m. 5/2-ç) gibi durumlarda, ilgili kişinin açık rızası aranmaksızın veri aktarımı gerçekleştirilebilecektir. Örneğin, bir üniversitenin öğrenci bilgi sistemi verilerini, öğrencinin burs başvurularını değerlendirme amacıyla Kredi ve Yurtlar Genel Müdürlüğü ile paylaşması⁴⁰⁸ veya bir belediyenin, sosyal yardım süreçlerinde ihtiyaç sahibi bireylerin bilgilerini Aile ve Sosyal Hizmetler Bakanlığı ile paylaşması hukuki dayanağı olan veri aktarımına örnek olarak gösterilebilir.

İdarelerin farklı İdarelere veri aktarımında bulunurken Kanunda belirlenen şartlara uygun şekilde hareket etmesi gerekmektedir. Örneğin, kendisinden veri istenen İdare, buna ilişkin veri işleme şartlarının varlığını değerlendirdikten sonra yalnızca amaçla bağlantılı ve orantılı olacak ölçüde veri paylaşımında bulunmalıdır. Nitekim KVK Kurulu, bir İdari kurum tarafından ilgili ticaret sicil müdürlüğünden şirket ortakları ve yetkililerine ait kimlik numaraları ve adresleri gibi kişisel verilerinin paylaşılmasının hukuka aykırı olacağını değerlendirmiştir. Kurul kararında, 6102 sayılı Türk Ticaret Kanunu'nun 24/2. maddesinde, zikredilen kişisel verileri de içeren ticaret sicillerinin ticaret sicil müdürlükleri tarafından tutulmasının öngörüldüğü, bu sicillerin Kanunun 35. maddesi uyarınca herkese açık olduğu, bununla birlikte ticaret sicillerinin KVKK kapsamında bulunduğu ve ilgili mevzuatta bilgilerin korunmasına yönelik çeşitli önlemlerin belirlendiği ifade edilmiştir. Sonrasında, 5490 sayılı Nüfus Hizmetleri Kanunu hükümleri uyarınca nüfus kayıt örnekleri almaya yetkili olan kişi ve

⁴⁰⁷ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, s.77, Aralık 2019, Ankara.

⁴⁰⁸ Gençlik ve Spor Bakanlığı Burs Yönetmeliği, RG 3.11.2023/32358, **Madde 8** – "(1) Bakanlık tarafından, kamu kurum ve kuruluşlarından alınan bilgiler, öğrencinin beyanı ve gerektiğinde sunduğu belgeler değerlendirilerek uygun bulunan başvurular işleme konulur". Bu örnekte, öğrencinin açık rızası alınmak suretiyle kayıtlı olduğu üniversiteden bilgi teyidinde bulunulması da bir seçenek olarak değerlendirilebilir. Öğrencinin burs başvurusunu kendi rızasıyla yapması, bilgilerin paylaşımı noktasında bir irade beyanını işaret etse de KVKK gereği 'açık rıza' şartı bulunduğundan, başvuru sırasında öğrenciye, beyan ettiği bilgilerin ilgili kurumlardan teyit edileceğine dair aydınlatma yapılması ve bu veri aktarımına ilişkin açık rızasının alınması gerekmektedir. Bununla birlikte, yukarıda yer verilen Yönetmelik hükmü gereği, burs başvurusu yapan öğrencilere ilişkin bilgilerin kamu kurum ve kuruluşlarından alınarak kontrolün sağlanması öngörüldüğünden, yapılacak veri aktarımında 'bir hakkın tesisi, kullanılması veya korunması için zorunlu olması' ya da 'hukuki yükümlülüğün yerine getirilmesi' şartlarına dayanılması daha doğru olacaktır. Açık rızaya dayanılarak veri işlenmesi halinde, öğrenci rızasını geri çektiği takdirde bilgilerinin işlenmeyeceğine yönelik yanlış bir kanaat oluşabilir. Ancak, Yönetmelik uyarınca bursun devamlılığı sağlandığı sürece, öğrencinin bilgileri kayıtlı olduğu üniversiteden düzenli olarak istenebilecektir.

kurumların düzenlendiği, burada bazı kamu idarelerine de yer verildiği, dolayısıyla bu kanuna göre kimlik bilgisi paylaşmaya yetkili olarak nüfus müdürlüklerinin belirlendiği vurgulanmıştır. Ayrıca, kişisel verilerin belirli bir amaçla bağlantılı, sınırlı ve ölçülü olacak şekilde işlenmesi ilkesinin kabul edildiği, bu nedenle sonradan ortaya çıkması muhtemel ihtiyaçlara yönelik veri işlemenin Kanuna aykırı olacağı ifade edilmiştir⁴⁰⁹.

Bir başka husus, idareler arası veri paylaşımında kişisel veri içeren bilgi ve belgelerin birer kopyasının talep eden idareyle paylaşılması esas olmakla birlikte, bazı durumlarda belgenin aslına ihtiyaç duyulmasıdır. Örneğin, Devlet Memurları Disiplin Yönetmeliği'nin 21/4. maddesi uyarınca yüksek disiplin kurulu, disiplin cezasına konu eylemin gerçekleştiğini değerlendirmek için, imza teyidi gibi yalnızca belgenin aslı üzerinde yapılabilecek bir inceleme gerçekleştirme ihtiyacı duyabilir. Ancak, belgenin aslına ilişkin güvenlik endişeleri (örneğin, belgenin kaybolması ya da tahrif edilmesi) taşıyan idare, belgenin kendisinden talep edilme amacını yerine getirdikten sonra, işlemlere ilişkin sonuçlarla birlikte belgenin bir kopyasını talep eden idareye göndermeli ve böylece kamusal işleyişin aksamaması sağlanmalıdır.

Öte yandan, aynı tüzel kişilik içinde yer alan idari birimler arasında gerçekleştirilen veri paylaşımı, teknik olarak "veri aktarımı" sayılmasa da hukuki açıdan şeffaflık ve hesap verilebilirlik ilkeleri gereği belirli bir sistematığe bağlı olarak yapılmalıdır. Bu kapsamda, idarenin kendi iç yönergeleriyle veri paylaşım süreçlerini düzenlemesi önem arz eder⁴¹⁰. Örneğin, bir üniversitede öğrencinin güncel iletişim bilgilerini farklı birimlerden birinin talep etmesi durumunda, bu paylaşımın kayıt altına alınması, talebin ve cevabın belirli bir sistem üzerinden gerçekleştirilmesi, sürecin denetlenebilirliğini sağlayacaktır. Acil durumlarda ise bilginin ilgili birime iletilmesinden sonra en kısa sürede paylaşımın sisteme işlenmesi öngörülebilir. Böylelikle idare, hukuki sorumluluğunu yerine getirmiş olacak ve olası ihlallerin önüne geçecektir.

İdarenin farklı birimleri arasında veri paylaşımı sırasında, KVKK m. 4'te yer alan temel ilkelere uyulmaya devam edilmesi zorunludur. Özellikle "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi, aynı tüzel kişilikteki birimlerin genellikle aynı amaçları güttüğü varsayımını doğursa da aykırı durumların göz ardı edilmemesi gerekir. Örneğin, belirli bir kamu hizmetinin sunulabilmesi için işlenen iletişim bilgilerinin İdarenin farklı bir birimi tarafından sosyal etkinliklere davet amacıyla kullanılması bir "amaç değişikliği" olarak değerlendirilmelidir. Bu durumda, kişisel verilerin ilgili birimle paylaşılabilmesi için ilgili kişiye yeniden aydınlatma yapılmalı veya şartlar gerektiriyorsa açık rızası alınmalıdır⁴¹¹.

⁴⁰⁹ KVK Kurulu, 22.4.2020 tarih ve 2020/307 sayılı kararı, <https://kvkk.gov.tr/Icerik/6895/2020-307> (E.T. 10.8.2024).

⁴¹⁰ Bir üniversite tarafından hazırlanan yönerge buna örnek olarak gösterilebilir: Üsküdar Üniversitesi, Kurum İçi Veri Paylaşımı Usul ve Esasları Yönergesi, <https://uskudar.edu.tr/assets/uploads/sayfa/18/file/uu-kurumici-veri-paylasimi-usul-ve-esaslari-yonergesi.pdf?1> (E.T. 17.12.2024).

⁴¹¹ Kişisel verilerin işlenmesinde amaç değişikliğine ilişkin açıklamalarımız için bkz.: "2. İDARENİN KİŞİSEL VERİ İŞLEME SÜREÇLERİNDE UYULMASI GEREKEN İLKELER" başlığı.

Veri işleme sürecinin başında gerçekleştirilen aydınlatma yükümlülüğü de tüzel kişilik içindeki veri paylaşımını kapsayacak şekilde düzenlenmelidir. İlgili kişinin, kişisel verilerinin idarenin farklı birimleri arasında hangi amaçlarla paylaşılacağı konusunda bilgilendirilmesi, şeffaflık ilkesinin bir gereğidir. Bu tür bir bilgilendirme, idarelerin veri işleme faaliyetlerini daha öngörülebilir hale getirirken, bireyin hak ve özgürlüklerinin korunması açısından da güvence sağlar.

Ayrıca, İdarenin veri işleme faaliyetlerinin kendi iç denetimini sağlamak amacıyla, GDPR kapsamında düzenlenen veri koruma görevlisi (Data Protection Officer - DPO) gibi bir mekanizmanın oluşturulması, İdarenin veri işleme süreçlerinde hukuka uygunluğun temini açısından önemli bir adım olabilir. GDPR’da veri koruma görevlisi, kamu otoriteleri ve büyük çapta veri işleyen kuruluşlar için zorunlu tutulmuş, görev ve yetkileri açıkça tanımlanmış bir pozisyonudur. Veri koruma görevlisinin temel işlevi, veri sorumlusunun veya veri işleyenin yürüttüğü veri işleme faaliyetlerinin GDPR ile uyumlu olmasını sağlamak, süreçleri izlemek ve rehberlik etmektir.

GDPR’nın 37, 38 ve 39. maddeleri, veri koruma görevlisinin atanması, bağımsızlığı ve görevlerini düzenlemektedir. Buna göre, veri koruma görevlisi, veri sorumlusu veya veri işleyenden bağımsız olarak çalışmakta; veri işleme faaliyetlerini denetleyerek ilgili mevzuata uyumun sağlanması, çalışanların eğitimi ve veri işleme süreçlerine ilişkin danışmanlık gibi önemli görevleri üstlenmektedir. DPO, aynı zamanda ilgili denetim otoritesiyle iletişimden sorumlu olup, bireylerin haklarının korunmasında da aktif rol oynamaktadır.

Türk hukuku bağlamında ise KVKK kapsamında GDPR’daki veri koruma görevlisiyle benzer bir zorunluluk getirilmemiştir. KVKK’nin uygulamasında, veri sorumlusunun hukuki sorumluluklarını yerine getirmesini denetleyecek ve süreçleri izleyerek rehberlik edecek bir kişiye ilişkin düzenleme bulunmamaktadır. Ancak, Kişisel Verileri Koruma Kurumu tarafından yayımlanan Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ⁴¹² ile veri koruma görevlisi kavramı ihdas edilmiş, ancak bu düzenleme gönüllülük esasına dayalı bir yapı olarak şekillenmiştir. Tebliğde tanımlanan veri koruma görevlisi, veri sorumlusunun çalışanları arasından seçilebileceği gibi dışarıdan yetkilendirilecek kişiler arasından da belirlenebilmektedir. Bu kişilerin görevi, veri sorumlusuna danışmanlık yapmak ve veri işleme faaliyetlerinin hukuka uygunluğunu sağlama noktasında destek sunmaktır.

Öte yandan, 10 Aralık 2021 tarihli Kurum duyurusunda, KVKK çerçevesinde getirilen veri koruma görevlisinin, GDPR’daki veri koruma görevlisi (DPO) ile aynı şey olmadığı açıkça ifade edilmiştir⁴¹³. Bu duyuruda, veri koruma görevlisinin tamamen gönüllülük esasına dayalı bir yapı olduğu vurgulanmış; dolayısıyla hukuki olarak idareler açısından bağlayıcı bir mekanizma oluşturmadığı

⁴¹² RG. 6.12.2021/31681.

⁴¹³ Kişisel Verileri Koruma Kurumu, “Veri Koruma Görevlisi Hakkında Kamuoyu Duyurusu”, 10.12.2021, <https://www.kvkk.gov.tr/Icerik/7100/Veri-Koruma-Gorevlisi-Hakkinda-Kamuoyu-Duyurusu> (E.T. 17.12.2024).

belirtilmiştir. DPO'nun aksine, KVKK kapsamında veri koruma görevlisinin atanması zorunlu değildir ve atanmış olsa dahi görevleri, bağımsızlık ve etkinlik açısından GDPR'daki yapıdan farklıdır.

Sonuçta, GDPR'da düzenlenen veri koruma görevlisi (DPO) mekanizmasının, kamu idarelerinde veri işleme faaliyetlerinin hukuka uygunluğunu sağlamak adına etkin bir rol oynadığı açıktır. Türk hukuku açısından bu tür bir düzenlemenin eksikliği, idarenin iç denetim mekanizmalarında bir boşluk oluşturmaktadır. Ancak, KVKK kapsamında isteğe bağlı olarak veri koruma görevlisi atanması, idarelerin kendi iç yönergeleri ve prosedürleriyle veri işleme faaliyetlerinin denetimini sağlama yolunda bir adım olarak değerlendirilebilir. Buna rağmen, gönüllülük esasına dayanan bu yapının, GDPR'daki zorunlu veri koruma görevlisi mekanizması ile eşdeğer bir etki yaratmadığını ve Kurum tarafından da bu farkın açıkça ifade edildiğini göz önünde bulundurmak gerekir. Bu nedenle, kamu idarelerinde veri işleme süreçlerinin hukuka uygunluğunu temin edecek bağımsız ve etkili bir denetim mekanizmasının oluşturulması, idarenin hesap verebilirliğini ve şeffaflığını artırmak adına önemli bir ihtiyaç olarak kabul edilmelidir.

Sonuç olarak, gerek idarenin farklı birimleri arasındaki veri paylaşımında gerekse idareler arasında veri aktarımı yapılırken hukuki düzenlemelere uygun hareket edilmesi, veri işlemenin denetlenebilirliğini ve şeffaflığını güvence altına alır. İdarelerin kendi birimleri arasındaki veri paylaşımına ilişkin bir iç yönerge oluşturması, veri paylaşım taleplerinin kayıt altında tutulması, süreçlerin sistematik hale getirilmesi ve bunların GDPR'da yer verilen veri koruma görevlisi (DPO) benzeri görevlilerle iç işleyişte de denetlenmesi, hem hukuki sorumlulukların yerine getirilmesini sağlayacak hem de bireylerin kişisel verilerinin korunması bakımından güvenli bir çerçeve sunacaktır.

Öte yandan, idareler arası veri aktarımında da benzer şekilde KVKK hükümleri çerçevesinde hareket edilmesi, kamu işleyişinin hukuka uygun şekilde devamını sağlar. Bu kapsamda, veri paylaşımının ilgili mevzuatta belirlenen şartlara uygun olması ve yalnızca talep edilen amacın gerçekleştirilmesine yönelik ölçüde bilgi ve belge paylaşımında bulunulması önem arz eder. Özellikle kişisel veri içeren bilgi ve belgelerin paylaşımında, hukuki dayanağın varlığı değerlendirilmeden işlem yapılmamalı; ilgili kişinin açık rızası aranmaksızın veri aktarımı gerçekleştirilmesi gereken durumlarda, KVKK'nın 5. ve 6. maddelerinde belirtilen istisnalardan birinin varlığı teyit edilmelidir. Ayrıca, idareler arasında paylaşılan belgelerin asıllarına yönelik güvenlik endişelerinin giderilmesi amacıyla gerekli tedbirlerin alınması ve belgenin bir kopyasının talep eden idareye sunulması, kamusal işleyişin aksamaması açısından büyük önem taşır. Tüm bu hususlara riayet edilmesi, hem kamu idarelerinin hukuki yükümlülüklerini yerine getirmelerini sağlayacak hem de bireylerin kişisel verilerinin korunması bakımından güvenli bir çerçeve sunacaktır.

4.4.3.2. İdarenin Kişisel Verileri Yurt İçinde Gerçek Kişilere Aktarması

İdarenin gerçek kişilere kişisel veri aktarması, KVKK'nın 8. maddesi kapsamında bir veri aktarımı olarak kabul edilmektedir. Bu bağlamda, idarenin diğer idarelerle veri paylaşımında olduğu

gibi, gerçek kişilerle gerçekleştirdiği veri aktarımında da esasen hukuki dayanak ve sınırlamalara uygun hareket etme zorunluluğu bulunmaktadır. KVKK'ye göre, kişisel verilerin aktarılması kural olarak ilgili kişinin açık rızasına tabidir. Ancak, KVKK m. 5/2 ve m. 6/3 hükümlerinde öngörülen belirli şartların varlığı halinde, ilgili kişinin açık rızası aranmaksızın veri aktarımı mümkündür. Bu şartlar arasında, hukuki yükümlülüklerin yerine getirilmesi, bir hakkın tesisi, kullanılması veya korunması için zorunluluk, kişinin hayatı veya beden bütünlüğünün korunması gibi durumlar yer almaktadır.

Bu çerçevede, idarenin kişisel verileri gerçek kişilere aktarması, veri koruma hukuku açısından hassas ve dikkat gerektiren bir işlem olarak öne çıkmaktadır. Çünkü veri aktarılan tarafın, kamu otoritesine kıyasla bireysel bir konumda bulunması, verinin korunması açısından ek riskler doğurabilir. Uygulamada bu konuya ilişkin tartışmalı birçok örnek mevcuttur. Bu bölümde, idarenin veri aktarımına ilişkin yaygın ve dikkat çeken iki örnek üzerinden bir değerlendirme yapılacaktır. Bu örneklerden ilki, HIV virüsü taşıyan kişilere ilişkin sağlık verilerinin, kişinin eşi veya birlikte olduğu partnerine bildirilmesi; diğeri ise, yurttan kalan bir öğrencinin yurttan olup olmadığı ya da sağlık durumu gibi kişisel verilerinin, velisi veya acil durumlarda irtibat kurulacak kişilerle paylaşılmasıdır. Her iki örnek de kamu sağlığının korunması, bireyin üstün yararı ve hukuki yükümlülüklerin yerine getirilmesi gibi temel gerekçelerle veri aktarımına dayanak oluşturmakta; bu aktarımın hangi şartlarda ve ne ölçüde hukuka uygun olacağı, uygulamada karşılaşılan önemli sorun alanlarından biri olarak karşımıza çıkmaktadır.

Kişisel sağlık verilerinin korunması ile toplum sağlığının korunması arasındaki hassas denge, özellikle bulaşıcı hastalıklar söz konusu olduğunda daha da önem kazanmaktadır. Bu bağlamda, HIV gibi ciddi ve bulaşıcı hastalıkların eş ya da eş adayına bildirilmesi meselesi hem tıbbi etik hem de hukuki açıdan tartışmalı bir konu olarak karşımıza çıkmaktadır. Bu durum, bireyin mahremiyet hakkı ile potansiyel olarak risk altında olan kişilerin sağlığını koruma yükümlülüğü arasında bir ikilem yaratmaktadır.

Başta ifade etmek gerekirse, Türkiye'de HIV pozitif olan kişilerin eşlerine ya da eş adaylarına sağlık personeline bilgi verilmesi yönünde açık bir yasal düzenleme bulunmamaktadır⁴¹⁴. Umumi Hıfzıssıhha Kanunu'nun 'zührevi (cinsel yolla bulaşan) hastalıklarla mücadele' kısmında, bu tür hastalıklara yakalananların Sağlık Bakanlığı'na bildirilmesi gerektiği ifade edilse de eş ya da yakınlarına bildirilmesini öngören açık bir hüküm bulunmamaktadır. İstisna olarak, zührevi hastalığa yakalananın çocuk olması halinde ebeveynlerinin bilgilendirilmesi gerektiği 109. maddede kabul edilmiştir. Türk Ceza Kanunu ise bir yandan göreve ilişkin sırrın açıklanmasını suç olarak kabul etmişken (m.258), diğer yandan sağlık mesleği mensuplarının suçu bildirmemesi halinde cezalandırılacağını kabul etmiştir (m.280). Öte yandan, Türk Tabipler Birliği'nce kabul edilen 'Hekimlik Meslek Etiği Kuralları'nın 'sır saklama yükümlülüğü' başlıklı 9/2. maddesinde "*Hastanın onam vermesi ya da sırrın saklanması*

⁴¹⁴ Mehmet KARATAŞ, Adnan ATEŞ, Muharrem UÇAR, M. Nabi KANTARCI, "HIV Pozitif Kişilerin Eşlerine Hastalığı Bildirme(me)nin Yasal ve Etik Açısından Değerlendirilmesi", *İnönü Üniversitesi Tıp Fakültesi Dergisi*, 17(3), 2010, s.217.

hasta ya da öteki insanların yaşamını tehlikeye sokması durumunda, hastanın kişilik haklarının zedelenmemesi koşuluyla, hekim bu sırrı saklamakla yükümlü değildir” kuralına yer verilmiştir. Yine 26. maddesinde hastanın dışında bilgilendirilecek kişilerin, hastanın kendisi tarafından belirleneceği kuralı kabul edilmiştir.

Günümüzde HIV/AIDS hastalığı ölümcül bir hastalık olarak kabul edilmemekte, düzenli şekilde takip ve tedavi edilmesi halinde hastanın normal bireyler gibi yaşam sürebileceği ifade edilmektedir⁴¹⁵. Bununla birlikte, hasta kişinin tedaviyi reddetmesi yahut düzenli şekilde devam etmemesi, cinsel birlikteliklerinde korunmaması halinde eşin, hatta gebe olması halinde çocuğun beden bütünlüğünü tehlikeye sokması ihtimali yüksek görünmektedir. Dolayısıyla, hastanın kişisel verilerinin korunması hakkı ile üçüncü kişilerin yaşam hakkı arasında bir çatışma söz konusudur. Bu durumda, üçüncü kişilerin yaşam hakkının, hastanın kişisel verilerinin korunması hakkından daha büyük değer taşıdığı kabul edilerek, eş veya eş adayına bilgilendirme yapılması gerektiği kabul edilmelidir⁴¹⁶.

Nitekim, ambulansla hastaneye kaldırılan ve bilinci kapalı olan bir hastanın yakınları tarafından ambulanstaki görevlilere hastanın HIV virüsü taşıdığı bilgisinin verilmesi, bu görevlilerinse hastanedeki diğer görevlilerle bu bilgiyi paylaşması ve birçok görevlinin konudan haberdar olması nedeniyle uğranılan zararın tazmini için yapılan başvuruya ilişkin AİHM kararında şu ifadelerle yer verilmiştir: *“Bununla birlikte Mahkeme, tıbbi verilere saygı gösterilmesi hakkının da mutlak bir hak olmadığına altını çizmektedir... Özellikle, HIV taşıyan hastalar dahil olmak üzere hastanelerde ve sağlık hizmetlerinde hastaların tedavileri söz konusu olduğunda salt hastanın uygun tedaviyi almasını sağlamak için değil ayrıca gerekli ihtiyati tedbirlerin alınmasına izin vererek hastanın tedavisinde yer alan bakım yapan personelin haklarının ve menfaatlerinin de korunmasına dikkat edilmesi amacıyla hastanın durumuna ilişkin bilginin aktarılması bazı koşullarda doğru ve gerekli olarak gözükebilir. Dolayısıyla bilgiyi aktaracak kişinin sağlık profesyonellerine özgü gizlilik kurallarına veya benzer gizlilik kurallarına uymasına dikkat edilmesi gerekir.”* Bu bağlamda mahkeme, HIV taşıyan hastanın tedavisi için müdahalede bulunan sağlık personellerine bilgi verilmesinin, görevleri nedeniyle sağlık personellerinin HIV’e yakalanmasını engelleyebileceği gerçeğine dikkat çekmiştir⁴¹⁷.

HIV pozitifin tespiti halinde bu bilginin eş ya da eş adayı ile paylaşılmasına ilişkin Halk Sağlığı Genel Müdürlüğü’nün 5.9.2023 tarihli yazısında, konuya ilişkin olarak KVK Kurulu’na danışıldığı, Kurul’un 16.5.2019 tarih ve 2019/134 sayılı cevabi yazısından hareketle, 6698 sayılı Kanun’un 6. maddesinde sağlık verilerinin koruyucu hekimlik kapsamında işlenmesine izin verildiğinden, HIV pozitif olan kişinin eş ya da eş adayıyla bu bilginin paylaşılmasının mümkün olduğu, ancak her vakanın

⁴¹⁵ Selma TOSUN, “HIV Pozitif Kişilerin Cinsel Partnerlerine ve Yakınlarına Hastalığın Bildirilmesi”. ERKOL ZZ, DOĞRAMACI YG (Editörler), **Tıp Hukuku**. 1. Baskı. Ankara: Türkiye Klinikleri; 2019. s.88-96.

⁴¹⁶ Hakan HAKERİ, **Tıp Hukuku Cilt 1: Genel Hükümler**, Seçkin Yayıncılık, 26. Baskı, 2024, s.287.

⁴¹⁷ AİHM, Y / Türkiye, B.n. 648/10, T.17.2.2015, §74-78, <https://hudoc.echr.coe.int/tur?i=001-157633>.

ayrı şekilde değerlendirilerek üçüncü kişinin yaşam hakkını korumayı gerektirecek bir kamu yararı bulunup bulunmadığının tespit edilmesi gerektiği ifade edilmiştir. Bu bağlamda, önce hastanın kendisiyle konuşularak durumu hakkında eş ya da eş adayıyla paylaşması için ikna edilmeye çalışılması gerektiği, bu konuda ikna edilemezse ölçülülük ilkesine riayet edilmek suretiyle durumun aciliyetinin değerlendirilmesi, sonuçta hastalığın eş ya da eş adayına açıklama yapılmasında yaşama hakkı gibi kişisel verilerin korunması hakkına daha üstün gelebilecek nitelikte bir kamu yararının bulunduğu sonucuna varılması halinde bu durum hakkında hastanın aydınlatılmasına müteakip bilginin eşe ya da eş adayına açıklanması gerektiği, tüm bu sürecinse gerekçeli olarak belgelendirilmesi gerektiği ifade edilmiştir⁴¹⁸. Sonuçta, yaşam hakkı söz konusu olan üçüncü kişinin bilgilendirilmesinin KVKK hükümleriyle de uyumlu olduğu ancak, ölçülülük ilkesi bağlamında bu bilgilendirmenin öncelikle hasta tarafından yapılmasının teşviki, bunda başarısız olunması halinde hekim tarafından eşin ya da eş adayının bilgilendirilmesi gerektiği söylenebilir.

Öte yandan, HIV virüsü bulaşmış kimsenin evlenmesine engel bir durum bulunmamaktadır. Nitekim, 1593 sayılı Umumi Hıfzıssıhha Kanunu’nun 123. ve 124. maddelerinde evlenmeye engel hastalıklar frengi, bel soğukluğu, yumuşak şankr, cüzzam ve ilerlemiş sarî verem olarak belirlenmiştir. Evlendirme Yönetmeliği’nin 15/3. maddesinde “*Umumi Hıfzıssıhha Kanununa dayanılarak, 17/8/1931 tarihli ve 11682 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Evlenme Muayenesi Hakkında Nizamnamede öngörülen usul ve esaslar doğrultusunda sağlık raporu alınmaması durumunda evlenme yapılamaz*” kuralına yer verilmiştir. İlgili Nizamname’nin 7. maddesi uyarınca, yapılan tetkiklerde eş adaylarından birinin evlenmeye engel hastalıklardan birine sahip olduğu anlaşılırsa kişilere sağlık raporu verilmeyecektir. HIV, ilgili Kanun’da sayılan hastalıklardan biri olmadığı için, tespit edilse de gerekli sağlık raporu yazılarak taraflara verilmelidir. Bununla birlikte, yukarıda izah edilen gerekçelerle, hasta olmayan eş adayının durumdan haberdar edilmesi gereklidir. Bu bağlamda, öncelikle hastalık teşhisi konulan kişinin eş adayına durumu anlatması için fırsat verilmeli, hastalığın gizli tutulmasına yönelik talebi kabul edilmemelidir. Hastanın, tüm çabalara rağmen ikna edilememesi halinde, sorumlu doktorun bu sağlık verisini eş adayı ile paylaşması KVKK bağlamında da hukuka uygun olacaktır.

Ayrıca, yukarıda yapılan değerlendirmelerin yalnızca HIV virüsü ile sınırlı olmadığı, bulaşıcılığı bulunan, tedavi edilmediği takdirde hastada ölüm tehlikesi yaratan ya da hayatını çekilmez kılacak türde ömür boyu belirli ilaçları kullanmak durumunda bırakan hastalıkların da bu kapsamda kabul edilmesi gerektiği değerlendirilmektedir. Nitekim, Türk Medeni Kanunu’nun 149/2. maddesinde, “*eşinde bulunmaması onunla birlikte yaşamayı kendisi için çekilmez bir duruma sokacak derecede önemli bir nitelikte yanılarak evlenmişse*” bu yanılma nedeniyle diğer eşin evlenmenin iptalini dava edebileceği; 150/2. maddesinde ise, “*Davacının veya altsoyunun sağlığı için ağır tehlike oluşturan bir hastalık kendisinden gizlenmişse*” bilgi kendisinden gizlenen eşin bu aldatma nedeniyle evliliğin iptalini

⁴¹⁸ HAKERİ, **Tıp Hukuku** Cilt 1, s. 287-288.

dava edebileceği kabul edilmiştir. Evliliğin iptaline imkân veren bir hususun evlilik öncesinde tespit edilmesine rağmen İdare eliyle gizlenmesi hukuk mantığıyla da çelişir.

İdarenin veri paylaşımına ilişkin bir başka husus, yurtlarda kalan öğrencilere ait bilgilerin velileriyle paylaşılmasıdır. Gençlik ve Spor Bakanlığı Kredi ve Yurtlar Kurumu'na ait öğrenci yurtları, öğrencilerin konakladığı ve eğitim hayatını tamamladığı önemli sosyal alanlardır. Bu bağlamda, idarenin, yurtlarda kalan öğrenciler hakkında velilerden gelen bilgi taleplerini karşılaması hem idarenin Anayasa'dan kaynaklanan görevleri hem de bireylerin temel hak ve özgürlükleri çerçevesinde ele alınmalıdır. Anayasa'nın 41. maddesi, devletin çocukları her türlü istismara ve şiddete karşı koruma yükümlülüğünü düzenlerken, 58. maddesi gençlerin zararlı alışkanlıklardan korunmasını ve sağlıklı bir şekilde yetiştirilmesini vurgulamaktadır. Bu anayasal hükümler, idareye öğrencilerin üstün yararını gözetme sorumluluğunu yüklerken, aynı zamanda bilgi paylaşımı gibi veri işleme süreçlerinde ölçülülük ilkesine uygun hareket edilmesini gerektirir.

Bu çerçevede, KVKK'nın 5. maddesinde yer alan veri işleme şartlarının ve diğer kanuni düzenlemelerin, Anayasa'nın çocukların ve gençlerin korunmasına ilişkin bu hükümleriyle birlikte değerlendirilmesi gerekir. Özellikle, velilerden gelen bilgi taleplerine yanıt verirken, idarenin, çocuğun üstün yararını ve gençlerin korunmasını anayasal bir yükümlülük olarak göz önünde bulundurması, bu yükümlülüklerin KVKK bağlamında nasıl yerine getirileceğinin somut olay bazında açıklığa kavuşturulmasını sağlayacaktır.

KVKK'nın 5. maddesinin 2. fıkrasında ya da 6. maddesinin 3. fıkrasında sayılan veri işleme şartlarından birinin varlığı halinde bu şartlara istinaden veri paylaşımında bulunulabileceği gibi, bu şartlardan hiçbirinin sağlanamaması durumunda öğrenciden açık rıza alınarak bilgi paylaşımı yapılabilir⁴¹⁹. Bu bakımdan, Öğrenci İzin İşlemleri Uygulama Usul ve Esasları Hakkında Yönerge'nin 4. maddesinde yer verilen öğrenci yakını tanımı yol göstericidir⁴²⁰. Buna göre, öğrenci yakını “18 yaşından büyük öğrenciler için, acil durumlarda veya idarece gerek görüldüğünde irtibat kurulacak olan ve öğrenci tarafından kayıt işlemleri sırasında beyan edilen, adres ve GSM numarası bildirilen kişi” şeklinde tanımlanmıştır. Dolayısıyla, öncelikle öğrenci hakkında bilgi isteyen kişinin öğrenci 18 yaşından büyükse kayıt sırasında bilgileri alınan kişi olup olmadığı; 18 yaşından küçükse anne ve babası olup olmadığı (duruma göre vesayet yetkisini elinde bulunduran kişi) kontrol edilmelidir.

Sonrasında, paylaşımı istenen bilginin niteliği değerlendirilmelidir. Örneğin, Yurt Hizmetleri Yönetmeliği'nin 31/5. maddesi uyarınca, reşit olmayan öğrencinin almış olduğu disiplin cezalarının

⁴¹⁹ Yaşı küçük çocuklardan alınacak rıza beyanlarına ilişkin açıklamalarımız için bkz.: “4.4.1.1. Kişisel Verinin İşlenebilmesinin Genel Şartı Olarak “Açık Rıza” başlığı.

⁴²⁰ Gençlik ve Spor Bakanlığı Öğrenci İzin İşlemleri Uygulama ve Esasları Hakkında Yönerge, <https://kygm.gsb.gov.tr/Sayfalar/2432/2387/mevzuat.aspx> (E.T. 10.8.2024)

öğrenci velisine bildirilmesi gerekir⁴²¹. Dolayısıyla İdare, hukuki yükümlülüğün yerine getirilmesi için zorunlu olması şartına dayanarak, reşit olmayan öğrencinin disiplin cezası aldığına dair bilgiyi öğrencinin velisiyle paylaşacaktır. Öğrenci bilgilerinin velilerle paylaşımı, çocuğun üstün yararını korumak ve velilerin eğitim sürecine katılımını sağlamak amacıyla idarenin anayasal yükümlülükleriyle doğrudan ilişkilidir. Anayasa'nın 41. maddesi, devletin çocukları her türlü istismara ve şiddete karşı koruma yükümlülüğünü düzenlerken, 58. maddesi, gençlerin zararlı alışkanlıklardan korunması ve sağlıklı bir şekilde yetiştirilmeleri için idareye hem bir gözetim hem de müdahale yetkisi tanımaktadır. Bu anayasal hükümler, idareye çocukların ve gençlerin eğitim süreçlerini destekleyecek bir sorumluluk yükler. Bu doğrultuda, Yurt Hizmetleri Yönetmeliği'nin 31/5. maddesi uyarınca, reşit olmayan öğrencinin disiplin cezası aldığına ilişkin bilginin velilere iletilmesi, idarenin çocukların üstün yararını koruma yükümlülüğünün bir yansımasıdır. Çocuğun davranışlarına ilişkin velilerin bilgilendirilmesi, onların eğitim sürecine etkin bir şekilde katılımını sağlamakta ve çocukların sosyal gelişimini desteklemektedir. Dolayısıyla, getirilen bu yükümlülüğün ayırt etme gücünü haiz ancak ergin olmayan öğrenciler bakımından da geçerli kabul edilmesinin, ölçülülük ilkesi bağlamında değerlendirildiğinde, çocuğun üstün yararının korunması ve velilerin eğitim sürecine katılımının sağlanması bakımından hukuka uygun bir düzenleme olduğu ifade edilmelidir⁴²².

Öte yandan Yönergede, öğrenci yakını “18 yaşından büyük öğrenciler için, acil durumlarda veya idarece gerek görüldüğünde irtibat kurulacak olan ve öğrenci tarafından kayıt işlemleri sırasında beyan edilen, adres ve GSM numarası bildirilen kişi” şeklinde tanımlanmıştır. Bu kapsamda, öğrencinin üstün menfaatlerini koruma amacıyla bilgi paylaşımı yapılması, yalnızca 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 5/2(b) maddesi çerçevesinde meşru kabul edilebilir. Söz konusu hüküm, “*fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması*” şartını düzenlemektedir. Örneğin, öğrenciyle uzun bir süredir iletişim kurulamaması, telefonunun kapalı olması ve öğrencinin yurttan bulunup bulunmadığına ilişkin bir bilgi talebinin hayati risk içermesi durumunda, bu bilgi paylaşılabilir.

Ancak, bu tür bir paylaşımın KVKK m. 5/2(b) kapsamında değerlendirilmesi için, “hayatın veya beden bütünlüğünün korunması” gerekçesinin açık ve somut bir şekilde ortaya konması gerekmektedir. Söz konusu bilgi paylaşımı, yalnızca fiili imkânsızlık durumunda ve hayati risklerin varlığı halinde zorunlu bir tedbir olarak ele alınmalıdır. Bu sınırlar dışında, öğrencinin bilgileri ancak açık rızasına dayalı olarak paylaşılabilir. Yurt sorumlularının, öğrenciye ulaşmayı denemesi, durumu açıklaması ve

⁴²¹ Gençlik ve Spor Bakanlığı Yurt Hizmetleri Yönetmeliği, RG, 9.4.2021/31449. **Madde 31-** (5) Disiplin cezaları reşit olmayan öğrencinin velisine bildirilir. Yurttan çıkarma cezaları ise ayrıca öğrencinin kayıtlı bulunduğu öğretim kurumuna yazılı olarak bildirilir.

⁴²² Konuya ilişkin ayrıntılı değerlendirmemiz için bkz.: “**2.1.1. Eğitim Hizmetlerinde Dijitalleşme ve Kişisel Veri Güvenliği**” başlığı.

bilginin paylaşılmasına ilişkin rızasını alması temel bir yükümlülük olarak kabul edilmelidir. Rıza alınamaması durumunda, öğrenci yakınına yalnızca öğrencinin durumuna ilişkin genel bir bilgilendirme yapılmalı, detaylı bilgi paylaşımından kaçınılmalıdır.

“Acil durum” kavramının, KVKK m. 5/2(b) hükmüne uygun bir şekilde dar yorumlanması gereklidir. Örneğin, yalnızca iletişim kurulamaması gibi bir gerekçe, hayati risk taşımadığı sürece, bilgi paylaşımı için yeterli değildir. Bu nedenle, her veri paylaşımında, hem öğrencinin temel hak ve özgürlüklerini hem de KVKK’nın veri işleme şartlarını gözetten bir yaklaşım benimsenmelidir.

Öğrencinin bir olay sonucunda suç soruşturması kapsamında gözaltına alınması ya da bir sağlık sorunuyla karşılaşarak tedavi altına alınması gibi durumlarda, genellikle özel nitelikli kişisel verilerin işlenmesi söz konusu olmaktadır. Bu gibi hallerde, eğer öğrenciyle iletişim kurulabiliyorsa, durumunun velisi veya belirttiği başka bir kişiyle paylaşılmasına ilişkin açık rızası alınmalı ve bu rızaya uygun şekilde hareket edilmelidir. Ancak, fiili imkânsızlık nedeniyle öğrenciyle iletişim kurulamıyorsa, KVKK m. 6/3(c) gereğince, fiili imkânsızlık hali gerekçesiyle, öğrencinin hayatını veya beden bütünlüğünü korumak amacıyla veri paylaşımı yapılabilir. Ancak bu tür durumlarda Kanunun 4. maddesinde belirlenen veri işleme ilkelerinin titizlikle değerlendirilmesi gerekmektedir.

Öğrencinin sağlık sorunlarında, hayati risk taşıyan veya acil tıbbi müdahale gerektiren durumlarda bilgi paylaşımı yapılması zorunlu olabilir. Örneğin, bir alerjik reaksiyon, ciddi bir yaralanma ya da bilinç kaybı gibi durumlarda, velinin bilgilendirilmesi öğrencinin sağlık ve güvenliğinin sağlanması açısından meşru bir veri işleme faaliyetidir. Buna karşın, rutin tıbbi kontroller ya da ciddi risk taşımayan tedavi süreçlerinde bilgi paylaşımı, öğrencinin açık rızasına dayalı olarak yapılmalıdır.

Benzer şekilde, öğrencinin emniyette ifade vermek üzere bulunduğu hallerde, yalnızca öğrencinin haklarını doğrudan etkileyebilecek bir soruşturma ya da ciddi bir suçlama söz konusu olduğunda bilgi paylaşımı yapılması gereklidir. Örneğin, öğrencinin bir ifadeye tanık sıfatıyla çağırılması ya da idari bir süreç kapsamında bilgi vermesi, acil veya gerekli bir bilgi paylaşımı kapsamında değerlendirilmemelidir. Böyle bir durumda, durumu açıklığa kavuşturmak için makul bir süre beklenmeli ve gerekirse öğrencinin açık rızasının alınması sağlanmalıdır.

Bu tür değerlendirmelerde, reşit olmayan öğrenciler için çocuğun üstün yararını koruma ilkesi ön planda tutulmalı ve veliye bilgi paylaşımı bu doğrultuda geniş yorumlanmalıdır. Ancak, reşit öğrenciler açısından, kişisel veri işleme faaliyetleri dar bir yoruma tabi tutulmalı ve öğrencinin açık rızasına dayalı olarak gerçekleştirilmelidir. Bu, hem veri minimizasyonu ilkesine uygun hareket edilmesini hem de öğrencinin kişisel veri hakkının korunmasını sağlar.

Sonuç olarak, idarenin özellikle gerçek kişilere kişisel veri aktarımına ilişkin uygulamalarının iki temel eksen üzerinden şekillenmesi gerektiği ifade edilebilir. Bunlardan ilki, bireyin özel hayatına ve kişisel verilerine saygı gösterilmesi, temel hak ve özgürlüklerin hukuka uygun ve ölçülü şekilde

sınırlandırılmasıdır. İkincisi ise, meşru ve üstün nitelikli kamusal menfaatlerin, özellikle çocukların ve gençlerin korunması gibi anayasal sorumluluklar çerçevesinde tesisi için, verilerin gerektiği ölçüde ve kanuni sınırlar içinde işlenebilmesidir. Çocuğun üstün yararını gözetmek, gerek çocuğu dış tehditlerden koruma gerekse çocuğun kendi davranışlarının olası olumsuz sonuçlarından koruma amacıyla, bu menfaatlerin somut bir şekilde belirlenmesini gerektirir. İdarenin bu iki yan arasında makul bir denge kurması, somut olayın özelliklerini dikkate alarak, veri işleme ilkeleri ve pozitif düzenlemeler ışığında hareket etmesini gerektirir. Kişisel verilerin korunması hakkının istisnalarının dar yorumlanması ve bu alanda özgürlüklerin esas, sınırlamaların istisna olduğu unutulmamalıdır. Bununla birlikte, meşru amaçlarla ve hukuka uygun olarak işlenen verilerin, kamusal ihtiyaçların karşılanması ve hizmet kalitesinin artırılmasına da katkı sağlayacağı açıktır.

4.4.3.3. İdarenin Kişisel Verileri Yurt Dışına Aktarması

Kişisel verilerin yurt dışına aktarılmasına ilişkin olarak KVKK'nin 9. maddesinde yer verilen düzenlemeye uygun şekilde hareket edilmesi gerekmektedir. Bu itibarla, öncelikle maddenin ilk fıkrasına göre, kişisel veriler ancak KVKK'nin 5. ve 6. maddelerindeki şartlardan birinin varlığı halinde ve aktarımın yapılacağı ülke hakkında Kurul tarafından "yeterlilik kararı" verilmişse yurt dışına aktarılabilir. Yeterlilik kararı verilirken, 3. fıkra da sayılan hususlar dikkate alınır. Bunlar arasında, aktarım yapılacak ülkedeki mevzuat, bağımsız veri koruma kurumunun varlığı, uluslararası sözleşmelere taraf olma durumu gibi kriterler yer almaktadır.

Bununla birlikte, yeterlilik kararı bulunmadığı durumlarda maddenin 4. fıkra hükmü işletilebilmektedir. Buna göre, Kanunun 5. ve 6. maddelerinde sayılan şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkanının bulunması şartıyla, söz konusu fıkra da belirlenen 'uygun güvenceler' arasından birinin varlığı halinde İdarenin yurt dışına veri aktarması mümkün kılınmaktadır. Örneğin, fıkranın (a) bendine göre, yukarıdaki şartlarla birlikte yurt dışındaki kamu kurum ve kuruluşları ile Türkiye'deki kamu kurum ve kuruluşları arasında yapılan uluslararası nitelikte olmayan bir anlaşmanın varlığı ve Kurulun aktarıma izin vermesi halinde İdare yurt dışı aktarımı yapabilecektir.

Öte yandan, 6. fıkra ile, yeterlilik kararının bulunmaması ve 4. fıkra da sayılan güvencelerin de sağlanamaması halinde dahi, arızı olmak kaydıyla bu fıkra altında belirlenen hallerde yurt dışına kişisel veri aktarımında bulunulması mümkün kılınmıştır⁴²³. Ancak, 7. fıkra uyarınca, kamu kurum ve kuruluşlarının kamu hukukuna tabi faaliyetleri için 6. fıkranın (a), (b) ve (c) bentlerinin uygulanamayacağı kabul edilmiştir⁴²⁴. Bu halde İdare, arızı olsa bile ilgilinin açık rızası, sözleşmenin

⁴²³ Arızı olmak kaydıyla veri aktarımı yapılabilecek haller hakkında açıklamalar için bkz.: KAYA, s.47 vd.

⁴²⁴ **KVKK, Madde 9 – (6) a)** İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.

ifası ya da ilgili kişi yararına üçüncü kişilerle yapılacak sözleşmenin kurulması veya ifası için zorunlu olması istisnalarına dayanarak yurt dışına veri aktarımı yapamayacaktır⁴²⁵.

Arızı olmak ifadesi sözlük anlamıyla ‘geçici, sonradan olan’, rastlantısal şeklinde ifade edilebilir⁴²⁶. KVKK bağlamında ise, 6. fıkrada sayılan ve istisnai nitelik taşıyan yurt dışı aktarım şartlarının düzenli ve sürekli değil, sadece belirli durumlarda uygulanabileceği şeklinde anlaşılması yerinde olacaktır. Örneğin, ilgili kişinin sağlığı ve hayati öneme sahip menfaatleri için gerekli olması (m.6/1-e) veya bir hakkın tesisi, kullanılması ya da korunması için veri aktarımının zorunlu olması (m.6/1-d) gibi haller, süreklilik arz eden rutin aktarımlar olarak değil, münferit ve geçici nitelikte aktarımlar olarak değerlendirilmelidir. Kanun koyucunun buradaki amacı, istisnaların kural haline gelmesini ve yurt dışı aktarımın serbest dolaşım ilkesinin önüne geçmesini engellemek olabilir.

Son olarak, KVKK’nin 9. maddesinin 9. fıkrası kişisel verilerin yurtdışına aktarılmasına ilişkin belirli bir düzenleme getirmektedir. Bu hükme göre, *"kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir."* Bu hüküm, uluslararası sözleşmelerin öncelikli olduğunu açıkça ifade etmekle birlikte, KVKK’nin diğer kısımlarının tamamen devre dışı kalacağı anlamına gelmemektedir. Veri işleme ve aktarım süreçlerinin uluslararası metinlerle çelişmediği durumlarda, KVKK’nin genel ilkeleri hâlâ geçerliliğini korumaktadır.

Dolayısıyla, çifte vergilendirmeyi önleme anlaşmaları, Yabancı Hesaplar Vergi Uyum Kanunu (FATCA)⁴²⁷, Ortak Raporlama Standardı (CRS)⁴²⁸ gibi düzenlemeler kapsamında yapılan veri paylaşımları, söz konusu anlaşmalarda açık veri aktarım hükümlerinin bulunması hâlinde KVKK m.9/9’un öngördüğü "Kurul izni" gibi prosedürlere tabi olmayabilir. Ancak uluslararası metinlerde veri aktarımına ilişkin özel hükümler yer almıyorsa veya ek koruma tedbirleri talep edilen durumlar söz

b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.

c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.

⁴²⁵ Özel hukuk kişileri söz konusu bentlere dayanarak yurt dışına veri aktarımında bulunabilecektir. Buna ek olarak hem kamu idarelerinin hem de özel hukuk kişilerinin veri aktarmada dayanabileceği haller ilgili hükümde şu şekilde düzenlenmiştir:

KVKK, Madde 9 – (6) ç) Aktarımın üstün bir kamu yararı için zorunlu olması.

d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması.

e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.

f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması.

⁴²⁶ Türk Dil Kurumu, **Güncel Türkçe Sözlük**, <https://sozluk.gov.tr/> (E.T. 11.8.2024).

⁴²⁷ United States, Congress. *Foreign Account Tax Compliance Act (FATCA)*. Hiring Incentives to Restore Employment Act, Title V, Subtitle A, Public Law 111–147, 18 Mar. 2010, 124 Stat. 71.

⁴²⁸ Organisation for Economic Co-operation and Development (OECD). *Common Reporting Standard (CRS): Standard for Automatic Exchange of Financial Account Information in Tax Matters*. Second Edition, OECD Publishing, 2017, <https://doi.org/10.1787/9789264267992-en>. (E.T. 3.1.2025)

konusuysa, Kurul izni alınması gerekebilecektir. Bu durum, Türkiye'nin uluslararası yükümlülüklerini yerine getirmesi bağlamında önemli bir istisna teşkil etmekle birlikte, kişisel verilerin işlenmesi ilkelerinin tamamen devre dışı kaldığı anlamına gelmez⁴²⁹.

KVKK m.9/9'un uygulanabilirliği, uluslararası bir sözleşme veya anlaşmanın bulunmadığı ve Türkiye ile ilgili kişinin menfaatinin ciddi şekilde zarar görebileceği durumlarla sınırlıdır. Örneğin, Türkiye'nin vergi anlaşması bulunmayan bir ülkede yaşayan bir Türk vatandaşının finansal bilgilerinin talep edilmesi, Kurul izni ve ilgili kamu otoritelerinin görüşü alınarak karara bağlanabilir. Benzer şekilde, yabancı bir sağlık kuruluşunun, Türkiye'de tedavi gören bir hastanın verilerini talep ettiği bir senaryoda, uluslararası bir anlaşma bulunmuyorsa, veri aktarımı KVKK m.9/9'a göre değerlendirilmelidir. Burada, "Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği" kriteri, somut olayın koşullarına göre değerlendirilecek olup özellikle kamu düzeni, bireylerin hayatı veya beden bütünlüğü gibi hususlarda Kurulun takdir yetkisi önem kazanmaktadır.

⁴²⁹ FATCA ve CRS gibi düzenlemeler, uluslararası vergi uyumu sağlama amacı taşımakta ve ülkeler arasında finansal bilgilerin otomatik olarak paylaşılmasını öngörmektedir. Amerika Birleşik Devletleri (ABD) tarafından, ABD vatandaşı veya ABD vergi mükellefi olan gerçek ve tüzel kişilerin gelir ve varlıkları üzerinden vergilendirmeden kaçınmasının önlenmesi ile şeffaf ve izlenebilir bir vergi sistemi oluşturulması amacıyla 2010 yılında kabul edilen FATCA, 2014 yılında yürürlüğe girmiştir. FATCA çerçevesinde, Türkiye Cumhuriyeti Hükümeti ile Amerika Birleşik Devletleri Hükümeti arasında karşılıklılık esası temel alınarak "Türkiye Cumhuriyeti Hükümeti ile Amerika Birleşik Devletleri Hükümeti arasında Genişletilmiş Bilgi Değişimi Yoluyla Vergi Uyumunun Artırılması Anlaşması" 29 Temmuz 2015 tarihinde imzalanmıştır. Bu anlaşmayı onaylayan Kanun, 16 Mart 2016 tarihli Resmî Gazete'de yayımlanmıştır. Ardından, Bakanlar Kurulu 19 Eylül 2016 tarihinde hem anlaşma metnini hem de anlaşmanın ekindeki mutabakat zaptını onaylamış, bu onay 5 Ekim 2016 tarihli Resmî Gazete'de duyurulmuştur.

CRS ise OECD tarafından ülkeler arasında finansal hesap bilgilerinin otomatik değişimi, vergi kayıp ve kaçaklarını önlemek amacıyla geliştirilen ve daha geniş bir uluslararası kapsama sahip olan bir düzenlemedir. Bu standardın hayata geçirilmesi içinse Finansal Hesap Bilgilerinin Otomatik Değişimine İlişkin Çok Taraflı Yetkili Makam Anlaşması (MCAA) imzalanmıştır. CRS, ülkelerin finansal kuruluşlarından hangi bilgilerin toplanacağını, bu bilgilerin nasıl raporlanacağını ve paylaşılacağını tanımlayan bir teknik standarttır. Buna göre, finansal kuruluşlar (örneğin bankalar, sigorta şirketleri, aracı kurumlar), hesap sahiplerinin vergi mukimlik bilgilerini ve hesap bakiyesi gibi finansal detayları belirleyerek ulusal mali otoritelere raporlar. Türkiye'de bu bilgiler, Gelir İdaresi Başkanlığı tarafından toplanmakta ve uluslararası bilgi değişimi kapsamında diğer ülkelerle paylaşılmaktadır.

CRS'in uygulanabilirliğini sağlamak amacıyla oluşturulan MCAA, ülkeler arasında karşılıklılık esasına dayalı hukuki bir bağlayıcılık getirmektedir. Türkiye, MCAA'yı 21.04.2017 tarihinde imzalamış ve 31.12.2019 tarihinde onaylamıştır. Bu mekanizma, Türkiye'nin de dahil olduğu ülkelerin finansal kuruluşlardan aldığı bilgileri her yıl otomatik olarak diğer katılımcı ülkelerin mali otoriteleriyle paylaşmasına olanak tanımaktadır. Dolayısıyla CRS, teknik bir çerçeve sunarken, MCAA bu çerçevenin işleyişini uluslararası alanda bağlayıcı hale getirmektedir. Bu süreç, özellikle yurt dışında saklanan varlıkların tespiti, vergi kayıplarının önlenmesi ve mali şeffaflığın sağlanması açısından önemli bir rol oynamaktadır. Söz konusu anlaşma gereği, ilgili hesap sahibinin kimlik ve vergi numarası ile ikamet bilgileri, hesaplarının yıl sonu bakiyeleri, hesaplarının faiz ve temettü gibi finansal gelirleri gibi kişisel veri niteliğindeki bilgiler Gelir İdaresi Başkanlığı tarafından ilgilinin mukim kabul edildiği ülkenin ilgili idaresiyle paylaşılmaktadır. Ayrıntılı bilgi için bkz.: Gelir İdaresi Başkanlığı, **Finansal Hesap Bilgilerinin Vergi Konularında Karşılıklı Olarak Otomatik Değişim Standardı Bilgilendirme Rehberi**, <https://www.gib.gov.tr/finansal-hesap-bilgilerinin-vergi-konularinda-karsilikli-olarak-otomatik-degisim-standardi> (E.T.: 29.12.2024).

2. BÖLÜM:

İDARENİN FAALİYETLERİNDE İŞLENEN KİŞİSEL VERİLER

Dijital çağın getirdiği teknolojik imkânlar, idarenin kamu hizmeti sunumu ve kolluk faaliyetlerinde köklü dönüşümlere neden olmuştur. Bu dönüşüm sürecinde, kişisel verilerin toplanması, işlenmesi ve aktarılması, idarenin faaliyetlerinin ayrılmaz bir parçası haline gelmiştir. Birinci bölümde incelenen hukuki çerçeve, bu bölümde ele alınacak olan idarenin somut faaliyetlerindeki kişisel veri işleme süreçlerinin değerlendirilmesinde temel dayanak noktasını oluşturmaktadır.

İdarenin kişisel veri işleme, kamu hizmetlerinin etkin ve verimli sunumu ile temel hak ve özgürlüklerin korunması arasında hassas bir denge kurulmasını gerektirmektedir. Söz konusu dengenin kurulmasında, idarenin farklı faaliyet alanlarının özgül nitelikleri ve bu alanlarda gerçekleştirilen veri işlemenin kendine has dinamikleri belirleyici rol oynamaktadır. Bu bağlamda, kamu hizmeti sunumu, kolluk faaliyetleri ve idarenin iç işleyişi gibi farklı faaliyet alanlarında işlenen kişisel verilerin tabi olduğu hukuki rejimin, bu alanların kendine özgü koşulları gözetilerek incelenmesi zorunluluk arz etmektedir.

Bilgi ve iletişim teknolojilerinin kamu hizmetlerinin sunumunda yaygın biçimde kullanılması, eğitim, sağlık ve ulaşım gibi temel alanlarda kişisel verilerin yoğun olarak işlenmesine yol açmaktadır. Benzer şekilde, kamu düzeninin korunmasına yönelik kolluk faaliyetlerinde gerek genel sağlığın korunması gerekse kamu güvenliğinin sağlanması amacıyla kişisel verilerin toplanması ve işlenmesi kaçınılmaz hale gelmektedir. Ayrıca, kamu görevlilerinin özlük dosyalarında ve disiplin süreçlerinde işlenen kişisel veriler de idarenin veri işleminin önemli bir boyutunu oluşturmaktadır.

Bu bölümde, idarenin farklı faaliyet alanlarında işlenen kişisel veriler, faaliyet bazlı bir yaklaşımla ele alınacaktır. Öncelikle, kamu hizmeti sunumu ve kolluk faaliyetlerinde işlenen kişisel verilerin tâbi olacağı hukuki rejimin farklılaşması gerekip gerekmediği normatif bir perspektifle incelenecektir. Ardından, İdarenin faaliyetleri çerçevesinde işlediği kişisel veriler, kamu hizmetlerinin sunumu, kolluk faaliyetleri ve kamu görevlilerinin kişisel verilerinin işlenmesi başlıkları altında detaylı biçimde analiz edilecektir. Son olarak, idarenin kişisel veri işleminin doğan hukuki sorumluluğu ve kişisel verilerin korunmasına ilişkin denetim mekanizmaları değerlendirilecektir.

Bu çok boyutlu inceleme, idarenin kişisel veri işleminin hukuki çerçevesini teorik düzeyde ortaya koyan birinci bölümle birlikte, söz konusu çerçevenin pratikte nasıl işlediğini ve uygulamada karşılaşılan sorunları analiz etmeyi amaçlamaktadır. Böylece, kişisel verilerin işlenmesi ve idare hukuku kesişiminde ortaya çıkan özgün sorunlara yönelik bütüncül bir bakış açısı geliştirilmesi ve bu sorunlara ilişkin çözüm önerilerinin sunulması hedeflenmektedir.

1. KAMU HİZMETİ VE KOLLUK FAALİYETLERİNDE ELDE EDİLEN KİŞİSEL VERİLERİN İŞLENMESİ BAKIMINDAN AYRI BİR HUKUKİ REJİMİN UYGULANMASI GEREKLİ VE/VEYA MÜMKÜN MÜ?

İdarenin kamu hizmeti ve kolluk faaliyetleri arasında, kişisel verilerin işlenmesi hukuku bakımından farklı bir hukuki rejim uygulanıp uygulanmayacağı meselesi, bu iki faaliyet türünün doğasında yer alan farklılıklar nedeniyle önem taşımaktadır. Kamu hizmetleri, İdare tarafından ya da onun gözetim ve denetimi altında özel kişilerce yürütülen toplumun ortak ve sürekli ihtiyaçlarını gidermeye yönelik etkinlikleri⁴³⁰ ifade ederken, kolluk faaliyetleri ise kamu düzeninin sağlanması ve korunması amacıyla İdare tarafından yürütülen ve çoğunlukla sınırlandırıcı faaliyetleri kapsar⁴³¹. Dolayısıyla, kamu hizmetinde, hizmetten yararlananlar bakımından bireylerin ihtiyaçlarını gidermeye yönelik, onların istifadesine sunulmuş çeşitli hizmetler söz konusu iken; kolluk faaliyetlerinin düzenin, güvenliğin ve genel sağlığın sağlanması ve korunması amacıyla bireylerin özgürlüklerinin kısıtlanması odaklı olduğu söylenebilir. Kamu hizmetlerinden yararlanma, çoğu zaman vatandaşın talebi üzerine gerçekleşir. İdare, bu hizmetleri sunmakla yükümlü olup, kimi durumlarda resen harekete geçebileceği gibi, çoğunlukla vatandaşın başvurusu ve ihtiyacı doğrultusunda hizmeti sunar. Örneğin, toplu taşıma hizmetleri, kültür sanat etkinlikleri, kütüphane hizmetleri, halk eğitim kursları, İdarelerce hizmete sunulan spor tesisleri gibi hizmetlerden yararlanma genellikle vatandaşın talebi üzerine gerçekleşir. Elbette eğitim hizmetleri bakımından ilk, orta ve lise düzeyindeki eğitimin zorunlu olması ya da günümüzde elektrik, su, kanalizasyon gibi temel altyapı hizmetlerinden yararlanmanın çoğu insan için pratikte vazgeçilemez hizmetlerden olması gibi yararlanılmasında taleple bağlılık esasının geçerli kabul edilemeyeceği kamu hizmetleri de bulunmaktadır. Kolluk faaliyetlerinde ise “zorunluluk” ve “bağlayıcılık” unsurları ve kural ihlalinde yaptırımlara maruz kalınması söz konusudur. Örneğin, trafik denetimleri, çevre koruma tedbirleri, halk sağlığının korunmasına yönelik alınan tedbirlerde belirlenen kurallar herkes için bağlayıcı ve uyulması zorunludur.

Öyleyse, kamu hizmeti ve kolluk faaliyeti arasındaki bu temel farklar, bu faaliyetlerin yerine getirilmesi sırasında elde edilen kişisel verilerin işlenmesi farklı hukuki sonuçlar doğurur mu? Öncelikle, kişisel verilerin korunmasını isteme hakkı Anayasa'nın 20/3 maddesinde düzenlenmiş kişisel bir haktır ve bu düzenlemeye göre kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla, ister kamu hizmetlerinin sunulması amacıyla isterse kolluk faaliyetlerinin yerine getirilmesi amacıyla olsun, kişisel verilerin işlenmesi bu hakkın sınırlandırılması anlamına gelmektedir.

⁴³⁰ Melikşah YASİN, “Kamu Hizmeti”, içinde **İdare Hukuku**, Turan YILDIRIM (ed.), s. 530; AYM, E.2019/27, K.2019/56, K.t. 26.6.2019, §6.

⁴³¹ Şerife YILDIZ, “İdari Faaliyetlerin Devri Bağlamında Özel Güvenlik”, **Marmara Üniversitesi SBE**, Doktora Tezi, 2010, s.104.

Ancak, ifade edilmelidir ki, işleme amacı ne olursa olsun kişisel veri işlemenin ilgisine etkisi kişisel bir hakkının sınırlandırılması olduğundan, bu sınırlamanın her halde özellikle Anayasa'nın 20/3. maddesinde belirlenen sınırlama şartları ile 13. maddesiyle belirlenen temel hak ve özgürlüklerin sınırlandırılması kurallarına ve veri işleme ilkelerine uygun olması aranacaktır⁴³². Her ne kadar KVKK'nın 28. maddesinin birinci fıkrasında sayılan kolluk faaliyetleri kanunun kapsamı dışında bırakılmış olsa da bu durum temel hak sınırlandırma rejiminin farklılaşması anlamına gelmemektedir. Nitekim aşağıdaki Anayasa Mahkemesi kararları incelendiğinde, kişisel verilerin korunması hakkına yönelik müdahalelerin, faaliyetin niteliğinden bağımsız olarak, aynı anayasal ilkeler çerçevesinde değerlendirildiği görülmektedir.

Anayasa Mahkemesi gerek kamu hizmeti kapsamında gerekse kolluk faaliyetlerinde olsun, hangi tür idari etkinlik gerçekleşirse gerçekleşsin, müdahaleyi kanunilik, meşru amaç ve ölçülülük ilkeleriyle değerlendirmektedir. Mahkemeye göre, Anayasa'nın 20/3. maddesinin lafzından hareketle, *“bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir”*⁴³³. Bu yaklaşım, faaliyet türü ne olursa olsun kişisel verilerin işlenmesi bakımından yeknesak bir anayasal denetimin bulunduğunu göstermektedir.

Örneğin, 5253 sayılı Dernekler Kanunu'nun 23. maddesinde dernek üyeliğine kabul edilenler ile üyelikleri sonra erenlerin adını, soyadını, doğum tarihini ve kimlik numarasını kabul edilme ve sona erme tarihinden itibaren kırk beş gün içinde dernekler birimine bildirme yükümlülüğü getiren düzenlemeyi inceleyen Mahkeme, dernek üyeliğine ilişkin bilginin özel nitelikli veri olduğuna yönelik tespiti yaptıktan sonra, kişisel verilerin korunmasını isteme hakkına getirilen bu sınırlamanın Anayasa'nın 13. maddesine uygun olup olmadığını değerlendirmiştir⁴³⁴. Düzenlemenin, sahte dernek üyeliklerinden doğan mağduriyetlerin engellenmesi ve dernek üye sayılarının doğru ve düzenli tespit edilerek hatalı hukuki işlemlerin önüne geçilmesini sağlamayı amaçladığı, dolayısıyla kuralın kamu düzeninin sağlanması ve suç işlenmesinin önlenmesiyle ilgililerin rızaları dışında bir işleme maruz kalmalarını engelleme gibi nedenlerle kabul edildiği, bu bağlamda meşru bir amacının bulunduğu kabul edilmiştir. Ölçülülük ilkesine ilişkin yaptığı incelemedeyse, yapılan yasal düzenlemenin belirlenen amaçlara ulaşmak bakımından elverişli ve gerekli olmadığının söylenemeyeceği, öte yandan, 5237 sayılı Türk Ceza Kanunu'nun kişisel verilere ilişkin hükümleri ve 6698 sayılı KVKK hükümlerinde sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer

⁴³² Temel hak ve özgürlüklere müdahale bakımından kolluk ve kamu hizmeti ayrımının net biçimde yapılmasının mümkün olmadığı ifade edilmektedir: SEVER, s.207

⁴³³ AYM, H.Ö., B. No: 2019/20473, 3.2.2022, §35.

⁴³⁴ AYM, E.2020/47, K.2023/36, 22.02.2023, §62-80.

verildiği, böylelikle elde edilmek istenen amaç ile sınırlanan özgürlük arasında makul dengenin gözetildiği sonucuna varılmıştır.

6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun ile getirilen müsabakalara girişte elektronik kart uygulaması, kart sahibinin bazı kişisel verilerinin merkezi sisteme kaydedilmesini gerektiren hükümleri bakımından AYM'nin incelemesine konu olmuştur. AYM, Anayasa'nın 59. maddesinin gereği olarak vatandaşlarının beden ve ruh sağlığını geliştirecek tedbirleri ve sporun yayılmasını teşvik etmek maksadıyla sporda şiddetin önlenmesine yönelik tedbirleri almasının İdarenin yükümlülüğü olduğunu ifade etmiştir. Mahkeme, itiraz konusu kuralların, kamu güvenliğinin ve vergi denetiminin sağlanması amacıyla, bu amaçla sınırlı olarak belirli sayıda kişisel verinin işlenmesini, merkezi sistemde tutulmasını, bu sistem içindeki verilerin İçişleri Bakanlığı ve Maliye Bakanlığı'yla paylaşılmasını öngördüğünü, bu bağlamda demokratik toplum düzeni yönünden zorlayıcı toplumsal ihtiyaçları karşılamaya yönelik olduğunu belirlemiştir. Ayrıca, sınırlama aracının hak ve özgürlüğü en az sınırlayacak şekilde belirlendiğini, kamu düzeninin korunması ile kişisel verilerin korunması hakkı arasında makul bir denge kurulduğunu, bu sebeple itiraz konusu kuralın ölçülülük ilkesine de aykırı olmadığına karar vermiştir⁴³⁵.

926 sayılı Türk Silahlı Kuvvetleri Personel Kanunu'na eklenen ek 39. maddesiyle, Milli Savunma Bakanlığı'nın müfettiş kadrolarına askeri kaynaktan yapılacak atamalar için müfettişliğe giriş sınavı yapılacağı ve bu giriş sınavıyla ilgili olarak yönetmelikte belirlenen hususlar dışında herhangi bir kayıt sisteminin kullanılmayacağı kuralı getirilmiştir. Söz konusu kuralla, giriş sınavında herhangi bir kayıt sisteminin kullanılıp kullanılmayacağı, kullanılacaksa bunun ne tür bir sistem olacağı ve ne tür kişisel verilerin işleneceği hususlarının idarenin takdir yetkisine bırakılmak suretiyle kişisel verilerin korunmasını isteme hakkına getirilen bu sınırlamanın hukuka aykırı olduğuna yönelik itirazı inceleyen Mahkeme, *"Kişisel verilerin korunmasını isteme hakkına getirilen sınırlama Anayasa'nın 13. maddesinde belirtilen ölçütlere uygun olmadığı takdirde Anayasa'nın 20. maddesinin üçüncü fıkrasını ihlal edecektir. Bu sebeple sınırlamanın kanun tarafından öngörülme, meşru amaç taşıma, demokratik toplum düzeninin gereklerine uygun olma ve ölçülülük ilkesine aykırı olmama koşullarına uygun olup olmadığının belirlenmesi gerekir."* diyerek yine aynı ilkelere dayalı olarak itirazı incelemiştir⁴³⁶.

Yine, sağlık hizmetlerinden faydalanmak isteyen genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin biyometrik yöntemlerle kimlik doğrulaması yapmasını ve/veya nüfus cüzdanı, sürücü belgesi ve evlenme cüzdanı gibi resimli belgelerden birinin gösterilmesini zorunlu kılan kanun hükmüne ilişkin yapılan itirazı değerlendiren AYM, Anayasanın 2. maddesinde belirlenen hukuk devleti ve belirlilik ilkelerini vurguladıktan sonra Anayasanın 20/3. maddesini hatırlatarak kişisel verilere yapılacak sınırlandırmanın ancak kanun ile yapılabileceğini, yapılacak sınırlamanın Anayasanın 13.

⁴³⁵ AYM, E.2014/196, K.2015/103, 12.11.2015, §28-35.

⁴³⁶ AYM, E.2021/84, K.2022/117, 13/10/2022, §62.

maddesine uygun olması gerektiğini belirtmiştir. Biyometrik yöntemler kullanılarak yapılan kimlik doğrulama sayesinde, izinsiz kullanımların engellendiğini, kamu kuruluşlarına karşı yolsuzlukların azaltıldığını ve sosyal güvenliği olan kişilerin de güvenli hizmet almasını sağladığını ifade eden Mahkeme, toplanan verilerin sadece sağlık alanında sunulan hizmetten faydalanabilmek için elde edildiğini, bu amaçla sınırlı olarak ve hizmetin devamı için zorunlu olduğu müddetle sınırlı olarak saklanabileceğini, aksi halde Türk Ceza Kanunu’nun kişisel verilere ilişkin ceza hükümlerinin uygulanacağını hatırlatmıştır. Bu sebeple itiraz konusu hükmün belirlilik ilkesine uygun ve ölçülü olduğuna karar vermiştir⁴³⁷.

Bütün bu değerlendirmelerin ışığında, “İdarenin yürüttüğü faaliyetin kamu hizmeti veya kolluk faaliyeti olmasına göre farklı bir kişisel veri koruma hukuku rejimi uygulanmalı mıdır?” sorusuna verilecek yanıt, ağırlıklı olarak tek bir anayasal çerçevenin geçerli olduğu yönündedir. Ancak faaliyet türü, ölçülülük analizinde etkili bir parametre olarak işlev görebilir. Kolluk faaliyetlerinde millî güvenlik, kamu düzeni veya suçun önlenmesi gibi daha yoğun gerekçeler idareye geniş bir takdir alanı sağlamaktadır. Nitekim gerek ulusal gerekse uluslararası düzenlemelerde millî güvenlik, kamu güvenliği, kamu düzeni gibi amaçlarla kişisel verilerin işlenmesine yönelik getirilecek sınırlamalarda İdarenin daha geniş yetkilere sahip olduğu kabul edilmektedir⁴³⁸.

Ancak bu durum, idarenin kolluk yetkisi kapsamında sınırsız ve keyfî bir şekilde kişisel veri işleyebileceği anlamına gelmemektedir. Anayasa Mahkemesi içtihatlarında da vurgulandığı üzere, millî güvenlik veya kamu düzeni gibi gerekçelerle getirilen sınırlamaların dahi kanunilik ve ölçülülük ilkelerine uygun olması gerekmektedir. Örneğin, MİT’in 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamı dışına çıkarılmasına ilişkin düzenlemeyi iptal eden kararda, bilgi edinme hakkı ve kişisel verilerin korunması hakkı aleyhine “tamamen kategorik bir yasak” getirildiği için ölçülülük ilkesinin ihlal edildiğine hükmedilmiş, millî güvenlik amacı gibi çok önemli bir alanda dahi kişilerin temel haklarının orantısız biçimde daraltılamayacağı sonucuna varılmıştır⁴³⁹. Dolayısıyla idare, kolluk faaliyetleri bağlamında sahip olduğu takdir yetkisini, hukuk devleti ilkesi ve temel hak ve özgürlüklerin korunması perspektifiyle kullanmak durumundadır.

Bununla birlikte, KVKK’nin 28/1-ç maddesinde yer verilen hükümle kolluk kapsamında işlenecek birçok kişisel verinin kanunun kapsamı dışına çıkarıldığı görülmektedir. İlgili hüküm uyarınca, kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik işlenecek kişisel veriler kanunun kapsamı dışında bırakılmıştır. Söz konusu kuralla, kanun koyucunun ilgili veri işleme faaliyetleri bakımından İdareye

⁴³⁷ AYM, E.2014/180, K.2015/30, 19.3.2015.

⁴³⁸ Ayrıntılı bilgi için bkz. “3.1. Tamamen Kanun Kapsamı Dışında Bırakılan Haller” başlığı.

⁴³⁹ AYM, E.2018/137, K.2022/86, K.t. 30.6.2022, §187-188.

belli bir hareket alanı tanıdığı açıktır. Örneğin, açık rıza, VERBİS’e kayıt, aydınlatma yükümlülüğü gibi birçok yükümlülük bu veri işleme faaliyetleri bakımından uygulanmayacaktır. Ancak bu hüküm kapsamında tanınan takdir yetkisinin kullanımı da hukuki denetime tabidir ve keyfi biçimde kullanılamaz.

İdare, kolluk faaliyetleri kapsamında kişisel veri işlerken de anayasal ilkelere, idare hukukunun genel prensiplerine ve bilhassa ölçülülük ilkesine riayet etmek zorundadır. Nitekim, İdarenin bilhassa kolluk yetkilerini kullanımına ilişkin hukuka uygunluk denetiminde ölçülülük ilkesi önemli bir yer tutar⁴⁴⁰. Kolluk yetkilerinin kullanımı sırasında çoğu zaman kamu düzeni, milli güvenlik, kamu güvenliği gibi soyut kavramlara başvurulmak suretiyle idari işlem tesis edildiğinden, bu işlemlerin denetiminde başvuru ölçülülük ilkesiyle, kolluğun sınırlandırmada kullandığı araç ve usullerin gerekliliği, amaca ulaşmadaki elverişliliği ve sınırlanan hakla ulaşılan amaç arasındaki dengenin varlığı İdari yargı tarafından sıkı şekilde denetlenmektedir⁴⁴¹. Bu sebeple, KVKK’nin 28/1-ç hükmü, kanun kapsamında birtakım yükümlülüklerden muafiyet bağlamında İdareye sağlanan serbestlik olarak kabul edilmeli, kolluk faaliyetleri kapsamında kişisel veri işleme noktasında İdareye geniş bir takdir yetkisi alanı oluşturduğu düşünülmemelidir.

Öte yandan, kamu hizmetlerinde vatandaşın talebi üzerine sunulan ve alternatif yöntemlerin mevcut olduğu hizmetler de ölçülülük testi çerçevesinde dikkate alınacak bir husus olarak karşımıza çıkabilir. Örneğin, bazı büyükşehir belediyeleri tarafından yapılan aplikasyonlarla, vatandaşlara akıllı bilet (AKBİL) olarak da bilinen elektronik kartlarıyla alışveriş yapmaları ya da faturalarını ödemeleri karşılığında çeşitli indirim imkanları tanınmaktadır. Yine bazı kişisel verilerini sisteme tanımlamak şartıyla bu aplikasyona üye olan kişilerin belli noktalarda ücretsiz internet hizmetinden faydalanması sağlanmaktadır. İşte bu örneklerde olduğu gibi hizmetin geleneksel yöntemlerle sunulması mümkün iken, vatandaşın tercihi doğrultusunda teknolojik imkanlarla sunulan alternatif hizmet yöntemlerinde kişisel veriler işlenebilir. Ancak bu durum, İdarenin kişisel verilerin işlenmesi konusundaki temel yükümlülüklerini ortadan kaldırmaz. İdare hem anayasal konumu hem de kamu gücünü kullanıyor olması nedeniyle, sunduğu tüm hizmet kanallarında kişisel verilerin işlenmesi için gerekli tedbirleri almakla yükümlüdür.

Sonuç olarak gerek yasal düzenlemelerde gerekse de Anayasa Mahkemesi kararları incelendiğinde kişisel verilerin işlenmesi bakımından faaliyet türüne göre “tamamen farklı” veya “birbirinden kopuk” iki hukuki rejim benimsenmesi yönünde bir düzenlemenin ve içtihadın bulunmadığı, hem kolluk hem de kamu hizmeti söz konusu olduğunda aynı anayasal ilkelerin -kanunilik, meşru amaç, ölçülülük ve temel hakların özüne dokunmama- geçerli olduğu görülmektedir. Dolayısıyla

⁴⁴⁰ Felemez GÜNEŞ, *İdari Yargı Yetkisinin Sınırları*, Seçkin Yayıncılık, 2022, s.141.

⁴⁴¹ DURAN, s. 260 vd.; ÖZAY, *Günışığında Yönetim*, s. 742 vd.; OĞURLU, s.102; Özge OKAY TEKİNSOY, “Kolluk Faaliyetleri”, içinde *İdare Hukuku*, Turan YILDIRIM (ed.), s. 646.

idareye tanınan takdir yetkisi, faaliyetin niteliğine göre çeşitlenebilir; fakat rejim birliği korunmakta ve her hâlükârda kanunî dayanak, öngörülebilirlik, keyfiliğe karşı güvenceler gibi unsurlar aranmaktadır. Bu sebeple, ayrı bir kişisel veri koruma rejimi öngörülmesinden ziyade tek bir anayasal çerçevenin her somut olayda farklı gerekçeler ve amaçlar üzerinden ölçülülük testine tabi tutulduğu sonucu ortaya çıkmaktadır.

Bununla birlikte, idare hukuku doktrinde yerleşik bir ayrıma işaret eden “kamu hizmeti” ve “kolluk faaliyeti” tasnifinin, her ne kadar kişisel verilerin işlenmesine getirilen sınırlamaların incelenmesi bakımından anayasal çerçevede yeknesak ilkeler uygulanmakta ise de, somut örneklerin daha anlaşılır biçimde incelenmesini sağladığı görülmektedir. Dolayısıyla, aşağıdaki bölümlerde öncelikle “kamu hizmeti” ve “kolluk” kategorileri altında yer alan uygulamalara ilişkin örnekler, 6698 sayılı Kanun ile getirilen veri işleme kuralları, kanunilik ve ölçülülük ilkesi gibi anayasal ilkeler bağlamında ele alınacak; böylece farklı faaliyet türlerinde kişisel veri işleme süreçlerinin benzerlikleri ve farklılıkları, idare hukuku anlayışına uygun bir tasnifle ortaya konulmaya çalışılacaktır. Bu yaklaşım, sonuç bölümünde belirtilen “ortak anayasal ilkelerin farklı gerekçelerle yorumlanması” tespitini değiştirmeyip, aksine bu çerçevenin somut olaylara nasıl yansıdığını örneklerle açıklamayı amaçlamaktadır.

2. İDARENİN FAALİYETLERİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN İŞLENMESİ

2.1. Kamu Hizmetlerinin Sunumunda Kişisel Verilerin İşlenmesi

Kamu hizmetlerinin sunumunda kişisel verilerin işlenmesi, modern idare anlayışının merkezi unsurlarından biri haline gelmiştir. Dijitalleşen kamu hizmetleri, bir yandan hizmet kalitesini artırıp bürokrasiyi azaltırken, diğer yandan büyük miktarda kişisel verinin toplanmasını ve işlenmesini beraberinde getirmektedir. Bu başlık altında, idarenin çeşitli kamu hizmeti alanlarında kişisel veri işleme incelenenektir. İncelememizde eğitim, sağlık ve ulaşım hizmetleri özelinde kişisel verilerin işlenmesi süreçlerine odaklanılmaktadır. Bu hizmet alanları hem yaygın kullanımları hem de hassas kişisel verilerin yoğun olarak işlendiği alanlar olmaları sebebiyle özel bir öneme sahiptir. Burada ele alınan hizmet örnekleri, idarenin kişisel veri işleme sürecinin tamamını kapsamayıp çalışmamızın sınırları içinde en belirgin örnekler olarak seçilmiştir.

2.1.1. Eğitim Hizmetlerinde Dijitalleşme ve Kişisel Veri Güvenliği

2.1.1.1. Genel Olarak

Türkiye’de, 69. ayını dolduran tüm çocuklar için başlayan ve 12 yıl boyunca süren zorunlu eğitim sürecinin, bir öğrencinin kişiliğinin baştan sona oluşumuna tanıklık ettiği söylenebilir.

Geleneksel eğitim modelinde öğrencilerin bir sınıfa girerek öğretmenlerini dinlemesi usulü günümüzde de devam etmekle birlikte, teknolojik gelişmeler eğitim ortamını önemli ölçüde değiştirmiştir. Örneğin, artık öğrencilerin hangi saatlerde okula giriş çıkış yaptığı dijital kartlarla kaydedilmekte⁴⁴², yemekhane alışverişleri elektronik sistemlerle takip edilmekte, sınıf içi kameralar ile davranışları izlenebilmekte, tablet veya bilgisayarlarda yaptıkları tüm işlemler log kayıtlarında tutulabilmekte ve hatta bazı okullarda yapay zekâ destekli yüz tanıma sistemleriyle öğrencilerin duygu durumları bile analiz edilebilmektedir⁴⁴³. Oysa geçmişte öğrenciler hakkında tutulan kayıtlar çoğunlukla ders notları, varsa disiplin kayıtları, aile bireylerine ilişkin temel bilgiler (kardeş sayısı, anne-baba meslek bilgisi, medeni durumları, sağ olup olmadıkları), hanenin aylık ortalama gelir bilgisi gibi sınırlı verilerden ibaretti. Görüldüğü üzere geçmişte öğrencilerden istenen bu temel bilgiler günümüzde özel bir kanun ile korunan kişisel verilerden ibaret olmakla birlikte, teknolojinin ilerlemesiyle birlikte eğitimde kullanılan çeşitli araçlar, işlenebilecek verilerin hem çeşitliliğini hem de miktarını önemli derecede artırmıştır.

Günümüzde eğitimde kalite ve verimliliğin artırılması amacıyla internet, tablet, bilgisayar gibi teknolojik araçlar eğitim hayatına dahil edilmiş ve dijital dönüşüme hız kazandırılmıştır. Bunların eğitim hayatına olan katkıları yadsınamaz bir gerçekse de bu araçlarla işlenen kişisel verilerin hukuka uygun olup olmadığı incelenmelidir. Türkiye’de uygulamaya konulan Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (FATİH) projesi ve Eğitim Bilişim Ağı (EBA) sistemi bunlara örnek olarak verilebilir.

Başka bir örnek ise uzaktan eğitim modeliyle işlenen kişisel verilerdir. Özellikle COVID-19 salgını ile kullanımı önemli derecede artan bu eğitim modelinde öğrencilerin görüntü ve seslerinin kayda alınması, saklanması, paylaşılması, bu verilere erişim süreleri, derslerde kamera ve mikrofon açma zorunluluğu gibi konular kullanıcıların görüntü, ses ve biyometrik verilerinin akıbeti hakkında tartışmalara neden olmuştur.

Yukarıda da ifade edildiği üzere, kişiler, bireysel özelliklerini kazandığı çocukluk ve gençlik evresinde İdare tarafından sunulan eğitim hizmetlerinden öğrenci olarak faydalanmaktadır. Bu süreçte işlenebilecek kişisel verilerin çeşitliliği göz önüne alındığında, İdare öğrencideki her türlü değişim ve gelişime yakından tanıklık edebilir, bunları kayıt altında tutabilir ve bu veriler ışığında eğitim hizmetlerini yenileyerek verimliliği ve kaliteyi artırabilir. Ancak bunun yanında, verilerin çeşitli analizler sonucu farklı amaçlarla kullanılması, ilgisiz üçüncü kişilerle paylaşılması ya da bu verilerin kişileri öğrencilik hayatı dışında da şöyle veya böyle etki etmesi tehlikesi de bulunmaktadır. Örneğin Amerika Birleşik Devletleri’nde bulunan çeşitli web sitelerinde veri komisyoncularının (data brokers)

⁴⁴² İstanbul’da bulunan bir lisede, öğrencilerin giriş çıkış saatlerinin velilerine bildirilmesi uygulaması örneği için bkz.: https://lkml.meb.k12.tr/icerikler/okul-giris-cikis-kart-sistemi-veli-bilgilendirme-uygulamasi_13754335.html?utm_source (E.T. 19.1.2025).

⁴⁴³ Buket İŞLER, Mehmet Yaşar KILIÇ, “Eğitimde Yapay Zekâ Kullanımı ve Gelişimi”, **e-Journal of New Media**, Y. 2021, C.5, S.1, s.7.

“aile içi şiddete maruz kalmış öğrenciler”, “lise öğrencileri” ve aile içi sorunlar yaşayan kız çocuklarının profilini çıkarmak ve hedeflemek için “aile planlaması hizmetleri için on dört ve on beş yaşındaki kızlar” şeklindeki listelerle öğrencilere ait e-postaları pazarladıkları tespit edilmiştir⁴⁴⁴. Bu sebeplerle, eğitim hizmetlerinde hukuka uygun şekilde kişisel veri işleme faaliyetlerinin yürütülmesi ve yine bunlara ilişkin güvenlik önlemlerinin alınması büyük önem taşımaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 5. ve 6. maddelerinde genel ve özel nitelikli verilerin işleme şartları sayılmıştır. Dolayısıyla, eğitim hizmetlerinin sunulması sırasında hukuka uygun şekilde veri işlenebilmesi için kişisel verinin türüne göre bu maddelerde belirlenen işleme şartlarından birinin varlığı aranacaktır. Öte yandan, veri işlemenin hukuka uygun kabul edilebilmesi için her halde Kanunun 4. maddesinde belirlenen genel ilkelere uygun hareket edilmesi gerekir.

İdare, eğitim hizmetlerini yasa koyucunun kendisine yüklediği bir görev neticesinde ve onun çizdiği yasal sınırlar çerçevesinde kamu yararı amacına uygun olarak yerine getirmektedir. Dolayısıyla genel nitelikli kişisel veriler bakımından, bu hizmetin yerine getirilmesi sırasında veri sorumlusu sıfatıyla İdare, kanun hükümlerinin uygulanması, kendisine verilen hukuki bir yükümlülüğün yerine getirilmesi ya da bir hakkın tesisi, kullanılması veya korunması amaçlarına dayanarak kişisel veri işleyebilmektedir. Bunun dışında İdare, eğitim hizmetlerinin sunulması, kalite ve verimliliğinin artırılması amacıyla açık rızaya dayalı olarak da veri işleyebilmektedir. Ayrıca, 6698 sayılı Kanunun 6/3. maddesinde kabul edilen veri işleme şartları uyarınca İdarenin kanunda açıkça öngörülmesi, bir hakkın tesisi, kullanılması veya korunması için zorunlu olması, ilgilinin açık rızası ve alenileştirilmiş kişisel verinin alenileştirme iradesine uygun olacak şekilde özel nitelikli verileri işleyebileceği kabul edilmelidir.

Örneğin, 5 Ocak 1961 tarihinde kabul edilen 222 sayılı İlköğretim ve Eğitim Kanunu’nun⁴⁴⁵ halen yürürlükte bulunan bazı hükümlerinde İdareye kişisel veri işleme faaliyetini gerektiren çeşitli görevler verildiği görülmektedir. Kanunun 48. maddesinde, her yıl derslerin başlamasından 15 gün önce, muhtarlar okul müdürleriyle iş birliği yaparak görevli oldukları sınırlar içerisinde öğrenim çağında bulunan çocukların bilgilerini içeren çizelgeyi hazırlayarak okul idarecilerine ve ilçe eğitim müdürlüğüne vermekle görevlendirilmiştir. Kanunun 49. Maddesinde ise nüfus cüzdanı bulunmayan ya da henüz nüfus kaydı yaptırılmamış çocukların yaşlarının ihtiyar heyetlerince tespit edilerek mecburi öğrenim çağında olanlar çizelgesine yazılmaları öngörülmüştür. Yine Kanunun 53. Maddesi uyarınca okul idareleri ve ilköğretim müfettişlerine, okula devam etmeyen öğrencilerin devamsızlık sebeplerinin araştırılması ve bu sebeplerin giderilmesine çalışılması görevi verilmiştir. Sebeplerin giderilememesi halinde durumun köylerde muhtarlara, diğer yerlerde mülki amirlere bildirilmesi istenmiştir. Dolayısıyla

⁴⁴⁴ Alistair SIMMONS, “The Vulnerability and Protection of Student Data”, **LAWFAREMEDIA**, 4.12.2023. <https://www.lawfaremedia.org/article/the-vulnerability-and-protection-of-student-data> (E.T. 11.3.2024).

⁴⁴⁵ RG, 12.1.1961/10705.

İdare, zorunlu temel eğitimin sağlanması ve eğitim hakkının gerçek anlamda hayata geçirilebilmesi amacıyla kanunda açıkça belirlenen kişisel verileri işleyebilecektir. Ancak, İdarenin veri işlemenin genel ilkelerine uygun hareket etmesi, özellikle “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesi uyarınca örneğin, çocukların isim, soyisim ve nüfus bilgileri dışında, gerçekten ihtiyaç duyulmayan ilave verilerin toplanmaması veya süreç sonunda verilerin gereğinden uzun süre tutulmaması hususlarına dikkat edilmesi gerekir.

İdarenin eğitim hizmetlerinin sunumunda kendisine verilen hukuki yükümlülüklerini yerine getirmek için zorunlu olması şartına dayalı olarak kişisel veri işlemesine Millî Eğitim Bakanlığı Okul Öncesi Eğitim ve İlköğretim Kurumları Yönetmeliği’nde yer verilen düzenlemeler örnek gösterilebilir. İlgili Yönetmeliğin 18. maddesinde “*bir derse girdiği halde bir veya daha fazla derse özürsüz olarak girmeyen öğrencinin durumu*”nın okul yönetimince derhal velisine bildirileceği düzenlenmiştir. Aynı Yönetmeliğin 23. maddesinde ise yapılan sınavlara katılamayan ya da projesini zamanında teslim edemeyen öğrencinin durumunun velisine bildirileceği belirtilmiştir. Yine şube öğretmenler kurulunca öğrencinin sınıf geçmesi ya da sınıf tekrarına ilişkin alacağı kararın da velisine bildirileceği Yönetmeliğin 31/b maddesinde ifade edilmektedir. Yine Millî Eğitim Bakanlığı Ortaöğretim Kurumları Yönetmeliği’nde de öğrencilerin çeşitli kişisel verilerinin velilere bildirileceği düzenlenmiştir. Örneğin, devamsızlık yapan öğrencinin durumunun (m. 36/4) ve öğrenciye verilen bütün disiplin cezalarının (m. 169/5) velilere bildirilmesi öngörülmüştür. Ayrıca, öğrencinin davranış ve başarı durumları konusunda velilerle iş birliği yapılması öğretmenlerin görev ve sorumlulukları arasında sayılmıştır (m. 86/4(n)).

Yukarıdaki örneklerde görüldüğü üzere, ayırt etme gücüne sahip olup olmadığına bakılmaksızın çocukların eğitim ve öğretim sürecindeki kişisel verilerinin velileriyle paylaşılması veri sorumlusu olarak okul yönetiminin yükümlülüğündedir. Bu hukuki yükümlülüğün yerine getirilmesi bakımından çocuğun kişisel verilerinin velisi ile paylaşılması bir zorunluluk teşkil ettiğinden, mevzuat uyarınca ayırt etme gücüne sahip olan öğrencinin de açık rızasına başvurulmadan veri paylaşımı yapılması mümkündür. Bununla birlikte, Yönetmelikle yapılan bu düzenlemelerin özellikle ayırt etme gücüne sahip olan öğrenciler ile 18 yaşını doldurmuş ve kanunen tam ehliyetli ergin öğrenciler için hukuka uygunluğu eleştiriyeye açıktır.

Ayırt etme gücüne sahip ancak ergin olmayan öğrencilerin kişisel verilerinin bir hukuki yükümlülük gereği açık rızalarına başvurulmadan velileriyle paylaşılması, ölçülülük ilkesi kapsamında değerlendirildiğinde, çocuğun üstün yararının korunması ve velilerin eğitim sürecine katılımının sağlanması bakımından uygun bir düzenleme olarak kabul edilmelidir.

Velilere, çocuğun eğitim durumu, devamsızlığı veya disiplin sorunlarına ilişkin bilgi verilmesi, eğitimin etkin bir şekilde sürdürülmesi amacına hizmet etmektedir. Velilerin bu bilgileri edinmesi, çocuklarının eğitimine aktif bir şekilde katılım sağlamalarını kolaylaştırmakta ve çocuğun gelişimine

yönelik alınacak önlemlerin zamanında uygulanmasını mümkün kılmaktadır. Dolayısıyla, bu tür bir bilgilendirme, amaca ulaşma noktasında elverişli bir araçtır.

Bu bilgilendirme, aynı zamanda çocuğun üstün yararını korumak için başvurulabilecek en az müdahaleci yöntemler arasında yer almaktadır. Ayırt etme gücüne sahip çocuklarla doğrudan iletişim kurularak bilgi edinilmesi veya çocukların kendi kararları ile süreci yönetmelerinin beklenmesi gibi alternatifler, hem velilerin sorumluluklarını yerine getirmelerini zorlaştıracak hem de çocuğun gelişim sürecinde aksamalara neden olabilecektir. Bu bağlamda, çocuğun eğitim süreciyle ilgili bilgilerin velilere aktarılması, amaç doğrultusunda gerekli bir müdahale olarak kabul edilmelidir.

Velilere yapılan bilgilendirme, çocuğun mahremiyet hakkına yapılan müdahale ile elde edilmek istenen amacın dengeli bir şekilde korunmasını sağlamaktadır. Türk Medeni Kanunu'nun ebeveynlere çocuğun eğitimi ve gelişimi üzerindeki sorumluluklarına ilişkin hükümleri dikkate alındığında, velilere bilgi verilmesi, çocuğun üstün yararını korumaya yönelik bir tedbir olarak orantılıdır⁴⁴⁶. Bilgilendirme, ebeveynlerin çocuklarına ilişkin yasal sorumluluklarını yerine getirmelerine olanak tanımakta ve çocukların eğitimden tam anlamıyla faydalanmalarını sağlamaktadır. Bu nedenle, bu tür bir düzenleme hem çocuğun üstün yararını hem de velilerin sorumluluklarını dengelemesi bakımından ölçülülük ilkesine uygunluk göstermektedir.

Ancak, ortaöğretim seviyesindeki öğrencilerden 18 yaşını dolduran ve ergin kabul edilen bireyler için durum farklıdır. Türk Medeni Kanunu'na göre ergin bireyler, ana-baba velayeti sona ermiş ve tam ehliyetli bireyler olarak kişisel haklarını bağımsız bir şekilde kullanabilme hakkına sahiptir. Bu durum, kişisel verilerin korunmasına ilişkin hakları da kapsamaktadır. Dolayısıyla, devamsızlık yapan öğrencinin durumunun (m. 36/4) ve öğrenciye verilen bütün disiplin cezalarının (m. 169/5) velilere bildirilmesini öngören Millî Eğitim Bakanlığı Ortaöğretim Kurumları Yönetmeliği hükümlerinin ergin öğrenciler için geçerli olmadığı kabul edilmelidir. Bu sebeple, ergin öğrencilerin KVKK'nın 5. maddesi uyarınca açık rızaları alınmadan ana-babalarına bilgi aktarılması hukuka aykırı olacaktır⁴⁴⁷. Öte yandan, böyle bir düzenlemenin öngörülebilmesi kişisel verilerin korunmasını isteme hakkına bir sınırlama teşkil

⁴⁴⁶ Çocuklara yönelik belirlenen söz konusu yönetmelik hükümlerinin Türk Medeni Kanunu'yla ebeveynlere tanınan çocuğu tedip hakkına da uygun düştüğü ifade edilmelidir. Tedip kelimesi, Türk Dil Kurumu sözlüğünde “uslandırma, yola getirme, terbiye etme” anlamlarına gelmektedir. İlgili Kanun'un 339. maddesinde “Ana ve baba, çocuğun bakım ve eğitimi konusunda onun menfaatini göz önünde tutarak gerekli kararları alır ve uygularlar” hükmüne yer verilmiştir. Yine Kanunun 340. maddesine göre “Ana ve baba, çocuğu olanaklarına göre eğitirler ve onun bedensel, zihinsel, ruhsal, ahlâkî ve toplumsal gelişimini sağlar ve korurlar.” Dolayısıyla, anne ve babanın, çocuğun eğitim ve öğretim hayatındaki gelişmeleri, okulda yaşanan sorunlarına ilişkin bilgilendirilmesi, Türk Medeni Kanunu'nda kendilerine verilen bu hakkın kullanılmasını da kolaylaştıracaktır. Ana babanın terbiye (tedip) hakkına ilişkin ayrıntılı bilgi için bkz.: Zekeriya Alper İNANÇ, “TCK, TMK ve Uluslararası Sözleşmeler Kapsamında Terbiye Hakkı”, **Melikşah Üniversitesi Hukuk Fakültesi Dergisi**, C.2, S.2, Aralık 2013, s.101-132; Sevgi USTA, “Anne Babanın Tedip Hakkı”, **İ.Ü. Siyasal Bilgiler Fakültesi Dergisi**, No: 8 (Temmuz 1994), <https://dergipark.org.tr/tr/download/article-file/5505> (E.T. 8.8.2024)

⁴⁴⁷ Ancak bu noktada, ergin öğrencilerin okul idaresi karşısında eşit statüde olmadıkları dikkate alındığında, açık rızalarının özgür iradeyle beyan edilip edilmediği konusunda şüpheler doğabilir. Bu durum, özellikle taraflar arasındaki statü farkının rıza mekanizmasının etkinliğini ve güvenilirliğini zayıflatabileceği riskini doğurmaktadır. Bilgi için bkz.: “**4.4.1.2. Açık Rıza Şartının İstisnaları**” başlığı.

edeceği için kanuni bir dayanağın bulunması gerekir; ancak ilgili yönetmeliğe dayanak olarak gösterilen 222 sayılı İlköğretim ve Eğitim Kanunu ile 1739 sayılı Millî Eğitim Temel Kanunu'nda da ergin öğrencilere ilişkin ayrı bir hükme yer verilmediği görülmektedir.

Danıştay kararına konu olan bir olayda, YÖK tarafından tüm üniversitelere gönderilen bir yazıyla, üniversite ile aile iş birliğinin etkin hale getirilmesi amacıyla adli ve idari işlem yapılan öğrenciler ile yasa dışı faaliyette bulunan öğrencilerin durumlarının ailelerine bildirilmesi istenmiştir. Ancak söz konusu yazının iptalinin istenmesi üzerine Danıştay tarafından yapılan değerlendirmede, istisnalar haricinde üniversite öğrencilerinin 18 yaşının üzerinde ergin bireyler olduğu, ailelerle paylaşılması istenen bilgilerin öğrencilere ait kişisel veri olduğu, bu bilgilerin paylaşılmasına ilişkin kanuni bir dayanağın bulunmaması nedeniyle ilgili YÖK işleminin iptal edilmesine karar verilmiştir⁴⁴⁸.

6698 sayılı Kanun kapsamında eğitim hizmetlerinin sunumunda kişisel verilerin işleme şartlarına ilişkin olarak, dijital eğitim araçlarının veri işleme süreçleri ile sınav güvenliği kapsamında elde edilen kişisel verilerin veri koruma hukuku bağlamında değerlendirilmesi ayrıca ele alınması gereken hususlardır. Modern eğitim sistemlerinde söz konusu meselelerin veri koruma hukuku açısından incelenmesi, eğitim hizmetlerinin hukuka uygun şekilde yürütülmesi bakımından önem arz etmektedir.

2.1.1.2. Dijital Eğitim Araçları ve Veri Güvenliği

Dijital teknolojilerin eğitim alanında kullanımı, 21. yüzyılda küresel bir eğilim haline gelmiştir. UNESCO'nun 2021 tarihli 'Yapay Zekâ ve Eğitim: Politika Yapıcılar İçin Rehber' raporunda belirtildiği üzere, özel sektör, global eğitim kurumlarında kullanılmak üzere gittikçe artan bir oranda 'akıllı', 'uyarlanabilir' ve 'kişiselleştirilmiş' öğrenme sistemleri geliştirmekte ve bu gelişen sektörün 2024 yılında 6 milyar ABD doları değerinde bir pazar oluşturması öngörülmektedir⁴⁴⁹. Dijital eğitim araçları, öğrenme deneyimini zenginleştirme ve eğitim kaynaklarına erişimi kolaylaştırma gibi avantajlar sunarken, aynı zamanda veri güvenliği ve kişisel verilerin korunması gibi kritik konuları da beraberinde getirmektedir. Eğitim kurumları, öğrencilerin ve eğitimcilerin kişisel verilerini koruma yükümlülüğü ile yenilikçi eğitim teknolojilerini kullanma ihtiyacı arasında hassas bir denge kurmak zorundadır.

Bu bağlamda, çalışmamızın bu bölümünde, dijital eğitim araçları kullanılarak kişisel verilerin işlenmesi konusu incelenecektir. Ancak tüm dijital araçların tek tek incelenmesi kapsamı genişleteceğinden, örnek olarak, Türkiye'de uygulanan Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (FATİH) projesi ve Eğitim Bilişim Ağı (EBA) sistemi ele alınacaktır. Ardından, özellikle COVID-19 pandemisi sürecinde yaygınlaşan çevrimiçi eğitim uygulamalarında kişisel verilerin işlenmesi ve korunması konusuna odaklanılacaktır. Bu kapsamda, video konferans araçları, çevrimiçi

⁴⁴⁸ Danıştay İDDK, E. 2021/1733, K. 2022/286 (Lexpera).

⁴⁴⁹ UNESCO, AI and education: Guidance for policy-makers, s.5, 2021, <https://doi.org/10.54675/PCSP7350> (E.T. 25.3.2024).

öğrenme platformları ve dijital değerlendirme sistemleri gibi araçların kullanımında ortaya çıkan veri güvenliği riskleri ve bu risklerin yönetilmesine yönelik hukuki çözümleri tartışılacaktır.

2011 yılında tanıtılan Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (FATİH) projesi kapsamında Türkiye'deki 42.000 okulda 570.000 sınıf teknolojik ekipmanlarla donatılmış ve öğrencilere tablet bilgisayarlar dağıtılmıştır⁴⁵⁰. Projenin başarı esaslarından biri "ölçülebilirlik" olarak belirlenmiştir. Buna göre öğrenciler, teknoloji sayesinde elde edilen verilerle analiz edilerek ders dışı ilgi alanları, özel yetenekleri ve eğilimli oldukları alanlar keşfedilecek ve uygun yönlendirmeler yapılacaktır.

FATİH Projesi kapsamında İdarenin elde edebileceği veriler arasında öğrencinin kimlik numarası, aile bilgileri, tabletlerdeki kamera ve mikrofon yoluyla elde edilebilecek görüntü ve sesler, internet gezinme davranışları, konum verisi ve sosyal ağ paylaşımları sayılabilir⁴⁵¹. Bu verilerin analizi ile öğrencilerin yetenekleri, eksiklikleri ve verimli çalışma saatleri gibi bilgiler elde edilerek daha etkili eğitim desteği sağlanabilir. Ancak, bu analizler sonucunda öğrencinin ırkı, etnik kökeni, politik görüşü, dini inancı, sağlığı ve cinsel yönelimleri gibi özel nitelikli kişisel verilere de erişim sağlanabilir⁴⁵².

Eğitim ve öğretim hizmetinin sunulması İdare'ye Anayasa'nın 42. maddesiyle verilen bir görevdir. 1739 sayılı Milli Eğitim Temel Kanunu'nda, öğrencilerin ilgi ve kabiliyetlerine göre yetiştirilmeleri ve uygun programlara yönlendirilmeleri öngörülmüştür (m.6/1). "*Yöneltilmede ve başarının ölçülmesinde rehberlik hizmetlerinden ve objektif ölçme ve değerlendirme metotlarından yararlanılır.*" (m.6/3).

FATİH projesi, MEB bünyesindeki Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü tarafından yürütülmektedir. Bu Müdürlüğün görevleri arasında teknolojinin eğitimle buluşturulması ve ülke çapında eşit ve etkin şekilde kullanılmasının sağlanması yer almaktadır⁴⁵³.

Yukarıdaki düzenlemelerden hareketle, Millî Eğitim Bakanlığı'nın FATİH projesi kapsamında kişisel veri işleme faaliyetini Kanunlarda açıkça öngörülmesi ve hukuki yükümlülüklerini yerine getirebilmesi için zorunlu olması şartlarına dayalı olarak yürütebileceği söylenebilir. Ancak, 6698 sayılı Kanunun 6. maddesindeki 1 Haziran 2024 tarihinde yürürlüğe giren değişiklikler önemlidir⁴⁵⁴. Bu değişikliklerle özel nitelikli verilerin kanunlarda açıkça öngörülmesi halinde işlenebileceği kabul

⁴⁵⁰ Ali İNAN/Mehmet Ercan NERGİZ/Yücel SAYGIN, "Öğrenci Verilerinin Korunması: FATİH Projesi Işığında Teknik Değerlendirme", *Bilişim Teknolojileri Dergisi*, Cilt: 10, Sayı: 1, Ocak 2017, s. 68.

⁴⁵¹ İNAN/NERGİZ/SAYGIN, s.72-73.

⁴⁵² İNAN/NERGİZ/SAYGIN, s.73-74.

⁴⁵³ Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü'nün Teşkilat ve Görevlerine İlişkin Yönerge, m. 311.

⁴⁵⁴ Ancak, bu şartların geçerliliği işlenen veri türüne göre ayrı ayrı incelenmelidir. 6698 sayılı Kanunun 6. Maddesindeki değişiklikler 1 Haziran 2024 tarihinde yürürlüğe girmiştir. Bu tarihten önce sağlık ve cinsel hayata ilişkin olanlar dışındaki kişisel veriler kanunlarda öngörülmesi halinde işlenebilirken; sağlık ve cinsel hayata ilişkin kişisel verilerin yalnızca kanunda belirlenen amaçlarla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebileceği kabul edilmişti. Bu amaçlar arasında eğitim hizmetlerine yer verilmemesi nedeniyle yasa değişikliği öncesi dönemde İdarenin sağlık ve cinsel hayata ilişkin verileri işlemesi hukuka aykırı kabul edilecektir.

edildiğinden, İdare sağlık ve cinsel hayata ilişkin olanlar dahil özel nitelikli verileri bu şarta dayalı olarak işleyebilecektir⁴⁵⁵. Ayrıca, özel nitelikli veriler sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülükler kapsamında da işlenebilecektir.

Öte yandan, kişisel veri işleme faaliyetinin hukuka uygun olarak kabulü için 6698 sayılı Kanunun 5. ve 6. maddelerindeki veri işleme şartlarından birinin sağlanması gerekliyse de bu tek başına yeterli değildir. Nitekim, Kanunun 4. Maddesinde belirlenen genel ilkelere uyulmaması halinde hukuka aykırı bir veri işleme faaliyeti söz konusu olacaktır. Kişisel veri işlenirken uyulması gereken ilkelere biri, kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenmesidir. Bu nedenle, veri sorumlusu Millî Eğitim Bakanlığı, kanunlarla kendisine verilen görevlere uygun olarak, eğitim ve öğretim hizmetlerinin yerine getirilmesi, derslerin dijital sistemlerle desteklenmesi, öğrencilerin kabiliyet ve isteklerine uygun şekilde yönlendirilmesi amacıyla, bu amaçla sınırlı ve ölçülü olarak veri işleyebilir. Veri sorumlusu İdare, sadece kendisine verilen bu amaçlar kapsamında veri işlemelidir⁴⁵⁶.

FATİH projesi kapsamında öğrencilere dağıtılan tablet bilgisayarların kamera ve mikrofonları aracılığıyla görüntü ve ses verilerinin, konum bilgisinin, ya da internet geçmişi aracılığıyla diğer erişilebilecek genel ve özel nitelikli verilerinin işlenmesi ihtimalinde de ölçülülük ilkesi ihlal edilmiş olacaktır. Örneğin, öğrencinin ilgi duyduğu alanların veya öğrenim şekillerine olan yatkınlığının belirlenmesinde, sistem üzerinden sunulan çeşitli eğitim materyalleri (eğitim videoları ve eğitici oyunlar gibi) ya da ders videolarında geçirdiği süreler ve sınav sonuçları gibi unsurların analiz edilmesi gerekli ve yeterliyen; aynı amaçla öğrencinin internette dolaştığı diğer web sitelerinin analiz edilmesi, zorunlu olmayan çerezlerin tutulması gibi yöntemlerin kullanılması ölçülülük ilkesine aykırı olacaktır.

Öte yandan Bakanlık, öğrenciler için hazırladığı dijital eğitim materyallerini Eğitim Bilişim Ağı (EBA) sistemi üzerinden sunmaktadır. FATİH projesinin içerik sağlama kısmı EBA ile gerçekleştirilmekte olup, sisteme kişiye özel kullanıcı adı ve şifreyle giriş yapılmaktadır. EBA; ders videoları, dokümanlar ve eğitici uygulamalar barındırmakta, öğrencilere kişiselleştirilmiş içerikler sunabilmekte, öğretmenlerin ödev tanımlamasına ve öğrenci takibine imkân vermektedir. Ayrıca, öğrenciler arasında sosyal etkileşime olanak tanımakta ve COVID-19 pandemisi dönemindeki canlı dersler de bu sistem üzerinden yapılmıştır. Veliler de sisteme girerek çocuklarının eğitim durumlarını takip edebilmektedir.

⁴⁵⁵ Ayrıntılı bilgi için bkz.: “4.4.2. Özel Nitelikli (Hassas) Verilerin İşlenmesine İlişkin Şartlar” başlığı.

⁴⁵⁶ Bu bağlamda, görme ya da işitme problemi yaşayan öğrencilerin derslerde ön sıralarda oturtulması ve çeşitli kalıtsal hastalıklara sahip öğrencilerin buna uygun mesleklere yönlendirilmesi, engelli öğrenciler için gerekli düzeninin sağlanması gibi sebepler öğretmenlerin ve diğer okul yetkililerinin öğrencilerin sağlık verilerini işlemesine örnek olarak verilebilir. Ayrıca 1593 sayılı Umumi Hıfzıssıhha Kanunu’nda okul sağlığına ilişkin hükümlere de yer verilmiştir. Örneğin, Kanunun 164. maddesinde, okullarda belirli aralıklarla öğrencilerin ruh, beden, göz ve kulaklarına ait muayenelerinin görevlendirilecek doktorlar tarafından yapılması ve her öğrenci için ayrı kayıt tutulması öngörülmüştür. Ancak, öğrencinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi dini inancı, mezhebi veya diğer inançları, kılık ve kıyafeti gibi diğer özel nitelikli verilerin eğitim hizmetlerinin sunulması kapsamında işlenmesi mümkün görünmemektedir.

EBA'nın "Gizlilik Politikası"nda, kullanıcıların kimlik, iletişim, özlük, sosyal medya bilgileri ile görsel-işitsel kayıtlarının çeşitli teknolojiler vasıtasıyla işleneceği belirtilmektedir. Bu verilerin, *"aramızdaki hizmet ve sözleşme ilişkisi çerçevesinde ve meşru menfaat işleme şartına dayanılarak"* işleneceği ifade edilmiştir. Ancak, eğitim hizmetlerinin sunulması İdareye Anayasal ve yasal bir görev olarak verilmiştir. Öğrenci ile Bakanlık arasında imzalanmış bir hizmet sözleşmesi bulunmamaktadır. Öğrencilerin sisteme kayıtları sınıf öğretmenleri aracılığıyla yapılmakta, veliler sadece e-okulda kayıtlı oldukları öğrenci adına giriş yapabilmekte, öğretmenler ise MEBBİS'e kayıtlı olarak sisteme erişebilmektedir. Dolayısıyla EBA, eğitim kamu hizmetinin bir parçasıdır ve kullanımı için ayrı bir sözleşme imzalanmamaktadır.

Ayrıca, gizlilik metninde verilerin meşru menfaat şartına dayalı olarak işlendiği belirtilmektedir. Oysa İdare, kanunlarla kendisine verilen görevleri yerine getirirken kamu yararı amacıyla hareket etmek zorundadır⁴⁵⁷. EBA sistemi, eğitim kamu hizmetinin doğrudan bir parçasını oluşturan, yasaların Bakanlığa yüklediği görevler çerçevesinde sunulan bir hizmettir. Bu sebeple, EBA sistemiyle kişisel verilerin kanunlarda açıkça öngörülmesi ve veri sorumlusunun hukuki yükümlülüklerini yerine getirebilmesi şartları çerçevesinde işlenmesi gerekmektedir.

EBA için hazırlanan tek bir "Gizlilik Politikası" metninin tüm kullanıcılar için kullanılması da sorundur. Nitekim sistem, öğrenci, öğretmen ve veliler tarafından kullanılabilir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5/1-(ğ) maddesi gereği, ilgili kişiye yapılacak bildirimin açık ve anlaşılır bir dille yapılması öngörülmüştür. Bu nedenle, özellikle öğrenciler için teknik terimlerden arındırılmış, daha anlaşılır bir dille sahip ayrı bir aydınlatma metni hazırlanması gerekmektedir⁴⁵⁸.

Eğitimde hizmetlerinde dijitalleşmenin getirilerinden biri de çevrimiçi şekilde uzaktan sunulan ders etkinlikleri olmuştur. Uzun süredir kullanılan bu yöntemin kullanımı özellikle 2019 yılında başlayan Covid-19 pandemi süreciyle yüksek oranda artış göstermiştir. Bununla beraber, çevrimiçi eğitim ile işlenen kişisel verilerin akıbeti de tartışma konusu olmuştur. Nitekim, canlı derslere katılım gösteren öğrenci ve öğretmenlerin adı soyadı, kimlik bilgileri, eğitim bilgileri, öğrenci numarası, görüntü ve ses kaydı ile biyometrik verilerinin işlenmesi söz konusudur. Pandemi sürecinde birçok kamu hizmeti gibi eğitim hizmetlerinin de devamlılığının sağlanabilmesi için hızlı şekilde alınan bazı aksiyonlar kimi zaman ölçüsüz veri işlenmesi sonucunu doğurmuştur. Ancak yaşanan toplumsal panik havası ve acil çözüm arayışı da düşünüldüğünde, bu dönemde yapılan uygulamaların normal döneme kıyasla daha beklenebilir bir durum olduğu söylenebilir. Bununla birlikte, bu gibi durumlarda çevrimiçi

⁴⁵⁷ Ayrıntılı bilgi için bkz.: "4.4.1.2.7. Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlemesi: İdari Faaliyetlerde Meşru Menfaatin Yeri" başlığı.

⁴⁵⁸ Aydınlatmanın ilgili kişi ve sürece göre ayrı ayrı yapılması gerektiği yönünde bkz.: ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, s.66.

eğitim sürecinde gerçekleştirilen veri işleme faaliyetlerinin hukuka uygun şekilde yürütülmesi gerektiği gerçeğini değiştirmemelidir.

6698 sayılı Kanun incelendiğinde, İdarenin kişisel veri işlemek için 5/2-(ç) maddesinde yer verilen “*veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması*” şartına dayanabileceği kabul edilmelidir. Nitekim gerek MEB gerekse de kamu tüzel kişiliğini haiz olan üniversiteler, kanunlarla kendilerine verilen “eğitim-öğretim hizmetlerinin sunulması” görevini yerine getirmekle yükümlüdür. Özellikle, yüz yüze eğitimin yapılamadığı pandemi döneminde, çevrimiçi derslerle bu hizmetlerin devamı sağlanmıştır. Dolayısıyla, İdarenin yükümlülüklerini yerine getirebilmesi için çevrimiçi eğitim sürecinde işlenmesi zorunlu olan verileri ilgililerden açık rızası almaksızın Kanunun 5/2-(ç) hükmüne dayanarak işleyebilecektir⁴⁵⁹.

Öte yandan, çevrimiçi olarak gerçekleşen derslerde öğrencilerin ses ve görüntü verilerinin kaydedilmesi hususu ayrıca incelenmelidir. Öncelikle, görüntü ve ses verilerinin genel nitelikli kişisel verilerden olduğu ifade edilmelidir. Nitekim, Kişisel Verileri Koruma Kurumu’nun da atıfta bulunduğu Avrupa Birliği Genel Veri Koruma Tüzüğü’nün 4. Maddesinde biyometrik veri “*yüz görüntüleri veya daktiloskopi veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir.*” şeklinde tanımlanmaktadır⁴⁶⁰. Dolayısıyla, bir kişinin yalnızca görüntüsünün kaydedilmesi genel nitelikli veri işlenmesi anlamına gelirken, veri sorumlusunun belirli bir araç ya da yazılım kullanarak yüz tanıma işlemi yapması, başka bir deyişle gerçek bir kişinin görüntüsünü

⁴⁵⁹ Çevrimiçi olarak yapılan derslerde kişisel verilerin işlenmesini öngören açık bir kanun hükmü bulunmadığından İdare söz konusu verileri işlerken kanunlarda açıkça öngörülmesi şartına dayanamayacaktır. Öte yandan, İdare ile Devlet okullarında eğitim hizmeti alan öğrenciler arasında bir sözleşme ilişkisi bulunmadığından çevrimiçi dersler nedeniyle işlenen kişisel verilerde bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması şartına da dayanılamayacağı ifade edilmelidir. Milli Eğitim Bakanlığı’na bağlı olarak açılan özel okullar ile vakıf üniversitelerinde verilen çevrimiçi eğitimde de durum değişmemektedir. Vakıf üniversiteleri, Devlet üniversiteleri gibi birer kamu tüzel kişisidir (AYM, İhsan Doğramacı Bilkent Üniversitesi, B.n. 2013/1430, T.21.11.2013, §21.). 2547 sayılı Yükseköğretim Kanununa göre vakıf yükseköğretim kurumlarının eğitim – öğretim esasları, öğretim süreleri ve öğrenci hakları ile ilgili hususları bu Kanuna tabidir. Dolayısıyla, eğitim sürecinde işlenen kişisel veriler bakımından da Devlet üniversiteleriyle aynı kurallara tabi oldukları kabul edilmelidir (Aynı yönde görüş için bkz.: Fatma ESENYEL HANAZ, “Çevrimiçi Eğitimde Üniversite Öğrencilerinin Kişisel Verilerinin İşlenmesinin Hukuki Sebepleri”, **TBB Dergisi**, S.155, 2021, s. 420; Fatmagül KALE ÖZÇELİK, “Covid-19 Salgını Sürecinde Üniversite Eğitiminde Kullanılan Uzaktan Eğitim Platformlarının 6698 Sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi”, **SDÜHFD**, C.11, S.1, Y.2021, s.139.). Yine, 5580 sayılı Özel Öğretim Kurumları Kanunu’na göre okul öncesi, eğitim, ilköğretim, ortaöğretim, özel eğitim okulları ve özel öğretim kursları gibi kurumların Bakanlık’tan izin alması zorunlu olup (m.3/9), bu kurumlarda yürütülecek olan eğitim ve öğretimin 1739 sayılı Milli Eğitim Temel Kanununda belirlenen genel amaç ve ilkelere uygun olması, uygulanacak öğretim programının resmî kurumlarda uygulanan usul ve esaslara göre hazırlanması gerekmektedir (m.6/1). Dolayısıyla, kurum ile öğrenci velisi arasında öğrenim ücretine ilişkin bir özel hukuk sözleşmesi bulunsu da eğitim hizmetlerinin sunumu konusunda ilgili kanunlar çerçevesiyle sınırlı olarak yetkilendirildiğinden, özel okullar bu hizmetler sırasında işlenen kişisel verilerin işlenmesinde devlet okullarından farklı bir konumda yer almaz.

⁴⁶⁰ Kişisel Verileri Koruma Kurumu, **Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber**, s.4. <https://www.kvkk.gov.tr/Icerik/2030/Rehberler> (E.T. 3.4.2024).

benzersiz şekilde tanımlanmasını sağlayacak bir işlemten geçirmesi özel nitelikli veri işleme faaliyeti olarak kabul edilecektir⁴⁶¹.

Yalnızca görüntü ve ses verilerinin işlendiği durumlarda veri sorumlusu İdarenin 6698 sayılı Kanunun 5/2-(ç) maddesinde düzenlenen “*veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması*” şartına göre ilgisinin açık rızası olmaksızın veri işleyebileceği durumlar mevcuttur. Dersin niteliği, devam zorunluluğunun kontrolü ve öğrenci-öğretim elemanı etkileşiminin gerekliliği gibi hususlar, görüntü ve ses verilerinin işlenmesini zorunlu kılabilir. Örneğin, karma eğitim modelinde sınıfta bulunan öğrencilerle çevrimiçi katılan öğrenciler arasındaki etkileşimin sağlanması, derslere katılımın değerlendirilmesi veya dersin soru-cevap kısımlarının etkin şekilde yürütülmesi için en azından mikrofonun kullanılması gerekebilir. Bununla birlikte, İdarenin veri minimizasyonu ilkesi gereğince gerekli teknik ve idari tedbirleri alması, örneğin ders kayıtlarının dönem sonunda silinmesi, öğrenci görüntülerinin kaydedilmemesi gibi önlemleri uygulaması gerekmektedir. Ayrıca, öğrencinin derste aktif katılım göstermek istemediği durumlarda kamera açma zorunluluğu yerine, alternatif katılım ve değerlendirme yöntemlerinin geliştirilmesi düşünülmelidir.

Bununla birlikte, müzik ya da tiyatro gibi öğrencinin bireysel performansının duyulmasını, görülmesini gerektiren derslerde farklı bir değerlendirme yapmak gerekir. Nitekim, bazı derslerin gereği gibi yürütülebilmesi için öğrencinin derse aktif katılımı zorunlu ise bu halde kamera ve mikrofonun açık olması zorunlu kılınabilir. Benzer durum yapılan sınavlarda da geçerlidir. Adil bir değerlendirme yapılabilmesi için öğrencilerin kopya çekmesini engelleyecek yöntemlerin kullanılması esastır. Elbette, değerlendirmelerin mümkünse bireysel proje ödevleri aracılığıyla yapılması teşvik edilmelidir. Ancak her ders için bu yöntemin kullanılması beklenemez. Herkesin aynı anda soruları gördüğü ve kısıtlı bir zamanda cevaplayarak sisteme yüklemesi gerektiği klasik sınav yönteminde, kopya çekilmesinin önlenmesi için kamera ve mikrofon açılmasının zorunlu tutulması Kanunun 5/2-(ç) maddesi bağlamında hukuka uygun kabul edilmelidir.

Öte yandan, kopya çekilmesinin önlenmesi konusunda yapılan uygulamaların veri işleme ilkelerinden olan ölçülülük ilkesiyle de bağdaşır olması gerektiği unutulmamalıdır. Örneğin, Türkiye’de bir üniversite, Covid-19 pandemisi döneminde, çevrimiçi yapılacak sınavlarda kopya çekilmesinin önlenmesi amacıyla sınava girecek öğrencilere ayna göndermiş ve sınav esnasında bu ayna yardımıyla üçüncü kişilerden yardım alınmadığı, bilgisayar ekranında farklı pencerelerin açılmadığı gibi hususlarda emin olmak istemiştir⁴⁶². Söz konusu yöntem ya da ikinci bir kamera ile odanın tamamının görüntülenerek kayıt altına alınması yöntemi, sınavda kopya çekilmesini önlemeye yardımcı olarak

⁴⁶¹ KALE ÖZÇELİK, s.147; Melih R. ÇALIKOĞLU, “Görüntü ve Ses Biyometrik Veri Değildir”, **KVBLOG**, 16.4.2020, <https://kisiselveriler.blog/2020/04/16/goruntu-ve-ses-biyometrik-veri-degildir/> (E.T. 3.4.2024).

⁴⁶² “Uzaktan sınavda kopyaya aynalı önlem”, **NTV**, 18.2.2020, https://www.ntv.com.tr/video/turkiye/uzaktan-sinavda-kopyaya-aynali-onlem,h-r89QjnnkiFqq-8pj_rWQ (E.T. 8.8.2024).

akademik dürüstlüğü sağlamaya elverişlidir. Ancak yöntemlerin, bu amacın gerçekleştirilmesinde son çare olduğunu söylemek güçtür. Çünkü, ayna ya da ikinci bir kamera kullanılarak odanın içerisindeki diğer eşyaların (kitap, kıyafet, mobilyalar) kayıt altına alınması muhtemeldir. Bu durum öğrencinin özel hayatına açık bir müdahale niteliğindedir. Her öğrencinin ayrı bir odasının bulunmadığı gerçeği de göz ardı edilmemelidir. Ayrıca, bu yöntemlerle sınavla ilgisiz birçok verinin kayıt altına alınması veri minimizasyonu ilkesiyle de çelişmektedir. Dolayısıyla, kopya çekilmesini önlemek amacıyla alınan önlemin öğrencinin özel hayatına ve kişisel verilerinin korunması hakkına müdahale etmeyen veya daha az müdahale eden yöntemler olması gerekir. Bu bağlamda, öğrencilerin kaynaklara erişimine izin veren, ancak daha derinlemesine analiz ve uygulama gerektiren açık kitap sınavları; uzun süreli proje bazlı değerlendirmeler; video konferans yoluyla bireysel ya da küçük gruplarla yapılan sözlü sınavlar; öğrenciler arasındaki bilgi paylaşımını zorlaştırmak amacıyla geniş bir soru havuzundan her öğrenciye farklı sınav sorusunun atandığı sınavlar; sınav süresince öğrencinin bilgisayarında sadece sınav uygulamasının çalışmasına izin veren özel yazılımlar gibi yöntemlerden bazılarının ihtiyaca göre birlikte kullanımı tercih edilmesi kişisel veri koruma ilkelerine uygun olacaktır.

Yine eğitim kurumlarında sınavlarda kopya çekilmesinin önüne geçebilmek amacıyla yapay zekâ destekli yazılımlar kullanılarak öğrencilerin yüz tanıma, göz takibi, klavye tuşu vuruşu verilerinin biyometrik veri olarak işlenmek suretiyle, sınava giren kişinin ekran başında olduğu ve başkasıyla yer değiştirmede, sınav esnasında ekran dışında başka yerlere bakmadığı ve sınav alanında başka kimselerin bulunmadığı vb. şüpheli hareketlerin varlığı sürekli kontrol edilebilmektedir⁴⁶³. Bu şekilde toplanacak biyometrik verilerin işlenmesi 6698 sayılı Kanunun 6. maddesine uygun olarak işlenebileceğinden; bu veriler kanunlarda açıkça düzenlenmedikçe sadece ilgisinin açık rızası alınarak işlenebilir.

Ancak, açık rızanın özgür iradeyle verilmesi gerektiği unutulmamalıdır. Nitekim, bir üniversite öğrencisinin sınavı yapan, değerlendiren ve sonrasında mezuniyetini onaylayan kurumun kendisinden talep ettiği açık rıza konusunda karar verirken yeterince özgür olmadığı savunulabilir. İtalya Veri Koruma Otoritesi de 2021 Eylül ayında vermiş olduğu bir kararında, bir üniversitenin sınav güvenliğini sağlamak için öğrencilerden açık rıza alarak biyometrik veri işleyen bir yazılım kullanması hakkında, açık rızaya ilişkin bilgilendirmede, toplanan verilerin türü ve çeşidine ilişkin doğru ve yeterli bilginin verilmediğini belirtmiş, ayrıca söz konusu veri işlemenin yasal bir değeri olan not verme işlemi amacıyla yapıldığını ve üniversite ile öğrencilerin konumundaki bariz dengesizlik göz önüne alındığında, rızanın

⁴⁶³ Laura WALTERS, “Universities expand controversial AI monitoring of students taking online exams”, **STUFF**, 5.11.2021, <https://www.stuff.co.nz/national/education/126908715/universities-expand-controversial-ai-monitoring-of-students-taking-online-exams> (E.T.10.5.2024).

veri işlemenin yasal dayanağını oluşturamayacağına ve özgürce verilmiş olarak kabul edilemeyeceğine vurgu yapmış ve üniversite hakkında para cezası kararı vermiştir⁴⁶⁴.

Biyometrik verilerin işlenmesi için öğrencilerden alınacak açık rızanın geçerli olduğu kabul edilse bile, açık rızanın alınmış olması veri işlemeyi hukuka uygun hale getirmek için her zaman yeterli olmayacaktır⁴⁶⁵. Veri işlemenin genel ilkelere de uygun şekilde yapılması gerekir. Burada da sınav güvenliği ya da derse katılımın ispatı için biyometrik verileri işleyen yazılımların kullanılmasının her zaman ölçülü bir veri işleme faaliyeti olarak kabul edilip edilemeyeceği incelenmelidir. Örneğin, yaklaşık 30 kişinin katılacağı bir lisans dersinin çevrimiçi sınavında kopya çekilmesinin önlenmesi için bir gözetmen yerine iki ya da üç gözetmenin bulunması yeterli olabilecektir. Böyle bir sınavda biyometrik veri işlenmeden de amaca ulaşılabilir⁴⁶⁶. Ancak, sayıca çok daha fazla katılımcının bulunduğu bir sınav için aynı şey söylenemeyecektir. Örneğin, yurt genelinde şartları sağlayan herkesin katılabildiği ve aktif katılanların sayıca binleri bulduğu çevrimiçi sınavlarda biyometrik veri işlenmesi ölçülü kabul edilebilir. Burada katılımcı sayısı tek bir kriter olarak düşünülmemelidir. Amaç kopya çekilmesinin önlenmesi olduğunda, adaletsizliğin ortaya çıkmasından etkilenecek kitlenin büyüklüğü, toplum vicdanında oluşacak yara gibi kriterler de bu bağlamda işlenecek verilerin ölçülülüğü konusunda göz önünde bulundurulmalıdır.

Öte yandan, Avrupa’da çeşitli yerel mahkemelerin farklı yönde kararlar verdikleri göze çarpmaktadır. Hollanda’da yerel mahkeme tarafından pandemi döneminde verilen bir kararda, Amsterdam Üniversitesi tarafından çevrimiçi sınav gözetleme amacıyla biyometrik veri işleyen bir yazılımı kullanması hakkında, üniversitenin bir eğitim kurumu olarak eğitim vermek, sınavları yönetmek ve değerlendirmek gibi kamusal görevlerinin kanunlarla verildiğini, Avrupa Veri Koruma Tüzüğü’nün üniversitelerin görevlerini yerine getirmek için gerekli olduğu ölçüde kişisel veri işlemesine imkan tanıdığını, Covid-19 önlemlerinin belirli sınavların çevrimiçi olarak yapılmasını zorunlu kıldığını, üniversitelerin de bunu yaparken sahtekarlığı önlemek için gerekli çabayı göstermesi

⁴⁶⁴ İtalya Veri Koruma Otoritesi, Karar tarihi: 16.9.2021. <https://www.dataguidance.com/news/italy-garante-fines-luigi-bocconi-university-%E2%82%AC200000> (E.T. 12.5.2024).

⁴⁶⁵ Biyometrik veri toplayan yazılımlar ile sınav güvenliğini sağlama yöntemi özellikle Covid-19 pandemisinde dünyanın birçok yerinde kullanılmaya başlanmış ve bu durum öğrenciler tarafından tepkiyle karşılanmıştır: “Unfair surveillance”? Online exam software sparks global student revolt”, **Reuters**, 11.11.2020, <https://www.reuters.com/article/idUSKBN27Q1PY/> (E.T. 12.5.2024).

⁴⁶⁶ Öte yandan, hukuka aykırılık sadece ölçülülük ilkesinden kaynaklanmayabilir. Örneğin, Cleveland Devlet Üniversitesi’nde bir öğrenci, çevrimiçi sınava girmeden önce yazılım yüklü telefonun kamerasıyla sınava gireceği alanın tamamını göstermek zorunda olmasını dava etmiş, Federal Mahkeme, üniversitenin bu talebini Anayasa aykırı bularak öğrencilere böyle bir zorunluluk getirilemeyeceğine hükmetmiştir. Mahkeme, söz konusu talebin öğrencinin özel mülkünde yapılan bir arama niteliğinde olduğunu, Anayasa’ya göre kişinin özel mülkünde arama yapılabilmesi için istisnalar dışında mahkeme kararı gerektiğini, ve çevrimiçi sınavın bu istisnalardan biri olmadığını belirtmiştir: “Federal Judge: Invasive Online Proctoring 'Room Scans' Are Unconstitutional”, **Electronic Frontier Foundation (EFF)**, 25.8.2022, <https://www.eff.org/tr/deeplinks/2022/08/federal-judge-invasive-online-proctoring-room-scans-are-also-unconstitutional> (E.T. 12.5.2024).

gerektiğini, bu sebeple ilgili yazılımın kullanılmasının hukuka uygun olduğu sonucuna varmıştır⁴⁶⁷. Mahkeme ayrıca, bu tür yazılımların sınavların tamamını kayıt altına almadığı, sadece kopya şüphesinin tespit edildiği anları kaydettiği ve şifrelenmiş şekilde tutulan bu kayıtların 30 gün içerisinde otomatik olarak silindiği hususlarına da vurgu yapmıştır.

Benzer bir yazılımın üniversite tarafından kullanılmasının geçici olarak durdurulması talebini inceleyen Montreuil İdare Mahkemesi ise, ilgili uygulamanın sınava giren öğrencilerin kimliğini sürekli doğrulamak için biyometrik yüz verisini analiz ettiği, kopyanın engellenmesi için bilgisayardaki tüm verilere eriştiği, ses ve görsel ortamı yakaladığı ve sürekli olarak analiz ettiği, dolayısıyla kişisel verileri işlediği, ancak üniversitenin toplanan bu verilerin gerekliliğini, yeterliliğini, uygunluğunu ve sınırlarını detaylandırmadığı, bu sebeple Avrupa Genel Veri Koruma Tüzüğü'nün ihlal edildiği sonucuna vararak programın kullanılmasını yasaklamıştır⁴⁶⁸.

2.1.2. Sağlık Hizmetlerinde Kişisel Sağlık Verilerinin İşlenmesi

Sağlık hizmetleri, bireylerin en mahrem bilgilerini içeren kişisel sağlık verilerinin yoğun olarak işlendiği alanlardan biridir. Bu nedenle, sağlık verilerinin güvenli bir şekilde yönetilmesi, korunması ve paylaşılması büyük önem taşımaktadır. Kişisel sağlık verisinin tanımına Kişisel Sağlık Verileri Hakkında Yönetmelik'in 4/1(j) maddesinde yer verilmiştir. Buna göre, *“kişisel sağlık verisi kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileri ifade eder”*. GDPR'ın 4/15. maddesinde ise *“sağlığa ilişkin veriler(in), sağlık hizmetlerinin sağlanması da dahil olmak üzere, bir gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin olarak sağlık durumu hakkında bilgi veren kişisel veriler”* anlamına geldiği belirlenmiştir⁴⁶⁹.

⁴⁶⁷ “Court sides with University of Amsterdam on use of surveillance software”, **Cursor**, 12.6.2020, <https://www.cursor.tue.nl/en/news/2020/juni/week-2/court-sides-with-university-of-amsterdam-on-use-of-surveillance-software/> ya da <https://www.erasmusmagazine.nl/en/2020/06/12/court-sides-with-university-of-amsterdam-on-use-of-surveillance-software/> (E.T. 12.5.2024).

⁴⁶⁸ Tribunal Administratif de Montreuil, No: 2216570, 14.12.2022. Alıntıl原因: “After Students Challenged Proctoring Software, French Court Slaps TestWe App With a Suspension”, **Electronic Frontier Foundation (EFF)**, 31.3.2023, <https://www.eff.org/tr/deeplinks/2023/03/after-students-challenged-proctoring-software-french-court-slaps-testwe-app> (E.T. 12.5.2024).

⁴⁶⁹ GDPR'ın başlangıç bölümünün 35. paragrafında, sağlık verilerinin kapsamı detaylı bir şekilde ele alınmıştır. Bu tanıma göre, sağlık verileri yalnızca mevcut sağlık durumunu değil, aynı zamanda geçmiş ve gelecekteki fiziksel veya zihinsel sağlık durumuna ilişkin bilgileri de içermektedir. Bu geniş tanım, sağlık hizmetlerinin kaydı veya sunumu sırasında toplanan bilgileri, kişiyi sağlık amaçlı olarak benzersiz şekilde tanımlamak için atanan numara, sembol veya belirteçleri kapsamaktadır. Ayrıca, genetik veriler ve biyolojik örnekler de dahil olmak üzere vücut parçası veya vücut maddesinin test edilmesi veya incelenmesinden elde edilen bilgiler de sağlık verisi olarak kabul edilmektedir. GDPR, hastalık, engellilik, hastalık riski, tıbbi geçmiş, klinik tedavi veya kişinin fizyolojik veya biyomedikal durumu hakkındaki her türlü bilgiyi, kaynağına bakılmaksızın (örneğin, bir doktor, diğer sağlık profesyonelleri, hastane, tıbbi cihaz veya in vitro tanı testi) sağlık verisi kapsamında değerlendirmektedir. Çeşitli sağlık verisi örnekleri hakkında bkz.: Ozan GÜLHAN, “Kişisel Sağlık Verilerinin Korunması”,

Sağlık hizmetlerinden yararlanan bireylerin kişisel verileri, hizmetin sunumu sürecinin her aşamasında yoğun şekilde işlenmektedir. Hastanın ilk başvurusunda kimlik bilgileri, iletişim adresi ve sosyal güvenlik durumu gibi temel verilerle başlayan süreç; muayene esnasında hasta öyküsü, genetik bilgiler, laboratuvar sonuçları, radyoloji görüntüleri, tanı ve tedavi planları gibi doğrudan sağlık durumuyla ilgili hassas verilerin işlenmesiyle devam etmektedir. Örneğin, bir hastanın diyabet tedavisi sürecinde düzenli olarak kan şekeri ölçümleri, kullandığı ilaçlar, diyet programı ve yaşam tarzı değişiklikleri kayıt altına alınmakta; bir cerrahi operasyon öncesinde hastanın geçmiş ameliyatları, kullandığı ilaçlar, alerjileri ve genetik yatkınlıkları gibi kritik bilgiler sisteme işlenmektedir. Ayrıca hastanın rehabilitasyon sürecinde fizyoterapi uygulamaları, psikolojik destek görüşmeleri ve düzenli kontrol sonuçları da veri işleme faaliyetinin kapsamına girmektedir. Tüm bu veriler hem fiziksel hasta dosyalarında hem de hastane bilgi yönetim sistemlerinde elektronik ortamda saklanmakta ve sağlık hizmetinin etkin sunumu için ilgili sağlık personeli tarafından işlenmektedir.

Kişisel sağlık verileri özel nitelikli verilerden biri olarak kabul edildiğinden, bu verilerin işlenmesine ilişkin şartlar bakımından KVKK'nın 6. maddesi uygulanmaktadır. 7499 sayılı Kanunun 33. maddesiyle yapılan değişiklik öncesinde kişisel sağlık verileri ve cinsel hayata ilişkin veriler, yalnızca kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilmekteydi. Ancak bu şekliyle kural çeşitli eleştirileri de beraberinde getirmiştir⁴⁷⁰. Güncel ihtiyaçlar ve Avrupa Birliği Genel Veri Koruma Tüzüğü dikkate alınarak yapılan değişikliklerle sağlık verilerinin de içinde bulunduğu özel nitelikli verilerin işleme şartları sayıca artırılmıştır.

Bu bağlamda, sağlık hizmetlerinin sunumunda kişisel sağlık verisinin işlenmesi bakımından 6. maddede düzenlenen çeşitli veri işleme şartlarına dayanılabilir. Buna göre, öncelikle ilgili kişinin açık rızasının bulunması halinde kişisel sağlık verisi işlenebilmektedir; örneğin bir üniversite hastanesinde yürütülen klinik araştırmada hastanın tedavi sürecindeki verilerinin kullanılması için açık rıza alınması bu kapsamdadır. Kanunlarda açıkça öngörülmesi durumunda da veri işleme mümkündür; nitekim 3359 sayılı Sağlık Hizmetleri Temel Kanunu uyarınca e-Nabız sistemine veri aktarımı yapılması⁴⁷¹ ya da 5510

Marmara Üniversitesi SBE, Doktora Tezi, 2023, s. 15 vd.; Adem YELMEN, “Kişisel Sağlık Verilerinin Elektronik Ortamda İşlenmesi Üzerine Bir Değerlendirme”, **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, 18/2 (2023): 743-806, s.751.

⁴⁷⁰ Ayrıntılı bilgi için bkz.: “4.4.2.1. 2 Mart 2024 Tarihli 7499 Sayılı Kanun Değişikliği Öncesi Durum” başlığı.

⁴⁷¹ **3359 sayılı Kanun, Madde 3/f**: “(Değişik: 24/3/2016-6698/30 md.) Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi amacıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir.” Belirtmek gerekir ki mezkûr hükmün 24.3.2016 tarihli değişikliğinden önce “Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur” şeklindeki düzenlemeye istinaden çıkarılan ve tüm sağlık hizmeti veren kurumların e-Nabız sistemine sağlık verilerini aktarmasını öngören “E-Nabız Projesi” konulu genelge iptal edilmiştir. İptal kararında, ilgili hükmün genel bir düzenleme olduğu, kayıt ve bildirim sisteminin internet üzerinden bir yazılım yoluyla yapılacağı ve kişisel sağlık verisi kapsamındaki verilerin bu sisteme aktarılacağına yönelik bir düzenleme içermediği hassas veri kabul edilen kişisel sağlık

sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu gereğince SGK'ya sağlık verilerinin aktarılması bu şarta örnek gösterilebilir. Sağlık hizmetlerini sunmakla görevli ve yetkili olan Sağlık Bakanlığı da bu hizmetleri yerine getirirken kanunda açıkça öngörülmesi işleme şartına dayanarak kişisel veri işlemektedir. 3359 sayılı Kanun'a eklenen Ek Madde 19'un birinci fıkrasıyla, sağlık hizmeti almak üzere sağlık kuruluşları ve sağlık mesleği mensuplarına müracaat eden ilgililerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verilerinin işlenebileceği kabul edilmiştir⁴⁷².

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde de veri işlenebilmektedir; örneğin trafik kazası geçirmiş bilinci kapalı bir hastanın acil serviste tedavisi için geçmiş sağlık verilerine erişilmesi ve yeni sağlık verilerinin işlenmesi bu kapsamda değerlendirilmelidir. Ayrıca, istihdam ve sosyal güvenlik alanındaki hukuki yükümlülüklerin yerine getirilmesi amacıyla da veri işleme mümkündür; bu bağlamda çalışanların periyodik sağlık kontrollerinin yapılması ve kayıt altına alınması veya engelli bir bireyin sağlık kurulu raporunun hazırlanması ve sosyal hizmetlerden yararlanması için gerekli sağlık verilerinin işlenmesi örnek olarak gösterilebilir.

Öte yandan, yapılan kanun değişikliğine rağmen kanunda, sır saklama yükümlülüğü altında bulunan kişi ya da yetkili kurum ve kuruluşlarca kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla veri işlenebilmesi şartı 6/3-e maddesinde muhafaza edilmiştir. Değişiklik öncesinde, yalnızca sağlık ve cinsel hayata ilişkin verilerin işlenmesine ilişkin olarak kabul edilen bu hüküm için yeni düzenlemede böyle bir sınırlama öngörülmemiştir. Ancak, hükmün amaçsal yönden sınırlanma şekli ve getiriliş amacı göz önünde bulundurulduğunda, bu işleme şartına dayanarak sadece sağlık ve cinsel hayata ilişkin verilerin işlenebileceği kabul edilmelidir⁴⁷³.

6/3-e maddesinde belirlenen amaçlar dahilinde veri işleme sır saklama yükümlülüğü altında bulunan kişi ya da yetkili kurum ve kuruluşlarca mümkündür. Hekimler için sır saklama yükümlülüğü, Hekimlik Meslek Etiği Kuralları, Tıbbi Deontoloji Nizamnamesi ve Hasta Hakları Yönetmeliği'nde düzenlenmiştir. Hekimlik Meslek Etiği Kurallarının 9. maddesine göre hekim hastasından mesleğini

verilerinin toplanması ve işlenmesinin kapsamı, koşulları ve bu verilerin korunmasına ilişkin usul ve esasları içermeyen söz konusu yasal düzenlemelerin, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceyi sağlamaktan uzak olduğu gerekçelerine dayanılmıştır. Danıştay 15.D., E. 2015/2900, K. 2018/3876, T.18.4.2018. (danistay.gov.tr).

⁴⁷² 7538 sayılı Kanunun 2. maddesiyle 9.1.2025 tarihinde "Bilgi toplama, işleme ve paylaşma yetkisi" başlığı ile 3359 sayılı Kanuna eklenen bu düzenleme, daha önce 1 Sayılı CBK 378. maddesiyle düzenlenmiş; ancak kişisel verilerin korunması hakkını düzenleyen Anayasanın 20/3. maddesi uyarınca kişisel verilerin CBK'ler ile düzenlenemeyeceği gerekçesiyle AYM'nin 2018/118 Esas, 2023/189 Karar ve 26.10.2023 tarihli kararıyla Anayasa'ya aykırı bulunarak iptal edilmiştir.

⁴⁷³ KAYA, s.14.

icra ederken öğrendiği bilgileri açıklayamaz. Hastanın ölmesi ya da hekimle ilişkisinin sona ermesi hali de bu yükümlülüğü ortadan kaldırmaz. Yine Tıbbi Deontoloji Nizamnamesi'nin 4. maddesi uyarınca hekimlerin meslek ve sanatının icrası vesilesiyle elde ettiği sırları kanunda aksi öngörülmedikçe paylaşması yasaklanmıştır. Hasta Hakları Yönetmeliği'nin 23. maddesi ile de benzer şekilde sağlık hizmetlerinin verilmesi sebebiyle edinilen bilgilerin kanunlarda aksi öngörülmedikçe açıklanamayacağı kabul edilmiştir. Burada dikkat edilmesi gereken husus, sır saklama yükümlülüğünün yalnızca hekimlerle sınırlı olmamasıdır. Nitekim, Yönetmeliğin 3. maddesinde personel “Hizmetin, resmi veya özel sağlık kurumlarında ve kuruluşlarında veya serbest olarak sunulmasına bakılmaksızın, sağlık hizmetinin verilmesine iştirak eden bütün sağlık meslekleri mensuplarını ve sağlık meslekleri mensubu olmasa bile sağlık hizmetinin verilmesine sorumlu olarak iştirak eden kimseler” şeklinde tanımlanmış, Türk Ceza Kanunu'nun 280. maddesinde ise “sağlık meslek mensubu deyiminden tabip, diş tabibi, eczacı, ebe, hemşire ve sağlık hizmeti veren diğer kişiler”in anlaşılması gerektiği ifade edilmiştir. Öte yandan Yönetmeliğin 2. maddesinde düzenlemenin “sağlık hizmeti verilen resmi ve özel bütün kurum ve kuruluşları, bu kurum ve kuruluşlarda veya bunların dışında hizmete katılan her kademedeki ve unvandaki ilgilileri ve hizmetten faydalanma hakkını haiz olan bütün fertleri” kapsadığı ifade edilmiştir. Dolayısıyla, sağlık hizmetlerinin sunulmasına katılan herkesin sır saklama yükümlülüğü altında olduğu kabul edilmelidir⁴⁷⁴.

Sağlık hizmeti sunumu sürecinde işlenen kişisel verilerin hangilerinin sır kapsamında değerlendirilmesi gerektiği önemli bir hukuki sorundur. Öğretide sır kavramı sahibinin açıklanmamasında yarar gördüğü her türlü bilgi olarak tanımlanmaktadır⁴⁷⁵. Bu tanım çerçevesinde, kişinin toplum tarafından bilinen veya kolaylıkla öğrenilebilen özelliklerinin sır niteliği taşımayacağı kabul edilmektedir. Örneğin, kişinin görme engelli veya ortopedik rahatsızlığı gibi herkes tarafından gözlemlenebilecek sağlık durumlarının sır kapsamında değerlendirilemeyeceği ileri sürülmektedir⁴⁷⁶. Bununla birlikte, 6698 sayılı Kanun'un 6. maddesi sağlık ve cinsel hayata ilişkin kişisel verilerin, sır saklama yükümlülüğü altında bulunan kişilerce, üçüncü fıkra da belirlenen amaçlar doğrultusunda işlenebileceğini düzenlemektedir. Bu düzenlemede, söz konusu verilerin sır niteliği taşıması gibi bir koşul öngörülmemiştir. Bu durum, kişisel veri kavramının meslek sırrı kavramını kapsayan daha geniş bir içeriğe sahip olmasından kaynaklanmaktadır⁴⁷⁷. Bu bağlamda, sır saklama yükümlülüğünün ihlali

⁴⁷⁴ “Dolayısıyla, hekimin mahiyetinde çalışan asistan, stajyer, ebe, hasta bakıcı, hasta baş hekimi ve idare memurları da sır tutmakla yükümlüdürler.” Maral TÖRENLİ ÇAKIROĞLU, “Hekimin Borçlarından Özel Olarak Sır Saklama Borcu”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 12, S. 2, 2010, s. 159-181 (Basım Yılı: 2012), s. 172.

⁴⁷⁵ Sabire Senem YILMAZ, **Tıp Alanında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, 2021, 5. Baskı, s. 39.

⁴⁷⁶ YILMAZ, a.g.e., s. 42-43.

⁴⁷⁷ Murat Volkan DÜLGER, “Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, C. 1, S.2, 2015, s. 45. “TCK'nun 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özeldir ise kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin

nedeniyle uygulanacak disiplin cezaları açısından sır kavramı önem taşımakla birlikte⁴⁷⁸ 6698 sayılı Kanun'un uygulanması bakımından belirleyici olan husus, bilginin sır niteliği değil, sağlık ve cinsel hayata ilişkin kişisel veri olmasıdır. Dolayısıyla, toplum tarafından kolaylıkla gözlemlenebilen bir ortopedik rahatsızlığa ilişkin sağlık verisi, sır niteliği taşımasa dahi 6698 sayılı Kanun kapsamında koruma altındadır.

6698 sayılı Kanun'un 6/3-e maddesinde düzenlenen veri işleme şartında sağlık verilerinin kamu sağlığının korunması ve koruyucu hekimlik kapsamında işlenmesi, kamu düzeninin sağlanması ve korunması bakımından genel sağlık alanındaki kolluk faaliyetleri kapsamında işlenen sağlık verilerine ilişkin bulunduğundan bu kısma ilişkin açıklamalara aşağıda yer verilecektir⁴⁷⁹. Aynı hükümde yer verilen tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi kapsamında veri işlenmesi ise bir kamu hizmeti olarak sunulan sağlık hizmetleri çerçevesinde değerlendirilmelidir. Hükümde ayrıca düzenlenen sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla veri işlenmesi hususu ise, doğrudan kamu hizmeti niteliğindeki sağlık hizmetinin sunumuna değil, bu hizmetin organizasyonuna yönelik idari faaliyetlere ilişkindir⁴⁸⁰.

Tıbbi teşhis, semptomlarından hareketle bir kişinin hastalığının ne olduğunun belirlenmesi anlamına gelir. Hasta olan kişinin bir sağlık kurumuna başvurması üzerine hekim tarafından dinlenmesi, gerekli testlerin yapılması sonucunda hastanın sağlık sorunun tanımlanması tıbbi teşhis sürecini oluşturur. Tıbbi teşhisin amacının hastanın varsa hastalığının ortaya konulması olduğu dolayısıyla hiçbir hastalığa rastlanılmamış olmasının faaliyetin tıbbi teşhis niteliğini ortadan kaldırmayacağı ifade edilmektedir⁴⁸¹. Tıbbi tedavi hizmetleri ise teşhisi yapılan hastalığın iyileştirilmesi, hafifletilmesi ya da tamamen ortadan kaldırılması amacıyla gerçekleştirilen eylemlerin tümünü ifade eden bir kavramdır. Bu bağlamda tedavi amacıyla hastaya yapılacak tıbbi müdahalelerden teşhis, tedavi, önleme amaçlı müdahaleler, reçete yazılması, tahlil ve tetkikler, psikiyatrik müdahale, estetik cerrahi ve adli muayene

suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır." Yargıtay CGK, E. 2012/1510, K. 2014/331 (**Lexpera Hukuk Otomasyonu**).

⁴⁷⁸ Türk Ceza Kanunu'nun 136. maddesinde düzenlenen "verileri hukuka aykırı olarak verme veya ele geçirme" suçunun da sır saklama yükümlülüğüne aykırı hareket edilmesi halinde uygulanan bir hüküm olduğu ifade edilmektedir. YILMAZ, a.g.e., s. 44. 765 sayılı mülga Türk Ceza Kanunu'nda sır kavramına yer verilmesine karşın (Sırrın Masuniyeti Aleyhine Cürümler/ madde 198) 5237 sayılı Türk Ceza Kanunu'nda bu kavrama yer verilmemiştir. İlgili hükmün ayrıntılı anlatımı için bkz.: Sinem GÖÇMEN UYARER, **Kişisel Verilerin Korunması**, Seçkin Yayıncılık, 2. Baskı, 2020, s. 99 vd.; İbrahim KORKMAZ, **Kişisel Verilerin Türk Ceza Hukuku Kapsamında Korunması**, Seçkin Yayıncılık, 2. Baskı, s. 375 vd.

⁴⁷⁹ Bkz.: "2.2.1. Genel Sağlığın Korunmasında Veri İşleme" başlığı.

⁴⁸⁰ YÜZBAŞIOĞLU, s.58. Sağlık hizmetleri ve finansmanının planlanması ve yönetimi sürecinde kişisel sağlık verilerinin işlenmesi, sağlık sisteminin etkin işleyişi için kritik bir öneme sahiptir. 3359 sayılı Sağlık Hizmetleri Temel Kanunu çerçevesinde, sağlık hizmetlerinin eşit, kaliteli ve verimli sunumu için gerekli olan veri işleme faaliyetleri, 6698 sayılı KVKK kapsamında özel olarak düzenlenmiştir. Bu bağlamda, sağlık finansmanının sürdürülebilirliği için gerekli olan risk analizleri, kaynak planlaması ve hizmet dağılımı gibi temel fonksiyonların yerine getirilmesi amacıyla ilgili hükme dayalı olarak kişisel sağlık verileri işlenebilir. Örneğin, bölgesel sağlık ihtiyaçlarının belirlenmesi, sağlık sigortalarının risk değerlendirmelerinin yapılması ve primlerin hesaplanması gibi işlemler, bu kapsamda değerlendirilmektedir.

⁴⁸¹ Polat TUNÇER, **Sağlık Hukuku Temel Bilgileri**, Adalet Yayınevi, 4.Baskı, s.74.

gibi ameliyelerin⁴⁸² tamamı sırasında yapılacak veri işleme faaliyetlerinde 6/3-e maddesine dayanılabilir. İyileştirme amacı olmayan estetik operasyonlar, organ nakli, suni dölleme ve cinsiyet değişikliği gibi müdahalelerin de tedavi kapsamında olduğu ifade edilmektedir⁴⁸³. Tıbbi bakım hizmetleri ise yine sağlığın korunması, önlenmesi ile hastalığın tedavisini sağlayan hizmetlerin bütünü olarak ifade edilebilir. Özellikle ameliyat sonrası yara bakımı, enjeksiyon uygulaması, hemşirelik hizmeti, yaşlı ve engelli bakımı gibi hizmetler tıbbi bakıma örnek olarak verilebilir.

Sağlık hizmetlerinin sunumunda hasta mahremiyeti ve kişisel verilerin işlenmesi büyük önem taşır. Sağlık kuruluşlarında bu konuda hassas bir denge kurulması gerekmektedir. Özellikle eğitim ve araştırma hastanelerinde tıbbi teşhis, tedavi ve bakım hizmetlerinin görülmesi sırasında hastayla doğrudan ilgilenen hastane personeli dışında eğitim amacıyla tıp öğrencilerinin bulunması ve dolayısıyla hastanın kişisel sağlık bilgilerine bu kişilerce vakıf olunması hastanın açık rızası alınmadığı sürece hukuka aykırıdır. Nitekim, kişisel sağlık verilerinin işleme şartları arasında “eğitim” amacına yer verilmemiştir. Öte yandan Hasta Hakları Yönetmeliği’nin 21. maddesinin son fıkrasında da “*Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır*” kuralına yer verilmek suretiyle ilgisinden açık rıza alınması gerekliliği belirtilmiştir.

Yine kamu hastanelerinde yaşanan sorunlardan biri de kaynak yetersizliği nedeniyle aynı odada birden fazla hastaya tıbbi müdahalede bulunulması ve hastanın bilgilendirilmesidir. Bu durumda hastaların ve kimi zaman hasta yakınlarının birbirlerine ait kişisel sağlık verilerini öğrenmesi kişisel verilerin gizliliği kuralıyla bağdaşmamaktadır. Anayasanın 65. maddesinde yer verilen “*Devlet, sosyal ve ekonomik alanlarda Anayasa ile belirlenen görevlerini, bu görevlerin amaçlarına uygun öncelikleri gözeterek mali kaynaklarının yeterliliği ölçüsünde yerine getirir*” kuralı gereği bu durumun tek başına hukuka aykırılık yaratmayacağı kabul edilebilirse de İdarenin en azından imkânları nispetinde mahremiyeti sağlayacak önlemler alması gerekir⁴⁸⁴.

Sıkça karşılaşılan bir başka durum, muayene sırasında hastanın bir yakınının da odaya girmesi ve hasta hakkındaki sağlık bilgilerine vakıf olmasıdır. Hekimlerin sır saklama yükümlülüğü ve Hasta Hakları Yönetmeliği’nin hasta mahremiyetine ilişkin 21. maddesi birlikte değerlendirildiğinde, hastanın açık rızası olmadan yakınının muayene odasına girmesi ve bilgi edinmesi, sağlık verilerinin üçüncü kişiyle paylaşılması anlamına geleceğinden hukuka aykırıdır. Hastanın yakınıyla birlikte hekimin yanına girmesi, bilgiler açıklanırken üçüncü kişinin bulunmasına ses çıkarmaması bir rıza olarak kabul

⁴⁸² Hakan HAKERİ, **Tıp ve Sağlık Hukuku El Kitabı**, Seçkin Yayıncılık, 2022, s.28

⁴⁸³ Canan İMANÇLI, **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu**, On İki Levha Yayıncılık, Nisan 2020, s.148.

⁴⁸⁴ Aksi halde İdarenin sağlık hizmetini yürütürken kusurlu hareket ettiği kabul edilmelidir: YÜZBAŞIOĞLU, s.147. Sağlık kuruluşlarında yaşanan hasta mahremiyeti ihlallerine ilişkin bkz.: Yakup KORKMAZ, “Hasta Hakkı Olarak Özel Hayatın Korunması Bağlamında Beden Mahremiyeti”, **Uyuşmazlık Mahkemesi Dergisi**, Y.8, S.15, Haziran 2020, s. 581 vd.

edilebilirse de KVKK bağlamında “açık rıza” olarak değerlendirilemeyecektir. Bununla birlikte, ülkemizin sosyolojik şartları göz önüne alındığında, hekimin hasta yakınıni her zaman dışarı çıkarması mümkün olmayabilir. Üstelik, ısrarla dışarı alınan hasta yakını ile hasta arasında muayene sonrasında huzursuzluk veya şiddet olayları yaşanabileceği de bilinmektedir. Bu gibi durumlarda hastanın açık rızasının sorulması halinde, olası olumsuz sonuçları öngören hastanın rızasına yönelik beyanına da güvenmek zorlaşmaktadır.

Ancak, her vakada benzer olumsuz sonuçların doğmayacağı düşünülerek, öncelikle sağlık kurumlarında hasta yakınının odaya girmesinin yasak olduğuna dair bilgilendirici afişler ve kamu spotları gibi araçlarla toplumun bilinçlendirilmesine katkı sağlanabilir. Ayrıca bu hususun bir yönetmelikle düzenlenmesi ve belli durumlar için istisnalar öngörülmesi (örneğin 16 yaşından küçük çocukların aile yakınıyla birlikte girmesi) düşünülebilir⁴⁸⁵. Buna ek olarak, doktor değerlendirmesi ve gerekli açıklamaların hastanın yüzüne karşı yapılması kaydıyla, imkân dahilinde bazı tetkik ve tahlil sonuçlarının dijital araçlarla iletilmesi yöntemine ağırlık verilebilir. Son olarak, her vakanın kendine özgü koşulları olabileceği göz önünde bulundurularak, özellikle açık rızanın geçerliliği konusunda sağlık personeline karar verme yetkisi ve sorumluluğu verilmesi gerekir.

2.1.3. Akıllı Ulaşım Sistemleri ile Sunulan Ulaşım Hizmetlerinde Kişisel Veri İşleme

Akıllı Ulaşım Sistemleri (AUS), ulaşım ağlarının verimliliğini ve güvenliğini artırmak amacıyla geliştirilmiş bilgi ve iletişim teknolojilerine dayalı bütünleşik bir sistemdir. Bu sistem; sürücüler, araçlar, yol altyapısı ve kontrol merkezleri arasında çok yönlü veri alışverişi sağlayarak trafik akışını izleme, ölçme, analiz etme ve yönetme imkânı sunar⁴⁸⁶.

AUS, sürücülerin ve yayaaların güvenliğini sağlamak için kameralar, algılayıcılar ve benzeri uygulamalar yardımıyla araç, çevre ve altyapıdan elde edilen büyük veriyi analiz ederek ulaşım kolaylığı sunar. Özellikle kişisel verilerin işlenmesi bağlamında, AUS kapsamında toplanan veriler idare tarafından çeşitli amaçlarla kullanılabilir. Örneğin, trafik yoğunluğunu ve araç hareketlerini izlemek için kameralar kullanılabilir. Bu sayede trafik akışı optimize edilebilir, yolcu güvenliği artırılabilir ve acil durum müdahalesi kolaylaştırılabilir. Benzer şekilde, toplu taşıma araçlarındaki kalabalık seviyelerini ölçmek için basınç sensörleri kullanılabilir. Elde edilen veriler, sefer saatlerini ve güzergahları planlama

⁴⁸⁵ Kişisel sağlık verilerine erişim konusunda çocukların yetkinliği, güncel mevzuatta düzenlenmiştir. Kişisel Sağlık Verileri Hakkında Yönetmelik'in 8/1. maddesi uyarınca, ayırt etme gücüne sahip çocuklar, sağlık geçmişlerine ebeveynlerinin erişimini e-Nabız sistemi üzerinden izne tabi tutabilmektedir. Bu düzenleme, çocukların sağlık verilerine ilişkin kararlarda erginlik yaşından (18) daha erken bir dönemde söz sahibi olabileceklerini göstermektedir. Zira burada belirleyici olan husus, çocuğun kendi sağlığına ilişkin konularda ayırt etme gücüne sahip olup olmadığıdır.

⁴⁸⁶ T.C. Ulaştırma ve Altyapı Bakanlığı, Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı, s.11.

veya sosyal mesafe kurallarına uyumu sağlama gibi amaçlarla değerlendirilebilir. Ayrıca AUS, enerji verimliliği ve çevrenin korunmasına da katkı sağlar. Örneğin akıllı sinyalizasyon sistemleri, gereksiz bekleme sürelerini azaltıp trafik akışını optimize ederek yakıt tüketimini ve emisyonları azaltabilir. Yine elektrikli araçlar için şarj istasyonlarının konumlarını ve kullanılabilirliğini gösteren uygulamalar, bu araçların yaygınlaşmasını teşvik edebilir. Dolayısıyla, AUS'un sağladığı faydaların sadece ulaşım sınırlı olmadığı, enerji, çevre, güvenlik ve sağlık gibi pek çok alanı kapsadığı ifade edilmelidir⁴⁸⁷.

Ayrıca, akıllı ulaşım sistemlerinde yapay zekâ uygulamaları, kişisel veri işleme pratiklerini radikal biçimde dönüştürmektedir. Trafik yönetimi, yolcu güvenliği, rota optimizasyonu ve tahmin modellerinde kullanılan yapay zekâ sistemleri, büyük veri setlerini işlerken aynı zamanda hassas kişisel verilerin de toplanması ve analiz edilmesi sonucunu doğurmaktadır⁴⁸⁸. Örneğin, sürücülerin sağlık verileri (epilepsi, kalp rahatsızlığı gibi tıbbi bilgiler), biyometrik veriler (yüz tanıma sistemlerinde kullanılan biyometrik görüntüler) ve sürüş davranış profilleri gibi veriler yapay zekâ sistemleri tarafından işlenebilmektedir. Sürücüsüz araçlar, akıllı trafik yönetim sistemleri ve toplu taşıma uygulamaları, konum verileri, kimlik bilgileri, hareket profilleri gibi çok sayıda kişisel veriyi sürekli olarak işlemektedir⁴⁸⁹. Bu uygulamalar, kişisel verilerin korunması hukuku açısından yeni tartışma alanları ve düzenleme ihtiyaçları ortaya çıkarmaktadır⁴⁹⁰.

Dünya'da özellikle gelişmiş ülkelerde farklı akıllı ulaşım sistemleri yaygın olarak kullanılmaktadır. Örneğin Japonya'da 2011 yılında otoyollarda hayata geçirilen AUS Spot hizmeti ile bağlantılı araç teknolojileri (DSRC) aracılığıyla uyarlanabilir hız sabitleyici (ACC) donanımlı araçlarla iletişim kurarak hızlarını buna göre ayarlamak suretiyle trafik sıkışıklığını önemli oranda azaltmayı başarmıştır. Yine 2009 yılında başlatılan projeyle, arabalara takılan araç bilgi ve iletişim sistemi (VICS) ile sürücülerin hedeflerine en uygun rotayı bulmalarına yardımcı olunmuş, trafik yoğunluğunun azalmasına katkıda bulunulmuştur⁴⁹¹. Güney Kore ise trafik yoğunluğunun ve kazaların azaltılması için

⁴⁸⁷ T.C. Ulaştırma ve Altyapı Bakanlığı, Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi (2014-2023) Güncellemesi ve 2020-2023 Eylem Planı Hazırlama Projesi: 5 Ülkenin AUS Yaklaşımları ve Mevcut AUS Strateji Belgelerinin Analizi, 2018, s.17.

⁴⁸⁸ Lilian EDWARDS, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective", **European Data Protection Law Review (Lexxion)**, January 5, 2016, s.7, <https://ssrn.com/abstract=2711290>.

⁴⁸⁹ Şafak NARBAY, Şerife Nur KİRAZLI, "Otonom Araçlarda Yapay Zekâ, Kişisel Verilerin İşlenmesi ve Sonuçları", **Sakarya Üniversitesi Hukuk Fakültesi Dergisi**, C.1, S.1, Temmuz 2023, s. 58.

⁴⁹⁰ Aslında idarenin faaliyetlerinde yapay zekâ kullanımı akıllı ulaşım sistemleriyle sınırlı değildir. Kamu hizmetlerinin sunumu ve planlanması ile kamu düzeninin korunması amacıyla çok çeşitli alanlarda yapay zekâ teknolojilerinden yararlanılmakta ve bu süreçte kişisel veriler işlenmektedir. Örneğin, sosyal yardım başvurularının değerlendirilmesinde karar destek sistemleri, sağlık hizmetlerinde hastalık teşhis ve tedavi önerilerinde yapay zekâ uygulamaları, güvenlik ve kolluk faaliyetlerinde suç önleme ve risk analizi için kullanılan tahmine dayalı yapay zekâ sistemleri, vergi denetiminde usulsüzlük tespiti için geliştirilen algoritmalar gibi pek çok alanda yapay zekâ teknolojileri idari faaliyetlerin ayrılmaz bir parçası haline gelmiştir. İdarenin faaliyetlerinde yapay zekâ kullanımı hakkında detaylı bir inceleme için bkz.: Serkan SEYHAN, **Yapay Zekâ Teknolojileri Kapsamında İdarenin Sorumluluğu**, On İki Levha Yayıncılık, Mart 2023, s. 152 vd. Ayrıca, YZ sistemlerinin KVKK'de belirlenen veri işleme ilkeleriyle olan uyumuna dair bilgi için bkz.: E. Eylem AKSOY RETORNAZ / Osman Gazi GÜÇLÜTÜRK, "Yapay Zekânın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi" içinde **Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ**, E. Eylem AKSOY RETORNAZ ve Osman Gazi GÜÇLÜTÜRK (editörler), İstanbul, On İki Levha Yayıncılık, 2021, 275-302.

⁴⁹¹ T.C. Ulaştırma ve Altyapı Bakanlığı, Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı, s.101.

ilk çalışmalara başladığı 1990 yılından bu yana gerçek zamanlı trafik bilgileri sağlama, ileri toplu ulaşım bilgi sistemi, otoyol elektronik ücret toplama sistemi ve toplu taşımada kullanılan akıllı kart gibi farklı akıllı ulaşım sistemlerini uygulamaya koymuştur⁴⁹². AUS uygulamalarında lider ülkelerden biri olan ABD ise AUS mimarisini geliştirerek ülke genelinde yaygınlaştırmakta ve K-AUS sistemleri⁴⁹³, elektrikli araçlar, bağlantılı araç teknolojileri (DSRC) ile otonom araçlara odaklanmaktadır. AUS örnekleri arasında çarpışma önleyici teknolojiler, değişken hız sınırı sistemleri (VSL), dinamik şerit birleştirme sistemleri (DLMS) ve Kamyon Park Bilgi Sistemi (TPIS) bulunmaktadır⁴⁹⁴.

Türkiye’de uygulanan AUS örneklerini ise şu şekilde özetlemek mümkündür: Sinyalizasyon sistemleri, acil haberleşme sistemi, SCADA kontrol merkezi, elektronik toplu taşıma bileti (AKBİL), yerli sinyalizasyon sistemi, trafik kontrol merkezi, otomatik geçiş sistemi (OGS), kartlı geçiş sistemi, değişken mesaj sistemleri (DMS), trafik bilgi sistemi, web tabanlı trafik bilgilendirme sistemi, mobil trafik uygulaması, elektronik denetleme sistemi, kırmızı ışık ihlal tespit sistemi, otonom araç çalışmaları, araç-arac ve araç-altyapı iletişimi, ulusal ulaşım portalı, adaptif sinyalizasyon sistemi, temassız ödeme projesi, ulusal AUS mimarisi, kamera tabanlı sinyalizasyon sistemleri, elektronik denetleme sistemleri (EDS), ve akıllı otoyol uygulamaları⁴⁹⁵.

⁴⁹² T.C. Ulaştırma ve Altyapı Bakanlığı, Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı, s.104.

⁴⁹³ K-AUS, Kooperatif Akıllı Ulaşım Sistemleri'nin kısaltmasıdır. Bu sistem, araçların birbirleriyle ve yol altyapısıyla iletişim kurmasını sağlayan ileri teknoloji uygulamalarını ifade etmektedir. K-AUS'un temel amacı, trafik güvenliğini artırmak, ulaşım verimliliğini iyileştirmek ve çevresel etkileri azaltmaktır. Bu sistemler, araçlar, yol kenarı üniteleri ve trafik yönetim merkezleri arasında gerçek zamanlı bilgi paylaşımını mümkün kılmaktadır. K-AUS, geleneksel AUS'un bir adım ötesine geçerek, ulaşım sisteminin tüm bileşenleri arasında daha yoğun ve kapsamlı bir iş birliği sağlamayı amaçlar. Bu sistemde araçtan araca (V2V) iletişim, araçtan altyapıya (V2I) iletişim, gerçek zamanlı trafik ve yol durumu bilgileri, gelişmiş sürücü destek sistemleri ve acil durum uyarıları ile otomatik fren sistemleri gibi uygulamalar kullanılmaktadır. Ayrıntılı bilgi için bkz.: Buket ÇAPALI, “Akıllı Ulaşım Sistemleri Mimarisi: K-AUS için Öneri”, **El-Cezerî Fen ve Mühendislik Dergisi**, 2022, 9(4); 1249-1254.

⁴⁹⁴ T.C. Ulaştırma ve Altyapı Bakanlığı, Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı, s.107. Çeşitli ülkelerde uygulanan akıllı ulaşım sistemleri, şehir içi ulaşımı optimize etmek ve vatandaşlara daha iyi hizmet sunmak amacıyla teknolojiden yararlanmaktadır. Glasgow’da, toplu taşıma kullanıcılarına otobüslerin konumu, doluluk oranı ve varış süreleri gibi gerçek zamanlı bilgilerin sunulması, Seul’de, gece otobüs hatları planlanırken cep telefonu konum verilerinin analiz edilerek talep yoğunluğunun belirlenmesi; New Orleans’ta acil durum çağrı modelleri incelenerek ambulansların konumlarının optimize edilmesi; Sidney’de Avustralya’nın ilk tam otomatik metro sistemi hizmete girmesi; Kopenhag’da, 24 saat kesintisiz hizmet veren ve yüksek frekanslı seferler düzenleyen sürücüsüz bir metro hattının işletilmesi AUS uygulamalarına örnek olarak verilebilir: Guilherme SANTO, Leonel SANTOS, Rogério L. C. COSTA, Carlos RABADÃO, "Intelligent Transportation Systems Security and Privacy." **Information Security and Privacy in Smart Devices: Tools, Methods, and Applications**, Carlos RABADÃO, et al. (eds), IGI Global, 2023, s. 122-141. <https://doi.org/10.4018/978-1-6684-5991-1.ch005>. Yine Singapur’da Kara Ulaşım İdaresi, günlük 6,3 milyon yolculuğu kapsayan toplu taşıma sistemini optimize etmek için büyük veri yöntemlerinden faydalanmıştır. PLANET adı verilen projeye, günde 12 milyon toplu taşıma işlemi analiz edilerek, yolcu davranışlarını anlamak ve hizmet kalitesini artırmak için kullanılmaktadır. Bu sistem sayesinde, otobüs seferlerinin sıklığı talebe göre ayarlanabilmekte ve kalabalık rotalar tespit edilebilmektedir. Ayrıca, Singapur’da acil durum müdahalelerini iyileştirmek amacıyla FASTER teknolojisi kullanılmaya başlanmıştır. Bu teknolojinin, ücret kartı verileri, video görüntüleri ve anonim telekomünikasyon verilerini bir araya getirerek toplu taşıma sisteminin verimliliğini artırdığı ifade edilmiştir. Ülkede uygulanan bir diğer proje olan Travel Smart Programı ise, yoğun saatlerdeki yolcu trafiğini düzenlemek için teşvik ve ödül sistemleri kullanılmaktadır: MACIEJEWSKI, s.120-135.

⁴⁹⁵ T.C. Çevre ve Şehircilik Bakanlığı Coğrafi Bilgi Sistemleri Genel Müdürlüğü, **Akıllı Ulaşım**, s.11 vd. <https://www.akillisehirler.gov.tr/wp-content/uploads/Ulasim.pdf> (E.T. 7.8.2024).

Yukarıda örnekleri görüldüğü üzere, akıllı ulaşım sistemlerinde kullanılan sensörler, mobil uygulamalar, akıllı kartlar gibi farklı araçlarla kişilerin kimlik (isim, sürücü belgesi ve plaka bilgileri), konum (GPS koordinatları, seyahat rotaları, hız bilgileri), ödeme, seyahat alışkanlıkları, araç, sürüş davranışı, toplu taşıma kullanımı, trafik kamera görüntüleri gibi çok çeşitli kişisel verilerinin işlenmesi söz konusudur. Tüm bu verilerin işlenmesi kanuna uygun olarak yapılmalıdır. AUS uygulamalarında veri işlemenin bir kısmı özellikle otonom araçlardan toplanan veriler bağlamında özel hukuk kişileri tarafından gerçekleştirilirken, önemli kısmı ise İdare tarafından gerçekleştirilmektedir. Öte yandan, AUS uygulamalarının tam ve verimli çalışmasının sağlanması kimi zaman verilerin anlık olarak sürücüler-şirket-merkez arasındaki koordinasyon içerisinde paylaşılmasını da gerektirdiğinden, bu tür uygulamalarda işlenen tüm verilere İdarenin de temas edeceği, başka bir deyişle verileri işleyeceği söylenebilir. İşte İdarenin bu veri işleme faaliyetlerini de kişisel verilerin korunması mevzuatına uygun şekilde gerçekleştirmesi gerekmektedir.

Ulaştırma ve Altyapı Bakanlığı bünyesinde hazırlanan Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı'nda AUS altyapısının geliştirilmesi, sürdürülebilir akıllı hareketliliğin, yol ve sürüş güvenliğinin ve veri paylaşımı ile veri güvenliğinin sağlanması gibi amaçların belirlendiği ifade edilmektedir⁴⁹⁶. Bu bağlamda KVKK düzenlemesinin 5. ve 6. maddelerinde yer verilen veri işleme şartları düşünüldüğünde, genel nitelikli verilerin işlenmesi bakımından ilgisinden açık rıza alınması dışında, “kanunda açıkça öngörülme” ve “hukuki yükümlülüklerin yerine getirilmesi bakımından zorunlu olması” şartlarına; özel nitelikli veriler bakımındansa açık rıza ve “kanunlarda açıkça öngörülme” şartlarına dayanarak İdarenin veri işleyebileceği kabul edilmelidir.

Mevzuat incelendiğinde, akıllı ulaşım sistemlerinin kurulmasını ve buna bağlı veri işlenmesini doğrudan öngören bir kanun hükmü bulunmadığı görülmektedir. Bununla birlikte, kamu kurumlarına akıllı ulaşım sistemlerinin kurulması ve yönetimine ilişkin yükümlülükler getiren Cumhurbaşkanlığı Kararnamesi ve çeşitli yönetmeliklerle bu sistemlerin bileşenlerinden sayılan bazı uygulamaların gerçekleştirilmesine olanak sağlayan çeşitli yükümlülükler ve yetkiler öngören kanun düzenlemeleri bulunmaktadır.

Öncelikle kanun düzenlemelerine bakıldığında, 5216 sayılı Büyükşehir Belediyesi Kanunu'nun 7. maddesinin 1. fıkrasının (f) bendinde, büyükşehir belediyelerinin ulaşım ve toplu taşıma hizmetlerine ilişkin görev ve yetkilerinden bahsedilmektedir. Buna göre, büyükşehir belediyeleri, büyükşehir ulaşım ana planını yapmak, yaptırmak ve uygulamakla yükümlüdür. Ayrıca, ulaşım ve toplu taşıma hizmetlerini planlama ve koordine etme, çeşitli ulaşım araçlarının sayılarını, ücretlerini, güzergahlarını belirleme, durak ve park yerlerini tespit etme, işletme veya kiraya verme gibi görevleri de büyükşehir belediyelerine verilmiştir.

⁴⁹⁶ T.C. Ulaştırma ve Altyapı Bakanlığı, **Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı**, s.38.

Benzer şekilde, 5393 sayılı Belediye Kanunu'nun 15. maddesinin 1. fıkrasının (p) bendinde, belediyelerin ulaşım ve toplu taşıma hizmetlerine ilişkin görev ve yetkileri düzenlenmektedir. 5216 sayılı Kanun'da olduğu gibi, belediyeler de ulaşım araçlarının sayılarını, ücretlerini, güzergahlarını belirleme, durak ve park yerlerini tespit etme, işletme veya kiraya verme gibi görevleri yerine getirmekle yükümlüdür.

4925 sayılı Karayolu Taşıma Kanunu'nun 2. maddesinin 3. fıkrası, il sınırları içindeki ve 100 kilometreye kadar olan şehirlerarası taşımaların düzenlenmesinin, il ve ilçe trafik komisyonlarıyla iş birliği yapılarak valiliklere bırakılabileceğini, belediye sınırları içindeki şehir içi taşımaların ise belediyelere bırakılabileceğini hükme bağlamaktadır.

2918 sayılı Karayolları Trafik Kanunu'nun 12. maddesinin 1. fıkrasının (b) bendinin 1. alt bendinde, il ve ilçe trafik komisyonlarının görev ve yetkilerinden biri olarak, il sınırları içinde mahalli ihtiyaç ve şartlara göre trafik düzeni ve güvenliğini sağlamak amacıyla gerekli tedbirleri almak sayılmaktadır.

Öte yandan, 'akıllı ulaşım sistemleri' lafzının yer verildiği düzenlemeler de bulunmaktadır. Örneğin, 1 no'lu CBK'nin 474/1(a) maddesinde Ulaştırma ve Altyapı Bakanlığına "...akıllı ulaşım sistemleri...projelerinin geliştirilmesi, kurulması, kurdurulması, işletilmesi ve işlettilmesi hususlarında, ilgili kurum ve kuruluşlarla koordinasyon içerisinde, milli politika, strateji ve hedeflerin belirlenmesi amacıyla çalışmalar yapmak ve belirlenen hedefleri uygulamak" görevi verilmiştir. Yine CBK'nin 483. maddesiyle Haberleşme Genel Müdürlüğü'nün görev ve yetkilerinden biri de şu şekilde belirlenmiştir: "Akıllı ulaşım sistemlerine yönelik ulusal stratejileri, hedefleri, mimarileri, ulusal ölçekte uyulması gereken teknik kriterleri belirlemek, eylem planlarını hazırlamak ve izlemek, yenilikçi akıllı ulaşım sistemleri projeleri geliştirmek, kamu kurum ve kuruluşları, belediyeler, il özel idareleri, gerçek ve tüzel kişilerce akıllı ulaşım sistemleri kapsamında üretilen verilerin kullanılmasını ve değerlendirilmesini sağlamak amacıyla veri yönetim merkezi kurmak, kurdurmak, işletmek, işlettirmek, bu görevlerle ilgili uygulama usul ve esaslarını belirlemek".

Yine, Ulaşımında Enerji Verimliliğinin Artırılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 1. maddesinde "akıllı ulaşım sistemlerinin etkin uygulanması, sürdürülebilir şekilde ulaşım altyapılarının iyileştirilmesi" Yönetmelik'in amaçları arasında sayılmış ve başta Ulaştırma ve Altyapı Bakanlığı olmak üzere çeşitli kamu kurum ve kuruluşlarla iş birliği içerisinde AUS uygulamalarının gerçekleştirilmesi konusunda görevler ve yetkiler düzenlenmiştir⁴⁹⁷. Karayolları Genel

⁴⁹⁷ Örnek olarak şu hükümler verilebilir: **MADDE 4 – (1)** Bakanlık, ilgili Bakanlıklar ve Belediyelerce; yatay ve düşey trafik işaretlemeleri, elektronik yol yönlendirme ve denetleme sistemleri, seyahat talep yönetimi, trafiğin kontrol ve yönetimi, trafik bilgilendirme ve trafik sinyalizasyon sistemleri, ulaşım altyapılarının iyileştirilmesi ve planlanması, modlararası taşımacılık, toplu taşıma, yük taşımacılığı, akaryakıt tüketiminin izlenmesi ve çevre dostu araçların kullanılması hususlarında işbirliği sağlanarak ortak tedbirler alınır.

Müdürlüğü Görev, Yetki ve Sorumluluk Yönetmeliği'nin çeşitli maddelerinde de Genel Müdürlüğün sorumlu ve yetkili olduğu Devlet ve il yollarında AUS sistemlerinin kurulması ve işletilmesine ilişkin hükümlere yer verilmiştir⁴⁹⁸.

Yukarıda verilen kanuni düzenlemeler birlikte değerlendirildiğinde, çeşitli İdarelere trafiğin düzenlenmesi ve planlanması gibi genel bir yetkilendirme yapıldığı, bu bağlamda İdarelerin akıllı ulaşım sistemlerini kullanarak kişisel verileri işlemesine ilişkin hukuki yükümlülükleri bulunduğu söylenebilir. Büyükşehir belediyeleri ve belediyeler, ulaşım ve toplu taşıma hizmetlerini planlarken ve yürütürken, ayrıca il ve ilçe trafik komisyonları trafik düzeni ve güvenliğini sağlarken, akıllı ulaşım sistemleri kapsamında hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması şartına dayanarak kişisel verileri işleyebilecektir.

Yine, çıkarılan yönetmelikler ile de Ulaştırma ve Altyapı Bakanlığı, Karayolları Genel Müdürlüğü ve yerel yönetimlere, sorumlulukları dahilindeki sınırlar içerisinde ulaşımı daha hızlı, güvenli ve verimli kılmak için akıllı ulaşım sistemleri uygulamalarının gerçekleştirilmesi konusunda görev ve yetki verildiği görülmektedir. Dolayısıyla, söz konusu İdareler kendileri için belirlenen bu yükümlülükleri yerine getirebilmek için zorunluluk arz ettiği düzeyde kişisel veri işleme faaliyetinde bulunabilir. Şu kadar ki, mevcut kanun düzenlemelerinde AUS kapsamında açıkça özel nitelikli verilerin işlenmesini öngören bir hüküm bulunmadığından, söz gelimi sürücülerin biyometrik verilerinin

MADDE 7 – (1) Büyükşehir belediyeleri ve büyükşehir belediyesi sınırları dışındaki belediyelerden nüfusu yüz binin üzerinde olan belediyelerce kent içi toplu taşımaya yönelik aşağıdaki uygulamalar yapılır:

i) Özellikle nüfusun yoğun olduğu, trafik sıkışıklığının ve hava kirliliğinin olduğu bölgelerde kent içi ulaşım ağının bütününde yaya ve araç trafiğinin güvenli, akıcı ve etkin yönetilmesine yönelik önlemler alınır. Akıllı ulaşım sistemleri ile hareketlilik yönetimi desteklenir.

MADDE 16 – (1) Bakanlıkça, çağın gereklerine uygun olarak ulaşım ve iletişimde, etkin, hızlı, akıllı, güvenli ve entegre yönetim sisteminin kurulabilmesi için;

a) Belirli terminolojiye ve standartlara uygun olarak AUS mimarisi oluşturulur. AUS'un kamu yararı gözetilecek tarzda serbest, adil ve sürdürülebilir bir rekabet ortamında yapılmasına ilişkin politika, strateji, usul ve esaslar belirlenir.

b) Enerji verimliliğini sağlayacak çevre dostu AUS uygulamalarının geliştirilmesi ve kullanımı teşvik edilir.

c) AUS ile ulaşım elektronik ödeme sistemlerine ilişkin altyapı, şebeke, yazılım, donanım, hizmet gibi gerekli tüm yapıların ülke çapında entegre ve birlikte çalışabilirlik esaslarına göre kurulması, işletilmesi, yönetilmesi sağlanır.

ç) Elektronik ödeme ve araç tanımlama sistemlerinde, araçlara hızlı geçiş imkânı tanıyan ileri teknoloji ürünler tercih edilir.

d) Trafik yoğunluğu, araç tanımlama, akaryakıt tüketimi ve hava kirliliğinin izlenmesiyle ilgili verilerin toplanması, analiz edilmesi ve raporlanmasını sağlayacak AUS sistemlerin kurulması ve yaygınlaştırılması sağlanır.

⁴⁹⁸ **MADDE 14 –** (1) Trafik Güvenliği Dairesi Başkanlığının görevleri şunlardır:

m) Akıllı Ulaşım Sistemleri alanındaki gelişmeleri izlemek, uygun bulunan Akıllı Ulaşım Sistemlerini Devlet ve il yollarında tesis etmek, ettirmek, bakım ve işletmesini yapmak, yaptırmak, denetlemek.

n) Kurulumu ile görevli olduğu Akıllı Ulaşım Sistemleri ile ilgili standartları belirlemek, gerekli teknik dokümantasyonu hazırlamak, hazırlatmak.

o) Devlet ve il yollarında tesis edilecek Akıllı Ulaşım Sistemlerinin ihtiyacı olan enerji ve haberleşme altyapısını tesis etmek, ettirmek.

MADDE 25 – (1) Bilgi Teknolojileri Dairesi Başkanlığının görevleri şunlardır:

ğ) Genel Müdürlüğün görev alanındaki karayolları ağında hizmetin gerektirdiği haberleşme altyapısını kurmak ve ilgili birimlerle koordineli olarak akıllı ulaşım sistemleri kurulması ve kullanılarak çalışmaları yapmak.

toplanmasını gerektiren bir uygulamanın hayata geçirilmesi ilgililerin açık rızası alınmadığı müddetçe şu an için mümkün değildir.

Bununla birlikte, yukarıda ayrıntılarıyla ifade edildiği üzere⁴⁹⁹, 6698 sayılı Kanunun 5. maddesinde veri işleme şartlarından biri olarak belirlenen “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartındaki ‘hukuki yükümlülüklerin’ CBK ile getirilemeyeceği düşünüldüğünde, Haberleşme Genel Müdürlüğü tarafından akıllı ulaşım sistemleri kapsamında üretilen verilerin kullanılması ve değerlendirilmesini sağlamak üzere veri yönetimi merkezi kurulmasını ve işletilmesini öngören CBK hükmünün Anayasa’ya aykırı olduğu kabul edilmelidir. Nitekim veri yönetimi merkezi ile AUS bileşenleri aracılığıyla toplanan büyük verinin bu merkezde işlenmesi ve diğer paydaşlarla paylaşılması eylemleri gerçekleştirileceği düşünüldüğünde, kişisel verilerin korunması hakkını sınırlandıran bir niteliği haiz bu faaliyetin yasayla düzenlenmesi gerekir.

AUS uygulamaları aracılığıyla İdarenin veri işlemesine imkân veren çeşitli yükümlülüklerin yasalarda ya da bunlara uygun olarak çıkarılan yönetmeliklerde öngörülmesi nedeniyle veri işlenebileceği söylenebilir de AUS uygulamaları özelinde paydaşların sorumluluklarını, veri işleme yöntemlerini ve bu verilerin korunması, tutulma süresi, anonimleştirilmesi ya da silinmesine ilişkin usul ve esasları belirleyen ayrı bir kanun çıkarılması, kişisel verilerin korunması hakkına ilişkin düzenlemenin kanunla yapılabileceğini öngören Anayasanın 20/3 maddesine de uygunluk sağlanmış olur. Bununla birlikte, veri işlemenin KVKK’da belirlenen diğer kurallar çerçevesinde ve genel ilkelere uygun olarak gerçekleştirilmesi gerektiği belirtilmelidir. Akıllı ulaşım sistemlerinin tatbik edildiği yerlerde trafikte bulunan sürücü ve yayaların birçok kişisel verisi işlenebileceğinden, İdarenin özellikle veri minimizasyonu, şeffaflık ve belirli, açık ve meşru amaçlar için veri işleme ilkelerine uygun şekilde hareket etmesi gerekir. Aksi halde işlenen verilerle bir gözetim toplumunun yaratılması tehlikesi ortaya çıkabilir.

Nitekim, akıllı ulaşım sistemlerine ilişkin düzenleme olan 2010/40/AB sayılı Direktifin⁵⁰⁰ akıllı ulaşım sistemlerinde kişisel verilerin işlenmesine ilişkin kuralları düzenleyen 10. maddesine göre, kişisel veriler yalnızca karayolu emniyeti, güvenliği ve trafik yönetimi gibi belirli amaçlarla ve gerekli olduğu ölçüde işlenebilir. Kişisel verilerin işlenmesini gerektiren durumlarda, kabul edilen isterler veri kategorilerini belirlemeli ve uygun veri koruma güvencelerini sağlamalıdır. Ayrıca, bu durumlarda yapılacak etki değerlendirmesi, veri işlemenin kişisel verilerin korunması üzerindeki etkisini analiz etmelidir. Direktif, kişisel verilerin korunması bakımından anonimleştirme ve takma adlandırma yöntemlerine de vurgu yapmaktadır. Teknik olarak mümkün olduğu ve veri işleme amaçlarına

⁴⁹⁹ “5.4.1.2.4. Veri Sorumlusunun Hukuki Yükümlülükleri Gereği Kişisel Verilerin İşlenmesi” başlığı.

⁵⁰⁰ Akıllı Ulaşım Sistemlerinin karayolu ulaşımı alanında kullanılması ve diğer ulaşım modları ile ara yüzlere ilişkin çerçeve hakkında 2010/40/AB sayılı Direktif. Mezkûr düzenleme, Avrupa Parlamentosu ve Konseyi’nin 22 Kasım 2023 Tarihli ve 2023/2661/AB sayılı Direktifi ile değiştirilmiştir. Düzenlemenin güncel metni için bkz.: <http://data.europa.eu/eli/dir/2010/40/2023-12-20> (E.T. 7.8.2024).

ulaşılabildiği sürece, anonimleştirilmiş veriler tercih edilmelidir. Anonimleştirmenin mümkün olmadığı durumlarda ise takma adlandırma yöntemi kullanılmalıdır.

Sonuç olarak, akıllı ulaşım sistemleri, trafik yönetimi, güvenlik ve enerji verimliliği gibi alanlarda önemli kamu yararı sağlar. Ancak bu yarar, bireylerin temel haklarından olan kişisel veri mahremiyetini ihlal etmemelidir. Bu iki değer arasında optimal bir denge kurulmalıdır. Bunu sağlamak için, işlenen kişisel verilerin kapsamı, AUS amaçlarıyla orantılı olmalı, aşırı veri toplanmamalıdır. Ayrıca, İdare, veri toplama ve bunları kullanma süreçlerinde şeffaf ve hesap verebilir olmalı ve böylece vatandaşların sisteme olan güvenini artırmalı, sistemin etkinliğine katkı sunmalıdır.

2.2. Kolluk Faaliyetlerinde Kişisel Verilerin İşlenmesi

Kolluk faaliyetleri, kamu düzeninin sağlanması ve korunması amacıyla gerçekleştirilen ve kişisel verilerin yoğun olarak işlendiği bir diğer idari faaliyet alanıdır. Kamu düzeninin klasik unsurları olan genel sağlık, kamu güvenliği ile dirlik ve esenlik kapsamında yürütülen kolluk faaliyetlerinde, teknolojik gelişmelerin de etkisiyle, kişisel verilerin toplanması ve işlenmesi giderek artmaktadır. Bu başlık altında, kolluk faaliyetlerinde kişisel verilerin işlenmesine ilişkin seçili örnekler incelenecektir. Bu örnekler, kolluk faaliyetlerinin tüm alanlarını kapsamamakla birlikte, kamu düzeninin üç temel klasik unsuruna ilişkin alanlardaki veri işleme pratiklerini temsil eder niteliktedir. Kolluk faaliyetlerinde kişisel verilerin işlenmesi, temel hak ve özgürlüklerin korunması ile kamu düzeninin sağlanması arasındaki hassas dengenin kurulması bakımından kritik öneme sahiptir.

2.2.1. Genel Sağlığın Korunmasında Veri İşleme

2.2.1.1. Genel Olarak

Kamu düzeninin bir unsuru olarak genel sağlık, toplumun tamamını ilgilendiren ve kolektif nitelik taşıyan bir kavramdır. Burada amaç, bireysel tedavi hizmetlerinden ziyade, toplum sağlığının bir bütün olarak korunması ve geliştirilmesidir⁵⁰¹. Bu kavram, salgın hastalıklarla mücadele, çevre sağlığı, gıda güvenliği, bulaşıcı hastalıklarla mücadele gibi toplumun genelini etkileyen konuları kapsar⁵⁰². Öte yandan, kamu hizmeti olarak sağlık hizmeti daha çok bireysel düzeyde sunulan, kişilerin tek tek sağlık sorunlarının teşhis ve tedavisine yönelik hizmetleri ifade eder. Kamu hizmeti olarak sağlık hizmeti ise daha çok tedavi edici sağlık hizmetlerine odaklanır ve bireysel başvuru esasına dayanır. Hastanelerde

⁵⁰¹ DURAN, **İdare Hukuku Ders Notları**, s. 255; Ramazan ÇAĞLAYAN, **İdare Hukuku Dersleri**, Adalet Yayınları, 12. Baskı, 2024, s.275.

⁵⁰² Sebahattin NAÇAR, “Kamu Düzeninin Unsuru Olarak Genel Sağlığın Korunması”, **Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü**, Yüksek Lisans Tezi, 2023, s.61.

sunulan poliklinik hizmetleri, ameliyatlar, rehabilitasyon hizmetleri bu kapsamda değerlendirilir. Bu hizmetlerde kişiselleştirilmiş tedavi ve bakım ön plandadır.

Genel sağlık kavramının ayırt edici özelliği, koruyucu ve önleyici niteliğinin ön planda olmasıdır. Bu kapsamda devlet, toplumsal düzeyde sağlık tehditlerini öngörmek, bunlara karşı önlem almak ve gerektiğinde müdahale etmek zorundadır. Örneğin, aşılama kampanyaları, salgın hastalıklarla mücadele programları, halk sağlığı taramaları gibi faaliyetler genel sağlık kapsamında değerlendirilir. Bu faaliyetler, bireylerin sağlık durumlarından bağımsız olarak, toplumun tamamının sağlığını korumaya yönelik kolektif bir amaca hizmet eder.

Genel sağlığın korunması amacıyla yürütülen kolluk faaliyetlerinde, farklı nitelikteki kişisel verilerin işlenmesi söz konusu olabilmektedir. Bu veriler yalnızca sağlık verileriyle sınırlı olmayıp, idari kolluk faaliyetinin amacına ve niteliğine göre çeşitlilik gösterebilmektedir. Örneğin salgın hastalıklarla mücadelede kişinin kimlik bilgileri, ikamet adresi, seyahat geçmişi ve temaslı olduğu kişilere ilişkin bilgiler işlenebilmektedir. Benzer şekilde gıda güvenliği denetimlerinde işletme sahipleri ve çalışanların kimlik bilgileri yanında, sağlık raporları ve portör muayene sonuçları gibi özel nitelikli kişisel veriler de işlenebilmektedir. Çevre sağlığının korunması amacıyla yapılan denetimlerde tesis sahiplerinin kimlik bilgileri, işletme ruhsat bilgileri ve daha önce uygulanan idari yaptırımlara ilişkin kayıtlar tutulabilmektedir. Umumi yerlerin denetiminde ise işletme sahiplerinin kimlik bilgileri ve çalışanlara ait sağlık tarama sonuçları gibi veriler işlenebilmektedir. Bu noktada önemle belirtmek gerekir ki, kolluk faaliyetleri kapsamında işlenen verilerin bir kısmı özel nitelikli kişisel veri kategorisinde yer alırken, bir kısmı genel nitelikli kişisel veri kategorisindedir. Bu nedenle veri işleme faaliyetinin hukuki dayanağı belirlenirken, işlenen verinin niteliğine göre Kişisel Verilerin Korunması Kanunu'nun farklı hükümlerinin uygulanması gerekmektedir. Öte yandan, yine Kanunun 28/1-ç maddesi de özellikle kolluk faaliyetleri bağlamında işlenecek verileri Kanun kapsamı dışında tutması nedeniyle önemlidir⁵⁰³. İlgili madde uyarınca, yetkili kamu kurum ve kuruluşları tarafından, kamu düzenin korumak maksadıyla önleyici ve koruyucu faaliyetler kapsamında işlenen kişisel veriler KVKK kapsamı dışında kabul edilmiştir. Elbette bu durum, ilgili kişisel verilerin, kanunilik ve ölçülülük ilkeleri gibi temel hak ve özgürlüklerin sınırlandırılmasına yönelik korumadan muaf tutulduğu anlamına gelmemektedir⁵⁰⁴.

KVKK'nın 6. maddesinde düzenlenen özel nitelikli veri işleme şartları arasında, kamu sağlığının korunması ve koruyucu hekimlik amacıyla işlenen kişisel sağlık verilerine de yer verilmiştir. Kamu sağlığı kavramı “*Kamu sağlığı çevrenin temizliği, enfeksiyonların kontrolü, kişisel temizlik kuralları hakkında bireyin eğitimi, hastalığın erken teşhisi ve önleyici tedavisi için tıbbi hizmetler ve*

⁵⁰³ 6698 sayılı Kanun, m.28/1- Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

⁵⁰⁴ Ayrıntılı bilgi için bkz.: “3.1. Tamamen Kanun Kapsamı Dışında Tutulan Haller”

*bakım hizmetlerinin organizasyonu ile toplumdaki her bireyin sağlığının korunmasına yeterli bir hayat standardını temin edecek sosyal mekanizmanın geliştirilmesi için gösterilecek organize bir toplum gayreti aracılığıyla hastalığın önlenmesi, hayat süresinin uzatılması ve fiziksel sağlık ve verimliliğin geliştirilmesi bilimi ve sanatıdır”*⁵⁰⁵ şeklinde tanımlanmaktadır. Bu bağlamda kamu sağlığının korunması idarenin kamu düzenini sağlamak amacıyla sürdürdüğü kolluk faaliyetlerinin bir parçasını oluşturan genel sağlığın korunması amacını taşımaktadır.

Koruyucu hekimlik, adından da anlaşılacağı üzere, özellikle hastalıkların oluşmasından önce alınacak önlemlere ilişkin bir kavramdır. Hastalıkların tedavi edilmesinden ziyade bunların oluşumunun önlenmesi adına gerekli önlemlerin alınması, salgın ve bulaşıcı hastalıklarla mücadele, hasta yakınlarının bilgilendirilmesi, hastalığın ortaya çıkmasına sebep olabilecek çevre, su ve gürültü kirliliği gibi etmenlerin azaltılması, doğru beslenme ve hayat tarzının benimsenmesi için verilecek eğitimler koruyucu sağlık hizmetleri alanında gerçekleştirilen faaliyetlerdir⁵⁰⁶.

Örneğin, Sağlık Bakanlığı tarafından yayımlanan “Doğum Öncesi Bakım Yönetim Rehberi” adlı kitapçıkta gebe kadınlara en az 4 izlem yapılması planlanmış, bu izlemlerin ilkinde gebeye ait kişisel verilerin kayıt altına alınması öngörülmüştür. Kayıt altına alınacak bilgiler arasında akraba evliliği/derecesi, kalıtsal hastalıklarının varlığı, madde bağımlılığı, kronik hastalıklar, cinsel yolla bulaşan hastalıklar, geçirilmiş operasyonlar, sürekli kullanmak zorunda olduğu ilaçlar gibi bilgilere de yer verilmiştir. Ayrıca İstanbul İl Sağlık Müdürlüğü tarafından 2008 yılında kurulan “Gebe, Lohusa, Bebek ve Çocuk İzlem Sistemi (GEBLİZ)” ile İstanbul’da bulunan kamu ve özel tüm sağlık kuruluşlarınca gebe, lohusa, bebek ve çocuk tespit ve izlemlerinin bu sisteme kaydı yapılmaktadır. Yapılan kayıt sadece ilgili adresten sorumlu aile sağlığı merkezinin GEBLİZ sayfasında görünmekte ve ilgili kişiyle iletişime geçilerek koruyucu sağlık hizmetlerine ulaşması sağlanmaktadır⁵⁰⁷. Bu bağlamda örneğin, gebelik testi pozitif çıkan bir hastanın bilgilerinin görevli kişi tarafından sisteme kaydedilmesi koruyucu hekimlik amacıyla gerçekleştirildiğinden hukuka uygun kabul edilecektir.

Ancak, uygulamanın 6698 sayılı Kanunu ihlal eden sonuçlar doğurması mümkündür. Örneğin, gebelik testi pozitif çıkan bir kişiye aile hekimliği tarafından “Tebrikler, hamilelik testiniz pozitif çıktı. En kısa zamanda aile hekimine gidiniz” şeklindeki mesaj sistemde telefon numarası kayıtlı bulunan

⁵⁰⁵ Charles-Edward Amory WINSLOW, “The Untilled Fields of Public Health”, *Science*, C.LI, No: 1306, 1920, s. 30, aktaran: Hamza Demir, **Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, On İki Levha, Nisan 2020, s. 62.

⁵⁰⁶ Nuri Mehmet BASAN, Nazmi BİLİR, “Koruyucu Sağlık Hizmetlerinde Önleme Çelişkisi ve Nedenleri”, **TAFF Preventive Medicine Bulletin**, C. XV, No: 1, 2016, s. 45. <https://www.bibliomed.org/mnsfulltext/1/1-1427871712.pdf?1655285484> (Erişim Tarihi: 15.6.2022)

⁵⁰⁷ Savaş Başar KARTAL ve diğerleri, “İstanbul’da Gebe, Lohusa, Bebek ve Çocuk İzlemlerinin İyileştirilmesi: GEBLİZ”, **TAF Preventive Medicine Bulletin**, C. 9, S. 4, 2010, s. 291. https://www.bibliomed.org/mnsfulltext/1/khb_009_04-289.pdf?1655291380 (Erişim Tarihi: 15.6.2022)

ilgilinin babasına gönderilmiştir⁵⁰⁸. Yine gebe takibi için aile hekimlerinin ev ziyaretine gitmekle görevlendirilmesi gebe olduğunu ailesinden saklayan kişilerin can güvenliğinin dahi tehlikeye girmesine sebebiyet vermiştir. Sisteme sonradan eklenen “mahremiyet butonu” ile gebe takibi istemeyenler için buna imkân tanınmış olsa da ilgililerin sisteme kayıt işlemlerine devam edilmektedir. Ancak gebe takibi için ilgiliye ulaşılamaması halinde aile üyelerinin aranması örnekleri sıkça yaşandığından gebe takibi istemeyen kişiler dahil birçok insanın kişisel sağlık verilerinin hukuka aykırı şekilde işlenmesinden endişe duymasına sebep olmaktadır. Dolayısıyla, örneklerde olduğu gibi sağlık verilerinin ilgisiz kişilerle paylaşımı, ilgililer dışındakilerin eline geçmesi ve farklı amaçlar için kullanılmasının önüne geçilmesi için veri güvenliğinin sağlanması yönünde önlemler alınması gerektiği belirtilmelidir.

Kamu düzeninin önemli bir unsuru olan genel sağlığın korunması için yürütülen kolluk faaliyetlerinde, salgın hastalıklarla mücadele özel bir öneme sahiptir. Zira salgın hastalıklar, toplum sağlığını doğrudan tehdit eden ve hızlı yayılma potansiyeli nedeniyle acil müdahale gerektiren durumlardır. Bu kapsamda yakın tarihte yaşanan COVID-19 salgını, genel sağlığın korunması amacıyla yürütülen kolluk faaliyetlerinde kişisel verilerin işlenmesi konusunda önemli bir örnek teşkil etmektedir. Salgınla mücadele sürecinde, bir yandan toplum sağlığının korunması için gerekli önlemler alınırken, diğer yandan kişisel verilerin korunması hakkına yönelik müdahalelerin hukuka uygunluğu tartışma konusu olmuştur. Bu nedenle, aşağıda özellikle Covid-19 salgını özelinde kişisel verilerin işlenmesine ilişkin hukuki çerçeve ayrıntılı olarak incelenecektir.

2.2.1.2. Salgın Hastalık Dönemlerinde Kişisel Sağlık Verilerinin İşlenmesi

Salgın hastalıklarla mücadele sürecinde, hastalığın yayılmasını önlemek ve toplum sağlığını korumak amacıyla çeşitli kişisel verilerin işlenmesi kaçınılmaz hale gelmektedir. Bu süreçte bir yandan hastalığın tespiti ve takibi için sağlık verileri işlenirken, diğer yandan hastalığın yayılmasını önlemek için kişilerin seyahat bilgileri, temaslı oldukları kişiler, bulundukları mekanlar gibi özel yaşama ilişkin veriler de toplanmaktadır. Hastalığın toplum sağlığı üzerindeki ciddi tehdidi karşısında, kişisel verilerin geniş ölçekte işlenmesi zorunlu olmakla birlikte, bu işleminin hukuka uygun bir şekilde gerçekleştirilmesi ve toplanan verilerin amacı dışında kullanılmaması büyük önem taşımaktadır. Nitekim salgın hastalıklarla mücadele döneminde, kişisel verilerin korunması hakkına yönelik müdahalelerin ölçülü olması, temel hak ve özgürlüklerin özüne dokunulmaması gerekmektedir.

Salgın hastalık dönemlerinde yaşanan panik havası kişisel verilerin işlenmesine ilişkin kuralların ikinci plana atılabileceği izlenimini verse de yaşanabilecek mağduriyetlerin en aza indirilmesi bakımından bu gibi durumlarda da veri işleminin önceden belirlenmiş kurallar çerçevesinde yapılması

⁵⁰⁸ “Tebrikler kızınız hamile”, <https://www.haberturk.com/ekonomi/makro-ekonomi/haber/753536-tebrikler-kiziniz-hamile>, 25.6.2012. (Erişim Tarihi: 15.6.2022)

gerekir. Özellikle panik ve aciliyet anlarında insanlara “Hayatta kalmak mı yoksa özel hayatın gizliliği mi?” gibi bir soru sorulduğunda elbette toplum hayatta kalmayı tercih etmekte ve yaşanan veri işleme ihlallerine kayıtsız kalabilmektedir⁵⁰⁹. Ancak, kimi zaman fedakarlıkta bulunmak gerekse de özel hayatın gizliliğini koruyarak da hayatta kalınması mümkündür. Bunun için veri işleme faaliyetlerinin kuralına uygun olarak yapılması ve gerekli önlemlerin alınması icap eder.

İdare salgın hastalıkların ortaya çıktığı dönemlerde, ilgililerin sağlığının ve salgın hastalıklarda temas ettikleri insanların takibi, karantina uygulaması, kamu sağlığı ve sosyal yardım hizmetleri politikalarının belirlenmesi gibi amaçlarla veri işleyebilmektedir. İdare bu verileri e-Nabız, Halk Sağlığı Yönetim Sistemi (HSYS), Aile Hekimliği Sistemi ya da Covid-19 küresel salgını ile mücadele döneminde Sağlık Bakanlığınca çıkarılan Hayat Eve Sığar (HES) mobil uygulaması gibi farklı araçlarla işleyebilmektedir. Örneğin, Covid-19 salgını döneminde, PCR testi pozitif çıkan kişiye ait bilgiler önce ilçe sağlık müdürlüğünün filyasyon yapılacak kişiler listesine kayıt edilmiş, herhangi bir hastanede tedavi altına alınıp alınmadığı kontrol edildikten sonra ilaç tedavisine başlanmadıysa ilgisine teslim edilmek üzere ilaçları filyasyon ekiplerine teslim edilmiş, filyasyon ekibi ilgilinin temaslı olduğu kişilerin bilgisini kendisinden alarak bu kişilerle iletişime geçmiş, tespit edilen temaslılardan semptom gösterenler hastaneye yönlendirilmiştir⁵¹⁰. Üstelik, ilgililerin sağlık verileri dahil kayıt altına alınan diğer kişisel verileri kamu sağlığının korunması ve salgının yayılmasını önlemek amacıyla İçişleri Bakanlığı ve kolluk kuvvetleri ile de paylaşarak karantina uygulamasının devam edilmesine çalışılmıştır⁵¹¹.

Covid-19 salgınındaki örnekten de anlaşıldığı üzere, olağan durum dışına çıkıldığında, etkili ve hızlı çözüm almak amacıyla İdare veri paylaşımı konusunda oldukça cüretkâr davranabilmektedir. Ancak, bu davranışın biçiminin öncelikle yasal dayanakları bulunmalıdır. Dahası, yasalarla getirilen kuralların Anayasa’ya, bilhassa 13. maddesindeki temel hak ve özgürlüklerin sınırlandırılması kuralına, uygun olması gerekir.

6698 sayılı KVKK’nun özel nitelikli verilerin işlenmesine ilişkin 6. madde hükmü 7499 sayılı Kanunun 33. maddesiyle 2 Mart 2024’te değiştirilmiştir. Değişiklik öncesindeki hükümler afet veya

⁵⁰⁹ KÜZECİ, bu tür soruların yanıtıcı olduğunu, çünkü bir tarafa yaşamsal bir gereklilik (yaşam veya güvenlik) koyulduğunda, diğer seçeneğin (mahremiyet veya özgürlük) otomatik olarak daha az önemli görüldüğünü ifade etmektedir. Yazar, bu sorunun temelden yanlış olduğunu, bu ikisi arasında gerçek bir çelişki olmadığını, aksine birbirini desteklediğini ve beslediğini, bu bağlamda kişilerin güven duydukları ortamlarda özgürce yaşayabildiklerini ve özgür oldukları yerlerde güvenli bir sistem kurabildiklerini belirterek, özgürlük ve güvenlik arasında bir birliktelik olduğunu vurgulamaktadır. Elif KÜZECİ, “Covid-19 Pandemisinde Kişisel Verilerin Korunması”, **Kişisel Sağlık Verileri 4. Ulusal Kongresi**, 24-25 Ekim 2020, Webinar, İstanbul Türk Tabipler Birliği Yayınları, Nisan 2021, s. 145.

⁵¹⁰ Suat Hayri KÜÇÜK, “Covid-19 Pandemisinde Kişisel Sağlık Verilerinde Laboratuvar Çalışmaları ve Kullanımı”, **Kişisel Sağlık Verileri 4. Ulusal Kongresi**, 24-25 Ekim 2020, Webinar, İstanbul Türk Tabipler Birliği Yayınları, Nisan 2021, s.133.

⁵¹¹ “Hayat Eve Sığar uygulamasındaki veriler kolluk kuvvetleriyle paylaşıyor”, 18.5.2020, Siber Bülten, <https://siberbulten.com/sektorel/trky/hayat-eve-sigar-uygulamasindaki-veriler-kolluk-kuvvetleriyle-paylasiliyor/> (E.T. 20.7.2024).

salgın hastalık dönemlerinde sağlık verilerinin işlenmesini önemli derecede kısıtlamaktaydı. Nitekim, sağlık ve cinsel hayata ilişkin verilerin ilgilinin açık rızası dışında, kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, yalnızca sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebileceği öngörülmüştü. Bu düzenleme, sır saklama yükümlülüğü altında bulunan Sağlık Bakanlığı çalışanlarının sağlık verisi işleyebilmesi için yeterli kabul edilebilirse de Covid-19 sürecinde olduğu gibi bu verilerin İçişleri Bakanlığı ve benzeri kurumlar tarafından da işlenmesine imkân vermiyordu.

KVKK'nun 6. maddesinde yapılan değişiklikle, afet ve salgın hastalık dönemlerinde de veri işlemeyi kolaylaştıracak kurallar getirilmiştir. İkinci fıkrada belirlenen şartlar çerçevesinde özel nitelikli verilerin, eski düzenlemedeki veri işleme şartına ek olarak kanunlarda açıkça öngörülmesi, fiili imkânsızlık hallerinde ilgilinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, ilgilinin kendisince alenileştirilmiş olması ve sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması şartlarından birine dayanılarak işlenmesi mümkündür.

Öte yandan, özel nitelikli verilerin işlenmesine ilişkin 6. maddenin gerek eski gerekse de getirilen yeni işleme şartları arasında salgın hastalık gibi kamu düzeni ve kamu sağlığının bozulma tehlikesiyle karşı karşıya kalındığı ya da bozulan düzenin yeniden eski hale getirilmesi gerektiği durumlara yönelik sağlık çalışanları dışında farklı kamu kurumlarının sağlık ve diğer özel nitelikli verileri işleyebilmesine yönelik hükümler öngörülmemiştir. Ancak, böyle zamanlarda özellikle sağlık verilerinin işlenebilmesi önemli bir gerekliliktir. İşte bu gibi durumlarda KVKK'nun 28. maddesinin ilk fıkrasının (ç) bendi gereği KVKK'nun uygulanmayacağı öngörülmüştür. İlgili maddeye göre, kişisel verilerin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliğini sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinde bu Kanun hükümleri uygulanmayacaktır.

Covid-19 ile mücadele sürecinde Kişisel Verileri Koruma Kurumu tarafından yapılan kamuoyu duyurusunda da bu maddeye atıf yapılarak, Covid-19 küresel salgının kamu güvenliğini ve kamu düzenini tehdit etmesi nedeniyle kişisel verilerin Sağlık Bakanlığı ve madde kapsamına giren diğer kamu kurum ve kuruluşlarınca işlenmesinin önünde bir engel bulunmadığı ifade edilmiştir⁵¹². Dolayısıyla, kamu güvenliği ve kamu düzenini tehdit eden doğal afet ve salgın hastalık durumlarında söz konusu hüküm gereğince kamu güvenliğini ve kamu düzenini korumak ya da bozulan düzeni

⁵¹² “Kamuoyu Duyurusu”, Kişisel Verileri Koruma Kurumu, 27.3.2020, [\(https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-\(E.T. 20.7.2024\)\)](https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-(E.T. 20.7.2024)).

yeniden sağlamak amacıyla sınırlı olmak şartıyla başta Sağlık Bakanlığı olmak üzere diğer kamu kurum ve kuruluşlarınca işlenecek kişisel verilere ilişkin 6698 sayılı Kanunun uygulanmayacağı söylenebilir. Bu bağlamda, örneğin salgın hastalıkların yayılmasının önlenmesi için tecrit altında bulunan hasta veya hasta olma potansiyeli bulunan kişilerin bu durumuna ilişkin sağlık verilerinin kamu düzenini sağlamakla görevli emniyet güçleriyle paylaşılması KVKK'nun kurallarına tabi olmayacaktır.

Ancak, Kurum tarafından yapılan bir başka duyuruda da belirtildiği üzere⁵¹³, ilgili hüküm, Covid-19 salgını kapsamında yürütülen kamu güvenliği ve kamu düzenini koruma amacına yönelik faaliyetlerle sınırlı olarak uygulama bulacaktır. Bu amacın aşan ya da bunun dışında kalan nitelikteki veri işleme faaliyetlerinin KVKK kapsamında kalacağı kabul edilmelidir.

Türk hukukunda kişisel verilerin korunmasına ilişkin bu düzenlemeler, uluslararası hukuk normları ile paralellik göstermektedir. Özellikle GDPR ve AİHS gibi uluslararası metinler, kişisel verilerin korunması ile kamu güvenliği ve sağlığı arasındaki hassas dengeyi gözetmektedir. Bu bağlamda, GDPR'ın özel nitelikli veri işleme kurallarının ve AİHS'nin özel hayatın gizliliğine ilişkin hükümlerinin, Türk hukukundaki düzenlemelere ışık tuttuğu söylenebilir.

GDPR, özel nitelikli veri olarak kabul edilen sağlık verilerinin işlenmesi için ilgisinin açık rızasının alınması dışında kamu yararını esas alan özel bir işleme şartını da içermektedir. Tüzüğün 9. maddesinin 2. fıkrasının (i) bendi, kamu sağlığını ilgilendiren ciddi sınır ötesi tehditler gibi durumlarda, kamu yararı gerekçesiyle sağlık verilerinin işlenebileceğini öngörmektedir. Ancak bu işleme, AB veya üye devlet hukukunda özel bir düzenleme bulunması ve veri sahiplerinin hak ve özgürlüklerini koruyucu uygun önlemlerin alınması şartına bağlanmıştır. GDPR'ın 46 numaralı gerekçesinde, salgın hastalıkların izlenmesi ve yayılmasının önlenmesi gibi durumların hem kamu yararına hem de bireylerin hayati çıkarlarına hizmet edebileceği belirtilmiştir. Ayrıca, 52 numaralı gerekçesinde de bulaşıcı hastalıkların önlenmesi veya kontrolü amacıyla özel nitelikli kişisel verilerin istisnai olarak işlenebileceği vurgulanmıştır.

Öte yandan, Covid-19 döneminde birçok ülkede vatandaşları bilgilendirmek ve semptomları olan kişilerin tıbbi takibini kolaylaştırmak, enfeksiyon zincirlerini kesmek için enfekte bir kişiye yakın olan kişileri uyarmak, enfekte kişilerin karantinasının izlenmesi ve uygulanması gibi amaçlarla mobil uygulamalar kullanıma sunulmuştur. Avrupa Birliği, Covid-19 kriziyle mücadelede teknoloji ve veri kullanımına ilişkin ortak bir yaklaşım benimsemek amacıyla 8 Nisan 2020 tarihinde 2020/518 sayılı Komisyon Tavsiyesi'ni yayımlamıştır⁵¹⁴. Bu tavsiye, özellikle mobil uygulamaların kullanımı ve

⁵¹³ Kişisel Verileri Koruma Kurumu, Covid-19 PCR Test Sonucu ve Aşı Bilgisi Uygulamalarına İlişkin Kamuoyu Duyurusu, 28.9.2021, <https://www.kvkk.gov.tr/Icerik/7055/COVID-19-PCR-TEST-SONUCU-VE-ASI-BILGISI-UYGULAMALARINA-ILISKIN-KAMUOYU-DUYURUSU> (E.T. 26.5.2024).

⁵¹⁴ Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised

anonimleştirilmiş hareketlilik verilerinin işlenmesi konularında üye devletlere rehberlik etmeyi amaçlamıştır.

Tavsiye, kişisel verilerin korunması ve temel hakların gözetilmesi ilkelerini ön planda tutmaktadır. Üye devletlerin, sağlık verilerinin işlenmesine izin veren özel mevzuatlar getirirken, veri işleme amaçlarının ve araçlarının açık ve belirli olmasını sağlamaları gerektiği vurgulanmıştır. Bu bağlamda, veri minimizasyonu ilkesine uygun olarak, kamu sağlık otoriteleri ve araştırma kuruluşlarının kişisel verileri yalnızca gerekli olanla sınırlı tutmaları ve uygun güvenlik önlemlerini uygulamaları önem taşımaktadır.

Tavsiye, temel hak ve özgürlüklere getirilen kısıtlamaların demokratik bir toplumda gerekli, uygun ve orantılı olması gerektiğini vurgulamaktadır. Bu kısıtlamaların geçici nitelikte olması ve kriz sona erdikten sonra devam etmemesi gerektiği belirtilmiştir. Ayrıca, verilerin işlenmesinde şeffaflık ilkesinin gözetilmesi ve kamuoyunun düzenli olarak bilgilendirilmesi önemle vurgulanmıştır.

Mobil uygulamaların kullanımında, gizlilik ve veri koruma ilkelerine uyulması gerektiği belirtilmiştir. Özellikle, kişisel verilerin COVID-19 kriziyle mücadele amaçları dışında kullanılmaması, verilerin işlenmesine yönelik ihtiyacın düzenli olarak gözden geçirilmesi ve gerekli olmadığı durumlarda verilerin imha edilmesi gerektiği vurgulanmıştır. Uygulamaların tasarımında, temel haklara saygı gösterilmesi ve damgalanmanın önlenmesi için güvencelerin sağlanması önemle belirtilmiştir.

Tavsiye, mobil uygulamaların teknik özelliklerine de değinmektedir. Yakınlık verilerinin kullanılması ve kişilerin konum verilerinin işlenmesinden mümkün olduğunca kaçınılması, bunun yerine anonimleştirilmiş ve toplu verilerin tercih edilmesi önerilmektedir. Bluetooth Düşük Enerji gibi uygun teknolojilerin kullanılması, verilerin cihazda depolanması ve güvenliğinin sağlanması gibi teknik gereksinimlere de yer verilmiştir.

Siber güvenlik ve veri güvenliği konuları da tavsiyede önemli bir yer tutmaktadır. Verilerin erişilebilirliğini, gerçekliğini, bütünlüğünü ve gizliliğini korumak için etkili önlemlerin alınması gerektiği vurgulanmıştır. Ayrıca, alınan tedbirlerin sona ermesi ve elde edilen kişisel verilerin en geç salgının kontrol altına alındığının ilan edilmesiyle silinmesi gerektiği belirtilmiştir.

Tavsiye, uygulamaların şeffaflığına ve kamuoyu güvenine de önem vermektedir. Gizlilik ayarlarında şeffaflık sağlanması ve uygulamalara olan güvenin artırılması için gerekli adımların atılması önerilmektedir. Ayrıca, enfekte kişilerle yakın temasta bulunanların anonim kalacak şekilde uyarılması için uygun yöntemlerin geliştirilmesi gerektiği vurgulanmıştır.

AİHM ise sağlık verilerinin korunması hususunu AİHS'nin özel ve aile hayatına saygı hakkı başlıklı 8. maddesi bağlamında incelemektedir⁵¹⁵. Bu maddenin ilk fıkrasında herkesin özel ve aile hayatına saygı gösterilmesi hakkına sahip olduğu belirtildikten sonra ikinci fıkrasında bu hakka kamu makamlarınca müdahale edilebilmesinin şartları belirlenmiştir. Buna göre müdahale yalnızca yasalarda öngörülmesi, demokratik bir toplumda ulusal güvenlik, kamu güvenliği, düzenin korunması, sağlığın veya başkalarının hak ve özgürlüklerinin korunması gibi amaçlar için gerekli olması durumunda hukuka uygun kabul edilecektir. Dolayısıyla, salgın hastalıkların doğurduğu ihtiyaçlar nedeniyle kamu düzeninin sağlanması için sağlık verilerinin korunması hakkına müdahalede bulunulması, maddede belirlenen şartlara uyulması halinde, mümkündür.

AİHM'nin Doğrudan salgın hastalıklara ilişkin olarak verdiği kararları bulunmamakla birlikte, kişisel sağlık verilerinin korunması ve işlenmesiyle ilgili bazı önemli kararları bulunmaktadır⁵¹⁶. AİHM'nin Z. v. Finlandiya davasında verdiği karar, sağlık verilerinin korunması ve özel hayatın gizliliği hakkı arasındaki hassas dengeyi gözetmektedir⁵¹⁷. Dava, HIV pozitif bir kişinin tıbbi kayıtlarının ceza yargılaması sırasında kullanılması ve ifşa edilmesi üzerine odaklanmaktadır.

AİHM, kararında Avrupa Konseyi'nin 108 numaralı Protokolü ve HIV ile ilgili etik konulara ilişkin Bakanlar Komitesi Tavsiye Kararı'na atıfta bulunarak, tıbbi verilerin gizliliğinin önemini vurgulamıştır. Mahkeme, sağlık verilerinin korunmasının, bireylerin özel yaşamlarının korunmasının temel bir unsuru olduğunu ve bu korumanın sağlık hizmetlerine olan güvenin sürdürülmesi açısından kritik olduğunu belirtmiştir.

Kararda, ceza davalarında kamu yararı ile bireylerin özel hayatının gizliliği hakkı arasında bir denge kurulması gerektiği vurgulanmıştır. AİHM, somut olayda sağlık verilerinin mahkemede delil olarak kullanılmasını AİHS'nin 8. maddesinin 2. fıkrası kapsamında değerlendirmiş ve bu kullanımı ihlal olarak görmemiştir. Ancak, başvurucunun kimliği ve sağlık durumunun kamuya açık mahkeme kararında yer almasını özel hayatın gizliliğinin ihlali olarak değerlendirmiştir.

Mahkeme, taraf devletlerin iç hukuklarında kişisel verilerin korunmasına yönelik düzenlemeler yapması gerektiğini vurgulamıştır. Bu düzenlemelerin, verilerin toplanma amacı dışında kullanılmaması, gerektiğinde bireyin rızasının alınması ve üçüncü kişilerden korunması için önlemler içermesi gerektiği belirtilmiştir.

AİHM, özellikle HIV gibi hassas sağlık verilerinin korunmasının önemine dikkat çekmiştir. Bu tür verilerin ifşası, bireylerin toplumda ayrımcılığa uğrama korkusuyla sağlık hizmeti almaktan

⁵¹⁵ Aybeniz AKLAN, “Karşılaştırmalı Hukukta Kişisel Sağlık Verilerinin Hukuka Aykırı İşlenmesi ve Tazminat Sorumluluğu”, **Ankara Yıldırım Beyazıt Üniversitesi**, Yayınlanmamış Yüksek Lisans Tezi, 2024, s. 34 vd.

⁵¹⁶ Konuya ilişkin ayrıntılı bilgi için bkz.: Feray ÖZKAN, “Kişisel Sağlık Verilerinin Korunmasının Pozitif Temelleri ve AİHM Kararlarında Örnekler”, **Dokuz Eylül Üniversitesi**, Yayınlanmamış Yüksek Lisans Tezi, 2018, s. 70 vd.

⁵¹⁷ AİHM, Z. / Finlandiya, B.n. 22009/93, T. 25.2.1997.

kaçınmalarına ve dolayısıyla toplum sağlığının tehlikeye girmesine neden olabileceği uyarısında bulunmuştur. Bu karar, sağlık verilerinin korunması ile kamu yararı arasındaki dengenin nasıl kurulması gerektiğine dair önemli bir içtihat oluşturmaktadır⁵¹⁸.

AİHM'in HIV hastalarının sağlık verilerinin korunmasına ilişkin ortaya koyduğu ilkeler, COVID-19 gibi bulaşıcı hastalıklar bakımından da önemli bir referans noktası oluşturmaktadır. Her ne kadar COVID-19, HIV'den farklı olarak daha hızlı yayılan ve geniş kitleleri etkileyen bir hastalık olsa da enfekte kişilerin verilerinin korunması benzer bir hassasiyet gerektirmektedir. Nitekim COVID-19 sürecinde de hastalığa yakalanan kişilerin kimliklerinin ifşa edilmesi, bu kişilerin toplumda damgalanmasına ve sosyal dışlanmaya maruz kalmalarına neden olabilmektedir. Bu durum, tıpkı HIV vakalarında olduğu gibi, kişilerin test yaptırmaktan ve sağlık kuruluşlarına başvurmadan kaçınmalarına yol açabilir. Böyle bir sonuç ise salgınla mücadeleyi zorlaştırarak toplum sağlığını tehlikeye atabilir. Bu nedenle, COVID-19 ile mücadelede de sağlık verilerinin korunması ile kamu yararı arasındaki hassas dengenin gözetilmesi ve kişisel verilerin ancak gerekli olduğu ölçüde işlenmesi büyük önem taşımaktadır.

Ulusal ve uluslararası hukuki düzenlemeler incelendiğinde, kamu düzeninin sağlanması amacıyla kamu yararının özel çıkarlar karşısında öncelik kazanabileceği görülmektedir. Ancak bu öncelik, bireylerin temel hak ve özgürlüklerini tamamen göz ardı edecek şekilde uygulanmamalıdır⁵¹⁹. Yasal çerçeve, her somut olayın kendine özgü koşullarını dikkate alarak kamu yararı ile özel yarar arasında adil bir denge kurulmasını öngörmektedir. Bu dengenin sağlanmasında, ölçülülük ilkesi kritik bir rol oynamaktadır. Hukuk uygulayıcıları, kamu düzenini koruma amacıyla alınan tedbirlerin gerekli, elverişli ve orantılı olmasını sağlamakla yükümlüdür. Bu yaklaşım, hem kamu düzeninin etkin bir şekilde korunmasını hem de bireylerin temel haklarının gereksiz yere kısıtlanmamasını güvence altına alacaktır.

Yukarıda, Türk hukuku ile GDPR ve AİHS gibi uluslararası metinler arasında kurallaştırma bakımından paralellik bulunduğu ifade edilmişti. Ancak, en az kuralların varlığı kadar önemli olan bir

⁵¹⁸ Benzer kararlar için bkz.: AİHM, L.L. / Fransa, B.n.7508/02, T.12.2.2007; AİHM, Peruzzo ve Mertens / Almanya, B.n. 7841/08 ve 57900/12, T.4.6.2013.

⁵¹⁹ Kurum tarafından Covid-19 salgını sürecinde yayımlanan bir duyuruda şu ifadeler yer verilmiştir: “Belirtmek gerekir ki, bu istisnai zamanlarda dahi veri sorumluları ve veri işleyenlerin, ilgili kişilerin kişisel verilerinin güvenliğini sağlamaları gerekmektedir. Bu nedenle kişisel verilerin hukuka uygun olarak işlenmesi ve bu konuda alınan herhangi bir önlemin hukukun genel ilkelerine uygun olması, bu çerçevede kişilerin temel hak ve özgürlükleri açısından geri döndürülemez zararların ortaya çıkmaması önemlidir. Bu minvalde özellikle COVID-19 virüsüne karşı alınan önlemler kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri gerekli, amaçla bağlantılı, sınırlı ve ölçülü olmalıdır.” Kişisel Verileri Koruma Kurumu, Kamuoyu Duyurusu: Covid-19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler, 27.3.2020, <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-> (E.T. 26.5.2024).

başka şey bunların usulüne uygun olarak uygulanıyor olmasıdır. Bu noktadan bakıldığında, ülkemiz uygulamalarında Covid-19 süreci için bazı eksiklerin görüldüğü ifade edilmelidir⁵²⁰.

Covid-19 pandemisi sürecinde Sağlık Bakanlığı tarafından geliştirilen Hayat Eve Sığar (HES) mobil uygulaması, kişisel verilerin korunması açısından ciddi endişeler uyandırmıştır. Öncelikle, uygulamanın Kişisel Verileri Koruma Kurumu ile iş birliği içinde hazırlanmamış olması, veri güvenliği konusunda temel bir eksikliğe işaret etmektedir. Ayrıca, uygulamanın herhangi bir bağımsız güvenlik denetiminden geçip geçmediğine dair kamuoyuna sunulmuş bir bilgi bulunmamaktadır. Şeffaflık ilkesi gereğince, kullanıcıların kişisel verilerinin nasıl toplandığı ve kullanıldığına ilişkin düzenli bilgilendirmelerin yapılmaması da ayrı bir sorun teşkil etmektedir. Teknik açıdan bakıldığında, her bir kullanıcıya anonim bir takma ad atayarak sistem işletilebilecekken, uygulama daha giriş aşamasında ad, soyad, yaş, baba adı ve telefon numarası gibi hassas kişisel bilgileri talep etmiştir. Bu verilerin merkezi bir sistemde depolanıyor olması, olası bir siber saldırı veya veri sızıntısı durumunda milyonlarca vatandaşın kişisel bilgilerinin risk altına girmesi anlamına gelmektedir. Bu bağlamda, Avrupa'daki bazı ülkelerde kullanılan Covid-19 takip uygulamalarının, kullanıcı gizliliğini korumak adına daha gelişmiş önlemler aldığı ve çoğunlukla anonim veri toplama yöntemlerini tercih ettiği bilinmektedir. Bu eksikliklere rağmen KVK Kurumu tarafından aktif bir müdahalede bulunulmamıştır.

Öte yandan, Norveç'in "Smittestopp" uygulamasının askıya alınması, bireylerin mahremiyetini korumak adına yasal normların uygulanmasının önemli bir örneğini teşkil etmektedir. Söz konusu uygulama, gönüllülük esasına dayanmasına ve ülke nüfusunun yalnızca %10'undan az bir kesimi tarafından aktif olarak kullanılmasına rağmen, Norveç Veri Koruma Otoritesi tarafından geçici olarak durdurulmuştur. Otoritenin bu kararı vermesinde birkaç kritik faktör etkili olmuştur. Öncelikle, uygulamanın kullanıcıların hassas konum verilerini toplamasının, veri minimizasyonu ilkesine aykırılık teşkil ettiği tespiti yapılmıştır. Ayrıca, kullanıcılara verilerinin hangi spesifik amaçlar doğrultusunda işleneceğini seçme imkânı tanınmaması, veri işleme sürecinde şeffaflık ve kullanıcı kontrolü prensiplerini ihlal etmiştir. Dahası, iletişim takibi için veri sağlanması ile analiz ve araştırma amaçlı veri işlemenin otomatik rıza mekanizmasıyla birleştirilmesi, kullanıcıların özgür iradeleriyle rıza gösterme haklarını da kısıtlamıştır. Son olarak, veri kontrolörünün analitik amaçlar için toplanan verileri anonim hale getirmek ve toplu olarak işlemek adına gerekli tedbirleri almaması, veri güvenliği ve gizliliği açısından ciddi sorunlar olarak tespit edilmiştir. Sonuçta otorite, uygulamayı, kullanıcıların kişisel

⁵²⁰ Konuya ilişkin ayrıntılı inceleme için bkz.: Faruk ÇAYIR, **Pandemi Takip Uygulamaları ve Kişisel Verilerin İzlenmesi Raporu**, Alternatif Bilişim Derneği, 2020, <https://alternatifbilisim.org/covid-19-pandemi-sureci-raporlari-yayinda/> (E.T. 24.5.2024).

verilerinin korunması hakkına orantılı bir müdahale olarak değerlendirilemeyeceği gerekçesiyle geçici olarak durdurmuştur⁵²¹.

Bununla birlikte, dünyada kamu yararı ve kişisel yarar arasında tamamen kamu yararını tercih eden örnekler de bulunmaktadır. Örneğin, 2015 yılında MERS salgınının en çok görüldüğü ikinci ülke olan Güney Kore’de hükümet, o dönemde hastalanan kişilerle ilgili yeterince bilgi paylaşmadığı için eleştirilmiş, bunun üzerine ilgili yasal düzenlemelerde değişikliğe gidilmiştir. Covid-19 salgını sürecinde ise salgının önüne geçebilmek için, testi pozitif çıkan kişinin isim bilgisi hariç, kaç yaşında olduğu, hangi bölgede oturduğu, virüsün muhtemelen nerede bulaştığı (kimi zaman mağaza, bar, ya da bir kilise ismi verilmek suretiyle) gibi bilgiler salgın sürecinde kullanılan uygulamalara bildirim olarak düşmüş ve aynı zamanda ülkenin Sağlık Bakanlığı web sitesinde yayınlanmıştır. Basına yansıyan bilgilere göre, halkın bazen hastalanan kişileri tespit ettiği, bunlara sosyal medya ortamlarında ağır hakaretlerde bulunduğu ve bu sebeple çoğu insanın en az hastalanmaktan korktuğu kadar toplumda ayrımcılığa uğramaktan da korktuğu ifade edilmiştir⁵²².

Sonuç olarak, dünyanın farklı ülkelerinde toplum sağlığı ve kişisel mahremiyet arasında benzer normlarla kurulan dengenin uygulamada farklı şekillerde yorumlandığı ya da toplum sağlığına birincil öncelik verilerek kişisel mahremiyetin geri planda bırakıldığı yasalar ve uygulamaların varlığı göze çarpmaktadır. Dünyanın kişisel verilerin korunması bakımından küresel salgın hastalığa hazırlıksız yakalandığı ve bu sebeple farklı uygulamaların ortaya çıktığı söylenebilirse salgın hastalıklar her zaman yaşanabilecek olaylardır. Bu nedenle bir an önce uygulanacak kuralların belirli olması ve bunlara uyulması gerekir.

Öte yandan, eğer toplum “hayatta kalmak” veya “kişisel verilerin korunması” gibi salt iki tercih arasında bırakılacak olursa gelecekte mahremiyeti önemsiz gören ve kamu düzenini ne pahasına olursa olsun en hızlı şekilde onarmayı amaçlayan yasaların artacağı söylenebilir. Ancak, mahremiyet ve kamu yararı arasında bir denge sağlama yolunda ısrar edilirse, bireylerin ve toplumun özellikle dijital teknolojilerin kullanımı üzerindeki kontrolü artabilir ve böylece kişisel verilerin daha etkin şekilde korunması sağlanabilir⁵²³.

Mahremiyetin değerini kaybetmediği ihtimalin gerçekleşmesi için salgın hastalıkların yaşandığı dönemlerde GDPR ve AİHM kararlarında vurgulanan ilkelere uygun şekilde veri işlemeye devam edilmelidir. Öte yandan, 2020 yılının ilk yarısında global ölçekte gerçekleşen veri ihlali vakalarında, kasıtlı veya kazara olmasına bakılmaksızın, üç milyonu aşkın bireyin kişisel verilerinin ele geçirildiği

⁵²¹ Alexander KOTOV/Victor NAUMOV, “E-Governance and Privacy in Pandemic Times”, In: Yang, XS., Sherratt, S., Dey, N., Joshi, A. (eds) **Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems**, Springer, Vol 236. 2022, s. 976, https://doi.org/10.1007/978-981-16-2380-6_86.

⁵²² “Coronavirus privacy: Are South Korea’s alerts too revealing?”, BBC, 5.3.2020, <https://www.bbc.com/news/world-asia-51733145> (E.T. 20.5.2024).

⁵²³ KOTOV/NAUMOV, s.972.

ifade edilmektedir⁵²⁴. Bu nedenle, ALEXANDER ve VICTOR’a göre bu yaygın ve uluslararası boyuttaki veri güvenliği tehdidi karşısında, geleneksel yaklaşım olan veri toplandıktan sonra güvenlik önlemlerini tesis etme stratejisi, artık yetersiz ve etkisiz kalmaktadır⁵²⁵. Zira alınan önlemler genellikle reaktif bir nitelik taşımakta ve çoğunlukla veri ihlalleri gerçekleştikten sonra uygulamaya konulmaktadır. Bu durum, siber suçluların sürekli olarak yeni ve sofistike yöntemler geliştirmesine karşı etkili bir koruma sağlayamamaktadır. Bu bağlamda, veri güvenliğini sağlamak için paradigma değişikliğine ihtiyaç duyulmaktadır. Öncelikli hedef, veri minimizasyonu ilkesi doğrultusunda mümkün olan en az miktarda veri toplamak olmalıdır. Toplanan verilerin işlenmesi, önceden açıkça belirlenmiş ve meşru amaçlarla sınırlandırılmalıdır. Ayrıca, merkezi veri depolama sistemlerinin potansiyel riskleri göz önünde bulundurularak, gereksiz veri merkezileşmesinden kaçınılmalıdır. Son olarak, verilerin işlenme amacı ortadan kalktığında, bu verilerin gecikmeksizin ve güvenli bir şekilde imha edilmesi gerekmektedir.

2.2.2. Kamu Güvenliği Kapsamında Elektronik Gözetim Sistemleriyle Kişisel Veri İşleme

Kamu düzeninin temel unsurlarından biri olan güvenlik unsuru, bireylerin toplum içinde huzurlu ve endişesiz bir şekilde yaşamalarını sağlayan koşulların bütünüdür ifade eder. Bu unsur, genel ve kamuya açık alanlarda kişilerin can ve mallarına yönelik tehdit ve tehlikelerin yokluğunu, bireylerin herhangi bir saldırı, zorlama veya kazaya uğrama endişesi taşımadan hareket edebilmelerini ve bu yönde olumlu bir kanaate sahip olmalarını kapsar. DURAN’a göre kamu düzeninin bir unsuru olarak güvenlik *“kişilerin umumi veya umuma açık yerlerde, saldırıya, zorlamaya, itilip kakılmaya, kazaya ve engellemeye (durdurulma, bekletilme, alıkonulma) uğramadan dolaşmaları... can ve malları için hiçbir zaman endişe duymamaları”* anlamına gelmektedir⁵²⁶.

Kolluk makamları, güvenlik unsuru kapsamındaki görevlerini yerine getirirken çeşitli kişisel verileri işlemek durumunda kalmaktadır. Bu veriler arasında görüntü kayıtları, konum bilgileri, kimlik bilgileri ve iletişim bilgileri gibi farklı nitelikte veriler yer alabilmektedir. Özellikle teknolojinin gelişmesiyle birlikte, kolluk birimlerinin veri işleme faaliyetlerinin kapsamı ve yoğunluğu da artış göstermiştir. Bu noktada, güvenlik amacıyla işlenen kişisel verilerin niteliği, işlenme amacı ve yöntemi, temel hak ve özgürlüklerle olan ilişkisi önem kazanmaktadır.

Güvenliğin sağlanması amacıyla idarenin başvurduğu en yaygın yöntemlerden biri elektronik gözetim sistemleridir. Bu kapsamda özellikle kent güvenliğinin sağlanmasında etkin rol oynayan iki

⁵²⁴ KOTOV/NAUMOV, s.977.

⁵²⁵ KOTOV/NAUMOV, s.977.

⁵²⁶ DURAN, *İdare Hukuku Ders Notları*, s.254.

temel sistem öne çıkmaktadır: Mobil Elektronik Sistem Entegrasyonu (MOBESE) ve Elektronik Denetleme Sistemi (EDS). MOBESE, kent merkezlerinde huzur ve güven ortamının korunması, suçun önlenmesi, şüpheli şahıs ve araçların tespiti, trafik düzeninin sağlanması ve acil durumlara hızlı müdahale gibi çok yönlü güvenlik ihtiyaçlarına cevap verirken⁵²⁷; EDS ise ağırlıklı olarak trafik güvenliğinin sağlanması, kural ihlallerinin tespiti ve caydırıcılığın artırılması amacıyla kullanılmaktadır⁵²⁸. Bu sistemler aracılığıyla işlenen kişisel veriler çeşitlilik göstermektedir. MOBESE kapsamında, kişilerin görüntüleri, bulundukları konum bilgileri, hareket güzergahları ve davranış örüntüleri gibi veriler elde edilebilmektedir. EDS kapsamında ise araç plakası, aracın hızı, konumu, seyahat güzergahı ve zamanı, sürücünün görüntüsü gibi veriler işlenebilmektedir. Özellikle bu sistemlerin birbiriyle entegre çalışması durumunda, bir kişinin kent içindeki hareketleri, bulunduğu yerler ve zaman bilgileri gibi oldukça kapsamlı bir veri seti ortaya çıkabilmektedir. Her iki sistemin de ortak özelliği, kent yaşamında güvenliğin elektronik gözetim yoluyla sağlanması sürecinde çok sayıda kişisel verinin işlenmesini gerektirmesidir. Bu durum, güvenlik ihtiyacı ile kişisel verilerin korunması hakkı arasında hassas bir denge kurulmasını zorunlu kılmaktadır.

Bu sistemler aracılığıyla işlenen kişisel verilerin hukuki rejimi bakımından öncelikle 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun uygulama alanını değerlendirmek gerekir. Yukarıda da değinildiği üzere, Kanun'un 28. maddesinin birinci fıkrasının (ç) bendi gereğince, kamu düzeninin korunması amacıyla yetkili kurum ve kuruluşlar tarafından önleyici ve koruyucu faaliyetler kapsamında işlenen kişisel veriler, Kanun hükümlerinden istisna tutulmuştur.

Bununla birlikte, elektronik gözetim sistemleri aracılığıyla gerçekleştirilen veri işleme faaliyetleri, bireylerin temel hak ve özgürlüklerine müdahale niteliği taşımaktadır. Bu noktada, Anayasa'nın 20. maddesinin üçüncü fıkrası uyarınca, kişisel verilerin korunmasını isteme hakkına yönelik sınırlandırmaların ancak kanunla yapılması gerekir. Ayrıca bu sınırlandırmaların, Anayasa'nın 13. maddesi gereğince demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine uygun olması zorunludur. Dolayısıyla, KVKK'dan istisna tutulan bu veri işleme faaliyetlerinin de mutlaka bir kanuni dayanağının bulunması ve bu düzenlemenin anayasal ilkelere uygun olması gerekmektedir.

EDS'nin kanuni dayanağını 2918 sayılı Karayolları Trafik Kanunu'nun ek 16. maddesi oluşturmaktadır⁵²⁹. 2011 yılında yapılan düzenlemede, belediyelerin veya belediye şirketlerinin

⁵²⁷ Feridun YENİSEY, **Kolluk Hukuku**, Beta Yayınevi, 2.Baskı, 2015, s.351; Nur Nihal TAVLAN, “Hukuka Aykırı Olarak Mı Gözetleniyoruz?”, **Hukuki Haber**, 17.1.2021, https://www.hukukihaber.net/hukuka-aykiri-olarak-mi-gozetleniyoruz#_ftn22 (E.T.: 24.1.2025).

⁵²⁸ Zehra KARAKUŞ IŞIK, Kamile TÜRKOĞLU ÜSTÜN, “İdarenin Kolluk Yetkileri Kapsamında Trafik İhlallerinin Elektronik Denetleme Sistemleri ile Tespiti”, **İNÜHFD**, Cilt: 15, S. 2, 2024, s.360.

⁵²⁹ 2918 sayılı Kanun, **Ek Madde 16** – (Ek: 13/2/2011-6111/60 md.) “Belediyelerce veya sermayesinin tamamı belediyelere ait şirketler tarafından kendi bütçe kaynakları kullanılarak, karayollarında can ve mal güvenliğini sağlamak, düzenli ve güvenli trafik akışını temin etmek amaçlarına hizmet etmek üzere kurulmuş veya kurulacak elektronik sistemlerin Emniyet Genel Müdürlüğünce trafik ihlallerinin tespiti amacıyla kullanılması durumunda, aylık dönemler halinde yapılan tespitlere dayanılarak düzenlenen trafik idari yaptırım karar tutanaklarında yer alan trafik idari para cezasının % 30’u oranındaki tutar,

karayollarında can ve mal güvenliğini sağlamak, düzenli ve güvenli trafik akışını temin etmek amacıyla, kendi kaynaklarıyla tesis ettikleri elektronik sistemlerin, trafik güvenliğini sağlamak amacıyla Emniyet Genel Müdürlüğü tarafından kullanılabileceğini düzenlemektedir. İlgili maddenin ikinci fıkrasında, maddenin uygulanmasına ilişkin usul ve esasların Maliye ve İçişleri Bakanlıklarıyla müştereken belirleneceği öngörülmüş, buna ilişkin düzenleme ise “2918 Sayılı Karayolları Trafik Kanunu’nun Ek 16’ncı Maddesinin Uygulanmasına İlişkin Usul ve Esaslar” başlıklı düzenleyici işlemle yapılmıştır⁵³⁰.

EDS sistemlerinin kullanımına ilişkin ek 16. madde incelendiğinde, sadece sistemin kim tarafından kullanılacağına kanunla düzenlendiği görülmektedir. Oysa Anayasa Mahkemesi kararları uyarınca, kanunla düzenlenmesi öngörülen konularda temel ilkelerin belirlenmesi ve çerçevenin çizilmesi gerekmektedir. Bu temel ilkeler belirlendikten sonra, teknik detaylar ve uzmanlık gerektiren hususlar yürütme organının düzenleyici işlemleriyle belirlenebilir⁵³¹. Mevcut düzenlemede EDS’nin kurulma amacı "trafik akışını temin etmek" ve "karayollarında can ve mal güvenliğini sağlamak" olarak somut biçimde belirtilmiş ve sistem üzerinden toplanan görüntülerin yalnızca bu amaçla işlenebileceği öngörülmüştür. Ancak, toplanan görüntü ve verilerin saklama süresi ile kişisel verileri işlenen ilgililerin hakları (bilgilendirilme, verilere erişme, düzeltme ve silme talep etme gibi)⁵³² kanunda düzenlenmemiştir. Dolayısıyla, bu hususların da kanun kapsamında ele alınması gerekmektedir.

Öte yandan, MOBESE ile yapılan gözetlemenin kanuni bir dayanağı dahi olmadığı ifade edilmektedir⁵³³. Örneğin, PVSK’nın 1. maddesinde “*Polis, asayiş amme, şahıs, tasarruf emniyetini ve mesken masuniyetini korur. Halkın ırz, can ve malını muhafaza ve ammenin istirahatini temin eder.*” ifadelerinden sonra 2. maddesinde “*Polisin genel emniyetle ilgili görevleri iki kısımdır. A) Kanunlara, Cumhurbaşkanlığı kararnamelerine, yönetmeliklere, Hükümet emirlerine ve kamu düzenine uygun olmayan hareketlerin işlenmesinden önce bu kanun hükümleri dairesinde önünü almak, B) İşlenmiş olan bir suç hakkında Ceza Muhakemeleri Usulü Kanunu ile diğer kanunlarda yazılı görevleri yapmak*” düzenlemesine yer verilmiştir. Yine aynı kanunun ek 7. maddesinin altıncı fıkrasında “*İstihbarat faaliyetlerinde, bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla,*

izleyen ayın sonuna kadar Emniyet Genel Müdürlüğü bütçesinden ilgili belediyelere sistem kullanımı hizmet bedeli olarak ödenir. (Ek cümle: 20/8/2016-6745/30 md.) Elektronik sistemlerin belediyeler tarafından hasılat paylaşımı yoluyla kurdurulması ve işlettirilmesi hâlinde belediyelere ödenecek tutar, elektronik sistemlerin yatırım maliyetine ulaşınca kadar %30, sonrasında %15 olarak uygulanır.”

⁵³⁰ İlgili usul ve esasların tam metni için bkz.: https://www.trafik.gov.tr/kurumlar/trafik.gov.tr/03-Mevzuat/Ek16_usul_esas_18.11.2016.pdf (Erişim Tarihi: 24.1.2025)

⁵³¹ AYM, E.2017/143, K.2018/40, K.t.: 2.5.2018, §16; AYM, E.2013/47, K.2013/72, K.t.: 6.6.2013.

⁵³² Anayasa’nın 20/3. maddesinde kişisel verilerin korunmasını isteme hakkının burada sayılan hakları da kapsadığı açıkça düzenlenmiştir: “Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.”

⁵³³ YENİSEY, s.356; Buket ABANOZ, **Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu**, İstanbul, On İki Levha Yayıncılık, 2018, s. 135; Ersan Şen, “Mobese ve Güvenlik Kameralarının Özel Hayata Müdahalesi ve Delil Vasfı”, **Hukuki Haber**, 21.11.2019, <https://www.hukukihaber.net/mobese-ve-guvenlik-kameralarinin-ozel-hayata-mudahalesi-ve-delil-vasfi> (E.T.: 24.1.2025).

teknik araçlarla izleme yapılabilir.” hükmü düzenlenmiştir. Ancak 1. maddede kamusal alanların sürekli ve düzenli bir şekilde kameralarla gözetlenmesine yönelik açık bir belirleme bulunmamaktayken, ek 7. maddenin altıncı fıkrasında ifade edilen “teknik araçlarla izleme” tedbirine başvurulabilmesi için suçların işlendiğine dair somut delillerle desteklenen kuvvetli şüphenin bulunması ve başka şekilde delil elde edilememesi gerekir⁵³⁴. Oysa MOBESE kameraları önleyici kolluk bağlamında, caydırıcı bir etki uyandırması amacıyla kullanılmakta, doğrudan bir suçun araştırılması amacıyla aktif hale getirilmemekte, sürekli şekilde gözetleme yapmaktadır.

Ayrıca, 5442 sayılı İl İdaresi Kanunu’nda düzenlenen ve valiye il sınırları içinde huzur ve güvenliği sağlamak için önleyici kolluk yetkisi kapsamında gerekli tedbirleri alma yetkisi veren 11/C maddesinin MOBESE sisteminin kanuni dayanağı olabileceği akla gelebilir⁵³⁵. Ancak, temel hak ve özgürlüklerin sınırlandırılmasına ilişkin Anayasanın 13. maddesi ve kişisel verilerin korunmasını isteme hakkına yönelik sınırlamanın yalnızca kanunla yapılabileceğini öngören 20/3. maddesi karşısında, 5442 sayılı Kanun’un 11/C maddesinin yeterli bir kanuni dayanak olması mümkün değildir. Hürriyetlerin asıl, sınırlamanınsa istisna olduğu, bu nedenle temel hak ve özgürlüklerin sınırlandırılmasına ilişkin kuralların kanunda açıkça düzenlenmesi gerektiği unutulmamalıdır⁵³⁶. Bu bağlamda, kanun koyucu tarafından yapılacak bir düzenlemeyle, MOBESE sisteminin kurulması, hangi amaçlarla kullanılacağı, hangi şartları sağlayan alanlara kurulabileceği, görüntülerin saklanma süreleri, sisteme erişim yetkisi olan kişiler ve kişilerin bu veriler üzerindeki hakları belirlenmelidir⁵³⁷.

Bununla birlikte, MOBESE gibi sistemlerle kamusal alanların izlenmesi, kayıt altına alınması ve bu verilerin kullanılması bir kanun ile düzenlendiğinde kanunilik ilkesini karşılarsa da bu yeterli olmayacaktır. Çünkü, Anayasanın 13. maddesi bağlamında düzenlemenin meşru bir amacının ve ölçülülük ilkesine uygun olması da gerekir. AİHM tarafından verilen Beck / Birleşik Krallık kararına göre, kamusal alanda bireylerin hareketlerini anlık olarak izleyen ve kaydetmeyen güvenlik kameralarının varlığı, özel hayatın gizliliği hakkına müdahale teşkil etmemektedir. Bununla birlikte, görüntülerin kaydedilmesi ve sistematik biçimde depolanması durumunda özel hayatın gizliliği hakkının ihlali söz konusu olabilmektedir⁵³⁸. Nitekim Mahkeme, güvenlik kameraları tarafından kaydedilen ve

⁵³⁴ 5271 sayılı Ceza Muhakemesi Kanunu’nun “Teknik Araçlarla İzleme” başlıklı 140. maddesinin ilk fıkrası şöyledir: “Aşağıdaki suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir.”

⁵³⁵ 5442 sayılı Kanun, Madde 11/C: “İl sınırları içinde huzur ve güvenliğin, kişi dokunulmazlığının, tasarrufa müteallik emniyetin, kamu esenliğinin sağlanması ve önleyici kolluk yetkisi valinin ödev ve görevlerindendir. (Ek cümle: 25/7/2018-7145/1 md.) Bunları sağlamak için vali gereken karar ve tedbirleri alır.”

⁵³⁶ Kemal GÖZLER, “Korona Virüs Salgınıyla Mücadele İçin Alınan Tedbirler Hukuka Uygun mu? (2)”, 6.7.2020, www.anayasa.gen.tr/korona-2.htm (E.T.:25.1.2025).

⁵³⁷ ABANOZ, s. 149; ŞEN, “Mobese ve Güvenlik Kameralarının Özel Hayata Müdahalesi ve Delil Vasfı”.

⁵³⁸ AİHM, Beck / Birleşik Krallık, B.n.: 44647/98, K.t.: 28.1.2003, §59, <https://hudoc.echr.coe.int/eng?i=001-60898>. Konuya ilişkin AİHM kararlarının incelemesi için bkz.: ABANOZ, s. 117 vd.; Hazan Dicle ÖZER, “MOBESE İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme”, *DEUHFİD*, C.24, S.1, Mayıs 2022, s. 488 vd.

sonrasında yerel basında yayınlanan görüntülerin, kamusal alanda çekilmiş olsa dahi başvurusunun özel hayatının gizliliğini ihlal edebileceğini kabul etmiştir.

MOBESE sistemlerinin ölçülülük ilkesine uygun bir yasal çerçevede düzenlenmesi için öncelikle "elverişlilik" kriteri bakımından, sistemin kurulacağı alanların objektif kriterlere bağlanması gerekmektedir. Suç oranlarının yüksek olduğu, kamu düzeninin sık sık bozulduğu ve kalabalık bölgelerin tespitinde istatistiki verilerin esas alınması, bu kriterin karşılanması bakımından önem arz etmektedir.

"Gereklilik" ilkesi açısından, temel hak ve özgürlüklere en az müdahale eden yöntemin seçilmesi zorunludur. Bu bağlamda, yüz tanıma sistemleri gibi kişisel verilere yoğun müdahale oluşturan teknolojilerin kullanılmaması, kayıt alma işleminin risk analizi yapılarak belirlenen saatlerle sınırlandırılması ve sürekli gözetim yerine gereklilik durumuna göre yapılandırılması önem taşımaktadır.

"Orantılılık" ilkesi açısından, kamu güvenliğini sağlama amacıyla alınan tedbirlerin bireysel hak ve özgürlükler üzerinde oluşturduğu külfet arasında makul bir denge kurulmalıdır. Bu kapsamda, görüntülerin saklanma süresi, kullanım amacı ve erişim yetkisi gibi hususların açıkça düzenlenmesi gerekmektedir. AİHM'in Beck / Birleşik Krallık kararında vurgulandığı üzere, görüntülerin basınla paylaşılması gibi amaç dışı kullanımların engellenmesi, kişisel verilerin korunması bakımından kritik öneme sahiptir. Görüntülerin saklanma süresinin, suç soruşturmaları için gerekli asgari süreyle sınırlandırılması ve bu sürenin sonunda otomatik olarak silinmesinin öngörülmesi, orantılılık ilkesinin bir gereğidir.

2.2.3. Dirlik ve Esenlik Unsuru Kapsamında Toplantı ve Gösteri Yürüyüşlerinde Kişisel Verilerin İşlenmesi

İdarenin kamu düzenini sağlama görevi kapsamında öne çıkan unsurlardan biri olan dirlik ve esenlik, toplum yaşamının normal seyrinde devamını ve toplumsal hayatın karışıklık ve kargaşalardan uzak bir biçimde sürdürülmesini ifade eder. İdare hukuku öğretisinde dirlik ve esenlik kavramı, "yaşamın normal seyrini etkileyebilecek gürültü, toz, ışık, koku gibi her türlü rahatsızlığın bulunmaması" şeklinde tanımlanmaktadır⁵³⁹. Bu unsurun kapsamı, toplumsal yaşamın olağan akışını olumsuz yönde etkileyebilecek her türlü etkeni içine alır ve içinde bulunulan zaman, mekân, kültür düzeyi ve yaşam koşulları gibi değişkenlere göre farklılık gösterebilir.

⁵³⁹ Sıddık Sami ONAR, **İdare Hukukunun Umumi Esasları**, Cilt 2, İsmail Akgün Matbaası, 1960, s.1106; DURAN, **İdare Hukuku Ders Notları**, s.254-255; ÖZAY, **Günüşğinde Yönetim**, s.729; OKAY TEKİNSOY, "Kolluk Faaliyetleri", içinde **İdare Hukuku**, Turan YILDIRIM (ed.), s. 611.

Dirlik ve esenlik unsurunun günümüzdeki yansımalarında biri toplantı ve gösteri yürüyüşlerinin denetimi alanında görülmektedir. Bu durumun temelinde birkaç önemli etken yatmaktadır: Birincisi, toplantı ve gösteri yürüyüşü hakkı, demokratik toplumun temel taşlarından biri olarak anayasal koruma altındadır ve bu hakkın kullanımı doğrudan dirlik ve esenliği etkileme potansiyeline sahiptir. İkincisi, gözetim teknolojilerinin gelişmesiyle birlikte idarenin denetim kapasitesi artmış, bu da kişisel verilerin yoğun şekilde işlenmesini beraberinde getirmiştir. Üçüncü olarak, idarenin dirlik ve esenliği koruma amacıyla aldığı tedbirlerin, demokratik bir hakkın kullanımını engelleyici boyutlara ulaşabilmesi riski, bu alanı hukuki açıdan özellikle tartışılmalı hale getirmektedir.

Demokratik sistemin sağlıklı işleyişi için hayati öneme sahip olan toplantı ve gösteri yürüyüşü hakkı, bireylerin düşüncelerini kolektif olarak ifade edebilmelerinin en etkili araçlarından biridir. Ancak bu hakkın kullanımı, doğası gereği kamusal alanların toplu kullanımını gerektirmekte ve bu durum kaçınılmaz olarak gündelik hayatın olağan akışını etkileyebilmektedir.

İdareler, toplum huzurunun bozulmasına sebep olacak olayların ortaya çıkma riskini öneler, bu hakkın kullanımını sıkı bir denetime tabi tutma eğilimindedir. Belli sayıda insanın bir araya gelmesinin yaratabileceği potansiyel tehlikeler karşısında dirlik ve esenliğin korunması gerekçesiyle alınan tedbirler, makul bir zemine oturabilir. Ancak bu tedbirlerin ölçsüz kullanımı, bireylerin demokratik haklarını kullanmaktan çekinmelerine yol açan bir "caydırıcı etki" (chilling effect) yaratma riski taşımaktadır⁵⁴⁰. Bu durum, söz konusu denetim tedbirlerinin demokratik toplumun gerekleriyle uyumlu bir şekilde uygulanmasını zorunlu kılmaktadır.

Günümüzde teknolojik gelişmelerle birlikte, toplantı ve gösteri yürüyüşlerinin denetiminde kullanılan araçlar da çeşitlenmiştir. Drone'lar ile havadan gözetim, sürekli video kaydı yapan sistemler, yüz tanıma teknolojileri ve diğer biyometrik veri toplama araçları, idarelerin kullandığı başlıca denetim mekanizmalarıdır⁵⁴¹. Bu araçların kullanımı, özel nitelikli kişisel veriler de dahil olmak üzere, geniş çaplı bir veri işleme faaliyetini beraberinde getirmektedir. Söz konusu veri işleme faaliyetlerinin hukuka

⁵⁴⁰ Chilling effect" (caydırıcı etki) kavramı, ilk kez 1952 yılında ABD Yüksek Mahkemesi'nde görülen *Wieman v. Updegraff* davasında kullanılmıştır: Leslie KENDRICK, "Speech, Intent, and the Chilling Effect." **William & Mary Law Review**, 54(5), 2013, s.1636, dn.:7, <https://scholarship.law.wm.edu/wmlr/vol54/iss5/4/> (E.T.: 1.2.2025). Kavram, devlet eylem ve işlemlerinin, kişileri temel hak ve özgürlüklerini kullanmaktan caydırması veya bu hakları kullanırken çekimsiz davranmaya yöneltmesi durumunu ifade etmektedir. Özellikle ifade özgürlüğü ve toplantı özgürlüğü gibi demokratik hakların kullanımında, devletin aşırı gözetim ve denetim uygulamalarının yaratabileceği bu caydırıcı etkinin, hakların özüne dokunacak nitelikte bir sınırlama oluşturabileceği kabul edilmektedir. Ayrıntılı bilgi için bkz.: KENDRICK, "Speech, Intent, and the Chilling Effect."; Frederick SCHAUER, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect", **Boston University Law Review**, 58, 1978, s.685-732, <https://scholarship.law.wm.edu/facpubs/879> (E.T.: 1.2.2025); Fatih SÜNGÜ, "Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkemesine Bireysel Başvuru Kararlarında "Chilling Effect" Kavramı" **İnsan Hakları Yıllığı**, C.39, 2021, s.105.134.

⁵⁴¹ Burak KESGİN, "Güvenlik, Düzen ve Gözetim: Geleceğin Dünyasında Protesto Hakkı", **Sosyoloji Araştırmaları Dergisi**, C.26, S. 2, Ekim 2023, s.27.

uygunluğunun değerlendirilmesi, hem temel hakların korunması hem de idarenin gözetim yetkisinin sınırlarının belirlenmesi açısından büyük önem taşımaktadır.

Toplantı ve gösteri yürüyüşleri sırasında dirlik ve esenliğin korunabilmesi için işlenen kişisel veriler, 6698 sayılı Kanun'un 28/1-ç maddesinde yer alan düzenleme gereği, *"kamu düzenini ... sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici ... faaliyetler kapsamında"* işlendiğinden bu Kanun kapsamı dışındadır. Anayasanın 20/3. maddesinde kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği öngörülmüştür. Öyleyse, Anayasanın 20/3. maddesi gereği, toplantı ve gösteri yürüyüşleri sırasında kişisel verilerin işlenmesini gerektiren uygulamaların yasayla öngörülmesi ve 13. maddesi gereği, bu yasal düzenlemenin demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine uygun olması gerekir. Bu anayasal gereklilikler doğrultusunda, toplantı ve gösteri yürüyüşleri sırasında kişisel verilerin işlenmesine ilişkin yasal çerçeve incelendiğinde, konunun temel düzenlemesi olan 2911 sayılı Kanun önem kazanmaktadır.

Toplantı ve gösteri yürüyüşü hakkının kullanılmasına ilişkin usul ve esaslar, 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu ile düzenlenmiştir⁵⁴². Kanunun 1. maddesinde belirtildiği üzere, bu düzenleme toplantı ve gösteri yürüyüşlerinin yeri, zamanı, usul ve şartları ile düzenleme kurulunun görev ve sorumlulukları, yetkili merciin yasaklama ve erteleme halleri, güvenlik kuvvetlerinin görev ve yetkileri ile yasaklar ve ceza hükümlerini kapsamaktadır.

Kanun kapsamında, toplantı düzenlenebilmesi için birtakım kişisel verilerin işlenmesini gerektiren bir bildirim süreci öngörülmüştür. Kanunun 10. maddesi uyarınca, düzenleme kurulu üyelerinin tamamının imzalayacakları bir bildirimin, toplantının yapılmasından en az kırk sekiz saat önce ve çalışma saatleri içinde, toplantının yapılacağı yerin bağlı bulunduğu valilik veya kaymakamlığa verilmesi gerekmektedir. Bu bildirimde toplantının amacı, yapılacağı yer, gün, başlayış ve bitiş saatleri ile düzenleme kurulu başkan ve üyelerinin açık kimlikleri, meslekleri, ikametgahları ve varsa çalışma yerlerinin belirtilmesi zorunludur. Kanunun uygulanmasına dair yönetmelikte⁵⁴³ ise bildirimin içeriği daha detaylı düzenlenmiş, düzenleme kurulu başkan ve üyelerinin T.C. Kimlik numarası ve adli sicil beyanı gibi kişisel verilerinin de bildirimde eklenmesi öngörülmüştür.

Toplantı ve gösteri yürüyüşlerinin gerçekleştirilmesi sırasında kişisel verilerin işlenmesine ilişkin diğer bir düzenleme ise Kanunun 11. maddesinde yer almaktadır. 2014 yılında eklenen fıkra ile toplantı ve gösteri yürüyüşlerinde katılımcıların ve konuşmacıların ses ve görüntülerinin kolluk tarafından kaydedilebileceği düzenlenmiştir. Ancak bu kayıtların yapılması birtakım şartlara bağlanmıştır: Kayıt işleminin kolluk tarafından yapıldığının belli olması gerekmekte ve elde edilen kayıt

⁵⁴² R.G.: 8.10.1983/18185

⁵⁴³ Toplantı ve Gösteri Yürüyüşlerinin Uygulanmasına Dair Yönetmelik, R.G.: 8.8.1985/18836.

ve görüntülerin yalnızca şüphelilerin ve suç delillerinin tespiti amacıyla kullanılabileceği öngörülmektedir. Bu düzenleme, yönetmeliğin 16. maddesinde de aynen yer almaktadır.

Bu düzenlemeler, toplantı ve gösteri yürüyüşleri sırasında işlenecek kişisel veriler için kanuni bir dayanak teşkil etmektedir. Ancak, bu düzenlemelerin de Anayasa'ya uygunluğu değerlendirilmelidir. Örneğin, bildirim sürecini öngören Kanunun 10. maddesi ve aynı hususu düzenleyen Yönetmelik'in 5. maddesi kanunilik ilkesine aykırılık oluşturmaktadır. Zira Anayasa Mahkemesi'nin yerleşik içtihatları uyarınca, temel hak ve özgürlüklerin sınırlandırılmasında kanunla düzenlenmesi öngörülen konularda, temel ilkelerin belirlenmesi ve çerçevenin çizilmesi zorunludur⁵⁴⁴. İdarenin düzenleyici işlemleriyle ancak teknik detaylar ve uzmanlık gerektiren hususlar belirlenebilir. Toplantı ve gösteri yürüyüşü hakkının kullanımı için hangi kişisel verilerin işleneceği konusu, bir teknik detay olmayıp, temel ilke niteliğindedir. Nitekim, toplantı ve gösteri yürüyüşüne katılım için talep edilecek kişisel verilerin kapsamının genişletilmesi, bireylerin bu demokratik haklarını kullanmalarını doğrudan etkileyen ve potansiyel olarak sınırlayan bir nitelik taşıdığından, temel hak ve özgürlüklerin kullanımına ilişkin esaslı bir unsurdur. Bu nedenle, kanunda açıkça istenmesi öngörülen kişisel verilere yönetmelikle yeni veriler eklenmesi, kanun koyucunun öngörmediği ek sınırlamalar getirilmesi anlamına gelmektedir.

Öte yandan, adli sicil beyanının istenmesi özel nitelikli kişisel verilerin işlenmesi anlamına gelmekte olup, bu tür verilerin işlenmesi için meşru bir amacın varlığı da açıkça ortaya konulmamıştır. İdarenin adli sicil beyanı istemesinin ardındaki muhtemel amacın, Kanun'un 17. maddesindeki yasaklama ve erteleme yetkisinin kullanımına dayanak oluşturma çabası olduğu düşünülebilir⁵⁴⁵. Ancak böyle bir yaklaşım, hem hukuken sorunlu hem de ölçülülük ilkesine şu gerekçelerle aykırıdır:

Birincisi, toplantı ve gösteri yürüyüşü hakkı bildirim usulüne tabidir, izne tabi değildir. Bu sistemin temel mantığı, idarenin gerekli güvenlik tedbirlerini alabilmesi için önceden bilgi sahibi olmasıdır. İdarenin, adli sicil kaydını bir ön denetim aracı olarak kullanması, bildirim sisteminin özüne aykırı düşer. İkincisi, Kanun'un 17. maddesinde öngörülen yasaklama yetkisi, "suç işleneceğine dair açık ve yakın tehlike" kriterine bağlanmıştır. Düzenleme kurulu üyelerinin geçmişteki adli sicil kayıtlarının varlığı, tek başına gelecekte suç işleneceğine dair açık ve yakın tehlikenin varlığını göstermez. Böyle bir çıkarım yapmak, masumiyet karinesi ilkesine de aykırılık teşkil eder.

Düzenleme ölçülülük ilkesi bağlamında da açıkça sorunludur. Nitekim, adli sicil kaydının varlığı ile toplantının kamu düzenini bozma potansiyeli arasında doğrudan bir illiyet bağı kurulamayacağı için getirilen sınırlama, ulaşılmak istenen amaç bakımından "elverişli" değildir. Ayrıca, toplantı ve gösteri yürüyüşlerinde kamu düzeninin bozulma tehlikesinin tespiti için, yürüyüşün

⁵⁴⁴ AYM, E.2017/143, K.2018/40, K.t.: 2.5.2018, §16; AYM, E.2013/47, K.2013/72, K.t.: 6.6.2013.

⁵⁴⁵ **Madde 17** — "Bölge valisi, vali veya kaymakam, millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlığın ve genel ahlâkın veya başkalarının hak ve özgürlüklerinin korunması amacıyla belirli bir toplantıyı bir ayı aşmamak üzere erteleyebilir veya suç işleneceğine dair açık ve yakın tehlike mevcut olması hâlinde yasaklayabilir."

yapılacağı yer ve zaman bilgisi, emniyet güçlerine yapılacak ihbarların değerlendirilmesi gibi daha hafif tedbirler mevcut olduğundan böyle bir düzenlemenin “gerekli” olduğu da söylenemez.

Son olarak, bu tür bir uygulama “orantılılık” ilkesini de karşılayamaz. Çünkü kişilerin özel nitelikli kişisel verilerinin işlenmesi suretiyle uğradıkları dezavantaj, elde edilmek istenen kamu yararı ile orantısız bir müdahale oluşturur. Dahası, bu uygulama kişilerin toplumsal hayata katılımını ve rehabilitasyonunu zorlaştıracı bir etki yaratır. Bu nedenlerle, söz konusu düzenleme kanunda yer alsaydı bile ölçülülük ilkesine aykırı olacağı açıktır. Zira demokratik bir toplumda, geçmişteki adli sicil kayıtlarının varlığı, kişilerin demokratik haklarını kullanmasının önünde örtülü bir engel olarak kullanılmamalıdır.

Öte yandan, Kanun'un düzenleme kurulu üyelerinden talep ettiği bilgiler arasında yer alan meslek ve işyeri bilgilerinin de ölçülülük ilkesi bakımından değerlendirilmesi gerekmektedir. Bildirim sisteminin temel amacı, idarenin toplantı veya gösteri yürüyüşü hakkında önceden bilgi sahibi olarak gerekli tedbirleri alabilmesidir. Bu kapsamda, düzenleme kurulu üyelerinin kimlik ve ikametgâh bilgilerinin istenmesi, idare ile iletişimin sağlanabilmesi açısından makul ve gerekli görülebilir. Ancak meslek ve işyeri bilgilerinin talep edilmesi, ölçülülük ilkesi bakımından sorunludur.

Öncelikle, bu bilgilerin toplanmasının toplantı ve gösteri yürüyüşünün güvenli şekilde gerçekleştirilmesine nasıl bir katkı sağlayacağı belirsizdir. Ayrıca, bildirim sisteminin amacına ulaşması için ikametgâh ve iletişim bilgileri yeterli olup, meslek ve işyeri bilgilerinin gerekli olmadığı açıktır. Bu açıdan bakıldığında, idare ile iletişimin sağlanması için daha az müdahaleci alternatifler mevcutken bu ek bilgilerin istenmesi, gereklilik ilkesine aykırı düşmektedir. Orantılılık ilkesi bakımında ise, bu bilgilerin toplanması kişilerin çalışma hayatlarına ilişkin verilerin gereksiz yere işlenmesine yol açmaktadır. Özellikle hâkim, savcı, polis gibi belli meslek gruplarında çalışanlar için bu durum, hakkın kullanımı konusunda caydırıcı bir etki yaratabilir. Ayrıca çalışma hayatına ilişkin bilgilerin biriktirilmesi, kişilerde fişlenme endişesi oluşturarak toplantı ve gösteri yürüyüşü hakkının kullanımını dolaylı yoldan sınırlandırabilir. Elde edilmek istenen yarar (eğer varsa) ile kişilerin uğradığı dezavantaj arasında makul bir denge bulunmamaktadır.

Bu nedenlerle, meslek ve işyeri bilgilerinin talep edilmesi demokratik bir toplumda gerekli olmayan, aşırı bir müdahale niteliğindedir. Bu bilgiler olmaksızın da bildirim sistemi etkin şekilde işleyebilir ve idare gerekli tedbirleri alabilir. Dolayısıyla, kanundaki düzenleme kurulunun meslek ve işyeri bilgilerinin işlenmesini öngören kuralların ölçülülük ilkesine aykırı olduğu kabul edilmelidir.

Düzenleme kuruluna ilişkin verilerin yanı sıra, toplantı ve gösteri yürüyüşlerinin izlenmesi ve kaydedilmesi de kişisel verilerin işlenmesi bakımından özel önem arz eden bir diğer konudur. Son yıllarda, dünya genelinde hükümetler barışçıl nitelikteki toplantı ve gösteri yürüyüşlerini, gelişen

teknolojinin sunduğu imkanları da kullanarak artan oranda gözetim altında tutmaktadır⁵⁴⁶. Ülkemizde de 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu'nun 11. maddesinde 2014 yılında yapılan değişiklikle, toplantı ve gösteri yürüyüşlerine katılan tüm katılımcı ve konuşmacıların ses ve görüntülerinin kolluk tarafından kaydedilebileceği düzenlenmiştir. Bu düzenlemenin, temel hak ve özgürlüklerin sınırlandırılmasında esas alınması gereken demokratik toplum düzeninin gerekleri ile ölçülülük ilkesi bağlamında değerlendirilmesi gerekmektedir.

Toplantı ve gösteri yürüyüşü hakkı, AİHS'in 11. maddesi kapsamında koruma altına alınmış temel bir haktır. Bu hakkın kullanımı sırasında göstericilerin görüntülerinin kaydedilmesi meselesi hem toplanma özgürlüğü hem de özel hayata saygı hakkı bakımından değerlendirilebilir. Toplanma özgürlüğünün demokratik toplumun temel değerlerinden biri olduğu ve bu hakka yönelik sınırlamaların dar yorumlanması gerektiği bir AİHM kararında da vurgulanmaktadır⁵⁴⁷. Başka bir kararında Mahkeme, kamusal alanda gerçekleşen faaliyetler söz konusu olsa dahi, kişinin başkalarıyla etkileşim alanının özel hayat kapsamında değerlendirilmesi gerektiğini kabul etmektedir⁵⁴⁸.

Özellikle dikkat çekilmesi gereken bir husus, protestolara katılımı ilgili bilgilerin işlenmesinin, kişilerin siyasi görüşlerini veya dini inançlarını ortaya çıkarması nedeniyle, özel nitelikli (hassas) kişisel verilerin işlenmesi olarak değerlendirilebilmesidir⁵⁴⁹. Bu tür hassas verilerin kolluk amaçları için işlenmesi, müdahalenin ciddiyetini artıran bir unsur olarak kabul edilmektedir⁵⁵⁰.

⁵⁴⁶ KESGİN, s.20.

⁵⁴⁷ AİHM, Kudrevičius ve Diğerleri / Litvanya [BD], B.n.: 37553/05, K.t.:15.10.2015, §91. Tarım sektöründeki sorunlara dikkat çekmek amacıyla hükümetten izin alarak barışçıl protesto düzenleyen çiftçilere infazının bir yıl süreyle ertelendiği 60 günlük hafif hapis cezası ve ikametgahlarından yedi günden daha fazla ayrılmak istemeleri halinde izin alma yükümlülüğü getirilmesi üzerine sözleşmenin 11. maddesiyle korunan toplantı özgürlüğünün ihlal edildiği iddiasıyla yapılan başvuruda, Büyük Daire, toplanma özgürlüğüne yapılan sınırlamaların dar yorumlanması gerektiğini, bununla birlikte somut olayda izin alınan kapsamda başlayan toplantının hükümetten istenen taleplere yanıt gelmemesi üzerine, göstericiler tarafından genişletilerek üç büyük anayolun neredeyse tamamının kapatılmasını “menfur bir eylem” olarak kabul edilebileceğini, bunun sonuçlarının yerel mevzuatta açıkça öngörüldüğünü, buna rağmen göstericiler tarafından yapılan blokajın kaldırılmasını emretmek ve olası sorumlulukları hakkında uyarmaktan ibaret olan yetkililerin tutumu düşünüldüğünde, yerel makamların kargaşanın önlenmesi ve başkalarının hak ve özgürlüklerinin korunması meşru amaçları ile toplantı özgürlüğünün gerekleri arasında adil bir denge kurulduğu kanaatine vararak ihlal bulunmadığına karar vermiştir.

⁵⁴⁸ AİHM, Glukhin / Russia, B.n.:11519/20, K.t.: 4.10.2023, §67, aktaran: Amnesty International, **Recording Dissent: Camera Surveillance at Peaceful Protest in the Netherlands**, October 16, 2024, s.11, <https://www.amnesty.org/en/documents/eur35/8469/2024/en/> (E.T.: 1.2.2025). Karara konu olayda, Moskova metrosunda, elinde “Barışçıl protestolar için 5 yıl ile karşı karşıyayım” pankartını tutarak tek başına gösteri yapan Glukhin isimli vatandaşın istasyonlarda kullanılan kapalı devre kamera sistemi ve yüz tanıma teknolojisi ile kimliği ve yeri tespit edilmiştir. Yapılan başvuruda AİHM, Glukhin’in kişisel verilerinin, kamu düzeni ve güvenliği için bir tehlike yaratmayan gösterisi için işlenmesinin müdahaleci nitelikte olduğu, bu nedenle özel hayata saygı hakkı ve ifade özgürlüğü hakkının ihlal edildiğine karar vermiştir. Kararda, bir bireyin kamuya açık bir yerdeki eylemlerinin kayıt yapılmaksızın izlenmesinin tek başına özel hayata müdahale teşkil etmeyebileceğini, ancak kişinin görüntülerinin sistematik ve kalıcı biçimde kaydedilmesinin özel hayata müdahale teşkil edebileceği belirtilmiştir. §66.

⁵⁴⁹ AİHM, Glukhin / Rusya, B.n.:11519/20, K.t.: 4.10.2023, §76.

⁵⁵⁰ AİHM, Segerstedt-Wiberg ve diğerleri / İsveç, B.n.:62332/00, K.t.: 6.9.2006, §71-72, aktaran: Amnesty International, **Recording Dissent: Camera Surveillance at Peaceful Protest in the Netherlands**, s.11.

AİHM içtihatları uyarınca, yetkili makamların kişisel verileri topladığı ve işlediği durumlarda, kötüye kullanım ve keyfilik riskine karşı yeterli güvenceler sağlanmalıdır. Bu kapsamda verilerin toplanması, saklanması, kullanılması ve silinmesini düzenleyen açık ve ayrıntılı kuralların varlığı zorunludur⁵⁵¹.

AİHM kararları ışığında, 2911 sayılı Kanun'un 11. maddesindeki düzenlemenin katılımcı ve konuşmacıların ses ve görüntülerinin kayıt altına alınmasına ilişkin hükmü değerlendirildiğinde, bu uygulamanın demokratik toplum düzeninin gerekleri ve ölçülülük ilkesi bakımından makul kabul edilebileceği ifade edilmelidir. Zira büyük katılımlı toplantı ve gösteri yürüyüşlerinde kamu düzenini bozabilecek olayların çıkış anının, yerinin ve faillerinin tespiti ancak bu şekilde mümkün olabilmektedir. Özellikle kalabalık gösterilerde olayların hızlı gelişimi ve kalabalığın dinamik yapısı göz önüne alındığında, tüm katılımcıları kapsayan genel bir görüntü kaydı, suç teşkil eden fiillerin faillerinin belirlenmesi açısından etkili bir araçtır. Sadece şüpheli davranışlar sergileyen kişilerin kaydedilmesi gibi daha sınırlı bir yaklaşım, hem operasyonel açıdan zorluklara yol açacak hem de daha fazla kolluk görevlisi gerektireceğinden, aslında daha müdahaleci bir yöntem olacaktır.

Ayrıca kayıtların yalnızca "şüphelilerin ve suç delillerinin tespiti" amacıyla kullanılabileceğine ilişkin sınırlama ve kayıt işleminin kolluk tarafından yapıldığının açıkça belli olması şartı, gözetimin açık ve şeffaf olması gibi önemli güvenceler sağlamaktadır. Bu kayıtlar bir yandan suç faillerinin tespitini kolaylaştırırken, diğer yandan göstericilere yönelik hak ihlali iddialarının ve varsa kolluk şiddetinin belgelenmesine de hizmet edebilecektir.

Bununla birlikte, gözetleme için kullanılacak araçların niteliği de ölçülülük değerlendirmesinde önem taşımaktadır. Bu araçların sadece kamu düzeninin bozulması tehlikesini ortaya çıkaran olayları ve bunları gerçekleştiren kişileri teşhis etmeyi sağlayacak kalitede olması yeterli ve zorunludur. Bu bağlamda, biyolojik veri işleyen yüz tanıma sistemlerinin kullanılması hem ölçülülük hem de kanunilik ilkelerine aykırı olacaktır. Zira bu tür olayların tespiti için özel nitelikli veri işlemeyi gerektiren bir sistemin kullanılması, görüntü ve ses kaydı gibi daha az bir sınırlama imkânı varken "gereklilik" ilkesiyle bağdaşmayacaktır. Ayrıca kanunda açıkça "görüntü ve ses kaydı" ifadesi kullanılarak işlenebilecek kişisel veriler sınırlandırılmıştır. Yüz tanıma sistemlerinin kişilerin yüz geometrisi, göz mesafesi gibi fiziksel özelliklerini analiz ederek biyolojik veri işlemesi, kanunda öngörülme­yen bir veri işleme faaliyeti anlamına gelecektir.

Öte yandan, Kanunun 11. maddesindeki düzenlemenin en önemli eksikliklerinden biri, elde edilen kayıtların saklanma süresi, erişim yetkileri ve veri güvenliğine ilişkin yeterli güvencelerin öngörülmemiş olmasıdır. Yukarıda da ifade edildiği üzere, AİHM göre, yetkili makamların kişisel verileri topladığı ve işlediği durumlarda, verilerin saklanması, kullanılması ve silinmesini düzenleyen

⁵⁵¹ AİHM, Glukhin / Rusya, B.n.:11519/20, K.t.: 4.10.2023, §77.

açık ve ayrıntılı kuralların varlığı zorunludur⁵⁵². Mahkeme, özellikle gösterilere katılımı ilgili bilgilerin işlenmesinin hassas veri niteliğinde olduğunu ve bu nedenle daha yüksek bir koruma seviyesi gerektirdiğini vurgulamaktadır⁵⁵³.

Bu bağlamda, öncelikle verilerin saklanma süresinin belirlenmemiş olması önemli bir eksikliktir. Kamu düzeninin bozulmasına ilişkin hiçbir olayın gerçekleşmediği toplantı ve gösteri yürüyüşlerine ilişkin kayıtlar için Yönetmeliğin 15. maddesinden faydalanılabilir⁵⁵⁴. Buna göre, kanuna uygun gerçekleşen gösterilere ilişkin raporların 24 saat içinde mülki amire sunulması öngörülmüştür. Bu düzenlemeden hareketle, herhangi bir olay yaşanmayan gösterilere ait görüntü ve ses kayıtları için de kısa bir saklama süresi belirlenebilir. Ancak suç şüphesinin ortaya çıktığı durumlarda kayıtların ne kadar süreyle saklanacağı ayrıca düzenlenmelidir.

Diğer yandan, kayıtlara erişim yetkisinin kapsamı da belirsizdir. Hangi rütbe veya pozisyonundaki görevlilerin kayıtlara erişebileceği, bu yetkinin nasıl kullanılacağı ve denetleneceği konularında açık düzenlemeler bulunmamaktadır. Kayıtların nasıl muhafaza edileceği, üçüncü kişilerin erişimine karşı nasıl korunacağı konusundaki teknik ve idari tedbirlerin Kanunda ya da Yönetmelikte belirlenmemiş olması da bir diğer önemli eksikliktir. Son olarak, ilgili kişilerin kayıtlara erişim ve kayıtların silinmesini talep haklarına ilişkin bir düzenleme de bulunmamaktadır. Halbuki Anayasa'nın 20/3. maddesinde, kişisel verilerin korunmasını isteme hakkının, kişinin kendisiyle ilgili işlenen kişisel veriler hakkında bilgilendirilme, bunlara erişme, bunların düzeltilmesini veya silinmesini isteme gibi hakları da kapsadığı açıkça düzenlenmiştir.

2.3. Kamu Görevlilerine Ait Kişisel Verilerin İşlenmesi

İdarenin kamu görevlilerine ait kişisel verileri işlemesi, modern kamu yönetiminin ve hukuk devleti ilkesinin önemli bir boyutunu oluşturmaktadır. Kamu hizmetinin etkin, verimli ve adil bir şekilde sunulması, idari faaliyetler kapsamında kamu görevlilerine ait kişisel verilerin hukuka uygun şekilde işlenmesini gerektirir. İdarenin insan kaynakları yönetiminin temel unsuru olan kamu görevlileri, vatandaşlara hizmet sunarken devletin yüzü olarak kabul edilir ve bu nedenle onların kişisel verilerinin idare tarafından özenle işlenmesi, kamu hizmetlerinin düzenli işleyişi açısından büyük önem taşır.

İdari faaliyetler kapsamında kamu görevlilerine ait kişisel verilerin işlenmesi, sadece bireysel hakların korunması değil, aynı zamanda idarenin iç işleyişinin düzeni ve kamu yararının da bir gereğidir.

⁵⁵² AİHM, Glukhin / Rusya, B.n.:11519/20, K.t.: 4.10.2023, §77.

⁵⁵³ AİHM, Segerstedt-Wiberg ve diğerleri / İsveç, B.n.:62332/00, K.t.: 6.9.2006, §71-72.

⁵⁵⁴ **Toplantı ve Gösteri Yürüyüşleri Kanununun Uygulanmasına Dair Yönetmelik, Madde 15:** “Kanuna uygun olarak başlayıp biten veya kanuna uygun başlayıp kanunsuz hale dönüşmesi nedeni ile dağıtılan, toplantı ve gösteri yürüyüşleri ile ilgili raporlar, bitimi izleyen 24 saat içinde, tutanaklar da eklenerek (Değişik ibare:RG-5/8/2015-29436) yetkili kolluk amiri tarafından mahallin en büyük mülki amirine sunulur.”

Kişisel verilerin hukuka aykırı şekilde işlenmesi, idarenin personel yönetimini sekteye uğratmanın yanı sıra, kamu görevlilerinin görevlerini bağımsız ve tarafsız bir şekilde yerine getirmelerini de engelleyebilir. Ayrıca, idare tarafından işlenen kişisel verilerin yetkisiz kişilerin eline geçmesi durumunda hem kamu görevlilerinin hem de idarenin itibarı zedelenebilir ve kamu hizmetine olan güven sarsılabilir. Bu nedenle, kamu görevlilerine ait kişisel verilerin işlenmesi, sadece bir veri koruma meselesi değil, aynı zamanda idarenin işleyişi ve kamu hizmetinin kalitesi açısından da bir zorunluluktur.

Bu başlık altında, idarenin kamu görevlilerine ait kişisel verileri işlemesi konusu, idari sürecin farklı aşamalarında ele alınacaktır. İlk olarak, kamu görevine girişte veri işleme kapsamında, 7315 sayılı Kanun çerçevesinde yürütülen güvenlik soruşturması ve arşiv araştırması faaliyetleri incelenecektir. Daha sonra, kamu görevi süresince veri işleme bağlamında, özlük dosyalarının tutulması ve disiplin soruşturmaları sürecindeki veri işleme faaliyetleri değerlendirilecektir.

Konunun sınırlandırılması bakımından, ‘kamu görevlisi’ ifadesiyle kastedilenin de belirlenmesinde fayda bulunmaktadır. Anayasa'nın 128. maddesine göre, devletin genel idare esaslarına göre yürütmekle yükümlü olduğu kamu hizmetleri, memurlar ve diğer kamu görevlileri eliyle gerçekleştirilir. Kamu görevlisi kavramı geniş anlamda kamuda çalışan herkesi kapsarken, idare hukuku bu kavramı dar anlamda ele almaktadır⁵⁵⁵.

Anayasa'nın 68. maddesi, memurlar ve yaptıkları hizmet bakımından işçi niteliği taşımayan kamu görevlilerinin siyasi partilere üye olamayacağını belirtir. Bu bağlamda dar anlamda kamu görevlileri, devletin siyasal yapısını oluşturan organlardaki görevliler ve özel hukuk hükümlerine tabi olarak çalışanlar dışında kalan personeldir.

Asli ve sürekli görev kriteri, kamu görevlilerinin belirlenmesinde yeterli olmadığından, 128. maddedeki "nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve özlük işleri kanunla düzenlenen" personel tanımı daha uygun bir ölçüt olarak kabul edilmektedir⁵⁵⁶. Buna göre, Devlet Memurları Kanunu'nda düzenlenen personel ve özel kanunlarla düzenlenen hakimler, savcılar, silahlı kuvvetler mensupları, yükseköğretim kurumları öğretim elemanları gibi personel dar anlamda kamu görevlisi olarak kabul edilmektedir⁵⁵⁷. Bu başlık altında da dar anlamda kamu görevlilerinin kişisel verilerinin korunması konusu ele alınacaktır.

⁵⁵⁵ AKYILMAZ/SEZGİNER/KAYA, s.664.

⁵⁵⁶ Turan YILDIRIM, “Kamu Görevlilerinin Özel Hayatı: Cinsel Tercih”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.24, S.2, Aralık 2018, ss. 453-481, s.455.

⁵⁵⁷ KAMAN, s.262.

2.3.1. Kamu Görevine Girişte Veri İşleme: Güvenlik Soruşturması ve Arşiv Araştırması

Kamu görevine giriş ya da yeniden atama yapılmasının şartlarından biri de ilgili hakkında güvenlik soruşturması ve arşiv araştırması yapılmasıdır. İdare, soruşturma ve araştırma sırasında ilgili hakkında birçok kişisel veri işlemektedir. İşte bu verilerin de kişisel verilerin korunmasını isteme hakkı bağlamında korunması gerekir. Güvenlik soruşturması ve arşiv araştırması faaliyetleri, kamu kurum ve kuruluşlarına personel alımında gizlilik dereceli bilgilere erişimin uygunluğunun değerlendirilmesi ve özellikle ulusal güvenlik açısından önem taşıyan görevlere atanacak kişilerin incelenmesi amacıyla yürütülmektedir⁵⁵⁸. KVKK'nun 28. maddesinin 1. fıkrasının (ç) bendi, kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinde, KVKK hükümlerinin uygulanmayacağını belirtmektedir. Bu hüküm ışığında, güvenlik soruşturması ve arşiv araştırması faaliyetlerinin, kamu güvenliğini ve ulusal güvenliği sağlamak amacıyla 7315 sayılı Kanunla yetkilendirilmiş kurumlar tarafından yürütülen faaliyetler olduğu ve bu nedenle KVKK'nin koruyucu hükümlerinin kapsamı dışında kaldığı ifade edilmelidir⁵⁵⁹.

Kamu görevine girişte ve belirli görevlere atanmada güvenlik soruşturması ve arşiv araştırması yapılmasını düzenlemek amacıyla kabul edilen 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu 17 Nisan 2021 tarihinde yayımlanarak yürürlüğe girmiştir. Kanunu'nun 1. maddesi, kanunun kapsamını ve düzenlediği konuları genel olarak ortaya koymaktadır. Buna göre, kanun, güvenlik soruşturması ve arşiv araştırması faaliyetlerinin temel çerçevesini belirlemekte, bu faaliyetlerin kimlere uygulanacağını, hangi bilgi ve belgelerin inceleneceğini, elde edilen verilerin ne şekilde kullanılacağını ve hangi kurumların bu süreci yürüteceğini düzenlemektedir. Ayrıca, kanun, Değerlendirme Komisyonu'nun oluşumu ve çalışma usullerini, veri güvenliği ile verilerin saklanma ve silinme sürelerine ilişkin hükümleri de içermektedir.

Söz konusu Kanunun yürürlüğe girmesinden önce güvenlik soruşturması ve arşiv araştırması 4045 sayılı Güvenlik Soruşturması Kanunu⁵⁶⁰ uyarınca yapılmaktaydı. Ancak Kanunun ilgili maddesine ilişkin yaptığı incelemesinde AYM “...kişisel veri niteliğindeki bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına, bu bilgilerin ne suretle ve ne kadar süre ile

⁵⁵⁸ Ömer ÖZKAYA / İbrahim TOPRAK, “Türkiye’de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi”, **Manas Sosyal Araştırmalar Dergisi**, Y.2022, S.11(3), s.1296.

⁵⁵⁹ Kamile TÜRKOĞLU ÜSTÜN, “Güvenlik Soruşturmalarında Kişisel Verilerin Korunması”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. XXV, Y. 2021, S.2, s.807.

⁵⁶⁰ 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun, RG, 26.10.1994/22100.

saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin keyfiliğe izin vermeyecek şekilde belirli ve öngörülebilir kanuni güvenceler belirlenmeksizin güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ile üst kademe yöneticilerinin tespiti yönetmeliğe bırakılmıştır.” gerekçesiyle düzenlemenin Anayasanın 13. ve 20. maddelerine aykırı olduğuna ve bu nedenle iptaline karar vermiştir⁵⁶¹.

Bu karar üzerine kabul edilen 7315 sayılı Kanunda genel olarak AYM kararındaki iptal sebeplerinin gözetilerek düzenleme yapıldığı söylenebilir. Nitekim Kanunun 3. maddesinde belirlenen kişiler hakkında⁵⁶² ve bu Kanunda belirlenen şartlar altında ve yine Kanunda belirlenen kişi veya kurumlar tarafından güvenlik soruşturması ve arşiv araştırması yapılması öngörülmüştür. 7315 sayılı Kanunda bu Kanun kapsamında işlenecek kişisel verilerin korunmasına ilişkin bir bölüme yer verilmiştir. Kanunun 8. maddesine göre güvenlik soruşturması ve arşiv araştırması sürecinde elde edilen ve istihbari faaliyetlere konu olmayan kişisel veriler hakkında ilgisinin bilgilendirilmesi, verilere erişilmesi, bunların düzeltilmesi ve silinmesine ilişkin tedbirlerin alınması öngörülmüştür. Aynı madde uyarınca tutulan verilerin doğru ve güncel olmasının esas olduğu ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü şekilde kullanılacağı kabul edilmiştir. Maddenin son fıkrasında ise 6698 sayılı Kanuna atıfta bulunularak, ilgili Kanunun 4. maddesinde sayılan genel ilkelere göre hareket edilmesi gerektiği düzenlenmiş; bununla birlikte millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni ve ekonomik güvenlik ile ilgili istihbarat faaliyetleri kapsamında elde edilen bilgilerin ilgililere verilmeyeceği kabul edilmiştir. Kanunun 9. maddesinde ise güvenlik soruşturması ve arşiv araştırması yapmakla görevli olan organların veri güvenliğine ilişkin gerekli önlemleri alacağı, sürecin her evresinde gizlilik ilkesine uyulacağı ve Kanun kapsamında elde edilen bilgilerin amacı dışında kullanılamayacağı, 10. maddesinde ise istihbari faaliyete konu olmayan verilerin işlenme amacı ortadan kalktıktan sonra veya her halde iki yılın sonunda silineceği ve yok edileceği kurallarına yer verilmiştir.

⁵⁶¹ AYM, E.2020/24, K.2021/39, T.03.06.2021, §48-49.

⁵⁶² “MADDE 3- (1) Arşiv araştırması, statüsü veya çalışma şekline bağlı olmaksızın ilk defa veya yeniden memuriyete yahut kamu görevine atanacaklar hakkında yapılır. (2) Kurum ve kuruluşlarda, yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Milli Savunma Bakanlığı, Genelkurmay Başkanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ile ceza infaz kurumları ve tutukevlerinde çalışacak personel, kamu kurum ve kuruluşlarında çalışacak öğretmenler, üst kademe kamu yöneticileri, özel kanunları uyarınca güvenlik soruşturması ve arşiv araştırmasına tabi tutulan kişiler ile milli güvenlik açısından stratejik önemi haiz birim, proje, tesis, hizmetlerde statüsü veya çalışma şekline bağlı olmaksızın istihdam edilenler hakkında güvenlik soruşturması ve arşiv araştırması birlikte yapılır.”

Bununla birlikte, Kanunda eleştirilmesi gereken hususların da bulunduğu ifade edilmelidir. 7315 sayılı Kanunu'nun 7. maddesinde öngörülen Değerlendirme Komisyonu, adayın güvenlik soruşturması ve arşiv araştırması sonucunda elde edilen verileri inceleyerek, kişinin göreve atanmasına engel bir durumun olup olmadığına karar vermektedir. Ancak, kanunda, toplanan verilerin hukuka uygunluğunu ve özellikle kişisel verilerin korunmasına ilişkin hükümlere uygun şekilde elde edilip edilmediğini denetleyecek bağımsız bir komisyonun oluşturulması öngörülmemiştir. Bu eksiklik, hukuk devleti ilkesi ve kişisel verilerin korunması hakkı açısından önemli bir sorundur.

Güvenlik soruşturması ve arşiv araştırması kapsamında toplanan verilerin, somut ve kişinin memuriyetine doğrudan etki edecek nitelikte olması (m.5/1) ve KVKK'nin 4. maddesinde sayılan ilkeler doğrultusunda işlenmesi gerektiği kabul edilmiştir (m.8/3). Bu ilkelere uygunluğun sağlanması, eşitlik, şeffaflık ve ölçülülük ilkelerinin hayata geçirilmesi açısından büyük önem taşımaktadır. Ancak kanunda, bu ilkelere uygunluğun nasıl sağlanacağı ve denetleneceği konusunda yeterli düzenlemelerin bulunmaması, keyfi uygulamalara ve hak ihlallerine zemin hazırlamaktadır. Örneğin, 7315 sayılı Kanun'un 5. maddesinde güvenlik soruşturması için *'...kişinin görevine yansiyacak hususların denetime elverişli olacak yöntemlerle yerinden araştırılmak suretiyle tespit edilmesidir'* denilmektedir. Kişinin görevine yansıyan hususların neler olduğu belirsizdir. Eski tarihlerde, bir kişi hakkında mahallinde yapılan araştırmalar, görevli memurların topladığı duyumların bir rapor haline getirilmesi şeklinde gerçekleştirilmiştir. Bu duyumlar için başvuru kaynakları arasında o kişinin komşuları, apartman görevlisi, mahalle bakkalı, muhtarlar, iş arkadaşları ve uğrak yerleri olan kahvehaneler gibi yerler yer almış, bunlara ek olarak, kişinin okuduğu gazeteler ve hatta bıyık stili bile değerlendirme kriteri olarak ele alınmıştır⁵⁶³. Bu tarz bir soruşturma sürecinde, görevli memurların siyasi görüşleri, etik anlayışları, iktidardaki kişilerin memurlar üzerindeki nüfuzu, üstlerine yaranma çabaları gibi faktörlerin yanı sıra, bilgi alınan kişilerin yaklaşımı ve gizliliğin getirdiği sorumsuzluk, ciddiyetsizlik ve rahatlık gibi durumların, hazırlanan raporların objektiflikten uzak olma ihtimalini artırdığı haklı olarak ifade edilmiştir⁵⁶⁴. Günümüzde de bu tehlikeyi önleyecek bir mekanizmanın bulunmadığı düşünülmektedir.

Yönetmelikte⁵⁶⁵, 12. maddenin 3. fıkrasında, güvenlik soruşturması kapsamında elde edilen verilerin değerlendirilmesine ilişkin bir düzenlemeye yer verilmiştir. Buna göre, güvenlik soruşturması sürecinde toplanan bilgi ve beyanlardan, somut olarak gözlemlenemeyen, doğruluğu denetlenemeyen veya iftira, kin ve düşmanlık gibi saiklerle verildiği açıkça anlaşılanların, Değerlendirme Komisyonu'na iletilmeyeceği ve komisyon tarafından dikkate alınmayacağı hükme bağlanmıştır. Ancak, ilgili hükümde 'ayıklama' işleminin kim tarafından yapılacağını belirlenmemiş olması sorundur. Düzenlemelerden anlaşılan, söz konusu 'ayıklama' işleminin de verileri toplayan kişiler tarafından yapılacağıdır. Çünkü

⁵⁶³ Onur KARAHANOGULLARI, "Güvenlik Soruşturması", *Ankara Üniversitesi SBF Dergisi*, Y.1988, S.53(01), s. 165. https://doi.org/10.1501/SBFder_0000001946.

⁵⁶⁴ KARAHANOGULLARI, "Güvenlik Soruşturması", s.165.

⁵⁶⁵ Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik, RG, 3.6.2022/31855.

bu faaliyet için ayrı bir görevlendirme yapılmamıştır. Ancak bu ‘ayıklama’ işleminin, ayıklanacak bilgileri bizzat toplayan kişilerce yapılması hukuk mantığına aykırıdır. Çünkü, söz konusu kişilerin böyle bir yetkinliğe sahip olduğunun kabulü halinde, bu bilgilerin başlangıçta toplanmaması, kayıt altına alınmaması gerekirdi. Bu nedenle, toplanan tüm verilerin, KVKK ilkelerine uygun şekilde işlendiğinin bağımsız bir komisyon tarafından denetlenmesi, kişisel verilerin korunması hakkının etkin bir şekilde hayata geçirilmesi için gereklidir. Bu denetim görevi, kanunla oluşturulan Değerlendirme Komisyonu'na verilebilir. Ancak, komisyonun, kanuna aykırı şekilde elde edilen verileri ayıklaması durumunda dahi, bu verilerin değerlendirme sürecinde zihinlerde yer etmesi, objektif bir karar verilmesini güçleştirecektir. Dolayısıyla, ilgili bilgileri toplayan görevliler ile Değerlendirme Komisyonları arasında, toplanan bilgi ve beyanlardan somut olarak gözlemlenemeyen, doğruluğu denetlenemeyen veya iftira, kin ve düşmanlık gibi saiklerle verildiği açıkça anlaşılanlar ile kişisel verileri koruma mevzuatına aykırı şekilde elde edilen verileri ayıklamakla görevli üçüncü bir kurul ihdas edilmesi kamu görevlilerinin haklarını koruma noktasında en doğru yöntem olacaktır.

Yine, Kanunun 8. maddesinin 1. fıkrasında, güvenlik soruşturması ve arşiv araştırmasına yönelik olarak işlenen kişinin kendisiyle ilgili kişisel verileri hakkında bilgilendirilmesi, bu verilere erişmesi, bunların düzeltilmesi ve silinmesi taleplerine ilişkin tedbirlerin alınacağı belirtilmektedir. Ancak, bu hükmün uygulanmasına yönelik usul ve esaslar, bilgilendirmenin ne zaman yapılacağı, itirazların nasıl değerlendirileceği gibi hususlar açıkça düzenlenmemiştir. Ayrıca, istihbari faaliyetlere konu olan bulguların bu hakkın kapsamı dışında tutulması, kişinin kendi verileri üzerindeki kontrolünü önemli ölçüde sınırlandırmaktadır.

Sonuç olarak, 7315 sayılı Kanun'un kişisel verilerin korunması açısından önemli eksiklikler içerdiği, bağımsız denetim mekanizmalarının bulunmaması, usuli güvencelerin yetersizliği ve istihbari faaliyetlere ilişkin verilerin kapsam dışı bırakılması nedeniyle, kişisel verilerin korunması hakkını etkin bir şekilde korumadığı ifade edilmelidir.

2.3.2. Kamu Görevi Süresince Veri İşleme

2.3.2.1. Özlük Dosyalarında İşlenen Kişisel Veriler

Kamu görevlilerinin görevleri yaptığı süre boyunca genel ve özel nitelikli birçok kişisel verisi İdare tarafından özlük dosyası içerisinde düzenli olarak işlenmektedir. Söz konusu veri işleme faaliyeti, KVKK'nun 28. maddesinde sayılan istisna hallerinden biri olmadığından bu Kanun kapsamında korunmaktadır. İdare, Kanunun genel nitelikli verilere ilişkin 5. maddesinde yer alan kanunlarda açıkça öngörülme (f. 2/a) ve hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması şartları (f. 2/ç), özel nitelikli veriler içinse 6. maddede sayılan kanunlarda açıkça öngörülme (f. 3/a) ve istihdam ve sosyal güvenlik alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması (f. 3/f) şartlarına dayanarak bu verileri işleyebilmektedir.

Nitekim, 657 sayılı Devlet Memurları Kanunu'nun 109. maddesine göre, Devlet memurlarının özlük bilgileri, Türkiye Cumhuriyeti kimlik numaralarına göre ilgili kurumlarca tutulan personel bilgi sistemlerinde kayıt altına alınır. Her bir memur için ayrı bir özlük dosyası oluşturulur ve bu dosyada memurun mesleki bilgileri, mal bildirimleri, hakkında yapılan inceleme, soruşturma ve denetim raporları, disiplin cezaları, ödül ve başarı belgeleri gibi bilgi ve belgeler yer alır. İlgili hükümde, memurların başarı, yeterlik ve ehliyetlerinin belirlenmesinde, kademe ilerlemeleri ve derece yükselmelerinde, emekliye ayrılma süreçlerinde veya hizmet ilişkilerinin sona erdirilmesinde, hizmetin gerekleri ile birlikte özlük dosyalarının da dikkate alınacağı belirlenmiştir. Özlük dosyalarının nasıl tutulacağı ve bu dosyalarda hangi belgelerin yer alacağına ilişkin usul ve esasların ise Devlet Personel Başkanlığı tarafından belirleneceği kuralına yer verilmiştir.

Devlet Personel Başkanlığı'nca çıkarılan Tebliğin⁵⁶⁶ 'Özlük Dosyası Tutulmasına İlişkin Usul ve Esaslar' başlıklı bölümde konuya ilişkin esaslara yer verilmiştir. Buna göre özlük dosyasında memurun adı soyadı, T.C. kimlik numarası, cinsiyeti doğum tarihi ve yeri, öğrenimi, kadro unvanı ve derecesi gibi kişisel verileri ile sendika üyeliği ve özürzlülük durumuna ilişkin sağlık belgeleri gibi özel nitelikli verilerin işlenmesi öngörülmüştür.

Mezkûr tebliğde, özlük dosyalarının itina ile doğru ve tarafsız şekilde tutulmasından personel birimleri sorumlu tutulmuş, dosyaların tutulmasında ve korunmasında özel hayatın gizliliği ilkesine uygun hareket edileceği, içeriği hakkında yalnızca soruşturma ve kovuşturmayla yetkili mercilere açıklama yapılacağı ve kişinin rızası olmaksızın dosyada bulunan bilgi ve kayıtlar kullanılarak herhangi bir yayın yapılmayacağı belirlenmiştir.

657 sayılı Kanun düzenlemesi ve buna ilişkin çıkarılan Tebliğ hükümleri düşünüldüğünde, bu düzenlemelerde, KVKK'da belirlenen veri koruma kurallarından bazılarının aykırılıklarının bulunduğu ifade edilmelidir. İlk olarak, veri işleme ilkelerinden biri, işlenen verilerin işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesidir. Ancak, özlük dosyasında tutulacak bilgilere ilişkin olarak Tebliğ'de, özlük dosyasının 8 bölümden oluşacağı, 4. bölümde memur hakkında yapılan disiplin soruşturmalarına ilişkin evraklar ile verilen disiplin cezaları, yargı organlarınca memur hakkında verilmiş karar örnekleri, görevden uzaklaştırmaya ilişkin belgeler ile varsa inceleme, soruşturma ve denetim raporlarının tutulacağı belirlenmiştir. Buna göre hem disiplin soruşturmaları hem de disiplin cezalarına ilişkin evraklar tutulacaktır. Disiplin cezalarının silinmesine ilişkin süreler 657 sayılı Kanunun 133. maddesinde düzenlenmiş olup, uyarma ve kınama cezaları için 5 yıl, diğer cezalar içinse 10 yıl geçmesinden sonra atamaya yetkili amire başvurularak cezaların özlük dosyasından silinmesinin istenebileceği öngörülmüştür. Bununla birlikte, soruşturma başlatılıp da ceza verilmeyen dosyalara ilişkin Kanunda herhangi bir silinme süresi belirlenmemiştir.

⁵⁶⁶ Kamu Personeli Genel Tebliği (Seri No:2), RG, 15.4.2011/27906.

Bu konuya ilişkin olarak KVK Kurulu’na yapılan şikayetlerde Kurul, Devlet Arşiv Hizmetleri Hakkında Yönetmelik⁵⁶⁷ düzenlemesini işaret etmektedir. Bir kararında Kurul, mülga Devlet Arşiv Hizmetleri Hakkında Yönetmelik’in⁵⁶⁸ 3. maddesinde “arşiv malzemesi” ve “arşivlik malzeme” kavramlarının tanımlandığını, son işlem tarihi üzerinden yüz bir yıl geçmemiş memuriyet sicil dosyalarının arşivlik malzeme olarak kabul edildiğini; bununla birlikte sonradan çıkarılan Yönetmelik’te sicil dosyalarının arşivlik belge olarak tanımlanmadığını ve yüz bir yıl içerisinde silineceğine ilişkin bir kurala yer verilmediğini, bu sebeple bunların imha işlemine tabi tutulmadığını değerlendirerek, özlük dosyasına saklanan ceza dosyasının dosyadan çıkarılmasına ilişkin talebin kabul edilebilir olmadığına karar vermiştir⁵⁶⁹. Bu karardan anlaşılan, mevcut mevzuat uyarınca, özlük dosyalarında bulunan evraklar, disiplin cezalarına ilişkin 657 sayılı Kanun düzenlemesi hariç, hiçbir şekilde silinmeyecektir. Ancak bu durum kişisel verilerin işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkesine açıkça aykırıdır⁵⁷⁰.

Öte yandan, verilen disiplin cezalarının özlük dosyasından silinmesine ilişkin usulü düzenleyen 657 sayılı Kanunun 133. maddesi de eleştiriye açıktır. Nitekim hüküm, memurun silinme talebinin haklı görülmesi halinde isteğin yerine getirilmesine karar verilerek bu kararın özlük dosyasına işleneceği öngörülmüştür. Maddede ‘ilgili dosya imha edilir’ ya da ‘yok edilir’ gibi bir ibare yerine silinmesi talebinin yerine getirilmesine ilişkin kararın dosyaya işlenmesinden bahsedilmektedir. Özlük dosyasının tutulmasına ilişkin ayrıntıları düzenleyen ilgili tebliğ düzenlemesinde de bu hususa ilişkin bir açıklama bulunmadığına göre, aslında dosya yok edilmemekte, sadece talebin kabulü işlenmektedir. Özlük dosyalarının, kamu görevlilerinin “başarı, yeterlik ve ehliyetlerinin tespitinde, kademe ilerlemelerinde, derece yükselmelerinde, emekliye ayrılmalarda ve hizmetle ilişkilerinin kesilmesinde göz önünde bulundurulması” kabul edildiğinden, sürekli şekilde dosyada tutulan evrakların, haklarında silinme kararı verilmiş olursa bile bu değerlendirmelerde etkili olacağı inkâr edilemez. Dolayısıyla, KVKK’nin 7. maddesinde veri sahiplerine tanınan kişisel verilerin silinmesini isteme hakkının mevcut düzenlemeyle karşılanmadığı görülmektedir.

⁵⁶⁷ RG, 18.10.2019 / 30922.

⁵⁶⁸ RG, 16.5.1988 / 19816.

⁵⁶⁹ KVK Kurulu, 20.5.2020 tarih ve 2020/396 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6912/2020-396> (E.T.10.8.2024). 2019 tarihli Devlet Arşiv Hizmetleri Yönetmeliği’nin yürürlüğe girmesinden önce de Kurul, memuriyet döneminde haklarında açılan inceleme ve soruşturma dosyalarına ilişkin evrakların imha edilmesine yönelik şikâyet üzerine mülga yönetmelikteki yüz bir yıllık süreyi işaret ederek şikâyetçinin talebinin veri sorumlusunca karşılanmamasını hukuka uygun bulmuştur: KVK Kurulu, 28.6.2018 tarih ve 2018/69 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/5366/2018-69> (Erişim Tarihi: 10.8.2024).

⁵⁷⁰ Avrupa Veri Koruma Denetçisi tarafından hazırlanan İdari Soruşturmalar ve Disiplin İşlemlerinde Kişisel Bilgilerin İşlenmesine İlişkin Kılavuz’da her bir olayın sonucuna göre soruşturma ya da disiplin dosyalarında tutulan kişisel bilgiler için orantılı saklama sürelerinin benimsenmesi gerektiği ifade edilmiştir. Örneğin, herhangi bir şikâyet olmaksızın elde edilen bazı bilgiler nedeniyle başlatılan ön idari soruşturmanın herhangi bir disiplin işlemi öngörülmeden kapatılması halinde ilgili dosyadaki bilgilerin, denetim amacıyla en fazla iki yıl saklanması öngörülmüştür. European Data Protection Supervisor (EDPS), “Guidelines on processing personel information in administrative inquiries and disciplinary proceedings”, 18.11.2016, https://www.edps.europa.eu/sites/default/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf (E.T. 10.8.2024).

Bununla birlikte, tüm memurlar için öngörülen bu düzenlemenin sınırlandırılarak, sadece üst düzey yönetici, istihbarat ve özellikli bazı kamu görevlerinde bulunan memurlar bakımından uygulanması da kararlaştırılabilir. Nitekim, 7315 sayılı Kanunda arşiv araştırmasının kamu görevine alınacak herkes için yapılacağı, arşiv araştırması ile güvenlik soruşturmasının ise belirlenen bazı görevlere atanan kamu görevlileriyle sınırlı olarak yapılacağı öngörülmüştür⁵⁷¹. Benzer bir hükmün özlük dosyaları için öngörülerek, işlenen evrakların niteliğine göre yok edilmesi için belli süreler öngörüldükten sonra özellik arz eden görevlerde bulunanlar için daha uzun süreler kararlaştırılabilir.

Değinilmesi gereken bir başka husus ise, Devlet Personel Başkanlığı'nca çıkarılan Tebliğ'de özlük dosyasında tutulacak bilgiler sayıldıktan sonra *'...diğer mesleki bilgiler kaydedilir'*, *'yukarıdaki bölümler kapsamına girmeyen memurun hizmet durumuna ilişkin diğer mesleki bilgi ve belgeler'* şeklindeki ifadelerin durumudur. Bu ifadelerde, toplanacak verilerin memurun mesleki faaliyetlerine ilişkin olanlarla sınırlandırılması, keyfiligi önleyecek türden bir düzenleme olduğu kanaatini uyandırmaktadır. Fakat, bir KVK Kurul kararında yer verilen Devlet Personel Başkanlığı görüşü bu kanaatin aksini yansıtmaktadır. Kararda, mezkur Tebliğ'de özlük dosyasında tutulacak evraklar arasında sayılan *"yargı organlarınca memur hakkında verilmiş karar örnekleri"* ibaresinin ne anlama geldiğine yönelik Kurul tarafından Başkanlık'a görüş sorulduğu, Başkanlık tarafından verilen cevapta ise *"Mezkûr Tebliğde memurun özlük dosyasının sekiz bölümden oluştuğu belirtilmekte, bölümlerde hangi konulara ilişkin belgelerin yer alması gerektiği hususu düzenlenmekte olup, özlük dosyasında yer alan her bir bölüme ilişkin belgelerin tek tek zikredilmesinin mümkün bulunmadığı, kurumlarca lüzum görülen tüm belgelerin ilgili bölümlere konulmasının uygun olacağı, dosyanın dördüncü bölümünde memurun yalnızca çalışma hayatına ilişkin değil yargı organlarınca memur hakkında verilen tüm karar örneklerinin bulunması gerektiği değerlendirilmektedir"* şeklinde görüş bildirdiği ifade edilmektedir⁵⁷².

İlgili ifadenin bu geniş yorumu kişisel verilerin korunmasını isteme hakkının ölçsüz şekilde sınırlanması anlamına gelmektedir. Her kamu görevlisinin memurluk mesleğinde yükselmesini engelleyen ya da disiplin cezası almasını gerektiren bazı fiil ve davranışlarına ilişkin yargı kararlarının özlük dosyasında tutulması makul kabul edilebilir. Ancak, bir istihbarat çalışanın evlenip boşanması İdare için önem arz edebilirse de söz gelimi bir ilçe nüfus müdürlüğündeki personelin boşanma evrakının

⁵⁷¹ Madde 3- (1) Arşiv araştırması, statüsü veya çalışma şekline bağlı olmaksızın ilk defa veya yeniden memuriyete yahut kamu görevine atanacaklar hakkında yapılır. (2) Kurum ve kuruluşlarda, yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Milli Savunma Bakanlığı, Genelkurmay Başkanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ile ceza infaz kurumları ve tutukevlerinde çalışacak personel, kamu kurum ve kuruluşlarında çalışacak öğretmenler, üst kademe kamu yöneticileri, özel kanunları uyarınca güvenlik soruşturması ve arşiv araştırmasına tabi tutulan kişiler ile milli güvenlik açısından stratejik önemi haiz birim, proje, tesis, hizmetlerde statüsü veya çalışma şekline bağlı olmaksızın istihdam edilenler hakkında güvenlik soruşturması ve arşiv araştırması birlikte yapılır.

⁵⁷² KVK Kurulu, 20.5.2020 tarih ve 2020/396 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6912/2020-396> (E.T.10.8.2024).

İdare için aynı kıymette olduğu düşünülemez. Dolayısıyla, özlük dosyasında tutulacak veriler bakımından da icra edilen kamu görevinin mahiyetine göre bir ayırım yapılması gerekmektedir.

2.3.2.2. Disiplin İşlemleri Sürecinde İşlenen Kişisel Veriler

Disiplin soruşturması sürecinde İdare tarafından işlenen kişisel veriler, soruşturmanın selameti ve ilgililerin temel hak ve özgürlüklerinin korunması bakımından büyük önem taşımaktadır. Zira soruşturma sürecinde elde edilen deliller, tanık beyanları, bilirkişi raporları gibi belgeler kişisel veri niteliğindedir. Ayrıca disiplin suçu isnadı altında bulunan kamu görevlisinin savunması ile lehe ve aleyhe deliller de yine kişisel veri kapsamındadır. Dolayısıyla disiplin soruşturması sürecinde İdarenin veri sorumlusu sıfatıyla kişisel verileri hukuka ve dürüstlük kurallarına uygun olarak, belirli, açık ve meşru amaçlar için işlemesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması gerekmektedir.

Diğer taraftan, disiplin soruşturması ve kovuşturması bir ceza soruşturması niteliğinde olmamakla birlikte soruşturmanın gizliliği ilkesi burada da geçerli kabul edilmektedir⁵⁷³. Soruşturmanın gizliliği ilkesi kişisel verilerin korunması yönünden de önem arz etmektedir. Öyle ki soruşturma sürecinde elde edilen kişisel verilerin gizliliğinin ve güvenliğinin sağlanması, yetkisiz erişim ve ifşalara karşı gerekli teknik ve idari tedbirlerin alınması gerekmektedir. Keza disiplin suçu isnadı altında bulunan kamu görevlisinin lekelenmeme hakkı ve masumiyet karanesi de kişisel verilerin korunması ile yakından ilgilidir. Disiplin soruşturmasının gizliliği ilkesine aykırı olacak şekilde soruşturma kapsamında elde edilen kişisel verilerin ifşa edilmesi, bir yandan ilgilinin itibarını zedeleyecek diğer taraftan masumiyet karanesini ihlal edecektir.

Disiplin işlemleri sürecinde İdare tarafından işlenen kişisel veriler KVKK'nun kısmen uygulanmadığı bir alandır. Kanunun 28/2(c) maddesinde, disiplin soruşturma ve kovuşturması için gerekli olması halinde işlenen veriler hakkında *“Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz”* kuralına yer verilmiştir.

Disiplin işlemlerinde işlenen veriler hakkında KVKK'nun kısmen uygulanmamasına ilişkin hüküm, uluslararası kurallara da uygun düşmektedir. AİHS'in 8. maddesi özel hayatın ve aile hayatının korunması hakkını düzenlemekte, bu kapsamda kişisel verilerin korunmasını da güvence altına almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), 8. maddenin ihlal edildiği iddiasıyla önüne gelen

573 Ceza yargılaması ilkelerinin disiplin soruşturmalarında uygulanması gerektiğinin Danıştay kararlarında da kabul gördüğüne dair bkz.: Gül FİŞ ÜSTÜN, “Disiplin Soruşturmalarında Hukuka Aykırı Deliller”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.24, S.1, Haziran 2018, s.20.

başvurularda, kamu makamlarının keyfi ve orantısız müdahalelerine karşı bireyleri koruyan bir içtihat geliştirmiştir. Ancak AİHM, meşru bir amaç güden, kanunla öngörülen ve demokratik bir toplumda gerekli olan müdahalelerin, 8. maddeyi ihlal etmeyeceğini kabul etmektedir⁵⁷⁴. Bu bağlamda, disiplin soruşturmaları gibi meşru bir amaca dayanan ve kanuni düzenlemeye konu olan kişisel veri işleme faaliyetlerinin de AİHS'e aykırılık oluşturmadığı söylenebilir. Önemli olan, soruşturmalarda ölçülülük ilkesine riayet edilmesi ve keyfilğe kaçılmamasıdır.

Öte yandan, GDPR'ın 6. maddesinde kişisel verilerin işlenmesinin hukuka uygun olduğu haller sayılmış, 23. maddesinde ise üye ülkelerin bazı istisnalar getirebilmesine imkân tanınmıştır. Bu maddeye göre üye ülkeler, önlemlerin demokratik bir toplumda gerekli ve orantılı olması kaydıyla, ulusal güvenlik, savunma, kamu güvenliği, suç ve etik ihlallerin soruşturulması, yaptırım uygulanması gibi belirli amaçlarla GDPR hükümlerine istisna ve sınırlamalar öngörebilirler. Dolayısıyla GDPR, AİHS içtihadına benzer şekilde, disiplin soruşturmaları gibi meşru amaçlarla ve belirli güvenceler dâhilinde yürütülen kişisel veri işleme faaliyetlerine olanak tanımaktadır⁵⁷⁵.

657 sayılı Devlet Memurları Kanunu'nun 124. maddesi, kamu hizmetlerinin gereği gibi yürütülmesini sağlamak amacıyla, kanunların, Cumhurbaşkanlığı kararnamelerinin ve yönetmeliklerin Devlet memurlarına verdiği görevleri yurt içinde veya dışında yerine getirmeyen, uyulması zorunlu kılınan hususlara uymayan veya yasaklanan işleri yapan memurlara, durumun niteliği ve ağırlık derecesine göre 125. maddede belirtilen disiplin cezalarından birinin verileceğini ifade etmektedir. Kanunun 127. maddesi ise, 125. maddede belirtilen fiil ve halleri işleyen kişiler hakkında, bu durumun öğrenildiği tarihten itibaren belirli süreler içinde disiplin soruşturması veya kovuşturmasına başlanması gerektiğini belirtmektedir. Buna göre, uyarma, kınama, aylıktan kesme ve kademe ilerlemesinin durdurulması cezaları için bir ay içinde disiplin soruşturmasına başlanmazsa, memurluktan çıkarma cezası için ise altı ay içinde disiplin kovuşturmasına başlanmazsa, disiplin cezası verme yetkisi zamanaşımına uğrar. Yine Devlet Memurları Disiplin Yönetmeliği'nin⁵⁷⁶ 28. maddesinde, soruşturma açılmaksızın memur hakkında disiplin cezasının verilemeyeceği kabul edilmiştir. Söz konusu hükümlerden hareketle İdarenin, disiplin işlemleri süresince kanunlarda açıkça öngörülme ve hukuki

⁵⁷⁴ Örneğin, Leander/İsveç davasında, başvuran, güvenlik gerekçesiyle hakkında tutulan gizli dosyaya erişemediğinden ve dosyadaki iddiaları cevaplamak için kendisine fırsat verilmediğinden şikayetçi olmuştur. AİHM, gizli polis kaydı tutulmasının, özellikle de terörle mücadele bağlamında ulusal güvenlik amacına hizmet ettiğini ve bu nedenle meşru bir amaç taşıdığını belirtmiştir. Bununla birlikte, bu tür kayıtların tutulmasının kanunla öngörülmesi ve keyfilğe karşı yeterli güvencelerin sağlanması gerektiğine işaret etmiştir. Sonuç olarak, İsveç hukukunun başvuranın haklarını yeterince koruduğuna hükmederek, AİHS'in 8. maddesinin ihlal edilmediğine karar vermiştir. AİHM, Leander / İsveç, B.n. 9248/81, T.26.3.1987, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57519%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}).

⁵⁷⁵ GDPR bağlamında memurların kişisel verilerinin işlenmesine ilişkin inceleme için bkz.: Atilla ERKAL, “Avrupa Genel Veri Koruma Düzenlemesi Bağlamında Memurların Kişisel Verilerinin Korunması Hakkı” **Anayasa Yargısı**, C.37, S.2, Y.2020, s.205-253.

⁵⁷⁶ Devlet Memurları Disiplin Yönetmeliği, RG, 30.4.2021/31470.

yükümlülüklerin yerine getirilmesi için zorunlu olma şartlarına dayanarak kişisel veri işleyebileceği kabul edilmelidir.

Disiplin soruşturma ve kovuşturmalarında en önemli hususlardan biri, ilgili memurun kendisi hakkında toplanan bilgi ve belgelere erişmesi sorunudur. 6698 sayılı Kanun'un 11. maddesinde kişisel verilerinin işlenip işlenmediğini öğrenme ve bunlar hakkında bilgi talep etme ilgili kişinin hakları arasında sayılmışsa da Kanunun 28/2. maddesinde zararların giderilmesini isteme hakkı hariç 11. maddede sayılan hakların kullanılamayacağı kuralı kabul edilmiştir. Ancak, memura Anayasal bir hak olarak tanınan savunma hakkının (AY m.129/2) etkin bir şekilde kullanılabilmesi için kendisi hakkında hazırlanan dosyaya erişmesinin kabulü gerekir⁵⁷⁷. Yine 657 sayılı Kanun'un 130. maddesinde de savunma alınmadan memura ceza verilemeyeceği kabul edilmiştir. 4982 sayılı Bilgi Edinme Kanunu'nun 5. maddesinde de Kanunda yer alan istisnalar dışında tüm bilgi ve belgelerin başvurulara verilmesi kuralı kabul edilmiş, 19. maddesinde ise hangi hallerde idari soruşturmaya ilişkin bilgi ve belgelerin verilemeyeceği belirlenmiştir.

4982 sayılı Kanunun 19. maddesine göre, söz konusu bilgi veya belgelerin açıklanması veya zamanından önce açıklanması durumunda; kişilerin özel hayatına açıkça haksız müdahale sonucunu doğuracak, kişilerin veya soruşturmayı yürüten görevlilerin hayatını ya da güvenliğini tehlikeye sokacak, soruşturmanın güvenliğini tehlikeye düşürecek, gizli kalması gereken bilgi kaynağının açığa çıkmasına neden olacak veya soruşturma ile ilgili benzeri bilgi ve bilgi kaynaklarının temin edilmesini güçleştirecek nitelikte olması halinde, bu bilgi veya belgeler Kanun kapsamı dışında tutulacaktır.

Yukarıda sayılan mevzuat hükümleri karşısında, ilgililerin talebi doğrultusunda, savunma hakkının etkin biçimde kullanılmasını tesis etmek amacıyla, idari soruşturma dosyaları kendilerine ya da vekillerine verilirken hem dosyanın akıbetinin sekteye uğramaması hem de dosya içerisinde yer alan şikâyet sahibine, ifadeleri alınan kişilere ve diğer üçüncü kişilere ait kişisel verilerin korunması amacıyla birtakım karartmalar yapılması yerinde olacaktır. Nitekim 4982 sayılı Kanunun 9. maddesinde, talep edilen bilgilerde gizli ve açıklanması yasak olanlar ile açıklanabilir nitelikte olanların birlikte bulunması halinde, bunlar ayrılabilirse, ilgili belgeden gizli ve açıklanması yasak olan bilgilerin çıkarılarak talep eden kişiye sunulması gerektiği düzenlenmiştir.

Bilgi Edinme Değerlendirme Kurulu'na yapılan bir başvuruda, hakkında üniversite tarafından başlatılan soruşturmaya yönelik savunma için dosyanın bir örneğinin kendisine verilmesi talebinin üniversite tarafından reddedilmesi hakkında Kurul, başvuru sahibinin itirazına konu olan taleplerinin, kendisi hakkındaki "Disiplin Soruşturması" dosyasında bulunan bilgi ve belgelere yönelik olduğunu dikkate alarak, soruşturmanın tamamlanmış olması halinde başvuranın söz konusu verilere erişiminde

⁵⁷⁷ Sencer Abdullah AKKOYUNLU, "Disiplin Soruşturmasında Memurun Savunma Hakkının Kullanımında İdarenin Uyması Gereken Esaslar", **DÜHFD**, C.28, S.48, Y.2023, s. 19 vd.

güncel, somut, meşru ve kişisel menfaatinin bulunduğunu ifade etmiştir. Kurul, başvuru sahibi tarafından talep edilen belgelerin çalışma hayatına ve mesleki onuruna ilişkin olduğunu ve bu belge ve bilgilere erişimin, anayasal bir hak olan hak arama hürriyetinin kullanılabilmesi bakımından gerekli ve zorunlu olduğunu belirtmiştir. Ayrıca, Anayasa'nın 36. maddesinde güvence altına alınan silahların eşitliği ve çelişmeli yargılama ilkelerine uygun olacağı gerekçesine de dayanarak, başvuru sahibinin taleplerinin demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak bilgi edinme hakkının kullanımı kapsamında olduğuna karar vermiştir. Ancak, 4982 sayılı Bilgi Edinme Hakkı Kanununun 19. maddesinin (a) ve (d) bentleri gereğince, soruşturmanın tamamlanmış olması halinde, "Disiplin Soruşturması" dosyasında bulunan bilgi ve belgelerin, özel hayatın korunmasına riayet edilerek üçüncü şahıslara ait kimlik bilgileri ile kimliklerinin tespitine imkân veren her türlü bilgi ve ifadenin karartılması gerektiğini vurgulamıştır. Ayrıca, ifade tutanakları ile tanık ifadeleri, gizli kalması gereken bilgi kaynağının açığa çıkmasına neden olacak veya soruşturma ile ilgili benzeri bilgi ve bilgi kaynaklarının temin edilmesini güçleştirecek bilgi veya belgeleri içeren kısımların çıkartılması veya kapatılması suretiyle, söz konusu kanunun 5. maddesi gereğince kendisiyle ilgili bilgilerin başvuru sahibinin erişimine sunulması gerektiğini ifade etmiştir⁵⁷⁸.

Öte yandan, şikayetçisi olduğu bir soruşturmaya ait tüm evrakların kendisine verilmesini isteyen başvurana, ilgili İdare tarafından yalnızca soruşturma raporu ve Bakan onayının şikayetçiyi ilgilendiren bölümleri verilmesi üzerine, şikayetçi Bilgi Edinme Değerlendirme Kurulu'na başvurmuştur. Kurul, 4982 sayılı Kanunun 19. maddesinde belirlenen, kişilerin özel hayatına açıkça haksız müdahale teşkil etmesi (a bendi) ve gizli kalması gereken bilgi kaynağının açığa çıkmasına neden olacak veya soruşturma ile ilgili benzeri bilgi ve bilgi kaynaklarının temin edilmesini güçleştirecek nitelikte olması (d bendi) hükümlerine dayanarak başvuruyu reddetmiştir⁵⁷⁹.

Başka bir karara konu olayda başvuran, bir vakıf üniversitesinde asistan olarak görev yapan ilgili şahıs hakkında yapmış olduğu ihbar ve bilgilendirmelerin ne şekilde işlem gördüğü, soruşturma açılıp açılmadığı, açıldıysa ne şekilde sonuçlandığı ve bu kararların ilgili kurum ve kuruluşlara gönderilip gönderilmediğine ilişkin bilgileri ve açılan disiplin soruşturmalarına ilişkin belgelerin kendisine verilmesini talep etmiştir. Üniversite, 4982 sayılı Kanunun 21. maddesindeki kural gereği, talep edilen bilgi ve belgelerin talep eden verilmesinin ilgili kişinin özel hayatına, şeref ve haysiyetine haksız müdahale niteliği taşıyacağından talebi reddetmiştir. Ancak Kurul, talep edilen bilgilerin başvuranın olayın şikayetçisi olduğu gerekçesiyle 21. madde kapsamında bulunmadığına ve erişimine

⁵⁷⁸ BEDK, 28.9.2022 tarih ve 2022/1257 sayılı kararı.

⁵⁷⁹ BEDK, 2.12.2020 tarih ve 2020/1731 sayılı kararı. Başvuru sahibinin talep ettiği bilgi ve belgelerden 'Kendisinin Banka hakkında asılsız iddialarda bulunduğu dair TBMM Soruşturma Komisyonunca Ziraat Bankasına yazılan yazı ve raporun' 4982 sayılı Kanunun 19/c maddesinde yer alan 'soruşturmanın güvenliğini tehlikeye düşürecek' nitelikte olmadığı gibi aynı Kanunun 22. maddesinde yer alan 'haberleşmenin gizliliği' başlıklı maddeyle de ilgisi bulunmadığına, bu sebeple talebin yerine gerektiğine dair BEDK, 20.9.2004 tarih ve 2004/82 sayılı kararı.

açılması gerektiğine; açılmış olan disiplin soruşturmasına ilişkin belgelerinse 19. madde kapsamında değerlendirilmek üzere Kurula gönderilmesine karar vermiştir⁵⁸⁰.

Öte yandan, ilgili 4982 sayılı Kanunun bilgi edinme hakkının sınırlandırılmasına ilişkin hükümleri nedeniyle vakıf olamadığı bilgi ve belgeleri, ilgili idari işleme karşı dava açması halinde görebilmesi muhtemeldir. Söz gelimi, hakkında tesis edilen disiplin işlemine karşı süresi içinde dava açması halinde mahkeme, işleme konu bilgi ve belgeleri İdareden talep edeceğinden, ilgili de dava dosyasında bunları görebilir. Nitekim, 2577 sayılı Kanunun 20. maddesi uyarınca İdare davaya ilişkin kendisinden talep edilen bilgi ve belgeleri mahkemeye iletmek zorundadır. Davacının, bu bilgi ve belgeleri görmesi ve gerekli itirazlarda bulunması adil yargılanma hakkının bir gereğidir. Nitekim Danıştay bir kararında *“Davacılar ancak soruşturma raporunda yer verilen maddi olayı, tanık ifadelerini, inceleme yapanın görüş ve kanaatini, işlemin hukuki dayanağını, soruşturmacının önerilerini açık ve etraflı bir biçimde öğrenme suretiyle adil yargılanma hakkını kullanabilecektir. İncelenemeyen bir soruşturma raporuna karşı iddia ve savunmada bulunulamaz...Bu durumda makul bir süre verilmek suretiyle, davacıya hakkında düzenlenen soruşturma raporu ve eklerini incelemesi ve istemi halinde raporla ilgili görüşlerini dosyaya sunması olanağı sağlandıktan sonra işin esası hakkında yeniden bir karar verilmesi gerekmektedir.”* yönünde karar vermiştir⁵⁸¹.

3. İDARENİN KİŞİSEL VERİ İŞLEMESİNDEN DOĞAN HUKUKİ SORUMLULUĞU

6698 sayılı Kanun’un 14/3. maddesinde kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkının saklı olduğu kabul edilmiştir. Buna göre, kişisel verilerinin İdare tarafından işlenmesi ya da hukuka aykırı şekilde işlenmesi dolayısıyla zarar gören kişi, veri sorumlusu İdareye karşı zararlarının tazmini için dava açabilecektir. Nitekim, Anayasanın 125. maddesinin ilk fıkrasında İdarenin her türlü eylem ve işlemlerine karşı yargı yolunun açık olduğu düzenlenmiş, son fıkrasında İdarenin kendi eylem ve işlemlerinden doğan zararları ödemekle yükümlü olduğu kuralı kabul edilmiştir. Bununla birlikte, İdare aleyhine tazminata hükmedilebilmesi için İdarenin bu zarardan kusurlu ya da kusursuz sorumlu tutulabilmesi gerekir.

Kusur, kamu hizmetlerindeki nesnel eksiklik veya bozukluktur. Hizmet kusuru ise idarenin kamu hizmetlerinin işleyişindeki anonim ve nesnel kusurları ifade eder. Başka bir deyişle, kamu hizmeti

⁵⁸⁰ BEDK, 9.11.2005 tarih 2005/794 sayılı kararı.

⁵⁸¹ Danıştay 16.D., E.2015/10952, K.2015/1795, aktaran: KAMAN, s.329. Kişisel verilerin korunması ile bilgi edinme hakkı arasındaki denge, idari yargılama sürecinde özel bir görünüm kazanmaktadır. İdare tarafından bilgi edinme hakkı kapsamında başlangıçta verilmeyen bilgi ve belgeler, dava sürecinde adil yargılanma hakkının bir gereği olarak davacıya açılmaktadır. Bu kademeli koruma sistemi, bir yandan kişisel verilerin gereksiz yere açılmasını engellerken, diğer yandan ciddi hukuki menfaati bulunan ilgililerin hak arama özgürlüğünü güvence altına almaktadır. Böylece yargı denetimi altında gerçekleşen kontrollü bir veri paylaşımı sağlanmakta ve kişisel verilerin korunması ile hak arama özgürlüğü arasında makul bir denge kurulmaktadır.

kötü, eksik veya olması gerekenden farklı işletiliyorsa idarenin sorumluluğuna yol açan bir hizmet kusuru vardır⁵⁸². Bu bağlamda idareye atfedilebilir bir işlemin, eylemin ya da eylemsizliğin bulunması, fiilin kusurlu olması ve bu kusurlu fiilden kaynaklanan bir zararın bulunması şartlarının varlığı halinde İdarenin kusurlu sorumluluğuna gidilebilir⁵⁸³. Dolayısıyla, İdarenin bu çalışmada da değinilen, başta 6698 sayılı Kanun olmak üzere, mevzuatta belirlenen şartlara aykırı şekilde veri işlemesi, bunda kusurunun bulunması ve bundan zarar doğması halinde bir hizmet kusuru olduğu kabul edilecek, oluşan zararı tazmin etmesi beklenecektir⁵⁸⁴.

Öte yandan, İdarenin kusursuz sorumluluğu ise tehlike, kamu külfetleri karşısında eşitlik ve sosyal risk esaslarına dayandırılmaktadır⁵⁸⁵. İdarenin, askeri tatbikat, güvenliğin sağlanması, sağlık hizmetleri gibi zarar verme riski taşıyan, tehlikeli faaliyetlerinden ötürü oluşan zararlar için İdare tehlike esasına göre sorumlu tutulmaktadır⁵⁸⁶. Fedakarlığın denkleştirilmesi ya da hakkaniyet olarak da ifade edilen kamu külfetlerinde eşitlik ilkesi ise İdarenin özellikle bayındırlık hizmetlerinden dolayı belli kişi ya da grubun zarar görmesi durumunda, zararın kamu üzerinde denkleştirilmesi amacıyla, bu kişilerin

⁵⁸² DURAN, s.26.

⁵⁸³ ULUSOY, **Yeni Türk İdare Hukuku**, s.558.

⁵⁸⁴ Davacı, askerlik muayenesi sonucu düzenlenen "Askerliğe Elverişli Değildir" raporunun basın yayın organlarında elde edilmesi nedeniyle 300.000 TL manevi tazminat talep etmiştir. İdarenin talebi reddetmesi üzerine dava açılmıştır. Mahkeme, kişisel verilerin korunmasının anayasal ve uluslararası sözleşmelerle güvence altına alındığını, sağlık verilerinin hassas kişisel veri kapsamında olduğunu belirtmiştir. İdarenin hassas verilerin muhafazasında kusurlu olduğu tespit edilmiştir. Mahkeme, olayın oluş şekli, davacının konumu ve idarenin kusurunun niteliğini değerlendirerek 10.000 TL manevi tazminatın, dava tarihinden itibaren işleyecek yasal faiziyle birlikte ödenmesine karar vermiştir. Fazlaya ilişkin tazminat talebi reddedilmiştir, Danıştay 15.D., E.2015/10101, K.2016/664, T.8.2.2016 (Lexpera); "(...) Poliklinik kayıtlarının düzenli şekilde tutulmamasından kaynaklı tıbbi kayıt eksikliğinin hizmet kusurunun belirlenmemesindeki payı dikkate alındığında, davacının hakkında uygulanan tedavileri ve zararlı sonucun sebebinin öğrenilecek tıbbi kayıtların noksan olması, dolayısıyla tedavi sürecinde gelişen olaylarla ilgili maddi gerçeğe (rahatsızlığının nedenine) hiçbir zaman ulaşamayacak ve ömür boyu şüphe duyacak olması nedeniyle uğradığı manevi zararının tazmini zorunludur. Başka bir anlatımla; hastanın başvurduğu gün ve saatin, hastaya uygulanan tedavinin, tedaviyi uygulayan doktor ve sağlık personelinin adının, kullanılan ilaç bilgilerinin hasta dosyasında (poliklinik defterinde) yer alması, hasta haklarının da gereği olup; söz konusu kayıtların düzenli ve yeterli tutulmaması-kişinin doğruyu öğrenme hakkına engel olacağından- hizmet kusurunu oluşturmaktadır." İstanbul BİM, 8. İDD, E. 2017/5, K. 2017/305, T. 7.3.2017, aktaran: Ayşe Aslı ALÇIN, "Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü", **TAAD**, Y.13, S.51, Temmuz 2022, s.397, dn.135. Öte yandan veri koruma otoriteleri tarafından faaliyet nedeniyle idari para cezası tesis edilmiş olup hukuka aykırı veri işleme örneği olarak değerlendirilebilecek kararlara yer vermek yerinde olacaktır: İsveç Gizlilik Koruma Kurumu tarafından, diğer hükümet kurumlarına idari destek sağlayan Ulusal Hükümet Merkezi'ne, kullandıkları sistemde meydana gelen bir hata nedeniyle veri ihlaline sebep oldukları ve bu ihlali ilgililere yaklaşık 5 ay gecikmeli bildirdikleri gerekçesiyle yaklaşık 18.700 Euro para cezası verilmiştir, "Swedish Authority for Privacy Protection issues fine against the National Government Service Centre", **IMY** (Swedish Authority for Privacy Protection), 29.4.2020, <https://www.imy.se/en/news/swedish-authority-for-privacy-protection-issues-fine-against-the-national-government-service-centre/> (E.T.15.8.2024). Norveç Veri Koruma Otoritesi, Bergen Belediyesi'ne bilgisayar sistemindeki güvenlik açığı nedeniyle 170.000 Euro'luk para cezası vermiştir. Verilen para cezası miktarının, 35.000'den fazla öğrenci ve çalışanın kişisel verisini riske etmesi, yetersiz güvenlik önlemleri, yetkisiz kullanıcıların okul sistemlerine erişmesine olanak tanınması, etkilenenlerin çoğunun çocuk olması ve belediyenin önceden uyarılmış olması gerekçesiyle yüksek belirlendiği ifade edilmiştir, "Administrative fine of €170,000 imposed on Bergen Municipality", **EDPB**, https://www.edpb.europa.eu/news/national-news/2019/administrative-fine-eu170000-imposed-bergen-municipality_en (E.T. 15.8.2024).

⁵⁸⁵ Turan YILDIRIM, "İdarenin Sorumluluğu", içinde **İdare Hukuku**, s.777.

⁵⁸⁶ Turan YILDIRIM, "İdarenin Sorumluluğu", içinde **İdare Hukuku**, s.777.

zararlarının kusuru olmayan İdare tarafından karşılanması esasını ifade eder⁵⁸⁷. Son olarak sosyal risk ilkesi, İdarenin kusuru olmasa bile toplumsal yaşamın riskleri nedeniyle ortaya çıkan zararları tazmin etmesi gerektiğini ifade eden bir ilkedir. Bu ilke, toplumun huzur ve güvenliğini sağlamakla görevli olan idarenin, bu görevini yerine getirirken karşılaşılabileceği öngörülemeyen ve önlenemeyen olaylar sonucu ortaya çıkan zararları, topluma pay ederek gidermesi gerektiği düşüncesine dayanır. Sosyal risk ilkesi özellikle terör olayları, toplumsal şiddet, isyan, iç karışıklık gibi ani gelişen, öngörülmesi ve önlenmesi güç olan olaylarda uygulama alanı bulmakta, diğer esaslardan farklı olarak ortaya çıkan zarar ile idarenin herhangi bir eylemi arasında nedensellik bağı aranmamaktadır⁵⁸⁸.

Kişisel verilerin işlenmesi bağlamında, idarenin sorumluluğu ekseriyetle veri koruma kurallarına aykırı veri işleme faaliyetlerinden kaynaklandığından, açılacak davalarda idarenin hizmet kusurunun varlığı araştırılacaktır. Bununla birlikte, hizmet kusurunun bulunamadığı durumlarda, KVKK’de özel bir sınırlamaya yer verilmediğinden, kişisel verilerin işleme faaliyetinden kaynaklanan zararlar bakımından İdarenin kusursuz sorumluluk ilkelerine göre de zararların tazminiyle yükümlendirilebileceği ifade edilmektedir⁵⁸⁹.

Öte yandan, GDPR’ın 82. maddesi kusursuz sorumluluk ilkesini kabul etmemiştir. Maddenin ilk fıkrasında, Tüzük’ün ihlali nedeniyle maddi veya manevi zarar gören herkesin, uğradığı zararları veri sorumlusu veya veri işleyenden tazmin etme hakkı bulunduğu belirlendikten sonra, 3. fıkrasında, veri sorumlusu veya veri işleyenin zarara sebep olan olaydan hiçbir şekilde sorumlu olmadığını kanıtlaması halinde sorumluluktan kurtulabileceği kabul edilmiştir.

Kişisel verilerin günümüzde giderek artan önemi dikkate alındığında, verilerin ifşası ve yanlış kullanımının bireylerin özel hayatı ve hakları üzerinde ciddi sonuçlar doğurabileceği kabul edilmelidir. İdare, çeşitli kamu hizmetlerini yerine getirirken büyük miktarda kişisel veri toplamakta ve işlemekte, bu veriler arasında özel nitelikli verileri de barındırmaktadır. Bu bağlamda, özellikle büyük ölçekli ve hassas verilerin söz konusu olduğu durumlarda, potansiyel olarak tehlikeli bir faaliyetin var olduğu, dolayısıyla bu tehlikeli faaliyeti yürüten İdarenin doğacak zararlardan tehlike ilkesine dayanılarak kusursuz sorumluluğu kabul edilebilir⁵⁹⁰. Böylece İdarenin veri güvenliğini sağlama konusundaki sorumluluğu artırılarak bireylerin haklarının daha etkin bir şekilde korunması sağlanabilir.

Ancak, özel nitelikli veriler KVKK’nin 6. maddesinde tahdidi olarak sayılmışsa da yukarıda ifade edildiği üzere⁵⁹¹, birkaç genel nitelikli verinin bir araya gelmesiyle özel nitelikli veriler hakkında

⁵⁸⁷ Turgut CANDAN, *Açıklamalı İdari Yargılama Usulü Kanunu, Yetkin Yayınları*, 8. Baskı, 2020, s.224.

⁵⁸⁸ ULUSOY, *Yeni Türk İdare Hukuku*, s.563.

⁵⁸⁹ AYDOĞDU, s. 281; Mutlu KAĞITCIOĞLU, “Yapay Zekâ ve İdare Hukuku (Bugünden Geleceğe Yönelik Bir Değerlendirme)”, *Hacettepe HFD*, S.11(1), Y.2021, ss.118-168, s.153; Halil ALTINDAĞ, “Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu”, *İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi*, C.18, S.2, Temmuz 2019, s.389.

⁵⁹⁰ ALTINDAĞ, “Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu”, s.396.

⁵⁹¹ Bkz.: “2. ÖZEL NİTELİKLİ (HASSAS) KİŞİSEL VERİ KAVRAMI” başlığı.

çıkartım yapılabilirdi gibi, yine bazıları için özel nitelikli verilerinin ifşa olması durumu bazı genel nitelikli kabul edilen verilerinin bilinmesinden daha az etki doğurmakta, daha az tehlikeli kabul edilebilmektedir. Öyleyse ‘tehlikeli’ veri nedir? sorusunun cevaplanması gerekir. Nitekim, temel kimlik bilgileri olan ad, soyad, doğum tarihi ve yeri ile T.C. kimlik numarası ile finansal bilgiler kullanılarak banka hesapları açılabilir veya kredi başvuruları yapılabilir; resmî belge bilgileri sahte kimlik oluşturmak için kullanılabilir; çevrimiçi hesap bilgileri, dijital platformlarda kişinin kimliğini taklit etmek için kullanılabilir ya da kimlik hırsızları bu bilgileri bir araya getirerek, hedef aldıkları kişinin kimliğini daha inandırıcı bir şekilde taklit edebilirler. Bu nedenle, tehlikeli veri tehlikesiz veri ayrımı yapılmaması gerektiği savunulabilir. Öte yandan, sürekli gelişen ve gidişatı tahmin edilemeyen bir alanda, İdarenin kusursuz şekilde sorumlu tutulmasının İdareye ağır bir mali yük yükleyebileceği ve kamu hizmetlerinin sunumunu zorlaştırabileceği de düşünülmelidir. Bu gerekçelerle, İdarenin tehlike sorumluluğu ilkesi uyarınca kusursuz şekilde sorumlu tutulabileceği kabul edilmekle birlikte, sınırlarının daha dar şekilde çizilmesi gerektiği ifade edilmelidir.

Bununla birlikte, özellikle idari eylemlerden doğan tam yargı davalarında idarenin kusur sorumluluğuna gidilirken, kusurun, zararın ve nedensellik bağının ispatında davacı lehine yorum yapılması kişisel verilerin korumasını güçlendirecektir. İdari eylemlerden doğan tam yargı davalarında ispat külfeti kural olarak, hakkının ihlal edildiğini iddia eden davacıya düşmektedir⁵⁹². Ancak, kişisel verilerin korunması alanında bu genel kuraldan ayrılarak, İdarenin kusur sorumluluğuna gidilirken, İdarenin kusuru olmadığını ispat etmesi yerinde olacaktır. Bu önerinin gerekçesi, İdarenin kamu gücüne dayanarak veri işlemesi ve şeffaflık ilkesinin tam olarak uygulanmaması, vatandaşın teknik detaylara ve işlem süreçlerine hâkim olamamasıdır. Bu bağlamda, söz gelimi veri sızıntısı nedeniyle çalınan verilerinin medyaya servis edildiği ve zarara uğradığına yönelik bir davada, veri sızıntısının yaşanmasında İdarenin kusuru olmadığını ispat etmesi aranmalıdır. Bununla birlikte, sadece veri ihlalinin yaşanmış olması, İdarenin kanuni gereklere aykırı veri işlediği anlamına gelmemelidir. İdare, uzman görüşü ve bilirkişi raporları vasıtasıyla gerekli her türlü önlemi aldığını ispatlayabilmelidir.

Öte yandan, nedensellik bağının ispatında hukuk sisteminin vatandaşla bu konuda yararlı olabilecek kurumlarla donatılması sağlanabilir. Bu bağlamda, kademeli bir ispat sistemi belirlenerek, veri ihlali ile zarar arasında ilk görünüşte ispat (prima facie)⁵⁹³ ile bir bağlantı kurulması halinde ispat yükünün İdareye geçmesi kabul edilebilir. Somut veri ihlaline yönelik hazırlanacak potansiyel risk analizlerinden ve benzer veri ihlallerinin sonuçlarına dair istatistiksel verilerden nedensellik bağının kurulmasında faydalanılabilir. Ayrıca, veri ihlali ile zararın ortaya çıkması arasındaki zaman farkı da kullanılabilecek araçlardan biri olabilir.

⁵⁹² Melikşah YASİN, *İdari Yargılama Usulünde İspat*, On İki Levha Yayıncılık, 2015, s. 97.

⁵⁹³ Leyla KESER, “İlk Görünüş İspatı”, **Prof. Dr. Mahmut Bırsel’e Armağan**, DEU Yayını, 2001, <https://hukuk.deu.edu.tr/wp-content/uploads/2020/01/L.Keser-13.pdf> (E.T. 15.8.2024).

Bunun dışında veri sahibi, veri sızıntısı nedeniyle uğradığını iddia ettiği maddi zararlarını ispat edemese de gelecekte verilerinin kötüye kullanımına ilişkin kapıldığı korku nedeniyle, bu korkuyu ispatlamak şartıyla, İdarenin kendisine manevi tazminat ödemesi sağlanmalıdır. İdare çoğunlukla kanuna ve mevzuatın kendisine yüklediği yükümlülüklerle istinaden kamu gücünü kullanarak ve ilgisinden açık rıza almadan veri işleyebilmekte, bununla birlikte KVKK uyarınca hukuka aykırı veri işlediğinde idari para cezasına muhatap olmamaktadır. İdarenin, veri işleme faaliyetlerinden doğan manevi zararlar bakımından potansiyel zarar bağlamındaki sorumluluğu genişletilerek kullandığı kamu gücüne karşılık sahip olduğu sorumluluk arasında bir denge unsuru sağlanmış olacağı değerlendirilmektedir.

Avrupa Birliği Adalet Divanı (ABAD) da yakın tarihli bir kararında⁵⁹⁴, GDPR'ın 82/1. maddesi kapsamındaki "maddi olmayan zarar" kavramının geniş yorumlanması gerektiğine dikkat çekmiştir. ABAD, bu bağlamda GDPR'ın halihazırda gerçekleşmiş kişisel veri kötüye kullanımı ile gelecekte olası bir kötüye kullanım korkusu arasında ayırım yapmadığını vurgulamıştır (par.79). Mahkeme, veri sahibinin gelecekteki olası kötüye kullanım endişesinin de tazminat kapsamında değerlendirilebileceğini belirtmiştir. Bu bağlamda, GDPR'ın 85. gerekçesi hatırlatılarak⁵⁹⁵, "zarar" kavramının geniş bir yelpazede ele alınması gerektiği ifade edilmiştir (par.82).

ABAD'ın kararında özellikle dikkat çeken bir nokta, kişisel veriler üzerindeki kontrol kaybının bile başlı başına bir zarar olarak kabul edilebileceğidir. Mahkeme, GDPR'ın temel amacının Avrupa Birliği içerisinde kişisel verilerin işlenmesinde gerçek kişilere yüksek düzeyde koruma sağlamak olduğunu hatırlatarak, "maddi olmayan zarar" kavramının dar yorumlanmasının bu amaca ters düşeceğini vurgulamıştır (par.81). Bu bağlamda, veri sahiplerinin tazminat haklarının sadece gerçekleşmiş zararlarla sınırlı olmadığı, gelecekteki potansiyel zararlar ve bu zararların yarattığı endişeleri de kapsayacak şekilde genişletilmesi gerektiği belirtilmiştir. Bununla birlikte kararda, veri ihlali nedeniyle gelecekte kişisel verilerinin kötüye kullanılacağı korkusuna dayanarak manevi zarar uğradığının iddia edilmesi halinde, ulusal mahkemenin, söz konusu özel koşullarda ve veri sahibi açısından bu korkunun sağlam temellere dayandığını doğrulaması gerektiği ifade edilmiştir (par.85). Bu

⁵⁹⁴ CJEU, C-340/21 Natsionalna agentsia za prihodite, 14.12.2023, ECLI:EU:C:2023:986, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8652926> (E.T. 15.8.2024).

⁵⁹⁵ Gerekçe 85 – “Kişisel veri ihlali, uygun bir şekilde ve zamanında ele alınmadığı takdirde, gerçek kişilere, kişisel verileri üzerindeki kontrolü kaybetmeleri veya haklarının sınırlandırılması, ayrımcılık, kimlik hırsızlığı veya kimlikte sahtecilik, takma adın izinsiz şekilde geri getirilmesi, itibarın zedelenmesi, mesleki sır saklama ile korunan kişisel verilerin gizliliğinin kaybedilmesi veya söz konusu gerçek kişiye yönelik diğer önemli ekonomik veya sosyal dezavantajlar gibi fiziksel, maddi veya manevi zarara neden olabilir. Bu sebeple, hesap verebilirlik ilkesi doğrultusunda kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından riske sebebiyet vermesinin muhtemel olmadığını kanıtlayabildiği haller hariç olmak üzere, veri sorumlusu, kişisel veri ihlali olduğunu fark eder etmez fazla gecikmeksizin ve uygun olması hâlinde, ihlalden haberdar olduktan itibaren en geç 72 saat içinde, söz konusu kişisel veri ihlalinin denetim makamına bildirmelidir. Bu bildirimin 72 saat içinde yapılamadığı hallerde, bu bildirimde gecikme sebeplerine de yer verilir ve bilgiler, daha fazla gecikmeksizin aşamalı olarak sağlanabilir.”

korkunun temellerinin değerlendirilmesinde, sızdırılan verinin niteliği (HIV pozitif hastaların bilgilerinin sızdırılmasında, bunların ifşa edilmesinin yaratacağı ayrımcılık riski), veri sorumlusunun veri ihlali sonrasında takındığı tavır (ihlalin gizlenmeye çalışılması ve veri sahiplerin bilgilendirilmemesi gibi) ve veri sahibinin toplumdaki konumu gibi kriterler göz önünde bulundurulabilir.

İdarenin kusursuz sorumluluğuna ilişkin görüşlerimiz özellikle siber saldırılar karşısında veri güvenliğinin sağlanmasına ilişkin olmakla birlikte YZ tabanlı sistemler kullanılarak yasaya aykırı veri işleme faaliyeti gerçekleştirilmesi halinde farklı sonuçlara varılabilir. YZ sistemlerinin, özellikle makine öğrenmesi ve derin öğrenme algoritmalarına dayanan ileri düzey versiyonlarının, kararlarını nasıl aldığını tam olarak açıklamak veya öngörmek çoğu zaman mümkün olmamaktadır. Bu durum, "kara kutu" problemi olarak da adlandırılmakta ve idarenin YZ kullanımında ortaya çıkabilecek zararlardan sorumluluğunun belirlenmesinde yeni hukuki yaklaşımları gerekli kılmaktadır.

Avrupa Birliği'nin Yapay Zekâ Yasası'nda öngörülen risk sınıflandırması, idarenin sorumluluğunun belirlenmesinde yol gösterici olabilir. Bu bağlamda, ilgili Yasa'da yapılan risk ayrımı dikkate alınarak yüksek riskli olarak değerlendirilen elektrik, su, gaz gibi kritik altyapıların yönetiminde; eğitim veya mesleki yeterliliklerin belirlenmesinde; gözetim, suç tespiti veya adli süreçlerde; göç, sığınma ve sınır yönetiminin sağlanmasında kullanılan yapay zeka sistemleri gibi insanların temel haklarını etkileyebilecek kritik alanlarda kullanılan yapay zeka sistemlerinden kaynaklanan kişisel veri ihlalleri ile bu ihlallerden doğan zararların tazmininde İdarenin kusursuz sorumluluğunun kabulü gerekecektir.

KAĞITCIOĞLU'nun da belirttiği gibi, mevcut mevzuat çerçevesinde, idarenin kullandığı YZ kaynaklı bir zararda ispat güçlüğü nedeniyle, risk ilkesi çerçevesinde kusursuz sorumluluğa gidilmesi daha uygun bir yaklaşım olacaktır⁵⁹⁶. Bu yaklaşım hem vatandaşların haklarının korunması hem de idarenin YZ sistemlerini kullanırken daha dikkatli ve özenli davranmasını sağlama açısından önem taşımaktadır. Bununla birlikte, idarenin YZ kullanımında şeffaflık ve hesap verebilirlik ilkelerinin güçlendirilmesi, YZ sistemlerinin karar alma süreçlerinin mümkün olduğunca açıklanabilir olması, denetlenebilirliğin sağlanması ve etik ilkelere uygunluğun gözetilmesi de önem taşımaktadır.

İdarenin gerek hizmet kusuruna dayanan sorumluluğu gerekse risk esasına dayanan kusursuz sorumluluğu, kamu hizmetlerinin yürütülmesinde ortaya çıkan zararların tazmininde önemli rol oynamaktadır. Özellikle YZ sistemlerinin kullanımında, bu sistemlerin karar alma mekanizmalarının tam olarak açıklanamaması nedeniyle ortaya çıkan "kara kutu" problemi, idarenin kusursuz sorumluluğunun uygulanmasını gerekli kılabilmektedir. Ancak, idarenin sorumluluğu mutlak değildir ve bazı hallerde bu sorumluluk azalabilmekte veya tamamen ortadan kalkabilmektedir. Bu bağlamda,

⁵⁹⁶ KAĞITCIOĞLU, s.159.

idarenin kusurunu azaltan ya da kaldıran sebepler olarak mücbir sebep, beklenmedik hal, zarar görenin ya da üçüncü kişinin kusuru ile kamu görevlilerinin görevden ayrılabilen kişisel kusurları sayılabilirken; beklenmedik hal ve üçüncü kişinin kusuru yalnızca hizmet kusurunu azaltan ya da kaldıran haller arasında kabul edilmektedir⁵⁹⁷.

Deprem, sel ve toprak kayması gibi afetler nedeniyle İdarenin veri merkezinin yıkılması ve kişisel verilerin güvenliğinin bir süre sağlanamaması halinde idarenin sorumluluğunun azaldığı ya da tamamen ortadan kalktığı söylenebilir. Ancak, veri merkezinin bulunduğu bölgenin seçiminde bu tür afetlere karşı güvenli olup olmadığının irdelenmemesi ya da merkezin içinde bulunduğu yapının dayanıklılığında eksikler bulunması halinde İdarenin kusurundan bahsedilebilecektir. Öte yandan, İdarenin veri depolama sisteminde daha önce hiç rastlanmamış ve öngörülemeyen bir yazılım hatası nedeniyle kişisel verilerin kısa süreliğine erişilebilir hale gelmesi durumu beklenmeyen hal olarak nitelendirilebilir ve böyle bir durumda idarenin hizmet kusuru sorumluluğu azalabilir ya da tamamen ortadan kalkabilir.

İdarenin kusurunu azaltan ya da kaldıran bir başka durum ise zarar görenin kusurudur. İdarenin, vatandaşlara kişisel verilerinin yapay zekâ sistemleri tarafından işleneceğine dair açık bilgilendirme yapmasına ve gerekli izinleri ve önlemleri almasına rağmen, bir vatandaşın bilerek ve isteyerek yanlış bilgiler vermesi sonucunda zarara uğraması durumunda, idarenin kusursuz sorumluluğunun azalabileceği söylenebilir. Bununla birlikte, üçüncü kişi YZ sistemi üreticisinden alınan ve İdare tarafından kamu hizmetlerinden kullanılan sistemde, YZ sistemine ilişkin üreticiden kaynaklanan bir kusur nedeniyle zararın ortaya çıkması halinde, üçüncü kişinin zararı yalnızca kusur sorumluluğuna etki ettiğinden, İdarenin kusursuz sorumluluğu devam edecektir⁵⁹⁸.

4. KİŞİSEL VERİLERİN İDAREYE KARŞI KORUNMASINA İLİŞKİN DENETİM MEKANİZMALARI

4.1. İdari Denetim

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 11. maddesinde kişisel verileri işlenen ilgililerin hakları düzenlenmiştir. Buna göre ilgili kişi veri sorumlusuna başvurarak kendisiyle ilgili kişisel verilerin işlenip işlenmediği, işlenmişse bunların işlenme amacını ve verilerinin bu amaca uygun kullanılıp kullanılmadığı ile verilerinin yurt içi ya da yurt dışında bulunan üçüncü kişilere aktarılıp aktarılmadığı hususlarında bilgi talep edebilir. Ayrıca, kişisel verilerinin eksik ya da yanlış işlendiğini düşünüyorsa bunların düzeltilmesini, Kanunun 7. maddesinde belirlenen şartlar çerçevesinde verilerinin

⁵⁹⁷ Celal İŞIKLAR, “Danıştay Kararlarında İdarenin Kusursuz Sorumluluğunu Kaldıran veya Azaltan Haller”, **YBHD**, Y.4, S.2019/1, ss.115-158, s. 147; ALTINDAĞ, “Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu”, s.397.

⁵⁹⁸ KAĞITCIOĞLU, s.153.

silinmesini ya da yok edilmesini ve bu işlemlerden birinin gerçekleştirilmesi halinde yapılan işlemde kişisel verilerin aktarıldığı üçüncü kişilerin de haberdar edilmesini talep edebilir. Öte yandan ilgilinin işlenen kişisel verilerinin münhasıran otomatik sistemler aracılığıyla analiz edilmek suretiyle kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve verilerinin kanuna aykırı şekilde işlenmesi sebebiyle doğacak zararlarının giderilmesini talep etme hakları da bulunmaktadır.

6698 sayılı Kanunda veri sorumlusuna ve KVK Kurulu'na olmak üzere iki ayrı başvuru yöntemi düzenlenmiştir. Bunun dışında Kurula re'sen inceleme yapma yetkisi de Kanunun 15. maddesiyle tanınmıştır. Veri sorumlusuna yapılacak olan başvuru için "başvuru" kavramı kullanılırken Kurul'a yapılacak başvuru için "şikâyet" kavramı tercih edilmiştir. Buna göre Kanunun 13. maddesinde veri sorumlusuna yapılacak başvuru düzenlenirken 14. maddesinde ise Kurul'a yapılacak şikâyet hususuna yer verilmiştir. Ayrıca veri sorumlusuna yapılacak başvuruya ilişkin olarak Kurum tarafından "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ" Resmî Gazete'de yayımlanmıştır⁵⁹⁹.

Belirtmek gerekir ki, Kanunun 14. maddesinin 2. fıkrası uyarınca kişinin veri sorumlusuna başvurmadan doğrudan Kurul'a şikâyet başvurusu yapması mümkün değildir. Öte yandan ilgilinin kişisel verilerinin hukuka aykırı şekilde işlenmesinden doğan zararlarının giderilmesine yönelik dava açmadan önce veri sorumlusuna başvuruda bulunmasını zorunlu kılan bir hükme de yer verilmemiştir. Bu sebeple veri sorumlusunun gerçek ya da özel hukuk tüzel kişisi olduğu hallerde veri sorumlusu ya da Kurul'a bir başvuruda bulunmaksızın doğrudan genel hükümlere göre dava açılacağı söylenebilir. Veri sorumlusunun İdare olması halinde zararın tazmini amacıyla 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre bir tam yargı davası açılması gerekecektir. Bu zararın İdarenin veri işlemek suretiyle tesis ettiği idari işlemde doğması durumunda İYUK'un 12. maddesine göre hareket edilir. Öte yandan, zarar İdarenin mevzuat gereği alması gereken önlemleri almaması, kişisel verilerin korunması bakımından ihmalkâr davranması gibi idarenin bir eyleminden dolayı ortaya çıkmışsa bu halde İYUK'un 13. maddesine göre idareye yapılacak zorunlu başvuru sonrasında tam yargı davası açılacaktır.

4.1.1. Veri Sorumlusu İdareye Başvuru

Kişisel Verilerin Korunması Kanunu'nun 3. maddesinin "1" bendinde yapılan tanım uyarınca *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* veri sorumlusudur. Kanunda özel hukuk tüzel kişisi ya da kamu tüzel kişisi şeklinde bir ayırım yapılmadığından kamu tüzel kişisi olarak örgütlenen İdarelerin de birer veri sorumlusu olabileceğini daha önce ifade etmiştik. Bu bağlamda veri sorumlusu ile veri işleyen arasındaki farka da değinmek gerekmektedir. Kanun metninde belirtildiği üzere, veri sorumlusu kişisel verilerin işleme amacını ve vasıtalarını belirleyen kişidir. Öte yandan Kanun 3.

⁵⁹⁹ RG, 10.03.2018/30356.

maddesinin “ğ” bendine göre veri işleyen kişi veri sorumlusunun verdiği yetkiye dayanarak onun nam ve hesabına kişisel verileri işleyen gerçek ya da tüzel kişidir. Kamu tüzel kişiliğini haiz bir İdare kişisel verilerin işleme amacını ve vasıtalarını belirledikten sonra bu verileri işleme görevini kendi bünyesindeki bir birime verebileceği gibi bu bünye dışında üçüncü bir gerçek ya da tüzel kişiyi de yetkilendirebilir⁶⁰⁰. İlk halde veri işleyen ve veri sorumlusu sıfatları aynı tüzel kişide birleşirken ikinci halde bu iki kavram için ayrı kişilerin varlığından söz edilecektir.

Kanunda veri sorumlusu olarak gerçek kişi ya da tüzel kişi işaret edildiğinden veri sorumlusu olarak verinin işleme amaçlarını ve vasıtalarını belirleyen kamu tüzel kişiliğini haiz İdareye başvuruda bulunmak gerekecektir⁶⁰¹. Bir kamu tüzel kişiliğinde farklı idari birimlere yer verilmekle birlikte bu birimlerin ayrı kamu tüzel kişiliği bulunmamaktadır. Örneğin bir belediyenin Sosyal Yardım İşleri Müdürlüğü tarafından yardım talebinde bulunan ilgilinin adı, soyadı, aile bireylerinin sayısı ve aylık maddi geliri gibi kişisel verileri işlenmektedir. Bu kişisel verileriyle ilgili olarak 6698 sayılı Kanunun 11. maddesinde belirlenen haklarına ilişkin başvuruda bulunmak isteyen ilgilinin başvurusunu ilgili Müdürlük yerine doğrudan belediye başkanlığına yapması gerekir. Bu bağlamda idari teşkilat içerisinde ayrı kamu tüzel kişilikleri bulunan başta Devlet tüzel kişiliği olmak üzere yerinden yönetim idareleri olarak isimlendirilen il özel idareleri, belediyeler ve köyler, hizmet bakımından yerinden yönetim kurumları olarak kabul edilen ve kamu tüzel kişiliğini haiz üniversiteler, Yükseköğretim Kurulu, Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı (ÖSYM), düzenleyici ve denetleyici kurumlar olarak da adlandırılan Radyo ve Televizyon Üst Kurulu (RTÜK), Rekabet Kurumu, Kamu İhale Kurumu gibi kurumlar birer veri sorumlusudur.

Veri sorumlusunun belirlenmesi bakımından tüzel kişiliğinin esas alınması ayrı tüzel kişiliği bulunan kamu kurum ve kuruluşları için bir sorun teşkil etmemektedir. Bununla birlikte, tek bir kamu tüzel kişisi olan Devlet tüzel kişiliği içerisinde merkez teşkilatında bulunan bakanlıklar ve yine taşra teşkilatını oluşturan il ve ilçe idareleri gibi birçok idari birimin ayrı tüzel kişiliği bulunmamaktadır. Bu durumda, örneğin Millî Eğitim Bakanlığı’na bağlı tüm okullarda yapılan veri işleme faaliyetleri bakımından veri sorumlusu olarak Bakanlık değil Devlet tüzel kişiliği kabul edilecektir⁶⁰². Yine ayrı

⁶⁰⁰ BAŞAR, s.39.

⁶⁰¹ Kendi nam ve hesabına veri işleme faaliyeti yürüten gerçek kişiler de veri sorumlusudur. Doktorun kendi muayenehanesinde hastalarına ait verileri işlemesi yahut bir bakkal dükkânı sahibinin veresiye defteri tutması halinde doktor ve dükkân sahibi gerçek kişi veri sorumlusu olarak kabul edilir. ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, s.28.

⁶⁰² İdari yargıda iptal davalarında, husumetin işlemi tesis eden makama yöneltilmesi gerektiği öğretide ve yargı kararlarında kabul edilmektedir: GÖZÜBÜYÜK / TAN, **İdare Hukuku Cilt II**, s.779 vd.; Halil YOLAL, **Danıştay Kararları Işığında İptal Davalarında Dava Açma Ehliyeti**, On İki Levha Yayıncılık, 2019, s. 52; Zehra KARAKUŞ IŞIK, “İdari Eylemlerden Kaynaklanan Tam Yargı Davalarında Bir Bozma Nedeni Olarak Husumet”, **AndHD**, C.:9, S.:2, Temmuz 2023, s.336. Ancak bu durum veri sorumlusunun belirlenmesi bakımından ayrı bir sorun teşkil etmemektedir. Zira veri sorumlusu kavramı, dava ehliyetinden bağımsız olarak, kişisel verilerin işlenmesinin amacını ve yöntemini belirleyen kişiyi ifade eder. Dolayısıyla, kişisel verilerin korunması hukukunda tüzel kişilik esasına dayalı veri sorumlusu belirlenmesi, uygulamada işlemi tesis eden makamın farklı, veri sorumlusunun farklı olması gibi karmaşık bir durum yaratmaktadır.

tüzel kişiliği bulunmayan tüm hastanelerde ya da valilik ile kaymakamlıklarda yapılan veri işleme faaliyetlerinde de Devlet tüzel kişiliğinin veri sorumlusu olarak muhatap alınması gerekecektir. Bu durumun kişisel verilerin işlenmesi bakımından işlevsellik, şeffaflık ve uygulanabilirlik kriterlerinin gerçekleştirilmesinde önemli bir sorun teşkil ettiği ifade edilmektedir⁶⁰³. Bu bakımdan, idari teşkilat yapısı göz önüne alınarak bakanlıkların ve yetki genişliği esasıyla yönetilen valiliklerin de veri sorumlusu olduğuna ilişkin 6698 sayılı Kanun’a bir hüküm eklenmesi⁶⁰⁴ söz konusu soruna çözüm olacaktır⁶⁰⁵.

Valilerin merkezden aldığı yetkiyle merkez adına karar vermesi ve hareket edebilmesi karşısında ayrı bir kamu tüzel kişiliği bulunmasa da karar alabilme yetkisine sahip olmasından ötürü veri sorumlusu olarak kabul edilmesi yerinde olacaktır. Yine Bakanlıklar için de benzer bir durum söz konusu olabilir. Her biri kendilerine verilen görevleri yerine getirmek için geniş bir idari teşkilata sahip Bakanlıkların görevleri sırasında işledikleri kişisel veriler bakımından veri sorumlusu olarak kabul edilmesi yerinde olacaktır. Nitekim, veri sorumlusu “işlenen verilerin amacını ve işleme yöntemini belirleyen” kişi olarak tanımlanmaktadır. İdare içerisinde kişisel veri işleyen birçok birim bulunmakta ancak bu verilerin işleme amacı ve araçlarını belirleyen her İdarenin ayrı kamu tüzel kişiliği bulunmamaktadır. Dolayısıyla, 6698 sayılı Kanunda yapılan tanım birçok İdarenin veri sorumlusu gibi hareket etmesine karşın veri sorumlusu olarak kabul edilmemesi sonucunu doğurmaktadır.

Ayrıca, gerek mehzaz 95/46/EC sayılı Direktif metninde gerekse de 2016/679 sayılı Tüzük metninde yapılan veri sorumlusu (controller) tanımına göre gerçek veya tüzel kişinin yanı sıra kişisel verilerin işlenmesinin amaçlarını ve araçlarını tek başına veya başkalarıyla birlikte belirleyen kamu otoritesi, kurum veya diğer herhangi bir organ da veri sorumlusu olabilecektir⁶⁰⁶. Ancak, yukarıda da ifade edildiği gibi, Kanunumuzda yalnızca gerçek ve tüzel kişilerin veri sorumluluğu kabul edilmiş, mehzaz düzenlemede yer alan “kamu otoritesi, kurum veya diğer herhangi bir organ” ın veri sorumlusu olarak kabul edilmesine imkân verilmemiştir. Dolayısıyla Kanunumuzda, kişisel veri işlenmesinin amaçları ve araçlarını belirleme yetkisi bulunan İdarelerin ayrı bir tüzel kişilikleri bulunmasa da veri sorumlusu olarak kabul edileceğine yönelik bir düzenleme yapılarak bu eksikliğin giderilmesi sağlanmalıdır.

⁶⁰³ ÇEKİN, s.61 vd.

⁶⁰⁴ ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, s. 29.

⁶⁰⁵ Yetki genişliği, İdarenin merkezden yönetim ilkesinin sakıncalarını gidermek için kabul edilen bir kurumdur. İdarenin görevlerini merkezde bulunan ya da buraya bağlı olarak çalışan görevliler aracılığıyla yerine getirmesi olarak tanımlanabilecek olan merkezden yönetim ilkesi, kamu hizmetlerinin tek bir merkezden planlanması ve gerçekleştirilmesi gerekliliğini doğurmaktadır. İletişim olanaklarının önemli derecede gelişmesine karşın tüm hizmetlerin tek bir merkezden yürütülmesinin doğurabileceği karmaşa ve aksaklıkları önlemek amacıyla da merkeze bağlı bazı makamlara merkez adına karar alma ve uygulama yetkisi verilmiştir: Turan YILDIRIM, “Türkiye’nin İdari Teşkilatı”, s. 39. İşte bu yetkinin adı “yetki genişliği” olarak ifade edilmektedir. Yetki genişliği ilkesi Türk İdaresinde çok sınırlı olarak uygulanmaktadır; zira Anayasa’nın 126. maddesinde “*illerin idaresi yetki genişliği esasına dayanır*” denilmek suretiyle bu ilke yalnızca Valilere tanınmıştır.

⁶⁰⁶ 95/46/EC sayılı Direktif, Madde 2/(d).

6698 sayılı Kanunun 13. maddesinde veri sorumlusuna başvuru hususu düzenlenmiştir. Maddenin ilk fıkrası uyarınca ilgili kişi “*Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak ya da Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.*” Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’in (Tebliğ) 4. maddesine göre ilgili kişilerin bu başvuruyu Türkçe yapmaları gerekmektedir. Tebliğ’in 5. maddesinde ise veri sorumlusuna yazılı başvuru yöntemi dışında kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişiye ait veri sorumlusunun sisteminde kayıtlı bulunan e-posta adresi yahut veri sorumlusu tarafından bu başvuru için geliştirilmiş yazılım ya da uygulama vasıtasıyla başvuru yapılabileceği kabul edilmiştir.

Öte yandan Tebliğ’in 5. maddesinin ikinci fıkrasında veri sorumlusuna yapılacak başvuru metninde yer alması gereken bilgiler belirlenmiştir. Buna göre ilgili yapacağı başvuruda ad, soyad ve başvuru yazılı ise imza; T.C. kimlik numarası ya da pasaport numarası; tebligata esas yerleşim yeri ya da işyeri adresi; varsa e-posta, telefon ve faks numarası ve talep konusu bilgilerine yer vermek zorundadır. Ayrıca yapılan yazılı başvuruda evrakın veri sorumlusuna ya da temsilcisine tebliğ edildiği tarih, başvuru tarihi olarak kabul edilecek; diğer yöntemlerde ise başvuru tarihi başvurunun veri sorumlusuna ulaştığı tarih olacaktır.

Kanunun 13. maddesinde veri sorumlusunun başvuruda belirtilen talepleri, taleplerin niteliğine göre en kısa sürede ve en geç otuz gün içerisinde ücretsiz olarak cevaplaması öngörülmüştür⁶⁰⁷. Ancak Kanunda İdarenin bu başvuruya yanıt vermemesi halinde uygulanacak herhangi bir yaptırım öngörülmemiştir. Kanunun 13. maddesinin üçüncü fıkrasına göre İdare yapılan başvuruyu kabul eder ya da gerekçesini açıklayarak reddeder ve cevabını ilgiliye yazılı olarak yahut elektronik ortamda bildirir. İlgilinin taleplerinin kabul edilmesi halinde veri sorumlusunun taleplerin gereğini en kısa sürede yerine getirmesi ve bu konuda ilgiliyi bilgilendirmesi gerekir (Tebliğ, m.6/6).

6698 sayılı Kanunun 13. maddesi uyarınca veri sorumlusu İdareye yapılacak “başvuru” ile 14. maddesi uyarınca bir kamu tüzel kişisi olan Kişisel Verileri Koruma Kurumu’na yapılacak “şikâyet” birer idari başvuru niteliğindedir. Kişilerin taleplerini ve şikâyetlerini iletmek amacıyla İdareye yaptıkları başvurulara idari başvuru denilmektedir⁶⁰⁸. Yapılan daha geniş bir tanımda ise idari başvuru “*Kişilerin menfaatleri bulunan ve idari işlev kapsamına giren konularda kamusal makamlara yaptıkları başvuruların tümü ile kamu yararını korumak amacıyla, yetki verilen kamu görevlilerinin veya kamu*

⁶⁰⁷ Ancak, düzenlemenin devamında işlemin ayrıca bir maliyeti gerektirmesi halinde Kurul tarafından belirlenen tarife üzerinden ücret alınabileceği ifade edilmiş, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’in 7. maddesinde de bu tarife belirlenmiştir. Buna göre “*İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir. / Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.*” Bununla birlikte başvuru veri sorumlusunun hatasından kaynaklanmış ise alınan ücretin ilgiliye iade edilmesi gerekmektedir (6698 sayılı Kanun, m.13/3; Tebliğ, m.6/5)

⁶⁰⁸ Yusuf DENİZ ve diğerleri, “İdari Yargılama Usulü Kanunu’nun 11. Maddesine Göre Yapılan İdari Başvurular”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C.21, S.2, 2013, s.32.

tüzel kişilerinin, diğer idari makamlara yaptığı idari işlemlerin iptali, değiştirilmesi, geri alınması gibi nedenlerle, yine yasaların gösterdiği idari işleve sahip makamlara yaptıkları idare hukukuna ilişkin başvurular” şeklinde ifade edilmektedir⁶⁰⁹.

İdari başvuru müessesesinin iki farklı türü 2577 sayılı İdari Yargılama Usulü Kanununun 10. ve 11. maddelerinde düzenlenmiştir⁶¹⁰. 6698 sayılı Kanunun 13. ve 14. maddelerinde düzenlenen ve idari başvuru niteliğini haiz bu kurumların İYUK içerisinde düzenlenen idari başvuru çeşitlerinden hangisi içerisinde olduğunu belirlemek, bunlara ilişkin doğabilecek sonuçları öngörmek bakımından gereklidir. Bu belirlemenin yapılabilmesi amacıyla öncelikle İYUK’ta yer verilen 10. ve 11. maddelere kısaca değinmek istiyoruz.

İYUK’ta yer verilen 10. maddede ilgililerin, haklarında idari davaya konu olabilecek bir işlem veya eylemin yapılması için idari makamlara başvurabilecekleri düzenlenmiştir. Görüldüğü üzere, 10. maddede düzenlenen idari başvuruda, ilgilinin İdareden bir işlem tesis etmesi ya da eylemde bulunması yönünde bir talepte bulunması söz konusudur. Aynı Kanunun 11. maddesinde ise ilgililerin idari dava açılmadan önce, idari işlemin kaldırılmasını, geri alınmasını, değiştirilmesini veya yeni bir işlem yapılmasını üst makamdan, üst makam yoksa işlemi yapmış olan makamdan, idari dava açma süresi içinde isteyebileceği düzenlenmiştir. Bu idari başvuru türünde ise ilgili hakkında İdare tarafından daha önce tesis edilmiş bir idari işlemin kaldırılmasını, geri alınmasını, değiştirilmesini veya yeni bir işlem yapılmasını talep etmektedir.

Belirtmek gerekir ki, 10. maddede düzenlemesinde idari başvuru öncesinde bir işlem bulunmadığından, yapılan başvuru sonrasında İdare tarafından tesis edilen işleme karşı dava açılmaktadır. Oysa 11. maddede idari başvuru öncesinde idari davaya konu edilebilir bir işlem var olduğundan, bu başvuru sonrasında idare tarafından verilen yanıtı değil, başvuru konusu ilk işleme karşı dava açılır⁶¹¹.

Yine 10. madde düzenlemesine göre, yapılan başvuruya otuz gün içerisinde bir yanıt verilmezse istek reddedilmiş sayılmaktadır. Buna zımni ret denilmektedir⁶¹². Başvuruda bulunanlar bu otuz günün bittiği tarihten itibaren dava açma süresinde ilgili yargı yerinde dava açabilirler. Ancak bazı durumlarda İdare ilgililere yapılan başvuruyla ilgili olarak “inceleme devam ediyor”, “başvuru kurula sunuldu, kararı size iletacağız” gibi kesin olmayan cevaplar verebilmektedir. İşte bu durumlara ilişkin olarak 10.

⁶⁰⁹ Ramazan YILDIRIM, **İdari Başvurular**, Mimoza Yayınları, 2. Baskı, 2006, s.28.

⁶¹⁰ İdari başvuruların farklı başlıklar altında sınıflandırılmasına ilişkin bilgi için bkz.: YILDIRIM, **İdari Başvurular**, s. 63 vd.

⁶¹¹ CANDAN, s.542.

⁶¹² Zımni ret müessesesi farklı kanuni düzenlemelerde öngörülmüştür. Vatandaşların kendileriyle ya da kamu ile ilgili istek ve dilekleri hakkında İdareye başvurma hakkına sahip olduklarını ve yapılan bu başvurulara gecikmeksizin cevap verilmesi gerektiğini düzenleyen Anayasa’nın 74. maddesi karşısında İdarenin kendisine yapılan başvuruları zımnen reddedebileceği yönündeki bu düzenlemenin Anayasa’ya aykırı olduğu ifade edilmektedir: YILDIRIM/FİŞ ÜSTÜN, s.224. İdarenin zımni işlemlerine ilişkin ayrıntılı bilgi için bkz.: Yusuf Sinan CANATAR, “İdarenin Başvurular Karşısında Sessiz Kalmasına Getirilen Bir Çözüm Olarak Zımni İşlemler”, **İstanbul Üniversitesi SBE**, Yayımlanmamış Yüksek Lisans Tezi, 2019.

maddede bir çözüm belirlenmiştir. Buna göre İdarenin verdiği bir cevap olmakla birlikte bu cevap kesin bir nitelik taşııyorsa başvuran bu cevabı, talebinin reddedildiğini varsayarak dava açabileceği gibi, kesin cevabın gelmesini de başvuru tarihinden itibaren en fazla dört aylık bir süre bekleyebilir. Bu süre zarfında dava açma süresi işlemeyecektir. Bununla birlikte, dava açılmaması ya da açılan davanın süreden reddedildiği durumlarda otuz günlük sürenin ardından yetkili idarece cevap verilmesi halinde, ilgili cevabın kendisine tebliğinden itibaren altmış gün içinde dava açabilecektir.

Kanunun 11. maddesinde ise, ilgilinin dava açmadan önce bir işlemin kaldırılması, geri alınması, değiştirilmesi veya yeni bir işlem yapılması amacıyla yapacağı başvurunun idari dava açma süresini durduracağı, otuz gün içerisinde cevap verilmezse isteğin reddedilmiş sayılacağı ve isteğin reddedilmesi ya da reddedilmiş sayılmasından sonra dava açma süresinin yeniden işlemeye başlayacağı ve başvurma tarihine kadar geçen sürenin de hesaba katılacağı düzenlenmiştir.

6698 sayılı Kanunun 13. maddesinde veri sorumlusuna yapılan bir “başvuru”, 14. maddesinde ise KVK Kurulu’na yapılan bir “şikâyet” başvurusu düzenlenmiştir. Veri sorumlusuna başvuru tek başına zorunlu bir idari başvuru olmamakla birlikte, ilgilinin Kurula şikâyetle bulunabilmesi için öncesinde veri sorumlusuna başvuruda bulunması zorunlu kılınmıştır. Başka bir deyişle, Kurula yapılacak şikâyetin ön şartı veri sorumlusuna bir başvuruda bulunulmuş olmasıdır. Öte yandan ilgili, Kurula şikâyetle bulunmak zorunda da değildir. Veri sorumlusuna “başvuru” yapmadan ya da bu başvurudan aldığı yanıt sonrasında doğrudan yargı yoluna başvurabilir.

Hal böyleyken, veri sorumlusu İdareye 6698 sayılı Kanun kapsamında yapılan başvurunun niteliği, bu başvuruda İdareden talep edilen şeyin içeriğine göre değişecektir. Şöyle ki, ilgili kişi 6698 sayılı Kanunun 11. maddesi uyarınca veri sorumlusu İdareye başvuruda bulunarak kendisi hakkında bir veri işlenip işlenmediğini, işlenmişse hangi verilerin işlendiğini, bunların veri işleme amacına uygun şekilde kullanılıp kullanılmadığını veya işlenen verilerin başkalarına aktarılıp aktarılmadığını öğrenmek isterse, bu başvuruyla İdareden sadece bilgi talep edildiğinden başvuru İYUK’un ne 10. maddesi ne de 11. maddesi niteliğindedir. Nitekim, sadece bilgi edinme amacıyla yapılan bir başvuruya İdare tarafından verilecek yanıt icrai nitelik taşımayacağından idari yargıda dava konusu da olmayacaktır.

Öte yandan, ilgili kişi 6698 sayılı Kanunun 11. maddesi bağlamında veri sorumlusuna başvurarak, işlenen kişisel verilerinin eksik ya da yanlış tutulması nedeniyle bunların düzeltilmesini, Kanunun 7. maddesinde belirlenen şartları sağlaması nedeniyle kişisel verilerinin silinmesini veya yok edilmesini, düzeltilen, silinen ya da yok edilen kişisel veriler hakkında ilgili verilerin aktarıldığı üçüncü kişilerin bilgilendirilmesini istediği ya da işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine ortaya çıkan sonuca itiraz etmesi hallerinde bu başvurunun İYUK’un 11. maddesi bağlamında bir başvuru olduğu söylenebilir. Nitekim bu hallerde ilgili kişi veri sorumlusu İdareden hakkındaki kişisel verilerin işlenmesi suretiyle tesis edilen idari

işlemin kaldırılması, geri alınması, değiştirilmesi yahut yeni bir işlem yapılmasını içeren bir başvuruda bulunmaktadır.

Bu noktada, İdareye yapılan 11. madde başvurusunun idari dava açma süresini durdurduğu, dolayısıyla, 30 gün içerisinde idarenin cevap vermesi halinde bu tarihten, cevap vermemesi halinde 30 günün sonunda dava açma süresinin işlemeye devam edeceği düşünüldüğünde ilgili kişinin kişisel verilerinin düzeltilmesi, silinmesi ya da yok edilmesi gibi taleplerle yapacağı başvuru bağlamında dava açma süresinin başlayacağı tarihin belirlenmesi gerekmektedir.

Kişisel verinin işlenmesi bir idari işlem olması hasebiyle, bu “veri işleme” idari işlemine karşı açılacak davada dava süresi “veri işleme” tarihinden sonra başlayacaktır. Ancak, çoğu zaman ilgilinin hakkında veri işlendiğini, bunun yanlış ya da hukuksuz şekilde işlendiğini, yine hukuka aykırı şekilde üçüncü kişilere aktarıldığını sonradan (genellikle idareye yaptığı bilgi edinme talepli başvurudan sonra) öğrendiği düşünüldüğünde dava açma süresinin bu öğrenme tarihinden sonra başlaması gerektiği ifade edilmelidir.

Bunun dışında, yukarıda ilgilinin 6698 sayılı Kanunun 11. maddesine uygun olarak sadece bilgi edinmek için İdareye yapacağı başvurulara verilen yanıtların icrai nitelik taşımayacağından ötürü idari yargıda dava konusu olmayacağını, dolayısıyla İYUK bağlamında bir başvuru niteliği taşımadığını ifade etmiştik. Her ne kadar 6698 sayılı Kanunun 13. maddesi gereği İdarenin bu taleplere 30 gün içerisinde yanıt vermesi gerektiği düzenlenmişse de İdarenin yanıt vermemesi halinde ilgilinin İdarenin bu sessizliğini “zımni ret” işlemi sayarak iptal davası açabileceği kabul edilmelidir. Nitekim, hakkında işlenen verilerin kendisine verilmesi için veri sorumlusu şirkete yaptığı başvurunun reddedilmesi sonrasında Tüketici Mahkemesinde açtığı davanın da menfaat yokluğu nedeniyle reddedilmesine ilişkin yapılan bireysel başvuruda Anayasa Mahkemesi özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile bağlantılı etkili başvuru hakkının ihlal edildiğine karar vermiştir.⁶¹³ Mahkeme kararında, “*kişisel verilerin korunmasını isteme hakkının, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığını*” belirtmiştir (§ 49). Dolayısıyla, 6698 sayılı Kanun uyarınca hakkında işlenen kişisel veriler hakkında bilgi edinmek için yapılan başvuruya veri sorumlusu İdare tarafından verilen yanıt icrai nitelik taşımadığından idari davanın bir konusu olamazken; başvuru karşısında sessiz kalınması “zımni ret” işlemi olarak kabul edilerek idari yargıda açılacak bir iptal davasının konusu olabilir.

⁶¹³ AYM, Ümit Eyüpoğlu, B.n. 2018/6161.

4.1.2. KVK Kurulunca Denetim

4.1.2.1. İlgili Kişi Tarafından Kurula Yapılan Şikâyet

6698 sayılı Kanunun 14. maddesine göre veri sorumlusuna başvurulduktan sonra veri sorumlusunca ilgilinin talebi reddedilirse, yanıt verilmezse ya da verilen yanıt ilgili için yeterli olmazsa ilgili KVK Kurulu'na şikâyet başvurusunda bulunabilir. Kanun lafzı bu hallerde Kurula şikâyet başvurusunda “bulunabilir” şeklinde düzenlendiğinden ilgilinin veri sorumlusuna başvurduktan sonra doğrudan dava açması mümkündür. Burada veri sorumlusunun bir İdare olması halinde davanın idari yargı yerinde açılması gerekir. Öte yandan Kanunun 14/2. maddesi uyarınca veri sorumlusuna başvurulmadan, başka bir deyişle doğrudan Kurula bir şikâyet başvurusunun yapılamayacağı belirlenmiştir.

Kurula yapılacak olan şikâyet başvurusunda önemli hususlardan biri şikâyet başvuru süresidir. Kanunun 14/1. maddesinde ilgili kişinin veri sorumlusunun cevabını öğrendiği tarihten itibaren 30 gün, her halde 60 gün içerisinde Kurula şikâyetle bulunması gerektiği ifade edilmiştir. Veri sorumlusunun en geç 30 gün içerisinde ilgilinin yaptığı başvuruya yanıt vermesi gerektiği Kanunun 13. maddesinde belirtilmektedir. Buna göre, veri sorumlusuna yapılan başvuruya cevap verilmesi için otuz gün beklenecek, herhangi bir cevap verilmezse otuzuncu günü takip eden günden başlamak üzere otuz gün içerisinde ilgilinin Kurula şikâyet başvurusunda bulunması gerekecektir. Başka bir deyişle ilgilinin veri sorumlusuna yaptığı başvurunun üzerinden otuz gün geçmesinden sonra şikâyetle bulunabilmesi için altmış gün değil yalnızca otuz günlük süresi bulunmaktadır. Öte yandan, veri sorumlusunun onuncu gün cevap vermesi halinde ilgilinin cevabın kendisine ulaştığı günü takip eden günden başlamak üzere otuz gün içerisinde Kurula başvuruda bulunması gerekecektir. Aksi halde süresinde yapılmadığı gerekçesiyle yapılan şikâyet Kurul tarafından reddedilecektir.

Veri sorumlusuna yapılan başvurunun üzerinden otuz gün geçtikten sonra veri sorumlusunca bir cevap verilmesi halinde ilgilinin Kurula şikâyet başvurusunu hangi sürede yapabileceği hususu ise Kurul tarafından alınan bir kararda belirlenmiştir⁶¹⁴. Buna göre, veri sorumlusunun kendisine tanınan otuz günlük süre geçtikten sonra yanıt vermesi halinde ilgilinin Kurula şikâyetle bulunmak için sahip olduğu sürede bir değişiklik olmayacaktır. Başka bir deyişle, veri sorumlusunca otuz gün geçtikten sonra bir yanıt verilse bile ilgilinin bu yanıtın ardından 30 günlük süresi bulunmamakta; her halde veri sorumlusuna başvurduğu tarihten itibaren 60 gün içerisinde Kurula şikâyet başvurusunda bulunması gerekmektedir. Kurul, bu kararında gerekçe olarak veri sorumlusuna tanınan 30 günlük süre sona erdikten sonra ilgili kişinin daha fazla bekleme yükümlülüğünün bulunmaması ve 30 günden sonra Kurula şikâyetle bulunabilmesi gerekçesine dayanmıştır.

⁶¹⁴ KVK Kurulu, 24.1.2019 tarih ve 2019/9 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu> (E.T.3.10.2022).

Kurul tarafından verilen bu kararın uygulamada vatandaş aleyhine süreci uzatmak anlamına geleceği, nitekim 6698 sayılı Kanunda veri sorumlusunda başvuru konusunda herhangi bir sınırlama bulunmadığından süresini kaçırdığı için Kurul incelemesinin reddedilmesi karşısında ilgili kişinin yeniden veri sorumlusuna başvurarak süreci tekrar başlatabileceği düşünüldüğünde, veri sorumlusu tarafından 30 günden sonra verilecek bir cevap karşısında ilgili kişinin Kurul’a başvuruda bulunması için 30 günlük bir süresinin bulunduğu kabulü Kanunun amacına daha uygun olacaktır. Ayrıca, 2577 sayılı İYUK’un 10. maddesinde yer verilen ve idari davaya konu olabilecek bir işlem ya da eylemin yapılması için İdari makamlara başvurulmasına karşın 30 gün içerisinde İdarenin cevap vermemesi halinde dava açma süresinin başlayacağını, ancak bu süre sona erdikten ya da davanın süreden reddedilmesinden sonra idarenin başvuruya yanıt vermesi durumunda ilgilinin 60 gün içerisinde dava açabileceğini öngören düzenlemeye benzer şekilde 6698 sayılı Kanun kapsamında özellikle veri sorumlusu idari makama yapılacak başvurular için de İdarenin vereceği cevaptan sonra ilgilinin Kurul’a başvurmak için 30 günlük süresinin olduğu kabul edilmelidir.

İlgili kişi, Kurula şikâyet başvurusunda bulunmadan da doğrudan dava açma hakkına sahiptir. Bu nedenle, şikâyet başvurusunun Kurul tarafından reddedilmesi durumunda sadece Kurul incelemesi yapılmamış olur. İlgili kişi, veri sorumlusu İdarenin verdiği cevaba karşı veya İdarenin başvurusu yanıtı bırakması halinde dava açabilir.

6698 sayılı Kanunun 15. maddesinin ikinci fıkrasında Kurula yapılacak şikâyetlerde 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde belirlenen kurallara uyulması gerektiği, aksi takdirde başvuruların kabul edilmeyeceği belirtilmektedir. 3071 sayılı Kanundan hareketle Kurula yapılacak şikâyetlerde ilgili kişinin dilekçesinin belirli bir konuyu içermesi, yargı mercilerinin görev alanına giren bir konuyla ilgili olmaması ve dilekçede dilekçe sahibinin adı-soyadı, imzası ile iş veya ikametgâh adresinin bulunması gerekir.

Kurula yapılacak şikâyet hususunda Kanunda yer verilen bir başka düzenleme ise Kurulun veri sorumlusundan talep edebileceği bilgi ve belgelere ilişkindir. Buna göre devlet sırrı niteliğindeki bilgi ve belgeler haricinde veri sorumlusu, Kurul tarafından inceleme konusuna ilişkin istenmiş olan tüm bilgi ve belgeleri on beş gün içerisinde göndermek zorunda olup, Kurulun gerekli görmesi halinde yerinde inceleme yapılmasına imkân vermesi gerekir. Burada tartışma konusu olabilecek husus düzenlemenin “devlet sırrı” niteliğindeki bilgi ve belgelerin hariç tutulmasına ilişkin kısmıdır. Düzenlemede devlet sırrı ifadesinin içeriğinin ne olduğu ve bir belgenin devlet sırrı olduğu yönündeki tespitin nasıl yapılacağı sorularına cevap verilmemiştir.

Mevzuatımıza bakıldığında “devlet sırrı” kavramı tanımının 5271 sayılı Ceza Muhakemesi Kanununun 47/1. maddesinde yapıldığını görüyoruz. Buna göre “*Açıklanması, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek nitelikteki bilgiler, Devlet sırrı sayılır.*” İlgili hükümde bir suça ilişkin bilgilerin Devlet

sırrı olduğu gerekçesiyle mahkemeye karşı gizli tutulamayacağı kuralı kabul edilmiştir. Bununla birlikte hapis cezasının alt sınır beş yıl ya da bundan fazla olan suçlarda tanıklık konusu bilgilerin Devlet sırrı niteliği taşıması halinde tanığın mahkemece dinleneceği ve sadece suçu açığa kavuşturma niteliği bulunan bilgilerin tutanağa geçirileceği hükmü kabul edilmiştir. Görüldüğü üzere bilgilerin devlet sırrı niteliğinde olup olmadığını belirleyecek yetkinin kimde olduğuna ilişkin bir düzenlemeye CMK’da yer verilmemiştir. Ancak 47. maddenin son fıkrasında Cumhurbaşkanının tanıklığı söz konusu olduğunda sırrın niteliğini ve mahkemeye bildirip bildirmeyeceğini kendisinin takdir edeceği kabul edilmiştir.

2577 sayılı İdari Yargılama Usulü Kanununun 20. maddesinde de doğrudan “devlet sırrı” ifadesine yer verilme de bu ifadenin kapsamı içerisinde kaldığını söyleyebileceğimiz bir takım bilgi ve belgelerin idari yargılamada kullanılmasına ilişkin düzenlemeye yer verilmiştir. Hükmün üçüncü fıkrasına göre idari yargı mercii tarafından davanın çözümünde kullanılmak üzere İdareden isteyeceği bilgi ve belgeler “Devletin güvenliğine veya yüksek menfaatlerine veya Devletin güvenliği ve yüksek menfaatleriyle birlikte yabancı devletlere de ilişkin ise, Cumhurbaşkanı ya da ilgili Cumhurbaşkanı yardımcısı veya bakan, gerekçesini bildirmek suretiyle, söz konusu bilgi ve belgeleri vermeyebilir.” Ancak idari yargı mercii vereceği kararda mahkemeye bu gerekçeyle sunulmayan bilgi ve belgelere dayanarak karar veremeyecektir.

Yine 2575 sayılı Danıştay Kanunu’nun 49/2. maddesinde yargı merciince istenen bilgi ve belgelerin Devletin Güvenliğine ve yüksek menfaatlerine veya Devletin güvenliği ve yüksek menfaatleriyle birlikte yabancı devletlere de ilişkinse, ilgili makamın, gerekçesini bildirmek suretiyle söz konusu bilgi ve belgeleri vermeyebileceği düzenlenmiştir. Burada geçen “ilgili makam” ifadesinin de karmaşıklığa yol açtığı ancak 2577 sayılı Kanunun 20/3. maddesinde yer verilen düzenlemeyle aynı şekilde okunması gerektiği ifade edilmektedir⁶¹⁵.

Öte yandan 2011 yılından bu yana gündemde olan ancak günümüze kadar yasalaşmayan Devlet Sırrı Kanunu Tasarısında bilgi ve belgelerin devlet sırrı niteliğinde olup olmadığını belirleme yetkisi Devlet Sırrı Kurulu’na bırakılmaktadır. Tasarının 6. maddesine göre bu Kurul, Başbakanın başkanlığında, Adalet, Milli Savunma, İçişleri ve Dışişleri bakanlarından meydana getirilecektir. Tasarıya göre, Genelkurmay Başkanı, Bakanlar ve Milli Güvenlik Kurulu kendi görev alanlarına ilişkin bilgi ve belgelerin devlet sırrı olarak kabul edilmesi için doğrudan Kurula başvurabilirken, diğer kamu tüzel kişilerinin ise böyle bir talebi bağlı, ilgili ya da ilişkili bulundukları Bakanlıklar aracılığıyla Kurula iletebileceklerdir⁶¹⁶. Düzenleme hala tasarı aşamasında bulunduğundan bilgi ve belgelerin devlet sırrı olup olmadığına karar veren bir kurul da bulunmamaktadır.

⁶¹⁵ Mahmut CEYLAN, “İdari Yargıda Delil Serbestisi ve Sınırları”, *KTÜ Sosyal Bilimler Enstitüsü Sosyal Bilimler Dergisi*, Y.8, S.16, Aralık 2018, s. 333.

⁶¹⁶ Tasarıya ilişkin bilgi için bkz.: Mustafa Burak YETİŞKİN, “Mukayeseli Hukukta Devlet Sırrı”, *Gazi Üniversitesi SBE Yayınlanmamış Yüksek Lisans Tezi*, 2018, s.94 vd.

Bununla birlikte, yürürlükte bulunan mevzuat incelendiğinde, CMK’da Cumhurbaşkanının takdir ettiği bilgi ve belgeleri devlet sırrı olarak kabul edebileceği; İYUK’ta ise Cumhurbaşkanının yanı sıra ilgili Cumhurbaşkanı yardımcısı veya Bakan tarafından bilgi ve belgenin devlet sırrı niteliğini haiz olduğuna karar verebileceği düzenlemeleri göze çarpmaktadır. 6698 sayılı Kanuna göre kamu tüzel kişiliğini haiz her İdare veri sorumlusu olarak kabul edilmektedir. Ancak, mevzuat ve Devlet Sırrı Kanunu Tasarısı⁶¹⁷ göz önüne alındığında her kamu tüzel kişinin kendi görev alanına giren bilgi ve belgelerle ilgili devlet sırrı olup olmadığına karar verme yetkisi bulunduğunu söylemek güçtür. Böylesi bir kabul “devlet sırrı” niteliğindeki bilgi ve belgelerin niceliğinde büyük bir artışa sebep olabilir. Bu nedenle devlet sırrı kavramının sınırlarını çizen, bu tür bilgi ve belgelerin tespitini yapacak yetkili mercileri belirleyen bir kanuni düzenleme yapılması en makul çözüm yolu olarak görünmektedir.

Kanunun 22’nci maddesinde Kurulun görev ve yetkileri arasında sayılan işlerden biri de kendisine yapılan şikâyetleri karara bağlamaktır. Buna göre, Kurul şikâyetleri inceleyerek ilgisine bir cevap verecektir. Ancak, şikâyet tarihinden itibaren altmış gün içerisinde Kurul tarafından bir cevap verilmezse talep reddedilmiş sayılmaktadır (m. 15/4). Bu düzenlemeyle, bir kamu tüzel kişisi olan KVK Kurulu’nun altmış gün sessiz kalmak suretiyle başvuruyu zımnen reddetmiş sayılacağı kabul edilmiştir. Zımni ret kurumunu düzenleyen bir başka Kanun olan 2577 sayılı İdari Yargılama Usulü Kanunu’nda da bu süre altmış gün iken, 8/7/2021 tarihli ve 7331 sayılı Kanunun 2’nci maddesiyle otuz güne indirilmiş, böylelikle yargılama sürecinin kısaltılması amaçlanmıştır. Bu bakımdan, benzer şekilde 6698 sayılı Kanundaki zımni ret süresinin de altmış gün yerine otuz gün olarak değiştirilerek yeknesaklığın sağlanmasının faydalı olacağı düşünülmektedir.

Kurul tarafından yapılan inceleme sonucunda bir ihlalin var olduğunun anlaşılması halinde, tespit edilen hukuka aykırılıkların veri sorumlusunca giderilmesine karar verilerek bu karar ilgililere tebliğ edilmektedir. Tebliğinden itibaren kararda tespit edilen hukuka aykırılıklar veri sorumlusunca otuz gün içerisinde giderilmek zorundadır (m.15/5). Kanun koyucu, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık bulunması halinde, Kurula veri işlenmesinin veya yurt dışına aktarılmasının durdurulmasına karar verme yetkisi de tanımıştır (m.15/7).

Kurul, kendisine yapılan başvurularda kişisel verilerin korunmasına ilişkin mevzuata aykırılıkları tespit ederek bu aykırılıkların giderilmesine karar verebileceği gibi, bunun yanında Kanunda söz konusu eksikliklerin bir kabahat olarak kabul edilmiş olması halinde karşılığında öngörülen idari para cezalarına da hükmetmektedir⁶¹⁸. Ancak Kanunun 18 inci maddesi uyarınca

⁶¹⁷ Söz konusu tasarıya yöneltilen eleştirilere ilişkin bkz.: Hasan SINAR, “Devlet Sırrı Kanunu Tasarısı Üzerine Düşünceler”, **Fasikül Hukuk Dergisi**, C.5, S.42, Mayıs 2013, Sayfa: 7-10; Rukiye AKKAYA KİA, “Devlet Sırrı, Kimin Sırrı?”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Özel Sayı: Prof. Dr. Nur Centel’e Armağan, Y.2013, C.19, S.2, s.749-755.

⁶¹⁸ İfade edilmelidir ki, Kurul kendisine yapılan şikâyetlerde talep edilse bile veri sorumlusunun tazminat ödemesine dair bir karar veremez. Nitekim, Kanunun 14’üncü maddesinin üçüncü fıkrasında kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat hakkına sahip olduğu kuralı düzenlenmiştir. Bu bağlamda, veri sorumlusunun bir kamu tüzel kişisi olduğu hallerde,

öngörülen idari para cezaları veri sorumlusu gerçek ve özel hukuk tüzel kişileri hakkında uygulanabilirken; söz konusu aleyhinde karar verilen veri sorumlusunun bir kamu tüzel kişisi olması halinde Kurul tarafından idari para cezasına hükmedilememektedir. Bunun yerine, Kurulun vereceği karar üzerine ilgili İdare, kararda belirlenen hukuka aykırılıklardan sorumlu olan kamu görevlileri hakkında disiplin hükümlerine göre işlem yaparak sonucu Kurula bildirmektedir.

Ancak mevcut düzenleme kişisel verilerin ihlalinin sonuçları bakımından iki noktada eşitlik ilkesine aykırılık barındırmaktadır. İlk olarak, kişisel verilerin korunmasına aykırı eylemlerde bulunanlar gerçek kişi ya da özel hukuk tüzel kişisi olması halinde yüksek miktarda idari para cezalarıyla karşılaşmaktayken bunun bir İdare tarafından gerçekleştirilmesi halinde yalnızca disiplin cezasına hükmedilebilmektedir. İkinci olarak, İdare tarafından kişisel verinin korunmasına aykırı eylemlerden sorumlu olan kamu görevlilerine vereceği disiplin cezalarında da bir eşitlik söz konusu değildir. Nitekim, 657 sayılı Devlet Memurları Kanunu dahil, kamu görevlilerine ilişkin disiplin hükümleri içeren kanunlarda kişisel veri ihlaline ilişkin eylemler ayrı bir disiplin suçu olarak belirlenmemiştir. Bu nedenle, her bir İdare aynı nitelikteki eylem karşısında farklı bir disiplin cezasına karar verebilmektedir.

Mevcut düzenlemedeki eşitsizliğin giderilmesi bakımından, öncelikle veri sorumlusu gerçek ve özel hukuk tüzel kişilerinde olduğu gibi kamu tüzel kişilerinin de idari para cezalarına muhatap kılınması ve rücu sistemi işlevsel hale getirilerek söz konusu cezaların hukuka aykırı eylemden sorumlu kamu görevlilerince üstlenilmesi sağlanabilir⁶¹⁹. Hollanda, Polonya ve Portekiz gibi ülkelerde kişisel veri ihlali halinde İdare aleyhine de idari para cezasına hükmedildiği; buna karşın Almanya, Belçika, Estonya ve Çek Cumhuriyeti ülkelerinde ülkemizdeki düzenlemeye benzer şekilde, kişisel veri ihlali bulunan İdare aleyhine idari para cezasına hükmedilemediği ifade edilmektedir⁶²⁰.

Kanun koyucunun İdare aleyhine para cezasına hükmedilememesi yönündeki kabulünün devam etmesi halindeyse, kamu görevlileri hakkında disiplin cezalarını düzenleyen kanunlarda kişisel veri ihlalinin bir disiplin suçu olarak kabul edilmesi ve yine bu suçun karşılığında tesis edilecek disiplin cezasının da açıkça belirlenmesi yönünde değişiklik yapılması yerinde olacaktır⁶²¹. En azından, bu şekilde kişisel veri ihlali halinde tesis edilecek disiplin cezaları konusunda bir eşitlik sağlanmış olur.

4.1.2.2. KVK Kurulunun Resen Harekete Geçmesi

6698 sayılı Kanunun 15 inci maddesi “Şikâyet üzerine veya resen incelemenin usul ve esasları” başlığını taşımaktadır. Buna göre, Kurulun şikâyet üzerine veya ihlal iddiasını öğrenmesi halinde resen,

maddi ve/veya manevi bir zarara uğradığı gerekçesiyle tazminat talebinde bulunmak isteyen ilgililerin idari yargı yerinde tam yargı davası açması gerekir.

⁶¹⁹ ALTINDAĞ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, s.182.

⁶²⁰ ERDOĞMUŞ, Talha. "Kişisel Verileri İhlal Eden İdareye Karşı İdari Para Cezası Uygulanmaması Sorunu", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, C.10, Y.2023, S.1 s.144-146. <https://dergipark.org.tr/tr/pub/imuhfd/issue/78403/1211491> (E.T. 1.7.2023).

⁶²¹ TANSUĞ, s.199.

görev alanına giren konularda gerekli incelemeleri yapacağı kabul edilmiştir. Dolayısıyla, yukarıda “KVK Kuruluna Şikâyet Yoluyla Denetim” başlığı altında anlatılan hususlar Kurulun resen harekete geçtiği hallerde de geçerlidir. Bununla birlikte, Kurulun veri ihlali iddiasını tespit etmesi nedeniyle kendiliğinden veya 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşıyan bir dilekçe ile ihbarda bulunulması nedeniyle harekete geçtiği durumlarda ortada bir “şikâyetçi” ilgili kişi bulunmadığından, altmış gün içerisinde karar verme zorunluluğu bulunmamaktadır.

4.2.Yargısal Denetim

4.2.1. KVK Kurulu Kararlarına Karşı Yargı Yolu

6698 sayılı Kanunun 18. maddesinin 3. fıkrası uyarınca Kurulca verilen idari para cezalarına karşı açılacak davalarda idare mahkemeleri görevli kılınmıştır. Söz konusu düzenleme, 2 Mart 2024 tarihli 7499 sayılı Kanunun 35. maddesiyle getirilmiş olup bundan önce ikili bir denetleme uygulaması gerçekleştirilmekteydi. Nitekim 5326 sayılı Kabahatler Kanunu’nun 3. maddesinde, diğer kanunlarda idari yaptırım kararlarına karşı kanun yoluna ilişkin hükümler bulunmaması halinde bu Kanunun ilgili hükmünün uygulanacağı belirlenmiş, 27/8. maddesinde ise idari yaptırım kararı bir idari işlemin parçası olarak verilmiş ve aynı kişiyle ilgili idari yargının görev alanına giren başka kararlar da alınmışsa, idari yaptırıma ilişkin hukuka aykırılık iddialarının bu işlemin iptali talebiyle birlikte idari yargıda görüleceği kuralına yer verilmiştir.

KVKK’de 2 Mart 2024 tarihinden önce Kurul kararlarına karşı yapılacak itirazlara yönelik kanun yoluna ilişkin bir hüküm bulunmadığından, Kurulun vermiş olduğu idari para cezalarına karşı sulh ceza hakimliğine; idari para cezasıyla birlikte idari yargının görev alanına giren veri işleme faaliyetinin durdurulması, veri ihlalinin giderilmesi, yurt dışına veri aktarımının durdurulması gibi başka idari yaptırımlara da karar verildiğinde idari yargıya başvurulmaktaydı. Ancak sonradan yapılan düzenlemeyle tüm Kurul kararlarına karşı yapılan itirazlar idari yargı yerince incelenmektedir.

İki ihtimalli bir denetim uygulaması en başta kararın hangi yargı yerinde denetleneceği hususunda belirsizlik oluşturmakta, bu da zaman kaybına neden olmakta, denetimin gücü ve etkisini azaltmaktaydı. Ayrıca, sulh ceza hakimliği tarafından verilen kararların içtihadı dönüşmemesi nedeniyle KVKK’nin yorumlanmasına fayda sağlayacak kararlar da oluşmamaktaydı⁶²². Dolayısıyla, Kurul kararlarına karşı idari yargı yolunun belirlenmesi içtihat birliğini ve daha etkili bir denetimi sağlayacağı için olumlu bir değişim olduğu söylenebilir. Öte yandan, KVKK’nin 18/4. maddesi uyarınca

⁶²² KAYA, s.58 vd.

kamu idareleri hakkında idari para cezasına karar verilemediğinden, söz konusu düzenlemenin İdareler hakkında verilen kararlar bakımından bir etki yaratmadığı ifade edilmelidir⁶²³.

4.2.2. Veri Sorumlusu İdarenin Yargısal Denetimi

Kişisel verilerin korunması, modern hukuk devletinin en temel gereklerinden biridir. Anayasamızın 20. maddesinde herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu açıkça belirtilmiştir. Bununla birlikte, kamu hizmetlerinin etkin bir şekilde yerine getirilebilmesi için idarenin zaman zaman kişisel verileri işlemesi kaçınılmazdır. Ancak idarenin bu işleme faaliyetini yerine getirirken hukuka uygun davranması, keyfi ve ölçsüz müdahalelerden kaçınması gerekmektedir. Aksi takdirde, idarenin işlem ve eylemleri hukuka aykırı hale gelecek ve kişilerin temel hak ve özgürlüklerine zarar verecektir. İşte bu noktada, hukuk devleti ilkesinin bir gereği olarak idarenin hukuka aykırı işlem ve eylemlerine karşı yargı yolu güvencesi devreye girmektedir. Nitekim Anayasamızın 125. maddesinde, idarenin her türlü eylem ve işlemine karşı yargı yolunun açık olduğu ifade edilmektedir. Bu hüküm, idarenin kişisel verileri hukuka aykırı bir şekilde işlemesi durumunda, bireylerin hak arama özgürlüğünü ve hukukun üstünlüğünü teminat altına almaktadır.

İdarenin hukuka uygunluğunun denetlenmesi ve faaliyetleri nedeniyle hakları ihlal edilen kişilerin mağduriyetlerinin giderilmesi amacıyla, idari yargıda iptal davası ve tam yargı davası olmak üzere iki temel dava türü öngörülmüştür⁶²⁴.

4.2.2.1. İptal Davası

2577 sayılı İYUK'nun 2. maddesinin ilk fıkrasında iptal davası “*İdarî işlemler hakkında yetki, şekil, sebep, konu ve maksat yönlerinden biri ile hukuka aykırı olduklarından dolayı iptalleri için menfaatleri ihlâl edilenler tarafından açılan*” davalar şeklinde tanımlanırken, tam yargı davası “*İdari eylem ve işlemlerden dolayı kişisel hakları doğrudan muhtel olanlar tarafından açılan*” davalar şeklinde tanımlanmıştır. İptal davasının açılabilmesi için dava konusu işlem ile davacı arasında makul, akla yatkın, güncel ve meşru bir alaka bulunması, kanuni ifadesiyle davacının dava açmada bir menfaatinin bulunması gerekir; tam yargı davasında davacının kişisel bir hakkının zarara uğraması gerekir⁶²⁵.

İptal davasının açılabilmesi için, ortada kesin ve yürütülmesi zorunlu bir idari işlemin bulunması gerekir⁶²⁶. İdari işlem “*bir idari makam tarafından, bir kamu hizmetinin yürütülmesi amacıyla, İdare hukukunun kendisine tanıdığı kamu gücünü kullanarak ve tek yanlı iradeyle yapılan kesin (idari*

⁶²³ Ali BALKAN, “Türk İdare Hukukunda Kişisel Verilerin Korunması Hakkı ve İdarenin Sorumluluğu”, **Hatay Mustafa Kemal Üniversitesi**, Doktora Tezi, 2023, s.448.

⁶²⁴ CANDAN, s.76.

⁶²⁵ Turan YILDIRIM, içinde **Açıklamalı-Notlu İdari Yargılama Usulü Kanunu**, s.24.

⁶²⁶ Turan YILDIRIM, içinde **Açıklamalı-Notlu İdari Yargılama Usulü Kanunu**, s.20.

*prosedürün son aşamasını da geçmiş) ve yürütülmesi zorunlu (icrai) her türlü işlem” olarak tanımlanmaktadır*⁶²⁷. Bu bağlamda Danıştay'ın bir kararında, bir belediyede "Personel Devam Çizelgesi ve Kontrol Projesi" adı altında tüm kamu çalışanlarının parmak izlerinin alınarak kişisel verilerinin işlenmesinin, bu kişilerin hukuki statülerinde değişiklik meydana getirdiği belirtilmiştir. Kararda, söz konusu uygulamanın kesin ve yürütülmesi zorunlu bir idari işlem niteliğinde olduğu ve bu nedenle ilgililerin bu işleme karşı iptal davası açabileceği ifade edilmiştir⁶²⁸.

Öte yandan iptal davası, yalnızca bireysel çıkarların korunmasını hedefleyen bir hukuki çare olmanın ötesinde, idarenin hukuka uygun hareket etmesini sağlayarak kamu yararına hizmet eden önemli bir denetim mekanizmasıdır. Bu davanın hukuk devleti ilkesinin hayata geçirilmesindeki rolü göz önüne alındığında, objektif nitelikte olduğu kabul edilmektedir. Dolayısıyla, iptal davalarında verilen kararlar sadece dava konusu somut olay için değil, benzer nitelikteki tüm uyuşmazlıklar bakımından da geçerli ve bağlayıcı olmaktadır⁶²⁹.

Davacı tarafından bir belediye başkanlığına ait binada kamu çalışanlarının faaliyetlerini yürüttüğü servislerde uygulanan kameralı takip sistemine son verilmesi istemiyle yapılan başvurunun reddine ilişkin işleme karşı iptal davası açılmıştır. Yargıla süreci sonunda dosyayı inceleyen Danıştay, kamu kurumlarına ait binaların giriş ve çıkışlarının, bina çevresindeki alanların, koridorların ve otoparkların kamu düzeni ve güvenliğinin sağlanması amacıyla güvenlik kameraları ile izlenmesini ve görüntü kayıtlarının toplanmasını hukuka uygun bulmuştur. Ancak kararda, çalışanların ofislerini ve servislerini de kapsayacak şekilde kameraların yerleştirilmesi ve kişilerin görüntülerinin kaydedilmesinin kamu düzeni ve güvenlik amacını aşan, ölçülülük ilkesiyle bağdaşmayan bir uygulama olduğu yönünde karar vermiştir⁶³⁰.

Bir başka kararda Danıştay, bir üniversitenin hizmet binaları içerisinde mevcut kamera ile izleme sisteminin risk oluşturmeyen birim ve bölgelerden kaldırılması istemiyle yaptığı başvurunun reddine ilişkin idari işlemin iptali için açılan davada, uygulamanın sınırlarını ve usulünü belirleyen yasal bir dayanağın bulunmaması, toplanan görüntülerin ileride başka amaçlarla kullanılmayacağına dair bir güvencenin olmaması, üniversite alanındaki giriş-çıkış noktaları gibi güvenlik açısından kritik bölgelerin zaten kameralarla izlenmesi, anfi ve dersliklere yerleştirilen kameraların iş yerinin güvenliğini sağlama amacını aşarak çalışanların, öğrencilerin ve öğretim üyelerinin özel hayatını ve iletişimini izlemeye varacak şekilde kullanılmasının özel hayatın gizliliği hakkını ihlal ettiği ve Anayasal ilkelerle bağdaşmadığı gerekçeleriyle dava konusu işlemin iptaline karar verilmesi gerektiği yönünde karar vermiştir⁶³¹.

⁶²⁷ CANDAN, s.84.

⁶²⁸ Danıştay 12.D., E.2005/6811, K.2006/1959, aktaran: BAŞAR, s. 43.

⁶²⁹ Turan YILDIRIM, içinde **Açıklamalı-Notlu İdari Yargılama Usulü Kanunu**, s.19.

⁶³⁰ Danıştay 10.D., E. 2019/12230, K. 2021/41 (Lexpera).

⁶³¹ Danıştay 10.D, E. 2015/2995, K. 2018/1736 (Lexpera).

İdare, kimi zaman düzenleyici işlemleriyle de kişisel verilerin korunması hakkına müdahalede bulunabilmektedir. Düzenleyici işlemlerin uygulamasından etkilenen ya da yakın gelecekte etkilenecek olan kimseler⁶³², bu olumsuz sonuçların bertarafı için iptal davası açabilirler. Örneğin, özürlülük bilgisinin nüfus cüzdanlarında yer almasını öngören yönetmelik hükümlerinin iptali istemiyle iptal davası açılmıştır. Danıştay İDDK kararında, nüfus cüzdanının Türk vatandaşlığının ispatında ve çeşitli hukuki işlemlerde kullanılan temel bir belge olduğu gerçeğinden hareketle, özürlülük oranının bu belgede yer almasının, kişinin özel durumunun kimlik gösterilen her an başkaları tarafından öğrenilmesine sebep olacağına dikkat çekmiş, bunun sonucunda, özürlü vatandaşların gündelik hayatlarında sürekli olarak özel durumlarını ifşa etmek zorunda kalabileceklerini ve ayrımcılığa uğrama riskiyle karşı karşıya kalabileceklerini belirlemiştir. Bu nedenle Kurul, özürlü bireylere yalnızca gerekli hallerde ibraz edebilecekleri ayrı bir kimlik kartı verilmesinin hem hukuki düzenlemelere uygun olacağını hem de kişilerin temel hak ve özgürlüklerini daha iyi koruyacağını ifade ederek, dava konusu yönetmelik hükümlerinin hukuka aykırı olduğuna karar vermiştir⁶³³.

4.2.2.2. Tam Yargı Davası

İdarenin veri işleme faaliyetlerinin sebep olduğu sonuçlar nedeniyle bireylerin maddi veya manevi zarara uğraması mümkündür. Bu gibi durumlarda, zarara uğrayan kişiler idari yargıda tam yargı davası açarak uğradıkları zararların tazminini talep edebilirler. 2577 sayılı Kanun'un 2. maddesinde tam yargı davası "*İdari eylem ve işlemlerden dolayı kişisel hakları doğrudan muhtel olanlar tarafından açılan*" davalar şeklinde tanımlanmıştır. Dolayısıyla, tam yargı davasını kişisel bir hakkı doğrudan zarara uğrayan kişiler açabilir. Ayrıca, tam yargı davasının açılabilmesi için ortada idarenin veri işleme faaliyetinden kaynaklanan bir zararın bulunması, bu zarar ile idari faaliyet arasında illiyet bağının mevcut olması ve idarenin kusurlu veya kusursuz sorumluluğunun doğması gerekmektedir⁶³⁴.

İdarenin faaliyetleri nedeniyle bireylerin mal varlığında veya şahsi varlığında meydana gelen zararların telafi edilmesi içinse tam yargı davaları kabul edilmiştir. Tam yargı davaları, sadece zararın giderilmesi sonucunu doğurmakla kalmaz; aynı zamanda idarenin hizmet sunumundaki aksaklıkları da yargılar ve ideal idare anlayışının hayata geçirilmesine katkı sağlar⁶³⁵. Örneğin, bir kamu kurumunda

⁶³² YILDIRIM, işlem ile davacı arasındaki menfaatin halihazırda veya yakın gelecekte bulunması gerektiğini, bu bağlamda özellikle düzenleyici işlemlerin ileride muhatabı olacak kimseler tarafından bunların kendilerine uygulanmasından önce dava açabilmelerinin mümkün olması gerektiğini ifade etmektedir: Turan YILDIRIM, içinde **Açıklamalı-Notlu İdari Yargılama Usulü Kanunu**, s.26.

⁶³³ Danıştay İDDK, E. 2008/1763, K. 2012/2340, DD, Y.2013, S.133, s.128 vd. Ayrıca e-Nabız konulu Genelge'nin iptaline ilişkin Danıştay 15.D., E. 2015/2900, K. 2018/3876, T.18.4.2018. (danistay.gov.tr). YÖK tarafından, üniversite ile aile iş birliğinin etkin hale getirilmesi amacıyla adli ve idari işlem yapılan öğrenciler ile yasa dışı faaliyette bulunan öğrencilerin durumlarının ailelerine bildirilmesini öngören ve tüm üniversitelere gönderilen yazının, öğrencilere ait kişisel verilerin işlenmesini gerektirdiği ve buna yönelik kanuni bir dayanağının bulunmadığı gerekçesiyle iptaline ilişkin Danıştay İDDK, E. 2021/1733, K. 2022/286 (Lexpera).

⁶³⁴ Ayrıntılı bilgi için bkz.: "**3. İDARENİN KİŞİSEL VERİ İŞLEMESİNDEN DOĞAN HUKUKİ SORUMLULUĞU**" başlığı.

⁶³⁵ Onur KARAHANOGULLARI, **İdari Yargı: İdarenin Hukuka Zorlanması**, Turhan Kitabevi, 2019, s.224.

alıřan memurun, kurum tarafından hukuka aykırı řekilde iřlenen saėlık verileri nedeniyle iř yerinde ayrımcılıėa uėraması ve bunun sonucunda psikolojik rahatsızlık geirmesi durumunda memur, yařadığı maddi ve manevi zararların tazmini iin tam yargı davası aabilir.

Yine, bir okulun, ėrencilerin psikolojik geliřimini izlemek amacıyla topladıėı verileri gerekli gvenlik nlemlerini almadan saklaması ve bu verilerin siber saldırı sonucu ele geirilmesi nedeniyle ėrencilerin ruh saėlıėının olumsuz etkilenmesi halinde, idarenin kusurlu sorumluluėuna dayanılarak tam yargı davası aılabilir. Nitekim, askerlik muayenesi sonucu dzenlenen “Askerliėe Elveriřli Deėildir” raporunun İdarenin kusuruyla basına sızdırılması nedeniyle uėranılan manevi zararın tazmini nedeniyle aılan davada Danıřtay kiřinin manevi zararı bulunduėunu belirlemiř, bu nedenle tazminat talebini kısmen kabul etmiřtir⁶³⁶. Bařka bir davada, ruhsatsız silah bulundurmaktan ceza alan kiřinin, cezasının infaz edilmesine raėmen bu bilginin Genel Bilgi Toplama (GBT) sisteminde gncellenmemesi sebebiyle tekrar tekrar gzaltına alınması nedeniyle uėradığı manevi zararların tazmini talebini, Danıřtay İdarenin hizmeti kusuru bulunduėu gerekesiyle kabul etmiřtir⁶³⁷.

⁶³⁶ Danıřtay 15.D. E.2015/10101, K.2016/664, T.8.2.2016 (Lexpera)

⁶³⁷ Danıřtay 10.D., E. 2007/1376, K. 2007/4756, T.17.10.2007 (Kazancı).

SONUÇ

Kişisel verilerin işlenmesine ilişkin mevzuat incelendiğinde, ülkemizde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda kişisel verinin "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde tanımlandığı ve tüzel kişilere ilişkin verilerin kapsam dışında bırakıldığı tespit edilmiştir. Uluslararası metinlerde de benzer bir yaklaşımın benimsendiği görülmüştür. Kişisel verilerin korunması hakkının temel bir hak olduğu ve özünde insanın kişiliği ile onun özel alanını korumayı amaçladığı dikkate alındığında, tüzel kişilerin bu kapsamda korunmamasının hakkın amacıyla uyumlu olduğu sonucuna varılmıştır.

Ölmüş kişilerin verilerinin korunmasına ilişkin olarak mevzuatta bazı sorunlar tespit edilmiştir. Kural olarak, kişilik ölümle sona erdiğinden, ölmüş kişilerin kişisel verilerinin korunmadığı görülmektedir. Bu sorunun çözümü için iki önemli husus ön plana çıkmaktadır. Bunlardan ilki, parasal değeri olan sosyal medya ve çeşitli bulut hesaplarının miras olarak kabul edilerek mirasçılara verilmesi; ikincisi ise kişinin yaşadığı dönemdeki özel hayatının gizliliğinin öldükten sonra da korunmasıdır. Çözüm önerisi olarak, ilgili kişinin ölümünden önce kişisel verilerinin korunması için bir kişi tayin etmesi (uzatılmış kişilik hakkı teorisi) veya kişisel verilerinin ölümünden sonra kimlere iletebileceğini çeşitli veri türleri için ayrı ayrı belirlemesi yoluyla koruma sağlanabileceği değerlendirilmiştir.

KVKK'de sınırlı sayıda veri türü özel nitelikli olarak kabul edilmiştir. Ancak, teknolojik gelişmeler sonucunda, örneğin bir kişinin yüz ya da boy fotoğrafından madde bağımlısı olup olmadığının anlaşılabilmesi veya sosyal medya platformlarına yüklenen fotoğraflardan ilgilinin depresyonda olup olmadığının tespit edilebilmesi gibi durumlar ortaya çıkmıştır. Bu nedenle, özel nitelikli kişisel verilerin sınırlı sayıda belirlenmesine yönelik eleştirel yaklaşımlar mevcuttur. Bu yaklaşımlardan ilki 'bağlamsal görüş' olup, bir verinin hassas nitelikte olup olmadığının değerlendirilmesinde verinin işlenme koşulları ve mevcut şartların bütüncül olarak ele alınması gerektiğini savunmaktadır. İkinci yaklaşım ise 'amaçsal görüş' olarak tanımlanmakta ve bir verinin hassas niteliğinin işlenme amacına göre belirlenmesi gerektiğini ileri sürmektedir. Fotoğraf verisinin doğrudan özel nitelikli veri olarak kabul edilmesinin mümkün olmadığı, ancak fotoğrafın kişi hakkında dini veya siyasi görüşünü belirlemek amacıyla işlenmesi halinde özel nitelikli veri olarak kabul edilmesi gerektiği sonucuna varılmıştır.

KVKK'nin 28. maddesinde, kanunun tamamen veya kısmen uygulanmayacağı veri işleme halleri (istisnalar) düzenlenmiştir. Ancak, bu istisnaların kapsamı ve uygulanması konusunda bazı belirsizlikler ve çelişkiler tespit edilmiştir. İlk olarak, KVKK'nin 28/1-c maddesine göre, kişisel verilerin sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi halinde, ilgili kanun hükümleri uygulanmayacaktır. Burada en dikkat çeken husus, kişisel verilerin ifade özgürlüğü kapsamında işlenmesidir. İdarenin ifade özgürlüğü kapsamında kişisel veri işleyip işleyemeyeceğine ilişkin olarak, temel hak ve özgürlükler birer insan hakkı olduğundan, idarenin bu

hakların kullanıcısı olamayacağı savunulabilirse de İdarenin ifade özgürlüğünün kullanımını sağlamaya yönelik yine bu hak kapsamında kalan pozitif yükümlülüklerini yerine getirmesine yardımcı olmak amacıyla Türkiye Radyo ve Televizyon Kurumu (TRT) kurulduğu, dolayısıyla bu ve benzeri kurumlar aracılığıyla yapılan yayınlarda işlenen kişisel verilerin ifade özgürlüğü kapsamında işlendiğinin kabul edilebileceği sonucuna varılmıştır.

İkinci olarak, KVKK'nın 28/1-ç ve 28/2-a maddeleri arasında bir çelişki olduğu görülmektedir. 28/1-ç maddesine göre, millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak önleyici faaliyetler kapsamında, kanunla görev ve yetki verilmiş kamu kurum ve kuruluşlarının yürüttüğü önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenen kişisel veriler kanun kapsamı dışındadır. İlgili düzenlemedeki "kamu düzenini ve kamu güvenliğini sağlamaya yönelik... önleyici ...faaliyetler" ifadesinden idari kolluk faaliyetlerinin bu kapsamda olduğu anlaşılmaktadır. Ancak, 28/2-a maddesi de idari kolluk ve adli kolluk faaliyetlerini içerecek şekilde, suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması halinde, bazı maddeler hariç kanunun diğer hükümlerinin uygulanacağını belirtmektedir. Bu durum, idari kolluk ve adli kolluk faaliyetleri açısından bir belirsizlik yaratmaktadır. Bu belirsizliğin, "kamu düzeni" ve "kamu güvenliği" ifadelerinin 28/1-ç maddesinden çıkarılmasıyla giderilebileceği önerilmektedir.

Son olarak, KVKK'nın 28/2-ç maddesi ile 28/1-ç maddesi arasında da bir çelişki olduğu tespit edilmiştir. 28/2-ç maddesi, bütçe, vergi ve mali konulara ilişkin olarak devletin ekonomik ve mali çıkarlarının korunması için kişisel veri işlenmesi halinde, bazı maddelerin uygulanmayacağını belirtirken; 28/1-ç maddesi, ekonomik güvenliği sağlamaya yönelik önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenen kişisel verilerin kanun kapsamı dışında olduğunu ifade etmektedir. Halbuki, "*bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik çıkarlarının korunması*" amacıyla yapılacak işlemlerin genel anlamda ekonomik güvenliğin sağlanması amacını taşıyacağı söylenebilir. Dolayısıyla, hangi hükmün ne zaman uygulanması gerektiği konusunda ortaya çıkan bu çelişkinin giderilmesi için, somut olaya göre değerlendirme yapılması ve nihai kararın görevli yargı yeri tarafından verilmesi gerektiği sonucuna varılmıştır.

Veri güvenliğine ilişkin alınan önlemlerin, veri sorumlusunun kusurunun belirlenmesi bakımından önem taşıdığı tespit edilmiştir. Bu bağlamda, veri sorumlusunun makul teknik ve idari tedbirleri almasına rağmen kişisel verilerin hukuka aykırı şekilde işlenmesine veya verilere erişilmesine engel olamaması durumunda sorumluluğunun devam edip etmeyeceği sorusu gündeme gelmiştir. 6698 sayılı Kanunu'nun 12/1. maddesi, veri sorumlusunun "uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak" zorunda olduğunu belirtmektedir. Buna göre, veri sorumlusunun piyasada yeterli kabul edilecek düzeyde ve KVK Kurulu kararlarını da dikkate alarak veri güvenliğini sağlayan teknik ve idari tedbirleri aldıktan sonra, Kanunun 18/1-b maddesinde düzenlenen "veri güvenliğine ilişkin yükümlülüklerini yerine getirmeme" kabahatinden dolayı cezalandırılmaması gerektiği sonucuna varılmıştır.

KVKK'de her türlü kişisel verinin işlenmesi için "açık rıza" aranması nedeniyle, kanunun daha ağır koşullar barındırdığı ve bunun bir tür "rıza yorgunluğuna" sebep olabileceği eleştirisi yapılmıştır. Genel nitelikli veriler ile hassas veriler arasında ayırım yapılmaksızın her türlü veri işleme faaliyeti için açık rıza alınmasının, ilgililerin açık rıza vermekten kaçınmasına veya rıza metnini okumadan onay vermesine yol açabileceği belirtilmiştir. Ayrıca, her veri işleme faaliyeti için açık rıza alınmasının ek iş yükü ve prosedür anlamına geleceği de vurgulanmıştır. Bu nedenle, Avrupa Birliği düzenlemelerinde olduğu gibi, genel nitelikli kişisel verilerin işlenmesinde açık rıza yerine sadece "rıza" verilmesinin aranması ve örtülü rıza beyanının da yeterli kabul edilmesi önerilmiştir.

Kişisel verilerin korunması hakkının, Anayasa ve AİHS kapsamında özel hayatın gizliliği hakkı içerisinde değerlendirildiği ve bir kişilik hakkı olarak kabul edildiği tespit edilmiş, bu bağlamda, kişisel verilerin işlenmesine rıza gösterme hakkının da kişiye sıkı sıkıya bağlı haklardan biri olduğu sonucuna varılmıştır. Buradan hareketle Türk Medeni Kanunu'nun 16. maddesi uyarınca, ayırt etme gücüne sahip küçüğün kendisine sıkı sıkıya bağlı haklarını kullanırken kanuni temsilcisinin iznine ihtiyacı olmadığından, kişisel verilerin işlenmesine rıza gösteren ayırt etme gücüne sahip küçüğün rızasının hukuken geçerli bir rıza olarak kabul edilmesi gerekir. Ancak, küçüğün ayırt etme gücünün varlığı konusunda her somut olaya göre ayrı değerlendirme yapılması ve kişisel verilerinin işlenmesine gösterdiği rızanın hukuki sonuçlarını öngörüp öngöremediğinin dikkatle irdelenmesi gerekmektedir.

Anayasa'nın 104. maddesinin 17. fıkrasında, CBK'lerin çıkarılamayacağı konular arasında "Anayasada münhasıran kanunla düzenlenmesi öngörülen konular" sayılmıştır. Anayasa Mahkemesi kararlarında, anayasa koyucunun kanunla düzenlenmesini öngördüğü konuların bu kapsamda kabul edilmesi gerektiği ifade edilmektedir. Anayasa'nın 20. maddesinde, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtildiğinden, bu konuda CBK ile düzenleme yapılmasının mümkün olmadığı sonucuna varılmıştır. Ayrıca, Anayasa'nın 104. maddesinin 17. fıkrasına göre, olağan dönem CBK'lerinin konu bakımından sınırlarından biri de Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleridir. Kişisel verilerin korunmasını isteme hakkı, Anayasa'nın ikinci kısmının ikinci bölümünde düzenlenen özel hayatın gizliliği hakkının bir parçası olduğundan, bu konuda CBK ile düzenleme yapılması Anayasa'ya aykırı olacaktır. Son olarak, kişisel verilerin işlenebileceğinin öngörülmesi, kişisel verilerin korunması hakkına getirilen bir sınırlama niteliği taşımaktadır. Anayasa'nın 13. maddesi uyarınca temel hak ve özgürlüklere getirilecek sınırlamalar ancak kanunla yapılabileceğinden, bu alanda yapılacak bir CBK düzenlemesinin de Anayasa'ya aykırı olacağı kabul edilmelidir.

KVKK'nin 5. maddesinde, veri sorumlusunun hukuki yükümlülükleri gereği kişisel veri işleme halinde açık rızanın aranmayacağı düzenlenmiştir. Ancak, "hukuki yükümlülük" kavramının kapsamı Kanun'da açıkça belirtilmemiştir. Avrupa Birliği mevzuatında (Direktif ve Tüzük) yer alan benzer düzenlemelerin sözleşmeden kaynaklanan yükümlülükleri kapsamadığı ifade edilmektedir. KVKK bakımından da "hukuki yükümlülük" ifadesinin sözleşmeden kaynaklanan yükümlülükleri

kapsamadığı sonucuna varılmıştır. Bu nedenle, kural olarak veri sorumlusu İdarenin, mevzuattan kaynaklanan hukuki yükümlülükleri nedeniyle açık rıza olmaksızın veri işleyebileceği kabul edilmelidir.

İdarenin bir veri sorumlusu olarak, KVKK'nin 5/2(f) maddesinde belirlenen meşru menfaatinin korumak amacıyla kişisel veri işleyip işleyemeyeceği hususu da değerlendirilmiştir. 6698 sayılı Kanuna göre kamu tüzel kişileri veri sorumlusu olabilir ve bu nedenle İdarenin kural olarak meşru menfaatinin korumak amacıyla veri işlemesi mümkündür. Ancak İdarenin, idari faaliyetleri yerine getirirken kamu yararı amacıyla hareket etmesi gerektiğinden, kamusal görevlerini yerine getirirken meşru menfaatine dayalı olarak veri işleyemeyeceği, bunun yerine aynı maddenin (a) ve (ç) bentlerine düzenlenen 'kanunlarda öngörülmesi' ve 'hukuki yükümlülüklerinin yerine getirilmesi için zorunlu olması' şartlarına dayanabileceği sonucuna varılmıştır. Bununla birlikte, İdarenin özel hukuka dayalı hukuki işlemlerinde ise meşru menfaatleri doğrultusunda açık rıza olmaksızın kişisel veri işleminin mümkün olduğu kabul edilmelidir.

Sağlık hizmetlerinin sunumunda, hasta mahremiyeti ve kişisel verilerin korunması büyük önem taşımaktadır. Eğitim ve araştırma hastanelerinde, hastanın açık rızası alınmadan, tedaviyle doğrudan ilgili olmayan kişilerin (örneğin tıp öğrencileri) tıbbi müdahale sırasında bulunması ve hastanın kişisel sağlık bilgilerine vakıf olması hukuka aykırıdır. Nitekim, kişisel sağlık verilerinin açık rıza olmaksızın işlenebilmesi için sayılan amaçlar arasında "eğitim" amacı yer almamaktadır. Benzer şekilde, muayene sırasında hastanın yakınının da odaya girmesi ve hasta hakkındaki sağlık bilgilerine vakıf olması, hastanın açık rızası olmadan sağlık verilerinin üçüncü kişiyle paylaşılması anlamına geleceğinden hukuka aykırıdır. Hastanın yakınıyla birlikte hekimin yanına girmesi ve ses çıkarmaması bir rıza olarak kabul edilebilirse de KVKK bağlamında "açık rıza" olarak değerlendirilemez. Ülkemizin sosyolojik şartları göz önüne alındığında, hekimin hasta yakınına her zaman dışarı çıkarması mümkün olmayabilir ve bu konudaki ısrar bazı olumsuz sonuçlar doğurabilir. Bu nedenle, konunun yönetmelikle düzenlenmesi, toplumun bilinçlendirilmesi, dijital araçların kullanılması ile sağlık personeline karar verme yetkisi ve sorumluluğu verilmesi gibi çözüm önerileri sunulmuştur.

Kişisel sağlık verilerinin korunması ile toplum sağlığının korunması arasındaki hassas denge, özellikle bulaşıcı hastalıklar söz konusu olduğunda daha da önem kazanmaktadır. Örneğin, Türkiye'de HIV pozitif olan kişilerin eşlerine ya da eş adaylarına sağlık personeline bilgi verilmesi yönünde açık bir yasal düzenleme bulunmamaktadır. Günümüzde HIV/AIDS hastalığı ölümcül bir hastalık olarak kabul edilmemekle birlikte, hasta kişinin tedaviyi reddetmesi, düzenli şekilde devam etmemesi veya cinsel birlikteliklerinde korunmaması halinde eşin, hatta gebenin çocuğunun beden bütünlüğünü tehlikeye sokması ihtimali yüksektir. Bu durumda, üçüncü kişilerin yaşam hakkının, hastanın kişisel verilerinin korunması hakkından daha üstün olduğu kabul edilerek, eş veya eş adayına bilgilendirme yapılması gerektiği sonucuna varılmıştır.

Millî Eğitim Bakanlığı, öğrencilere sunduğu dijital eğitim materyallerini Eğitim Bilişim Ağı (EBA) sistemi üzerinden sağlamaktadır. EBA'nın internet sitesindeki "Gizlilik Politikası" metninde, kullanıcıların çeşitli kişisel verilerinin işleneceği belirtilmekte ve bu işlemenin "aramızdaki hizmet ve sözleşme ilişkisi çerçevesinde ve süresince, meşru menfaat işleme şartına dayanılarak" gerçekleştirileceği ifade edilmektedir. Ancak, bu ifadelerin hukuki açıdan hatalı olduğu tespit edilmiştir. Öncelikle, eğitim hizmetlerinin sunulması İdareye Anayasal ve yasal bir görev olarak verilmiştir. Çocuk, okula kaydolmakla "öğrenci" statüsü kazanmakta ve Bakanlık ile öğrenci arasında imzalanmış bir hizmet sözleşmesi bulunmamaktadır. EBA sistemi de eğitim kamu hizmetinin bir parçasıdır ve kullanıcılarla Bakanlık arasında özel hukuka dayanan bir sözleşme ilişkisi yoktur. Dolayısıyla, "aramızdaki hizmet ve sözleşme ilişkisi çerçevesinde ve süresince" ifadesi hatalıdır. İkinci olarak, İdarenin kanunlarla kendisine verilmiş görevleri yerine getirirken kamu yararı amacıyla hareket etmesi gerektiği ve bu hizmetlerin yerine getirilmesi sırasında kişisel verileri bu görev ve yetkilere dayanarak işleyeceği kabul edilmektedir. İdare, özel hukuk alanında kalan eylem ve işlemlerinde meşru menfaate dayalı olarak veri işleyebilirse de EBA sistemi doğrudan eğitim kamu hizmetinin bir parçasıdır. Bu nedenle, EBA sistemiyle kişisel verilerin genel olarak kanunlarda açıkça öngörülmesi ve veri sorumlusunun hukuki yükümlülüklerini yerine getirebilmesi için zorunlu olması şartları çerçevesinde işlenmesi gerekir.

Çalışma kapsamında, özellikle Covid-19 küresel salgını döneminde kullanımı artan çevrimiçi dersler ve sınavlarda işlenen kişisel verilerin korunması konusu da incelenmiştir. Bu kapsamda, çevrimiçi olarak yapılan derslere katılım gösteren öğrencilerin kişisel verilerinin işlenmesi konusunda açık bir kanun hükmü bulunmadığından, İdarenin 6698 sayılı Kanunun 5/2-(ç) maddesinde yer verilen "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" şartına dayanabileceği kabul edilmelidir. Nitekim, MEB ve üniversiteler, kanunlarla kendilerine verilen "eğitim-öğretim hizmetlerinin sunulması" görevini yerine getirmekle yükümlü olduğundan, özellikle pandemi döneminde çevrimiçi derslerle bu hizmetlerin devamını sağlamak için zorunlu olan verileri ilgililerden açık rıza almaksızın işleyebileceklerdir. Bununla birlikte, görüntü ve ses verilerinin işlenmesinin zorunlu olup olmadığı, dersin niteliğine göre değerlendirilmelidir. Bu bağlamda, öğrencinin edilgen durumda kaldığı derslerde kamera veya mikrofon açmanın zorunlu tutulmasının hukuka aykırı olacağı; ancak müzik ya da tiyatro gibi öğrencinin bireysel performansının önemli olduğu derslerde bu uygulamanın hukuka uygun kabul edilebileceği sonucuna varılmıştır.

Çevrimiçi yapılan sınavlarda ise adil bir değerlendirme yapılabilmesi için kopya çekilmesini engelleyecek yöntemlerin kullanılması esastır. Herkesin aynı anda soruları gördüğü ve kısıtlı bir zamanda cevaplayarak sisteme yüklemesi gerektiği klasik sınav yönteminde, kopya çekilmesinin önlenmesi için kamera ve mikrofon açılmasının zorunlu tutulması hukuka uygun kabul edilebilir. Ancak, yapay zekâ destekli yazılımlar kullanılarak öğrencilerin biyometrik verilerinin işlenmesinin, 6698 sayılı Kanun'un 6. maddesine uygun olarak, kanunlarda açıkça düzenleme olmadıkça sadece

ilgilisinin açık rızasıyla mümkün olacağı açıktır. Burada, öğrencinin açık rızayı verirken yeterince özgür olmayabileceğine de dikkat çekilmiştir. Öte yandan, her halde veri işlemenin genel ilkelerine uyulması gerekecektir. Bu bağlamda, sınav güvenliği ya da derse katılımın ispatı için biyometrik verileri işleyen yazılımların kullanılmasının ölçülülüğü, katılımcı sayısı, adaletsizliğin etkileyeceği kitlenin büyüklüğü, toplum vicdanında oluşacak yara gibi kriterler göz önünde bulundurulmalıdır.

Salgın hastalık dönemlerinde kişisel sağlık verilerinin işlenmesine ilişkin yapılan değerlendirmede, 6698 sayılı KVKK'nın 6. maddesinde 2 Mart 2024'te yapılan değişikliğin, ilgili dönemlerde veri işlemeyi kolaylaştıracak kurallar getirdiği tespit edilmiştir. Değişiklik öncesinde sağlık verilerinin işlenmesi önemli ölçüde kısıtlanmışken, yeni düzenleme ile ikinci fıkrada belirlenen özellikle fiili imkânsızlık hallerinde, ilgilinin kendisince alenileştirdiği durumlarda ve sosyal hizmetler ile sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesinde veri işlemek mümkün hale getirildiğinden salgın hastalık dönemlerinde yapılan veri işleme faaliyetlerinin çoğu zaman yasal sınırlar içerisinde kaldığı tespit edilmiştir.

Diğer yandan, Türkiye'de Covid-19 süreci uygulamalarında kişisel verilerin korunmasına ilişkin bazı eksikliklerin olduğu tespit edilmiştir. Sağlık Bakanlığı tarafından geliştirilen Hayat Eve Sığar (HES) mobil uygulamasının KVK Kurumu ile iş birliği içinde hazırlanmamış olması, bağımsız bir güvenlik denetiminden geçip geçmediğine dair bilgi verilmemesi, şeffaflık ilkesi gereği düzenli bilgilendirmelerin yapılmaması ve anonim veri toplama yöntemlerinin tercih edilmemesi gibi hususlar uygulamayı yasallıktan uzaklaştıran etmenlerdir. Avrupa'daki bazı ülkelerin Covid-19 takip uygulamalarında kullanıcı gizliliğini korumak adına daha gelişmiş önlemler aldığı belirtilmiş, Türkiye'de ise bu eksikliklere rağmen KVK Kurumu tarafından aktif bir müdahalede bulunulmadığı vurgulanmıştır.

Akıllı ulaşım sistemleri (AUS) uygulamalarında, çeşitli araçlarla kişilerin kimlik, konum, ödeme, seyahat alışkanlıkları, araç, sürüş davranışı, toplu taşıma kullanımı ve trafik kamera görüntüleri gibi kişisel verilerinin işlenmesi söz konusudur. Bu verilerin işlenmesinin bir kısmı özel hukuk kişileri tarafından gerçekleştirilirken, önemli bir kısmı İdare tarafından yürütülmektedir. İdarenin genel nitelikli verileri "kanunda açıkça öngörülme" ve "hukuki yükümlülüklerin yerine getirilmesi bakımından zorunlu olması" şartlarına; özel nitelikli verileri ise "kanunlarda açıkça öngörülme" şartına dayanarak işleyebileceği sonucuna varılmıştır. Ancak, akıllı ulaşım sistemlerinin kurulmasını ve buna bağlı veri işlenmesini doğrudan öngören bir kanun hükmü bulunmadığı tespit edilmiştir. Bununla birlikte, kamu kurumlarına bu sistemlerin kurulması ve yönetimine ilişkin yükümlülükler getiren CBK ve yönetmelikler ile bazı uygulamaların gerçekleştirilmesine olanak sağlayan kanun düzenlemeleri mevcuttur. Bu düzenlemeler birlikte değerlendirildiğinde, İdarelerin trafiğin düzenlenmesi ve planlanması gibi genel yetkilerle akıllı ulaşım sistemleri kapsamında kişisel verileri işleyebileceği sonucuna varılmıştır. Ancak, CBK ile getirilen Haberleşme Genel Müdürlüğü bünyesindeki veri yönetimi merkezinin kurulması ve işletilmesine ilişkin hükmün, kişisel verilerin korunması hakkını

sınırlandıran niteliği nedeniyle Anayasa'ya aykırı olduğu sonucuna varılmış, söz konusu düzenlemenin kanun koyucu tarafından yapılması gerektiği ifade edilmiştir.

Kamu görevine girişte güvenlik soruşturması ve arşiv araştırması kapsamında kişisel verilerin işlenmesine ilişkin olarak KVKK ile 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu hükümleri birlikte değerlendirilmiştir. Güvenlik soruşturması ve arşiv araştırması faaliyetlerinin, KVKK'nin 28. maddesinin 1. fıkrasının (ç) bendi uyarınca, kamu güvenliğini ve ulusal güvenliği sağlamak amacıyla 7315 sayılı Kanun'la yetkilendirilmiş kurumlar tarafından yürütüldüğünden KVKK'nin koruyucu hükümlerinin kapsamı dışında kaldığı tespit edilmiştir.

7315 sayılı Kanun ise kişisel verilerin korunmasına ilişkin hükümler içermekle birlikte bazı eksiklikleri de bulunmaktadır. Öncelikle, toplanan verilerin hukuka uygunluğunu ve kanunun kişisel verilerin korunmasına ilişkin hükümlerine uygun şekilde elde edilip edilmediğini denetleyecek bağımsız bir komisyonun oluşturulmaması, hukuk devleti ilkesi ve kişisel verilerin korunması hakkı açısından bir eksiklik teşkil etmektedir. Ayrıca, güvenlik soruşturması ve arşiv araştırması kapsamında toplanan verilerin KVKK'nin 4. maddesinde sayılan ilkelere uygun olarak işlenmesi gerekmeyle birlikte, kanunda bu ilkelere uygunluğun nasıl sağlanacağı ve denetleneceği konusunda yeterli düzenlemelerin bulunmamasının, keyfi uygulamalara ve hak ihlallerine yol açabileceği sonucuna varılmıştır.

Kamu görevi süresince işlenen kişisel verilerin özlük dosyalarında ve disiplin işlemlerinde kullanımına ilişkin mevzuat hükümleri incelendiğinde, KVKK'de yer alan bazı veri koruma kurallarıyla uyumsuzluklar tespit edilmiştir. Öncelikle, 657 sayılı Devlet Memurları Kanunu'nun 133. maddesinde disiplin cezalarının özlük dosyasından silinmesine ilişkin sürelerin düzenlenmiş olmasına rağmen, soruşturma başlatılıp da ceza verilmeyen dosyalara ilişkin herhangi bir silinme süresinin belirlenmemiş olması, verilerin işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkesiyle çelişmektedir. Ayrıca, disiplin cezalarının silinmesi usulünde, dosyanın imha edilmesi veya yok edilmesi yerine silinme talebinin kabulüne ilişkin kararın dosyaya işlenmesinin öngörülmesi, KVKK'nin 7. maddesinde veri sahiplerine tanınan kişisel verilerin silinmesini isteme hakkının etkin bir şekilde karşılanmadığını göstermektedir. Bu durum, özlük dosyalarının memurların başarı, yeterlik, ehliyet gibi niteliklerinin değerlendirilmesinde dikkate alınması nedeniyle, haklarında silinme kararı verilmiş olsa bile bu dosyaların değerlendirmelerde etkili olmaya devam edeceği anlamına geleceğinden, tüm memurlar için öngörülen bu düzenlemenin, sadece üst düzey yönetici, istihbarat ve özellikli bazı kamu görevlerinde bulunan memurlarla sınırlandırılması ve işlenen evrakların niteliğine göre farklı yok etme sürelerinin belirlenmesi öneri olarak sunulmuştur.

Disiplin soruşturma ve kovuşturmalarında ise kişisel verilerin işlenmesi ile ilgili kişinin kendisi hakkında toplanan bilgi ve belgelere erişim hakkı arasında hassas bir denge kurulması gerekmektedir. Bu itibarla yapılan değerlendirmede, KVKK'nin 28/2. maddesi uyarınca, kural olarak kişisel verilerin ilgili kişinin kendisi hakkında işlenip işlenmediğini öğrenme ve bunlar hakkında bilgi talep etme

hakkının disiplin soruşturmaları bakımından uygulanmadığı tespit edilmiş; ancak Anayasa'nın 129/2. maddesi ve 657 sayılı Kanun'un 130. maddesi gereğince memura savunma hakkının tanınmasının zorunlu olduğu değerlendirildiğinden, bu kapsamda memurun kendisi hakkında hazırlanan dosyaya erişmesine imkân tanınması gerektiği sonucuna varılmıştır.

İdarenin kişisel veri işleme faaliyetlerinden kaynaklanan hukuki sorumluluğunun kapsamı ve niteliği incelendiğinde, 6698 sayılı KVKK'nın 14/3. maddesindeki, kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat hakkının saklı tutulduğu hükmüne istinaden kişisel verileri İdare tarafından hukuka aykırı şekilde işlenmesi nedeniyle zarar gören kişilerin, veri sorumlusu İdareye karşı zararlarının tazmini için dava açabileceği sonucuna varılmıştır. İdarenin sorumluluğunun genellikle veri koruma kurallarına aykırı veri işleme faaliyetlerinden kaynaklandığı dikkate alındığında, açılacak davalarda idarenin hizmet kusurunun varlığının araştırılacaktır. Ancak, hizmet kusurunun bulunamadığı durumlarda, KVKK'de özel bir sınırlamaya yer verilmediğinden, İdarenin kusursuz sorumluluk ilkelerine göre de zararları tazminle yükümlendirilebilecektir. Diğer yandan, GDPR'ın hukuki sorumluluğa ilişkin 82. maddesinde kusursuz sorumluluk ilkesinin benimsenmediği tespit edilmiştir.

İdarenin, kamu hizmetlerini yerine getirirken büyük miktarda kişisel veri topladığı ve işlediği, bu veriler arasında özel nitelikli verilerin de bulunduğu dikkate alındığında, özellikle büyük ölçekli ve hassas verilerin söz konusu olduğu durumlarda, potansiyel olarak tehlikeli bir faaliyetin varlığından bahsedilebileceği, bu nedenle, tehlikeli faaliyeti yürüten İdarenin doğacak zararlardan tehlike (risk) ilkesine dayanılarak kusursuz sorumluluğunun kabul edilebileceği değerlendirilmektedir. Bununla birlikte, "tehlikeli veri" kavramının tanımlanmasındaki güçlükler dikkat çekilerek, kusursuz sorumluluğun belirlenmesinde tehlikeli-tehlikesiz veri ayrımı yapılmaması gerektiği savunulmuştur.

İdarenin kusursuz sorumluluğuna ilişkin değerlendirmelerimiz, özellikle makine öğrenmesi ve derin öğrenme algoritmalarına dayanan ileri düzey YZ tabanlı sistemler kullanılarak gerçekleştirilen yasaya aykırı veri işleme faaliyetleri söz konusu olduğunda da geçerlidir. Bu noktada, Avrupa Birliği'nin Yapay Zekâ Yasası'nda öngörülen risk sınıflandırmasının idarenin sorumluluğunun belirlenmesinde yol gösterici olabilir. İlgili Yasa'da yapılan risk ayrımı dikkate alınarak, kritik alanlarda kullanılan yüksek riskli YZ sistemlerinden kaynaklanan kişisel veri ihlalleri ve bu ihlallerden doğan zararların tazmininde İdarenin risk ilkesi çerçevesinde kusursuz sorumluluğunun kabul edilmesi gerektiği sonucuna varılmıştır.

KVKK'de, ilgilinin Kanunda belirlenen haklarını veri sorumlusuna yapacağı bir başvuru ile ileri sürebileceği kabul edilmiştir. Bu bağlamda, veri sorumlusunun belirlenmesinde tüzel kişiliğin esas alınması, ayrı tüzel kişiliği bulunan kamu kurum ve kuruluşları için uygun bir yaklaşım olarak tespit edilmiştir. Ancak, Devlet tüzel kişiliği içerisinde yer alan ve ayrı tüzel kişiliği bulunmayan idari birimler için bu durumun sorun teşkil ettiği görülmüştür. Bu durumun, kişisel verilerin işlenmesinde işlevsellik, şeffaflık ve uygulanabilirlik açısından önemli sorunlar doğurduğu sonucuna varılmıştır. Bu soruna

özüm olarak, 6698 sayılı Kanun'a bakanlıkların ve yetki genişlięi esasıyla yönetilen valiliklerin de veri sorumlusu olabileceęine ilişkin bir hüküm eklenmesinin uygun olacağı kanaatine varılmıştır.

KVK Kurulu'nun yaptırım yetkisi bağlamında, mevzuata aykırılıkları tespit etme ve idari para cezası uygulama yetkisinin, veri sorumlusunun nitelięine göre farklılık gösterdiği görölmüşür. Ancak, gerçek kişiler ve özel hukuk tüzel kişilerine idari para cezası uygulanabilirken, kamu tüzel kişilerine yönelik yaptırımların disiplin hükümleriyle sınırlı kalmasının, kuralların İdare üzerindeki etkinliğini azalttığı sonucuna varılmıştır. Ayrıca, kamu görevlilerine uygulanan disiplin cezalarında bir standardın bulunmamasının ve kişisel veri ihlalinin ayrı bir disiplin suçu olarak tanımlanmamasının da veri ihlali yapan İdarelere uygulanan yaptırımlar bakımından eşitsizlik yaratmaktadır. Bu sorunların çözümü için ilk olarak, kamu tüzel kişilerinin de idari para cezalarına tabi tutulması ve rücu sistemiyle sorumlu kamu görevlilerine yansıtılması; ikinci olaraksa, kişisel veri ihlalinin disiplin suçu olarak tanımlanması ve karşılığında uygulanacak cezanın net bir şekilde belirlenmesi önerilmiştir.

KAYNAKÇA

- ABANOZ, Buket, **Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu**, İstanbul, On İki Levha Yayıncılık, 2018.
- AKGÜL, Aydın, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması Hukuku**, Beta Yayınevi, 2. Baskı, 2016.
- AKILLIOĞLU, Tekin, “Kamu Yararı Kavramı Üzerine Düşünceler”, **İHİD**, C.9, S.1-3, 1988, <https://dergipark.org.tr/tr/download/article-file/13697> (Erişim Tarihi: 2.3.2022).
- AKINCI, Ayşe Nur, “Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti”, **T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı**, Uzmanlık Tezi, 2019.
- AKKAYA KİA, Rukiye, “Devlet Sırrı, Kimin Sırrı?”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Özel Sayı: Prof. Dr. Nur Centel’e Armağan**, Y.2013, C.19, S.2, s. 749-755.
- AKKOYUNLU, Sencer Abdullah, “Disiplin Soruşturmasında Memurun Savunma Hakkının Kullanımında İdarenin Uyması Gereken Esaslar”, **DÜHFD**, C.28, S.48, Y.2023, s.3-63.
- AKKURT, Sinan Sami, “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, **Kişisel Verileri Koruma Dergisi**, C. 2, S.1, 2020, s. 20-32.
- AKLAN, Aybeniz, “Karşılaştırmalı Hukukta Kişisel Sağlık Verilerinin Hukuka Aykırı İşlenmesi ve Tazminat Sorumluluğu”, **Ankara Yıldırım Beyazıt Üniversitesi**, Yayımlanmamış Yüksek Lisans Tezi, 2024.
- AKSOY RETORNAZ, E. Eylem/ GÜÇLÜTÜRK, Osman Gazi, “Yapay Zekânın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi”, içinde **Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ**, E. Eylem AKSOY RETORNAZ ve Osman Gazi GÜÇLÜTÜRK (editörler), İstanbul, On İki Levha Yayıncılık, 2021, 275-302.
- AKSOY, Hüseyin Can, “Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu”, **Haluk Konuralp Anısına Armağan**, Cilt 3, Yetkin Yayınları, Ankara 2009.
- AKYILMAZ, Bahtiyar/SEZGİNER, Murat/KAYA Cemil, **Türk İdare Hukuku**, Savaş Yayınevi, 12. Baskı, Eylül 2020.
- AKYÜZ, Emine, **Çocuk Hukuku**, Pegem Akademi Yayıncılık, 7. Baskı, 2020.
- ALBAYRAK SEKBAN, Esengül, “İdari İşlem: Hukuka Uygunluk Karinesi”, **İstanbul Barosu Dergisi**, Cilt: 92, S.: 3, Mayıs 2018, s. 354-369.
- ALÇIN, Ayşe Aslı, “Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü”, **TAAD**, Y.13, S.51, Temmuz 2022.
- ALTINDAĞ, Halil, “Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu”, **İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi**, C.18, S.2, Temmuz 2019, s.387-401.

- ALTINDAĞ, Halil, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, Adalet Yayınevi, Ankara, 2021. (“Kişisel Verileri Koruma Kurulu ...”)
- ANAYURT, Ömer, **Anayasa Hukuku**, Seçkin Yayıncılık, 3. Baskı, 2020.
- ANTALYA, O. Gökhan / TOPUZ, Murat, **Medeni Hukuk**, Cilt 1, Seçkin Yayıncılık, 4. Baskı, 2021, Ankara.
- ARDIÇOĞLU, Artuk, “Cumhurbaşkanlığı Kararnamesi”, **Ankara Barosu Dergisi**, S. 3, 2017, s. 20-51.
- Article 29 Working Party, **Guidelines on consent under Regulation 2016/679**, 10.4.2018, <https://ec.europa.eu/newsroom/article29/items/topic/6936> (Erişim Tarihi: 15.1.2022).
- ASLAN, Zehreddin/ALTINDAĞ, Halil, “Bağımsız Spor Federasyonlarının Kamu Tüzel Kişiliği Sorunu”, **İstanbul Spor Hukuku Dergisi**, Y. 2019, Ay: 1 C.1, S.1, s. 181-196.
- ATAR, Yavuz, **Türk Anayasa Hukuku**, Seçkin Yayıncılık, 14. Baskı, 2021.
- AYAN, Mehmet/AYAN, Nurşen, **Kişiler Hukuku**, 8. Baskı, Seçkin, Ankara, Ekim 2016.
- AYAN, Mehmet/AYAN, Nurşen, **Medeni Hukuka Giriş**, Seçkin Yayıncılık, 12. Baskı, 2016.
- AYANOĞLU, Taner: “Türkiye Futbol Federasyonu’nun Özel Hukuk Tüzel Kişiliği Görüşü Hakkında Düşünceler ve Eleştiriler”, **Legal Hukuk Dergisi**, Yıl 2017, Sayı 174, s. 2839-2858.
- AYBAY Rona, “Uluslararası Antlaşmaların Türk Hukukundaki Yeri”, **TBB Dergisi**, S. 70, 2007.
- AYDOĞDU, Yasin, “Kamu İdaresinde Kişisel Verilerin Korunması”, **SÜHFD.**, C.29, S.1, 2021, s.263-293.
- AYÖZGER ÖNGÜN, A. Çiğdem, **Kişisel Verilerin Korunması Hukuku**, Beta, 2. Baskı, Ocak 2019.
- AZRAK, Ülkü, “İdari Yargıda Anayasaya Uygunluk Sorunu”, **Anayasa Yargısı Dergisi**, S. 9, 1992, s. 323-340.
- BALKAN, Ali, “Türk İdare Hukukunda Kişisel Verilerin Korunması Hakkı ve İdarenin Sorumluluğu”, **Hatay Mustafa Kemal Üniversitesi**, Doktora Tezi, 2023.
- BAŞALP, Nilgün, **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayınları, 2004.
- BASAN, Nuri Mehmet / BİLİR, Nazmi, “Koruyucu Sağlık Hizmetlerinde Önleme Çelişkisi ve Nedenleri”, **TAFF Preventive Medicine Bulletin**, C. XV, No: 1, 2016, s. 44-50, <https://www.bibliomed.org/mnsfulltext/1/1-1427871712.pdf?1655285484> (Erişim Tarihi: 15.6.2022)
- BAŞAR KARTAL Savaş ve diğerleri, “İstanbul’da Gebe, Lohusa, Bebek ve Çocuk İzlemlerinin İyileştirilmesi: GEBLİZ”, **TAF Preventive Medicine Bulletin**, C. 9, S. 4, 2010.
- BAŞAR, Cemal, “Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması”, **Dokuz Eylül Üniversitesi SBE**, Doktora Tezi, 2019.
- BASKIN Onur, **Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2021.

- BAYRAKTAR Aynur, “Ekonomik İş birliği ve Kalkınma Örgütü (Organisation For Economic Cooperation and Development – OECD) ve Çevre”, **Biyoloji Bilimleri Araştırma Dergisi**, S. 3 (2), s. 5-8, 2010.
- BOSTANCI BOZBAYINDIR, Gülşah, “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, S.2018/2, s.51-103.
- BOZ, Selman Sacit, **Kamu Görevlilerinin Mali Sorumluluğu Bağlamında Kişisel (İdari) Kusur**, Adalet Yayınevi, Mart 2024.
- BOZLAK, Ayhan, **ABD Hukukunda Özel Hayatın Gizliliği Hakkının Korunması**, Beta, Ocak 2015.
- BROOMFIELD, Heather/REUTTER, Lise, “In search of the citizen in the datafication of public administration”, **Big Data & Society**, 9(1), 2022, <https://doi.org/10.1177/20539517221089302> (Erişim Tarihi: 7.6.2024).
- BULUT, Metin, “Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler”, **Ankara Barosu Dergisi**, 2020/3, s.99-150.
- BUYLE, Raf/TAELMAN Ruben/MOSTAERT Katrien/JORIS Geroen/MANNENS Erik/VERBORGH Ruben/BERNERS-LEE Tim, “Streamlining Governmental Processes by Putting Citizens in Control of Their Personal Data”, İçinde: Chugunov, A., Khodachek, I., Misnikov, Y., Trutnev, D. (Eds.) **Electronic Governance and Open Society: Challenges in Eurasia**. EGOSE 2019, Springer, s. 346-359, https://doi.org/10.1007/978-3-030-39296-3_26 (Erişim Tarihi: 7.6.2024).
- BYGRAVE, Lee A./ TOSONI, Luca, “Article 4(1). Personal Data”, in **The EU General Data Protection Regulation (GDPR) A Commentary**, Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY (Eds.), Oxford University Press, 2020.
- CAN, Osman, “Cumhurbaşkanlığı Kararnamelerinin Hukuki Rejimi ve Anayasa Mahkemesi Yaklaşımı”, **Anayasa Yargısı**, C.37, S.1, 2020.
- CANATAR, Yusuf Sinan, İdarenin Başvurular Karşısında Sessiz Kalmasına Getirilen Bir Çözüm Olarak Zımni İşlemler, **İstanbul Üniversitesi SBE**, Yayımlanmamış Yüksek Lisans Tezi, 2019.
- CANDAN, Turgut, **Açıklamalı İdari Yargılama Usulü Kanunu**, Yetkin Yayınları, 8. Baskı, 2020.
- CANDAN, Turgut, **Açıklamalı İdari Yargılama Usulü Kanunu**, Yetkin Yayınları, 8. Baskı, 2020.
- CANKURT, Ezgi, “Kişinin Hatırasına Hakaret Suçu (TCK m.130)”, **Beykent Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 1, Sayı: 1, 2015, s. 147-176.
- CANSEL, Erol/ÖZEL, Çağlar, **Borçlar Hukuku Genel Hükümler**, Seçkin Yayıncılık, Cilt:1, 2. Baskı, 2017.

- CAREY, Peter, “Data Protection Principles”, **Data Protection**, Peter Carey (Ed.), Oxford University Press, Fifth Edition, 2018.
- CERAN, Aslı Şeyma, “Yargı Kararları Işığında Hizmet Kusuru ve Kişisel Kusur Ayrımı”, **İstanbul Kültür Üniversitesi**, Yayınlanmamış Yüksek Lisans Tezi, 2022.
- CEYLAN, Mahmut, “İdari Yargıda Delil Serbestisi ve Sınırları”, **KTÜ Sosyal Bilimler Enstitüsü Sosyal Bilimler Dergisi**, Y.8, S.16, Aralık 2018.
- ÇAKIR, Hüseyin Melih, “Yerinden Yönetim”, içinde İdare Hukuku, Turan YILDIRIM (ed.), 8. Baskı, On İki Levha Yayıncılık, İstanbul, Kasım 2020.
- ÇAPALI, Buket, “Akıllı Ulaşım Sistemleri Mimarisi: K-AUS için Öneri”, **El-Cezerî Fen ve Mühendislik Dergisi**, 2022, 9(4); 1249-1254.
- ÇAYIR, Faruk, **Pandemi Takip Uygulamaları ve Kişisel Verilerin İzlenmesi Raporu**, Alternatif Bilişim Derneği, 2020, <https://alternatifbilisim.org/covid-19-pandemi-sureci-raporlari-yayinda/> (E.T. 24.5.2024).
- ÇEKİN, Mesut Serdar, **Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, 3. Baskı, İstanbul, Temmuz 2020.
- de TERWANGNE, Cecile, “Article 5: Principles relating to processing of personal data”, in **The EU General Data Protection Regulation (GDPR) A Commentary**, Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY (Eds.), Oxford University Press, 2020.
- DEMİR, Hamza, **Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, On İki Levha, Nisan 2020.
- DENİZ, Yusuf ve diğerleri, “İdari Yargılama Usulü Kanunu’nun 11. Maddesine Göre Yapılan İdari Başvurular”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C.21, S.2, 2013.
- DUMAN, Berat, “Anayasa Hukukunda Kişisel Verilerin Korunması”, **Selçuk Üniversitesi SBE**, Yayınlanmamış Doktora Tezi, 2020.
- DURAN, Lütfi, **İdare Hukuku Ders Notları**, Fakülteler Matbaası, 1982.
- 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.
- EDWARDS, Lilian, “Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective”, **European Data Protection Law Review (Lexxion)**, January 5, 2016, <https://ssrn.com/abstract=2711290>.
- ER, Cüneyd, **Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı**, Yetkin Yayınları, Ankara, 2007.

- ERARSLAN, Sevgi, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, On İki Levha, 2. Baskı, İstanbul, Aralık 2020.
- ERAVCI, Deniz Boz, “Kurumların Dijital Dönüşümü: Büyük Veri”, **Çalışma İlişkileri Dergisi**, Ocak 2020, Cilt 11, Sayı 1, s. 90-112.
- ERDOĞAN, İhsan/ KESKİN, A. Dilşad, **Türk Medeni Hukuku (Başlangıç Hükümleri – Kişiler Hukuku)**, Gazi Kitabevi, 2. Baskı, 2019.
- ERDOĞMUŞ, Talha. "Kişisel Verileri İhlal Eden İdareye Karşı İdari Para Cezası Uygulanmaması Sorunu", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, C.10, Y.2023, S.1, s. 137-168, <https://dergipark.org.tr/tr/pub/imuhfd/issue/78403/1211491> (Erişim Tarihi: 1.7.2023).
- EREN, Abdurrahman, “Anayasa Mahkemesinin Kanun Hükmünde Kararnamelere İlişkin İçtihadı Doğrultusunda Cumhurbaşkanlığı Kararnamelerinin Değerlendirilmesi”, **Anayasa Yargısı Dergisi**, Cilt: 36, S. 1, 2019, s. 1-72.
- ERKAL, Atila, “Avrupa Genel Veri Koruma Düzenlemesi Bağlamında Memurların Kişisel Verilerinin Korunması Hakkı” **Anayasa Yargısı**, C.37, S.2, Y.2020, s.205-253.
- ERTAŞ, Şeref/PETEK, Hasan, **Spor Hukuku**, Yetkin Yayınları, Ankara, 2011.
- ESENYEL HANAZ, Fatma, “Çevrimiçi Eğitimde Üniversite Öğrencilerinin Kişisel Verilerinin İşlenmesinin Hukuki Sebepleri”, **TBB Dergisi**, S.155, 2021.
- EVREN, Çınar Can / UÇAR, İsmail, **Kamu Görevlileri Hukuku**, Seçkin Yayıncılık, 2. Baskı, 2020.
- FİŞ ÜSTÜN, Gül, “Disiplin Soruşturamalarında Hukuka Aykırı Deliller”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.24, S.1, Haziran 2018.
- FİŞEK, Nusret, “Koruyucu ve Tedavi Edici Hekimlik Hizmetlerinin Planlanmasında Örgütlenme Modelleri”, **Türkiye Tıp Akademisi Mecmuası**, C. 9, S. 3, 1974. https://www.ttb.org.tr/n_fisek/kitap_1/10.html#_ftn1 (Erişim Tarihi: 15.6.2022)
- GÖZLER, Kemal, **İnsan Hakları Hukuku**, Ekin Yayınevi, 2. Baskı, Ekim 2018.
- GÖZLER, Kemal, **Türk Anayasa Hukuku Dersleri**, Ekin Yayınevi, 22. Baskı, Eylül, 2018.
- GÖZÜBÜYÜK, A. Şeref/TAN, Turgut, **İdare Hukuku Cilt I**, Turhan Kitabevi, 12. Baskı, Ankara, 2018.
- GÖZÜBÜYÜK, A. Şeref/TAN, Turgut, **İdare Hukuku Cilt II**, Turhan Kitabevi, 8. Baskı, Ankara, 2016.
- GUADAMUZ Andres, “Habeas Data vs the European Data Protection Directive”, **The Journal of Information, Law and Technology (JILT)**, 2001, Issue: 3, <http://elj.warwick.ac.uk/jilt/01-3/guadamuz.html>. (Erişim Tarihi: 28.7.2021).
- GÜLHAN Ozan, “Kişisel Sağlık Verilerinin Korunması”, Marmara Üniversitesi, Doktora Tezi, 2023.

- GÜNEŞ, Felemez, **İdari Yargı Yetkisinin Sınırları**, Seçkin Yayıncılık, 2022.
- GÜNTÜRK, Mümin Serdar, **Özel Hayatın Gizliliğinin Korunması**, Seçkin Yayıncılık, 2012.
- GÜR, Necip Taha, **İdarenin Özendirme ve Destekleme Faaliyeti**, On İki Levha Yayıncılık, İstanbul, 2019.
- GÜRAN, Sait, “Türkiye Futbol Federasyonu’nun İdare Hukuku ile İlişkisi”, **Prof. Dr. Rona Serozan’a Armağan**, Cilt II, 1. Baskı, On İki Levha Yayınları, İstanbul, 2010, s. 1913-1919.
- HAKERİ, Hakan, **Tıp Hukuku Cilt 1: Genel Hükümler**, Seçkin Yayıncılık, 26. Baskı, 2024.
- HAKERİ, Hakan, **Tıp ve Sağlık Hukuku El Kitabı**, Seçkin Yayıncılık, 2022.
- HAZAR, Zeynep, “İnsan Hakları Çatışmalarının Çözümlemesinde Çocuğun Üstün Yararı İlkesinin İşlevi: Türk Anayasa Mahkemesi Kararları Çerçevesinde Bir Değerlendirme”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C.XXVI, Y. 2022, S.2, s.647-684.
- İMANÇLI, Canan, **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu**, On İki Levha Yayıncılık, Nisan, 2020.
- İNAN, Ali/NERGİZ, Mehmet Ercan/SAYGIN, Yücel, “Öğrenci Verilerinin Korunması: FATİH Projesi Işığında Teknik Değerlendirme”, **Bilişim Teknolojileri Dergisi**, Cilt: 10, Sayı: 1, Ocak 2017.
- İNANÇ, Zekeriya Alper, “TCK, TMK ve Uluslararası Sözleşmeler Kapsamında Terbiye Hakkı”, **Melikşah Üniversitesi Hukuk Fakültesi Dergisi**, C.2, S.2, Aralık 2013, s.101-132.
- İŞIKLAR, Celal, “Danıştay Kararlarında İdarenin Kusursuz Sorumluluğunu Kaldıran veya Azaltan Haller”, **YBHD**, Y.4, S.2019/1, s.115-158.
- İSTANBULLUOĞLU Hakan / GÜLEÇ Mahir / OĞUR Recai, “Sağlık Hizmetlerinin Finansman Yöntemleri”, **Dirim Tıp Gazetesi**, 2010, Y. 85, S. 2 (86-99), https://www.dirim.com/Dirim_2010-2_files/Sag%CC%86l%C4%B1k%20hizmetleri.pdf (Erişim Tarihi: 4.7.2022).
- İŞLER, Buket / KILIÇ, Mehmet Yaşar, “Eğitimde Yapay Zekâ Kullanımı ve Gelişimi”, **e-Journal of New Media**, Y. 2021, C.5, S.1, s. 1-11.
- KAGITCIOĞLU, Mutlu, “Yapay Zekâ ve İdare Hukuku (Bugünden Geleceğe Yönelik Bir Değerlendirme)”, **Hacettepe HFD**, S.11(1), Y.2021, s.118-168.
- KALE ÖZÇELİK, Fatmagül, “Covid-19 Salgını Sürecinde Üniversite Eğitiminde Kullanılan Uzaktan Eğitim Platformlarının 6698 Sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi”, **SDÜHFD**, C.11, S.1, Y.2021.
- KALYON, Arzu, “Türk Vergi Hukukunda Kişisel Verilerin Korunması”, **Marmara Üniversitesi SBE**, Doktora Tezi, 2021.

- KAMA, Sezen, ÇEKİN, M. Serdar, DORU, S. Rasim, TAŞTAN, F. Güven, KARADUMAN, Ozan, “Reformun Sebebi, İçeriğinin Tanıtılması ve Müstakbel Değişiklikler” [Konferans 1. Oturumu], **KVKK Reformu Konferansı**, 8 Mayıs 2024, İstanbul, Türkiye.
- KAMAN, Nur, “Kamu Görevlileri”, içinde **İdare Hukuku**, Turan Yıldırım (Ed.), 8. Baskı, On İki Levha Yayıncılık, İstanbul, Kasım 2020.
- KANGAL, Zeynel T., **Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması**, On İki Levha Yayıncılık, Eylül 2019.
- KARAHANOGULLARI, Onur, “Güvenlik Soruşturması”, **Ankara Üniversitesi SBF Dergisi**, Y.1988, S.53(01), https://doi.org/10.1501/SBFder_0000001946.
- KARAHANOGULLARI, Onur, **İdarenin Hukukla Kavranması: Yasallık ve İdari İşlemler**, Turhan Kitabevi, 4. Baskı, Ankara, 2018.
- KARAHANOGULLARI, Onur, **İdari Yargı: İdarenin Hukuka Zorlanması**, Turhan Kitabevi, 2019.
- KARAKUŞ IŞIK, Zehra, “İdari Eylemlerden Kaynaklanan Tam Yargı Davalarında Bir Bozma Nedeni Olarak Husumet”, **AndHD**, C.:9, S.:2, Temmuz 2023, s.333-349.
- KARAKUŞ IŞIK, Zehra / TÜRKOĞLU ÜSTÜN, Kamile, “İdarenin Kolluk Yetkileri Kapsamında Trafik İhlallerinin Elektronik Denetleme Sistemleri ile Tespiti”, **İNÜHFD**, Cilt: 15, S.2, 2024, s. 358-371.
- KARATAŞ DURMUŞ, Neslihan, “Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti”, **TAAD**, Y. 8, S. 31 (Temmuz 2017), s. 371-409.
- KARATAŞ Mehmet/ATEŞ Adnan/UÇAR Muharrem/KANTARCI M. Nabi, “HIV Pozitif Kişilerin Eşlerine Hastalığı Bildirme(me)nin Yasal ve Etik Açısından Değerlendirilmesi”, **İnönü Üniversitesi Tıp Fakültesi Dergisi**, 17(3), 2010, s.215-222.
- KAYA, Mehmet Bedii, **KVKK Reformu: 2024 Değişiklikleri (Dijital Baskı 1.0)**, 2024, <https://mbkaya.com/hukuk/kvkk-reformu.pdf>.
- KAYA, Seyithan, **Kamu Görevlisinin Kişisel Kusuru ve Sorumluluğu**, Adalet Yayınevi, 2021.
- KAYIHAN, Şaban / ÜNLÜTEPE, Mustafa, **Medeni Hukuk Bilgisi**, Seçkin Yayıncılık, 4. Baskı, Eylül 2017, Ankara.
- KENDRICK, Leslie, "Speech, Intent, and the Chilling Effect", **William & Mary Law Review**, 54(5), 2013, s.1633-1691, <https://scholarship.law.wm.edu/wmlr/vol54/iss5/4/> (E.T.: 1.2.2025).
- KESER, Leyla, “İlk Görünüş İspatı”, **Prof. Dr. Mahmut Birsell’e Armağan**, DEU Yayını, 2001, <https://hukuk.deu.edu.tr/wp-content/uploads/2020/01/L.Keser-13.pdf> (E.T. 15.8.2024).
- KESGİN, Burak, “Güvenlik, Düzen ve Gözetim: Geleceğin Dünyasında Protesto Hakkı”, **Sosyoloji Araştırmaları Dergisi**, C.26, S. 2, Ekim 2023.

Kişisel Verileri Koruma Kurulu, **6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar**, <https://www.kvkk.gov.tr/>

Kişisel Verileri Koruma Kurulu, **6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı**, <https://www.kvkk.gov.tr/>

Kişisel Verileri Koruma Kurulu, **KVKK Yayınları No: 43**, s.36-37, *kvkk.gov.tr*. (Erişim Tarihi: 13.10.2023).

Kişisel Verileri Koruma Kurulu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, KVKK Yayınları, Mart 2019, Ankara.

Kişisel Verileri Koruma Kurulu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, KVKK Yayınları, Mart 2019.

Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlıklar – 2 Kitapçığı

KOÇ, Celalettin, “İdari İşlemin Amaç Unsuru”, **Bursa Uludağ Üniversitesi SBE**, Yayınlanmamış Yüksek Lisans Tezi, 2019.

KOCA, Mahmut, “Ceza Hukuku Açısından Kişisel Verilerin Korunması Ve Verilerin İmha Edilmemesinin Sonuçları”, içinde **Kişisel Verilerin İmhası**, Seçkin, 2. Baskı, Ekim 2022.

KOCA, Mahmut/ÜZÜLMEZ, İlhan, “Kişisel Verilerin Kaydedilmesi Suçu (m.135)”, **D.E.Ü. Hukuk Fakültesi Dergisi**, Prof. Dr. Durmuş TEZCAN’a Armağan, C.21, Özel S., 2019, s. 69-93.

KONUKPAY Cenk / TABAK Uğur, “Kişisel Verilerin İşleme Amacının Sonradan Değişmesi: Uyumluluk Kriterlerinin Uygulanması Sorunu”, **Kişisel Verileri Koruma Dergisi**, Cilt: 3, S.:2, s.15-33.

KORKMAZ, Yakup, “Hasta Hakkı Olarak Özel Hayatın Korunması Bağlamında Beden Mahremiyeti”, **Uyuşmazlık Mahkemesi Dergisi**, Y.8, S.15, Haziran 2020, s. 573-598.

KÖSE AYSUN, Melike, **Kişisel Verilerin Kaydedilmesi Suçu**, Seçkin, 2. Baskı, Ekim 2021.

KÖSEOĞLU, Özer/DEMİRCİ, Yılmaz, “Türkiye’de Büyük Veri ve Veri Madenciliğine İlişkin Politika ve Stratejiler: Ulusal Politika Belgelerinin İçerik Analizi”, **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Y.2017, C.22, Kayfor15 Özel Sayısı, s.2223-2239.

KOTOV, Alexander/NAUMOV, Victor, “E-Governance and Privacy in Pandemic Times”, In: Yang, XS., Sherratt, S., Dey, N., Joshi, A. (eds) **Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems**, Springer, Vol 236. 2022, https://doi.org/10.1007/978-981-16-2380-6_86.

KOTSCHY, Waltraut, “Article 6 Lawfulness of Processing”, in **The EU General Data Protection Regulation (GDPR) A Commentary**, Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY (Eds.), Oxford University Press, 2020.

- KÜÇÜK, Suat Hayri, “Covid-19 Pandemisinde Kişisel Sağlık Verilerinde Laboratuvar Çalışmaları ve Kullanımı”, **Kişisel Sağlık Verileri 4. Ulusal Kongresi**, 24-25 Ekim 2020, Webinar, İstanbul Türk Tabipler Birliği Yayınları, Nisan 2021.
- KÜPELİ Ceren, **Tüzel Kişi Verilerinin Korunmasında İdarenin Sorumluluğu**, Adalet Yayınevi, Ankara, 2020.
- KÜZECİ Elif, “Covid-19 Pandemisinde Kişisel Verilerin Korunması”, **Kişisel Sağlık Verileri 4. Ulusal Kongresi**, 24-25 Ekim 2020, Webinar, İstanbul Türk Tabipler Birliği Yayınları, Nisan 2021.
- KÜZECİ, Elif, **Kişisel Verilerin Korunması**, Turhan Kitabevi, 3. Baskı, Ankara, 2019.
- MACIEJEWSKI, Mariusz, “To do more, better, faster and more cheaply: using big data in public administration”, **International Review of Administrative Sciences**, 83(1_suppl), 2017, s. 120-135, <https://doi.org/10.1177/0020852316640058> (Erişim Tarihi: 8.6.2024).
- MARAŞLI DİNÇ, Yasemin, “Ölümden Sonra Sosyal Medya Hesaplarının Hukuki Akıbeti: Dijital Miras”, **TBB Dergisi**, 2019 (142), s. 273-287.
- NAÇAR, Sebahattin, “Kamu Düzeninin Unsuru Olarak Genel Sağlığın Korunması”, **Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü**, Yüksek Lisans Tezi, 2023.
- NARBAY, Şafak / KİRAZLI, Şerife Nur, “Otonom Araçlarda Yapay Zekâ, Kişisel Verilerin İşlenmesi ve Sonuçları”, **Sakarya Üniversitesi Hukuk Fakültesi Dergisi**, C.1, S.1, Temmuz 2023, s.49-65.
- ODYAKMAZ, Zehra, “Genel Olarak İdarenin Sözleşmeleri”, **GÜHFD**, 1998, Cilt: 2, S.:1-2, https://webftp.gazi.edu.tr/hukuk/dergi/2_12.pdf (Erişim Tarihi: 11.2.2022).
- OĞURLU, Yücel, **Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi**, Seçkin Yayıncılık, 2002.
- OKAY TEKİNSOY, Özge, “Kolluk Faaliyetleri”, içinde İdare Hukuku, Turan YILDIRIM (ed.), 8. Baskı, On İki Levha Yayıncılık, İstanbul, Kasım 2020.
- OLSEN, Thomas/MAHLER, Tobias, “Identity management and data protection law: Risk, responsibility and compliance in ‘Circles of Trust’ – Part II”, **Computer Law & Security Review**, Volume 23, Issue 5, 2007, s. 415-426, <https://doi.org/10.1016/j.clsr.2007.07.001> (Erişim Tarihi: 7.6.2024).
- ONAR, Sıddık Sami, **İdare Hukukunun Umumi Esasları Cilt II**, İsmail Akgün Matbaası, 1960.
- ONAR, Sıddık Sami, **İdare Hukukunun Umumi Esasları Cilt III**, 3. Bası, İstanbul, 1966.
- OSMANOĞLU, Bilal, “Türk Ceza Muhakemesi Hukukunda Cumhuriyet Savcısı ve Mahkemelerin Bilgi ve Belge İsteme Yetkisi”, **TBB Dergisi**, 2020, S.151, Kasım-Aralık, s.103-138.
- ÖZAY, İl Han, **Günüşğinde Yönetim**, Filiz Kitabevi, 2017.
- ÖZAY, İl Han, **İdari Yaptırımlar**, İstanbul Üniversitesi Hukuk Fakültesi Yayınları, İstanbul, 1985.

- ÖZBUDUN, Ergun, **Türk Anayasa Hukuku**, Yetkin Yayınları, 19. Basım, Aralık, 2019.
- ÖZENÇ, Berke, “İnancını Açıklamama Hakkı Açısından Türkiye Cumhuriyeti Kimlik Kartlarındaki Din Hanesi”, **TBB Dergisi**, S.141, s. 9-42.
- ÖZER, Hazan Dicle, “MOBESE İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme”, **DEUHFD**, C.24, S.1, Mayıs 2022, s. 459-500.
- ÖZGÜN TEKİN, Esra, “1982 Anayasası’nın 90. Maddesi Uyarınca Uluslararası Andlaşmaların Türk Hukukundaki Yeri Sorunu”, **Journal Of Social, Humanities and Administrative Sciences**, Vol: 5, Issue: 14, 2019, s. 137-149.
- ÖZKAN, Feray, “Kişisel Sağlık Verilerinin Korunmasının Pozitif Temelleri ve AİHM Kararlarında Örnekler”, **Dokuz Eylül Üniversitesi**, Yayınlanmamış Yüksek Lisans Tezi, 2018.
- ÖZKAN, Oğulcan, **Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2020.
- ÖZKAYA, Ömer/TOPRAK, İbrahim, “Türkiye’de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi”, **Manas Sosyal Araştırmalar Dergisi**, Y.2022, S.11(3), s.1291-1305.
- ÖZTOPRAK, Sezin, “İdari Sözleşmelerde Kamu Gücü Ayrıcalıkları”, **Selçuk Üniversitesi SBE**, Doktora Tezi, 2019.
- PRINS, Corien, “When Personal Data, Behavior And Virtual Identities Become A Commodity: Would A Property Rights Approach Matter?”, **Script-ed**, C. 3, S. 4, 2006, s. 274-275.
- REDDEN, Joanna, “Democratic governance in an age of datafication: Lessons from mapping government discourses and practices” **Big Data & Society**, Vol. 5(2), 2018, <https://doi.org/10.1177/2053951718809145> (Erişim Tarihi: 7.6.2024).
- REGAN, Priscilla M. “Privacy, Government Information, and Technology.” **Public Administration Review**, vol. 46, no. 6, 1986, p. 629–34, <https://doi.org/10.2307/976229> (Erişim Tarihi: 7.6.2024).
- ROCH, Michael P., “Filling the Void of Data Protection in the United States: Following the European Example”, **Santa Clara High Technology Law Journal**, Volume: 12, Issue: 1, January, 1996, <https://digitalcommons.law.scu.edu/chtj/vol12/iss1/3/> (Erişim Tarihi: 15.7.2021).
- ROUVROY Antoinette/POULLET Yves, “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy”, in Gutwirth S., Pouillet Y., De Hert P., de Terwangne C., Nouwt S. (Eds.) **Reinventing Data Protection?**, Springer, Dordrecht, January 2009.
- SACİT, Yılmaz, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Adalet Yayınları, Ankara, Nisan 2016.
- SAĞLAM, Fazıl, **Temel Hakların Sınırlanması ve Özü**, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, Ankara, 1982.

- SAKA, Rıza/ÇAĞLAYAN, Ramazan/KOCA Mahmut, **Avrupa Birliği Hukuku İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası**, Seçkin Yayıncılık, 2. Baskı, Ankara, 2022.
- SAMUELSON, Pamela, "Privacy As Intellectual Property?", **Stanford Law Review**, Vol. 52, No: 5, 2000, s.1125-1173.
- SANTO Guilherme/ SANTOS Leonel/ COSTA Rogério L. C./ RABADÃO Carlos, "Intelligent Transportation Systems Security and Privacy." **Information Security and Privacy in Smart Devices: Tools, Methods, and Applications**, Carlos RABADÃO, et al. (eds), IGI Global, 2023, s. 122-141. <https://doi.org/10.4018/978-1-6684-5991-1.ch005>.
- SCHAUER, Frederick "Fear, Risk and the First Amendment: Unraveling the Chilling Effect", **Boston University Law Review**, 58, 1978, s.685-732, <https://scholarship.law.wm.edu/facpubs/879> (E.T.: 1.2.2025).
- SERT, Şeyma, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin, 2. Baskı, Mayıs 2023.
- SEVER, D. Çiğdem, **İdare Hukukunda Kanuna Dayanma İlkesi**, Turhan Kitabevi, Ankara, 2021.
- SEVİNÇ, Şule / YILMAZ, Fatma Özlem, "Türkiye’de Sağlık Hizmetleri Finansman Yöntemleri", **Selçuk Sağlık Dergisi**, 2020, 1(2),s. 118-132.
- SEYHAN Serkan, **Yapay Zekâ Teknolojileri Kapsamında İdarenin Sorumluluğu**, On İki Levha Yayıncılık, Mart 2023.
- SHAW, David M./GROSS, Juliane V./ERREN, Thomas C., "Data Donation After Death", **Embo Reports**, Vol.: 17, Issue: 1, January 2016, <https://doi.org/10.15252/embr.201541802> (Erişim Tarihi: 1.9.2021).
- ŞEN, Ersan, "Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", **İstanbul Barosu Dergisi**, Cilt: 83, Sayı: 3, Mayıs 2009, s.1197-1214.
- ŞİMŞEK, Oğuz, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta, Şubat 2008.
- SINAR, Hasan, "Devlet Sırrı Kanunu Tasarısı Üzerine Düşünceler", **Fasikül Hukuk Dergisi**, C.5, S.42, Mayıs 2013, s. 7-10.
- SINAR, Hasan, **Kişisel Verilerin Ceza Normlarıyla Korunması**, Der Yayınevi, Haziran 2023.
- SOLOVE, Daniel J., "A Brief History of Information Privacy Law", **PROSKAUER ON PRIVACY**, PLI, 2016, GWU Law School Public Law Research Paper No. 215, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271 (Erişim Tarihi: 15.7.2021).
- SOLOVE, Daniel J., "Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data", **118 Northwestern University Law Review**, 1081 (2024), GWU Legal Studies Research Paper No. 2023-22, GWU Law School Public Law Research Paper No. 2023-22, 21.1.2024, <http://dx.doi.org/10.2139/ssrn.4322198> (Erişim Tarihi: 3.7.2024).

- SÖYLER, Yasin, **Yeni Başkanlık Sisteminde Cumhurbaşkanlığı Kararnamesi**, Seçkin Yayıncılık, 2018.
- SÜNGÜ, Fatih “Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkemesine Bireysel Başvuru Kararlarında “Chilling Effect” Kavramı”, **İnsan Hakları Yıllığı**, C.39, 2021, s.105.134.
- TANSUĞ, Çağla, **İdari Faaliyetlerde İşlenen Kişisel Verilerin İdare Tarafından Korunması**, On İki Levha Yayıncılık, 2023.
- TAŞTAN, Furkan Güven, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, On İki Levha, 2. Baskı, 2017.
- TOSUN, Selma, “HIV Pozitif Kişilerin Cinsel Partnerlerine ve Yakınlarına Hastalığın Bildirilmesi”. ERKOL ZZ, DOĞRAMACI YG (Editörler), **Tıp Hukuku**. 1. Baskı. Ankara: Türkiye Klinikleri; 2019. s.88-96.
- TUNÇER, Polat, **Sağlık Hukuku Temel Bilgileri**, Adalet Yayınevi, 4. Baskı, 2019.
- TURAN BAŞARA, Gamze, “Kişiliğin Korunması Kapsamında Ölümden Sonra Hatıranın Korunması Teorisi”, **ÇÜHFD**, C.5, S.1, Nisan, 2020, s. 341-390.
- TÜRKOĞLU ÜSTÜN, Kamile, “Güvenlik Soruşturmalarda Kişisel Verilerin Korunması”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. XXV, Y. 2021, S.2, s.787-837.
- UÇAK, Murat, "Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası". **Kişisel Verileri Koruma**, 2021, S.3, s.41-60, <https://dergipark.org.tr/tr/pub/kvkd/issue/62960/826099> (Erişim Tarihi: 14.3.2022).
- UÇAR, İsmail, “İdare Hukukunda Kamu Gücü Ayrıcalığı Kavramı ve Bir Kamu Gücü Ayrıcalığı Olarak Hukuka Uygunluk Karinesi”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C.XX, S.3, 2016, s. 331-373.
- ULUSOY, Ali, “Cumhurbaşkanlığı Kararnameleri: Varoluşsal, Yapısal ve Hukuksal Bir Değerlendirme”, **Anayasa Yargısı**, Cilt: 37, S.:2, 2020.
- ULUSOY, Ali, **Yeni Türk İdare Hukuku**, Yetkin Yayınları, Ankara, 2019.
- USTA, Aydın, “Bilimsel Araştırmalarda Yapısal Etmenler ve Evreler”, **İnönü Üniversitesi Uluslararası Sosyal Bilimler Dergisi**, Cilt 1, Sayı 1, 2012, s.98-112, <https://dergipark.org.tr/tr/pub/inijoss/issue/8624/415750> (Erişim Tarihi: 13.10.2023).
- USTA, Sevgi, “Anne Babanın Tedip Hakkı”, **İ.Ü. Siyasal Bilgiler Fakültesi Dergisi**, No: 8 (Temmuz 1994), <https://dergipark.org.tr/tr/download/article-file/5505> (E.T. 8.8.2024).
- ÜÇÜNCÜ, S. Hilal, **Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması**, On İki Levha Yayıncılık, Temmuz 2019.
- ÜZELTÜRK, Sultan, **Özel Hayatın Gizliliği Hakkı**, Beta, 2004, İstanbul.
- UZUNÖZ, Ali, “6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kapsamı: İstisna hükümleri açısından bir değerlendirme”, **Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü**, Yüksek Lisans Tezi, 2022.

- VAN OOIJEN, Charlotte/UBALDI, Barbara/WELBY, Benjamin, “A data driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance”, **OECD Working Papers on Public Governance No.33**, 2019, <https://dx.doi.org/10.1787/09ab162c-en> (Eriřim Tarihi: 7.6.2024).
- VAN ZOONEN, Liesbet. “Data Governance and Citizen Participation in the Digital Welfare State.” **Data & Policy**, Vol. 2 2020: e.10, [doi:10.1017/dap.2020.10](https://doi.org/10.1017/dap.2020.10) (Eriřim Tarihi: 7.6.2024).
- WARREN, Samuel D./BRANDEIS Louis D., “The Right to Privacy”, **Harvard Law Review**, Vol:IV, December 15, 1890, No.5. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (Eriřim Tarihi: 28.7.2021)
- YAřAR, Hasan Nuri, **İdare Hukuku**, DER Yayınları, 3. Baskı, 2016.
- YASİN, Melikřah, “Cumhurbaşkanlığı Kararnamelerinin Türk İdari Teřkilat Hukukuna Etkileri”, **Anayasa Yargısı Dergisi**, Cilt: 36, S. 1, 2019, s. 315-333.
- YASİN, Melikřah, “İdarenin Özendirme ve Destekleme Faaliyetleri” içinde **İdare Hukuku**, Turan YILDIRIM (ed.), 8. Baskı, On İki Levha Yayıncılık, İstanbul, Kasım 2020.
- YASİN, Melikřah, “Kamu Hizmeti”, içinde **İdare Hukuku**, Turan YILDIRIM (ed.), 8. Baskı, On İki Levha Yayıncılık, İstanbul, Kasım 2020.
- YASİN, Melikřah, **İdari Yargılama Usulünde İspat**, On İki Levha Yayıncılık, 2015.
- YELMEN, Adem, “Kiřisel Saęlık Verilerinin Elektronik Ortamda İşlenmesi Üzerine Bir Deęerlendirme”, **Erciyes Üniversitesi Hukuk Fakóltesi Dergisi**, 18/2 (2023): 743-806.
- YENİSEY, Feridun, **Kolluk Hukuku**, Beta Yayınevi, 2.Baskı, 2015.
- YETİřKİN, Mustafa Burak, Mukayeseli Hukukta Devlet Sırrı, **Gazi Üniversitesi SBE Yayınlanmamış Yüksek Lisans Tezi**, 2018.
- YILDIRIM, Ramazan, **İdari Bařvurular**, Mimoza Yayınları, 2. Baskı, 2006.
- YILDIRIM, Turan / Fİř ÜSTÜN, Gül, **Açıklamalı-Notlu İdari Yargılama Usulü Kanunu**, On İki Levha Yayıncılık, İstanbul, Ekim 2020.
- YILDIRIM, Turan, “İdarenin Kanunilięi İlkesi Baęlamında Cumhurbaşkanlığı Kararnamelerinin Anayasal Sınırı”, **Anayasa Yargısı Dergisi**, Cilt: 36, S. 1, 2019, s. 293-314.
- YILDIRIM, Turan, “Kamu Görevlilerinin Özel Hayatı: Cinsel Tercih”, **Marmara Üniversitesi Hukuk Fakóltesi Hukuk Arařtırmaları Dergisi**, C.24, S.2, Aralık 2018, s. 453-481.
- YILDIZ, Bülent ve dięerleri, **İlamat ve İnfaz Eęitim Modülü**, T.C. Adalet Bakanlığı Eęitim Dairesi Bařkanlığı Rize Personel Eęitim Merkezi, <https://rayp.adalet.gov.tr/resimler/591/dosya/ilamat-ve-infaz-egitim-modulu16-12-202110-01-pm.pdf> (Eriřim Tarihi: 15.11.2023).

YILDIZ, Şerife, “İdari Faaliyetlerin Devri Bağlamında Özel Güvenlik”, **Marmara Üniversitesi SBE**, Doktora Tezi, 2010.

YILMAZ Berrak, “Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması”, **Hacettepe Üniversitesi SBE**, Doktora Tezi, 2019.

YOLAL, Halil, **Danıştay Kararları Işığında İptal Davalarında Dava Açma Ehliyeti**, On İki Levha Yayıncılık, 2019.

YÜCEL, Özge, “Çocuğun Yüksek (Üstün) Yararı Bağlamında Çocuğun İradesi”, **Ufuk Üniversitesi Hukuk Fakültesi Dergisi**, C.1, S.2, Aralık 2013, s.117-137.

YÜZBAŞI TOBAZ, Firdevs, “Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması”, **Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü**, Doktora Tezi, 2021.

YÜZBAŞIOĞLU, Cihan, **İdare ve Personel Yönüyle Sağlık hizmetlerinden Kaynaklanan Sorumluluk**, On İki Levha, Ocak 2020.

ZEYBEK CEBECİ, Ebru, **Kamu Hizmetlerinin Gördürülmesine İlişkin Sözleşmeler**, Seçkin Yayıncılık, 2021.

ZITTRAIN, Jonathan, “What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication”, **Stanford Law Review**, Vol. 52, No: 5, 2000, s. 1201-1250.

İNTERNET SAYFALARI:

“After Students Challenged Proctoring Software, French Court Slaps TestWe App With a Suspension”, **Electronic Frontier Foundation (EFF)**, 31.3.2023, <https://www.eff.org/tr/deeplinks/2023/03/after-students-challenged-proctoring-software-french-court-slaps-testwe-app> (Erişim Tarihi: 12.5.2024).

“Coronavirus privacy: Are South Korea’s alerts too revealing?”, **BBC**, 5.3.2020, <https://www.bbc.com/news/world-asia-51733145> (E.T. 20.5.2024).

“Court sides with University of Amsterdam on use of surveillance software”, **Cursor**, 12.6.2020, <https://www.cursor.tue.nl/en/news/2020/juni/week-2/court-sides-with-university-of-amsterdam-on-use-of-surveillance-software/> ya da <https://www.erasmusmagazine.nl/en/2020/06/12/court-sides-with-university-of-amsterdam-on-use-of-surveillance-software/> (Erişim Tarihi: 12.5.2024).

“Federal Judge: Invasive Online Proctoring "Room Scans Are Unconstitutional”, **Electronic Frontier Foundation (EFF)**, 25.8.2022, <https://www.eff.org/tr/deeplinks/2022/08/federal-judge-invasive-online-proctoring-room-scans-are-also-unconstitutional> (Erişim Tarihi: 12.5.2024).

“Mahkeme çocuklarını reklam malzemesi yapan blogger annenin iki çocuğunu babaya verdi” **NTV**, 30.6.2017.
<https://www.ntv.com.tr/turkiye/mahkeme-cocuklarini-reklam-malzemesi-yapan-blogger-annenin-iki-cocugunubabaya-verdi,qS8Pj79Zc0SNNhjagnJu8A> (Erişim Tarihi: 14.3.2022).

“Maliyeti açıklanırsa ülke ekonomisi çıkarları zarar görür”, **Dünya**, 2.12.2014,
<https://www.dunya.com/gundem/039maliyeti-aciklanirsa-ulke-ekonomisi-cikarlari-zarar-haberi-264593>, (Erişim Tarihi: 7.12.2023).

“MEB’in Eğitim Programı ‘EBA’ tanıtıldı”, **memurlar.net**, 7.10.2015,
<https://www.memurlar.net/haber/540343/meb-in-egitim-programi-eba-tanitildi.html> (Erişim Tarihi: 22.4.2024).

“The world’s most valuable resource is no longer oil, but data”, **The Economist**, 6.5.2017,
<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (E.T.: 24.10.2021).

“TOKİ, Cumhurbaşkanlığı Sarayı’nın maliyetini mahkemeye de açıklamadı”, **CNN Türk**, 28.1.2015,
<https://www.cnnturk.com/turkiye/toki-cumhurbaskanligi-sarayinin-maliyetini-mahkemeye-de-aciklamadi> (Erişim Tarihi: 7.12.2023).

“Unfair surveillance”? Online exam software sparks global student revolt”, **Reuters**, 11.11.2020,
<https://www.reuters.com/article/idUSKBN27Q1PY/> (Erişim Tarihi: 12.5.2024).

ATALAY, Figen, “FATİH projesi çöpe gitti: ‘Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi’, milyonlarca öğrenciye ulaşamadı”, **Cumhuriyet**, 13.9.2023,
<https://www.cumhuriyet.com.tr/egitim/fatih-projesi-cope-gitti-firsatlari-artirma-ve-teknolojiyi-iyilestirme-hareketi-milyonlarca-ogrenciye-ulasamadi-2118710> (Erişim Tarihi: 24.4.2023).

ÇALIKOĞLU, Melih R., “Görüntü ve Ses Biyometrik Veri Değildir”, **KVBLOG**, 16.4.2020,
<https://kisiselveriler.blog/2020/04/16/goruntu-ve-ses-biyometrik-veri-degildir/> (Erişim Tarihi: 3.4.2024).

ÇALIŞKAN, Necdet, “Öldükten sonra sosyal medya hesaplarınız ne oluyor?”, **Habertürk**, 19.12.2020,
<https://www.haberturk.com/oldukten-sonra-sosyal-medya-hesaplari-ne-oluyor-haberler-2907289-teknoloji> (Erişim Tarihi: 2.9.2021).

EKMEKÇİ Ömer, YÜCEDAĞ Nafiye, AKKANAT-ÖZTÜRK Elif Beyza, AŞIKOĞLU Şhrıban İpek, “Ceza Muhakemesi Kanunu ile Bazı Kanunlarda ve 659 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılmasına Dair Kanun Teklifi ile 6698 Sayılı Kanun’da Yapılan Değişiklikler”, **Lexpera Blog**, 02.03.2024, <https://blog.lexpera.com.tr/cm-k-659-6698-degisiklikler/> (Erişim Tarihi: 5.7.2024).

ELİBOL, Kamil, “Adrese Teslim MOBESE Cezalarına Özel Makyaj”, **Memurlar.net**, 21.3.2011,
<https://www.memurlar.net/haber/191437/adrese-teslim-mobese-cezalarina-ozel-makyaj.html> (Erişim Tarihi: 6.1.2022).

- INGRAM, Mike, “Microsoft’s new ‘Productivity Score’ helps employers spy on workers”, **World Socialist Web Site**, 29.11.2020, <https://www.wsws.org/en/articles/2020/11/30/micr-n30.html>. (Erişim Tarihi: 28.10.2021).
- MOSTROUS, Alexi/BROWN, David, “Microsoft seek patent for Office ‘spy’ software”, **The Times**, 16.1.2008, <https://www.thetimes.co.uk/article/microsoft-seeks-patent-for-office-spy-software-h0dd5zmtfnt>. (Erişim Tarihi: 28.10.2021).
- ÖVGÜ, Pınar, “Oğlunun fotoğraflarını izinsiz sosyal medyada paylaşan anne suçlu bulundu”, **BBC News Türkçe**, 8.1.2018. <https://www.bbc.com/turkce/haberler-dunya-42604622> (Erişim Tarihi: 15.3.2022).
- SIMMONS, Alistair, “The Vulnerability and Protection of Student Data”, **LAWFAREMEDIA**, 4.12.2023. <https://www.lawfaremedia.org/article/the-vulnerability-and-protection-of-student-data> (Erişim Tarihi: 11.3.2024).
- The UK’s Information Commissioner’s Office (ICO), “What are the rules about an ISS and consent?”, **Guide to the GDPR**, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/> (Erişim Tarihi: 20.1.2022).
- The UK’s Information Commissioner’s Office (ICO), “What is an unambiguous indication (by statement or clear affirmative action)?”, **Guide to the GDPR**, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/> (Erişim Tarihi: 17.1.2022).
- The UK’s Information Commissioner’s Office (ICO), “What is explicit consent?”, **Guide to the GDPR**, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/> (Erişim Tarihi: 17.1.2022).
- Türk Dil Kurumu Sözlükleri, Güncel Türkçe Sözlük, <https://sozluk.gov.tr/>.
- TÜRKMEN, Sevgi, “Özel Nitelikli Kişisel Veri Kavramının Ortaya Çıkışı, Gerekliliği ve Özel Nitelikli Kişisel Veri Tanım ve Kapsamları”, **Lexpera Blog**, 18.10.2019, <https://blog.lexpera.com.tr/ozel-nitelikli/> (Erişim Tarihi: 27.8.2021).
- WALTERS, Laura, “Universities expand controversial AI monitoring of students taking online exams”, **STUFF**, 5.11.2021, <https://www.stuff.co.nz/national/education/126908715/universities-expand-controversial-ai-monitoring-of-students-taking-online-exams> (Erişim Tarihi: 10.5.2024).
- YILMAZ, Sabire Sanem, “Bilimsel Amaçlı Kişisel Veri İşlenmesine Hukuki Bakış”, **kisiselveriihlali.com**, 8.12.2021 (Erişim Tarihi: 13.10.2023).