KADİR HAS ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
HUKUK ANABİLİM DALI

KİŞİSEL VERİLERİN SORUŞTURMA EVRESİNDE İŞLENMESİ VE İNSAN HAKLARI KAPSAMINDA KORUNMASI

MUHAMMET SEFA MUTLU

DANIŞMAN: DR. ÖĞR. ÜYESİ, FULYA EROĞLU

YÜKSEK LİSANS TEZİ

İSTANBUL, EKİM, 2019

KİŞİSEL VERİLERİN SORUŞTURMA EVRESİNDE İŞLENMESİ VE İNSAN HAKLARI KAPSAMINDA KORUNMASI

MUHAMMET SEFA MUTLU

DANIŞMAN: DR. ÖĞR. ÜYESİ, FULYA EROĞLU

YÜKSEK LİSANS TEZİ

Hukuk Anabilim Dalı Kamu Hukuku Programı'nda Yüksek Lisans derecesi
için gerekli kısmi şartların yerine getirilmesi amacıyla
Kadir Has Üniversitesi Lisansüstü Eğitim Enstitüsü'ne
teslim edilmiştir.

İSTANBUL, EKİM, 2019

Ben, MUHAMMET SEFA MUTLU;

Hazırladığım bu Yüksek Lisans Tezinin tamamen kendi çalışmam olduğunu ve başka çalışmalardan yaptığım alıntıların kaynaklarını kurallara uygun biçimde tez içerisinde belirttiğimi onaylıyorum.

ÖĞRENCİNİN ADI SOYADI

Muhammet Sefa MUTLU

TARİH VE İMZA

04.10.2019

KABUL VE ONAY

MUHAMMET SEFA MUTLU tarafından hazırlanan **KİŞİSEL VERİLERİN SORUŞTURMA EVRESİNDE İŞLENMESİ VE İNSAN HAKLARI KAPSAMINDA KORUNMASI** başlıklı bu çalışma **04.10.2019** tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından **TEZİN/PROJENİN TÜRÜ** olarak kabul edilmiştir.

Dr. Fulya EROĞLU (Danışman)	Üniversite Altınbaş Üniversitesi	İMZA
Dr. Aysun ALTUNKAŞ (Eş Danışman)	Üniversite Kadir Has Üniversitesi	İMZA
Prof. Dr. Tuğrul Bayazıt KATOĞLU	Üniversite Kadir Has Üniversitesi	İMZA
Gülşah BOSTANCI BOZBAYINDIR	Üniversite Sabahattin Zaim Üniversitesi	İMZA

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

İMZA
Müdür
Lisansüstü Eğitim Enstitüsü
ONAY TARİHİ: Gün/Ay/Yıl
Prof. Dr. Sinem Akgül Açıkmeşe

İÇİNDEKİLER

BİRİNCİ BÖLÜM

KİŞİSEL VERİ TERİMİ, KAPSAMI VE İNSAN HAKKI BOYUTU

İKİNCİ BÖLÜM

ULUSLARARASI BELGELERDE VE TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

ÜÇÜNCÜ BÖLÜM

SORUŞTURMA SÜRECİNDE KİŞİSEL VERİLERİN İŞLENME İLKELERİ VE ULUSLARARASI STANDARTLAR

DÖRDÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN SORUŞTURMA EVRESİNDE KORUMA TEDBİRLERİ VE DİĞER DELİL DEĞERLENDİRME YÖNTEMLERİ İLE İŞLENMESİ

KISALTMALAR

AB	: Avrupa Birliği
AK	: Avrupa Konseyi
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AY	: Anayasa
AYM	: Anayasa Mahkemesi
bkz.	: Bakınız
BEHK	: Bilgi Edinme Hakkı Kanunu
BM	: Birleşmiş Milletler
CGK	: Yargıtay Ceza Genel Kurulu
CMK	: Ceza Muhakemesi Kanunu
CGTİHK	: Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun
D.	: Danıştay
E.	: Esas
GDPR	: General Data Protection Regulation
K.	: Karar
KVK	: Kişisel Verilerin Koruması
KVKK	: Kişisel Verilerin Korunması Kanunu
m.	**:** Madde
OECD	:Organization for Economic Cooperation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü)

par.	: Paragraf
PVSK	: Polis Vazife ve Salâhiyet Kanunu
s.	: Sayfa
TCK	: Türk Ceza Kanunu
TBK	: Türk Borçlar Kanunu
TDK	: Türk Dil Kurumu
TKK	: Tanık Koruma Kanunu
vb.	: ve benzeri
vd.	: Ve devamı
VKS	: Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme
Y.	: Yargıtay

ÖZET

MUTLU, MUHAMMET SEFA. *SORUŞTURMA EVRESİNDE KİŞİSEL VERİLERİN İŞLENMESİ VE BİR İNSAN HAKKI OLARAK KORUNMASI,* YÜKSEK LİSANS TEZİ, İstanbul, 2019.

Bu tez çalışmasının amacı, kişisel verilerin soruşturma evresinde insan hakları bağlamında korunması gerektiğini çeşitli argümanlar vasıtasıyla ortaya koyabilmektir. Bu amaç doğrultusunda tezin kapsamında öncelikle kişisel veri teriminin hukuki metinlerindeki düzenleniş biçimi bağlantılı olduğu diğer temel hak ve hürriyetlerle birlikte ortaya konulmaktadır. Akabinde kişisel verilerin korunması ile ilgili yerel ve uluslararası hukuk metinler incelenmekte, AİHM'in kararları ışığında bu düzenlemeler yorumlanmaktadır. Bu yorum faaliyetiyle kişisel verilerin korunması hakkının ihlal edilmemesi için soruşturma evresinde kişisel verilerin işlenmesine yönelik ilkeler çıkarılmaktadır. Nihayet, CMK ve diğer hukuk kurallarına dayanan kişisel verilerin soruşturma evresinde işleme yolları bu ilkeler nazarından değerlendirilmektedir. İlgili yerel ve uluslararası mevzuatın incelenmesi ve yorumlanması sonucunun ürünü olan söz konusu ilkeler, Türk hukukunda soruşturma evresinde kişisel verilerin korunmasına yönelik doğrudan ve yeterli uygulanacak hükümlerin olmaması nedeniyle anahtar niteliğindedir. Bunu ortaya koyabilmek adına, tez yazım yöntemi olarak parçalardan tüme varım metodu kullanılmıştır.

Tez çalışmasının sonunda varılan sonuç, Türk hukukunda kişisel veriler konusunda özel düzenleme olan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun çağın şartlarına uyum sağlayamıyor oluşudur. Daha özel olarak ifade etmek gerekirse, Kanun m. 28'de yer alan istisna hükümleri soruşturma evresinde işlenmekte olan kişisel verileri, kanunun sağladığı koruma kapsamına almaması nedeniyle çeşitli hukuka aykırılıklar olabileceği gözlemlenmiştir. Bunlardan en önemlisi, soruşturma evresinin istisna hükmü kapsamında olması sebebiyle kişisel verilerin koruma kapsamı dışında bırakılmasının hakkın özüne müdahale teşkil edebilecek olup Anayasa'ya aykırı olabileceğidir. Oysa AB hukukunda GDPR'ı ceza hukuku yönünden tamamlayan 2016/680/EU sayılı Direktif'in varlığı

sebebiyle kişisel veriler soruşturma evresinde de korunabilmektedir. Zikredilen direktif benzeri düzenlemelerin Türk hukukunda hala yer almıyor oluşu, mevcut hükümlerdeki hukuka aykırılık tartışmalarını en azından belli bir süre daha devam edeceğini göstermektedir.

Anahtar Sözcükler: kişisel veri, soruşturma evresi, kişisel verilerin korunması hakkı, özel ve aile hayatının gizliliği, GDPR, 2016/680/EU sayılı Direktif, KVK Kanunu.

ABSTRACT

MUTLU, MUHAMMET SEFA. *PROCESSING OF PERSONAL DATA IN CRIMINAL INVESTIGATION AND PROTECTING AS A HUMAN RIGHT*, MASTER'S THESIS, İstanbul, 2019.

The purpose of this thesis is to demonstrate the need to protect personal data as a human right in the investigation phase by means of various arguments. For this purpose, within the scope of the thesis, firstly the configuration of the personal data term in the legal texts are displayed together with the other fundamental rights and freedoms. Then, the local and international legal texts related to the protection of personal data are examined and these regulations are interpreted in the light of the decisions of the ECtHR. In order to prevent any violation of the right to the protection of personal data, the principles for the processing of personal data are drawn up in the investigation phase, by this interpretation activity. Finally, the means of processing the personal data based on the Code of Criminal Procedure(CMK) and other legal rules in the investigation phase are evaluated according to these principles. These principles, which are the result of review and interpretation of relevant local and international legislation, are key to Turkish law due to the absence of provisions to be applied directly to the protection of personal data during the investigation phase. In order to reveal this, the method epagoge was used as a writing method throughout the thesis.

The conclusion reached at the end of the thesis study is that the Code on the Protection of Personal Data No. 6698(KVKK), which is a special regulation on personal data in Turkish law, does not comply with the current modern conditions. More specifically, it is observed that the exception provisions contained in Article 28 may cause infringement of constitutional rights since the personal data processed during the investigation phase are kept out from the protection provided by the law. The regulation can cause many legal problems but the crucial one is that the fact that the personal data is not protected at all due to investigation phase is within the scope of the exemption provisions may interfere with the essence of the right and may be against the Constitution. However, in EU law,

personal data can be protected during the investigation phase due to the existence of Directive No. 680 which complements the GDPR in terms of criminal law. The fact that the aforementioned directive-like arrangements are still not included in Turkish law shows that the discussions of illegality in the current provisions will continue for at least a certain period of time.

Keywords: personal data, investigation phase, right to protection of personal data, right to respect for private and family life, GDPR, 2016/680/EU Directive, the Code on the Protection of Personal Data.

GİRİŞ

Son yıllarda gerek Türkiye gerekse dünyanın geri kalan modern ülkelerinde kişisel verilerin korunması alanında dinamik bir gelişim süreci yaşanmaktadır. Daha çok hukuki olmakla birlikte teknik yönü de olan bu süreci ateşleyen bir yön insan hakları söyleminin yaygınlaşması ve daha fazla önem kazanması iken, diğer bir yön kitlesel olarak kişisel verilerin ekonomik amaçlarla işlenmeye başlamasıdır. Önceleri temel hak ve hürriyetler içerisinde özel hayatın gizliliği kapsamında mütalaa edilen ve kısmen korunan kişisel verilerin korunması hakkı ihtiva ettiği niteliklerinin ortaya çıkmasıyla birlikte bağımsız bir hak olma eğilimine yönelmiştir. Bu doğrultuda, verilerin yeterli düzeyde korunmasının sağlanması ve ülkelerin hukuk kuralları arasındaki düzenleme farklılıklarının ortadan kaldırılması amacıyla, çeşitli uluslararası anlaşmalar imzalanmıştır. İlkin daha çok özel hukuka dönük hükümleriyle koruma altına alınan verilerin korunması konusu, ortak tecrübe ve bilinç sonucunda belirginleşen veri işleme ilkeleri sayesinde kamu hukuku alanına da sirayet etmeye başlamıştır.

Türk hukukunda ise 2010 yılında Anayasa m. 20'ye eklenen üçüncü fıkra ile kamu hürriyetleri arasında ilk defa yer alan kişisel verilerin korunması hakkı, 6698 sayılı KVK Kanunu'nun 2016 yılında yürürlüğe girmesiyle detaylı ve özel bir düzenlemeye kavuşmuştur. AB düzenlemeleri temel alınarak hazırlanan bu kanun, meclisteki kanunlaşma sürecinde hakkı korumaktan uzak olacağı sebebiyle tartışmalarla yürürlüğe girmiştir. AB, kişisel verilerin koruması alanında oldukça ses getiren Genel Veri Koruma Tüzük'ü(GDPR) çıkarma hazırlığındayken yürürlüğe giren KVK Kanunu, Tüzük'ün yeterli koruma sağlamadığı sebebiyle ilga ettiği 95/46/EC sayılı AB Direktif'i esas alarak hazırlanmıştır. Esasında özel hukuk saikiyle ortaya çıkan AB'nin GDPR düzenlemesi kişisel verilerin korunmasına ilişkin genel fakat detaylandırılmış hükümler barındırmaktadır. GDPR ile aynı gün 2016/680/EU sayılı Direktif çıkarılarak soruşturma evresi de dâhil olmak üzere kişisel verilerin ceza hukukuna bakan yönüne özel hükümler getirilmiştir.

Verilerin korunmasının tabiri caizse anayasal hükümleri olan kişisel verilerin işlenmesine ilişkin genel ilkeler, kişisel verilerle ilgili hemen hemen her düzenlemede yer almaktadır. Fakat KVK Kanunu m. 28'de getirdiği istisna hükümleri ile soruşturma evresinde KVK Kanunu'nun hiçbir şekilde uygulama alanı bulmayacağını düzenlemiştir. Bu sebeple,

KVK Kanunu'nda yer alan ne verilerin korunmasındaki genel ilkeler ne de verilerin korunmasına ilişkin işleme şartları ve veri sahibinin hakları, soruşturma evresinde hiçbir surette uygulama alanı bulamamaktadır. Dolayısıyla, kişisel verilerin korunması amacıyla getirilen KVK Kanunu soruşturma evresinde kişisel verileri korumamaktadır. Oysa AB hukuku örneğinde olduğu gibi, ceza hukukuna ilişkin meselelerde kişisel verileri koruma kapsamından çıkarmak yerine özel hükümlerle bu alanın düzenlenmesi, kişisel verilerin korunması konusunda olması gerekendir. CMK'da yer alan koruma tedbirleri ve delil değerlendirme yöntemlerine ilişkin hükümler vasıtasıyla dolaylı olarak korunmanın dışında, KVK Kanunu bu haliyle, verilerin hangi usul ve şartlarla işleneceği ve veriyi işleyen kamu görevlilerin keyfi davranışlarını belirlemekte olan bir düzenleme niteliğinde değildir. Fakat verilerin korunması anayasal bir hak olduğu için kanunun verilerin soruşturma evresinde hiç korunmayacak şekilde düzenlenmesi, hakkın özüne müdahale teşkil edebilecektir.

İşte bu sebeple, bu tez çalışması kapsamında, KVK Kanunu'nda yer aldığı şekliyle kişisel verilerin soruşturma evresinde işlenmesine karşılık insan hakları bağlamında nasıl korunması gerektiği analiz edilmektedir. İncelenen uluslararası belgeler, ilgili kanunlar ve ulusal yüksek mahkeme ve AİHM kararları doğrultusunda KVK Kanunu m. 28'de yer alan soruşturma evresini koruma kapsamı dışında bırakan istisna hükmünün hukuka uygun olup olmadığı ortaya çıkarılmak istenmektedir. Bu çerçevede öncelikle kişisel veri teriminin hukuken neyi ifade ettiği ve insan hakları bağlamında neden koruma kapsamında olması gerektiği ortaya koyulmaktadır. Akabinde çeşitli AİHM kararları başta olmak üzere, incelenen uluslararası hukuk kuralları sonucunda kişisel verilerin soruşturma evresinde işlenmesine ilişkin ilkeler ve veri sahibinin hakları çerçevesi oluşturulmaya çalışılmaktadır. Olması gereken standardın parametreleri kullanılarak ilkin KVK Kanunu geniş bir perspektifle eleştirilmektedir. Son olarak ise kişisel verilerin soruşturma evresinde işlenme yöntemleri ve diğer veri işleme alanları olması gerekenin süzgecinden geçirilerek yorumlanmaktadır.

BİRİNCİ BÖLÜM:

KİŞİSEL VERİ TERİMİ VE KİŞİSEL VERİLERİN KORUNMASI

I. KİŞİSEL VERİ

A. Genel Olarak

Kişisel veri, en basit tanımıyla bir kişiye ait şahsi bir veriyi ifade etmektedir. Ancak onu gerçek anlamıyla tanımlamak için kişisel verilerin terimini, kapsamını ve özelliklerini açıklamak gerekmektedir. "Kişisel veriler" kelimesinin, kavramsal boyutunun yanı sıra hukuk disiplini içerisinde bir terim boyutu da olduğu için öncelikle kişisel verilerin dil bilimsel olarak kavram ve terim boyutunu ortaya koymak önem taşımaktadır.

Kavram, bir nesnenin zihinde sınırlandırılmaya yahut nitelendirilmeye elverişli bir tasavvurunu ifade etmektedir. Her somut veya soyut anlamlı kelimenin kavramsal boyutundan bahsedebilmek mümkündür. Bir kelime ya da kelime öbeğinin kavram dünyasındaki sınırları oldukça geniştir. Terim ise kavrama benzemekle birlikte bilim, meslek yahut sanat dalı içerisinde belirginleşmiş olan bir anlamı ifade etmektedir. Her terim bir kavram iken, her kavram bir terim değildir. Dolayısıyla terimler, ifade ettiği anlamlar bakımından kavramların alt kümesi şeklinde de düşünülebilir. Bir kelimenin terim olarak kullanılabilmesi için ifade ettiği anlamın belli bir disiplin içerisinde belirgin bir yere sahip olması gerekir. Yani o kelime bilimsel bir terim halini aldığında, ifade etmekte olduğu anlam belli şartlar ve koşullar altında artık oldukça somutlaşmış ve sınırlandırılmış bir hale gelmiş olmaktadır. Ayrıca, aynı terimin farklı disiplinler içerisinde farklı anlamları da olabilir. Özetle, kavram, nesnelerin ve olguların zihinde uyandırdığı sınırı belli olmayan soyut ve genel tasarımı işaret etmekteyken; terim, belli bir disiplin içerisinde sınırı belirginleşmiş olan durum veya yargıyı ifade etmektedir[1].

Kişisel veriler kelime öbeğinin kavram dünyası içerisinde ifade ettiği anlam bir kişiye ait olan verileri işaret etmektedir. Öte yandan, belli bir disiplin ve metodolojiye sahip olan hukuk biliminin kendi dünyasındaki kişisel veriler ise bir kavramdan ziyade bir terim olarak karşımıza çıkmaktadır. Çünkü kişisel verilere atfen hukuk dünyasında haklar,

[1] Hava, Y. F. 2016. *Türk Dış Politikasında TİKA Bağlamında Yumuşak Güç Kullanımı Ve Balkanlar*. Yayınlanmamış Yüksek Lisans Tezi, Çanakkale: Çanakkale Onsekiz Mart Üniversitesi, Sosyal Bilimler Enstitüsü, s. 4.

borçlar ve yaptırıma tabi cezalar bulunmaktadır. Bu kavramı hukuk biliminde içsel olarak sınırlayan kurallar sebebiyle, kişisel veriler kelime öbeği, hukuk dünyasına özgü bir anlam ifade ettiği için hukuki mülahazalar içerisinde kavram yerine terim olarak ifade edilmesi gerekmektedir.

B. Kişisel Veri Terimi

Türk Dil Kurumu'na göre, "kişisel" kelimesi "*kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zatî, tek kişiye özgü*", "veri" kelimesi ise "*işlenebilir duruma getirilmiş bilgi veya olgu ve belirtilmiş anlatımlardan bilinmeyeni bulmaya yarayan şey*" olarak tanımlanmaktadır[2]. Dolayısıyla TDK açısından kişisel veriler tek bir kişinin zatına özgü olan ve onun ayırt edilmesini sağlayan bilgi ve olgular olarak ifade edilebilir. Her ne kadar hukuk kuralları içerisinde kişisel bilgi ve verinin aynı anlamda kullanılması söz konusu olsa bile esasen bu iki kavram farklı anlamlara gelmektedir. Buna göre, bilgiyi veriden ayıran unsur anlam unsurudur. Veriye anlam yüklenilmiş hali bilgiyi oluşturmaktadır[3]. Yani, verinin kullanıp işlenmesi sonucu bilgi oluşmaktadır[4].

Bilişim sistemleri açısından bakıldığında bu alan içerisinde veri terimi, tüm sisteme kaynaklık etmektedir. Öyle ki bilişim sistemlerinin amacını şekillendiren temel bir unsuru teşkil etmektedir. Buna göre, saklanma, işlenme ve sonuç çıkartılmasıyla veriler belirli bir formata dönüşerek bilgiyi oluşturmaktadırlar[5].

Hukuk dünyasındaki kişisel veriler terimi ise, bir kişi ile ilintili ve o kişiyi tanımlamaya elverişli olan, o kişiye ait her türlü veriyi belirtmektedir. Kişisel verilerin örnekleyici olarak sayıldığı Yargıtay'ın yerleşmiş içtihadına bakılırsa söz konusu verilerin "*kişinin, ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri, adli sicil kaydı, banka hesap bilgileri, telefon numarası, elektronik posta adresi, parmak izi, DNA'sı, saç, tükürük, tırnak gibi*

[2] Türk Dil Kurumu Büyük Türkçe Sözlük. 2019. "Kişisel" Erişim Tarihi: Mart 2019 http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5c979f3cbbb497.33853275; "Veri" Erişim Tarihi: 19 Mart 2019 http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5c97a2f190afa3.80189263.

[3] Dülger, Murat Volkan: Kişisel Verilerin Korunması Hukuku, İstanbul 2019, s. 6.

[4] Henkoğlu, Türkay: Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015, s. 27.

[5] Bük, Alaattin: Bilişim Alanında Kişisel Verilerin Korunması, Ankara 2018, s. 51.

biyolojik örnekleri, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları" [6] gibi veriler olduğu görülmektedir.

Kişisel verinin ne olduğunu tanımlayan ve açıklayan hükümler Türk hukuku içerisinde muhtelif düzenlemelerde yer almaktadır. Öncelikle belirtmek gerekir ki, 1982 Anayasasında kişisel verilerin korunmasının bir anayasal hak olduğunun belirtilmesinin dışında, kişisel veriler ile ilgili tanım yahut açıklamaya yer verilmemiştir.

Anayasa Mahkemesi'nin bu konuda istikrar kazanmış tanımına göre ise, kişisel veri terimi "*belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri*" ifade etmektedir[7].

Türk hukukunu etkileyen uluslararası belgeler açısından ise 1980 yılında çıkarılan OECD'nin Rehber İlkeleri m. 1(b)'ye göre, kişisel veri, "*tanımlanmış veya tanımlanabilir bir bireye (veri sahibi) ilişkin herhangi bir bilgi*" anlamına gelmektedir.

KVK Kanunu'nun dayanaklarından biri olan 1981 yılına ait Avrupa Konseyi Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme(VKS) m. 2'ye göre kişisel veriler ise, "*kimliği belirli veya belirlenebilir bir gerçek kişi(ilgili kişi) hakkındaki tüm bilgileri*" ifade etmektedir.

Kişisel veriler teriminin tanımına Avrupa Birliği hukuku çerçevesinde bakılacak olursa, 1995 yılında yürürlüğe giren 95/46/EC sayılı Direktif m. 2(a)'ya göre kişisel veriler, "*fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir gerçek kişiye ilişkin herhangi bir bilgiyi*" ifade etmektedir. Yaşanan gelişmeler doğrultusunda 95/46/EC sayılı Direktif'in yerine 2018 yılında yürürlüğe giren GDPR'a göre kişisel veri ise, "*tanımlanmış veya tanımlanabilir bir gerçek kişiye(veri sahibine) ilişkin her türlü bilgi*" anlamına gelmektedir. Buradaki tanımlama unsurunu sağlayan söz konusu veriler özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla

[6] Y. 12. CD, 05.09.2018, E. 2018/2571 K. 2018/7821, Kazancı İçtihat Bilgi Bankası.
[7] Başvuru No: 2014/7256, 27.02.2019, par. 57; Başvuru No: 2013/2941, 11.5.2016, par. 49, Erişim Tarihi: 15 Mart 2019; E. 2014/149, K. 2014/151, KT: 02.10.2014, RG. 29223, 01.01.2015; E.2013/84, K.2014/183, KT: 04.12.2014, RG. 29294, 13.03.2015; ; E.2014/180, K.2015/30, KT: 19.3.2015, RG. 29321, 09.04.2015, Erişim Tarihi: 19 Mart 2019.

sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak bir kişiyi tanımlamaktadır[8].

Yargıtay'ın tanımına göre ise, "*kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü veridir*"[9].

Kanun düzeyinde ise, *inter alia*[10], 2016 yılında özel kanun olarak çıkarılan 6698 sayılı Kişisel Verilerin Korunması Kanunu m. 3(d)'deki tanıma göre kişisel veri, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmaktadır. Bu kanunun genel gerekçesinde ise, kişisel veriler, "*bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi olarak kişinin kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına, dini inancına ve siyasi görüşüne ilişkin bilgiler*" olarak nitelendirilmektedir[11].

Türk Ceza Kanunu'nda kişisel verileri konu alan suçlar (m.135 vd.) düzenlenmekte olsa bile bunlar içerisinde kişiler verilerin tanımı yapılmamaktadır. Sadece m. 135(2)'de kişisel verilerin kaydedilmesi suçunun konusunu kişilerin siyasi, felsefi veya dini görüşleri, ırki kökenleri; hukuka aykırı olarak ahlaki eğilimleri, cinsel yaşamları, sağlık durumları veya sendikal bağlantıları oluşturması halinde bu durum nitelikli hal olarak belirtilmektedir[12].

Ceza Muhakemesi Kanunu'nda ise kişisel verilerin tanımı yapılmamakla birlikte muhtelif maddelerinde kişisel veriler ile bağlantılı hükümler bulunmaktadır[13]. Ayrıca, CMK m. 80(1)'de bazı verilerin kişisel veri olduğu da açıkça belirtilmektedir. Buna göre, şüpheli, sanık ve diğer kişiler üzerinde yapılan beden muayenesi, vücuttan örnek alınması ve

[8] GDPR, m. 4(1).
[9] Y. 12. CD, 05.09.2018, E. 2018/2571 K. 2018/7821, Erişim Tarihi: 18 Mart 2019, Kazancı İçtihat Bilgi Bankası.
[10] Latince bir kavramdır. "Diğerlerinin yanında" anlamına gelmektedir.
[11] 6698 sayılı Kanun Gerekçesi, s. 4.
[12] Nitelikli hal olarak düzenlenmesinin anlamı, sayılan unsurların hassas nitelikli kişisel veri olması ve ayrımcılığa yol açabileceği düşüncesi sebebiyle daha fazla korumak amacıyla cezada artırıma gidiliyor oluşudur.
[13] Örneğin, tanığa ait kişisel bilgiler ile ilgili CMK m. 58(2), gizli soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgiler ile ilgili CMK m. 139(6), duruşmada anlatılması zorunlu belge ve tutanaklardan sanığa veya mağdura ait kişisel verilerin yer aldığı belgeler ile ilgili CMK m. 209(2).

moleküler genetik incelemeler sonucu verilerin kişisel veri niteliğinde olduğu hükme bağlanmıştır.

Elektronik haberleşme sektöründe kişisel verilerin korunması amacıyla 24.07.2012 tarihinde çıkarılan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik m. 3(1)(h)'ye göre kişisel veri, "*belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgilerini*" ifade etmektedir.

Kişisel verilerin sağlık alanında korunması amacıyla Sağlık Bakanlığı'nca 20.10.2016 tarihinde çıkarılan 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'te de kişisel veri tanımı yapılmamakla birlikte kişisel sağlık verisinin tanımı yapılmaktadır. Yönetmelik m. 4(1)(g)'e göre, kişisel sağlık verisi, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisini*" ifade etmektedir.

Kişisel verilerin zikredilen belgelerde yapılan bu ortak tanımının, doktrinde de kabul görmekte olduğunu belirmek gerekir. Bu doğrultudaki bir görüşe göre, *"kişisel veri, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi"* anlamına gelmektedir[14]. Doktrinin büyük çoğunluğu bu tanım etrafında birleşmiş olmasına rağmen yapılan farklı tanımlar da bulunmaktadır. Buna göre bir görüş kişisel verileri, "*bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli her türlü bilgi"* olarak tanımlamaktadır[15]. Başka bir görüşe göre ise, bir kişinin yaşı, cinsiyeti, doğum yeri, dini, T.C. kimlik numarası, cinsel hayatı, cep telefonu numarası, medeni durumu, ailesi, işi, ekonomik durumu, özel zevkleri ve buna benzer bilgileri kişisel verilerini ifade etmektedir[16]. Bir başka görüşe göre kişisel veri terimi, veri, bilgi ve kimliği belirli veya belirlenebilir bir kişi unsurlarının bir arada bulunmasıyla oluşan verilerdir[17].

[14] Küzeci, Elif: Kişisel Verilerin Korunması, Ankara 2019, s. 9.
[15] Şen, Ersan: Yeni Türk Ceza Kanunu Yorumu, İstanbul 2006, s. 601.
[16] Sırabaşı, Volkan: İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Ankara 2007, s. 195.
[17] Akgül, Aydın: Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014, s. 10-16.

Sonuç olarak, görüldüğü üzere kişisel veri terimi, bir gerçek kişiyi doğrudan ya da dolaylı olarak belirlenebilir kılacak her türlü bilgi ya da veri olarak ifade edilebilir. Ayrıca bir kişinin özel hayatı içerisinde yer alan diğer kişilere ait bilgiler de somut olayda odaklanılan kişiyi tanımlama unsurunu yerini getirdiği takdirde kişisel veriler kapsamında yer alabilecektir[18]. Bu takdirde, kişisel verilerin iç içe geçmesinden bahsedilebilir. Örneğin A kişinin yakını B'yi tanımlayan bir veri A üzerinden işleniyorsa, bu veri hem A kişisinin hem de B kişisinin kişisel verisi olmaktadır. Bu yüzden, yakınlar arasında her kişinin kişisel verisi diğer yakınlar için de kişisel veri olabilecektir. Bu durum özellikle bir kişinin yakını vefat ettiğinde vefat edene ait verilerin yakınlarını tanımlama kudretinde olması sebebiyle önem arz etmektedir.

C. Kapsam

1. Genel olarak

Bir kişiyi belirli kılabilecek verilerin tamamının nelerden ibaret olduğunu ifade edebilmenin imkânı yoktur. Yani kişisel veriler yapısı itibariyle saymakla bitip tükenmeye elverişli değildir. Fakat hukuki koruma talep edilebilecek kişisel verileri nitelikleri ve sınıflandırılmaları itibarıyla göstermek, terimin sınırlarını ve kişisel verilerin yapısal dünyasını anlamayı kolaylaştıracaktır.

Kapsamı anlamaya yardımcı diğer özelliklerin yanı sıra, kişisel verilerin üç ortak özelliği onları alelade verilerden ayırt etmektedir. Bu özellikler, ilkin bir kişinin kimliğini belirlemesi veya belirlenebilir kılması; ikincisi kişiyi toplumda yer alan diğer kişilerden ayıran niteliklerini ortaya koymaya elverişli olması ve nihayet gerçek kişiye ait olmasıdır[19]. Bu özelliklere birlikte haiz olamayan bir veri, özel hayat verisi olarak sayılma ihtimali olsa bile kişisel veri terimi kapsamı içerisinde hukuk dünyasında bir karşılık bulmayacaktır. Örneğin, bir şirketi belirlenebilir kılan ve onu diğer şirketlerden ayıran bir özelliği ya da ticari sırrı kişisel veri terimi içerisinde yer almayacaktır. Bir başka örnekte, bir gerçek kişinin fiziksel veya ruhsal özellikleri, mesleği, inanışı, cinsel eğilimleri gibi verileri somut olayda o kişiyi belirlenebilir kılmaya yetmiyor ya da toplumdaki diğer

[18] Akgül, s. 8.
[19] Y. 12. CD, 13.01.2014, E. 2013/9043 K. 2014/151, Erişim Tarihi: 5 Nisan 2019, Kazancı İçtihat Bilgi Bankası.

kişilerden ayıran bir nitelikte olmuyorsa o halde bu veriler koruma kapsamındaki kişisel veri teriminin içerisinde yer almayacaktır.

2. Kimliği belirleyen veya belirlenebilir kılan bir verinin bulunması

Kimliği belirleyen veya belirlenebilir kılan bir verinin varlığı için, ortada bir kişi olmalı, bir veri olmalı, bu veri ile bu kişiyi belirlemek mümkün olmalıdır. Üstelik belirleyici fonksiyonun doğrudan olması da gerekmediğinden, dolaylı olarak bir kişiyi tanımlaması yeterli olacaktır. Hemen belirtmek gerekir ki, doğrudan ayırt etme isimle veya başka bir doğrudan ayırt edici unsurla; dolaylı ayırt etme ise kimlik numarasına veya kişiye özgü bir karakteristik özelliğe atıf yaparak ayırt etmeyi içermektedir[20]. Bu açıdan, bir kişinin çevrim içi davranışlarının izlenmesi olan çerezler de dolaylı yoldan kişiyi işaret etmekte olduğundan kişisel verilerin korunması kapsamında yer almaktadırlar[21]. O halde, bir kişinin kullanmakta olduğu takma ad da yeterli anonimleştirmeyi sağlayamadığından ve kişiyi belirlenebilir kıldığından onun kişisel verisidir[22].

Ayrıca kişinin soy ismi gibi sadece ona ait olmayan ve yaygın bir biçimde kullanılan veriler doğrudan o kişiyi belirlenebilir kılmayacak olsa bile bu şekildeki verilerden birkaçının bir araya gelmesi halinde kişi belirlenebilir olabilecektir[23]. O halde, verinin, kullanması makul olan tüm vasıtalar kullanılarak herhangi bir kişiyi belirlenebilir kılması halinde kişisel veri olması için aranan şart sağlanmış olmaktadır[24].

3. Gerçek kişiye ait olması

Kapsam ile ilgili ikinci olarak belirtmemiz gereken, sadece gerçek kişilerin kişisel verileri olabileceğidir[25]. Tüzel kişilerin ise durumun icabına göre özel hükümlerle korunmakta olan ticari sırları yahut devlet sırları olabilecektir.

Kural her ne kadar tüzel kişilerin verilerinin kişisel verilerden sayılmaması olsa da söz konusu verilerin bir gerçek kişi ile ilişkilendirilebilmesi ve kişinin kimliğini belirliyor

[20] Bozkurt Yüksel, Armağan Ebru: Bulut Bilişimde Kişisel Verilerin Korunması, Ankara 2016, s. 101.
[21] GDPR m. 3'te çerezler, kişisel veri olarak sayılmaktadır.
[22] Sarıusta, K. 2018. *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması.* Yayınlanmamış Yüksek Lisans Tezi, Gaziantep: Gaziantep Üniversitesi, Sosyal Bilimler Enstitüsü, s. 30.
[23] Taştan, Furkan Güven: Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul 2017, s. 38.
[24] Aksoy, Hüseyin Can: Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010, s. 24.
[25] Tezimiz bağlamında en güncel hukuki metin olan GDPR m. 1'de belirtildiği üzere, yalnızca gerçek kişilerin kişisel verileri koruma altına alınmaktadır.

olması da mümkündür. Böyle hallerde söz konusu verilerin, kişiyi tanımlamaya elverdiği ölçüde kişisel veriden sayılması gerekir ki bu durumda asıl korunan gerçek kişiye ilişkin kişisel verilerdir[26]. Üstelik bu verilerin veri sahiplerini doğrudan ya da dolaylı yoldan belirliyor olmalarının bir önemi de bulunmamaktadır[27]. Dolayısıyla, kişisel verilerin öznesi her hâlükârda gerçek kişi olacaktır da denebilir.

4. Veri sınıfları

Kişisel veri teriminin kapsamını belirlemeyi kolaylaştıran üçüncü yol ise kişisel veri sınıflandırmasıdır. Birinci sınıflandırma metodu doğrultusunda kişisel veriler, veri türlerine göre üst başlıklarda toplanabilmektedir. Buna göre kişisel kimlik belirleyiciler, kişisel özellikler, mali belirleyiciler, akademik özellikler, üyelik bilgileri, adli sicil bilgileri ve diğer aile üyelerine ilişkin bağları olarak ayrılabilmektedirler[28].

İkinci metot ise, daha çok hukuk kurallarının benimsediği yol olarak verilerin, genel, ve hassas nitelikli olarak ikiye ayrılmasıdır. Genel nitelikli kişisel veriler, özel bir kategorizasyona tabi tutulmayan ve kişiyi belirlenebilir kılan her türlü kişisel veriyi ifade etmektedirler. Sınırlı sayıda olmadıklarından hassas nitelikli olmayan tüm kişisel verilerin genel nitelikli kişisel veri olduğu söylenebilir.

Hassas ya da özel nitelikli olarak belirtilen kişisel veri türleri ise, KVK Kanunu m. 6(1)'de sınırlı olarak sayılmaktadır, *numerus clausus*tur. Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri hassas nitelikli kişisel veridir. Bu tür veriler, genel nitelikli kişisel verilere göre kişinin bireysel hayatının en mahrem kısımlarına aittir. Bu yüzden açıklandığı takdirde ilgili aleyhine başta ayrımcılık olmak üzere zararlı etkileri olabilecek nitelikteki verilerdir[29]. Dolayısıyla yeterli derecede korunmaları gerektiği düşünülerek hukuki düzenlemelerde daha fazla önlem

[26] Başalp, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s. 35; Dülger, 2019, s. 199.
[27] Şimşek, Oğuz: Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008, s. 122.
[28] Turan, Metin: Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Ankara 2017, s. 8.
[29] Höfelmann, Elke, Das Grundrecht auf informationelle Selbstbestimmung anhand der Ausgestaltung des Datenschutzrechts und der Grundrechtsnormen der Landesverfassungen, Frankfurt am Main 1997, s. 55 (ŞİMŞEK, s. 121'den naklen)

alınmaktadır[30]. İşlenmeleri kural olarak herkes için yasak olan hassas verileri tespit edebilmek adına üç başlık altında toplayabilmek mümkündür. Bunlar, ırk ve etnik unsurlara dayalı veriler; düşünce özgürlüğü kapsamında şekillenen veriler; geniş anlamıyla sağlık verileridir[31].

Genel ve hassas nitelikli kişisel veriler ayırımının yanı sıra doktrinde bir de anonim veriler yeni bir tür olarak dile getirilmeye başlanmıştır. Bu tarz veriler, kaynağı belli olmayan veya belirli bir kişi ile ilişkilendirilemeyen bir çeşit kitlesel bilgiler olarak ifade edilmektedirler[32]. O halde anonim veriler, hem hali hazırda kimseyi tanımlamayan veriler hem de anonimleştirilmiş hale getirilmiş veriler olarak tanımlanabilir. Özellikle, sağlık hizmeti bilgilerinin gizli tutulması gerekliliği çerçevesinde gizliliğin ihlalini en aza indiren yöntemdir[33]. Veri maskeleme, takma isim kullanma, kümeleme, bantlama bazı temel anonimleştirme tekniklerine örnektir[34].

5. Özel hayat verisi ve kişisel verilerin farklı yönleriyle birbirinde ayrılması

Kişiler veriler teriminin mahiyetini ortaya koyabilmek için bu noktaların dışında son olarak özel hayat verisi ile kişisel verilerin farklılaşma eğiliminden de bahsetmek gerekmektedir. Günümüzdeki hukuk kurallarına bakıldığında kişisel veriler, özel hayat verilerinin bir alt kümesi şeklinde olan fakat özel hayat verilerine göre getirilen özel hükümler sayesinde daha fazla korunan veriler konumundadırlar. Hali hazırdaki süreç içerisinde özel hayat verilerinden tam olarak ayrılamamış olması sebebiyle, kişisel

[30] Örneğin, KVK Kanunu m. 5 ve 6'dan anlaşıldığı üzere, kişinin açık rızası olmaksızın işlenebilecek özel nitelikli kişisel verilerin kapsamı, genel nitelikli kişisel verilere göre daha dardır. Yine, Türk Ceza Kanunu m. 135(2)'de, kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması cezayı ağırlaştıran nitelikli hal olarak düzenlenmiştir. Sayılan hususlara daha ağır yaptırım uygulanmasının sebebi suç konusu verilerin özel nitelikli veri oluşlarıdır.

[31] Tinnefeld Marie-Therese/Ehmann, Eugen/Gerling, W. Rainer: Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheir in europaeischer Sicht, 4. Auflage, München, Wien 2005, s. 277, (ÖZDEMİR, Hayrunnisa: Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009, s. 126'dan naklen)

[32] Bayraktar, Köksal (Akyürek, Güçlü/Keskin Kiziroğlu, Serap/Yıldız, Ali Kemal/Zafer, Hamide/Aksoy Retornaz, Eylem/Evik, Ali Hakan/Sınar, Hasan/Altunç, Sinan/Aytekin İnceoğlu, Asuman/Erman, Barış/Eroğlu Erman, Fulya): Özel Ceza Hukuku - Cilt III - Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar (TCK m. 106-140), İstanbul 2018, s. 641.

[33] Yılmaz, Sabire Sanem: Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Ankara 2017, s. 46.

[34] Keser Berber, Leyla: Çevrimiçi Davranışsal Reklamcılık(Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014, s. 56.

verilerin özel hayat verilerinden büsbütün ayrı olduğu kanun koyucu açısından benimsenmemektedir.

Bununla birlikte kişisel verilerin korunmasının kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olduğu da ifade edilmektedir[35]. Yargıtay bu konuda verdiği bir kararda, özel hayat verisinin bir üst kavram olarak kişisel verilerden içerik bakımından farklılaştığını belirtmiştir. Buna göre kişisel veriler kişiyi belirlenebilir kılan veriler iken, özel hayat verileri*, "herkesin bilmediği veya bilmemesi gereken, istenildiğinde başka kişilere açıklanabilen, tamamen kişiye özel hayat olayları ve bilgilerin tamamını ifade eder"*[36]. Bu açıdan örneğin bir kişinin fotoğrafı, geniş kapsamlı ele alındığında o kişinin özel hayat verisi olarak düşünülebilir. Fakat bir gerçek kişiyi diğerlerinden ayıran ve belirlenebilir kılan verileri, kişisel veriyi ifade etmekte olduğundan özel hayat verilerinden daha dar kapsamda olan kişisel veri sınıfındadır. Fakat aynı fotoğrafta kişinin belirlenmesini engelleyen bir maske veya kamuflaj varsa o halde söz konusu fotoğraf kişisel veri sınıfına girmeyecek, özel hayat verisi kapsamında değerlendirilebilecektir. Bir başka örnek olarak ünlü bir şarkıcının arabasının markası verilebilir. Eğer arabasının markası üzerinden o şarkıcının kim olduğunu belirlenebilir kılınabiliyorsa o halde kişisel veri; aksi halde özel hayat verisi olacaktır.

Uygulamadaki pratik gerekçelerle gün geçtikçe özel hayat verilerinden ayrı, münhasır bir alana kaymakta olan kişisel verilerin, farklı bir bütünlük oluşturmakta olması sebebiyle özel hayat verisi-kişisel veri ayırımının hukuk dünyasında ilerleyen yıllarda daha fazla gerçekleşeceğini düşünmekteyiz. Bunu destekler mahiyetteki bir görüş de kişisel verilerin korunmasına farklı bir yaklaşım getirerek, özel ve aile yaşamına saygı hakkının statik bir hak olması dolayısıyla çoğu kez negatif koruma gerektiren bir hak olduğunu fakat kişisel verilerin korunmasının dinamik koruma gerektiren bir hak olarak pozitif hak özelliği gösterdiğini belirtmektedir[37].

6. Verinin korunmaya değer olması ya da olmaması

Öte yandan, verinin kişisel veri kapsamında olmaktan çıkmayacağı fakat korunmaya değer olmayacağı bir ayrımı da ortaya koymak gerekir. Ayrıma yol açan bu durum, veri

[35] Küzeci, s. 69.
[36] Y. 14. CD, 8.12.2014, E. 2013/5239 K. 2014/13911, Kazancı İçtihat Bilgi Bankası.
[37] Küzeci, s. 74.

sahibinin kişisel verilerini ilgisiz üçüncü kişilerin bilgisine sunarak alenileştirmesi halidir. Kişinin kendi verilerini alenileştirmiş olması halinde o verilerin kişisel verilerin korunması kapsamında yer alamayacağı sebebiyle kişisel veri olarak nitelenemeyeceği düşünülebilir.

Bizim düşüncemize göre, kişisel verinin alenileştirilmiş olması onu kişisel veri olmaktan çıkartmaz. Çünkü veri sahibinin kendi rızasıyla kişisel verilerini alenileştirmesi halinde alenileştirilen veriler de kişisel veri özelliğini taşımağa devam edecektir. Fakat artık üçüncü kişilere karşı korunmaya değer olmayacak ve kişisel verilerin korunması hükümlerindeki güvencelere haiz olamayacaktır. Bunun temel gerekçesi ise, verilerin korunması hükümlerinde kişinin iradesinin esas alınıyor oluşudur.

Dolayısıyla, bir veriyi kişisel veri yapan unsurlar ile hangi verilerin koruma kapsamında olacağı birbirinden bağımsız olup farklı konulardır. Bu yüzden koruma kapsamında olmayan verilerde yapısı itibariyle kişisel veri olabileceği unutulmamalıdır.

7. Sır ile kişisel verinin karşılaştırılması

a) Genel olarak

Kişisel verilerin kapsamını belirlemede, kişisel verinin sır kavramından farklarını ortaya koymak önemli taşımaktadır. Bir kişiyi belirlenebilir kılan her veri kişisel veri olarak tanımlanmaktadır. Sır kavramı ise kişinin kendisine veya bir başkasına ait sınırlandırılmış sayıda kişilerin bilebileceği ve mahrem kalması gereken bir bilgiyi işaret etmektedir.

Arapça kökenli bir isim olan sır, TDK'ya göre, *varlığı veya bazı yönleri açığa vurulmak istenmeyen, gizli kalan, gizli tutulan şey* anlamına gelmektedir[38].

Mevzuatta kişisel verinin tanımı birçok yerde yapılıyor olmasına rağmen sırrın tanımı yapılmamakta, yalnızca ticari sır ve devlet sırrının tanımı düzenlemelerde kendisine yer bulmaktadır. Doktrinde ise sır, işitmek, görmek veya hissetmek suretiyle öğrenilen ve hem maddi varlığa sahip olmayan hem de aleni olmayan bir şey olarak tanımlanmaktadır[39].

[38] Türk Dil Kurumu Sözlükleri, 2019. "Sır" Erişim Tarihi: Ağustos 2019 https://sozluk.gov.tr/?kelime=sir.
[39] Erem, Faruk: "Ceza Hukukunda Meslek Sırrı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, 1, Ankara 1943, s. 36.

O halde sırrın yapısal özelliklerinden biri soyut olması yani maddi âlemde sınırlandırılmış olmaması iken diğer özelliği aleni olmaması yani herkesçe bilinmeyen yahut bilinebilir düzeyde olmamasıdır.

Aynı zamanda, sırrın objektif olarak sır olması gerekmektedir. Aksi halde sır gibi saklanan fakat objektif olarak bakıldığında herkes tarafından bilinebilecek olan verilerin sır diye saklanıyor olması onları koruma kapsamında yer alması gereken veriler sınıfına sokmayacaktır.

b) Sır türleri

Sırrın kapsamını belirleme de çeşitli türlerinin olduğunu belirtmek gerekmektedir. Sır, kişisel, mesleki, ticari ve devlet sırrı olmak üzere dört çeşittir.

Kişisel sır, kişinin kendisi ile ilgili olup başkası ile paylaştığı sırdır. Bu sır türü en geniş kapsamlı tür olmakla birlikte diğer sır türlerinin kapsamına girmeyen sırlar da bu tür kapsamında yer almaktadır.

Ticari sır, TTK'da yer verilen sır saklama yükümlülüğü çerçevesinde işletme sırlarını öğrenen kişilerin dışarıya izinsiz olarak açmamasını ifade etmektedir[40]. Ticari sırlar, gerçek kişilere veya işletmenin tüzel kişiliğine ait olabilmektedir.

Mesleki sır, meslek ilişkisi sebebiyle öğrenilen sırrı ifade eder. Avukatın[41], hekimin[42] vs. diğer mesleklerin gördükleri iş sebebiyle diğer kişi/kurumlarla ilgili öğrenmiş oldukları gizli bilgiler bu tür içerisinde yer almaktadır. Bu bağlamda, TBK'da yer alan hizmet sözleşmesi çerçevesinde işçinin özen ve sadakat borcunun bir gereği olarak sır saklama yükümlülüğü bulunmaktadır[43].

Devlet sırrı, devlete zarar verebilecek devletle ilgili gizli bilgiyi ifade etmektedir[44]. Bu tarz verilerin her ne kadar mahrem kalması gereken verilerden olması gerekli olsa da

[40] Örnek olarak TTK m. 404, 441, 527'a bakılabilir.
[41] Avukatlık Kanunu m. 36.
[42] Hekimlik Meslek Etiği Kuralları m. 9.
[43] TBK m. 396.
[44] Devlet sırrı niteliğindeki bilgilerle ilgili tanıklık maddesi CMK m. 47'de düzenlenmektedir:
"(1) Bir suç olgusuna ilişkin bilgiler, Devlet sırrı olarak mahkemeye karşı gizli tutulamaz. Açıklanması, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek nitelikteki bilgiler, Devlet sırrı sayılır…"

kişisel verilerden farklı olduğunu belirtmek gerekir. Çünkü kişisel veriler sadece gerçek kişiye ait olan verileri ifade etmektedir.

Bir gerçek kişiyi tanımlanabilir kılan sırların da kural olarak kişisel verilerin korunması kapsamında olması gerekmektedir. Bu noktada kişisel veri ile sırrın aynı unsurları ifade etmekte oldukları düşünülebilir. Gerçek kişilere ait kişisel, ticari, mesleki ya da devlet sırrı niteliğindeki kişisel verilerin, özel hükümlerde daha fazla bir koruma sağlamadığı takdirde kişisel verilerin korunması kuralları çerçevesinde korumaya sahip olması gerekmektedir. Bunun sebebi, söz konusu verilerin gerçek kişilere ait olmasının yanı sıra, hukuki metinlerde koruma kapsamı dışında yer alan kişisel veriler arasında da yer almamakta olmasıdır. Ayrıca kişilerin iradesinin bu verileri alenileştirme yönünde olmayışı ve mahrem kalması gereken verilerden oluşu diğer gerekçelerdir.

c) Sır ile kişisel verinin benzerlikleri ve farklılıkları

Kişisel veri ve sır, nitelikleri açısından birbirine benzemekle birlikte kapsam ve hukuki korumaya sahip olması açısından farklılaşmaktadır.

Öncelikle benzerlikleri açısından belirtmek gerekir ki, her ikisinde de verilerin kural olarak gizli tutulmak istendiği düşüncesi hâkimdir. Bu yüzden her iki tür veri de korunmaya muhtaçtır. Yine bu özellikleri sebebiyle bazen iç içe geçebilmekte ve karışıklık söz konusu olmaktadır. Gizlilik için verinin gizli kalıp, saklanması asıldır.

Farklılıkları ise, kapsam açısından bakıldığında, sırrın kişisel verilere göre çok daha geniş kapsamlı olmasıdır. Bir kişiyi belirlenebilir kılan her şey kişisel veri iken, sırlar bu verilerin dışındaki özel hayat verileri gibi verileri de kapsayabilmektedir. Aynı zamanda hukuk düzleminde korunması açısından da sırrın kişisel verilerden daha kapsamlı olacağı savunulabilir. Örneğin, hastası ile ilgili sır niteliğindeki verilerinin doktorunun yahut şüpheli ile ilgili verilerin kolluk ya da savcının hafızasında yer alması, kişisel verilerin korunması açısından değerlendirmeye konu olmamaktadır.

Bu tarz verilerin kişisel veri kapsamında korunabilmesi için bir kişiyi belirlenebilir kılmasının yanı sıra çeşitli vasıtalarla dış dünyaya aktarılması gerekmektedir. Çünkü bir kişinin hafızasında yer alan hususların ne olduğu dışarıdan bir müdahale ile kanıtlanamaz, ölçülemez. Bu verilerin korunması meslek sırrı gibi çeşitli düzenlemelerle sağlanmakta olup sır olarak tutulabilecek şeylerin kişisel veri olup olmaması önem taşımamaktadır.

Dolayısıyla sırlar, kişisel verilerin korunması alanının dışına çıkmakta olup, kişisel verilerden bu yönüyle daha kapsamlı bir alan oluşturmaktadırlar.

Bizim düşüncemize göre, kişilere ait ve onları belirlenebilir kılan verileri içeren sırların kişisel veri niteliğinde olacağını, bu nedenle de kural olarak kişisel verilerin korunmasından yararlanıyor olması gerektiğini düşünmekteyiz. O halde, her ne kadar kişisel veri ile sır aynı şeyi ifade etmiyor olsa bile aynı koruma potası altında buluşabilecektir. Bu yüzden bir kişinin kişisel verilerini ihtiva eden sırlar kişisel verilerin korunması güvencesi altındadırlar. Ayrıca bir kişinin bir sırrı bildiği bilgisi de o kişiyi "o sırrı bilen kişi" olarak nitelemekte olduğundan, bu bilgi o kişinin kişisel verisidir. Bu açıdan, kişisel sır olan hususlar, kişisel verilerde olduğu gibi, kural olarak aynı koruma kapsamında olmalı ve bu konuda özel kanun olan KVK Kanunu güvencelerinden yararlanmalıdırlar. Kural olarak kişisel veri, meslek sırrı, ticari sır ve devlet sırrı kapsamına girmemekle birlikte kişisel sır alanı içerisinde yer alan verilere yönelik açıklayıcı ve koruyucu hukuki düzenlemelerin yapılmasının verilerin korunmasına katkı sağlayacaktır.

D. Hak Boyutuyla Kişisel Veriler

1. Genel olarak

Kişiler verilerin bu kısımda hak boyutu yönüyle ele alınmasındaki amaç, son yıllarda kişiler verilerin elektronik veri sistemleriyle gittikçe artan bir düzeyde işlenmesi sebebiyle kaçınılmaz bir ihtiyaç haline gelen verilerin korunması hususunun hem insan hakları bağlamında korunacak hukuki değerini ortaya çıkarmak hem de temel hukuki-felsefi dayanaklarını tanıtıcı düzeyde göstermekten ibarettir. Bu bağlamda, kişisel verilerin kişilik hakkına, kendi kaderini tayin etme hakkına, haberleşme özgürlüğüne ve özel hayatın gizliliği hakkına dayanan kökleri incelenmektedir.

Hiç şüphesiz zikredilen bu hakların hukuk kurallarınca korunmasıyla kişisel veriler de korunmaktadır. Karşılıklı ilişkinin göstergesi olarak kişisel verilerin korunmasıyla da zikredilen bu haklar korunmaktadır[45]. Kişisel verilerin korunmasını hakkına yönelik karşılıklı güvence sağlayan diğer temel hak ve özgürlükleri de burada zikretmek gerekir.

[45] GDPR'ın konu ve hedefler başlıklı birinci maddesinde de belirtildiği üzere, kişisel verilerin korunması hakkı dışında, bağlantılı olan diğer temel hak ve hürriyetler de koruma kapsamına alınmaktadır.

Bunlar: inanç özgürlüğü, bilgi edinme özgürlüğü, düşünceyi açıklama özgürlüğü, toplantı özgürlüğü ve haberleşme özgürlüğüdür. Özel hukuk doktrini açısından kişisel verilerin hukuki niteliğini mülkiyet ve fikri mülkiyet hakkına bağlayan görüşler de bulunmaktadır[46].

Ayrıca koruma sürecini daha iyi anlamak adına hukuk coğrafyası açıdan bakıldığında Kıta Avrupası ekolünde hak ve sosyal değer merkezli bir yaklaşım mevcut olduğu görülmektedir Anglo-Amerikan hukuk sistemine dâhil ülkelerde ise, kişisel verilerin korunması özel hayatın gizliliği ile sınırlandırılmakta ve bu hali ekonomik ve teknolojik yaklaşım üzerinden mütalaa edilmektedir[47].

2. Kişilik hakkının bir uzantısı olarak kişisel veriler

Kişisel verilerin insan hakları nazarındaki dayanaklarına bakıldığında ilkin kişilik hakkı ile doğal bir bağlantısının olduğu açıkça öne çıkmaktadır. Bu bağlantıyı ortaya koymak adına öncelikle kişi ve kişilik hakkı kavramlarını açıklamak gerekmektedir.

Bir hukuki terim olarak kişi, sağ ve tam doğumla başlayıp ölümle sona erecek süre zarfı içerisinde hak ve borçlara sahip olabilen insana denir (TMK m. 28). Dolayısıyla kişi doğmadan ya da öldükten sonra onun hakkında kişilik hakkından bahsedebilmek kural olarak mümkün değildir[48]. Ceninin durumuna bakıldığında ise, cenin hak ehliyetini sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde etmekte olduğundan(TMK m. 28/2), ceninin tam ve sağ doğması halinde kişisel veri sahibi olabileceğini kabul etmek gerekmektedir. Bu bağlamda ceninin DNA'sı gibi özellikleri onun kişisel verisi olabilecektir.

Cenin olmadan önce embriyonun verileri, annenin kendi vücudu olması sebebiyle doğrudan, babanın ise dolaylı olarak kişisel verisi olacaktır. Çünkü TMK hem embriyo olmayı kişi bahsi içerisinde düzenlememekte hem de hak sahibi olabilmeyi cenin(fetus) olduktan sonra başlatmaktadır. Bu yüzden embriyonun DNA'sının, embriyonun kişisel verisi olup olmayacağı sorgulanmaya açıktır. Kanun koyucu haklarla ilgili cenin olmaya dayalı bir sistematiği kabul ettiğinden embriyonun kişisel verisinin olması kanun

[46] Uncular, Selen: İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara 2014, s. 21-23; Köse Aysun, Melike: Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135), Ankara 2018, s. 37-39.
[47] Aşıkoğlu, Şehriban İpek: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul 2018, s. 25.
[48] Kişi öldükten sonra fikri mülkiyet hukukunca korunan haklarına ilişkin istisna hükümler saklıdır.

açısından mümkün değildir. Fakat kanun, kişiliğin başlangıcını embriyoya dayandıracak olsaydı embriyonun da DNA'sı başta olmak üzere kişisel verisinin olabileceğini de kabul etmek gerekirdi diye düşünmekteyiz. Sonuç olarak embriyo örneğinde olduğu gibi sadece hukuk kuralları kapsamında kişi olarak tanınmakta olanlar, kişilik terimi içerisinde yer almakta olacaklarını belirtmek gerekmektedir.

Öte yandan, tüzel kişiler de hukuk dünyasında bir kişi olarak tanımlanmaktadır. Hatta tüzel kişiler de aynen gerçek kişilerde olduğu gibi hak ve fiil ehliyetine sahiptirler. Fakat kişisel verilerin korunmasındaki çerçeve bir insanın haklarının korunması olduğundan tüzel kişilerin kendisine ait olarak kişisel verisinin olması söz konusu olamaz. Sahip olduğu veriler özel hükümler uyarınca ticari sır vs. olarak adlandırılabilir olsa da kişisel veri sınıfına isabetli olarak dâhil edilmemektedirler.

Hukuki anlamda kişi teriminin ne olduğunu ortaya koyabilmenin aksine kişilik haklarını belirlemek oldukça güçtür. Çünkü Türk hukukunda kişilik haklarının hangi haklardan ibaret olduğu sayılmamaktadır. Genellikle bireyin kişiliğinin korunmasının söz konusu olduğu durumlarda gündem gelen kişilik hakkı ile ilgili, TMK m. 23-27'de kişiliğin korunması başlığı altında düzenlenen hükümlerden hareketle neyin kişilik hakkı dairesinde yer alabileceğine ilişkin çıkarımlar yapılabilmektedir. Fakat ne TMK'da ne de diğer pozitif hukuk kurallarında kişilik hakkının bir tanımı bulunmamaktadır. Doktrinde ise bu konuyla ilgili muhtelif tanımlar bulunmaktadır. Kişilik hakları, *Centel/Zafer/Çakmut'*a göre, kişiye bağlı, vazgeçilemeyen, devredilemeyen, yasaya ve ahlak kurallarına aykırı biçimde sınırlandırılamayan, parayla ölçülemeyen haklardır[49]. *Ayan/Ayan*'a göre, kişinin, kişisel değerleri üzerinde sahip olduğu mutlak ve tekel kurduğu haktır[50]. *Velidedeoğlu*'na göre, şahsın bedeni, manevi ve fikri varlığı üzerindeki bütün haklarını ifade eden haktır[51]. *Arpacı*'ya göre, hak ve fiil ehliyeti, hayatı, sağlığı, bedeni bütünlüğü, şeref ve haysiyeti vb. diğer değerleri üzerindeki hakları ifade etmektedir[52]. *Hatemi/Kalkan Oğuztürk*'e göre, kişilik değerlerini koruma kapsamına alan temel kişi varlığı hakkıdır[53]. *Öztan*'a göre, kişilik hakları kişiye kişi olması nedeniyle

[49] Centel, Nur/Zafer, Hamide/Çakmut, Özlem: Kişilere Karşı İşlenen Suçlar, İstanbul 2017, s. 126.
[50] Ayan, Mehmet/Ayan, Nurşen: Kişiler Hukuku, Konya 2015, s. 65.
[51] Velidedeoğlu, Hıfzı Veldet: Türk Medeni Hukuku, İstanbul 1963, s. 174.
[52] Arpacı, Abdülkadir: Kişiler Hukuku (Gerçek Kişiler), İstanbul 2000, s. 103.
[53] Hatemi, Hüseyin/Kalkan Oğuztürk, Burcu: Kişiler Hukuku (Gerçek Kişiler-Tüzel Kişiler), İstanbul 2014, s. 57.

tanınan hakları ifade etmektedir[54]. *Oğuzman/Seliçi/Oktay-Özdemir*'e göre ise, kişilik, insanın insan olması dolayısıyla ayrılmaz bir biçimde sahip olduğu, para ile ölçülemeyen, devredilemeyen, kural olarak mirasçıya geçmeyen mutlak hakları içermektedir[55]. Yargıtay'a göre ise, "*Kişinin doğumla kazandığı bağımsız varlığını ve bütünlüğünü oluşturan; hayat, beden ve ruh tamlığı, vicdan, din, düşünce ve çalışma özgürlüğü, onuru, ismi, resmi, sırları ile aile bütünlüğü, sosyal ve duygusal değerlerinin tümü* olarak tanımlanmaktadır"[56]. Ayrıca kişilik hakkının kişisel veriler ile olan ilişkisi mahremiyet hakkı üzerinden de şekillenmektedir. Buna göre mahremiyet ve özel hayat, kişilerin kişilik hakkının bir görünümü olduğundan, kişisel verilerin korunmasıyla aynı zamanda mahremiyet hakkının korunmasına da hizmet edilmektedir[57]. O halde kişilik hakları, mutlak haklar içerisinde sınıflandırılmanın yanı sıra bireyin insan olmasından kaynaklanan, üzerinde sahip olduğu, objektif olarak maddi/manevi kişisel değer ifade edebilecek unsurlar olarak ifade edilebilirler. İnsanın insan olması dolayısıyla sahip olduğu haklar olarak ifade edilen insan hakları tanımıyla da bir bakıma eş değerdir.

Kişilik hakkının konusu objektif olarak kabul edilebilecek olan kişisel değerlerdir. Kişisel değerler ise en temelde kişinin maddi(ad, resim, vücut bütünlüğü vb.) ve manevi bütünlüğü(şeref, haysiyet vb.) yönünden ikiye ayrılmakla birlikte bunların içindekileri sayarak bitirebilmek mümkün değildir. Bir kişiyi belirlenebilir kılan kişisel veriler, en içkin kişisel değerler olarak kişilik hakkının doğrudan konusunu oluşturmaktadır. Çünkü kişinin vücudunun özellikleri, adı, resmi, sesi gibi özellikleri hem o kişiyi belirlenebilir kılmakta, hem o kişinin kişiliğinden ayrılmaz durumda bulunmakta hem de kişinin kişisel değerlerini oluşturması sebebiyle kişilik hakkının konusunu oluşturmaktadır. Kişilik hakkının kişiye sıkı sıkıya bağlı mutlak bir hak olması nedeniyle, hem herkese karşı ileri sürülebilmekte hem de devredilmesi, vazgeçilmesi ve zaman aşımına uğraması mümkün değildir[58].

Öte yandan, kişisel veriler, kişilik hakkıyla eş değer değildir. Şöyle ki, kişisel veri olan her şey kişilik hakkının konusunu oluşturabilecekken, kişilik hakkının konusunu

[54] Öztan, Bilge: Medeni Hukukun Temel Kavramları, Ankara 2014, s. 75.
[55] Oğuzman, M. Kemal/Seliçi, Özer/Oktay-Özdemir, Saibe: Kişiler Hukuku (Gerçek ve Tüzel Kişiler), İstanbul 2015, s. 154.
[56] Y. 4. HD, 10.4.2008, E. 2007/9966 K. 2008/5096, Erişim Tarihi: 1 Mayıs 2019, Kazancı İçtihat Bilgi Bankası.
[57] Sert, Şeyma: Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara 2019, s. 69.
[58] Uncular, s. 25.

oluşturan her unsur kişisel veri değildir. Örneğin, bir kişinin vücut bütünlüğüne yönelik fiili müdahaleyle işlenen kasten yaralama suçu ile kişilik hakkı ihlal edilmiş olsa bile kişisel veri ihlali söz konusu değildir. Fakat TCK'da konusunu kişisel verilerin oluşturduğu suç düzenlemeleri ile ilgili bir suç (örneğin kişisel verilerin kaydedilmesi suçu) işlendiğinde, kişiyi belirlenebilir kılan veriler hukuka aykırı olarak işlenmiş olacağından kişilik hakkı da ihlal edilmiş olacaktır. Bu halde, somut vakaya göre özel hukuk hükümlerine göre tazminat davası açılması da mümkündür. Sonuç olarak kişisel değerlerin kişisel verilerden daha kapsamlı olması kişisel verileri kişilik hakkının bir uzantısı konumuna indirgemektedir.

3. Kendi kaderini tayin etme hakkı açısından kişisel veriler

Birleşmiş Milletler Uluslararası Medeni ve Siyasi Haklar Sözleşmesi ile Birleşmiş Milletler Uluslararası İktisadi, Sosyal ve Kültürel Haklar Sözleşmesi'nin (İkiz Yasaların) ortak birinci maddesinde yer alan halkların kendi kaderini tayin etme hakkı, bütün halkların, kendi siyasal statülerini özgürce belirlemeleri ve ekonomik, sosyal ve kültürel gelişmelerini özgürce gerçekleştirmeleri olarak tanımlanmaktadır.

Öte yandan sadece halkların değil, bireylerin de kendi kaderini tayin etmek hakkı bulunmaktadır. Şöyle ki, tüm temel hak ve hürriyetlerin dayanağı olan ve soyut bir şekilde tasvir edilen insan onurunun gerçekleştirilmesi için en temel hak olarak özgürlük kurgulanmıştır. Diğer hak ve özgürlüklerin hayata geçirilebilmesi için bireyin özgür olması merkezi öneme sahiptir. Özgür kişi, temel hak ve hürriyetlere teoride *de jure* olarak sahip olduğu gibi pratikte de *de facto* olarak sahip olan kişidir. Temel hak ve hürriyetlere sahip olma ifadesi gerçekliğini bireyin bu haklar üzerinde serbestçe tasarruf edebiliyor oluşundan alır. İşte bireyin kendisine bırakılan bu tasarruf, pratikte somutlaşarak hak düzeyinde kendi kaderini tayin etme hakkı olarak ifade edilir.

Bu hak, kişinin dışarıdan bağımsız yani otonom olarak kişiliğini geliştirerek soyut bir biçimde tasavvur edilen insan haklarını somutlaştırarak etkin bir biçimde kullanabilmesi için temel önceliktir. Devlet bu gaye doğrultusunda kişinin kendisini gerçekleştirmesinde bir araç konumundadır. Zaten bu yüzden Anayasa m. 17'de herkesin, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahip olduğu düzenlenmiştir. Burada söz edilen gelişimden kasıt, kişinin diğer temel hak ve hürriyetlere sahip olarak yaşayabilmesini ve bu hakları üzerinde serbestçe tasarrufta bulunabilmesini ifade eder.

Kişisel verilerin hak boyutunun bağlamının anlaşılmasında önemli bir yer tutan kendi kaderini tayin etme hakkı, kişiliğin geliştirilmesi ortamının sağlanması amacıyla kişisel verilere saygı duyulmasını ve korunmasını talep etme imkânına kaynaklık etmektedir. Bu açıdan örneğin şirket mail hesabı kullanılarak gerçekleştirilen mail etkileşimi gibi mesleki hayat çerçevesinde yürütülen faaliyetlerin kişinin çevresiyle ilişkilerini geliştirerek sosyal kimliğini şekillendirmesi üzerinde etkilerinin olabileceği unutmamak gerekir[59].

Dolayısıyla, kişinin verilerine müdahale edilmemesi sayesinde kişi, temel hak ve özgürlüklerini gerçekleştirebileceği özerk alanı elde etmektedir. Kişisel verilerin korunmasına yönelik güvencelerin olmadığı düşünüldüğünde ise kişinin başta ifade özgürlüğü ve haberleşme özgürlüğü olmak üzere diğer temel hak ve hürriyetlerini fişlenme tehlikesi sebebiyle kullanmaktan kaçınmasına yol açacaktır. Şöyle ki kişisel verisi işlenen kişinin hareket serbestisi kısıtlanacak ve kişiliğini geliştirme, geleceğini şekillendirme imkânı dahi elinden alınacaktır[60]. Bu yüzden, veri bankalarında kişilerin haberi dahi olmadan haklarındaki bilgilerin toplanması ve depolanması kişinin kendi kaderini tayin etme hakkını ihlal edecektir[61]. Keza, kişinin sürekli olarak izlenmesi, denetim altında bulunması, veri ve sırlarının rızası olmadan alenileştirilmesi kişi hakkındaki duygu ve düşüncelerin değişmesini de yol açabilecektir[62]. Bu durumda, devlete düşen pozitif yükümlülük, her kişiye kendi kaderini tayin hakkının icra etmesi için bu tehlikelerden bağımsız ve özgürce yaşayabileceği bir alanının oluşturulmasını sağlamaktır.

Sonuç olarak, bir yandan bir üst hak olarak düşünülebilecek kendi kaderini tayin etme hakkının sonucu olarak kişisel veriler alanı oluşmakta; diğer yandan oluşturulan kişisel veriler alanı içerisinde birey kişiliğini geliştirirken farklı hak talepleri çerçevesinde kendi kaderini tayin etme hakkını kullanmaktadır. Bu durum, kişisel veriler ile kendi kaderini tayin etme hakkı arasında karşılıklı ve çok sıkı bir ilişkinin söz konusu olduğunu göstermektedir. Keza AİHM'in temyiz mercii olan Büyük Daire de, bireylerin, tarafsız ve kolektif olarak toplanıp işlenen verilerinin gizliliğini AİHS m. 8 kapsamındaki hakların yanı sıra doğası gereği kendi kaderini tayin etme hakkına da dayandırarak bu

[59] Sodan/Türkiye, Başvuru No: 18650/05, 02.02.2016, par. 37, Erişim Tarihi: 1 Mayıs 2019.
[60] Çekin, Mesut Serdar: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul 2018, s. 20.
[61] Akdağ, Hale: Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013, s. 16.
[62] Bayraktar, s. 634.

yargıya katılmaktadır[63]. Bu sıkı ilişkinin bir sonucu olarak kişinin iradesi kişisel verilerinin korunmasına temel alınmaktadır. Kendi kaderini tayin etme hakkının bir sonucu olarak kişilerin kişisel verilerin korunması hakkına sahip oldukları gibi özgür iradenin varlığı halinde verilerini ifşa etme hakları da bulunmalıdır.

4. Haberleşme özgürlüğü açısından kişisel veriler

Kişisel verilerin korunmasına öne çıkan insan haklarından biri de haberleşme özgürlüğüdür. Bilgi, düşünce ve tutumlarım ortak semboller sistemi aracılığıyla kişisel veya gruplar arasında değiş tokuş edildiği bir süreç olan haberleşme, haberleşmenin taraflar ve haberi simgeleyen mesaj olmak üzere üç öğeden oluşmaktadır[64]. Özel hayatın gizliliği hakkı ile de yakından ilişkili olan haberleşme özgürlüğü temelde bireyin hiçbir sınırlamaya tabi olmaksızın istediği kişi, zaman, mekân ve araçlarla istediği veriyi paylaşabilmesini ifade etmektedir. Çağımızda artık insanın kişiliğinin ayrılmaz bir parçası haline gelmiş olan haberleşme hürriyeti, bireyin kendini ifade edebilmesinde kilit rol oynamaktadır[65].

Anayasa Mahkemesi'nin de belirttiği üzere, özellikle bilgiye ulaşma ve bilgi ve düşüncelerin paylaşılması açısından çok etkili ve yaygın bir yöntem olan internetin modern demokrasilerde haberleşme hürriyeti ve ifade özgürlüğünün kullanılması bakımından önemi tartışmasızdır[66].

Anayasal bir hak olarak Anayasa m. 22'de yer alan haberleşme hürriyeti ile ilgili hükme göre, herkes, haberleşme hürriyetine sahiptir ve haberleşmenin gizliliği esastır. Mutlak bir hak olmadığı için devlet tarafından hakka yönelik sınırlamalar getirilebilmektedir[67]. Gizliliğin esas tutulmasındaki amaç, haberleşmenin tarafları dışındaki kimselerce, onların izni veya rızası olmaksızın anlaşılmaması ve bunlara müdahale edilememesi anlamına

[63] Oy ve Oy/Finlandiya, Başvuru No: 931/13, Büyük Daire Kararı, 27.06.2017, par. 137, Erişim Tarihi: 9 Mart 2019.
[64] Gürocak, İsmail: Türk Ceza Kanununda Haberleşmenin Gizliliğini İhlal Suçları, Ankara 2015, s. 64.
[65] Birtek, Fatih: Haberleşmenin Gizliliğini İhlal Suçları (TCK m. 132), Ankara 2013, s. 65.
[66] E. 2015/76, K. 2017/153, KT: 15.11.2017, RG. 30325, 07.02.2018, par. 21, Erişim Tarihi: 10 Nisan 2019.
[67] Getirilebilecek istisna hükümleri Anayasa m. 22'de düzenlenmektedir: "*Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.*"

gelmektedir[68]. Fakat haberleşme teknolojisindeki gelişmelerin çok hızlı gelişmesi sonucu geldiği noktada hem diğer kişilerce hem de kamu otoritelerince yapılan kişisel verilerin korunmasına yönelik ihlal edici müdahaleler oldukça kolaylaşmış ve artmıştır[69]. Özellikle, akıllı telefonların sadece özel sebeplerle değil iş için de kullandığından verilerin çalınması, sızdırılması ve ifşasına yönelik güvenlik tehditleri ve riskler sadece özel yaşamı değil iş organizasyonları için de endişe kaynağı oluşturmaktadır[70]. Kamu otoritelerin müdahalesi açısından belirtmek gerekir ki, hakka yönelik her müdahalenin kanuni bir dayanağı ve usulü olmalıdır. Örneğin, kamu otoritesinin içeriğine bakmadığını ileri sürerek kişilerin veri trafiğini keyfi olarak izleme ve bundan sonuçlar çıkarma gibi hak ve yetkisi söz konusu olamaz[71].

Kişisel verilerin haberleşme özgürlüğü ile kesiştiği noktası ise, haberleşmenin nesnesi olan bilgilerin kişisel veriler olmasıdır. Haberleşmeyi sağlayan her türlü ses ve görüntü içeren unsur bir kişiyi belirlenebilir kıldığı ölçüde kişisel veridirler. Sadece iletilen mesaj değil, başarısız kalmış haberleşme girişimine ilişkin detaylar, haberleşme trafik verileri olarak adlandırılan haberleşen tarafların isim ve adresleri, aranan yahut aranılan numaralar, gerçekleşen görüşmelerin süresi gibi hususlarda haberleşmenin gizliliği kapsamındadır[72].

Sonuç olarak, akıllı telefonlar, elektronik postalar, görüntülü iletişimler, konuşmalar gizlilik tanımayan bir süreç izlemekte, bu durum sonucunda iletişimde gizli noktalar ortadan kalkması sebebiyle, kişisel verilerin gizliliğinin hukuken koruma altına alınması iletişim özgürlüğünün de bir çeşit güvencesi olmaktadır[73]. Elbette, haberleşmenin unsurları kişisel verilerden çok daha geniş olduğundan haberleşme özgürlüğüne yönelik her müdahale kişisel verilere yönelik bir müdahale teşkil etmemektedir. Fakat haberleşme verilerinin kişisel veri olduğu durumlarda kişisel verilere yönelik bir müdahale aynı zamanda haberleşme özgürlüğüne yönelik bir müdahale teşkil etmektedir. Aynı şekilde, haberleşme özgürlüğü kapsamında haberleşme verilerinin korunması ile kişisel verilerin

[68] Özdemir, s. 85.
[69] Akgül, s. 332.
[70] Fehér-Polgár, Pál/Németh, Zsolt. 2016. "Safety Consciousness of the Mobile Phone Users." 11th IEEE International Symposium on Applied Computational Intelligence and Informatics, Timişoara, 12-14 Mayıs 2016. s. 346.
[71] Küzeci, s. 96.
[72] Birtek, s. 67.
[73] Bayraktar, s. 635.

korunması hakkı da korunuş olmaktadır. Aralarındaki işin doğası gereği var olan bu içsel ilişkiden ötürü haberleşmenin gizliliğinin sağlanması ve kişisel verilerin korunması birbirini tamamlayan insan hakları olarak düşünülebilecektir.

5. Özel hayatın gizliliği hakkı açısından kişisel veriler

a) Genel olarak

Kişisel veriler fikirsel boyutuyla kişilik haklarına ve kendi kaderini tayin etme hakkına dayanmakla birlikte Türk hukukunda ve uluslararası metinlerde daha çok özel hayatın gizliliği hakkı ve özgürlüğü içinde mütalaa edilmektedir. 6698 sayılı Kanun m. 1'de ifade edildiği üzere, kişisel verilerin işlenmesinde en başta özel hayatın gizliliğini korunması amaçlanmaktadır. Bunun en büyük sebebi, hem özel hayatın gizliliği hakkının hem de kişisel verilerin korunması hakkının nesnesi konumunda bulunan verilerin oldukça benzeşmesi ve ortak olduğunun düşünülmesidir.

AİHM ise özel hayat teriminin dar bir şekilde yorumlanmaması gerektiğine dikkat çekerek özel hayat verilerini kişisel verileri kapsamakta olduğunu belirtmektedir[74]. Dolayısıyla, kişisel verilerin korunması hakkı, temel hak ve hürriyetlerin düzenlendiği Anayasa ve uluslararası hukuk metinleri arasında henüz özel hayatın gizliliğinden bağımsız bir insan hakkı olarak düzenlenmemektedir.

Aynı zamanda özel hayatın gizliliği içerisinde özel hayat verisi-kişisel veri ayrımının yapılmaması, kişisel verilerin kavramsal düzeyde temel bir hak olarak ileri sürülebilmesini engellemekte ve özel hayatın gizliliğine bağımlı olarak gelişmeye zorlamaktadır. Bu sebeplerden ötürü, özel hayatın gizliliği hakkı ve özgürlüğü hukuk kuralları arasında kişisel verilerin korunmasına doğrudan kaynaklık etmektedir. Özel hayatın gizliliği içinde mütalaa edilmesi sebebiyle kişisel verilerin hak boyutu yönüyle özel hayatın gizliliği hakkından doğmuş olduğu da söylenebilir.

Öte yandan, Danıştay vermiş olduğu bir kararında, kişisel verilerin münhasır olarak korunması hususunun, insan hakları kavramı ve insan haklarının korunmasına paralel olarak gelişmekte olduğunu ifade etmektedir[75]. Ayrıca doktrinde kişisel verilerin artık

[74] Amann/İsviçre, Başvuru No: 27798/95, Büyük Daire Kararı, 16.02.2000, par. 65; Erişim Tarihi: 10 Nisan 2019.
[75] D. 10. D, 26.5.2015, E. 2011/7001 K. 2015/2573, Erişim Tarihi: 17 Mart 2019, Lexpera Hukuk Bilgi Sistemi.

başlı başına bir insan hakkı olarak değerlendirilmesinin gerekli olduğu da ifade edilmeye başlanmıştır[76]. Üstelik kişisel verilerin korunmasının temel hak ve hürriyetler arasında yer almasının sağlanması, bireyin kişisel verilerinin sınırsız ve hukuka aykırı olarak toplanıp, işlenmesi karşısında kişi özgürlüklerini daha çok güvence altına alacağı savunulmaktadır[77].

Kişisel verilerin hem doğası gereği hem de verilerin korunmasında istenen korumanın sağlanması adına bizim de benimsemekte olduğumuz görüşe göre kişisel verilerin Anayasa'da münhasır bir insan hakkı olarak değerlendirilmesi daha isabetli olacaktır.

Bunun bir gerekçesi, Anayasa m. 20(3)'de düzenlenen kişisel verilerin korunması hakkına yönelik getirilecek sınırlama sebepleri özel olarak belirtilmediğinden sınırlama sebeplerinin ne olduğu bilinmemekte oluşudur. Böyle özel sınırlandırma belirtilmemesi halinde hakkın içkin sınırları, kötüye kullanma yasağı ve başkalarının temel hak ve özgürlükleri ile çatışması halinde orantılı olarak sınırlandırılabileceğinden bahsedilmektedir[78]. Anayasa Mahkemesi bir kararında, bu hakkın Anayasa'da güvence altına alman temel hak ve özgürlüklerin korunması veya Anayasa'nın devlete bir görev olarak yüklediği millî güvenliğin, kamu düzeninin korunması ya da suç işlenmesinin önlenmesi gibi nedenlerle sınırlandırılabileceğini belirtmektedir[79]. Fakat sonuçta Anayasa m. 20(3)'de sınırlama sebeplerinin düzenlenmemiş oluşu uygulamada suiistimallere yol açmakta ve kamu otoriteleri hakka yönelik müdahalelerde oldukça geniş takdir yetkisi kullanmaktadırlar.

İkinci gerekçemiz ise, kişisel verilerin korunmasının Anayasa'da ayrı bir maddede düzenlenmesi ve bu hakka yönelik getirilebilecek olan meşru sınırlama sebeplerinin belirtilmesi sayesinde sınırlamanın öngörülebilirliğinin sağlanacak oluşudur. Bu gelişmeler yaşanmaktayken, Anayasa Mahkemesi kişisel verilerin korunması hakkını özel hayatın gizliliğinde bağımsız ve insan onurunun korunması ve kişiliğin serbestçe geliştirilmesi hakkının özel bir biçimi olarak değerlendirmiştir[80].

---

[76] Dülger, 2019, s. 77
[77] Küzeci, s. 69; Şimşek, s. 207.
[78] Akdağ, s. 88-90.
[79] E. 2014/122, K. 2015/123, KT: 30.12.2015, RG. 29640, 01.03.2016, par. 20, Erişim Tarihi: 17 Mart 2019.
[80] E. 2015/61, K. 2016/172, KT: 02.11.2016, RG. 29913, 09.12.2016, par. 192, Erişim Tarihi: 16 Mart 2019.

Sonuç olarak, kişisel veriler bağlamında özel hayat gizliliği hakkı Anayasa'da ilkesel olarak yer almış olsa da kanunlara bırakılan detaylandırma süreci -tezin ilerleyen kısımlarda KVK Kanunu ile ilgili eleştirilerde daha detaylı değinmekte olduğumuz üzere- henüz tamamlanmış değildir. Pozitif hukukun bıraktığı bu boşluk, günümüzde AİHM kararları, Yargıtay içtihatları ve doktrin yorumları ile doldurmaktadır. Bu doğrultuda, kişisel verilerin özel hayatın gizliliği hakkı bağlamında kapsamını incelerken sırasıyla özel hayat verisi-özel olmayan hayat verisi, üç alan teorisi, kişisel verilerin özel hayat verilerinden farklılaşan yönleri ve diğer insan haklarıyla çatıştığı yönler ortaya koyulmaya çalışılmaktadır.

b) Üç alan teorisi

İfade edilen ikili ayırımın dışında, özel hayatın sınırlarını belirlemede doktrinde Alman ekolünün etkisiyle yaygın bir biçimde üç alan teorisi benimsenmektedir[81].

Bu teoriye göre kişinin özel hayatı, merkezden çevreye doğru yayılan üç farklı alana bölünmektedir. En iç kısımda bireyin en gizli ve mahrem hayat alanı bulunmaktadır. Akabinde bireyin özel hayat alanı gelmekte ve en dışta ise kamuya açık hayat alanı yer almaktadır.

Verilerin yer alacağı alan belirlenirken kullanılan ölçütün ne olacağı hususunda doktrinde farklı görüşler bulunmaktadır. Buna göre, birinci görüş makul beklenti ölçütünü savunmaktadır[82]. İkinci görüş verinin veri sahibi tarafından üçüncü şahıslarla paylaşılma iradesini savunmaktadır[83]. Üçüncü görüş ise irade ile birlikte verinin kendisinin mahremiyet derecesini esas almaktadır[84]. Bizim görüşümüze göre, üçüncü şahıslarla paylaşma iradesi, alanlar arası ayırımı belirlemede esas alınamaz. Çünkü verinin niteliği bireyin iradesinden bağımsızdır. Ayrıca her bir bireye yönelik sübjektif mahremiyet belirlenemeyeceği için mahremiyet konusunda da objektif mahremiyet ölçüsü esas olmalı, üçlü ayırım da buna göre yapılmalıdır. Burada kişinin iradesi verinin alenileştirilmesi yönünde ise, söz konusu veri ne kadar mahrem olursa olsun, korunmaya

[81] Birtek s. 46; Akdağ, s 43; Dinç, Güney. 2009. "Uluslararası Belgeler Açısından Özel Yaşam." Türkiye Barolar Birliği Özel Yaşamın Gizliliği Paneli, Ankara, 18 Ekim 2009, s. 16; Taştan, s. 62; Sert, s. 57; Yılmaz, s. 47.
[82] Akdağ, s. 45.
[83] Zafer, Hamide: Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK m. 132-134), İstanbul 2010, s. 14.
[84] Birtek, s. 46.

değer veri olmadığı iddia edilebilmesinin yanı sıra bu durum onun mahrem veri niteliğinde olduğu gerçeğini değiştirmemelidir.

Üçlü ayırımın en dışındaki alan olarak kamusal alan, sıradan bir kişinin dışarı ile paylaşmada objektif olarak çekince göstermeyeceği verilerden oluşmaktadır. Bu alan, üçüncü kişilerce paylaşılması yaşadığı toplumca mahrem olarak telakki edilmeyen ve ayıplanmayan verilerden müteşekkildir[85]. Bu tip veriler daha çok kişinin idare ile veya üçüncü kişilere dönük iş ve eylemleri sonucu ortaya çıkmaktadır. Herkesçe bilinmesinde bir mahzur görülmediği için kural olarak hukuk düzeni tarafından korunma kapsamı dışında kalan alandır[86].

Buna karşılık, bireyin kamusal mahiyetteki verilerinin o bireyi belirli kılabilecek bir surette işlenmesi halinde hukuk düzeni buna kural olarak cevaz vermeyecektir[87]. Keza AİHM de AİHS m. 8'in kişinin kişisel gelişim hakkını ve dış dünyayla ilişkiler kurma ve geliştirme hakkını teminat altına almakta olduğundan kişilerin kamusal anlamda özel hayat kapsamına girebilecek şekilde etkileşim alanının mevcut olabileceğini belirtmektedir[88]. Bu duruma örnek olarak, çay bahçesinde oturan kişilerden bir kişiye odaklanarak onu belirlenebilir kılacak bir fotoğrafının üçüncü kişiler tarafından çekilmesi verilebilir. Bu fiilin hukuka aykırı olması bir yana, TCK m. 134'te düzenlenmekte olan özel hayatın gizliliğinin ihlali suçu da gündeme gelebilecektir.

Üçlü ayrımın ikinci aşamasında yer alan özel hayat alanı ise, bireyin kamunun bilgisine sunmadığı verilerden oluşur. Birey bu verileri sosyal hayat içerisindeki yaşamın olağan akışı içerisinde sadece yakın çevresi ile paylaşır ve çevresinin dışındaki kişilere açma isteği duymaz. Buna örnek olarak kişilerin aile hayatı gibi kapalı kapılar arkasında yaşadığı iç hayatını oluşturan unsurlar verilebilir[89]. Kişinin üçüncü kişilerce bilinmeyen meslek hayatı, meslek sırları[90] ve hatta kullandıkları IP adresleri bile bu kısımda yer almaktadır. Bu alanın vurgulanması gereken yönü, ilgili kişisel verinin özel hayat kapsamı içerisinde kalması gerekecek düzeyde diğer kişilerle bir etkileşim alanı sağlayan

[85] Helvacı, Serap: Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul 2001, s. 62.
[86] Şen, Ersan: Özel Hayatın Gizliliği ve Korunması, İstanbul 1996, s. 213.
[87] Birtek, s. 47.
[88] Uzun/Almanya, Başvuru No: 35623/05, 02.09.2010, par. 43, Erişim Tarihi: 16 Mart 2019.
[89] Özbek, Veli Özer/Kanbur, Mehmet Nihat/Doğan, Koray/Bacaksız Pınar/Tepe, İlker: Türk Ceza Hukuku Genel Hükümler, Ankara 2018, s. 537.
[90] Akipek, Jale/Akıntürk, Turgut/Ateş, Derya: "Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, İstanbul 2018, s. 390.

özelliğe sahip olarak bireyle ilişkilendirilmesinin mümkün olmasıdır[91]. Bireyin bu kısımdaki verilerinin koruma beklentisi altında olması söz konusu koruma mutlak olsun ya da olmasın AİHM tarafından makul görülmektedir[92].

Dolayısıyla, bireyin yakın çevresi ile paylaştığı verilerin veri sahibinin rızası dışında üçüncü kişilerle paylaşılmaması gerekir. Keza kişinin iç dünyasını temsil eden bu verilere, kişinin özgürlüğüne saygının bir gereği olarak bu şekilde müdahale edilmemesi gerekmektedir. Çünkü bu kısımdaki verilerin hangi kitle ile paylaşılacağı hususunda veri sahibinin iradesi aksi yönde olmadığı müddetçe sadece yakın çevresiyle paylaşılması yönünde olacaktır. Hatta bizim görüşümüze göre, kişinin rızası yoksa birlikte yaşamakta olduğu kişilerin bile bu kısımdaki verileri öğrenmemesi gerekir. İş korunma kısmına geldiğinde bireyin iradesi esas olduğundan burada objektif irade tartışmasına girmeye de gerek bulunmamaktadır.

Son olarak, üçlü ayrımın çekirdek kısmını ifade eden kişinin gizli hayat alanı, bir kişinin hiç kimseyle paylaşmadığı kişisel sırlarını ifade etmektedir. Kişinin bu sırlarını bir başkası ile paylaşma iradesi olmadan kendisine sakladığı düşünülmekte olduğundan bu alana kişiliğin çekirdek benliği de denmektedir[93]. Bu alan, dışarıdan bağımsız ve kopuk bir biçimde bireyin kendi içine dönük düşünceleri ve bunları içeren her çeşit dışavurumundan oluşmaktadır. Örneğin, bireyin tuttuğu günlükler, eserleri, inançları, ümitleri, korkuları, planları[94] vb. hususlar bu kısımda yer almaktadırlar. Bu kısım, her kişi ve düşünceden beri olarak yalnız kalma hakkına da dayandırılmaktadır[95]. Bir olay veya davranışın sır alanına girebilmesi için, herkes tarafından izlenebilir ve bilinebilir olmaması gerekmektedir[96].

Bu alan için bireyin kırmızı çizgileri de denilebilir. Bu çizgilerin kesin surette aşılmaması gerekir. Aşıldığı takdirde kişisel verilerin gizliliğinin ihlali sebebiyle TCK'da cezai müeyyideye tabi tutulmuş suçlar da gündeme gelecektir. Ayrıca çekirdek alanla ilgili

[91] Benedik/Slovenya, Başvuru No: 62357/14, 24.04.2018, par. 109, Erişim Tarihi: 16 Mart 2019.
[92] Bărbulescu/Romanya, Başvuru No: 61496/08, Büyük Daire Kararı, 05.09.2017, par. 73, Erişim Tarihi: 14 Nisan 2019.
[93] Özbudun, Ergun: "Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği", Ankara Hukuk Fakültesi Ellinci Yıl Armağanı 1925-1975, Ankara 1975, s. 26.
[94] Özbek, Veli Özer/Kanbur, Mehmet Nihat/Doğan, Koray/Bacaksız Pınar/Tepe, İlker: Türk Ceza Hukuku Özel Hükümler, Ankara 2018 s. 538; Serdar, İlknur: Radyo ve Televizyon Yoluyla Kişilik Hakkının İhlali ve Kişiliğin Korunması, Ankara 1999, s. 41; Birtek s. 50; Özbudun s. 266.
[95] Dinç, s. 16.
[96] Aksoy, s. 53.

verilerin elde edilemeyeceği hususu, soruşturma tedbirleri çerçevesinde çekirdek alana dokunması yetkisini veren kanuni düzenlemelerde olabildiğince geniş şekilde garanti edilmelidir[97].

Hülasa, söz konusu üçlü ayrım üzerinde kişisel verilerin korunması açısından şunu belirtmek gerekir ki bir kişiyi tanımlanabilir kıldığı ölçüde kişisel veriler her bir ayrım içerisinde yer alabilecektir. Her ne kadar özel hayat verilerini sınıflandırmada etkili bir yol olarak görülebilecek olsa da üç alan teorisinin kişisel verilerin korunmasına katkı sağlamak amacıyla verilerin ayrımını doğrudan belirginleştirmede fayda sağlamayacağı görüşündeyiz.

c) Kişisel verilerin özel hayat verilerinden farklılaşan yönleri

Özgürlük boyutuyla dokunulmazlığı işaret ettiğinden negatif ve korunmasının talep edilebilmesinin Anayasal güvence altına alınmış olmasıyla pozitif bir haklar arasında mütalaa edilen özel hayatın ve kişisel verilerin gizliliğinin korunmasındaki amaç bireyin mahrem kalması gereken bilgilerinin rızası dışında ifşa edilmemesi veya kanun hükmü başta olmak üzere hukuka uygunluk sebepleri dışında işlenmemesidir.

Özgürlüğün kural sınırlamanın istisna olması şeklinde formüle edilen liberal anlayışın özel hayattaki yansıması özel hayata saygı duyulması ilkesi olduğundan, bu haklar bütün hakların kökeninde yer alan bireyin özgürlüğüne dayanmaktadır. Biraz daha özelleştirerek ifade etmek gerekirse, hem kişisel verilerin hem de özel hayatın gizli olması gereği yalnız bırakılma hakkına dayanmaktadır[98]. Bu sebeple, her iki veri türü için de korumanın en önemli kısmını gizlilik unsuru oluşturmaktadır. Gizlilik ise, kişiliği, kişinin özgürlüğünü, haysiyetini ve bütünlüğünü korumakta ve insan onurunun yanı sıra toplanma ve ifade hürriyeti gibi temel değerleri desteklemektedir[99].

Öte yandan, kişisel veriler ile özel hayat verilerini ayırabilmek oldukça çetrefilli bir iştir. Keza birbiri ile iç içe geçmiş bir veri sınıflandırması ortadadır. Ayrıca, Anayasa'da ve kanunlarda özel hayatın ne anlama geldiğini açıklayan bir tanım da bulunmamaktadır.

[97] Kanadoğlu, Korkut. 2009. "Türkiye Cumhuriyeti Anayasasında Özel Yaşam" Türkiye Barolar Birliği Özel Yaşamın Gizliliği Paneli, Ankara, 18 Ekim 2009, s. 93.
[98] Henkoğlu, s. 31.
[99] Rodrigues, Roberto J./Wilson, Petra/Schanz, Stephen J.: The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases, Washington 2001, s. 25.

Özel hayat verileri üzerinde yapılan üçlü ayrımı, objektif ölçütlerin belirlenmesinde yaşanan zorluklar sebebiyle kişisel veriler üzerinde yapma imkânı bulunmamaktadır. Dolayısıyla her zaman olmasa da özel hayatın gizliliği kapsamında korunması gereken verilerin kişisel veri de olabileceği kuvvetle muhtemeldir.

Bu ikisi arasında bir ayrım yapmak gerekirse şöyle bir farklılık söz konusu olabilir: özel hayat verisi bir kişi ile ilgili her türlü veriyi ifade ederken, kişisel veriler kişiyi belirli kılabilecek her türlü veriyi ifade etmektedir. Koruma kapsamındaki özel hayat verileri bireylerin hayatında gizli kalması gereken verilere odaklanmışken, kişisel veriler yine gizli kalması gerekmekle birlikte daha çok verinin kişiyi belirlenebilir kılıp kılmadığı odaklanmaktadır. Bir görüşe göre kişisel verilerin korunmasının temelinde gizlilik yatarken özel hayatın gizliliğin korunmasının temelinde tercih hürriyeti ve kişi özerkliği yatmaktadır[100].

II. KİŞİSEL VERİLERİN KORUNMASININ ÖNEMİ

A. Genel Olarak

Özel hayatın gizliliği ile ilgili Türk hukukunda hem anayasal hem de kanuni düzenlemeler kendisine uzun zamandan beri yer bulmaktayken, kişisel verilerin korunması ile ilgili düzenlemelerin Türk hukukunda oldukça yeni olduğu aşikârdır. Dünyadaki gelişmiş hukuk sistemleri de benzer bir durumda olduğu gerçeğinden yola çıkarak, bu alanda dünya genelinde son yarım yüzyılda büyük bir atılımın mevcut olduğunu ifade etmek gerekir. Bu atılımın sonucunda kişisel verilerin korunması hukukuna bakıldığında, bu gelişimin temelini şekillendiren üç sacayağının gizlilik, veri koruması ve etik sorunlar olduğu görülmektedir[101].

1982 Anayasası'nın ilk halinde kişisel veriler bahsi yer almamaktaydı. 2010 yılı Anayasa değişikliğiyle özel hayatın gizliliği maddesine getirilen ek fıkrayla kişisel verilerin korunması konusu anayasal güvenceye kavuşmuştur. Buna göre, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı olup, kişisel veriler ancak kanunda öngörülen

[100] Wacks, Raymond: Privacy: A Very Short Introduction, Oxford 2015, s. 2.
[101] Finn, Rachel L./Wright, David/Jacques, Laura: Study on Privacy, Data Protection and Ethical Risks in Civil Remotely Piloted Aircraft: Final Report, Brüksel 2014, s. 11.

hallerde ya da kişinin açık rızası varsa işlenebilecektir. Bu hak kapsamı içerisinde kişinin kendisiyle ilgili kişisel verilerin akıbeti hakkında bilgilendirilmesi, bu verilere erişebilmesi, bunların düzeltilmesini veya silinmesini talep edebilmesi ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme yer almaktadır[102].

Verilerin korunmasıyla hedeflenen aslında verilerin değil, bu verilerin ilişkili olduğu kişilerin korunmasıdır[103]. Burada kişilerin korunması kişisel statünün gizliliği, vücudun gizliliği, iletişimin gizliliği ve alansal gizlilik olarak dört farklı alana bölünen gizliliğin sağlanması anlamına gelmektedir[104]. Kişisel verilerin korunması konusunda, kişi çok önemli yer tutmaktadır. Bu konu ile ilgili olarak Avrupa Birliği'nin temel yapı taşını oluşturan kişi, artık devletin karşısında yer aldığı şekil olan soyut insan tasavvuru yerine Avrupa toplumun merkezi olarak kabul edilmeye başlanmıştır[105].

Verilerin işlenmesi yeni bir olgu olmamasına karşın artan veri koruma ihtiyacının iki yönü bulunmaktadır. Birincisi gelişmiş telefon uygulamaları gibi kişisel kullanıma sunulan teknolojik yazılım ve donanımların varlığıdır. Geleneksel yollardan farklı olarak kişinin kalp hızını birebir ölçme ve bulunduğu yeri nokta atışıyla hesaplama gibi özelliklere sahip olarak anlık, sürekli ve çoğu zaman da kullanıcının bilgisi olmadan verilerinin otomatik olarak işlenebilmesidir[106]. İkincisi, günümüzde sadece devlet değil şirketler de kişisel verilere kolayca erişebilmekte ve işlemekte olmasıdır. Bu sebeple, verilerin korunması kapsamındaki hükümlerin sadece dikey değil, yatay olarak yani birey-birey arasında uygulama alanı bulacağını ifade etmek gerekir[107].

Ayrıca belirtmek gerekir ki, veri ihlallerini önlemede işin doğası gereği veri işleme sistemlerini hukuka uygun hale getirmek esastır. Bu yüzden veri korunmasının temelini oluşturan bilgi güvenliği politikalarındaki öncelikli amaç, verinin korunmasını önleyici

---

[102] İlgili hakkın kapsamı Anayasa m. 20(2)'de düzenlenmektedir:
"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."
[103] Küzeci, s. 13.
[104] Ramage, Sally: Privacy-Law of Civil Liberties, Nebraska 2007, s. 3.
[105] Alston, Philip/Bustelo, Mara/Heenan, James: The EU and Human Rights, 1999 New York, s. 902.
[106] Fong, Adrian: "The Role of App Intermediaries in Protecting Data Privacy", International Journal of Law and Information Technology, 25, Oxford 2017, s. 90.
[107] Çekin, s. 16.

yöntemlerle sağlamaktır[108]. Bu doğrultuda kişisel verilerin korunmasına yönelik hukuki tedbirlerin yanı sıra teknolojik önlemlerin alınması da korunmayı tamamlayan bir unsur olarak giderek önemini artırmaktadır[109].

Alınacak teknolojik önlemlere örnek olarak, uçtan uca şifreleme teknolojisinin kullanılması, verilerin işlenmesinde çevresel güvenliğin[110] sağlanması, güvenliği onaylanmış açık-kaynak yazılımlarla (SOSS) teknolojik bağımsızlığın artırılması, yapısal problemlerin internet protokolleriyle çözülmesine dönük çabaların artırılması ve şifreleme sertifikalarını veren bağımsız bir kurumun oluşturulması verilebilir[111]. Ayrıca, veri perdeleme tekniği ile akıllı sistemlerden aktarılmakta olan verilerin tam koruma sağladığı ve kamu güçlerinin müdahalelerinde aranan yeterli meşruiyet dengesini sağladığı iddia edilmektedir[112].

Bu yüzden, kişisel verilerin korunması bölümünde öncelikle korunma ihtiyacının ortaya çıkmasına neden olan işleme terimi açıklanmaktadır. Akabinde ise kanuni düzenlemenin varlığının önemi üzerinde durulmaktadır. Son olarak, bireyin özgürlüğü-devletin güvenliği arasındaki denge analiz edilmekte ve kişisel verilerin korunması hakkının sınırları ele alınmaktadır.

B. Kişisel Verilerin İşlenmesi Terimi

Kişisel verilerinin korunmasını gündeme getiren en önemli olgu kişisel verilerin işlenmesidir. Bu yüzden söz konusu "işleme" kelimesinden anlaşılması gerekenleri ortaya koymak tezimiz açısından çok önemlidir.

---

[108] Henkoğlu, s. 112.
[109] Turan, s. 206.
[110] Margaret R. 2009. "Deperimeterization." Techtarget.com. Etişim Tarihi: Nisan 2019 https://searchsecurity.techtarget.com/definition/deperimeterization/: Bir ağ güvenliği terimi olarak çevresel güvenlik, şifreleme ve dinamik veri düzeyinde kimlik doğrulama kullanarak bir şirketin verilerini birden fazla düzeyde koruma stratejisini ifade etmektedir.
[111] Berg, M. van den/Kwant, P.O/Graff, P. de/Slewe, T: Mass Surveillance : What are the risks for the citizens and the opportunities for the European information society? What are the possible mitigation strategies? Part 2 Technology foresight, options for longer-term security and privacy improvements, Brüksel 2015, s. 54.
[112] Posadas, Dalmacio V. Jr.: "The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption." Gonzaga Law Review, 53, Washington 2017, s. 108.

Belirtmek gerekir ki işleme hususu başta sadece kişisel verilerin toplu olarak bir veri tabanına kaydedilmesi olarak akla geliyor olsa bile işlemenin kapsamı çeşitli hukuki metinlerde çok daha geniş olarak tanımlanmaktadır.

KVK Kanunu m. 3(1)(e)'ye göre işleme faaliyeti, "*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 işlemi*" ifade etmektedir.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'e göre işleme faaliyeti ise, "*kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen işlem ya da işlemler bütünü*" olarak tanımlamaktadır.

Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'e göre kişisel sağlık verilerinin işlenmesi ise, "*kişisel sağlık verilerinin 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi sağlık verileri üzerinde gerçekleştirilen her türlü işlemi*" ifade etmektedir.

VKS'nin m. 2(c)'ye göre ise, "*tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılmasını*" ifade etmektedir.

AB'nin 95/46/EC sayılı Direktif'i m. 2(b)'ye göre işleme faaliyeti, "*kişisel veriyi silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle*

açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisini" ifade etmektedir.

95/46/EC sayılı Direktif'in değişen koşullar doğrultusunda güncellenmiş hali olan GDRP m. 4(2)'e göre ise, işleme faaliyeti, "*otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi*" olarak tanımlanmaktadır. "Gibi" lafzından dolayı maddede sayılan hususların kısıtlayıcı değil örnekleyici olduğuna dikkat edilmelidir.

Sonuç olarak kişisel verilerin işlenmesi, kişisel verilerin ele geçirilmesi, depolanması ve yok edilmesi gibi bu süreçler içerisinde yapılan her türlü eylem olarak tanımlanabilir. Yine bu açından belirtmek gerekir ki soruşturma evresinde kişisel verilerin öğrenilmesi başta olmak üzere veriler üzerinde yapılabilecek her türlü işlem, kişisel verilerin işlenmesi olarak ifade edilebilecektir.

C. Verilerin Korunmasında Kanuni Düzenleme Şartının Önemi

Anayasa m. 20(3)'de kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmü yer almaktadır. Bu doğrultuda kişilerin kişisel verilerinin korunmasında güvence sağlamak üzere 2016 yılında Kişisel Verilerin Korunması Kanunu çıkmış ve Kişisel Verileri Koruma Kurumu kurulmuştur. Böylece, Anayasa'da soyut olarak belirtilen hak, somutlaştırılmış ve güvence hususu kısmen ve şeklen açıklığa kavuşturulup öngörülebilir şekilde detaylandırılmıştır.

Ayrıca 28.10.2017 tarihinde KVK Kurumu tarafından 6698 sayılı kanuna dayanılarak Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik çıkarılarak veri sorumlularınca işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esaslar belirlenmiştir. Bunun

dışında, KVK Kurumu tarafından çıkarılan 6 adet yönetmelik ve çeşitli konulardaki ilke kararları ile kanun hükümleri açıklanmaya ve detaylandırılmaya devam edilmektedir[113].

Özel hayatın gizliliğinden ayrıldığı ölçüde, kişilerin temel hak ve hürriyetleri arasında yer alan kişisel verilerin gizliğine yönelik müdahalenin yani verilerin işlenmesinin hukuka uygun olması için kanunen düzenlenmiş olması gerekir. Hem AİHS m. 8 hem de AİHM'in temel hak ve hürriyetlere yönelik müdahaleler konusunda var olan temel içtihadına göre, temel hak ve hürriyetlerin kısıtlanmasının açıklanmasında kanuni düzenlemenin var olması aranan şartlardandır. Aynı şekilde Anayasa m. 13 uyarınca da temel hak ve hürriyetlerin sınırlanmasında kural, yapılacak sınırlamanın hakkın özüne dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanmasıdır.

Kişisel verilerin işlenmesinin şartlarının kanun ile düzenleneceği Anayasa'da açıkça belirtilmiş olması, işleme şartlarının ve hassas veri ayrımının kanunlarca yapılmasını gerektirir. Keza, KVK Kanunu'nun genel gerekçesinde de belirtildiği üzere, kişisel verilerin korumasına ilişkin alanı bütüncül olarak düzenleyen bir kanunun yapılmasındaki hedef, verilerin işlenmesine ilişkin hükümlerin düzenlenmesi ile hak ihlalleri önlenmek istenmesidir. Ayrıca, Anayasa m. 20(3)'te kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği hükme bağlanmıştır. Bu doğrultuda Anayasa Mahkemesi bir kararında, kanuna dayanarak yapılacak sınırlamada kanunda öngörülen hallerin belirtilmemesi halinde düzenlemenin kişisel verilerin gizliliğine saygısızca dokunacağını ve Anayasa hükmüne aykırılık teşkil edeceğini belirtmektedir[114].

Kanun ile detaylandırılmakta olan kişisel verilerin korunması hakkına yönelik sınırlamaların taşıması gereken bazı Anayasal nitelikler bulunmaktadır. Bunlar, hakkı sınırlayan kanun hükmünün Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olmamasıdır. Sınırlamadaki

[113] 16 Kasım 2017'de Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik,
30 Aralık 2017'de Veri Sorumluları Sicili Hakkında Yönetmelik,
9 Şubat 2018'de Kişisel Verileri Koruma Uzmanlığı Yönetmeliği,
26 Nisan 2018'de Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği ve
5 Mayıs 2018'de Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği çıkarılmıştır.
[114] E. 2014/149, K. 2014/151, KT: 02.10.2014, RG. 29223, 01.01.2015, Erişim Tarihi: 12 Nisan 2019.

meşru sebepler olarak ifade edilebilecek bu özellikleri dikkate almayan sınırlamalar Anayasaya aykırı olacaktır.

Anayasa Mahkemesi bir kararında, kısıtlama getiren hukuk normlarının süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki usullere ilişkin muhataplarının yetki aşımı ve keyfîliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralları içermesi gerektiğini belirtmektedir[115]. Diğer sebeplerden bağımsız olarak ölçülülük açısından öne çıkan özellik, kişisel verilerin korunması hakkına yönelik bir müdahalenin esas ve miktar açısından orantılı olmasıdır[116]. Bu yönden, esas açısından ölçülülük, müdahale edilecek kişisel veri çeşidi yelpazesini; miktar açısından ölçülülük ise tedbirin uygulanması sonucu elde edilecek veri miktarının makul olmasını ifade etmektedir.

Kanuni düzenlemenin zikredilen nitelikte haliyle var olması üzerinde bu kadar önemle durulmasının iki temel sebebi bulunmaktadır. Bunlar, diğer alt normlarının sahip olmadığı farklı nitelikteki şekli ve maddi özelliklerin kanun ile sağlanmakta oluşudur. Buna göre, kanunların yapım sürecinde tüm ülkede geçerli, devamlı ve herkese uygulanacak kurallar konmaktadır. Bu süreç, getirilecek hükümlerin milletin egemenliğinin tecelli ettiği yer olan ulusal meclislerde kanun yapım aşamalarını geçirerek ve mecliste farklı partilerden müteşekkil ilgili komisyonlarca tartışılarak gerçekleşmektedir. Böylece, hem aleniyet hem de kamuoyu denetimi sağlanmış olmaktadır[117].

Ayrıca, kanun yapım sürecinin farklı görüşlerin katılımını sağlayan ayrıntılı usullere tabi olması ve Anayasaya uygunluğunu ortaya koymaya çalışan bir gerekçesinin bulunması sebebiyle kişi açısından daha fazla güvence sağlamaktadır. Üstelik yasama faaliyeti sayesinde kişiler kanunlar yoluyla idareye karşı daha orantılı olarak korunmaktayken, idarenin takdirinin baskın olduğu yönetmelik gibi genel düzenleyici işlemlerde kişisel verilerin korunması hususu bir nevi idarenin geniş yetkisine bırakılmaktadır. Bu ikisinin farkı, idari tasarrufla düzenlenmiş olsa yürütmenin tasarrufuna bırakılacak olan

[115] Başvuru No: 2014/7256, 27.02.2019, par. 90, Erişim Tarihi: 13 Nisan 2019.
[116] Akgül, s. 154.
[117] Gözler, Kemal: Anayasa Hukukunun Genel Teorisi, Bursa 2011, s. 549.

düzenlemelerin, kanuni düzenleme olarak çıkarılmasıyla yasamanın yetkisine dayanmasıdır.

İdarenin istisnai olarak yasamanın alanına müdahale ederek yaptığı genel düzenleyici işlemlere nazaran yasamanın hem asliliği, hem genelliği ve hem de devredilmezliği ilkeleri doğrultusunda düzenlenmiş olan kanunlar güçler ayrılığı açısından hukuki meşruiyetini daha kolay sağlayacaktır. Aksi durum, örneğin kanunla düzenlenmesi gerekli olan bir hususun yönetmelik ile düzenlenmesi hali, yasamanın görevine yürütmenin dâhili anlamına geleceğinden bu durum genel hukuk teorisiyle ve pratiğiyle uyuşmaz, fonksiyon gaspı gündeme gelebilir.

Bu arada unutmamak gerekir ki, hakkın pozitif hukuk normları arasındaki kurucu kaynağı Anayasa'nın hükmüdür. Kanunun yapım amacı, Anayasa ile getirilen hükmün açıklanmasıdır. Elbette ki, kişisel veriler bahsi kanunların nasıl uygulanacağını göstermek amacıyla yönetmelik ya da yönergelerle detaylandırılabilir, açıklığa kavuşturulabilir. Fakat kanuni düzenleme olmadan sadece yönetmelik ile düzenleyici işlem yapılmış olması hem normlar hiyerarşisine aykırı olacak hem de kanunun sağlayacağı güvencelerden yoksun kılınacağı sebebiyle demokratik toplum düzeninin gereklilikleri ile bağdaşmamış olacaktır. Bu doğrultuda kanunun gerekçesinde yer alan karşı oy yazısında da belirtildiği üzere, kurula çıkaracağı yönetmelik ve genelgeler aracılığıyla sistemi yönetme anlamında geniş serbesti tanınması yasa yapma tekniğiyle bağdaşmamaktadır[118].

Kanuni düzenleme gereğinin ikinci temel dayanağı ise, yukarıda da belirttiğimiz üzere kanunun maddi özelliğidir. Kanunun maddi özelliği, düzenlemenin kişiler tarafından açık, öngörülebilir ve erişilebilir olmasıdır. Bunun anlamı, kanunların birbirinden farklı anlamlara gelecek şekilde düzenlenmemesi, kişilerin kanuna kolayca erişebilmelerini ve demokratik toplum gereklilikleri doğrultusunda ölçülü olmasıdır. Öngörülebilirlik ise kişilerin kanuni düzenlemeyi önceden ön görmelerini sağlar ve ayrıca idarenin yetkisi sınırlar, şekillendirir ve şartlara bağlar. Kanunun hukukun üstünlüğüne uygun olacak şekilde, yeteri kadar erişilebilir ve öngörülebilir olarak keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini

[118] 6698 sayılı Kanun Gerekçesi, s. 71.

yeterli bir netlikte tanımlaması gerektirir[119]. Böylece, idarenin keyfi müdahale tehlikesi bertaraf edilmiş ve insan hakları korunmuş olur. Keza bir hukuk devletinde, kamu hürriyetlerinin sınırlanması mevzubahis ise orada idarenin keyfiliği gerekçe olamaz. Üstelik hak ve özgürlükleri kısıtlayan bir yasanın açık, kesin ve yorum yoluyla genişletilemez olma zorunluluğu[120] kanuni düzenlemeleri daha güvenceli kılmaktadır. Kanunun kişisel verileri koruyucu niteliğe sahip olarak var olmaması diğer bir deyişle iç denetimi sağlamayan güvencelerin yokluğu kolluk kuvvetlerine olan güveni de olumsuz etkilemektedir[121].

Sonuç olarak, burada kanuni düzenlemenin varlığının önemi kanuni şekil ile birlikte hükmün içeriğinin taşıdığı özellik ve niteliklerle ilgilidir. Yani sadece şekli kanun değil maddi kanun özelliklerinin de oluşmuş olması gerekmektedir. Bu yüzden, KVK Kanunu öncesinde kanun dışındaki hukuki normlarla kişisel verilerin işlenmesi alanının düzenlenmesi girişimleri Anayasa Mahkemesi tarafından iptal edilmiştir. İdari makamlar arasında kişisel verilerin paylaşımının KHK ile düzenlenmesinin konu olduğu bu davada, Anayasa Mahkemesi'nin iptal gerekçesi, Anayasa m. 91 doğrultusunda KHK ile kişi hak ve hürriyetlerinin sınırlandırılamayacağı olmuştur[122]. Dolayısıyla, kişisel verilerin temel hak ve hürriyetler arasında yer aldığı ve bu hakkı sınırlandıracak bir düzenlemenin şekli açıdan kanun olması düşüncesi ağırlık kazanmıştır.

Özetle, kişisel veriler üzerinde hedeflenen koruma amacına ulaşabilmek için kanuni düzenlemelerin zikrettiğimiz özellikleri haiz olması gerekmektedir. Böylece, hakka yönelik müdahalede yani kişisel verilerin işlenmesinde idareyi ve üçüncü kişileri hukuk sınırları içerisinde tutacak sınırlar çizilmiş olmaktadır. Tüm bu sebeplerden ötürü, kanuni düzenlemenin idareyi ve üçüncü kişileri bağlayıcı özellikleri aranan korumanın kanunla yapılmasını kaçınılmaz olarak gerektirmektedir. Bir diğer deyişle, verilerin işlenmesinde kişileri idarenin takdirinden kurtaracak ve korunma taleplerini dayandırabilecekleri kanuni kurallar bütününün varlığı gerekli güvenceyi sağlayacaktır. Sonuçta kanun sadece bir sınırlandırma yönetimidir, sınırlama sebebi olarak kabul edilemez, bu yüzden sadece

[119] S. ve Marper/Birleşik Krallık, Başvuru No: 30562/04 ve 30566/04, Büyük Daire Kararı, 04.12.2008, par. 95, Erişim Tarihi: 11 Nisan 2019; Malone/Birleşik Krallık, Başvuru No: 8691/79, 02.08.1984, par. 66-68, Erişim Tarihi: 1 Nisan 2019; Amann/İsviçre, par. 56, Erişim Tarihi: 3 Mart 2019.
[120] Dülger, 2019, s. 88.
[121] H. Flaherty, David: Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, North Carolina, 2014, s. 145.
[122] E. 2011/141, K. 2013/10, KT: 10.01.2013, RG. 28865, 28.12.2013, Erişim Tarihi: 4 Nisan 2019.

kanunda yer aldığı için bir düzenleme anayasaya uygun hale gelmez, sayılan özellikleri de taşıması gerekir[123].

D. Özgürlük-Güvenlik İkilemi Bağlamında Kişisel Verilerin Korunması

İnsanlar güvenli bir şekilde temel hak ve hürriyetlerini kullanabilmek adına bu özgürlüklerinden kısmen ödün vererek devlet örgütünü oluşturmuşlardır. Bu amaç doğrultusunda oluşturulan devlet, kişilerin temel hak ve hürriyetlerini hem devlet(idare) olarak kendisine karşı hem de diğer kişilere karşı koruma görevini üstlenmiştir[124]. Hatta devletin varlığının yegâne sebebinin bu olduğu da iddia edilebilir.

Kişinin güvenliği, diğer haklar ile birlikte özel hayatın gizliliği hakkına tecavüz edilmemesini de kapsamaktadır. Devletin bunu sağlayabiliyor olması gerekmektedir. Keza, kişiler özgürlüklerinden kısmen vazgeçmenin yanı sıra hem bir yandan vergi ödevi ile hem de diğer yandan bazı temel haklarının kısıtlanmasına katlanarak devletin bunu sağlamasını kolaylaştırmaktadırlar.

Kişi-kişi ilişkilerinde bir kişinin özgürlük alanı içerisinde tasarrufta bulunacağı alan diğer kişilerin alanına tecavüz etmesi ile son bulur. Fakat kişi-devlet ilişkilerinde kamu düzeninin sağlanması için kamu yararı gibi toplumun tamamını ilgilendiren ve kamu gücü kullanımının devreye girebileceği durumlarda kişinin temel hak ve hürriyetlerine daha fazla müdahale edilebilmektedir. Bunun gerekçesi toplum hayatının doğal bir gereği olan nizamın kurulması amacı doğrultusunda ortak iyinin ve menfaatin sağlanıyor olmasıdır.

Diğer bir deyişle, toplumun iyiliği gerekiyorsa kişinin temel hak ve hürriyetleri hakkın özüne dokunulmaksızın sınırlanabilecek ve hatta durdurulabilecektir. Tamamen durdurmanın istisnası ise sert çekirdek haklar olup bunlar mutlaktırlar yani sınırlanamaz ve durdurulamazlar[125]. Bu haklar kişinin, yaşama hakkı; maddî ve manevî varlığının bütünlüğü dokunulmazlığı; din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamama ve bunlardan dolayı suçlanamama; suç ve cezalar geçmişe yürütülememesinden ibarettir.

[123] Akdağ, s. 87.
[124] İdare ve kişi arasında dikey, kişi ve kişi arasında yatay olarak görünmekte olan ilişkilerde kişilerin hak ve hürriyetleri sağlamakla yükümlü oluşu devletin varlık sebeplerinden birisidir.
[125] Bunun tek istisnası, yaşama hakkına getirilmiş olan savaş hukukuna uygun fiiller sonucu meydana gelen ölümlerdir.

Özel hayatın gizliliği bu haklar arasında doğrudan zikredilmediği için kişisel veriler alanına kamu yararı gerekçe gösterilerek müdahale edilebilmektedir.

Öte yandan, son yüzyılda başta artan terör faaliyetlerinin sebep olmasıyla birlikte devletlerin güvenlik algısında bir değişiklik yaşanmaktadır. Özellikle Amerika ve Avrupa Birliği gibi ülkelerde, terörizmin, ciddi ve organize suçların siber suçların, sınır aşan suçların, doğal ve insanın sebep olduğu felaketlerin yaygınlaşması sebebiyle güvenlik konusu artık kaçınılmaz olarak gündeme oturmuştur. Artan bu güvenlik ihtiyacı sonuç olarak kişilerin verilerinin güvenlik amacıyla işlenmesine yol açan bir alan oluşmasına neden olmaktadır[126].

Bu açıdan, kişisel verilerin korunması hakkı ve özgürlüğü ile güvenlik hakkı arasında bir dengenin oluşturulması ve bu hususun ilkelere dayanan kurallara tabi olması gerekmektedir. Bu hususta KVK Kanunu'nun çıkarılması son yıllarda ortaya çıkan bu ihtiyaca yönelik verilen cevaplardan birisidir. Böylece, idare kamu düzeni çerçevesinde meşru sebeplerin varlığında kişilerin kişisel veri alanına hukuka uygun olarak müdahale edebilecektir. Fakat bu müdahalenin kişilerin kişisel verilerinin korunması hususunda dikkatli ve hakkın özüne dokunmayan bir ölçüde olması gerekmektedir.

Bizim görüşümüze göre, idare gerekli koşulların varlığında kişilerin kişisel verilerini işlerken bir insanın sırf insan olmak doğan temel hak ve hürriyetlerini kullanmasını engelleyecek şekilde o kişiyi yabancılaştıran bir çerçeve içerisinde bu faaliyeti göstermemelidir. Her bir kişinin kişisel verilerinin işlenmesinde, suçluluğu bağımsız mahkemeler önünde delillerle kanıtlanana kadar masum olan her bir vatandaş gibi görülerek eşit mesafede durulmalıdır. Aksi halde vatandaşlarının bir kısmını güvenlik nedeniyle ayrıştırıp ötekileştiren tavır, seküler devlet ve insan hakları kuramının altını dinamitleyecek, temel hak ve hürriyetleri siyasileştirip bu kuramı çıkmaza sokacaktır.

Ayrıca, kişisel verilerin korunması hakkı insan hakları bağlamında korunduğundan Türk vatandaşı olsun ya da olmasın bu haktan her bir kişinin yararlanması gerektiği özellikle terörü önleme saiki ile verilerin korunması hakkının sadece vatandaşlara hasredilmesi uygun düşmeyecektir. Çünkü aksi yönde bir tavır günün sonunda idarenin yabancıların verilerinin işlerken, vatandaşlarımızın değil yabancıların verilerini güvenlik amacıyla

[126] Gutwirth, Serge/Leenes, Ronald/de Hert, Paul: Reforming European Data Protection Law, Dordrecht 2015, s. 273.

işliyoruz savunmasıyla çıkıp gelmesine yol açabilecektir[127]. Ayrıca bunun toplumlarda var olan yabancı düşmanlığını artıracağını da unutmamak gerekir.

E. Kişisel Verilerin Korunması Hakkının Sınırlandırılması

1. Kamu otoritesince getirilecek sınırlama: Dikey sınırlama

Anayasa m. 20(3)'te kişisel verilerin korunması hakkına yer verilmiştir. Fakat bu hakkı sınırlayan özel sebepler düzenlememiştir. Anayasa m. 20'nin birinci ve ikinci fıkralarında özel ve aile hayatının gizliliğine yönelik getirilebilecek sınırlama sebeplerinin kişisel veriler yönünden uygulama alanı bulamayacağını belirtilmektedir[128]. Çünkü bu sınırlamalar özel hayatın gizliliği için düzenlenmiş olan bağımsız hükümlerdir. Yargıtay'ın da belirttiği üzere, demokratik toplumda asıl olan kişilerin temel hak ve özgürlüklerinin korunması olup, bir hakkın kullanımı ve kısıtlanması hükümleri düzenlemelerde birlikte yer almalıdır[129]. Bu yüzden geriye, temel hak ve hürriyetlerin sınırlanmasındaki genel dayanak olan Anayasa m. 13 doğrultusunda kişisel verilerin korunması hakkına yönelik sınırlama getirilmesi kalmaktadır.

Bu doğrultuda, kişisel verilerin korunması hakkına getirilecek sınırlandırmalar kanunla yapılmalıdır. Kanunun ise ölçülülük ilkesi ve normların açıklığı ilkesine uyması gerekmektedir[130]. Bu noktada Danıştay'ın, belediye personelinin mesai takibini parmak izi uygulamasıyla yapılmasının yasal dayanaktan mahrum olması sebebiyle hukuka aykırı olduğuna hükmettiğini hatırlatmak gerekir[131]. Bunların dışında ayrıca, sınırlama sebebi olarak AİHS m. 8(2) kapsamında yer alan sınırlama sebeplerinin ileri sürülmesi mümkün olmamalıdır. Çünkü Türk hukuku Anayasa'da kişisel verilerin korunmasına yönelik özel sınırlama sebebi görmeyerek kişilere AİHS'ten daha fazla özgürlük alanı tanımaktadır.

Tezimiz bağlamında ifade etmek gerekir ki, AY m. 20(3)'te kişisel verilerin kamu otoriteleri tarafından soruşturma evresinde sınırlandırılabileceğine ilişkin bir anlam

[127] Lubin, Asaf: "We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance", Chicago Journal of International Law, 18/2, Şikago 2018, s. 508.
[128] Sert, s. 73
[129] Y. 16. CD, 24.04.2017, E. 2015/3 K. 2017/3, Erişim Tarihi: 5 Şubat 2019; Kazancı İçtihat Bilgi Bankası.
[130] Korkmaz, İbrahim: Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara 2017, s. 109.
[131] D. 5. D, E. 2013/5342, K. 2013/9525, 10.12.2013, Erişim Tarihi: 6 Şubat 2019; Kazancı İçtihat Bilgi Bankası.

çıkmamakta olduğundan KVK Kanunu m. 4 ile 22 birbiri ile çatışmaktadır[132]. Çatışan nokta, m. 22 düzenlemesine göre soruşturma evresinde m. 4'te düzenlenen genel ilkelerin dahi uygulanmayacak oluşu anlamı çıkmasından kaynaklanmaktadır. Keza, genel ilkelerin korunma şartlarından bağımsız olarak her alanda uygulanması gerekmektedir. Dolayısıyla olması gereken, ilgili hükümlerin kişisel verilerin işlenmesi şartlarından bağımsız olarak işleme ilkelerinin soruşturma evresinde de geçerli olacak şekilde yeniden düzenlenmesidir.

2. Temel hak ve hürriyetlerden yararlanılması bakımından kişisel veriler alanına müdahale: Yatay sınırlama

Kişisel verilerin korunması hakkı sınırlanabilir bir hak olduğundan uygulanabilir norm alanının daraltılması mümkündür[133]. Bu sebeple, bu hakkın koruyucu norm alanının diğer kişilerin hak ve hürriyetleri karşısında da daraltılması söz konusudur.

Kişisel verilerin korunması yönünde alınacak güvencelerin diğer temel hak ve hürriyetlerin birçoğu ile çatışması ihtimal dâhilinde olması sebebiyle haklar arasında dengeli bir orantının kurulması önem taşımaktadır. Özellikle ifade hürriyeti, basın hürriyeti ve bilgi edinme hakkı kapsamında kişisel verisi ifşa edilen kişinin bu yöndeki menfaati ile bu verilerin öğrenilmesi hususundaki menfaatin dengelenmesi önem taşımaktadır.

Diğer temel hak ve hürriyetlerin kullanılması açısından kişisel veriler alanına yapılacak bir müdahalenin sınırlarını belirlemeye geçmeden önce Türk hukukunda ifade hürriyeti ile basın hürriyeti arasında var olan belli farkları ele almak gerekmektedir. Bu doğrultuda belirtmek gerekir ki, bir haberin ifade özgürlüğü mü yoksa basın özgürlüğü kapsamında verilebileceğine ilişkin kullanılabilecek ölçütler bulunmaktadır. Buna göre, haber konusunun içeriğinin aktarımı bunu belirlemektedir. Eğer söz konusu haber verisi, haber verme amacı doğrultusunda yorum katılmadan objektif bir biçimde haberciliğin sınırları aşılmadan verilebiliyorsa o takdirde aktarım basın hürriyeti kapsamında değerlendirilmelidir. Eğer söz konusu verilerin aktarımında aktarılan verilerle ilgili yorum ya da eleştiriler yapılıyorsa o takdirde yapılan aktarım ifade özgürlüğü kapsamında

[132] KVK Kanunu m. 4 kişisel verilerin korunmasında genel ilkeleri, m. 22 ise kanunun kapsamına girmeyecek olan istisnaları düzenlemektedir.
[133] Sert, s. 70.

olmalıdır. O halde, bilgi vermenin söz konusu yerde basın özgürlüğü; eleştiri ve yorumun olduğu yerde ise ifade özgürlüğü gündeme gelmektedir.

Her ne kadar 1982 Anayasa'sı ifade hürriyetini ve basın hürriyetini farklı maddelerde birbirinden bağımsız kurallar çerçevesinde düzenliyor olsa bile, Avrupa kurumları ve AİHM basın hürriyetini AİHS m. 10'da yer alan ifade hürriyeti kapsamında düzenleyerek farklı bir yol izlemektedir. 95/46/EC sayılı Direktif de, edebi veya sanatsal açıklama amaçlarının yanı sıra gazetecilik amaçları için kişisel verilerin ifade özgürlüğü doğrultusunda işlenebileceği düzenlenmektedir[134].

İfade özgürlüğü ve basın özgürlüğü arasındaki var olan farklılığı bu şekilde ortaya koyduktan sonra kişisel veriler ile diğer temel hak ve hürriyetlerden yararlanılması bakımından kişisel veriler alanına müdahalenin sınırlarını göstermek gerekmektedir.

AİHM, basın özgürlüğü ile özel hayatın gizliliği hakkına dayanan kişisel verilerin korunması hakkının çatıştığı *Peck/Birleşik Krallık* davasında, herhangi bir suçtan bağımsız bir şekilde yoldan geçen sıradan bir kişinin kimliğinin ailesi, arkadaşları, komşuları ve meslektaşları tarafından tanınacak şekilde basında servis edilmesini özel hayata saygı gösterme hakkına yönelik ciddi bir müdahale olarak değerlendirmiştir[135].

Basın özgürlüğü ile ilgili *Delfi AS/Estonya* davasında, özel yaşama saygı gösterilmesini isteme hakkının bir parçası olan şöhretin korunması hakkı ile basın özgürlüğü arasında bir üstünlük olmadığını belirtmektedir. Fakat şöhrete yönelik müdahalelerde ihlal kararı için ciddi bir seviyeye ulaşmasının şart olduğunu ifade etmektedir[136]. Elbette ki basın özgürlüğü çerçevesinde yapılan yayının onur kırıcı seviyede olması mümkün değildir[137].

Bu noktada şunu ayırmak gerekir ki, başta siyasi figürler olmak üzere kamuya mal olmuş toplum önündeki ünlü kişilerin de özel hayatının gizli yönü olabileceği fakat bu hakka

---

[134] İfade özgürlüğü ve kişisel verilerin işlenmesi hükmü 46 sayılı Direktif m. 9'da düzenlenmektedir: *"Üye Devletler, kişisel verilerin ifade özgürlüğünü yöneten kurallarla kişisel gizlilik hakkını uzlaştırmak için gerekirse, yalnızca, edebi veya sanatsal açıklama amacı veya gazetecilik amaçları için kişisel verilerin işlenmesinde Kısım IV ve Kısım VI, bu Bölümün hükümlerinden muafiyetler veya derogasyonlar sağlayacaktır."*

[135] Peck/Birleşik Krallık, Başvuru No: 44647/98, 28.01.2013, par. 62, Erişim Tarihi: 13 Şubat 2019.

[136] Delfi AS/Estonya, Başvuru No: 64569/09, Büyük Daire Kararı, 16.06.2015, par. 28, Erişim Tarihi: 19 Mart 2019.

[137] Delfi AS/Estonya, par 30.

yönelik müdahalenin gazetecilik mesleği çerçevesinde daha geniştir[138]. Bu durum, bu kişilerin özel hayatlarının herkesten gizli kalma yetisini niteliksel olarak kaybetmiş olması dolayısıyla bu kişilerin kamuya mal olan hayatlarıyla ilgili konuların herkesten gizli kalmasını isteme haklarının olmamasından kaynaklanmaktadır[139]. Bu bağlamda, TCK m. 285(6) düzenlemesi de soruşturma işlemlerinin haber verme sınırları aşılmaksızın haber konusu yapılmasının suç teşkil etmeyeceğini öngörmektedir. Elbette ki, sanatsal ifade özgürlüğü ve haber alma özgürlüğüne ilişkin kurallar ile kişisel verilerin gizlilik hakkı ve korunması boyutu arasında ölçülü bir orantının her somut olayda ayrıca değerlendirilmesi gerekmektedir.

Her ne kadar aksini düşünen bir görüş bulunsa da[140], kişisel verilerin korunması ve ifade özgürlüğü arasında temel bir çatışma bulunmadığı, çünkü her iki hakkın bir arada gerçekleşmesi için organik bir engel söz konusu olmadığı ifade edilmektedir[141]. O halde, kişisel verilerin korunmasının istisnası olarak basın özgürlüğüne dayanan işleme fiilinin daha geniş tutulmaması kural olarak hukuka uygun olmakla birlikte olayın kendi özgü koşulları çerçevesinde orantılı ve gereken mahremiyet hassasiyetini gözetiyor olmalıdır. Aksi halde yapılan her müdahale kişisel verilerin korunması hakkına yönelik olarak ciddi bir müdahale teşkil edecektir. Keza iletişim araçları ile ihlal edilen veriler geniş kesimlere yayılabilmektedir. Dolayısıyla, kişisel nitelikteki verilerin veya haberleşme kayıtlarının medyada ifşa edilmesini önleyici ve adli yolların usulü ve şartlarının kanunla düzenlenerek belirtilmesi isabetli olacaktır.

Öte yandan, diğer kişi ve kurumlarca kullanılacak bilgi edinme hakkının, bir kişiye ilişkin kişisel verileri öğrenilmesi durumunda, kişisel verilerin korunması hakkıyla karşı karşıya geleceği aşikârdır. Dolayısıyla, kişisel verilerin korunması hakkının negatif yönü sebebiyle diğer kişilerin, kişinin kişisel verilerine erişimi engellenebilecektir. Ayrıca bilgi edinme hakkının negatif yönüyle de aynı durum söz konusu olduğundan kişisel verilerin öğrenilememesi noktasında toplanan karşılıklı negatif bir güvence söz konusu olmaktadır. Bu iki hak arasındaki negatif ilişki sayesinde kişisel verilerin işlenmesi karşısında veri

[138] Akyürek, Güçlü (Bayraktar, Köksal/Keskin Kiziroğlu, Serap/Yıldız, Ali Kemal/Zafer, Hamide/Aksoy Retornaz, Eylem/Evik, Ali Hakan/Sınar, Hasan/Altunç, Sinan/Aytekin İnceoğlu, Asuman/Erman, Barış/Eroğlu Erman, Fulya): Özel Ceza Hukuku - Cilt III - Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar (TCK m. 106-140), İstanbul 2018, s. 622.
[139] Akipek/Akıntürk/Ateş, s. 390.
[140] Çekin, s. 14.
[141] Küzeci, s. 85.

sahibi, verilerin nasıl ve niçin işlendiği hakkında hem bilgi sahibi olabilmekte hem de buna karşı çıkmak amacıyla bu yönde kendisine sunulan hukuki imkânları kullanabilmektedir[142].

[142] Ayözger Öngün, A. Çiğdem: Kişisel Verilerin Korunması Hukuku, İstanbul 2019, s. 51; bilgi edinme hakkı konusunda daha fazla bilgi için BEHK m. 21 ve devamı hükümlerine bakınız.

İKİNCİ BÖLÜM:

ULUSLARARASI BELGELERDE VE TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

I. ULUSLARARASI BELGELERDE KİŞİSEL VERİLERİN KORUNMASI

A. Genel Olarak

Türk hukukunu detaylı olarak incelemeye geçmeden önce kişisel veriler ile ilgili uluslararası hukuk metinlerini değerlendirmek gerekir. Çünkü özel hayat verilerinin kişisel veri olarak korunması hususu 1980'lerin başından günümüze gelişmekte olan bir süreçtir ve dönüm noktalarının bilinmesi konunun kavranması açısından oldukça elzemdir.

Buradan hareketle, kronolojik olarak kişisel verilere münhasıran yer veren ilk uluslararası düzenlemenin, OECD tarafından 1980 yılında çıkarılan ve 2013 yılında güncellenen Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri olduğunu belirtmek gerekir.

Akabinde, Avrupa Konseyi tarafından 21 Ocak 1981 tarihinde, 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi çıkarılmıştır. Avrupa Konseyi ayrıca, farklı sektörlerde uygulanmak üzere kişisel verilerin korunmasına yönelik çeşitli tavsiye kararları da almıştır. Bu doğrultuda, tıbbi veri bankaları, bilimsel araştırma ve istatistik, doğrudan pazarlama, sosyal güvenlik, sigorta, polis kayıtları, istihdam, elektronik ödeme, telekomünikasyon ve internet gibi çeşitli sektörlerde uygulanacak ilkeleri belirleyen tavsiye kararları kabul edilmiştir. KVK Kanunu hazırlanırken, kanunun çerçeve niteliğini bozmamak adına bu kararlara kanunda doğrudan yer verilmemiş olsa da göz önünde bulundurulmuştur[143].

Daha sonra BM tarafından, 14 Aralık 1990'da Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri çıkarılmıştır.

Bu süreç içerisinde Avrupa Birliği tarafından, 25 Ekim 1998'de 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin

[143] KVK Kanunu, Genel Gerekçe, par. 19.

Direktif, en son olarak ise 2018 yılında 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) yürürlüğe girmiştir.

Birbirini destekleyici mahiyette olan bu düzenlemelerden bazıları ekonomik menfaat birliğinden hareketle çıkarılmışken bazılarında ise tetikleyici güç kişisel verilerin insan hakları bağlamında korunması amacı olmuştur. Sayılan tüm bu metinler kişisel verilerin korunması konusunda Türk hukukuna etki ve kaynaklık etmektedir.

KVK Kanunu'na yönelik eleştirileri değerlendirebilmek için hem kişisel verilerin korunması sürecini hem de uluslararası hukukta gelinen son noktayı ortaya koymak gerekmektedir. Bu doğrultuda yukarıda kısmen zikredilen OECD, Avrupa Konseyi ve Avrupa Birliği kaynaklı Rehber İlkeler, 108 sayılı Sözleşme ve Avrupa İnsan Hakları Sözleşmesi akabinde ise AB direktifleri ilkeleri çalışmamızın bu kısmında ele alınmaktadır.

B. OECD Rehber İlkeler

Kronolojik açıdan bakıldığında kişisel verilere münhasıran yer veren ilk uluslararası düzenleme, OECD tarafından 1980 yılında çıkarılan ve 2013 yılında güncellenmiş olan Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeler olmuştur.

Söz konusu ilkelerin düzenlenmesinin temel sebebi, ulusal sınırlar arasında ve hatta kıtalar arasında büyük miktarlarda veriye saniyeler içinde hukuka aykırı olarak ulaşan, kopyalayan ve aktarmayı sağlayan otomatik veri işleme sistemlerinin geliştirilmesi nedeniyle kişisel verilerle ilgili gizliliğin korumasının uluslararası ilkelere bağlanması ihtiyacıdır.

Rehber İlkeler düzenlemesinin temel amacı ise, kişisel verilerin gizliliğinin korunmasıyla ilgili asgari standartları belirlemek ve ülkelerin ilgili iç kurallar arasındaki farklılıkları en aza indirerek ülkeler arası ilişkilerde ekonomik çıkarların korunmasını sağlamaktır. Bu yolda, üye ülkelerin aralarındaki kişisel veri akışlarına aşırı müdahaleden kaçınılması

gereğini göz önünde bulundurmalarını sağlamak ve kişisel veri akışını sınırlamadaki farklılıkları mümkün olduğunca ortadan kaldırmak hedeflenmiştir[144].

İlkelerin gerekliliği ile ilgili olarak ise, ulusal mevzuatlardaki eşitsizliklerin üye devletlerin bankacılık ve sigorta gibi ekonominin önemli sektörlerinde ciddi bozulmalara neden oluşu sebebiyle, kişisel verilere ilişkin mevzuata sahip ülkeler için temel ilkeler üzerinde bir uzlaşmayı temsil edeceği ve henüz bir düzenlemeye sahip olmayan ülkeler için de bir temel teşkil edeceği olarak belirtilmiştir[145]. Bu doğrultuda, sınır ötesi kişisel veri akışlarının yeknesaklaştırılmasının hem ekonomik ve sosyal kalkınmaya katkıda bulunması hem de üye ülkeler arasında serbest bilgi akışını ilerletmek, ekonomik ve sosyal ilişkilerin gelişmesine ilişkin haksız engellerin yaratılmasından kaçınmaya çaba gösterilmesi amacıyla çıkarılmıştır. Söz konusu ilkeler, madde 7 ila 14 arasında düzenlenmektedir. Bu ilkeler sırasıyla,

a- Verilerin Toplanmasında Sınır Olması İlkesi,
b- Veri Kalitesi (Toplanan Kişisel Verilerin Kullanım Amacı Doğrultusunda Kullanılması) İlkesi,
c- Belli Bir Amaç Doğrultusunda Toplanma İlkesi,
d- Veri Sahibinin İzni ya da Kanun Yetkisi Doğrultusunda Kullanılabilme İlkesi,
e- Toplanan Kişisel Verilerin Yeterli Güvenlik Tedbirleri Altında Korunması İlkesi,
f- Veri İşlemede Açıklık İlkesi, Veri Sahibinin Veriye Erişim İlkesi ve
g- Sayılan İlkelere Uymayan Veri Sahibinin Sorumluluğu İlkesinden müteşekkildir.

Bu ilkelerin üye devletler açısından kabul edilmeleri zorunlu değil, tavsiye ya da rehber niteliğindedir.

2013 yılında ise Rehber İlkelere ek olarak üç yeni ilke getirilmiştir: İlk ilke, kişisel verilerin korunmasında etkili yasaların getirilme zorunluluğu ile birlikte, günümüzde gizliliğin stratejik öneminin aynı zamanda en üst düzey hükümetlerde koordine edilen çok yönlü bir ulusal strateji gerektirmekte olduğundan ulusal gizlilik stratejilerinin varlığı ilkesidir.

[144] OECD Kişisel Verilerin Gizliliğinin Korunması ve Sınır Aşan Kişisel Verilere İlişkin Kılavuz İlkeler, par. 25.
[145] OECD Kişisel Verilerin Gizliliğinin Korunması ve Sınır Aşan Kişisel Verilere İlişkin Kılavuz İlkeler, Önsöz.

İkinci ilke, kuruluşların gizlilik korumasını uygularken temel operasyonel mekanizma görevi görecek olan gizlilik yönetimi programlarının oluşturulması zorunluluğudur.

Üçüncüsü, veri güvenliği ihlali bildirimi ilkesidir. Bu ilke hem bir otoriteye bildirimi hem de kişisel verileri etkileyen güvenlik ihlallerinden etkilenen bir kişiye bildirimin gerekliliği ifade etmektedir.

Bu rehber ilkeler, hem ilk olması hem de kişisel verilerin korunması hususunda temel ve koruma odaklı geniş bir çerçeve çizmesi sebebiyle oldukça önemlidir. Birazdan göreceğimiz üzere, kendisinden daha sonra çıkarılan ilgili ulusal ve uluslararası belgeler için yol gösterici bir etkiye sahip olmuştur. Keza Türk hukuku açısından da, 6698 sayılı Kanun'un gerekçesinde belirtildiği üzere KVK Kanunu'nun hazırlanmasında bu ilkelerden de yararlanılmıştır.

C. Avrupa Konseyi Belgelerinde Kişisel Verilerin Korunması

1. 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi(VKS)

VKS'yi Türkiye 28.01.1981 yılında imzalamasına rağmen meclis tarafından onaya uygun bulma kanunu tam 35 yıl sonra, 18.02.2016 tarihinde çıkarılmıştır. 01.09.2016 tarihinde yürürlüğe girerek bağlayıcılık kazanan VKS'nin amacı, her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisi ile ilgili kişisel verilerin korunmasını, diğer bir deyişle otomatik işleme tabi tutulan kişisel verilerin sınırlar ötesi akışının yoğunluk kazanması karşısında özel hayata saygı hakkını güvence altına almaktan ibarettir.

VKS sadece gerçek kişilerin kişisel verilerini kapsayıcı nitelikte görünmekle beraber taraf devletlerin VKS'nin kapsamını tüzel kişileri de içine alacak şekilde genişletmesine imkân tanımaktadır[146].

VKS'nin II. Bölümü m. 4 ila 11'de, verilerin korunmasına ilişkin temel kurallar düzenlenmektedir. Bunlardan, otomatik işleme yapılabilecek kişisel verilerin şartları şu şekilde belirtilmektedir:

[146] Bostancı Bozbayındır, Gülşah: "Avrupa Birliği Ceza Hukukunda 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, 2, İstanbul 2018, s. 59.

Kişisel veriler,

> *"a Adil biçimde ve yasal yollardan elde edilir ve işlenir;*
>
> *b Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılamaz;*
>
> *c Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;*
>
> *d Doğru bilgileri yansıtır ve gerektiğinde güncellenir;*
>
> *e Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkân veren bir biçimde saklanır.* "[147]

Zikredilen bu ilke-şartlardan sonra VKS m. 6'da hassas veri kategorileri belirtilerek kişisel verilerin korunmasında daha fazla özen gösterilmesi gerekli olan veri türleri açıklanmaktadır. Buna göre, kişinin ırksal kökeni, siyasi düşünceleri, dini veya diğer inançlarını ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler ve son olarak ceza mahkûmiyeti ile ilgili veriler otomatik işleme tabi tutulamamaktadır.

Hassas veri kategorisi içinde sayılan bu veri türleri hususunda sözleşmenin kesin bir biçimde yasaklama tavrı içerisinde olması dikkat çekicidir. KVK Kanunu ile karşılaştırıldığında hassas veri türlerinin daha dar kapsamlı olduğunu ifade etmek gerekir. Keza KVK Kanunu'nda yukarıda sayılanlara ek olarak kişinin etnik kökeni, felsefi inancı, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği ile biyometrik ve genetik verileri de hassas veri kategorisi içinde sayılmaktadır.

Akabinde m. 7'de, verilerin güvenliğinin sağlanmasında taraf ülkelerin sorumlu olduğunun belirtilmesinden sonra m. 8'de veri sahibi hakkında ek güvenceler sayılmıştır. Söz konusu ek güvenceler kısaca, veri sahibinin kişisel verilerinin işlenip işlenmediğini ve işleyenin kimliğini öğrenmesi, işlemenin hukuka aykırı yapılması halinde işlenmekte olan verilerle ilgili işleme yapan kuruma bildiri, düzeltme veya silme taleplerinde bulunabileceği ve hukuka aykırı işlemenin ortadan kaldırılmazsa yetkili kurumlara başvuru yapabileceği olarak sayılabilir. Görüldüğü üzere söz konusu güvenceler OECD ilkelerinde sayılanlarla oldukça benzeşmektedir.

VKS m. 9'da verilerin korunması hususunda VKS hükümlerine getirilebilecek istisnalar sınırlı bir biçimde sayılmaktadır. Bu doğrultuda, devlet güvenliğinin korunması, kamu

[147] 108 sayılı Sözleşme, m. 5.

güvenliği, devletin mali menfaatleri veya suçların önlenmesi adına yahut ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması adına istisna hükümleri getirilebilir. Fakat bu istisnaların sözleşmeci devletlerin kanunlarında öngörülmüş olması ve demokratik toplumda alınması gerekli bir önlem olması gerekmektedir.

VKS'nin bu haliyle soruşturma evresinde kişisel verilerin işlenmesini doğrudan kapsamı dışında bırakmaması dikkat çekicidir. Bununla birlikte, bu alanı da düzenlemesi amacıyla 1987 yılında sözleşmeye ek Polis Veri Tavsiye Kararı'nı kabul etmiştir. R 87(5) sayılı bu tavsiye niteliğindeki karara göre soruşturma evresinde kişisel verilerin işlenebilmesi mümkün iken bunun kişisel verilerin sınırsız olarak ve herhangi bir ayrıma tabi tutulmadan toplanmaması gerekmektedir[148]. Buna ek olarak, veri sahiplerinin özel yaşamlarına tecavüz tehlikesi bulunmadığının açık olduğu durumlarda, veri sahibinin veriyi işleyenin kimliğini öğrenmenin dışında VKS m. 8'de düzenlenen diğer ek güvencelerinin kanunla sınırlanması da mümkündür. Elbette kanuni sınırlamalara dayanan müdahalelerle korunan haklar arasında belli bir orantının olması gerekmektedir.

Öte yandan çekince koyulamayacağı belirtilen bu sözleşmenin son kısmında Türkiye, VKS'nin m. 3(2)(a), (c) ve 13(2)(a) uyarınca beyanlar koymuş ve kabul ettiği sözleşme ile ilgili bazı açıklamalarda bulunmuştur. Bu beyanlara göre, VKS, gerçek kişilerin tamamen kişisel veya aynı konutta yaşayanlarla ilgili faaliyetlerine ilişkin olarak işlenmesine; kanun tarafından öngörülen kamu kayıtlarına; kanuna uygun olarak kamu bilgisine sunulan bilgilere; devlet kurumlarınca milli güvenlik, savunma ile soruşturma ve suç önleme amacıyla işlenen kişisel verilere uygulanmayacaktır. Ayrıca, VKS'nin otomatik olmayan yollarla işlenen kişisel verilere de uygulanacağı Türkiye tarafından beyan edilerek VKS'nin kullanım alanını Türk hukuku üzerinde genişletilmektedir[149].

Dikkat edilmelidir ki bu beyanlar doğrultusunda soruşturma evresinde kişisel verilerin işlenmesine uygulanması mümkün görünmemektedir. Bu beyanların getirilme amacı sorgulanabilir olsa da, bu beyan tezimizin konusunu doğrudan ilgilendirmekte olduğundan VKS'nin işleme ilkeleri kısmı tezimiz kapsamında soruşturma evresinde uyulması zorunlu bir kaynak olarak gösterilebilecektir.

[148] Bostancı Bozbayındır, s. 60.
[149] Beyanlar kısmında son olarak ise, Kişisel Verileri Koruma Kurulu'nun yetkili makam olduğu beyan edilmiştir.

Ayrıca belirtmek gerekir ki, Avrupa Konseyi'nin 2001 tarihli kişisel verilerin korunmasına ilişkin bir de ek protokolü bulunmaktadır. 20.04.2016 tarihinde TBMM'de kabul edilen ve 6705 sayılı Kanun halini alarak şu an yürürlükte olan bu protokolde iki husus bulunmaktadır. Bunlar, denetleyici makamlar ve verilerin üçüncü ülkelere transferi hakkındadır. Denetleyici makamlarla ilgili olarak bunların, soruşturma ve müdahale yetkilerinin yanı sıra, kanuni takibata dâhil olma ya da verilerin korunmasına ilişkin ilkeleri uygulamaya koyan iç hukuk hükümlerinin ihlallerini yetkili adli makamların dikkatine getirme yetkisine sahip olması istenmektedir. Ayrıca denetleyici makamların görevlerini tam bağımsızlıkla yerine getirmesi gerektiği vurgulanmaktadır.

2. Avrupa İnsan Hakları Sözleşmesi (AİHS)

AİHS, 1950 yılında imzaya açılan, 1951 yılında Türkiye'nin de taraf olduğu ve 1953 yılında yürürlüğe giren, başvuruculara ikincil yargılama imkânı sunan ve uluslararası yaptırıma sahip olan bir sözleşmedir. İçtihat ve kararlarıyla dünya genelinde takip edilmekte olan bir mahkemeye sahiptir. AİHM, önüne gelen uyuşmazlıklarda dinamik yorum olarak adlandırdığı metodu kullanarak günün şartlarına göre AİHS maddelerini yorumlamakta ve içtihatlarını da bu doğrultuda değiştirebilmektedir. AİHS ve AİHM, ülkelerin hukuk sistemlerini ve kurallarını etkileyerek Avrupa Konseyi devletlerinin hukuklarını insan hakları açısından yeknesaklaştıran ve geliştiren bir sözleşmedir. Tezimizin ilerleyen kısımlarında AİHM kararları daha detaylı olarak incelendiğinden burada AİHM'in konuya yönelik yapısal bakış açısı ortaya konulmaktadır.

Bu doğrultuda öncelikle kişisel verilerin son yıllarda artan ihtiyaç sebebiyle özel hayatın gizliliğinden ayrılma eğilimine rağmen kişisel verilerin korunması AİHS kapsamında doğrudan bağımsız bir hak olarak düzenlenmemekte olduğunu belirtmekte gerekir. Bunun sebebi AİHS'in yetmiş yıla yakın bir zaman önce düzenlenmiş olması olabilir. Özel hayatın gizliliğinin korunmasına ilişkin hükümlerin düzenlenmekte olduğu m. 8'de, kişilerin özel ve aile hayatı korunma altına alınmaktayken kişisel veriler lafzı madde içerisinde geçmemektedir[150]. Buradan hareketle kişisel verilerin AİHS kapsamında

[150] AİHS m. 8'e göre: *"1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. 2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."*

korunmamakta olduğu düşünülmemelidir. Çünkü konusu kişisel verilerin korunması olan birçok başvuruda AİHM, kişisel verilerin korunmasını özel ve aile hayatına saygı hakkı maddesi bağlamında ele almakta ve içtihadını bu madde bağlamında geliştirmektedir.

AİHM, kişisel veriden ziyade özel hayat verisi olabilecek verilerin tanımını yahut kapsamını belirleyebilme çabası içindedir ve özel hayat verilerini sınırlı olarak sayılamayacağı düşüncesindedir. Ayrıca, kimliği belirleyen yahut belirlenebilir kılmayı sağlayan her türlü özel hayat verisinin kişisel veri olacağı çeşitli AİHM kararlarında yer almaktadır. Örneğin, bu doğrultuda önüne gelen bir başvuruda kişilerin, parmak izlerini, DNA profillerini ve hücre örneklerinin oluşturduğu verileri açıkça kişisel nitelikli veriler olduğunu belirterek bir Avrupa Konseyi belgesi olan VKS'ye atıfla verilerin veri sahiplerinin kimliği belirlemeye ya da belirlenebilmeye imkân sağlıyor olup olmadığını araştırmıştır[151].

Başka bir başvuruda, bir Avrupa Birliği belgesi olan 95/46/EC sayılı Direktifine atıfta bulunan AİHM'e göre, kişisel veriler, özellikle, bir kimlik numarasıyla veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel ve sosyal kimliğine özgü bir veya birden fazla faktörle doğrudan veya dolaylı olarak kişiyi tanımlayan veriler olarak ifade edilmiştir[152].

Bir başka başvuruda, banka evraklarından elde edilen bilgilerin, hassas bilgi veya mesleki işlemlerle ilgili bilgi olup olmadığına bakılmaksızın, kişisel veri niteliği taşımakta olduğu belirtmektedir[153]. Ayrıca, elektronik verilerin korunmaya daha çok muhtaç olduğu da ifade edilmektedir[154]. Dolayısıyla, tüm bu örneklerden hareketle, VKS ve 95/46/EC sayılı Direktif'teki kişisel veri tanımının AİHM tarafından kararlarında referans alınmakta olduğunu belirtmek gerekir.

AİHM'in, kişisel verinin kapsamını belirlemede kullandığı ölçütlerden biri, verinin işlenmesinin arkasında yatan amacın kişisel veri sahibini tespit etmek olup olmadığıdır. Örneğin, kişilerin IP adresleriyle ilişkili abone bilgilerinin, belirli bir kişiyi tespit etmeyi sağladığından IP adresi kişisel veriler arasında sayılmaktadır[155]. Diğer ölçütler ise,

[151] S. ve Marper/Birleşik Krallık, par. 68.
[152] Benedik/Slovenya, par. 53.
[153] M.N. ve Diğerleri/San Marino, Başvuru No: 28005/12, 07.07.2015, Erişim Tarihi: 1 Mayıs 2019.
[154] Delfi AS/Estonya, par 24.
[155] Benedik/Slovenya, par 109.

verilerin kişinin belirlenmesi sağlayan unsurlar olarak en azından yansız, tarafsız ve çürütülemeyecek nitelikte olmalarıdır[156].

Öte yandan, AİHS m. 8(2) uyarınca kişisel verilerin korunmasına yönelik olarak getirilebilecek sınırlamalar bulunmaktadır. Bu doğrultuda hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilmektedir.

AİHM'in kararlarına esas aldığı Veri Koruma Direktifi'nin polis ve ceza adaleti alanında uygulanma kabiliyeti bulunmamakta olduğu da belirtilmekte olduğundan, AİHM'in kişisel verilerin korunmasına ilişkin AİHS'in uygulanmayacağı düşüncesinde olduğu düşünülebilir[157]. Keza bu doğrultuda AB 2008/977/JHA sayılı Adli Konularda Polis ve Adli İşbirliği Çerçeve Kararı'na göre de, 95/46/EC sayılı Direktif kuralları kamu güvenliği, devlet güvenliği veya devletin ceza hukuku alanındaki faaliyetlerinde uygulanmayacağı düzenlenmektedir. Fakat çerçeve kararın, suçun soruşturulması amacıyla yetkili makamlarca kişisel verilerin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin 2016/680/EU sayılı Direktif'in yürürlüğe girmesiyle ortadan kalkmasıyla bu gerekçenin geçerliliği kalmamıştır. Dolayısıyla, beklendiği üzere AİHM'in bu konudaki eğiliminin kişisel verilerin soruşturma evresinde korunmasına yönelik olacağı sürpriz olmayacaktır.

D. Avrupa Birliği Belgelerinde Kişisel Verilerin Korunması

1. Genel olarak

Avrupa Birliği veri koruma hukukunun tarihsel gelişimine göre, kişisel verilerin korunmasına yönelik ilk ve kapsamlı düzenleme 1995 yılına ait 95/46/EC sayılı Direktif'tir. Bu Direktif'in yanı sıra kişisel veriler ile ilgili ticari sektör bazlı olarak abonelerin kişisel verilerinin korunmasına yönelik hüküm barındıran 2002/58/AT sayılı Elektronik Haberleşme Yönergesi, 2006/24/AT sayılı İletişim Trafik Verilerinin

[156] S. ve Marper/Birleşik Krallık, par 81.
[157] Benedik/Slovenya, par. 53.

Saklanması Yönergesi ve soruşturma evresine ilişkin hükümler içeren 2008/977/JHA sayılı Adli Konularda Polis ve Adli İşbirliği Çerçeve Kararı gibi tamamlayıcı hukuk metinleri de bulunmaktadır[158]. Bunun dışında 95/46/EC sayılı Direktif m. 29 uyarınca kurulan Madde 29 Veri Koruma Çalışma Grubu da, direktif maddelerini yol gösterici olarak yorumlamakta ve kişisel verilerin işlenmesine yönelik gelişen koşullara göre çeşitli önerilerde bulunmaktaydı.

Öte yandan, 2000 yılında çıkarılan Avrupa Birliği Temel Haklar Şartı m. 8'de kişisel verilerin korunmasını özel ve aile yaşamına saygıdan bağımsız olarak düzenleyerek kişisel verileri doğrudan koruma altına almıştır[159]. Ayrıca, Avrupa Birliğinin İşleyişi Hakkında Antlaşma(2007) m. 16'da da herkesin, kendisiyle ilgili kişisel verilerin korunması hakkına sahip olduğu belirtilerek kişisel verilerin korunması hakkı güvence altına alınmıştır[160].

Nihayet, AB sınırları içerisindeki hükümleri yeknesaklaştırmak amacıyla dağınık vaziyetteki hükümleri toplayan ve geliştiren GDPR 2016 yılında çıkarılmıştır. 2018 yılında yürürlüğe giren GDPR, günümüzde AB hukukunu neredeyse evrensel olarak uygulanacak hükümler barındırması sebebiyle kişisel verilerin korunması hususunda dünya genelinde yollama yapılan bir hukuk metnidir. GDPR öncesinde 1995 yılından itibaren kişisel verilerin korunmasına ilişkin tüm düzenlemelerin önleyici müdahale yapısında olduğu belirtilmektedir[161].

GDPR'la aynı gün, suçun önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması amacıyla yetkili makamlarca kişisel verilerin işlenmesi ile ilgili gerçek kişilerin korunmasına ilişkin olarak 2016/680/EU sayılı ve 27 Nisan 2016 tarihli bir direktif daha çıkarılmıştır. Bu direktifle de GDPR'ın kişisel verilerin korunmasını genel mahiyetiyle düzenlemesi sebebiyle ceza muhakemesine bakan yönünün özelleştirilmekte ve tezimiz

---

[158] Oğuz, Habip. 2014. "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum." Çağ Üniversitesi Elektronik Ticaret Hukuku Sempozyumu, Tarsus, 25 Nisan 2014, s. 10.

[159] AB Temel Haklar Şartı'nda kişisel verilerin korunması hakkı m. 8'de düzenlenmektedir:
"1. Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.
2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir. 3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir."

[160] Van Ooik, Ronald/Vandamme, Thomas: European Basic Traties, Deventer 2013, s. 28.

[161] Henkoğlu, s. 105.

bağlamında oldukça önem arz etmektedir. Son olarak aynı gün yine bu doğrultuda terör suçlarının ve ağır suçların önlenmesi, tespiti, soruşturulması ve kovuşturulmasına ilişkin yolcu isim sicili (PNR) verilerinin kullanımı hakkında 2016/681/EU sayılı ve 27 Nisan 2016 tarihli bir başka direktif daha çıkarılmıştır. Bu direktifle de terör olaylarını engelleyebilmek adına alınabilecek önlemlerle kişisel verilerin korunması hakkı arasında dengeleyici bir düzenleme oluşturmak istenmiştir.

Tüm bu AB düzenlemeleri varlığı, gelişim süreci ve en güncel hallerinin yakın tarihlerde yürürlüğe girmiş olmaları sebebiyle, kişisel verilerin korunması hakkına ilişkin evrensel hukuk literatürü AB hukukundan oldukça etkileniş bir pozisyona gelmiştir. Hatta 11 Eylül 2001'den oldukça olumsuz etkilenen Amerikan hukukundaki kişisel verilerin korunması hükümlerine göre Avrupa Birliği hukukunun kişinin kişisel verilerin korunmasında açık ara önde olduğu da ifade edilmektedir[162]. AB metinleri ile AK metinleri karşılaştırıldığında ise AB düzenlemelerinin tüm birlik güvenliğini, AK metinlerinin ise ülkelerin ulusal güvenliğini esas alacak şekilde düzenlediği görülmektedir[163].

Bu kısımda, doğrudan kişisel verilerin hakkının korunmasına yönelik düzenlenen 95/46/EC sayılı Direktif, GDPR ve 2016/680/EU sayılı Direktif soruşturma evresinde kişisel verilerin işlenmesine ilişkin olarak detaylıca değerlendirilmektedir.

2. 95/46/EC sayı ve 24 Ekim 1995 tarihli Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki AB Konseyi ve Parlamentosu Direktifi

a) Genel olarak

95/46/EC sayılı Direktif, KVK Kanunu'nun yapım sürecinde dayanak norm olarak ele alınmıştır. Her ne kadar bu Direktif'in yerini 2018 yılından beri GDPR almış olsa da KVK Kanunu'nu nasıl etkilediği görmek açısından Direktif'te düzenlenen korumaya ilişkin hususları incelemek gerekmektedir. Bu noktada 95/46/EC sayılı Direktif'in bilhassa eksik yönlerini ortaya koymak bu Direktif doğrultusunda hazırlanan KVK Kanunu'nun, GDPR'a göre eksikliklerini de ortaya koyacağından Türk hukuku açısından oldukça önemlidir.

[162] Hayes, Darren R.: A Practical Guide to Computer Forensics Investigations, New Jersey 2014, s. 279.
[163] Bostancı Bozbayındır, s. 56.

Kişisel verilerin akışındaki engelleri kaldırmak ya da diğer bir deyişle kişilerin hak ve özgürlüklerinin korunma seviyesinin bu tür verilerin işlenmesine ilişkin olarak tüm üye devletlerde eşit olması AB iç pazarı için hayati öneme sahip olarak görülmektedir[164]. Bu doğrultuda Direktif'in getirilmesinin temel amacı, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini korumaktır[165].

Bir diğer amaç ise kişilerin ekonomik ve sosyal ilerlemesine, refahına ve ticari genişlemeye katkıda bulunacak olan kişisel veri işleme sistemlerinin insana hizmet etmek üzere tasarlanmasıdır. Bu açıdan, gerçek kişilere ilişkin ses ve görüntü verilerini yakalamak, iletmek, değiştirmek, kaydetmek, saklamak veya nakletmek için kullanılan teknolojilerin, bilgi toplumu çerçevesinde devam eden gelişmelerinin önemi dikkate alındığında, belli kurallara bağlanması ihtiyacına yönelik çıkarılmıştır. Doktrinde, yöntemine bakılmaksızın kişisel verilerin bu madde ile tüm işleme faaliyetlerini kapsaması ve spesifik bir sektör ya da kullanım alanı ile sınırlı olmaması direktifin en ilgi çekici özelliği olarak görülmektedir[166]. Hemen belirtmek gerekir ki, Direktif'in ekonomik ilişkilerin korunması amacının temel amaç olarak açıkça öngörülmesi geçen yıllar içerisinde kişisel verilerin korunması hususunun ana ekseninin artık bir insan hakkı oluşuna kaydığını göstermektedir.

Direktifin kapsamı bir dosyalama sisteminin parçasını oluşturması istenen veya oluşturan kişisel verilerin otomatik araçlar olsun veya olmasın işlenmesini içermektedir. Buna karşın, ceza hukuku alanındaki devlet faaliyetleri hakkında; devlet güvenliği, savunma, kamu güvenliğine ilişkin verilerin işlenmesinde; aynı evde yaşayan kişilerin birbirlerinin kişisel verilerini işlemelerinde uygulanmamaktadır. Hatta devletin ekonomik refahını güvenceye almak için gerekli olan verilerin işlenmesi, güvenlik konularıyla ilişkili olduğunda Direktifin kapsamı içerisinde korunmamaktadır[167]. Fakat bu yönelim, Madde 29 Veri Koruma Çalışma Grubu tarafından eleştirilmekte, kişisel verilerin soruşturma evresinde kamu gücü kullanılarak elde edilmesine yönelik, en azından genel ilkelerin

[164] 95/46/EC sayılı Direktif, Gerekçe, Giriş.
[165] 95/46/EC sayılı Direktif, m. 1.
[166] Gür, İkbal: Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Ankara 2010, s. 27.
[167] 95/46/EC sayılı Direktif, Gerekçe, par. 13.

uygulama alanı bulması savunulmaktadır[168]. Bu açıdan, VKS gibi bu Direktif de içerdiği korumaya ilişkin ilkeler yönünden tezimiz kapsamında uygulanması zorunlu hükümler kapsamında yer almaktadır.

Direktif'te veri işlemeyi yasallaştırma kriterleri adı altında hukuka uygunluk sebepleri sayılmaktadır[169]. Buna göre hukuka uygun bir işlemenin varlığı için veri öznesinin açık, kesin ve net bir biçimde rızasını vermiş olması kuraldır. Bu kuralın çeşitli istisnaları bulunmaktadır. İşlemenin, denetleyicinin yasal yükümlülüğü gereğince işleme yapıyor olması ilk yer verilen istisnadır. Bir diğer istisna ise, işlemenin, verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu makamının uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekli olması halidir. Son istisna ise, veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çiğnemesi haricinde, verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen meşru menfaatlerin amaçları için gerekli olması halidir.

b) Kişisel verilerin işlenmesinin esasına ilişkin ilkeler

Direktif'te işleme tabi tutulacak kişisel veriler ile ilgili ilkeler belirtilmektedir[170]. Bu ilkelerin hepsinde hâkim olan temel husus, işlenecek verilerin adil ve yasalara uygun olarak işlenmesi zorunluluğudur.

---

[168] Madde 29 Veri Koruma Çalışma Grubu, 16/EN WP 237, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), Adopted on 13 April 2016, s. 6. Belgede, soruşturma evresinde veri işlenmesine özellikle şu ilkelerin hakim olması gerektiği belirtilmektedir: İşlem, açık, kesin ve erişilebilir kurallara dayanmalıdır; izlenen meşru hedeflerle ilgili gereklilik ve orantılılık gösterilmelidir; bağımsız bir gözetim mekanizması bulunmalıdır; bireye etkin çözümler sunulması gerekir.

[169] Yasallaştırma kriterleri 95/46/EC sayılı Direktif m. 7'de düzenlenmektedir:
"(a) Veri öznesi açık, kesin ve net bir biçimde rızasını vermişse veya
(b)İşleme, bir sözleşme yapmadan önce veri öznesinin talebi üzerine önlem almak için ya da veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekliyse veya
(c) İşleme denetleyicinin konusu olan bir yasal yükümlülüğe uyum için gerekirse, veya
(d)İşleme, veri öznesinin hayati menfaatlerini korumak için gerekliyse; veya
(e)İşleme, verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu makamının uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekliyse; veya
(f) İşleme, bu tür menfaatlerin, madde 1 (1) kapsamında koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çiğnemesi haricinde, verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen meşru menfaatlerin amaçları için gerekliyse."

[170] Veri kalitesi hükmü 95/46/EC sayılı Direktif m. 6'da düzenlenmektedir:
"(a) adil ve yasal olarak işlenmiş;
(b) belirli, açık ve meşru amaçlar için toplanmış ve bu amaçlarla uyumsuz biçimde başkaca işlenmemiş. Üye Devletlerin uygun korunma önlemleri sağlaması koşuluyla; tarihsel, istatistiksel veya bilimsel amaçlar için verilerin detaylı işlenmesi; uyumsuz olarak kabul edilmeyecektir;

Birinci ilke kişisel verilerin belirli, açık ve meşru amaçlar için toplanmış olması ve bu amaçlarla uyumsuz biçimde işlenmemiş olmasıdır. Bu ilke, işlemenin amaca uygun ve bağlı olması olarak ifade edilebilir. Amacın belirli olması işleme faaliyetinin hangi nedenle ve hangi sınırlar dâhilinde verilerin toplanmakta ve işlenmekte olduğunu göstermektedir[171]. Amacın açıklığı işleme faaliyetinin belirsizliğe yol açmayacak şekilde hukuk kurallarıyla gösterilmesidir. Meşru amaçtan anlaşılması gereken ise, AB 29 Çalışma Grubu'na göre amacın başta tüm pozitif hukuk kurallarına ve kişisel verilerin işlenmesine ilişkin genel ilkelere uygun olmasıdır[172]. Bu yüzden soruşturma evresinde işlenen kişisel verilerin belirli, açık ve meşru nitelikleri haiz amaçlar doğrultusunda olmalıdır.

İkinci ilke, verilerin toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterli ve ilgili olarak öngörülen amacı aşmıyor olmasıdır. Bu ilkenin amacı, işlenecek verinin sadece istenen amaç doğrultusunda illiyet bağını sağlıyor olmasını ifade etmektedir[173]. Buna göre, veri sorumlusu amacına ulaşmak için gerekli olandan fazla veri temin etmemeli ve elde ettiği verilerin bir kısmını kullanarak amaca ulaşabiliyorsa fazlasını kullanmamalıdır[174]. Soruşturma evresinde veri işleyicileri ve kontrolörlerin verileri toplayıp işlerken suç ile doğrudan bağlantısız ve gereksiz kişisel verileri de işlememesi bu açıdan önem arz eder.

Üçüncü ilke, ilgili amaç doğrultusunda irtibat kurularak geçici olarak işlenen kişisel verilerin doğru ve güncel tutulmasını ifade etmektedir. İster soruşturma evresinde toplanarak elde edilen isterse başka yollarla elde edilmiş verilerin soruşturma evresinde

---

(c) toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterlidir, ilgilidir ve bu amacı aşmaz;
(d) doğrudur ve gerektiği yerde güncel tutulur. Toplanma ve sonrasındaki işlenme, silinme veya düzeltilme amaçlarını göz önünde tutarak verilerin yanlış veya eksik olmamasını sağlayacak tüm makul önlemler alınmalıdır;
(e) verilerin toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca, veri öznelerinin tespitine izin veren biçimde tutulur. Üye Devletler, tarihsel, istatistiksel veya bilimsel kullanım amacıyla daha uzun süreli depolanan kişisel veriler için uygun koruma önlemleri alacaktır."

[171] Başalp, s. 38.

[172] Oturaklı, Alper(Karaduman, Şebnem S./Karayazgan, Ahmet/Esatoğlu, Yahya Tekin/Süzel, Cüneyt): Sigorta Hukukunun Bazı Güncel Sorunları, İstanbul 2017, s. 19.

[173] Başalp s. 38.

[174] Develioğlu, Hüseyin Murat: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017, s. 47.

işlenmesinde veriler gerçeği yansıtmalı ve güncel nitelikte olmalıdır. Özellikle depolanan veriler ile ilgili önem arz eden bir ilkedir.

Son ve dördüncü ilke, verilerin toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca, veri öznelerinin tespitine izin veren biçimde tutulmasıdır. Bunun anlamı ise saklama süresinin aşılmayarak verilerin depolanmamasıdır. Fakat bu verilerin süre aşımı yapıldığı halde de anonimleştirerek saklanması mümkündür. Soruşturma evresinde işlenen veya işin gereğince veri tabanlarından çekilen verilerin saklama süresi çerçevesinde kullanılıyor olmasına dikkat edilmelidir. Aksi halde hukuka aykırı yollardan elde edilmiş olan verilerin kullanılması söz konusu olacaktır. Bu doğrultuda Avrupa Birliği Adalet Divanı, terör suçlarıyla mücadele edilmesi için kişilerin internete nereden, ne zaman ve ne sıklıkla girdiklerinin bilgisinin altı aydan iki yıla kadar internet sağlayıcılarında saklanabilmesine olanak sağlayan 2006/24/EC sayılı Direktif'i orantılı olmadığı gerekçesiyle iptal etmiştir[175].

Esas açısından ilkeler ile ilgili ifade özgürlüğü ve kişisel verilerin işlenmesi hususundaki özel bir hükme de yer verilmektedir. Buna göre, kişisel verilerin ifade özgürlüğünü yöneten kurallarla kişisel gizlilik hakkını uzlaştırmak için gerekirse, yalnızca, edebi veya sanatsal açıklama amacı veya gazetecilik amaçları için kişisel verilerin işlenmesinde ulusal hukuklarca getirilebilecek muafiyetler söz konusu olabilecektir[176]. Buna karşılık, soruşturma evresinde elde edilen verilere yönelik uygulanacak bu muafiyetlerin, verilerin saklama süresine ve güncel olmasına dikkat edilmelidir. Ayrıca, diğer tüm ilkeleri hiç uygulanmayacak çerçeveye indirgeyecek bir muafiyet uygulamasından da kaçınılmalıdır.

Direktif'te veri öznesi olarak kişisel verileri işlenen kişiye tanınan haklar da bulunmaktadır. Bunlar verisi işlenen kişinin kural olarak haberdar edilmesi; kişinin işlenen verisine ilişkin olarak bilgi edinme, düzeltilmesini veya silinmesini isteme haklarına ve işlemeye itiraz hakkından ibarettir. Geçmiş döneme ait bir düzenleme olması sebebiyle, güncel düzenlemelerde yer verilen haklara kıyasla daha dar kapsamlı olduğunu ifade etmek gerekir.

[175] Bostancı Bozbayındır, s. 54.
[176] 95/46/EC sayılı Direktif, m. 9.

Öte yandan, hassas verilerin işlenmesi kural olarak yasaklanmıştır[177]. Bu kuralın istisnaları bazı hallere özgülenmektedir[178]. Buna göre, üye devletin kanunlarının belirtmesi şartıyla, bu verilerin işlenmesinde veri öznesi açık rızasını vermesi ilk istisna hükmüdür.

Burada rıza kavramının unsurları, rızanın kesin, spesifik ve bilinçli olarak veri öznesinin özgür iradesine dayanması ve rıza öznesinin rızasını geri olma hakkı da olmasıdır[179]. Bu açıdan seçim özgürlüğünün altını oyan "al ya da bırak" gibi yaklaşımlar ilerlemek için mecburi verilen rızanın özgür irade ile verilmemesine yol açmaktadır[180]. İkinci istisna, kanununda yetkilendirilmesi şartıyla denetleyicinin yükümlülüklerini yerine getirme amacı için gerekli olmasıdır. Üçüncü öne çıkan istisna hükmü ise, veri öznesi tarafından açıkça halka duyurulan verilere ilişkinse ya da kanuni hakların tesisi, yerine getirilmesi veya savunulması için gerekli olması halidir. Bu sayılan hallerin varlığında verilerin işlenmesinin yasaklanması şart değildir. Ayrıca, önemli kamu menfaati nedenleri için, ya ulusal yasa ya da denetleme makamının kararıyla istisnanın istisnasına ek olarak muafiyetler koyulabilmesi de mümkündür.

Son öne çıkan istisna hükmüne göre ise, suçlara, adli hükümlere veya güvenlik tedbirlerine ilişkin verilerin işlenmesi yalnızca resmi makamın kontrolü altında yapılabilmektedir. Ayrıca uygun özel koruma önlemleri sağlanırsa ulusal hükümler kapsamında değişiklikler söz konusu olabilmektedir. Ancak, adli hükümlerin kaydının yalnızca resmi makamın kontrolü altında tutması gerekmektedir.

---

[177] Direktif m. 8'de hassas verilerin kategorilerini düzenlemektedir. Buna göre, üye devletlerin sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini kural olarak yasaklamaları gerekmektedir.

[178] İstisna halleri 95/46/EC sayılı Direktif m. 8'de düzenlenmektedir:
"a) Üye devlet kanunlarının belirtmesi şartıyla, bu verilerin işlenmesinde veri öznesi açık rızasını vermesi;
b) İstihdam kanununda yetkilendirilmesi şartıyla denetleyicinin yükümlülüklerini ve özel haklarını yerine getirme amacı için gerekli olması;
c) Veri öznesinin rızasını vermesinin fiziksel veya yasal olarak elverişsiz olduğu durumda, diğer bir kişinin veya veri öznesinin hayati menfaatlerini korumak için gerekli olması
d) Veri öznelerinin rızası olmaksızın verilerin üçüncü şahıslara açıklanmadığı ve işlemenin yalnızca amaçlarıyla bağlantılı olarak düzenli iletişimde oldukları kişileri veya kuruluş mensuplarını ilgilendirmesi koşuluyla bir vakıf, dernek veya siyasi, felsefi, dini veya ticaret birliği amaçlı başka bir kar amacı gütmeyen kuruluş tarafından uygun teminatlı meşru faaliyetler esnasında yapılması,
e) Veri öznesi tarafından açıkça halka duyurulan verilere ilişkinse ya da kanuni hakların tesisi, yerine getirilmesi veya savunulması için gerekli olması."

[179] Gürsel, İlke: İşçinin Kişisel Verilerinin Korunması Hakkı, Ankara 2016, s. 139-144.

[180] Madde 29 Veri Koruma Çalışma Grubu, 16/EN WP 240 Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), s. 16.

Bir görüşe göre Direktif'in bu fıkrasından çıkarılması gereken, somut olayla ilgili olması ve hassas verilerin işlenmesinde ilgili kişilere verilecek garanti ile gerçekleştirilecek işlem arasında orantı olması kaydıyla soruşturma sürecinde kişisel verilerin işlenmesi mümkün olduğudur[181].

Muafiyet ve sınırlamaların düzenlendiği m. 13'e göre, ceza gerektiren suçların önlenmesi, incelenmesi, tespiti ve kovuşturulması nedeniyle Direktif'te yer alan haklar ülkeler açısından sınırlandırılabilmektedir. Fakat ifade edildiği üzere, ülkelerin buradaki takdir payı, Direktif'te yer alan temel ilkelere dokunmamalıdır[182].

O dönemde, soruşturma evresinde kişisel verilerin işlenmesine yönelik 2008/977/JHA sayılı Adli Konularda Polis ve Adli İşbirliği Çerçeve Kararı çıkarılmıştır. Yine de sadece verilerin transferine ilişkin hükümler getirmesi sebebiyle kişisel verilerin soruşturma evresinde yeterince koruyan bir metin olmamıştır. Bu yüzden Avrupa Adalet Divanı, 08.04.2014 tarihinde Direktif'in özellikle uzun süre depolama imkânı tanıması ve soruşturma evresini hakkın özüne dokunacak bir sonuca çıkacak şekilde tamamen istisna kapsamına bırakılabilmesini öngörmesi nedeniyle orantısız olduğuna hükmetmişir[183].

c) Kişisel verilerin işlenmesinin usulü hakkında ilkeler

95/46/EC sayılı Direktif'te kişisel verilerin işlenmesindeki usule dair de ilkeler bulunmaktadır. Bu ilkeler, verinin esasına ilişkin işleme ilkelerinin tutarlılık kazanması için büyük önem arz etmektedir.

Söz konusu ilkelerin birincisi, işlemenin gizliliğidir[184]. Buna göre, kişisel verilere erişme hakkı olan işleyicinin kendisi de dâhil olmak üzere, işleyicinin veya denetleyicinin yetkisi altındaki herhangi bir kişi, bunu yapması kanun tarafından istenmezse, denetleyicinin talimatı haricinde verileri işlememelidir. Soruşturma evresinde işlenen verilerin gizliliği esas olmalıdır. Fakat bu tutum süresiz ve mutlak olacak şekilde uygulanması hak ihlallerine davetiye çıkaracağından soruşturmanın devam etmemesi yahut kovuşturma evresinde geçildiğinde veri öznelerine yönelik bu gizliliğin kaldırılması önem arz etmektedir.

[181] Özdemir, s. 130, 133.
[182] Başalp, s. 50.
[183] Dülger, 2019, s. 332.
[184] 95/46/EC sayılı Direktif, m. 16.

İkinci ilke, işlemenin güvenliği ilkesidir[185]. Buna göre, kanuni güvence ve sınırların dışına çıkacak bir işleme faaliyetini önlemek için, uygulamalarının durum ve maliyetini dikkate alarak, korunacak verinin yapısına ve işleme tarafından sunulan risklere uygun seviyede bir güvenlik sağlayacak şekilde görevli kişilerin tedbir alması gerekmektedir. Kişisel verilerin gizliliği hakkının soruşturma evresinde tesis edilebilmesi adına devletin pozitif yükümlülüğü bulunmaktadır. Aksi halde gerçekleşen zararlar için tazminat sorumluluğu gündeme gelmelidir.

Son ilke ise, denetleme makamına bildirimde bulunma yükümlülüğüdür[186]. Buna göre, kişisel veri işleyen veri sorumlularının işleme faaliyetine başlamadan önce verilerin korunması ile ilgili denetleyici kuruma kural olarak bildirim yapılması zorunludur. Tezimiz açısından belirtmek gerekir ki, m. 18(5) uyarınca kişisel verileri kapsayan otomatik olmayan işleme faaliyetlerinin bildirilmesinin taraf ülkelerin takdirinde olacak şekilde hem şart koşulabileceği hem de bu işleme faaliyetlerinin basitleştirilmiş bildirime tabi olabileceği düzenlenmesi önemlidir. Çünkü soruşturma evresinde işlenen veriler, otomatik olmayan yollarla işlenen veridirler ve bu halde işleme faaliyetlerinin basitleştirilmiş bildirime tabi olması yani bir bakıma bildirimden muaf tutulmasına imkan verilmektedir.

3. 2016/679/EU sayılı ve 27 Nisan 2016 tarihli Genel Veri Koruma Tüzüğü (GDPR)

a) Genel olarak

95/46/EC sayılı Direktif'in yerine 2016 yılında getirilen GDPR (General Data Protection Regulation), Avrupa Birliği hukukunda veri gizliliği konusunda 21. yüzyılda şu ana kadar yapılan ve çok ses getiren bir düzenlemedir. 25.05.2018 yılında yürürlüğe giren bu düzenleme, kişisel mahremiyetin korunması ve ihlallerin önlenmesi hususunda hemen hemen her ekonomik sektörü etkileyen kapsamlı hükümler içermektedir[187]. 95/46/EC sayılı Direktif ile kısaca mukayese edildiğinde, Türkiye'nin temel aldığı 95/46/EC sayılı Direktif'in niyet belirten, dikkat çekmeye çalışan, cezalandırma yönü ağır basmayan nispeten çerçeve niteliği taşıyan bir düzenleme olarak ülkelere kendi düzenlemelerini

[185] 95/46/EC sayılı Direktif, m. 17.
[186] 95/46/EC sayılı Direktif, m. 18.
[187] Hert, Paul/Papakonstantinou, Vagelis: "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection Of İndividuals", The Computer Law & Security Review, 28, İngiltere 2012, s. 131.

kendi ihtiyaçları doğrultusunda hazırlama imkânı sunmakta olduğunu ifade etmek gerekir[188]. Ayrıca GDPR ile Madde 29 Çalışma Grubu'nun çalışmaları durdurularak yerine Avrupa Veri Koruma Kurulu kurulmuştur.

Veri gizliliği hususunda Avrupa Birliği mevzuatında temel norm niteliğinde olan bu belge, şirketlerin, kişilerin kişisel verilerini nasıl koruyacağı göstermenin yanı sıra büyük ölçüde benzediği 95/46/EC sayılı Direktif'te yer almayan yeni düzenlemeler de içermektedir. 95/46/EC sayılı Direktif üzerine yukarıda detaylı inceleme yaptığımızdan dolayı, tezimizin bu kısmında GDPR'ın getirdiği yeniliklerden öne çıkan hususlar incelenmektedir. Tezimizin ilerleyen bölümlerde yeri geldiğinde bu kısımdaki yeni düzenlemelere atıfta bulunulacaktır.

b) Getirdiği yeniliklerden öne çıkan hususlar

GDPR'ın birinci öne çıkan özelliği, kişisel verilerin hem koruma kapsamının hem de yer yönünden uygulama alanının oldukça genişletilmiş olmasıdır. Bu doğrultuda, uygulanabilirliği neredeyse evrensel düzeye çıkarılmış olarak, AB'ye üye olan ve artık üye olmayan ülkelerin de uymalarını gerektirecek sıkı kurallar getirmektedir. Bunun sebebi, AB üyesi olmayan ülkelerdeki ticaret şirketlerinin AB ile ilişkili faaliyetleri sebebiyledir.

Kapsamın düzenlendiği m. 2'ye göre, GDPR, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya oluşturması amaçlanan araçlarla işlenmesine uygulanır. Yani en az dosyalama amacıyla işlemenin varlığı, GDPR kapsamında bir korumanın gündeme gelebilmesi için yeterlidir.

Öte yandan, yer yönünden uygulama alanı da genişletilmiştir. Önceki düzenlemede problemlere yol açan bu husus Avrupa Birliği Adalet Divanı'nda davaların açılmasına sebep olmaktaydı. GDPR m. 3 ise çok açık olarak düzenlemenin uygulama kapsamını belirlemiştir. Buna göre, bu belge, işleme faaliyetinin AB sınırları içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, AB içerisinde yer alan bir kontrolör veya işleyicinin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanmaktadır.

[188] Oturaklı, s. 15.

GDPR ayrıca, yerleşim yeri AB dışında olan bir gerçek veya tüzel kişi tarafından AB vatandaşlarının kişisel verilerinin işlenmesinde ve AB vatandaşlarına mal veya hizmet sunumuyla ilgili faaliyetlerinde uygulanmaktadır. Üstelik AB vatandaşlarının verilerini işleyen AB dışı işletmelere de AB'de bir temsilci atama zorunluluğu da getirilmiştir. Örneğin, Avrupa'daki Türklere internet ve TV başta olmak üzere herhangi bir iletişim kanalından ürün satma amacı güden Türk firmalarının kişisel verilerin işlenmesi politikalarının GDPR'a uygun olması gerekmektedir. Bu kuralların hem denetleyiciler hem de işlemciler için geçerli olduğuna dikkat edilmelidir. Bunun yanı sıra bulut teknolojisinin(cloud), GDPR'ın kapsamı içerisinde yer aldığı unutulmamalıdır[189].

İkinci önemli değişlik ise idari para cezası yaptırımı konusu ile ilgilidir. GDPR m. 83'te detaylı olarak düzenlenen hükümlerde kademeli idari para cezası yaklaşımı benimsenmiştir. Farklı hükümlere aykırılıkta farklı cezaların düzenlendiği bu maddede, GDPR'a aykırı teşebbüsler, bir önceki mali yılın yıllık dünya çapındaki cirolarının %4'üne veya 20 milyon Euro'ya[190] kadar para cezasına çarptırılmaktadır. Tahmin edilebileceği üzere, bu miktarlar en ciddi ihlaller için uygulanabilecek en yüksek para cezasıdır.

Üçüncü önemli değişiklik ise veri sahibinin rızası ve rızanın usulü ile ilgilidir. 95/46/EC sayılı Direktif'e oranla veri sahiplerinden alınacak olan rızanın koşulları daha sıkı şartlara bağlanmıştır. GDPR m. 7'ye göre, veri sahibinin rızasının yazılı bir beyan bağlamında verilmesi durumunda, rıza talebinin diğer hususlardan açık bir şekilde ayırt edilebilir, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulması gerekmektedir. Dolayısıyla özellikle ticari amaçlı internet sitelerinin ve tüzel kişilerin artık uzun okunaksız şartlarla donatarak düzenledikleri ve tüketiciye sundukları rıza formlarının hukuki geçerliliği olmayacaktır.

Ayrıca bu madde bağlamında artık veri sahibinin işlemeye rıza vermeden önce bu hususta nasıl bilgilendirileceği hükme bağlandığından, hem rıza talebinin hem de onayın veri işlenmesi amacı doğrultusunda olduğunun anlaşılır ve kolay erişilebilir bir biçimde olması gerekir. Yine maddede ifade edildiği üzere, veri sahibinin istediği zaman rızasını geri çekme hakkı vardır. Rızanın geri çekilmesinin de rızanın verilmesi kadar kolay

[189] *EU GDPR Portal*. Şubat 2019 https://eugdpr.org/the-regulation/, Erişim Tarihi: Erişim Tarihi: 6 Şubat 2019.
[190] Hangi miktar daha yüksekse o esas alınmaktadır.

olması gerekmektedir. Fakat rızanın geri çekilmesi, geri çekim işleminden önce rızaya dayalı olarak yapılan işleme faaliyetinin hukuka uygunluğunu etkilememektedir.

Bunun yanı sıra, maddede kişi tarafından verilen rızanın GDPR'a aykırı olması halinde bu beyan artık hiçbir şekilde kişi açısından bağlayıcı olmayacağı da düzenlenmekte olduğundan 95/46/EC sayılı Direktif'e uygun olsa bile GDPR'a aykırı usullerle elde edilen rıza hukuka uygun olmayacaktır. Dikkat edilmelidir ki bunun anlamı Türk hukukuna uygun olarak elde edilen rızanın, GDPR açısından hukuka aykırı olabileceğidir.

Dördüncü öne çıkan özellik, çocuğun rızasına ilişkin özel düzenlemenin yapılarak m.8'de çocuğun bilgi toplumu hizmetlerine ilişkin rızası açısından geçerlilik koşulları zikredilmiştir. Buna göre, 16 yaşından büyük çocukların kendi başlarına verdikleri rıza geçerliyken 16 yaşından küçüklerin rızası ancak rızanın velayet hakkı bulunan kişi tarafından verildiği veya onaylandığı ölçüde hukuka uygundur. Üstelik 16 yaş sınırının 13'e çekilebileceği de öngörülmüştür. Her durumda, kontrolörün mevcut teknolojiyi dikkate alarak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verildiğini veya onaylandığını doğrulamak adına makul çaba sarf etmesi gerekmektedir. Son olarak, bir çocuğa ilişkin bir sözleşmenin geçerliliği, oluşturulması veya etkisi ilgili kurallar gibi üye devletlerin genel sözleşme hukukunu etkilemez denilerek yerel borçlar hukuku hükümlerine üstünlük tanınmıştır.

c) Veri sahibinin hakları konusunda getirilen yenilikler

Diğer getirilen yenilikler veri sahibinin hakları konusunda olmuştur. Buna göre, kişisel veri ihlalinin veri sahibine iletilmesi hakkı[191], veri sahibinin erişim hakkı[192], unutulma

[191] Kişisel veri ihlalinin veri sahibine iletilmesi hakkı GDPR m. 34'te düzenlenmektedir:
"1. Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, kontrolör kişisel veri ihlalini gereksiz bir gecikmeye mahal vermeden veri sahibine iletir.
2. Bu maddenin 1. paragrafında atıfta bulunulan veri sahibine ilişkin bildirimde kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanır ve en azından 33(3) maddesinin (b), (c) ve (d) bentlerinde atıfta bulunulan bilgiler ve tedbirlere yer verilir.
3. Aşağıdaki koşulların herhangi birinin yerine getirilmesi durumunda, 1. paragrafta atıfta bulunulan veri sahibine ilişkin bildirim gerekmez:
(a) kontrolörün uygun teknik ve düzenlemeye ilişkin koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirler başta olmak üzere bu tedbirlerin kişisel veri ihlalinden etkilenen kişisel verilere uygulanmış olması;
(b) kontrolörün 1. paragrafta atıfta bulunulan veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alması;
(c) bildirimin ölçüsüz bir çaba gerektirecek olması. Bu durumda, bunun yerine, veri sahiplerinin aynı etkililikle bilgilendirildiği kamuya yönelik bir bildirim veya benzeri bir tedbir uygulanır.
4. Kontrolörün halihazırda kişisel veri ihlalini veri sahibine iletmemiş olması durumunda, denetim makamı, kişisel veri ihlalinin yüksek bir riske sebebiyet verme olasılığını değerlendirdikten sonra, kontrolörün bu bildirimi yapmasını şart koşabilir veya 3. paragrafta atıfta bulunulan koşullardan herhangi birinin yerine getirilmesine karar verebilir."
[192] Veri sahibinin erişim hakkı GDPR m. 15'te düzenlenmektedir:
"1. Veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini kontrolörden teyit etme ve, işleme faaliyeti olması halinde, kişisel verilere erişim ile aşağıdaki bilgileri talep etme hakkı bulunur:
(a) işleme amaçları;
(b) ilgili kişisel veri kategorileri;
(c) üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri;
(d) mümkün olması halinde, kişisel verilerin saklanması açısından öngörülen süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler;
(e) kontrolörden veri sahibine ilişkin kişisel verilerin düzeltilmesi veya silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işleme faaliyetine itiraz etme hakkının varlığı;
(f) bir denetim makamına şikayette bulunma hakkı;
(g) kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler;
(h) profil çıkarma da dahil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar vermenin varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları.
2. Kişisel verilerin üçüncü bir ülke ya da uluslararası bir kuruluşa aktarılması durumunda, veri sahibinin aktarımla ilgili olarak 46. madde uyarınca uygun güvenceler hususunda bilgilendirilme hakkı bulunur.
3. Kontrolör işleme faaliyetinden geçen kişisel verilerin bir nüshasını sağlar. Veri sahibi tarafından talep edilen diğer nüshalar açısında, kontrolör idari masraflara dayalı olarak makul bir ücret talep edebilir. Veri sahibinin talebi elektronik yollarla yapması halinde ve veri sahibi tarafından aksi talep edilmedikçe, bilgiler yaygın kullanılan bir elektronik yolla sağlanır.
4. 3. paragrafta atıfta bulunulan bir nüsha elde etme hakkı başkalarının hakları ve özgürlüklerini olumsuz yönde etkilemez."

hakkı[193], işleme faaliyetini kısıtlama hakkı[194] ve veri taşınabilirliği hakkı[195] yer almaktadır. Bunlara ek olarak kişisel verilere usulsüz şekilde ulaşılması(hacklenmesi) halinde bilme hakkı da getirilmiştir[196].

[193] Unutulma hakkı, GDPR m. 17'de düzenlenmektedir:
"1. Veri sahibinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini kontrolörden talep etme hakkı bulunur ve, aşağıdaki hallerden birinin geçerli olması durumunda, kontrolörün kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü bulunur:
(a) kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması;
(b) veri sahibinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendine göre işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması;
(c) veri sahibinin 21(1) maddesi uyarınca işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması ya da veri sahibinin 21(2) maddesi uyarınca işleme faaliyetine itirazda bulunması;
(d) kişisel verilerin yasa dışı biçimde işlenmiş olması;
(e) kontrolörün tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması;
(f) kişisel verilerin 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması.
2. Kontrolörün kişisel verileri kamuya açıklamış olduğu ve 1. paragraf uyarınca kişisel verileri silmek zorunda olduğu hallerde, kontrolör, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri sahibinin talep etmiş olduğu kişisel verileri işleyen kontrolörleri söz konusu kişisel verilere yönelik her türlü bağlantı veya bu verilerin her türlü nüshası ya da çoğaltmasının söz konusu kontrolörlerce silinmesi hususunda bilgilendirmek üzere teknik tedbirler de dahil olmak üzere makul adımları atar.
3. 1 ve 2. paragraflar işleme faaliyeti aşağıdaki amaçlar doğrultusunda gerekli olduğu ölçüde uygulanmaz:
(a) ifade ve bilgi edinme hakkının kullanılması;
(b) kontrolörün tabi olduğu Birlik veya üye devlet hukuku çerçevesinde işleme faaliyeti gerektiren bir yasal yükümlülüğe uygunluk açısından veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması açısından;
(c) 9(2) maddesinin (h) ve (i) bentlerinin yanı sıra 9(3) maddesi uyarınca halk sağlığı alanındaki kamu yararı sebeplerinden dolayı;
(d) 1. paragrafta atıfta bulunulan hakkın ilgili işleme hedeflerinin yakalanmasını imkansız hale getirmesi veya yakalanmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde, 89(1) maddesi uyarınca kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veya
(e) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından."
[194] İşleme faaliyetini kısıtlama hakkı GDPR m. 18'de düzenlenmektedir.
[195] Veri taşınabilirliği hakkı GDPR m. 20'de düzenlenmektedir:
"1. Aşağıdaki hallerde, veri sahibinin kendisi ile ilgili olarak bir kontrolöre sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı bulunur ve kişisel verilerin sağlandığı kontrolörün herhangi bir engellemesi olmaksızın bu verileri başka bir kontrolöre iletme hakkı bulunur:
(a) işleme faaliyetinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendi uyarınca bir rızaya veya 6(1) maddesinin (b) bendi uyarınca bir sözleşmeye dayanması ve
(b) işleme faaliyetinin otomatik yollarla gerçekleştirilmesi.
2. 1. paragraf uyarınca veri taşınabilirliği hakkını kullanırken, veri sahibinin, teknik açıdan uygulanabilir olması halinde, kişisel verilerin doğrudan bir kontrolörden diğerine ilettirme hakkı bulunur.
3. Bu maddenin 1. paragrafında atıfta bulunulan hakkın kullanımı ile 17. maddeye halel gelmez. Söz konusu hak kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması için gereken işleme faaliyetlerine uygulanmaz.
4. 1. paragrafta atıfta bulunulan hak başkalarının hakları ve özgürlüklerini olumsuz yönde etkilemez."
[196] Oturaklı, s. 13.

Yeni düzenlenen erişim hakkına göre, veri sahibine talebi üzerine işleme nüshalarının bir kopyasını elde etme imkânı sağlanmaktadır. 95/46/EC sayılı Direktif'te bu hususta yalnızca işlemeye ilişkin bilgi verilmekte, işleme faaliyetinin tüm nüshalarının kopyalarını alma hakkı tanınmamaktaydı. Bu düzenleme ile birlikte artık kontrolörün işleme faaliyetinden geçen kişisel verilerin, GDPR m. 15'teki erişim hakkına uygun olacak şekilde bir nüshasının talebi üzerine veri sahibine sağlanması gerekmektedir.

Öte yandan, GDPR'da ilk defa unutulma hakkı ayrı bir maddede düzenlenmiştir. GDPR m. 17'de düzenlenen bu hak, veri silme olarak da bilinmektedir. Temel dayanağı amaçla bağlılık ilkesi olan unutulma hakkı, veri denetleyicisini, başvuran kişinin kişisel verilerini silmesi ve verinin daha fazla yayılmasını durdurması hususunda yetkilendirmekte ve görevlendirmektedir. Bu verilerin kapsamı ise söz konusu kişisel verilerin işlenmesinde öngörülen amaçlar doğrultusunda ilgili olmayan ya da artık gerekli olmayan veya rızası geri çekilen verilerden ibarettir. Denetçinin, bu konudaki istekleri göz önüne alırken başvurucunun hakları ile verilerin erişilebilirliğinde kamu yararını karşılaştırmalarını gerektiği de düzenlenmektedir. Buna göre, denetçi işlenmesinde kamu yararı olan verileri silmeyeceği için kişinin unutulma hakkı kamu yararı gerekçesi ile sınırlanmış olmaktadır.

Ayrıca, GDPR m. 20'de ilk defa veri taşınabilirliği hakkı da düzenlenmiştir. Maddede sayılan hallerin varlığında, veri sahibine, kendisi ile ilgili olarak bir kontrolöre sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı ve kişisel verilerin sağlandığı kontrolörün herhangi bir engellemesi olmaksızın bu verileri başka bir kontrolöre iletme hakkı tanınmıştır.

d) Kişisel verilerin soruşturma evresinde işlenmesi açısından

GDPR m. 2(2)(d)'de, GDPR'ın suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkin makamlar tarafından kişisel verilerin işlenmesine uygulanmayacağı düzenlenmiştir. Her ne kadar GDPR, soruşturma evresinde kişisel verilerin işlenmesine kural olarak uygulanamamakta olsa bile, GDPR ve getirdiği yeni hükümler içerisinde kişisel verilerin soruşturma evresinde işlenmesine etki eden düzenlemeler de yer almaktadır.

Bunlardan ilki, genetik ve biyometrik verilerin hassas veriler arasında sayılmış olmasıdır. GDPR öncesi dönemde hali hazırda hassas veri olduğu üzerinde tartışma bulunmayan

genetik ve biyometrik verilerin GDPR ile de korunmaya devam etmesidir. Keza soruşturma evresinde kişilerin bu tarz hassas verileri, koruma tedbirleri ve delil değerlendirme yöntemleri ile delil elde etme amacı doğrultusunda işlenebilmektedir.

Öte yandan hassas verilerin işlenmesindeki rıza kuralının GDPR'da düzenlenmiş olan çeşitli istisnaları bulunmaktadır. Buna göre, işlemede hayati bir menfaatin varlığında, ilgili kişi tarafından verinin alenileştirilmiş olmasında, mahkemelerin yargı işlemlerinde ve kamu yararına yapılan çeşitli faaliyetler kapsamındaki işlemeler vs. söz konusu yasağın istisnası olarak düzenlenmektedir[197].

[197] İstisnalar, GDPR m. 9(2)'de düzenlenmektedir:
"2. 1. paragraf aşağıdakilerden birinin geçerli olması halinde uygulanmaz:
(a) Birlik veya üye devlet hukuku çerçevesinde 1. paragrafta belirtilen yasağın veri sahibi tarafından kaldırılamayacağına ilişkin bir hüküm sağlanması haricinde, veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi;
(b) Birlik veya üye devlet hukuku çerçevesinde ya da üye devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece, kontrolörün veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi;
(c) veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması;
(d) işleme faaliyetinin bir vakıf, birlik veya kar amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi;
(e) işleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması;
(f) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi;
(g) gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi;3e
(h) koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca ve 3. paragrafta atıfta bulunulan koşullar ve güvencelere tabi olarak çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;
(i) özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması veya sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartları sağlanması gibi halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;
(j) gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, 89(1) maddesi uyarınca kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi."

Bunun dışında, GDPR m. 9'da mesleki sır tutma yükümlülüğü altında olan kişilerin işleyebileceği hassas nitelikli verilerin çeşitli şartlara bağlanmış olması ve ülkelerin buna teşvik edilmekte olması dikkat çekicidir.

İkincisi, veri işleyicisi ve kontrolörünün uyması gerektiği bazı kısıtlamaların GDPR m. 23'te oldukça net olarak belirtilmiş olmasıdır. Bu doğrultuda, ne olursa olsun yapılacak işleme faaliyetinin hakkın özüne dokunmaması ve demokratik toplum gerekliliklerine uygun olması gerekmektedir.

O halde kişisel verilerin korunmasının genel ilkeleri kural olarak soruşturma da dâhil her türlü işleme faaliyetine uygulanmalıdır. Bu kuralın istisnası olabilecek müdahalelerin özelliği ise hakkın özüne dokunmamak ve demokratik toplum gereklilikleri ile bağdaşmak ve bununla ilgili gerekçe sunabilmekte olmasıdır.

Üçüncüsü, GDPR m. 23(1)(d)'nin tezimiz bağlamında çok önemli olmasıdır. Çünkü bu fıkraya göre suçların soruşturulması kapsamında yapılacak bir işlemenin hakkın özüne dokunmaması ve demokratik toplumda gerekli olması için uyması gereken koşullar belirtilmektedir.

Buna göre, soruşturma sürecinde delillerin işlenmesinde, işlemenin veya işleme kategorilerinin amaçları; kişisel veri kategorileri; kötüye kullanım veya yasa dışı yollarla erişim veya aktarımın engellenmesine yönelik güvenceler belirtilmelidir.

Ayrıca, GDPR m. 23(2)'ye göre, işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanabilir güvenceler; veri sahiplerinin hakları ve özgürlüklerine yönelik riskler ve kısıtlama amacına halel getirmemesi durumunda veri sahiplerinin kısıtlamayla ilgili bilgi sahibi olma hakkının soruşturmaya hâkim olması gerekmektedir. Dolayısıyla, GDPR, Kısıtlamalar başlıklı bu maddesiyle soruşturma evresinin tamamıyla koruma kapsamı dışı bırakmamaktadır.

Belirtmek gerekir ki, söz konusu fıkra hükmünde belirtilen haklar ideal hukukta değer arz etmektedir. Keza GDPR m. 23 uyarınca, soruşturma evresindeki verilerin işlenmesinde m. 5'te sayılan kişisel verilerin işlenmesine ilişkin ilkelere uygun olması gerektiği anlamı çıkmaktadır. Bu yüzden, KVK Kanunu'nun soruşturma evresini, kişisel verilerin korunmasına ilişkin genel ilkeleri de dâhil olmak üzere tamamen kapsamı dışında tutması GDPR ile uyuşmamaktadır. Bu minvalde KVK Kanunu'nda soruşturma evresini

doğrudan koruma kapsamı dışında bırakmak yerine, veri işleme ilkelerini ve ilgili kişinin haklarını ihlal etmeden dengeleyen düzenleyici değişikliklerin yapılması yerinde olacaktır.

Bunun dışında öne çıkan dördüncü husus, mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenmesi ve depolanması ile ilgilidir[198]. Buna göre, mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin ya da ilgili güvenlik tedbirlerine ilişkin kararlardaki kişisel verilerin hukuka uygunluk sebeplerinden birine dayalı olarak işlenmesi gerekmektedir. Ayrıca resmi merciinin denetimi altında veya veri sahiplerinin hakları ve özgürlüklerine uygun güvenceler sağlanması ile gerçekleştirilmelidir. Mahkûmiyet kararlarına ilişkin kapsamlı herhangi bir sicilin yalnızca resmi merciinin denetimi altında tutulması gerekmektedir.

Dikkat çekmek gerekir ki, veriyi işleyen ve depolayan kamu otoritesinin kişisel verilerin korunmasına ilişkin uygun güvenceler sağlama şartını yerine getirmelidir. Fakat soruşturma evresinde işin doğası gereği verilerin geniş kapsamlı olarak kaydedilme ihtiyacı karşısında bu hükümlerin unutulma hakkı ile arasında gerginliğe yol açacağı oldukça muhtemeldir[199].

Beşincisi, kişisel verilerin soruşturma evresinde işlenmesinde işlenen verilere ilişkin güvenliği sağlanması hususudur. Kişisel verilerin korunmasına ilişkin ilkelere uygun işleme yapıldığı takdirde yapılan işleme, büyük ölçüde hukuka uygun olarak addedilecektir. Fakat hakkın özüne müdahale etmeden orantıyı sağlamaya yönelik bir müdahalenin varlığından bahsedebilmek için işlem güvenliğine ilişkin düzenlenen hükümlerin de soruşturma evresinde alınan tedbirlere hâkim olması gerekir. Buna göre, kişisel verilerde takma ad kullanımı ve şifreleme; işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi; fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi gibi güvenlik önlemlerinin sağlanmalıdır[200].

---

[198] Mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenmesi GDPR m. 10'da düzenlenmektedir.

[199] Thanaraj, Ann: "Studying Law in a Digital Age: Preparing Law Students for Participation in a Technologically-Advanced Multidisciplinary and Complex Professional Environment", Nottingham Law Journal, 27/2, Nottingham 2018, s. 75.

[200] İşleme güvenliği GDPR m. 32 düzenlenmektedir:

Bunlardan en öne çıkan tedbir sadece görevli kişiye özel erişim imkanı sunan ve diğer kişilere karşı veriyi okunamaz hale getiren kişisel verilerin kripto haline getirilmesidir[201]. Zikredilen hususların veriler üzerinde belirli bir koruma sağlayacağı muhakkaktır. Aksi bir durumda ise kişisel verilerin kötüye kullanılması ve ilgisiz kişilerin eline çeşitli saiklerle kullanılmak üzere geçeceği ihtimali bulunmaktadır. Dolayısıyla veri güvenliğine ilişkin zikredilen güvencelerin sağlanması halinde soruşturma evresinde işlenen verilerin korunması amacı doğrultusunda müspet bir adım atılmış olacaktır.

Son olarak belirtmek gerekir ki, soruşturma evresindeki kişisel verilerin kamu yararı amacıyla depolanabilmektedir[202]. Bu verilerin depolanmasında, GDPR'da yer verilen tüm

"1. Kontrolör ve işleyici, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde, aşağıdakiler de dahil olmak üzere uygun teknik ve düzenlemeye ilişkin tedbirler uygular:
(a) kişisel verilerde takma ad kullanımı ve şifreleme;
(b) işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi;
(c) fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi;
(d) işleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve düzenlemeye ilişkin tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç.
2. Uygun güvenlik seviyesi değerlendirilirken, iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı olarak imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişim başta olmak üzere özellikle işleme faaliyetinin yol açtığı riskler göz önünde bulundurulur.
3. 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmasına uygun hareket edilmesi bu maddenin 1. paragrafında ortaya konan gerekliliklere uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.
4. Kontrolör ve işleyici kontrolör ya da işleyicinin yetkisi ile hareket eden ve kişisel verilere erişimi bulunan herhangi bir gerçek kişinin, Birlik ya da üye devlet hukuku çerçevesinde bu yönde hareket etmesinin gerekmemesi durumunda, kontrolörden aldığı talimatlar haricinde bu verileri işlememesini sağlamak üzere adımlar atar."

[201] Gioioso, Kaylie: "Small Companies, Big Breaches: Why Current Data Protection Laws Fail American Consumers in Cases of Third-Party Hacking", Journal of Business & Technology Law Proxy, 10, Maryland 2016, s. 18.

[202] Kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetine ilişkin güvenceler ve derogasyonlar hükmü GDPR m. 89'da düzenlenmektedir: "*1. Kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyeti bu Tüzük uyarınca veri sahibinin hakları ve özgürlükleri açısından uygun güvencelere tabidir. Bu güvenceler ile özellikle verilerin en alt düzeye indirilmesi ilkesine uygun hareket edilmesinin sağlanması amacı ile teknik ve düzenlemeye ilişkin tedbirlerin uygulamaya konması sağlanır. Bu amaçların bu şekilde yerine getirilebilmesi koşuluyla, bu tedbirler takma ad kullanımını içerebilir. Bu amaçların veri sahiplerinin teşhis edilmesine olanak tanımayan veya artık olanak tanımayan ek işleme faaliyetleri ile yakalandığı hallerde, söz konusu amaçlar bu şekilde yakalanır.*
2. Kişisel verilerin bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlendiği hallerde, Birlik veya üye devlet hukuku çerçevesinde, 15, 16, 18 ve 21. maddelerde atıfta bulunulan hakların spesifik amaçlara ulaşılmasını imkansız hale getirmesinin veya ulaşılmasına ciddi şekilde zarar vermesinin muhtemel olduğu ve derogasyonların bu amaçlara ulaşılması için gerekli olduğu ölçüde, bu maddenin 1. paragrafında atıfta bulunulan koşullar ve güvencelere tabi olarak böylesi haklardan derogasyonlar sağlanabilir.

güvenceler uygulama alanı bulmalıdır. Bu güvencelerin yanı sıra taraf olan devletlerin pozitif yükümlülükleri gereğince özellikle veri minimizasyonu ilkesine uygun hareket edilmesinin sağlanması amacı ile teknik tedbirlerin uygulamaya konması sağlanmalıdır. Bu doğrultuda, verilere kimlerin hangi verilere ve hangi sürelerle erişebileceği, verileri silebileceği, değiştirebileceği, kopyalayabileceği ve işleyebileceği belirli olmalı ve sınırlanmalıdır. Böylece soruşturma evresinde kişisel verilerin işlenmesinde yetkili olan tüm görevlilere geniş takdir yetkisi tanınmasının önüne geçilmiş, kişisel verilerin korunması hakkı orantılı olarak tesis edilmiş olur.

4. 2016/680/EU sayılı ve 27 Nisan 2016 Tarihli Suçun Önlenmesi, Soruşturulması, Tespit Edilmesi veya Kovuşturulması Amacıyla Yetkili Makamlarca Kişisel Verilerin İşlenmesi ile İlgili Gerçek Kişilerin Korunmasına İlişkin Direktif

a) Genel olarak

Soruşturma evresinde kişisel verilerin korunması konusu, 95/46/EC sayılı Direktif'te veri korumaya ilişkin genel düzenleyici Direktif olması hasebiyle kapsam dışı olup, bu alan diğer çerçeve kararların yanı sıra daha çok 2008/977/JHA Çerçeve Kararı ile doldurulmaya çalışılmıştı. Fakat 2008/977/JHA Çerçeve Kararı tüm adli süreçleri kapsamına alması ve de sadece ülkeler arası veri paylaşımına ilişkin hükümler getirmesi sebebiyle hem bu alanda kapsamlı bir koruma hem de ülkeler arası yeknesaklığı sağlayamamaktaydı.

Bu doğrultuda, 27.04.2016 tarihinde 679 sayılı Direktif olan GDPR'la birlikte aynı gün, suçun önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması amacıyla yetkili makamlarca kişisel verilerin işlenmesi ile ilgili gerçek kişilerin korunmasına ilişkin 2016/680/EU sayılı Direktif çıkarılmıştır. Nasıl GDPR kendisinden önce yürürlükte bulunan 95/46/EC sayılı Direktifi yürürlükten kaldırmışsa, bu direktif de kendi alanında yürürlükte bulunan 2008/977/JHA Çerçeve Kararını yürürlükten kaldırmıştır. Suçların

3. Kişisel verilerin kamu yararına arşivleme amaçları doğrultusunda işlendiği hallerde, Birlik veya üye devlet hukuku çerçevesinde, 15, 16, 18, 19, 20 ve 21. maddelerde atıfta bulunulan hakların spesifik amaçların yakalanmasını imkansız hale getirmesinin veya yakalanmasına ciddi şekilde zarar vermesinin muhtemel olduğu ve derogasyonların bu amaçların yakalanması için gerekli olduğu ölçüde, bu maddenin 1. paragrafında atıfta bulunulan koşullar ve güvencelere tabi olarak böylesi haklardan derogasyonlar sağlanabilir.

4. 2 ve 3. paragrafta atıfta bulunulan işleme faaliyetinin aynı zamanda başka bir amaca hizmet ettiği hallerde, derogasyonlar yalnızca bu paragraflarda atıfta bulunulan amaçlara yönelik işleme faaliyetine uygulanır."

soruşturulması amacıyla kişisel verilerin işlenmesine dair düzenlendiği için tezimiz bağlamında oldukça önemli olan bir direktiftir. AB hukukuna hâkim olan reaktif değil proaktif yaklaşımının yani olması gereken ilkelerin önceden öngörülerek düzenlenmesi anlayışının veri koruma alanındaki bir ürünüdür[203].

Hem AB ülkeleri arasında soruşturma evresinin yeknesaklığına hem de özgürlük, güvenlik ve adaletin sağlanmasına katkı sağlamak amacı güden bu Direktif, kişisel verilerin soruşturma evresinde daha güçlü bir biçimde korunması gerektiğini belirtmektedir[204]. 2016/680/EU sayılı Direktif, kişisel verilerin soruşturma evresinde korunmasına ilişkin getirilmiş özel bir direktif olması sebebiyle kişisel verilerin soruşturma evresinde korunmayacağı yönündeki KVK Kanunu hükümleriyle uyuşmayan bir direktiftir.

Etkin iş birliği ve bilgi alışverişini sağlama amacıyla GDPR'a ek olarak getirilen 2016/680/EU sayılı Direktif, kişisel verilerin korunmasına ilişkin genel ilkeler, veri sahibinin hakları ve usule ilişkin diğer hükümler açısından GDPR düzenlemesiyle aynı olduğu görülmektedir.

Ayırıcı yönleri ise öncelikle, kişisel verilerin korunmasının sadece özel hukuk için değil kamu hukuku için de gerekli olduğu düşüncesini vermesidir.

İkinci olarak, kişisel verilerin korunmasına ilişkin ilkelerin yalnızca şeffaflık özelliği dışında ceza hukukunda da uygulama alanı bulacağını göstermesidir. Şeffaflık hükümlerinin yer almamasıyla soruşturma evresinde görev alan kamu otoritelerine gerekli işlemleri yapabilmeleri için yeterli alanın var olduğunu ortaya koymasıdır.

Üçüncü olarak ise, soruşturma evresinde kişisel verilerin korunabilmesi için bağımsız kamu otoritelerinin oluşturulması gerektiğidir.

Dördüncü olarak ise, GDPR'ın bir tüzük, bu 2016/680/EU sayılı Direktif'in ise bir direktif olmasıdır. Esasen her iki norm da birliğe üye ülkeler tarafından bağlayıcı olsa da tüzükler üye ülkelerde doğrudan uygulama alanı bulurken, direktiflerin üye ülkeler açısından yerel hukuk kurallarıyla yeknesaklaştırılması gerekli olup genellikle doğrudan

[203] Akıncı, A. N. 2019. *Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti*. Uzmanlık Tezi, Ankara: T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Sektörler ve Kamu Yatırımları Genel Müdürlüğü, s. 149.
[204] 2016/680/EU sayılı Direktif, Gerekçe, par 4.

uygulama alanı bulmamaktadırlar[205]. Bu noktada, gizlilik ve veri koruması konusunda birliğin önemi vurgulanmakta, insan haklarının korunmasına ulus üstü yönetim ve regülasyonların kapsamlı ve kaçınılmaz rol oynadıkları belirtilmektedir[206].

İfade etmek gerekir ki, 2016/680/EU sayılı Direktif, günümüz hukuk kuralları arasında soruşturma evresinde kişisel verilerin işlenmesine ilişkin olarak bir insan hakkı olan kişisel verilerin korunması konusunu yeterli görünen bir derecede koruyan en güncel metin konumundadır. GDPR'da özel hukuk bağlamında kişilere tanınan kişisel verilerin korunmasına ilişkin hakların hemen hemen tamamını kamu gücünün ağır basan otoriter pozisyonu karşısında bulunan kişilere tanıyor olması sebebiyle yapay ayrımları ortadan kaldırmaktadır. Böyle kişisel verilerin korunmasının insan hakkı olarak soruşturma evresinde de korunmaya değer olduğu göstermektedir. Artık kişisel verilerin ceza muhakemesinde korunmasına ilişkin atıfta bulunulması gereken en önemli düzenlemedir. Sadece Avrupa Birliği sınırları içerisinde yürürlükte olmasına karşın, Avrupa Birliği uyumlaşma paketleri çerçevesinde, Türk hukukunda da bu Direktif temelli yasal düzenlemelerin yapılacağını düşünmekteyiz.

b) Kişisel verilerin soruşturma evresinde işlenmesi açısından Direktif'in özel önemi

Belirtmek gerekir ki GDPR düzenlemesinin soruşturma evresinde neredeyse hiç uygulanmayacak oluşundaki amaç, kişisel verilerin soruşturma evresinde korunmaması ne hakkın bu alanda sınırlanması ne de işin niteliği gereği olması sebebidir. Buradaki amaç, soruşturma evresinde korunacak kişisel verilerin özel hükümlerin yer aldığı ayrı bir Direktif'te düzenleniyor oluşudur[207].

Zaten Avrupa Birliğinin İşleyişi Hakkında Antlaşma m. 16(2) hükmü de AB Konseyi ve Parlamentosu'nu kişisel verileri bu şekilde özel koruyucu tedbirler almakla yükümlü tutmaktadır[208]. Tüm ceza muhakemesi süresince uygulanacak olan bu direktif, genel

[205] Açıklamalarla Avrupa Birliği Avrupa Birliği nasıl çalışır?, Avrupa Komisyonu İletişim Genel Müdürlüğü, Vatandaşlara Bilgi, 1049 Brüksel BELÇİKA, Avrupa Birliği Yayın Ofisi, 2014, https://ec.europa.eu/cyprus/sites/cyprus/files/je0115325trc.pdf

[206] Alston, Philip/Bustelo, Mara/Heenan, James: The EU and Human Rights, 1999 New York, s. 24.

[207] 2016/680/EU sayılı Direktif, Gerekçe, par. 8-11.

[208] Bahsedilen hüküm Avrupa Birliğinin İşleyişi Hakkında Antlaşma m. 16'da düzenlenmektedir:
"1. Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir.
2. Avrupa Parlamentosu ve Konsey, Birlik hukuku kapsamına giren faaliyetlerin yürütülmesinde, Birlik kurum, organ, ofis veya ajansları ile üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolaşımına ilişkin kuralları olağan yasama usulü uyarınca belirler. Bu kurallara uyulması, bağımsız otoritelerin denetimine tabidir.

düzenleme olan GDPR'ın kapsamına almadığı soruşturma evresine özgü hükümler getirmesi sebebiyle, soruşturma evresinde bu direktifin varlığında GDPR genel hüküm mahiyetine bürünecektir[209].

GDPR'ın uygulama kapsamından farklı olarak AB sınırları içinde geçerli olan bu direktif, tüm gerçek kişiler için uygulama alanı bulmaktadır[210]. Fakat hem AB sınırları içerisinde sıkıştırılması, hem de üye devletlere verilerin silme, bilgi edinme ve düzeltme hakkı gibi konularda ulusal makamlara takdiri genişletici olarak vermesi sebebiyle kapsamın görünüşte geniş fakat esasen dar olduğu gerekçesiyle eleştirilmektedir[211].

Öte yandan, Direktif'in getirilişinde bazı içsel motivasyonlar bulunmaktadır.

Birincisi, soruşturma evresinde kişisel verilerin işlenmesi sırasında yeterli güvenlik sağlanması amacıyla yetkisiz erişimin engelleniyor olmasıdır[212].

İkincisi, alınacak tedbirlerin yasal dayanağında işlenecek verinin hedefini açıklıyor olup keyfiliğe karşı garanti sağlayacak düzeyde verilerin aktarımı ve imhasına ilişkin güvenlik sağlanıyor olması gerekliliğidir. Bu yüzden hükümlerin AİHM standartlarında, açık, kesin ve öngörülebilir olmaları şarttır[213].

Üçüncüsü, ayrımcılığa yol açabilecek olan profil çıkarmada ve hassas verilerin işlenmesinde kişilerin rızasının yanı sıra kanuna uygunluğun da gözetilmesi gerekmekte oluşunun vurgulanmak istenmesidir[214].

Dördüncüsü, veri sahibinin haklarını etkin olarak kullanabilmesi için işleme sürecinin düzenlemelerde kolay anlaşılabilir, açık, sade bir dille ve çocukların durumunu göze alarak anlatılıyor olması gerekliliğidir[215].

Sonuncusu ise, güncel gelişmeler sonucunda farklı yorumları ortadan kaldıracak hükümlerle, veri sahibinin haklarına yönelik getirilecek herhangi bir sınırlama konusunda

Bu maddeye dayanarak kabul edilen kurallar, Avrupa Birliği Antlaşması'nın 39. maddesinde yer alan spesifik kurallara halel getirmez."

[209] 2016/680/EU sayılı Direktif, Gerekçe, par. 11. (paragrafı tartış)
[210] 2016/680/EU sayılı Direktif, Gerekçe, par. 14, 17.
[211] Bostancı Bozbayındır, s. 71.
[212] 2016/680/EU sayılı Direktif, par. 28.
[213] 2016/680/EU sayılı Direktif, par. 33, 34.
[214] 2016/680/EU sayılı Direktif, par. 37.
[215] 2016/680/EU sayılı Direktif, par. 39.

AİHM ve Avrupa Adalet Divanı içtihatlarıyla uyumlu birlikteliğinin sağlanmak istenmesidir[216].

c) Kişisel verilerin soruşturma evresinde işlenmesinin ölçüsü ve sınırları

2016/680/EU sayılı Direktif, kısmen veya tamamen otomatik yollarla işlenen ve dosyalama parçası olarak veya bu amaçlı tüm işleme faaliyetlerinde uygulama alanı bulmaktadır[217]. Dolayısıyla verilerin işlenmesi üzerindeki teknik farklılıklar verilerin korunması açısından dikkate alınmamakta, temel değer olarak kişisel verilerin soruşturma evresinde işlenmesine yol açabilen her türlü faaliyet kapsama alınmaktadır.

Tanımların düzenlendiği m. 3'te tanımlanan yetkili otorite terimine göre, soruşturma evresinde yer alan kamu görevlisi yahut kurumu olsun ya da olmasın tüm gerçek ve tüzel kişiler, Direktif kapsamı içerisinde yetkili otorite terimi kapsamında yer alacaktır. O halde, soruşturma evresinde kişisel verilerin işlenmesi ile ilişkisi olan her gerçek veya tüzel kişinin bu Direktif kapsamındaki maddeler bağlamında uyması gereken yükümlülükler söz konusu olacaktır.

Öte yandan, kontrolör terimi ise verilerin işleme kararını veren yetkili otorite olarak tanımlanmışken, işleyici terimi işleme kararını ifa eden kolluk görevlisi olarak tanımlanmıştır. O zaman, soruşturma evresinde kişisel verilerin işlenmesi kararını verebilecek olan hâkim, savcı veya kolluk amiri kontrolör; işleme kararını yerine getiren kolluk ve diğer görevli memurlar işleyici sıfatını taşımaktadırlar. Öte yandan maddeden çıkan anlama göre kamu görevlisi olmayan özel güvenlik personeli gibi kişisel de kamu yetkilisi niteliğinde olabilmektedir. Düzenlemenin bu şekli, GDPR ile Direktif'in uygulama alanını ayırt etmeyi zorlaştırdığı için haklı olarak eleştirilmektedir[218].

Direktif'in belki de öne çıkan en önemli maddesi olan m. 4'te soruşturma evresinde kişisel verilerin işlenmesine ilişkin ilkelere yer verilmiştir. GDPR m. 5'te yer alan kişisel verilerin işlenmesi ilkelerinin küçük farklarla tekrarlanmakta olduğu görülmektedir. Üye

[216] 2016/680/EU sayılı Direktif, par. 46.
[217] 2016/680/EU sayılı Direktif, m. 2.
[218] Caruana, Mireille M.: "The Reform of the EU Data Protection Framework in The Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement", International Review of Law, Computers & Technology, 2017, s. 5.

devletlerin maddede yer sayılan bu ilkelerle ilgili yerel hukuk düzenlemelerini uyumlulaştırmaları gerekmektedir:

1- Veri sahibi ile ilgili olarak hukuka uygun ve adil bir biçimde işleme (hukuka ve dürüstlük kurallarına uygunluk)[219]
2- Özel olarak belirtilmiş, açık ve meşru amaçlara yönelik olarak toplanma ve bu amaçlara uygun olmayan bir şekilde işlenmeme (amacın sınırlandırılması)
3- İşlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlanma (verilerin en az seviyeye indirilmesi)
4- Verilerin doğruluğu ve gereken şekil ve miktarda güncel olması, aksi halde gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanması (doğruluk ve güncellik)
5- Veri sahiplerinin yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece teşhis edilmesini (saklama süresinin sınırlandırılması)
6- Yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dâhil olmak üzere teknik veya düzenlemeye ilişkin uygun tedbirlerin alınması (bütünlük ve gizlilik)
7- İlkelere uygun davranmakla yükümlü olma ve bundan sorumlu olma (hesap verebilirlik).

Maddede ayrıca, bu madde bağlamında zikredilen ilkelerin kapsamı dışındaki bir amaç doğrultusunda yapılacak bir işleme faaliyetinin hem kanunen yetkilendirilmiş hem de kişisel verilerin korunması hakkı karşısında gerekli ve orantılı olması gerektiği yer almıştır. Bunun dışında kamu yararına yapılacak arşivlemenin, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla zikredilen ilkeler doğrultusunda veri sahibinin haklarına uygun güvenceler sağlaması kaydıyla yapılabileceği belirtilmektedir.

Bu doğrultuda kamu yararı gibi hakkın korunmasına dönük geniş ve muğlak istisnaların olması Direktiften beklenen koruma etkisinin aşındırabileceği ve yeknesaklığı sağlayamayacağı gerekçesiyle eleştirilmektedir[220].

[219] GDPR düzenlemesinde bu ilke içerisinde yer alan şeffaflık özelliğine burada yer verilmemektedir. Fakat şeffaflık özelliği yine de kural olarak yer almalıdır. Buna ilişkin olarak sınırlamanın, gerekçesi ortaya koyulması ve dengeli olması suretiyle yapılması mümkündür. Yoksa şeffaflık özelliğini doğrudan devre dışı bırakmak hakkın korunmasına zarar verecektir.
[220] Bostancı Bozbayındır, s. 89.

Verilerin işlenmesine uygulanacak genel ilkelerin dışında soruşturma evresinde hâkim olması gereken başka yükümlülükler takip eden maddelerde yer almaktadır. Buna göre, Direktif m. 5 uyarınca verilerin görüntülenmesi ve depolanmasında uygun süre sınırlarının usulî yasal güvencelerde belirtiliyor olması gerekmektedir.

Direktif m. 6'da ise, kontrolör, veri sahiplerine ilişkin verileri şüpheli, hükümlü, mağdur, tanık ve sair kişiler olarak birbirinden açıkça ayıran bir kategorizasyona tabi tutmakla yükümlendirmektedir. Bizim çıkarımımıza göre uygulanacak hükümlerin farklılaşabileceği ihtimaliyle burada hepsinin aynı kefeye koyulması engellenmek istenmektedir.

Direktif m. 7'de ise, veri kalitesine ilişkin bir hüküm getirilerek, soruşturma evresinde işlenmekte olan verinin doğru, tam, güvenilir ve güncel olması gerektiği aksi halde bu verilerin soruşturmada kullanılamayacağı belirtilerek yetkili görevliler bunu kontrol etmekle yükümlü tutulmaktadır.

Ayrıca, işlemenin meşruluğu hükmünün düzenlendiği Direktif m. 8'de, var olan hukuki düzenlemeler en azından işleme hedefini ve amacını içermesinin şart olduğunu; özel işleme şartlarının düzenlendiği Direktif m. 9'da ise, genel ilkelere uymayan amaçlar dışındaki işleme faaliyetlerinin bu Direktif ve GDPR'a aykırı olamayacağı düzenlenmiştir.

Hassas verilerin işlenme şartlarının düzenlendiği m. 10'da ise, işleme gerekliliği ortaya koyulmuş olan hassas verilerin işlenebilmesi için seçimlik üç durumun varlığı öngörülmektedir. Buna göre, hukuki düzenlemenin varlığı veya kişinin kendisinin veya başkasının hayati çıkarlarının korunması maksadının varlığı veya kişinin kendisi tarafından açıkça alenileştiriliyor olması şart koşulmaktadır.

Öte yandan, soruşturma evresinde kişisel verileri işlenmekte olan veri sahibinin hakları m. 12-18 arasında düzenlenmektedir. GDPR'daki veri sahibinin haklarına ilişkin hükümlerin aynıları şeffaflığa ilişkin hükümler çıkartılmak suretiyle küçük farklılıklarla yer almışlardır. Burada bizim görüşümüze göre şeffaflık özelliği yine de kural olarak yer almalıydı. Keza yapılacaksa buna ilişkin olarak sınırlamanın, gerekçesi ortaya koyulması ve dengeli olması suretiyle yapılması mümkündür. Yoksa şeffaflık özelliğini doğrudan devre dışı bırakmak hakkın korunmasına zarar verecektir. Bu doğrultuda, Madde 29 Veri

Koruma Çalışma Grubu da bir görüşünde, verilerin işlenmesine dönük şeffaflık ilkesinin olmayışının, veri sahibinin yürütülen bir soruşturma çerçevesinde verilerinin işlenmekte olup olmadığı öğrenmesini engellemeyeceği ifade etmektedir. Hatta veri öznesinin hukuka aykırı bir işlemenin varlığı halinde verilerin imhasını talep edebileceğini belirtmektedir[221].

Düzenlenen haklara bakıldığında, m. 12'de veri sahibinin haber alma hakkına yer verilmiştir.

Direktif m. 13'te ise veri sahibine bildirim, veriye erişim, doğrulama ve sınırlama hakkına yer verilmesinin yanı sıra işin gereği ve kamu yararı gibi düzenlemede ifade edilen diğer sair sebeplerle bu hakların orantılı olmak kaydıyla sınırlandırılabileceği düzenlenmiştir.

Direktif m. 14'te veriye erişim hakkına yer verilip, işleme ile hangi bilgilerin öğrenilebileceği zikredilmiş, m. 15'te bu hakkın sınırlarına yer verilmiştir.

Direktif m. 16'da işlenmekte olan verilerin silinmesi, sınırlanması ve doğrulanmasına ilişkin hakları yer almıştır. Ayrıca bu maddede silme talebindeki iddianın kanıtlanmaması ve verinin delil olarak kullanılmaya devam edilmesinin yanı sıra kamu yararı gibi maddede zikredilen sair sebeplerle de bu talebin ret olunabileceği ve bunun da bildirilmesi gerektiği düzenlenmiştir. Kamu yararı çerçevesinde bu haklara getirilecek sınırlamalar hakların sağladığı korumayı tamamen geçersiz kılacak şekilde uygulanamayacaklardır[222].

Son olarak m. 17 ve 18'de ceza soruşturmasında veri sahibinin m. 13, 14 ve 16'da zikredilen haklarının ceza soruşturmasında kişisel veri içeren mahkeme kararlar, kayıt ve dosyalarında uygulanabileceği belirtilmiştir.

Hülasa, soruşturma evresinde kişisel verilerin işlenmesi ile ilgili olarak Direktif, dördüncü bölümde, kontrolör ve işleyicinin yükümlülüklerini; beşinci bölümde, kişisel verilerin üçüncü veya uluslararası organizasyonlara transferine ilişkin hükümleri; altıncı bölümde bağımsız denetleyici otoritenin oluşturulmasına ilişkin hükümleri; yedinci

[221] Madde 29 Veri Koruma Çalışma Grubu, 1806/16/EN WP 239 Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector, Adopted on 8 June 2016, s. 14.
[222] Bostancı Bozbayındır, s. 79.

bölümde ülkeler arasında işbirliğine ilişkin hükümleri ve sekizinci bölümde kanun yolları, sorumluluk ve cezalara ilişkin hükümleri düzenlemiştir.

Zikredilen tüm bu hususlardan hareketle, 2016/680/EU sayılı Direktif'in GDPR'da yer verilen aynı koruyucu hükümleri içeriyor olması dikkat çekicidir. Ayrıca, verilerin soruşturma evresinde korunmasına olan yaklaşımı sebebiyle kişisel verilerin korunması hakkının tesisi adına özel önem taşımakta olduğunu belirtmek gerekir. Bu yönüyle Direktif'in, kişisel verilerin soruşturma evresinde korunmasına ilişkin Türk hukukunda yapılacak olası değişikliklerde etkili olacağını düşünmekteyiz.

II. TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

A. Kişisel Verilerin Korunması Kanunu Öncesi Durum

KVK Kanunu öncesinde kişisel verilerin korunmasına ilişkin duruma bakıldığında, verilerin korunmasında uluslararası belgeler ve daha çok özel hukuk olmak üzere mevzuatta parçalı olarak yer alan çeşitli kanun hükümleri bulunmaktaydı.

Türk hukukunda kişisel veriler ile ilgili ilk etki sahibi metinlerin uluslararası anlaşma hükümleri olduğu görülmektedir. 1981 yılına ait OECD tavsiye kararları başta olmak üzere 2016 yılında yürürlüğe girmesine rağmen 1981 yılında imzalanan Avrupa Konseyi'nin 108 sayılı Sözleşmesi ve AİHS de kişisel verilerin korunması konusunda Türk hukukunu bağlayıcı nitelikte olan ilk önemli metinler olmuştur. Ayrıca yukarıda zikredilen AB metinlerinin de Türk hukukunda kişisel verilerin korunması konusunda etki sahibi olduğunu belirtmek gerekir.

Bunun metinlerin dışında, Türk hukukunda da birbirinden farklı kanunlarda kişisel verilerin korunmasına yönelik hükümler az da olsa yer almıştır. 2010 yılı Anayasa değişikliği sonrası ve KVK Kanunu öncesinde de hukukumuzda kişisel verilerin korunmasına yönelik çeşitli kanunlar da yürürlüğe girmiştir. Buna göre, KVK Kanunu öncesi düzenlenen diğer hükümler konunun özel hukuka bakan yönünde olsa da ceza hukuku bağlamında da yer verilen kanun hükümleri bulunmaktadır.

Buna göre, 2005 yılında yürürlüğe giren 5237 Sayılı Türk Ceza Kanunu'nda m. 135 ila 140'ta özel hükümler yer almış; kişisel verilerin kaydedilmesi (m. 135), verileri hukuka

aykırı olarak verme veya ele geçirme (m. 136), verileri yok etmeme (m. 137) suçları düzenlenmiştir. 5271 sayılı Ceza Muhakemesi Kanunu m. 80'de beden muayenesi ve vücuttan örnek almaya ilişkin hükümler doğrultusunda alınan örneklerin kişisel veri niteliğinde olduğu belirtilerek, bu verilerin korunmasına yönelik hükümler getirmiştir.

Özel hukuk alanında ise, kişisel verilerin korunmasına yönelik hükümlerin çeşitli kanunlarda yer aldığı görünmektedir. Bu hükümlerin genelde sır saklama yükümlülüğü üzerinden kişisel verilerin korunmasını sağlamakta olduğunu ifade etmek gerekir.

Bu doğrultuda, örneğin, 2003 yılında yürürlüğe giren 4857 Sayılı İş Kanunu m. 75'te işveren, işçinin kişisel bilgilerini açıklamamakla yükümlü tutulmuştur. 2006 yılında yürürlüğe giren 5411 Sayılı Bankacılık Kanunu m. 73'te, kanunda zikredilen görevlilerin, görevleri sırasında öğrendikleri müşterilerine ait sırları yetkili olanlardan başkasına açıklamamakla ve kendilerinin veya başkalarının yararlarına kullanamamakla yükümlü tutulmuştur. 2012 yılında yürürlüğe giren 5684 Sayılı Sigortacılık Kanunu m. 31/A'da, sigorta sözleşmesinde ilgili kişilere ait sırların korunmasına ilişkin hükme yer verilmiştir.

Sır saklama yükümlülüğünün yanı sıra doğrudan kişisel verileri korunmasına yönelik getirilmiş hükümler de bulunmaktadır. Burada, madde hükümlerinde kişisel verilerin korunması lafzının yer alması kanun koyucunun kişisel verilerin korunmasına özel önem verdiğini göstermektedir.

Örneğin, 2004 yılında yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu m. 12'te, kişisel verilerin ilgili kişinin rızası dışında işlenmesi yasaklayan hükümler getirilmiştir.

5510 Sayılı Sosyal Sigortalar Ve Genel Sağlık Sigortası Kanunu m. 78'de, sigortalı ve bakmakla yükümlü olduğu kişinin sağlık bilgilerinin gizliliğinin esas olduğuna ilişkin hükme yer verilmiştir.

5718 sayılı Milletlerarası Özel Hukuk Ve Usul Hukuku Hakkında Kanun m. 35'te, kişisel verilerin işlenmesi ile kişilik haklarının ihlaline uygulanacak hukuku belirleyen bir hükme yer vermiştir.

6098 sayılı Türk Borçlar Kanunu m. 419'te işverenin, işçinin kişisel verilerini kullanması, çeşitli şartlara bağlanmıştır.

6102 Sayılı Türk Ticaret Kanunu m. 24'te, ticaret siciline kayıt edilecek kişisel verilerin, kişisel verilerin korunması kurallarına uygun şekilde korumaya sahip olması gerektiği belirtilmiştir.

6114 sayılı Ölçme, Seçme Ve Yerleştirme Merkezi Hizmetleri Hakkında Kanun m. 6'da, görevli personelin görevi sırasında öğrendiği kişisel verileri ve ticari sırları işlemesi kural olarak yasaklanmıştır.

6362 sayılı Sermaye Piyasası Kanunu m. 87'de, veri depolama kuruluşları madde başlığı altında diğer verilerle birlikte kişisel verilerin de depolanması usulüne ilişkin kurallar belirlenmiştir.

6458 sayılı Yabancılar Ve Uluslararası Koruma Kanunu m. 99'da, kişisel verilere ilişkin bir başlık oluşturulmuş ve ilgili mevzuata ve taraf olunan uluslararası anlaşmalara uygun olarak işleneceği hükme bağlanmıştır.

6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun m. 10'da kişisel verilerin korunması başlıklı madde ele alınmış ve hizmet sağlayıcıların elde ettikleri kişisel verilerin saklanması ve güvenliğinden sorumlu tutulup ilgili kişinin rızasının kapsamı dışında işlenemeyeceği düzenlenmiştir.

Kişisel verilerin insan hakları bağlamında korunmasının talep edilebilmesinin önü 2010 yılında Anayasa m. 20'ye eklenen fıkra ile açılmıştır. Özel hayatın gizliliği maddesine eklenen fıkra ile kişisel verilerin korunması hakkı güvence altına alınmıştır.

Bu doğrultuda, 2016 yılında KVK Kanunu yürürlüğe girmiştir. Türk hukukunda 2003 ve 2008 yıllarında da AB müktesebatı ve uluslararası hukuk normlarıyla uyumlaşma amacı çerçevesinde kişisel verilerin korunması konusunda kanun taslakları hazırlanmış olsa da bunların kanunlaşamamış olduğunu belirtmek de gerekir.

Dolayısıyla, son 20 yılda çıkarıldığı görülen tüm bu kanun maddeleri ele alındığında, kişisel verilerin korunması konusunun öteden beri daha çok özel hukuk bağlamında gündeme geldiği ortadadır. Keza hali hazırda genel olarak ceza hukuku, özel olarak ise kişisel verilerin soruşturma evresinde korumaya yönelik uygulanacak bir hukuk metni de henüz Türk hukukunda bulunmamaktadır. Fakat tezimizin ilerleyen kısımlarında göstereceğimiz üzere ceza hukuku alanında da verilerin korunmasına yönelik hükümlerin varlığı bir ihtiyaçtır.

B. Kişisel Verilerin Korunması Kanunu İle Kişisel Verilerin Korunması

1. Genel Olarak

Yazımızın bu kısmında geniş kapsamlı olarak değerlendirmekte olduğumuz 6698 sayılı KVK Kanunu, hem kişisel verilere ilişkin yerel hukuk kuralları arasında bütünsellik sağlanması hem de uluslararası hukukun yeni gelişmelerle geldiği noktaya uyum sağlamak amacıyla 24.03.2016 tarihinde çıkarılmıştır. Son 20 yıl içinde farklı yıllara ait birden fazla tasarıya sahip olan fakat kanunlaşma süreci geciken bir kanundur. Bu kanun öncesinde, Türkiye'nin taraf olduğu uluslararası anlaşmalar ile yerel hukuk kuralları arasında kişisel veriler konusunda yeknesaklık bulunmamaktaydı. Bu doğrultuda, iç hukuktaki kanun eksikliği 6698 sayılı Kanun ile şeklen doldurulmuştur. Artık bu kanun, kişisel veriler ile ilgili temel düzenleyici hukuk metni konumundadır. Öte yandan, KVK Kanunu'ndaki genel nitelikli hükümleri özelleştirmek ve yer verilmeyen hususları düzenlemek adına 2017 yılında KVK Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik çıkarmıştır. KVK Kanunu'na dayanılarak çıkarılan bu yönetmelikte, kişisel verilerin saklanma ve imhasına ilişkin politikalar, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin esaslar düzenlenmektedir.

KVK Kanunu'nun eleştirilmeye açık temel bir noktası, daha eski düzenlemelerin takip edilerek düzenlenmiş olması nedeniyle yerel hukukun güncel uluslararası düzenlemelerle yeknesaklaştırılamamış olmasıdır. Avrupa Birliği metinlerine kıyaslandığında hem eksik yönleri hem de en güncel metin olan GDPR'ye göre geri kalmışlığı söz konusudur[223]. Üstelik kişisel verilerin korunmasının tali, istisnalarının ise esas olacak şekilde düzenleyen bir bakış açısıyla ele alınmıştır[224]. Dolayısıyla, hem GDPR ve 2016/680/EU sayılı Direktif'e göre hazırlanmayışı hem de bağdaşmayan hükümler içeriyor oluşu sebebiyle bu kanunda ilerleyen dönemlerde AB ile uyumlaşma çerçevesinde değişiklik yapılması gerekeceği aşikârdır. Bu durumun, sadece idareye karşı değil, yerel ve uluslararası kar amaçlı tüzel kişilere karşı ve kendileri arasındaki sözleşme ilişkilerine de olumsuz anlamda etki edeceği aşikârdır.

[223] Oturaklı, s. 13.
[224] 6698 sayılı Kanun Gerekçesi, s. 71.

2. Kanunun Düzenlenme Amacı, Kapsamı ve Kanunda Yer Verilen Tanımlar Açısından

a) Kanunun düzenlenme amacı ve kapsamı

6698 sayılı Kanun'un amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir. Dolayısıyla, değişik temel hak ve hürriyetlere dayanan taleplerin konusunun kişisel veri ile bağlantılı olması halinde bu kanun gündeme gelebilecektir. Diğer bir deyişle, koruma amacı kapsamında birden fazla temel hak ve hürriyetin korunması amacı güdülmektedir.

Ayrıca, hangi hakların korunacağının sayılmamış olması sebebiyle kişisel verilerin korunması adı ve amacı doğrultusunda çıkarılan bu kanunun kişisel verileri özel hayatın gizliliğinden bağımsız bir temel hak olarak koruma amacında olabileceği çıkarımını da yapabilmek bizce mümkündür. Çünkü aksi düşünüldüğünde korunması gereken temel hak ve hürriyetler sayılabilirdi. Fakat bu yoldan gidilmeyerek korunması gereken haklar belirsiz bırakılarak bu haklar içerisinde kişisel verilerin münhasıran bir insan hakkı olarak korunmasına kapı aralanmaktadır. Yine de, kanunun getiriliş amacı olan kişisel verilerin korunmasının KVK Kanunu'nda açıkça bir hak olarak belirtilmemesi de eleştirilmektedir. Bu doğrultuda, kişisel veriler konusunda sağlıklı bir koruma sağlanması için kişisel verilerin korunmasının hukuki metinlerde diğer anayasal temel hak ve hürriyetler gibi artık açıkça belirtiliyor olması gerektiği düşünülmektedir[225].

Kanunun kapsamı verilerin tamamen veya kısmen otomatik yollarla ya da herhangi bir veri kayıt sistemini parçası olmak kaydıyla otomatik olmayan yollarla işlenmesini kapsamaktadır[226]. Buna göre, kanun koyucunun esasında verilerin işlenmesinde kanunun kapsamı itibariyle etki etmediği bir alan bırakmamak gayesinde olduğu anlaşılmaktadır. Ayrıca, koruma ihtiyacının ortaya çıkabilmesi için işlemenin vuku bulmasının gerekli olacağı da bu maddeden anlaşılabilmektedir. Yani kişisel verilerin korunmasının bu kanun kapsamında talep edilebilmesi için öncelikle bir işleme faaliyetinin gerçekleşmiş olması gerekmektedir.

[225] Dülger, 2019, s. 73.
[226] KVK Kanunu, m. 2.

KVK Kanunu bilindiği üzere kural olarak gerçek kişilerin verilerini kapsamakta, tüzel kişilerin verilerini kapsamamaktadır. Tüzel kişilerin kapsam dışında bırakılması uluslararası eğilimlerle de örtüşmektedir[227]. Gerçek kişi ile ilişkilendirilebilecek bir tüzel kişi verisinin ise korunma kapsamına dâhil olması gerektiğini yukarıda ifade etmiştik. Bu görüş doğrultusundaki bir eleştiriye göre, gerçek kişi ile ilişkilendirilebilecek tüzel kişi veri türlerinin ne olduğunun kanunda sayılmaması önemli bir eksikliktir[228].

b) Tanımlar

KVK Kanunu'ndaki tanımlardan ilk olarak, kişisel veri tanımına değinmek gerekir. Buna göre, kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi tanımladığı ifade edilerek veri kelimesi yerine bilgi kelimesi tercih edilmiştir. Dolayısıyla buradan, kişisel veriler kişisel bilgilerden müteşekkildir anlamı da çıkmaktadır. Fakat kanunun genelinde, diğer hükümlere bakıldığında bilgi ve veri ayırımının yapılmamakta olduğu ve bunların eş anlamlı olarak kullandığı görülmektedir. Dolayısıyla, her ne kadar farklı çağrışımlar yapsa da, kişisel veri ya da kişisel bilgi KVK Kanunu açısından aynı şeyi ifade etmektedir.

Tanımlarla ilgili ikinci husus, kişisel verilerin işlenmesi tanımı ile ilgilidir. Kişisel verilerin işlenmesi, verilerin elde edilmesi, kaydedilmesi, depolanması, elde edilebilir hâle getirilmesi, sınıflandırılması gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir[229]. Bu doğrultuda internet sitelerindeki verilerin sistemli bir şekilde tarama motorlarınca taranması ve listeler halinde sunulmasında da işlenme fiili gerçekleşmektedir[230].

Kişisel verilerin işlenmesi tanımlanırken, bizim görüşümüze göre, kişisel verilerin işlenmesini herhangi bir veri kayıt sisteminin parçası olması şartına bağlı olarak tanımlama yapılmış olması izaha muhtaçtır. Aksi halde, kişisel verilerin veri kayıt sistemi dışında kaydedilmesi KVK Kanunu kapsamında hukuka uygun işlemeymiş intibaı

---

[227] Çekin, s. 21.
[228] Dülger, 2019, s. 199.
[229] Kişisel verilerin işlenmesi hükmü KVK Kanunu m. 3(1)(e)'de düzenlenmektedir:
"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 işlemi, …" ifade etmektedir.
[230] Çekin, s. 40.

uyandırmaktadır ki bu yönde böyle bir sınırlama getirilmesinin sebebini sorgulatmaktadır. Keza TCK m. 135'te kişisel verilerin kaydedilmesi suçu herhangi bir nesne üzerinde işlenebilmekte ve kayıt işleminin herhangi bir veri kayıt sisteminin parçası olup olmadığına bakılmamaktadır. Üstelik KVK Kanunu ile TCK'da kişisel verilerle ilgili hükümlerin destekleyici olarak birlikte uygulanması söz konusu olacağından bu iki kanun arasında böyle bir uyumsuzluk olmaması gerekmektedir. Bu yüzden, kişisel verilerin işlenmesini herhangi bir veri kayıt sisteminin parçası olması şartının kaldırılması hukuka daha uygun olacağını belirtmek gerekir. Genel gerekçede de TCK atfı ile ilgili görüşümüz desteklenmekte fakat neden kayıt sisteminin parçası olması gerektiğine ilişkin sebeplere yer verilmemektedir.

Tanımlarla ilgili üçüncü olarak, KVK Kanunu'nun diğer maddelerinde sıkça gönderme yapılan açık rıza hususuna değinmek gerekmektedir. KVK Kanunu'na göre, bu kanunun uygulanmasında açık rızanın belirli bir konuya ilişkin olmak kaydıyla hem bir bilgilendirmeye dayanması hem de özgür irade ile açıklanıyor olması gerekmektedir. Öyle ki, bu iki şarttan birinin yokluğunda açık rızadan bahsedilemeyecektir. Bilgilendirmeye dayanmasından maksat anlaşılabilirlik ve erişilebilirlik olarak ifade edilmekteyken, özgür iradeden maksat TBK uyarınca irade bozukluğunun oluşmamasını ifade etmektedir[231].

Tanımlarla ilgili dördüncü husus, anonimleştirmenin tanımı ile ilgilidir. Buna göre kanun, anonimleştirmede can alıcı unsur olarak verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getiriliyor olmasını öne çıkarmaktadır. Buradan hareketle, kişisel verilerin bir kişi ile ilişkilendirilebiliyor olması, kişisel verilerin işlenmesinin gündeme gelmesine sebep olan ve bir tehlikeyi yansıtan unsur olarak görülebilecektir. Ayrıca, ilişkilendirilecek ilgili kişi, kişisel verisi işlenen gerçek kişi olacağı belirtilerek tüzel kişilerin kesin olarak kişisel veri sahibi olamayacağı ortaya konulmuştur.

Tanım maddesi ile ilgili son değinmek istediğimiz husus, veri sorulusu terimidir. Buna göre veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmaktadır. KVK Kanunu'nu m. 28'deki istisnalardan bağımsız olarak yorum yapıldığında, soruşturma evresinde delil toplama amacıyla kişisel verilerin

[231] Oturaklı, s. 22.

işlenmesi kararını veren hâkim, savcı yahut kolluk görevlilerinin bu açıdan veri sorumlusu olarak görülebileceğini ifade etmek gerekmektedir. Ayrıca bu yorumun önemli olduğunu düşünmekteyiz çünkü ideal hukuk açısından tezin diğer kısımlarında daha detaylı olarak belirtmekte olduğumuz üzere veri sorumlusunun varlığı kişisel verilerin soruşturma evresinde korunabilmesi için gereklidir. Kanunda düzenlenen koruyucu hükümlerin işlerliğini orantısız bir bıçak gibi kesen ve önleyen m. 28'deki bu istisna hükümlerinin değiştirmesi gerekmekte olduğunu yeri gelmişken bu hüküm açısından da bir kez daha ifade etmek gerekir.

3. Korumaya İlişkin İlkeler ve Verilerin Niteliği Açısından

a) Kişisel Verilerin İşlenmesinin Genel İlkeleri

KVK Kanunu m. 4'te kişisel verilerin işlenmesine yönelik genel ilkeleri düzenlenmektedir. Buna göre, kişisel veriler ancak bu kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilecektir.

Buradaki diğer kanunlar ibaresi, 1982 Anayasasının m. 90(5) hükmü uyarınca usulüne göre yürürlüğe konulmuş milletler arası anlaşmaları kapsamakta olduğunu hatırlatmak gerekir. Bilindiği üzere bunlar da kanun hükmünde olarak artık yerel mevzuatın bir parçası konumundadırlar ve yürürlükte olma açısından diğer kanunlardan hiçbir farkları bulunmamaktadır.

Dolayısıyla, hükümden çıkan anlama göre, kişisel verilerin korunması konusunda Türkiye'nin kabul ederken çekince ya da beyan koyduğu hususlar hariç olmak üzere ilgili uluslararası anlaşmalarda öngörülen usul ve esasların meri hukuk açısından bağlayıcıdır. Diğer bir deyişle taraf olunan uluslararası anlaşmalara uymadan yapılacak bir işleme faaliyeti, kanuna aykırı bir işleme olacaktır. Öte yandan, Anayasa m. 90(5)'in devamında, usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletler arası anlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletler arası anlaşma hükümlerinin esas alınacağı kesin ve açık bir biçimde hükme bağlanmıştır. İster kişisel verilerin korunması isterse özel hayatın gizliliği bağlamında kabul edilsin, konusu kişisel veri olan uluslararası anlaşmaların temel hak ve özgürlüklere ilişkin olduğu ortadadır. Bu sebeple, iç hukuktaki düzenlemeler ile uluslararası anlaşmaların kişisel verilerin işlenmesine ilişkin hükümler içermesi

nedeniyle çıkabilecek uyuşmazlıklarda milletler arası antlaşma hükümleri esas alınacaktır.

Kişisel verilerin işlenmesinde uyulması gereken genel ilkeler, kişisel verilerin korunmasının anayasası gibidirler. Bu yüzden, genel yahut hassas nitelikli verilerin işlenme şartlarından bağımsız olarak her daim mutlak olarak uyulması gerekmektedir. KVK Kanunu'ndaki genel ilkeler şu şekilde düzenlenmektedir:

- İşlemenin hukuka ve dürüstlük kurallarına uygun olması;
- Doğru ve gerektiğinde güncel olması;
- Belirli, açık ve meşru amaçlar için işlenmesi;
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi.

Diğer ilkelerin yanı sıra işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin tezimiz kapsamında anahtar niteliğinde bir ilke olduğunu belirtmemiz gerekmektedir. Keza soruşturma evresinde delil toplama amacıyla işlenecek her verinin diğer ilkelerle birlikte bu ilke doğrultusunda da işlenme amacıyla bağlantılı, sınırlı ve ölçülü olması gerekeceği hususuna tezimizin ilerleyen kısımlarında sıklıkla atıfta bulunacağız. Bu ilkeyi açmak gerekirse, amaçla bağlılık ilkesinin, kişisel verilerin önceden belirlenmiş veya belirlenebilen hukuka uygun amaçlar için işlenmesini ifade etmekte olduğunu belirtmek gerekir[232]. Ölçülülük ilkesi, uygunluk, gereklilik ve orantılılık olmak üzere üç alt ilkeyi kapsamakla birlikte kişisel verilerin korunmasına ilişkin diğer ilkelerle içsel bağlantısı olan bir ilkedir[233]. Öyle ki diğer ilkelerin ihlal edilmesi büyük olasılıkla ölçülülük ilkesinin de ihlal edilmesine yol açmaktadır.

Öte yandan, kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesinin, GDPR m. 5 ile bağdaşmamakta olduğunu belirtmek gerekir. GDPR hükmü verilerin yalnızca amaç doğrultusunda sınırlı süre boyunca muhafaza edilebileceğini söylemekteyken, KVK Kanunu hükmü buna ek olarak, kanuni düzenleme varsa da hukuka uygun kabul etmektedir. Ayrıca diğer yönden

[232] Ayözger Öngün, s. 138.
[233] Gürsel, s. 235.

soruşturma evresinde kişisel verilerin işlenmesine yönelik süre sınırı getiren herhangi bir mevzuat hükmü de bulunmamaktadır.

b) Genel Nitelikli Kişisel Verilerin İşlenme Şartları

Kişisel verilerin işlenme şartları, genel ilkelerden farklı fakat onlara bağlıdır[234]. Bu şartların ve istisnalarının her birinin kişisel verilerin işlenmesinde m. 4'te sayılan genel ilkelere ve tarafı olduğumuz milletler arası antlaşma hükümlerine uygun olması gerekmektedir.

Kişisel verilerin işlenmesinde ilgili kişinin açık rızası olması temel kuraldır. İşleme şartının kural olarak kişinin rızasına bırakılmış olması ise kişisel verilerin korunmasında kişinin rızasının esas alınmakta olduğuna işaret etmektedir. Dolayısıyla hukuka uygun olarak rıza verilmiş verilerin işlenmesinin önünde hiçbir engel bulunmamaktadır. Burada ilgili kişinin açık rızasının temel işleme şartı olduğuna dikkat edilmelidir. Fakat ilgilinin açık rızası alınırken, verilerin işlenmesindeki görünen amaç dışında işleyene fayda sağlayacak farklı bir amaç varsa bunun da ilgiliye açıkça belirtilmesi gerekmektedir[235].

Ayrıca her ne kadar açık rıza temel alınacak olsa da kişinin vücut bütünlüğü üzerindeki hakkının sınırsız olmaması ilkesi gözetildiğinde rızanın özellikle sağlık verileri söz konusu olduğunda meslek mensubu tarafından somut olaya göre değerlendirilmesi gerekir[236].

Çocukların rızası açısından durumun ne olacağı konusunda ise, 16 yaşından küçüklerin ancak yasal temsilcilerin onayı ile geçerli bir rıza beyanında bulunmaları şartı aranması ve çocuğun rıza açıklamasının sonuçlarını öngörebilecek nitelikte olup olmadığı öncelikle incelenmesi gerektiği belirtilmektedir[237].

Rızanın alınması kuralının birkaç tane istisnası bulunmaktadır. Bu istisnalardan birincisi, kanunlarda açıkça öngörülmesi halidir. Kanunda açıkça öngörüldüğü takdirde artık verilerin işlenmesinde kişinin rızasının aranmayacaktır. Kişisel verilerin soruşturma evresinde kapsam dışı bırakılmamış olsaydı, verilerin işlenmesinde bu istisna hükmü

[234] KVK Kanunu, m. 5.
[235] Hildebrandt, Mireille/Gutwirth, Serge: Profiling the European Citizen: Cross-Disciplinary Perspectives, Berlin 2008, s. 203.
[236] Yılmaz, s. 49.
[237] Çekin, s. 63.

doğrudan gündeme gelecekti. Çünkü kişinin rızası dışında verileri işlenerek kişisel verilerin korunması hakkına müdahale edilmektedir. Ayrıca, söz konusu kanun hükümleri kişisel verilerin korunması hakkını kısıtlayan hükümler oldukları için, temel hak ve hürriyetlerin sınırlanması hükümlerine uygun olarak düzenlenmesi gerekmektedir. Aksi halde hukuka uygun bir sınırlamadan bahsedilemez.

İkinci istisna, 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 halidir. Buna, kendisine karşı bir suç işlendikten sonra mağdurun komaya girmesi hali örnek gösterilebilir.

Üçüncü istisna, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halidir. Buna örnek olarak ise işe alım sürecinde işveren tarafınca işçinin kişisel verilerinin alınması gösterilebilir.

Dördüncü istisna, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için verilerin işlenmesinin zorunlu olması halidir. Burada veri sorumlusunun hukuki yükümlülüğünün olması ve bir zorunluluk bulunması şartlarının birlikte olması gerektiğine dikkat edilmelidir. İki şarttan birinin aynı anda yokluğunda bu istisna kapsamında hukuka uygun bir işlemenin varlığından bahsedilemez.

Beşinci istisna, kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması halidir. Kişinin kendi iradesiyle alenileştirilmiş olan verilerin korunmaya değer veri olarak görülmemesi gerekir. Alenileştirilmiş verinin kanun kapsamında korunmadığının benimsenmesi hangi verilerin korunacağını belirlemeye daha elverişli bir sınıflandırma imkânı sunmaktadır. Dolayısıyla, bu hüküm istisnalar içerisinde değil korunmaya değer olan ve olmayan veriler ayırımı sınıfı içerisinde korunmaya değer olmayan veriler sınıfı kapsamında düzenlenmelidir.

Bu istisnaya ilişkin bir diğer önemli nokta ise, kişisel verinin veri sahibi tarafından alenileştirilmemesine rağmen, veri sahibinin açık veya örtülü rızası olması halidir. Her ne kadar kişisel verinin ilgili kişinin açık rızası olmadan işlenemeyeceği bu madde bağlamında kural olarak benimsenmiş olsa da örtülü rızanın varlığında ne olacağı açıkça düzenlenmemektedir. Bizim görüşümüze göre örtülü rızanın varlığında açık rıza kuralı

hükmü bu iki durum farklı olduğundan dolayı uygulanmamalıdır. Olması gereken, her ne kadar ilgili kişinin kendisi tarafından alenileştirilmese de alenileştirmeye örtülü de olsa rızasının varlığı sebebiyle bu istisna kapsamında düşünülmesidir.

Altıncı istisna, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması halidir. Bu istisna ile ilgili olarak özellikle şunu belirtmek gerekir ki, haber alma özgürlüğü gibi kişisel verilerin korunması hakkı ile diğer hakların çatıştığı durumlarda, kişisel verilerin işlemesinde gerçek bir zorunluluğun varlığı aranmalıdır. Keza özel hayatın gizliliği bağlamında hukuka uygun bir işleme faaliyetinin varlığı, demokratik toplum düzeninde gerekli olması, üstün bir sosyal ihtiyacı karşılaması ve özellikle de hedeflenen meşru amaçla orantılı olması ve ulusal makamlar tarafından öne sürülen gerekçelerin yeterli olmasını gerektirmektedir[238]. Bu, demokratik bir toplum düzeni sağlanmasının asgari şartlarından olup aksi halde kanuna aykırı bir işleme söz konusu olacaktır.

Son istisna hükmü ise, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halidir. Meşru menfaat gerekçede bir örnekle açıklanmaya çalışılmıştır[239]. Fakat esasen kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi olarak nitelendiğinden orantılı bir ölçü anlamına gelmektedir.

Anayasa Mahkemesi kanunun bu hükmü için açılan iptal davasında, bu terimin çalışanların temel hak ve özgürlüklerine zarar vermemek kaydıyla, temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi olduğunu belirtmektedir[240]. Bununla birlikte bu açıklamalar yeterli görünmemektedir çünkü zikredilen dengeyi sağlayacak unsurların nasıl belirleneceğinin belirtiliyor olması şarttır. Bu eksiklik terimden anlaşılması gereken anlamın ne olduğunu belirsiz bırakmaktadır.

---

[238] S. ve Marper/Birleşik Krallık, par. 101; Coster/Birleşik Krallık, Başvuru No: 24876/94, Büyük Daire Kararı, 18.01.2001, par. 104, Erişim Tarihi: 6 Şubat 2019.

[239] Zikredilen örneğe 6698 sayılı Kanun Gerekçesi, s. 9'da yer verilmektedir:
"…örneğin bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki şirket sahibinin meşru menfaati cümlesindendir…"

[240] E. 2016/125, K. 2017/143, KT: 28.09.2017, RG. 30310, 23.01.2018, par. 41, 47, Erişim Tarihi: 6 Şubat 2019.

Doktrinde de, hangi durumlarda veri sorumlusunun meşru menfaatinin kişinin kişisel verilerinin korunması hakkı karşısında üstün geleceğinin açıklığa kavuşturulmasının gerekli olduğu ifade edilmektedir[241]. Meşru menfaat, bize göre ya kanunun verdiği bir yetkiden ya da örf adet gereği işin icabından kaynaklanabilecektir. Bunun yanı sıra, meşru menfaat hükmü kapsamında öne sürülecek bir gerekçenin işlemenin belirli ve açık olması gerektiği ilkesine uygun nitelikleri haiz olması gerekeceği unutulmamalıdır.

c) Hassas (Özel) Nitelikli Kişisel Verilerin İşlenme Şartları

(1) Genel olarak

Hassas nitelikli kişisel veriler, alelade kişisel verilere göre kişinin hayatının en mahrem yönüne tekabül etmesi ve sadece belli bir kişiye münhasır olabilecek verileri içinde barındırması sebebiyle hukuk kurallarında daha çok korumaya haiz olan verilerdir.

Hassas veriler, KVK Kanunu'nda özel nitelikli kişisel veri olarak adlandırılmakta ve bu tür verilerin işlenme şartları m. 6'da sınırlayıcı olarak sayılmaktadır. Buna 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 mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verilerdir.

Kişisel verilerin işlenmesinde özel nitelikli veri türleri kapsamının KVK Kanunu'nda 1981 yılı tarihli VKS'ye göre daha geniş olduğunu ifade etmek gerekir. Keza KVK Kanunu'nda VKS'ye ek olarak kişinin etnik kökeni, felsefi inancı, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği ile biyometrik ve genetik verileri de özel veri kategorisi içinde sayılmaktadır.

Bir görüşe göre, sağlık verilerinin bir bütün halinde özel nitelikli veri olarak görülmesi, bütün sağlık verilerinin bu nitelikte olmayacağı nedeniyle isabetli değildir. Bu noktada örnek olarak bir kişinin ayağının kırıldığı bilgisinin her zaman özel nitelikli bir sağlık verisi olmayacağını, bu nedenle de özel nitelikli verilerle aynı kapsamda değerlendirilmemesi gerektiğini ileri sürmektedir[242].

[241] Dülger, 2019, s. 219.
[242] Hervey, Tamara/McHale, Jean: Health Law and the European Union, Cambridge 2004, s. 171.

Özel nitelikli kişisel verilerin işlenmesi kapsamında son olarak belirtmek gerekir ki, KVK Kurulu tarafından belirlenen yeterli önlemlerin alınması şart koşularak bu konudaki ayrıntılar KVK Kurulu tarafından çıkarılacak yönetmelik, tebliğ vs. düzenlemelere bırakılmıştır.

(2) TCK m. 135(2)'te özen nitelikli verilerin kaydedilmesinin nitelikli hal olarak düzenlenmesi

TCK m. 135 kişisel verilerin kaydedilmesi suçunu düzenlemektedir. TCK m. 135(2)'ye göre ise, kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda bu madde bağlamında verilecek cezanın artırılacağı hükme bağlamıştır.

Belirtmek gerekir ki bu fıkrada sayılan veriler özel nitelikli kişisel veri olduğu için cezada artırım yapılmaktadır. Fakat KVK Kanunu'nda belirtilen etnik köken, mezhep, kılık ve kıyafet, dernek, vakıf üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler bu madde kapsamına alınmamıştır. Dolayısıyla, kişisel verilerin kaydedilmesinin düzenlenmekte olduğu bu suçta, kapsama alınmayan özel nitelikli kişisel verilerin işlenmesi halinde TCK'ya hâkim olan kanunilik ilkesi gereğince genel nitelikli kişisel verinin işlenmesi hükmü olan m. 135(1)'e tabi olacaktır[243].

İki kanun arasında bütünlük sağlanmaması nedeniyle TCK m. 135(2)'deki düzenlemenin güncel şartlara uygun olarak değiştirilmesi gereklidir. Ayrıca eğer özel nitelikli kişisel verilerin kendi içinde bir ayırım söz konusu ise bunun KVK Kanunu'nda açıkça düzenlenmesi gerekirdi diye düşünmekteyiz. Bu doğrultuda, TCK m. 135(2) içerisinde kapsama alınmayan KVK Kanunu'na göre özel veri türlerinin de m. 135(2) kapsamı içerisinde yer alması daha isabetli olurdu. Bu tutum benimsenmediğinden TCK maddesinin kişisel verilerin bütünsel olarak korunması amacına, olması gerektiği düzeyde hizmet edememektedir.

(3) İlgilinin açık rızasının alınması kuralı

[243] TCK m. 243 ve devamında düzenlenmekte olan bilişim alanındaki suçların da gündeme gelebileceği unutulmamalıdır.

KVK Kanunu m. 6(2) özel nitelikli kişisel verilerin, ilgilinin açık rızası olmadan işlenmesini yasaklamıştır. Çok açık olan bu hükme göre, işlemenin yapılabilmesi için kişinin örtülü rızası değil açık rızasının olması gerektiğine dikkat edilmelidir. Yani genel nitelikli kişisel verilerin işlenmesinde rıza yeterli iken, özel nitelikli verilerde açık rıza esastır.

Özel nitelikli kişisel verilerin işlenmesinin düzenlendiği GDPR m. 9'da, KVK Kanunu ile benzer bir düzenleme söz konusudur[244]. Fakat bir görüşe göre, kanunun bu hükmü değiştirilip özel nitelikli verilerin işlenmesi kişinin iradesine bırakılmaksızın kural olarak yasaklanması gerekmektedir[245].

(4) Açık rıza alınması kuralının istisnaları

Özel nitelikli kişisel verilerin işlenmesi için kural olarak ilgilinin açık rızasını almak gerekli olmakla birlikte bunun iki istisnası bulunmaktadır.

Birincisi, KVK Kanunu m. 6(3)'te de belirtildiği üzere sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin kanunlarda öngörülen hâllerde işlenebilecek olmasıdır. Kişinin rızası dışında verilerin işleme kapsamının bu kadar genişletilmiş olması yeterli korumanın sağlanacağı konusunda şüphelere yol açmaktadır. Kanunun gerekçesinde yer alan karşı oy yazında belirtildiği üzere, kişinin rızası dışında mezhebi ile kılık kıyafetinin dahi işlenmesine ortam sağlanması açıkça hem bir fişleme girişimine hem de ayrımcılığa kapı aralamaktadır[246].

İkincisi ise, sağlık ve cinsel hayata ilişkin kişisel verilerin 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

[244] Özel kategorilerdeki kişisel verilerin işlenmesinin düzenlendiği GDPR m. 9'a bakıldığında, ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaklanmış olduğu görülmektedir.

[245] Başalp, s. 112. Yazara göre kurala istisna olarak şu haller düzenlenmelidir: kişisel verilerin "*iş hukuku çerçevesinde işlenmesi, hayati çıkarların korunması, kamuya yararlı kurumlar, siyasi partiler, vakıflar, dernekler tarafından işlenme, kişinin kendisi tarafından kamuya açıklanan hassas verilerin işlenmesi, yargılama nedeniyle işlenen hassas veriler, tıbbi tedbirler çerçevesinde işlenme, önemli kamusal yarar, cezalara dair verilerin kaydedilmesi, ulusal kimlik numarası."* Bu görüşten anlaşıldığına göre, yazar verinin hassaslığının belirlenmesi hususunda kişinin iradesine ve kamu yararına öncelik tanımaktadır.

[246] 6698 sayılı Kanun Gerekçesi, s. 71.

işlenmesidir. Burada "ancak" ibaresine dikkat edilmelidir. Keza sayılan durumlar söz konusu değilse sağlık ve cinsel hayata yönelik bir işlemenin hukuka uygunluğundan kesinlikle bahsedilemeyecektir. Ayrıca bu süreç içerisinde tıbbi veri bankalarının hiçbir zaman başka veri bankalarıyla ilişkili olmaması esastır[247]. Bu doğrultuda, sağlık hizmeti sunucularında veri işleyen kişiler, kişisel sağlık verilerini sadece sınırlı sistemlerde depolayabilir[248], aktarabilirler[249] ve silebilirler[250].

Aynı durum sağlık verileri ile ilgili özel düzenleme olan, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'te de belirtilmektedir. Yönetmelik m. 7'e göre, kişilerin sağlık verilerinin işlenmesinde, yukarıda zikrettiğimiz KVK Kanunu m.6(3) şartlarının varlığında kural olarak kişinin açık rızası aranmamaktadır. Açık rızanın arandığı istisna durumlarda ise kişinin KVK Kanunu m. 10'da düzenlenen aydınlatma yükümlülüğü çerçevesinde bilgilendirildikten sonra açık rızasının alınabileceği öngörülmektedir. Yönetmelik'e göre verilen rızanın her zaman geri alınabilir ve geri alınması halinde, o tarihe kadar yapılmış bulunan işlemler bakımından etkili olmamaktadır.

Öte yandan, merkezi sağlık veri sistemine aktarılan verilerin, aktarımın yapıldığı tarihten 10 yıl sonra yerel veri tabanından silinebileceği düzenlenmiştir. 10 yıl, değil hassas veriler, genel nitelikli kişisel verilerin depolanması için bile oldukça uzun bir süredir.

---

[247] Yılmaz, s. 51.

[248] Kişisel sağlık verilerinin işlenmesinde genel ilke ve esaslar hükmü Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik m. 5(5)'te düzenlenmektedir:
"Sağlık hizmeti sunucularında veri işleyen kişiler, kişisel sağlık verilerini; sağlık hizmeti sunucularının tamamen veya kısmen otomatik olan ya da otomatik olmayan her türlü sistemleri, Bakanlığın ülke genelinde hizmet vermek amaçlı kurulan sistemleri ve merkezi sağlık veri sistemi ile Genel Müdürlüğün onayladığı diğer veri kayıt ortamları haricinde hiçbir yere kopyalayamaz, kaydedemez ve depolayamaz."

[249] Kişisel sağlık verilerinin aktarılması hükmü Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik m. 8'de düzenlenmektedir:
"(1) Kişisel sağlık verileri, ancak Kanunun 8 inci ve 9 uncu madde hükümleri uyarınca aktarılabilir.
(2) Kişisel sağlık verileri, Kanunun 8 inci ve 9 uncu madde hükümlerinde yer alan şartların sağlanamaması hâlinde ancak anonim hâle getirilmek suretiyle aktarılabilir."

[250] Kişisel sağlık verilerinin silinmesi hükmü Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik m. 9'da düzenlenmektedir:
"(1) Kanun, bu Yönetmelik ve ilgili diğer mevzuat hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel sağlık verileri, resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.
(2) (Mülga:RG-24/11/2017-30250)
(3) Merkezi sağlık veri sistemine aktarılan veriler, aktarımın yapıldığı tarihten 10 yıl sonra yerel veri tabanından silinebilir.
(4) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır."

Ayrıca depolama sırasında depolanan verinin özelliği açısından ciddilik seviyesi, süresi, bağımsızca değerlendirilmesi, hassaslığı ve masumiyet karinesine aykırı olup olmayacağına dikkat edilmelidir[251]. Fakat uygulamada bu hususların denetim altında olduğunu söylemek pek mümkün görünmemektedir. Keza bu alanı düzenleyen hukuk kuralları yeterli seviyede değildir.

Ezcümle, nasıl özel nitelikli verilerin genel nitelikli verilere göre daha fazla korunması gerekiyorsa, sağlık ve cinsel hayat verilerinin de diğer özel nitelikli verilere göre daha fazla korunması gerekmektedir. Bu doğrultuda, kanun koyucunun da sağlık ve cinsel hayata yönelik kişisel verileri daha fazla koruma niyetinde olduğu da ortadadır. Kanuni düzenleme bu yönüyle her ne kadar GDPR düzenlemesine yakın olsa da istisna hükümlerinin GDPR'dan daha geniş olduğu görülmektedir. Üstelik hassas verilerin vurgusu KVK Kanununda eksik bırakılmıştır. Bunun sebebi AB metinlerinde hassas verilerin işlenmesi yasaklanmaktayken KVK Kanunu kural olarak kişinin iradesini esas alınıyor olmasıdır[252].

Tezimizin ilgili kısımlarında daha detaylı olarak değineceğimiz üzere, soruşturma evresinde şüpheli ve mağdurun sağlık ve cinsel hayatına ilişkin kişisel verileri özellikle tıbbi teşhis amacı doğrultusunda işlenebilmektedir. Oldukça hassas nitelikli olan bu verilerin işlenmesinde sır saklama yükümlülüğü altında olan kişiler başta olmak üzere işleme süreci safhasında kişisel veriyi öğrenebilecek herkesin işleme ilkelerine en fazla düzeyde riayet etmesi gerekmektedir.

Keza, GDPR m. 90 uyarınca kişisel verilerin korunması hakkı ile gizlilik yükümlülüğünün bağdaştırılması amacıyla gerekli ve orantılı olduğu hallerde, mesleki gizlilik yükümlülüğü açısından ek spesifik kuralların kabul edilmesi teşvik edilmektedir[253]. Bu doğrultuda bir görüşe göre, sağlık verileri işlenirken ilgili kişiyi ayırt

---

[251] Murray, Andrew: Information Technology Law The Law and Society, 2016 Oxford, s. 594

[252] Ayözger Öngün, s. 24. Yazara göre, sağlık gerekçeleri hariç ilgili kişinin açık rızası aranmaksızın kanunlarda öngörülen hallerde özel nitelikli verilerin işlenebileceğinin geniş ve belirsiz istisnalar yoluyla öngörülmesi hem 95/46/EC sayılı Direktif'le çelişmiş hem de temel hak ve özgürlüklere yönelik müdahalelere kapı aralamaktadır.

[253] Gizlilik yükümlülükleri hükmü GDPR m. 90'da düzenlenmektedir:
"1. Üye devletler, kişisel verilerin korunması hakkı ile gizlilik yükümlülüğünün bağdaştırılması amacı ile gerekli ve orantılı olduğu hallerde, Birlik veya üye devlet hukuku ya da ulusal yetkin makamlar tarafından koyulan kurallar çerçevesinde bir mesleki gizlilik yükümlülüğüne ya da diğer eşdeğer gizlilik yükümlülüklerine tabi kontrolörler veya işleyiciler ile ilgili olarak denetim makamlarının 58(1) maddesinin (e) ve (f) bentlerinde belirtilen yetkilerini ortaya koymak üzere spesifik kurallar kabul edebilir. Bu kurallar

etmek için ismi gibi sübjektif özelliklerinin yerine kimlik numarasını kaydetmek daha güvenli ve yeterli olacaktır[254].

4. Kişisel Verileri Koruma Kurulu'nun Bağımsızlığı ve Soruşturma Evresine Olan Etkisi

KVK Kanunu m. 21'de KVK Kurumu'nun temel yürütme organı olan KVK Kurulu'nun kuruluşuna ilişkin hükümler yer almaktadır. Buna göre, KVK Kurulu'nun, görev ve yetkilerini kendi sorumluluğu altında ve bağımsız olarak yerine getirip kullanacağı, görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişinin, KVK Kurulu'na emir ve talimat veremeyeceği, tavsiye veya telkinde bulunamayacağı düzenlenmektedir[255].

Dolayısıyla, özerk olan KVK Kurumu bünyesinde kurulacak olan bu kurula âdeta bağımsız hareket etme imkânı tanınmaktadır. Fakat bu durum, bir kurum özerk iken onun içerisindeki bir kurul oluşumunun pratik hayatta nasıl bağımsız olacağı ile ilgili endişelere yol açmaktadır.

Kaldı ki dokuz üyeden oluşan bu Kurul'un beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi de Cumhurbaşkanı tarafından seçilmektedir. Her ne kadar Kurul'a üye olmada tarafsızlık ilkesi doğrultusunda herhangi bir siyasi parti üyesi olmama şartı aranmakta olsa da partili cumhurbaşkanı sistemine geçilmiş olduğundan Cumhurbaşkanı'nca seçilecek üyeler üzerinde tarafsızlıkları hususunda şüpheler devam edecektir. Ayrıca, kanunun gerekçesinde yer alan karşı oy yazısında da belirtildiği üzere, kurulun bu oluşum biçimi hem üyelerin seçimi hem de soruşturma izninin Cumhurbaşkanına bağlanması nedeniyle özerk ve bağımsız bir yapıdan uzaktır[256].

Bunun dışında, KVK Kanunu m. 22'de, KVK Kurulu'nun görev ve yetkilerini düzenlemektedir. Buna göre Kurul'un bir görevi, kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamaktır. Fakat bu hususun nasıl yapılacağı

---

yalnızca kontrolör veya işleyicinin bu gizlilik yükümlülüğü kapsamına giren bir faaliyet sonucu aldığı veya bu faaliyet esnasında elde ettiği kişisel veriler açısından uygulanır."

[254] Solomon, Julie/Berman Jacquelin: Tools for Building Culturally Competent HIV Prevention Programs, New York 2008, s. 114.

[255] 16.11.2017'de KVK Kurumu'nca Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik çıkarılmıştır. Kurul hükmünün m. 4(3)'te düzenlenmektedir:
"Kurul, kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz."

[256] 6698 sayılı Kanun Gerekçesi, s. 71.

belirtilmemiştir. En azından, "temel hak ve özgürlüklere uygun" gibi soyut kelimeler dizgesinin yerine "bu ve ilgili kanun hükümlerine uygun olarak işlenmesini sağlamak" olarak düzenlenebilirdi diye düşünmekteyiz. Ayrıca bu maddede verilen yetki uyarınca, KVK Kurulu'nun kişisel verilerin korunması konusunda yönlendirici bildiriler yayınlaması halinde bu bildirilerin hukuki niteliğinin ne olacağı hususunda tartışmalı olacağını düşünmekteyiz[257].

Öte yandan, KVK Kanunu m. 15(5)'te KVK Kurulu'nun kişisel verilerin soruşturma evresinde hukuka aykırı olarak işlenmesini, yapacağı resen inceleme sonucunda öğrenip ilgili makamlardan aykırılıkların giderilmesini isteyebileceği düzenlenmektedir. Bu hüküm de yürütme ile dolaylı yoldan organik bağı söz konusu olan Kurul'un yani yürütmenin yargıya müdahalesi olarak tartışmalara yol açabilecektir.

KVK Kanunu m. 15(6)'da ise, KVK Kurulu'nun yaptığı inceleme sonucunda kişisel verilerin işlenmesinde söz konusu olan ihlalin yaygınlığını tespit etmesi halinde, bu konuda ilke karar alabileceği ve bu kararı yayımlayabileceği düzenlenmektedir[258]. KVK Kanunu m. 15(7)'de ise KVK Kurulu'nun telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebileceği yetkisi düzenlenmektedir. Buradan hareketle, KVK Kurulu'na bir bakıma idari mahkemelerin yetkisi altında olan yürütmeyi durdurma yetkisi tanınmaktadır ki bu hukuk devletinin temel ilkelerinden olan güçler aykırılığı ilkesine uygunluk teşkil etmemektedir.

5. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi

KVK Kanunu m. 7'de kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi hususlarını düzenlemektedir. Buna göre, ilgili tüm kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması

[257] Gene bir başka görev olarak, KVK Kurulu'nun görev alanı ile KVK Kurumu'nun işleyişine ilişkin konularda gerekli düzenleyici işlemleri; veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlemleri; ve veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapması düzenlenmektedir. Bu düzenleyici işlemlerin hangi norm sıfatıyla normlar hiyerarşisinde nerede duracağı ve bağımsız mahkemelerin önlerine gelen uyuşmazlıklarda bu normlara dayanıp dayanamayacağı şimdiden tartışmalara gebedir. Ayrıca bu kurulun düzenleyici işlem yapabiliyor oluşu hukuken mümkün olup olmadığına bakılması gerekmektedir. Ayrıca m. 4(3)(b)'ye göre kurul kararlarının tebliğ niteliğinde olduğu belirtilmiştir.

[258] Kurulun bu kararlarının normlar hiyerarşisindeki yerinin ne olacağı tartışılabilir.

hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

Soruşturma evresinde hukuka uygun işlenen verilerin, işlemesini gerektiren sebeplerin ortadan kalkması hâlinde silinmesi, yok edilmesi veya anonimleştirilmesinin gerekli olduğu üzerine bir tartışma bulunmamaktadır. Bunun yanı sıra hukuka aykırı olarak işlenen tüm kişisel veriler için de aynı usul işlemlerinin yapılmalıdır.

Her ne kadar kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin usul ve esasların tabi olacağı belirtilen yönetmelik, 2017 yılında KVK Kurumu'nca çıkarılmış olsa da Yönetmelik hükümleri içerisinde kişisel verilerin soruşturma evresinde nasıl silineceği, yok edileceği ve anonim hale getirileceğine ilişkin hükümlere yer verilmemesi önemli bir eksikliktir.

Dolayısıyla, kişisel verilerin soruşturma evresinde işlenmesine yönelik olarak, bu verilerin nasıl silineceği, yok edileceği ve anonim hale getirileceği konusunda uygulanacak hukuk kuralları bulunmamaktadır. Düzenleme eksikliği sebebiyle, kişisel verileri işleyen kamu görevlilerini bağlayan hükümler olmadığından verilerin imhasına hem hangi kuralların uygulanacağı konusunda belirsizlik yaşanmakta hem de görevliler sınırlanmamış yetkilere sahip olmaktadır.

Sonuç olarak bu konunun kamu görevlilerinin geniş takdirine bırakılması, bu boşluğun kötüye kullanımına kapı aralamasının yanı sıra anayasal bir hakkın tatbikini kaderine terk etmektedir. Bu durum, devletin kural koyma yönündeki pozitif yükümlülüğünü yerine getirmemesi sebebiyle kişisel verilerin gizliliği hakkına sürekli olarak bir müdahalenin olduğu gösterir. Bir an önce hukuk kurallarıyla donatılması gereken bu alan, ne AB ne de AİHM standartlarıyla da bağdaşmaktadır.

6. Veri Sorumlusunun Yükümlülükleri Ve Veri Sahibinin Hakları ile İlgili Hükümler Açısından

Veri sorumlusunun kişisel verilerin elde edilmesi sırasında ilgili kişilere, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere hangi amaçla aktarılabileceği ve diğer hakları konusunda bilgi vermesi gerekmektedir[259].

[259] Veri sorumlusunun aydınlatma yükümlülüğü hükmü KVK Kanunu m. 10'da düzenlenmektedir:

Yukarıda ifade ettiğimiz gibi, her ne kadar istisna kapsamında tutulmuş olsa da varsayım olarak bakıldığında soruşturma evresinde kişisel verilerin işlenmesi kararını verebilecek olan hâkim, savcı veya kolluk amirinin bu bölümdeki hükümler bağlamında veri sorumlusu olabileceğini ifade etmek gerekir. Bu ön kabulden hareketle, işleme kararını veren kişilerin bu yükümlülüklere uyması, ilgili kişi olarak ise kişisel verisi işlenen şüpheli, mağdur ve diğer kişileri aydınlatmasının gerekeceği ifade edilebilir. Elbette bu durumun soruşturmanın gizliliği ilkesiyle çatışıyor olduğu düşünülebilir. Fakat söz konusu bildirimin soruşturma sonrası yapılmasına yönelik bir engel bulunmamaktadır.

KVK Kanunu m. 11'de kişisel verisi işlenen kişilerin sahip olduğu haklar düzenlenmektedir. Bu haklara aynı varsayımımız doğrultusunda soruşturma evresinde kişisel verisi işlenen şüpheli ve mağdurun hakları gözüyle bakılabilecektir[260]. Buna göre, ilgili kişi başta kişisel verisinin işlenip işlenmediğini öğrenme olmak üzere eğer verileri işlenmişse buna ilişkin bilgi talep etme, verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme gibi hakları bulunmaktadır.

GDPR düzenlemesi de bu maddeyle oldukça benzeşmektedir[261]. Ayrıca, GDPR kapsamında verilerinin silinmesini veya yok edilmesini ve verilerinin aktarıldığı üçüncü

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

[260] İlgili kişinin hakları hükmü KVK Kanunu m.. 11'de düzenlenmektedir:
"Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;
a) Kişisel veri işlenip işlenmediğini öğrenme,
b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."

[261] Veri sahibinin erişim hakkı hükmü GDPR m. 15'te ve düzeltme hakkı hükmü GDPR m. 16'da düzenlenmektedir:
"Madde 15 Veri sahibinin erişim hakkı:
1. Veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini kontrolörden teyit etme ve, işleme faaliyeti olması halinde, kişisel verilere erişim ile aşağıdaki bilgileri talep etme hakkı bulunur:
(a) işleme amaçları;
(b) ilgili kişisel veri kategorileri;
(c) üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri;

kişilere bildirilmesini istemenin yanı sıra işlenen verilerinin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme gibi haklar da yer almaktadır. Fakat GDPR m. 17'de bağımsız bir hak olarak düzenlenen unutulma hakkına KVK Kanunu kapsamında yer verilmemiştir[262].

(d) mümkün olması halinde, kişisel verilerin saklanması açısından öngörülen süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler;
(e) kontrolörden veri sahibine ilişkin kişisel verilerin düzeltilmesi veya silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işleme faaliyetine itiraz etme hakkının varlığı;
(f) bir denetim makamına şikâyette bulunma hakkı;
(g) kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler;
(h) profil çıkarma da dahil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar vermenin varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları.
2. Kişisel verilerin üçüncü bir ülke ya da uluslararası bir kuruluşa aktarılması durumunda, veri sahibinin aktarımla ilgili olarak 46. madde uyarınca uygun güvenceler hususunda bilgilendirilme hakkı bulunur.
3. Kontrolör işleme faaliyetinden geçen kişisel verilerin bir nüshasını sağlar. Veri sahibi tarafından talep edilen diğer nüshalar açısında, kontrolör idari masraflara dayalı olarak makul bir ücret talep edebilir. Veri sahibinin talebi elektronik yollarla yapması halinde ve veri sahibi tarafından aksi talep edilmedikçe, bilgiler yaygın kullanılan bir elektronik yolla sağlanır.
4. 3. paragrafta atıfta bulunulan bir nüsha elde etme hakkı başkalarının hakları ve özgürlüklerini olumsuz yönde etkilemez.

Madde 16 Düzeltme hakkı: Veri sahibinin kendileri ile ilgili doğru olmayan kişisel verilerin gereksiz gecikmeye mahal verilmeksizin düzeltilmesini kontrolörden talep etme hakkı bulunur. İşleme amaçları dikkate alınarak, veri sahibinin, bir ek beyan yoluyla da dâhil olmak üzere, eksik kişisel verileri tamamlatma hakkı bulunur."

[262] Silme(unutulma) hakkı hükmü GDPR m. 17'de düzenlenmektedir:
"1. Veri sahibinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini kontrolörden talep etme hakkı bulunur ve aşağıdaki hallerden birinin geçerli olması durumunda, kontrolörün kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü bulunur:
(a) kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması;
(b) veri sahibinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendine göre işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması;
(c) veri sahibinin 21(1) maddesi uyarınca işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması ya da veri sahibinin 21(2) maddesi uyarınca işleme faaliyetine itirazda bulunması;
(d) kişisel verilerin yasa dışı biçimde işlenmiş olması;
(e) kontrolörün tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması;
(f) kişisel verilerin 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması.
2. Kontrolörün kişisel verileri kamuya açıklamış olduğu ve 1. paragraf uyarınca kişisel verileri silmek zorunda olduğu hallerde, kontrolör, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri sahibinin talep etmiş olduğu kişisel verileri işleyen kontrolörleri söz konusu kişisel verilere yönelik her türlü bağlantı veya bu verilerin her türlü nüshası ya da çoğaltmasının söz konusu kontrolörlerce silinmesi hususunda bilgilendirmek üzere teknik tedbirler de dâhil olmak üzere makul adımları atar.
3. 1 ve 2. paragraflar işleme faaliyeti aşağıdaki amaçlar doğrultusunda gerekli olduğu ölçüde uygulanmaz:
(a) ifade ve bilgi edinme hakkının kullanılması;

KVK Kanunu m. 12'de veri güvenliğine ilişkin yükümlülükler başlığı altında veri sorumlusuna, verilerin güvenliğini sağlamaya yönelik bazı yükümlülükler getirmektedir. Bu yükümlülüklerin veri sahibi tarafından talep edilebileceği için bunlara veri sahibinin hakları başlığı altında burada yer vermenin uygun olacağını düşünmekteyiz.

Bu yükümlülükleri yukarıda da belirttiğimiz üzere soruşturma evresinde delil işleme kararını veren makamın yükümlülükleri olarak görebilmek bizce mümkündür. Örneğin bu doğrultuda, m. 12(3)'te ifade edilen, veri sorumlusunun kendi kurum veya kuruluşunda bu kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda oluşunu, savcının kendisi emir ve talimatı doğrultusunda hareket eden kolluk üzerindeki yükümlülükleri olarak anlamak mümkündür.

Ayrıca, veri sorumluları ile veri işleyen kişilerin, öğrendikleri kişisel verileri KVK Kanunu hükümlerine aykırı olarak başkasına açıklayamayacakları ve işleme amacı dışında kullanamayacakları yükümlülüğünün görevden ayrılmalarından sonra da devam edeceği düzenlenmektedir. Fakat uygulamada bunun aksine sıklıkla rastlanmakta olduğundan özellikle basına karşı bu bilgilerin açıklanmamasına dikkat edilmesi gerekmektedir.

Önemle belirtmek gerekir ki kişisel verilerin soruşturma evresinde tam bir bütünlük içerisinde korunabilmesi için burada sayılan hakların, ceza muhakemesine ilişkin düzenlemeler ayrı bir maddede düzenlenmelidir. Yukarıda zikredilen hakların bu doğrultuda, CMK içerisinde "Soruşturma Evresinde Kişisel Verisi İşlenen Mağdur, Şüpheli Veya İlgilisinin Hakları" başlığı altında bir maddede düzenlenmesi, kişisel verilerin soruşturma evresinde korunmasına yönelik güvence sağlayacaktır.

7. Kişisel Verilerin Korunması Kanunu'nda Düzenlenen İstisnalar

---

(b) kontrolörün tabi olduğu Birlik veya üye devlet hukuku çerçevesinde işleme faaliyeti gerektiren bir yasal yükümlülüğe uygunluk açısından veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması açısından;
(c) 9(2) maddesinin (h) ve (i) bentlerinin yanı sıra 9(3) maddesi uyarınca halk sağlığı alanındaki kamu yararı sebeplerinden dolayı;
(d) 1. paragrafta atıfta bulunulan hakkın ilgili işleme hedeflerinin yakalanmasını imkânsız hale getirmesi veya yakalanmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde, 89(1) maddesi uyarınca kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veya
(e) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından."

a) Genel olarak

Tezimizin konusu bağlamında esas problemin yaşanmakta olduğu madde, KVK Kanunu'nun 7. bölümünde yer alan m. 28'dir. Bu maddede kanun koyucu tarafından KVK Kanunu'nun uygulama kapsamı dışında tutulmuş istisna haller *numerus clausus* olarak sayılmaktadır[263].

Belirtmek gerekir ki esasen istisna hallerinin varlığında soruşturma evresinde işlenmekte olan veriler de kişisel veridir. Fakat kanun koyucu buradaki hükümlerin varlığında söz konusu kişisel verileri diğer kişisel veriler gibi koruma kapsamına almamaktadır.

Dolayısıyla buradaki hükümler kapsamında veri sahibinin açık ya da zımni rızasının varlığına bakılmadan işleme faaliyeti gerçekleştirilmektedir. Böyle bir durumun insan onurunun korunmasını azaltacağı, idarenin gereğinden fazla güçlenmesine yol açacağı ve kişisel verilerin suiistimal edileceği hususlarında endişelere yol açmaktadır[264]. Kanun yapım sürecinde istisnalarla ilgili yapılan eleştiriler üzerine Adalet Komisyon Raporu'nda, tüm iç hukuk ve uluslararası hukuk verileri göz önünde bulundurulduğunda yapılan eleştirilerin aksine korunması gereken hak ile diğer kamusal ve kişisel menfaatler arasında denge ve ölçülülük temelinde bir düzenleme öngörüldüğü belirtilmiştir[265].

Avrupa Birliği Komisyon 2016[266] ve 2018[267] yılı raporlarında, istisna hükümlerinin çok geniş düzenlenerek soruşturma evresinin KVK Kanunu kapsamı dışında bırakılmasının

---

[263] İstisnalar hükmü KVK Kanunu m. 28'de düzenlenmektedir:
"(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:
a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere 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."
[264] Bennett, Colin J.: Regulating Privacy: Data Protection and Public Policy in Europe and the United States, New York 1992, s. 44.
[265] 6698 sayılı Kanun Gerekçesi, s. 67.
[266] Avrupa Birliği Komisyonu, 2016. *2016 Türkiye Raporu SWD(2016) 366 nihai*. Erişim Tarihi: 31 Ocak 2019 https://www.ab.gov.tr/files/pub/2016_ilerleme_raporu_tr.pdf, s. 5, 10, 16, 71.
[267] Avrupa Birliği Komisyonu, 2018. s. 5, 41, 42, 44.

AB standartlarıyla uyumlu olmadığı ve düzenlemenin bu haliyle kişisel verilerin korunmasını sağlamamakta olduğu ifade edilmektedir. Dolayısıyla Avrupa açısından bakıldığında Türkiye, veri koruması sağlaması açısından uzun zamandır güvensiz ülke olarak nitelendirilmektedir[268]. Doktrinde de istisna hükümlerinin 95/46/EC sayılı Direktif'e göre oldukça geniş düzenlenmesi, kişisel veriler üzerinde yeterli korunma sağlanmasını engelleyeceği sebebiyle eleştirilmektedir[269].

Soruşturma, kovuşturma ile yargılama ve infaz işlemleri istisna kapsamında yer almaktadırlar. Bu konuya ilişkin hiçbir mevzuatın bulunmadığı önceki durumla kıyaslandığında bu kanun, bir ilerleme olduğuna işaret etmektedir. Ancak, özellikle kişisel verilerin kullanılmasını denetlemekten sorumlu makamın oluşumu ve işleyişine ilişkin hükümlerin bu kurumun tamamen bağımsız hareket etmesine yönelik güvenceler sağlamaması ve infaz mercileri ile yargı makamlarının faaliyetlerinin, KVK Kanunu kapsamına dâhil edilmemesi kişisel verilerin korunması kurallarına riayet edilmesi yükümlülüğü çerçevesinde KVK Kanunu'nun yetersizliği göstermektedir.

Bu konuda kanunun genel gerekçesinde polis kayıtları hususunda ilerleyen zamanlarda yeni düzenlemeler yapılabileceği ifade edilmesine rağmen günümüze kadar bu konuda yapılmış bir düzenleme bulunmamaktadır.

b) Kişisel verilerin soruşturma işlemlerine ilişkin olarak işlenmesi

Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi, KVK Kanunu m. 28(1)(d) bendinde KVK Kanunu'na istisna tutulmuştur. Bunun anlamı, söz konusu işlemlerde yapılacak işleme faaliyeti hukuka uygun olacak ve işleme yapan veri sorumlularının ne cezai ne de hukuki müeyyideye tabi tutulması gündeme gelebilecektir. Başka bir yönetmelikle de bu konuların düzenlenmemiş olması AB düzenlemeleri ve AİHM içtihatlarına karşısında devletin düzenlemesi gereken alanı ihmal ettiği göstermektedir. Bu durum hiç şüphesiz devletin pozitif yükümlülüğüne aykırı davrandığını göstermektedir.

[268] Henkoğlu, s. 104.
[269] Köse Aysun, s. 81.

Bunun dışında söz konusu işlemlerin sadece yargı makamları ve infaz mercilerince yapılması istisna tutulduğundan kolluğun bunların dışında kendisine tanınan görev ve yetkileri çerçevesinde özellikle soruşturma sürecinde resen yapacağı işlemler "d" bendi açısından bu istisnaya tabi değildir. Çünkü özgürlük kural sınırlama istisnadır. Sınırlamanın olmadığı yerde kurallar özgürlük lehine yorumlanır. Bu çerçevede getirilecek hükümlerin başta 2016/680/EU sayılı Direktif olmak üzere, AB ve AİHM içtihatları doğrultusunda olması olumlu bir adım olacaktır.

Öte yandan, "d" bendinin sağladığı istisna hükümleri nedeniyle verilerin korunmasına yönelik ilkelerin ihlal edilmesi halinde ne olacağı belirsizdir. Hangi kanun olursa olsun yaratılan belirsizlikten dolayı, gizliliğin korunmasında disiplin ya da ceza hukuku normlarının uygulanmasının tatbik edilemiyor olması getirilen düzenlemeyi sorgulanabilir kılmaktadır[270].

Bizim görüşümüze göre, eğer kişisel verilerin gizliliği hakkının tesisi amaç ise ve veriler bu alanlarda hiç korunmayacaksa, verilerin korunması alanına özgü düzenlemeler sadece göstermelik düzenlemelerden ibarettir. Bu yüzden kişisel verilerin işlenmesine uygulanacak genel ilkeler, kişisel verilerin korunması hakkının asgari güvencesi olarak düzenlendiğinden, bu ilkelerin soruşturma evresindeki yöntemler üzerinde de tatbik edilmesi gerekir. Aksi halde anayasal bir hakkın soruşturma evresinde hiç tatbik edilemeyeceği sonucu çıkmaktadır. Müdahalede orantılılıktan uzak olacak bu tavır, Anayasaya aykırı olup hakkın özüne dokunacaktır.

c) Kişisel verilerin soruşturma evresinde işlenirken veri sorumlusu yükümlülükleri ve ilgili kişinin haklarının sınırlanması

Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması halinde, kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla bazı hükümlerin uygulanmayacağı KVK Kanunu m. 28(2)'de belirtilmektedir. Buna göre, veri sorumlusu açısından aydınlatma yükümlülüğü ve veri sorumluları siciline kayıt yükümlülüğü, ilgili kişi açısından ise zararın giderilmesini talep etme hakkı hariç diğer haklarının uygulama alanı bulamayacaktır. Düzenlemeyi benimseyen bir görüşe göre, bu hükümlerin kamu otoritelerince çok geniş yorumlanamayacağını ileri sürmek,

[270] Pollack, Michael C.: "Taking Data", The University of Chicago Law Review, 86, Şikago 2019, s. 89.

mahkemeler ve veri koruma yetkilileri için çok önemli fakat uygulamada zor bir meseledir[271].

Bizim görüşümüze göre zikredilen yükümlülük ve hakların tamamıyla istisna kapsamına kamu görevlilerine geniş takdir alanı bırakacaktır. Kişileri güvencesiz bırakan bu uygulama kişisel verilerin korunması hakkına orantısız bir müdahale etmektedir. Şöyle ki veri sorumlusunun aydınlatma yükümlülüğünün istisna kapsamına alınması, kişisel verisi işlenen bireylere yönelik işleme kararını veren ve uygulayan kişilerin haber vermemesini ifade etmektedir. Soruşturmanın gizliliği ilkesi çerçevesinde bir anlığına tutarlı gözükse bile, süreç içerisinde kişisel verileri işlenen kişilerin bunlardan hiç haberdar olmayacağı göz önünde bulundurulmalıdır. Kaldı ki her soruşturma süreci kovuşturma evresine geçememektedir. Üstelik elde edilen verilerin imhasına yönelik hali hazırdaki düzenlemeler zaten verilerin korumaktan uzaktır. Ayrıca 2016/680/EU sayılı Direktif m. 12'de veri sahibinin haber alma hakkının açıkça soruşturma evresinde uygulanacağı güvence altına alınmaktadır. Dolayısıyla, soruşturma faaliyeti sonrasında işleme faaliyeti ile ilgili müdahalenin amacı ve kişilerin haklarıyla dengeli olacak şekilde veri sahiplerine yönelik bilgi verilmesini sağlayacak düzenlemelerin varlığı gerekmektedir.

Ayrıca ilgili kişinin tazminat hakkı hariç diğer haklarının kapsam dışında bırakılması ve aksinin uygulamada zorluklara yol açabileceği düşüncesi tutarsızdır. 2016/680/EU sayılı Direktif'te soruşturma evresinde veri sahibinin haklarının, kişisel veri içeren mahkeme kararları, kayıt ve dosyaları üzerinde tatbik edilebileceğinin esas olduğu belirtilmektedir[272]. Dolayısıyla, kişisel verilerin korunması anayasal bir haksa, veri sahibinin sahip olduğu hakların da soruşturma evresinin gizliliğine halel getirmeyecek ölçüde, soruşturma sırasında ve sonrasında uygulama alanı bulmasının şart olduğunu düşünmekteyiz.

d) Kişisel verilerin soruşturma evresinde sınırlamaya tabi olmaksızın işlenmesinin hukuka aykırılığı

Konunun önemine binaen geniş çerçevede ortaya koyabilmek için, soruşturma evresi ile ilgili yargı barındıran KVK Kanunu m. 28(1)(ç), (d) ve 28(2) hükümleri açısından ortak

[271] Brouwer, Evelien Renate: The Other Side of Moon: The Schengen Information System and Human Rights : a Task for National Courts, Brüksel 2008, s. 4.
[272] 2016/680/EU sayılı Direktif, m. 17 ve 18.

bir yorum yapmak gerekir. Çünkü söz konusu maddelerde soruşturma evresinde delil elde etme amacıyla kişisel verilerin korunması hakkına getirilen sınırlamalar ciddi sorunlar barındırmaktadır. Burada tartışmaya yol açan problemin üç sacayağı bulunmaktadır.

Birincisi, kişisel verilerin soruşturma evresinde tamamen KVK Kanunu kapsamı dışında bırakılmasının, anayasal bir hak olan kişisel verilerin korunması hakkının soruşturma evresinde hiç kullanılamamasına yol açmakta olmasıdır. Temel hak ve özgürlüklerin sınırlanmasına yönelik bir müdahalenin Anayasa m. 13'te zikredilen şartlara bağlı olarak yapılması gerekmektedir. Bu doğrultuda, sınırlamanın hakkın özüne dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve kanunla yapılabilir. Bu sınırlamalar, Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olmaması gerekmektedir. Anayasa m. 20(3)'te kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme bir hak olarak tanımlanmıştır. Fakat KVK m. 28 hükümlerinden çıkan anlama göre, soruşturma evresinde kişisel verilerin işlenmesine yönelik herhangi bir işlem koruma kapsamında bulunmamaktadır.

Bizim görüşümüze göre bu maddenin oluşturduğu durum Anayasal bir hakkın özüne dokunup hiç kullanılmamasına yol açtığı için bu madde Anayasaya aykırıdır. Keza soruşturma işlemlerinin doğasından kaynaklanan düzeyde kişisel verilerin korunması ile arasında belli bir denge kurulması hali savunulabilir olsa da var olan düzenleme buna da imkân vermemektedir. Doktrinde de özellikle ç bendindeki istisna hükmünün uygulamada birçok insan haklarına aykırılık doğuracak bir düzenleme olduğu belirtilmektedir[273]. Hülasa, var olan düzenleme kişisel verilerin korunması hakkının, kanun hükmünün yorumu sebebiyle hiç kullanılamaz hale gelmesi sebebiyet vermekte bu yüzden de hakkın özüne apaçık müdahale teşkil etmektedir.

Öte yandan, KVK Kanunu'nun diğer maddelerinin yanı sıra ç bendinin de iptali için 2016 yılında dava açılmıştır. 2017 yılında verilen kararda Anayasa Mahkemesi, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceğini belirtmekte,

[273] Ayözger Öngün, s. 34.

buna gerekçe olarak kendi vermiş olduğu başka kararları kaynak göstermektedir[274]. Kanaatimizce AYM'nin bu kararı yerinde değildir çünkü Anayasa m. 13'te temel hak ve hürriyetlere ilişkin yapılacak sınırlamaların yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak yapılacağı düzenlenmektedir.

Ayrıca AYM, söz konusu sınırlama hükmünün, Anayasa'da devlete verilen görevlerin gereği olarak millî güvenliğin, kamu düzeninin ve suç işlenmesinin önlenmesini sağlamak amacıyla yapıldığından demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmakta olduğu belirtmektedir[275]. Kanaatimizce AYM'nin bu tespiti de hatalıdır. Çünkü AYM bu kararında hem eski tarihli bir AİHM kararının dayanak göstermekte hem de AİHM'in bu konuda demokratik bir toplumdaki kanuni güvencelerin taşıması gereken özelliklerine ilişkin yorumlarına hiç girmemektedir. Oysa AİHM kararlarında bu konu kestirilip bir kenara konulmamakta hakkın özüne müdahale etme tehlikesini bertaraf edici düzenlemelerin yer alması gerektiği belirtilmektedir[276].

Devamında AYM, TCK m. 136 hükmünün varlığı sebebiyle elde edilecek bilgilerin amacı dışında kullanılmasını önleyecek ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencenin sağlandığı belirtmektedir[277]. Kanaatimizce Mahkeme'nin bu görüşü de hatalıdır. Çünkü, kişisel verilerin korunmasına ilişkin olarak soruşturma evresinde hâkim olan ilkelere ve ilgili kişinin haklarına ilişkin özel hükümler sadece TCK m. 136'nın varlığı ile sağlanamayacağı aşikardır[278].

Anayasa Mahkemesi açılan bu iptal davasını tamamıyla reddetmiş ve meri KVK Kanunu'nun hukuka uygun bir düzenleme olduğunu belirtmiştir. Tezimizin ilerleyen kısımlarında daha detaylı gerekçelendireceğimiz üzere, yukarıdaki gerekçeler çerçevesinde, AYM'nin görüşünün hatalı, KVK Kanunu'nun da bu açıdan hukuka ve uluslararası normlara aykırı olduğunu düşünmekteyiz.

[274] E. 2016/125, K. 2017/143, KT: 28.09.2017, RG. 30310, 23.01.2018, par. 153, Erişim Tarihi: 19 Mart 2019.
[275] E. 2016/125, K. 2017/143, KT: 28.09.2017, RG. 30310, 23.01.2018, par. 157, Erişim Tarihi: 13 Şubat 2019.
[276] Daha fazla açıklama için tezin üçüncü bölümünün (II)(C)(3)(d) kısmına bakınız.
[277] E. 2016/125, K. 2017/143, KT: 28.09.2017, RG. 30310, 23.01.2018, par. 160, Erişim Tarihi: 7 Şubat 2019.
[278] Daha fazla açıklama için tezin üçüncü bölümünün (II)(D) kısmına bakınız.

İkincisi, zikredilen istisna düzenlemeleri sebebiyle kişisel verilerin anayasası olarak düşünülebilecek olan verilerin korunmasındaki genel ilkelerin bile soruşturma evresinde uygulama alanı bulamayacak olmasıdır. Belirtmek gerekir ki, bu düzenlemelerin verilerin işlenmesi hususundaki genel ilkelere uygun olması temel bir gerekliliktir. Bu gereklilik kanuni düzenlemede bu hususun eksik bırakılması ile ilgilidir. Bu sebeple kanuni düzenleme nihayete erecek düzeyde kesinliğe kavuşmamış olduğu ifade edilebilir.

Doktrinde de belirtildiği üzere, hukuka ve dürüstlük kurallarına uygun bir işlemenin söz konusu olması için yalnızca işleme faaliyetlerinin yasal sınırlarının belirlenmesi yetmemekte, aynı zamanda bu işlemenin hukukun genel ilkeleri ve evrensel hukuk prensiplerine de uygun olması gerekmektedir[279].

Bu doğrultuda, uygulamada her nasılsa istisna kapsamında diye değerlendirilmeyen genel ilkelerin, yapılan her işleme faaliyeti açısından ayrı ayrı değerlendirilmesi gerekmektedir. Üstelik GDPR m. 5'te sayılan kişisel verilerin işlenmesine ilişkin ilkeler veri sahibinin hakları ile bağlantılı olması halinde sınırlanabileceğini belirtilmektedir. Bunun anlamı, kişisel verilerin işlenmesine ilişkin ilkelerin soruşturma evresinde kural olarak uygulama alanı bulacağı ve bu ilkelerin sadece veri sahibinin haklarına temas ettiği noktada sınırlanabileceğidir. Ayrıca 2016/680/EU sayılı Direktif m. 4'te GDPR hükmünde soruşturma evresinde doğrudan uygulanması amacıyla aynı ilkeler birebir sayılmaktadır.

O halde veri sahibinin hakları ile ilişkili olmayan ve fakat soruşturma evresinde kişisel verilerin işlenmesine hâkim olan ilkelerin uygulanabileceği hususunda bir tereddüt olmaması gerekir. Çünkü verilerin işlenmesinde hukuka uygunluk, adalet, şeffaflık, doğruluk ve amacın sınırlandırılması gibi ilkeler soruşturmaya zarar vermesi bir yana zaten soruşturma süreci için gerekli olan ilkelerdir.

Üçüncüsü, soruşturma evresinin kapsam dışı bırakılması fikrinin kişisel verilerin korunması fikriyle çatışacak olmasıdır. Yani zikredilen istisna hükümlerinin, KVK Kanunu'nun amacına, ruhuna ve temel ilkelerinde belirtilen hususlara uygun ve orantılı olarak düzenlenmiş olduğunu iddia etmek güçtür. GDPR düzenlemesi m. 23'te getirdiği benzer istisna hükümlerinde, veri sahibinin haklarının sınırlanabileceği belirtmekte fakat külliyen kapsam dışı bırakılamayacağını belirtmektedir. Üstelik tezimizin önceki

[279] Dülger, 2019, s. 330.

bölümlerinde yer verdiğimiz GDPR ile aynı tarihte 2016/680/EU sayılı Direktif kişisel verilerin korunmasına ilişkin hemen hemen aynı hükümlerin soruşturma evresinde de uygulanması amacıyla çıkarılmıştır. Fakat Türk hukukundaki bu istisna hükümlerinin bir sonucu olarak işlemelerin yargı denetimine de tabi olmaması sebebiyle yasanın getirdiği güvenceler soruşturma evresinde tamamıyla ortadan kaldırılarak suiistimale ve fişlemeye yol açan bir hale getirilmektedir[280].

Soruşturma kurumlarının yetki ve nitelikleri dikkate alınarak kişisel verilerin işlenmesi açısından istisna kapsamında olması bir yana bunun hukuki güvenceye kavuşturulmamış olması önemli hak ihlallerini ortaya çıkararak hukuk güvenliğini tehlikeye atmaktadır[281]. Bu doğrultuda belirtmek gerekir ki, özellikle hassas nitelikli kişisel veriler hakkında olmak üzere çeşitli kanunlarda daha fazla koruyucu önlemler alan kanun koyucu[282], soruşturma evresine gelindiğinde hassas verilerin bile korunmaya değer olamayacağını benimsediği düşüncesi ortaya çıkmaktadır ki bu, hukuk metodolojisi ve mantığına aykırılık teşkil eder.

Farklı bir açıdan ortaya çıkan başka bir problem, zikredilen bu istisna hükümleri çerçevesinde elde edilen delillerin hiçbir kurala bağlı olmaksızın elde ediliyor olması sebebiyle hukuka aykırı delil olabileceğidir. Verilerin işlenmesi teriminin kapsamı düşünüldüğünde verilerin paylaşılması başta olmak yapılacak her türlü işlem esasen hukuki açıdan olması gereken seviyede bir yasal dayanaktan bağımsız olarak gerçekleştirilmiş olmaktadır. Bu doğrultuda, kişisel veri içeren kayıtlar uygulamada itiraz gelebileceği sebebiyle yok edilmemekte, kişisel verilerin korunmasını ihlal edebilecek bilgilerin, adli soruşturma ve kovuşturma dosyalarında almasının kısıtlanması ilgili idari ve yasal tedbirlerin alınması gerekmektedir[283].

Var olan ihtiyaca binaen, soruşturma organlarının elde edilen kişisel veri içeren delillerin diğer organlarla paylaşmasına ilişkin esas ve usullere ilişkin yasal düzenleme yapılması önem arz etmektedir[284]. Aksi halde, hukuka uygun olmayan, adil olmayan, şeffaf

[280] Bük, s. 91.
[281] Küzeci, s. 333.
[282] Örneğin, meslek ve sürekli uğraşıları sebebiyle hassas verilere erişebilen CMK m. 46'da düzenlenen tanıklıktan çekinebilecek olanlar.
[283] Gül, İbrahim/Alagöz İsmail: Kişisel Verilerin Korunmasına Yönelik İhlaller(Dinlemeler) ve Uluslararası Düzenlemeler, Ankara 2016, s. 164.
[284] Gül/Alagöz, s. 164.

olmayan, doğru olmayan ve amacı sınırlandırılmamış olarak verilerin korunması ilkeleri süzgecinde toplanmamış delillerin somut gerçekliğe ulaştırması elbette beklenemez. Böyle bir durumda delillerin hukuka aykırı delil sınıfında yer alacağı ortadadır.

Sonuç olarak, KVK Kanunu m. 28(ç), (d) ve 28(2)'de yer alan hükümlerin tasarıdaki haline göre daha kısıtlayıcı şekilde düzenlenmiş olması[285], Anayasa ile düzenlenerek açıkça verilen bir hakkın kanunla geri alınışı gibi bir duruma yol açmaktadır. Sonuçta nasıl bireyin kişisel verilerinin korunması mutlak değilse idarenin kişisel verileri toplama ve işleme yetkisi de sınırsız olmamalıdır[286]. Eğer kişinin kişisel verilerinin korunması hakkı ile devletin güvenlik sağlama görevi arasında çatışmada güvenlik her zaman ağır basacaksa kişisel verilerin korunması hakkında söz etmenin çok fazla bir anlamı kalmamaktadır[287]. Dolayısıyla, bu hükümlerin hiç bir detaya inmeden doğrudan soruşturma evresini kapsam dışı bırakması kişisel verilerin korunması hakkına yönelik orantısız bir müdahale teşkil etmektedir. Madde hükmünün bu orantısız müdahalesi, özetle Anayasa m. 2, 13, 20 ve 90'a aykırıdır. Özgürlüğün esas sınırlamanın istisna olduğu seküler ve liberal insan hakları kuramı açısından demokratik toplum gereklilikleri ile bağdaşmamakta olduğundan bu istisna hükümlerinin hukuki gerekçeye sahip olduğu iddia etmek de pek mümkün değildir.

[285] Küzeci, s. 326.
[286] Şimşek, s. 125.
[287] E. 2010/40, K. 2012/8, KT: 19.01.2012, RG. 28579, 06.03.2013, Erişim Tarihi: 6 Şubat 2019.

ÜÇÜNCÜ BÖLÜM:

SORUŞTURMA SÜRECİNDE KİŞİSEL VERİLERİN İŞLENME İLKELERİ VE ULUSLARARASI STANDARTLAR

I. SORUŞTURMA SÜRECİNDE KİŞİSEL VERİLERİN İŞLENMESİNE ÖN BAKIŞ

A. Soruşturma Sürecinde Alınan Adli Tedbirlerin Kapsamı Ve Amacı İtibariyle Önleyici Tedbirlerden Farkları

Soruşturma sürecinde alınan adli tedbir, bir suç şüphesinin varlığı sebebiyle başlayan soruşturma sürecinden itibaren kovuşturma aşamasının başlamasına kadar suç şüphesi altında bulunan şüpheli, mağdur veya diğer kişilere yönelik getirilen ve CMK'da düzenlenmiş olan tedbirlerdir. Bunlardan en çok öne çıkanları hiç şüphesiz şüphelinin tutuklanması, yakalanması ve gözaltına alınması ve şüphelinin vücudu üzerinde onun kişisel verilerini elde etmeye yönelik olabilecek tedbirlerdir.

Önleyici amaçlı alınan tedbirler ile adli tedbirler arasındaki temel fark, önleyici tedbirlerin suç öncesinde önleyici amaçla, adli tedbirlerin ise suç şüphesinin ortaya çıkmasından sonra cezalandırma amacı gütmeyen bastırıcı amaçla ve delillerin korunması amacıyla alınmakta olmasıdır. Önleyici tedbirlerin kaynağı, yetkisi kanuna dayanan idari iş niteliğindeki emir ve talimatlardır. Daha çok genel ve yaygın bir etkiye sahip olacak bir suç işleneceği ihbarı üzerine alınan önleyici tedbirin amacı, suçun işlenmesi üzerine ortaya çıkacak yıkım ve tahribatın suç işlenmeden önce önlenmek istenmesidir.

Suç işlenmesini önlemek amacıyla, idari kolluk olarak polis ve jandarma; siyasi kolluk olarak ise istihbarat teşkilatı faaliyet göstermektedir. PVSK başta olmak üzere, suçun işlenmesini önlemeye yönelik bu önleyici tedbirlere kaynaklık değişik düzenlemeler yer almaktadır.

Belirtmek gerekir ki kolluğa ilişkin idari-adli ayrımının polis teşkilatında yer alan görevliler açısından organik bir ayrım bulunmamaktadır. Yani PVSK m. 2'de belirtildiği üzere, polisin genel emniyetle ilgili görevleri iki kısımdan oluşmaktadır. Birincisi, idari kolluğun gerçekleştirdiği, kanunlara, Cumhurbaşkanlığı kararnamelerine,

yönetmeliklere, hükümet emirlerine ve kamu düzenine uygun olmayan hareketlerin işlenmesinden önce PVSK hükümleri dairesinde önünü almaktır.

İkincisi ise, adli kolluğun gerçekleştirmiş olduğu, işlenmiş olan bir suç hakkında CMK ile diğer kanunlarda yazılı görevleri yapmaktan ibarettir. Dolayısıyla, PVSK'da yetki ve görevleri açısından kolluk idari ve adli olarak ayrılmamış ve hem önleyici hem de adli işlerle aynı anda görevlendirilmiştir.

Buna göre, bastırıcı kolluk görevini yapan bir polis şartlar oluştuğunda aynı olay içerisinde önleyici kolluk olarak da davranma görev ve zorunluluğu altındadır. Örneğin, PVSK m. 20'ye göre, zabıta, imdat istenmesi veya yangın, su baskını ve boğulma gibi büyük tehlikelerin haber verilmesi veya görülmesi halleri ile ağır cezalı bir suçun işlenmesine veya yapılmakta devam olunmasına mani olmak için konutlara, iş yerlerine ve eklentilerine girebilmektedir. Buna göre, suçun önlenmesi safhasında yer alması gereken bir kolluk görevlisi aynı anda işlenmekte olan bir suçu bastırarak engel olmak için devreye girmesi gerekmektedir.

Öte yandan konumuz bağlamında yalnızca soruşturma evresindeki adli tedbirlerin ilgili olduğunu belirtmek gerekir. Suçun işlendiği veya işlenmekte olduğu şüphesi üzerine başlatılan adli tedbirlerin hepsi ceza muhakemesi açısından kural olarak CMK'da düzenlenmektedir. Ayrıca diğer kanunlarda yer alan ya da atıfta bulunulan bastırıcı amaçlı adli tedbir hükümleri de bulunmaktadır. Fakat bu durum, idari-adli tedbir farkını ortaya koymada karışıklıklara yol açabilmektedir.

Adli tedbirlerle ilgili son olarak belirtmek gerekir ki bu tedbirler önleyici olmadıkları gibi kişiyi cezalandırma maksadı güden infaz tedbirleri gibi cezalandırıcı tedbirlerden de beridirler. Ayrıca, kolluğa ilişkin görevlerinde üstlerinin emrinde olan adlî kolluk personelleri, Cumhuriyet savcısının adlî görevlere ilişkin emirlerini de yerine getirmektedirler. Bu yüzden, Cumhuriyet savcısının emir ve talimatları doğrultusundaki soruşturma işlemleri öncelikle adlî kolluğa yaptırılmaktadır[288].

İfade etmek gerekir ki, her iki tedbirin de muhtelif kişi hak ve hürriyetlerine yönelik olarak müdahale ettiği ölçüde kanuni dayanağa sahip olması şarttır. Bu konuda

[288] Adli kolluk, CMK m. 164'te açıklanmaktadır. Buna göre, adlî kolluk, Emniyet Teşkilatı'nın, Jandarma Teşkilatı'nın, Gümrük Müsteşarlığının Teşkilatı'nın ve Sahil Güvenlik Komutanlığı'nın ilgili özel kanunlarında belirtilen soruşturma işlemlerini yapan güvenlik görevlilerini ifade etmektedir.

düzenlenecek kanunun Anayasa m. 13 uyarınca şekli ve AİHM içtihatları uyarınca da maddi kanun özelliklerine sahip olması gerekmektedir. Ayrıca, idare içerisindeki kolluk makamlarından sadır olan emirlerin de kanunda belirtilen yetki sınırları içerisinde kalması gerekir ki aksi halde hukuka aykırı emirin varlığından bahsedilebilir. Üstelik yetkisini aşan bu emirin soruşturma evresinde yer alması halinde toplanan deliller hukuka aykırı delil olacaktır. Durum bu haliyle delil elde etme ve delil değerlendirme yasağı olarak iki gruba ayrılan delil yasakları kurumunun delil elde edilmesi sınıfına girecektir[289].

B. Önleyici Amaçlarla Elde Edilen Kişisel Verilerin Adli Amaçlarla Soruşturma Evresinde Kullanılması

1. Genel olarak

Polis, PVSK m. 2, Ek m. 4 ve 5'ten anlaşıldığı üzere hem önleyici hem de adli faaliyetlerde görevlendirilmekte ve kolluk görevlileri üzerinde bunun ayrımı yapılmamaktadır[290].

---

[289] Y. CGK, E. 2013/10-468 K. 2014/268 T. 20.5.2014, Kazancı İçtihat Bilgi Bankası.

[290] Polisin genel emniyetle ilgili görevleri PVSK m. 2'de düzenlenmektedir:
"... I – Can, ırz veya mal emniyetini korumak için,
II – Devletin şahsiyetine karşı işlenen cürümlerin faillerini yakalamak veya delillerini tesbit etmek için,
III – Devlet kuvvetleri aleyhine, yalnız veya toplu olarak taarruz veya mukavemette bulunanları yakalamak veya bunların taarruz veya mukavemetlerini def etmek için,
IV – Hükümete karşı, şiddet kullanan veya gösteren veya mukavemet edenlerin yakalanması, taarruz veya mukavemet edenlerin def edilmesi için,
V – Zabıtaca muhafaza altına alınan şahıslara, bina veya tesislere, meskün veya gayrimeskûn yerlere vaki olacak münferit veya toplu tecavüzleri def etmek için,
VI – Ağır cezalı bir suçun sanığı olarak yakalandıktan sonra zabıta kuvvetlerinin elinden kaçmakta olan şahısların yakalanması için,
VII – İşlenmekte olan bir suçun işlenmesine veya devamına mani olmak için,
VIII – Ceza Muhakemeleri Usulü Kanunu ile diğer kanunlarda, zabıta tarafından suç delillerinin tesbiti veya suç faillerinin yakalanması maksadiyle yapılacak aramalar için,
IX – Kanunsuz toplantı veya kanunsuz yürüyüşleri dağıtmak veya suçlularını yakalamak için,
X – Yangın, su baskını, yer sarsıntısı gibi afetlerde olay yerinde görevlilerce alınması gereken tedbirler için,
XI – Umuma açık yerlerde yapılan her türlü toplantı veya yürüyüşlerde veya törenlerde bozulan düzeni sağlamak için,
XII – Herhangi bir sebeple tıkanmış olan yolların trafiğe açılması için,
XIII – Yukardaki maddeler dışında diğer kanunlarda istisnai olarak zabıtanın sözlü emirle yapmaya mecbur tutulduğu haller için,
Yetkili amir tarafından verilecek sözlü emirler derhâl yerine getirilir. Bu emirlerin yazılı olarak verilmesi istenilemez. Bu hallerde emrin yerine getirilmesinden doğabilecek sorumluluk emri verene aittir."

PVSK Ek Madde 4 hükmüne göre: *"Polis, görevli bulunduğu mülki sınırlar içinde, hizmet branşı, yeri ve zamanına bakılmaksızın, bir suçla karşılaştığında suça el koymak, önlemek, sanık ve suç delillerini tesbit, muhafaza ve yetkili zabıtaya teslim etmekle görevli ve yetkilidir.*

PVSK Ek m. 6'da da polisin adli görev ve yetkileri düzenlenmekte, CMK'daki koruma tedbirlerine benzer tedbir hükümleri yer almakta ve bu doğrultuda kişisel verilerin işlenebileceği düzenlenmektedir[291]. Ayrıca bir adli tedbir olan ve CMK'da düzenlenen durdurma ve kimlik sorma, PVSK m. 4/A'da hem önleyici hem de adli amaçlı bir tedbir olarak düzenlenmiştir.

Yine bir başka adli tedbir olan CMK'da düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi ve teknik araçlarla izleme, PVSK Ek m. 7(2)'de bilişim suçlarını önleme amaçlı olarak düzenlenmiştir. Üstelik kolluğun emriyle dahi iletişim verilerinin tespit edebileceği, dinlenebileceği, sinyal bilgileri değerlendirilebileceği ve kayda alınabileceği hüküm altına alınmaktadır. Önemle üzerinde durmak gerekir ki kişisel verilerin işlenmesini hedef alan bu tedbirlerin alınabilmesi için CMK'da, hâkim veya savcı kararının gerekeceği düzenlenmiş ve fakat kolluk amirlerine böyle bir yetki tanınmamıştır.

PVSK hükümlerinden çıkan sonuca göre, önleyici amaçla elde edilen verilerin adli amaçlarla kullanılmasında kanuni düzenleme şartının varlığı sebebiyle hukuka aykırı bir durumun olmadığı düşünülebilir. Fakat esasında elde etme yetkisini aldığı önleyici amaçlı faaliyetleri düzenleyen hükümlerin genişletilmesi suretiyle suç sonrası yapılan ceza

---

Bu madde hükmü gereğince bir suça müdahale eden polise karşı işlenen suçlar görevli memura karşı işlenmiş suç; müdahalede bulunan polisin işlediği suçlar ise görevli memurun işlediği suç sayılır."

PVSK Ek Madde 5 hükmüne göre: *"Genel güvenlik, kaçakçılık ve uyuşturucu maddelerle ilgili önemli olayları takip etmek, gerekiyorsa müdahale ederek soruşturmasını yapmak üzere;*
A) İçişleri Bakanlığınca doğrudan veya ilgili valinin talebi üzerine merkez personelinden ekipler (timler) görevlendirilebilir.
B) Yukarıdaki bent hükmüne uygun olarak bir ilde soruşturması yapılan olayın aydınlatılması, delillerin toplanması, sanıkların yakalanması, başka illerde de araştırma ve soruşturma yapılmasını gerektiriyorsa iller arasında ilgili valiliklerce ekipler görevlendirilebilir. Bu ekiplerin polis yetkilerini kullanması, polis bölgesi sınırları ile kayıtlı değildir.
Bu ekipler görev yaptıkları mahallin en büyük mülki amirine bilgi vermek zorundadırlar. Görevin ifası sırasında mahallin en büyük mülki amirine karşı da sorumludurlar.
Genel ve özel kolluk makam ve memurları bu personele gereken her türlü yardımı yapmaya mecburdur."

[291] Adli göre ve yetkiler hükümleri PVSK Ek m. 6'da düzenlenmektedir:
"Polis, olaydaki failin, gözaltına alınan şüpheli ile aynı kişi olup olmadığının belirlenmesi bakımından zorunlu olması halinde, Cumhuriyet savcısının talimatıyla teşhis yaptırabilir. ...
Teşhis işlemine tâbi tutulan kişilerin, bu işlem sırasında birlikte fotoğrafları çekilerek veya görüntüleri kayda alınarak, soruşturma dosyasına konur. ...
Şüphelinin fotoğrafı üzerinden de teşhis yaptırılabilir. Ancak tek bir fotoğraf veya aynı kişinin farklı fotoğrafları üzerinden teşhis yaptırılamaz. Değişik kişilerin fotoğraflarının aynı büyüklük ve özellikte olmaları gerekir. ..."

yargılaması sürecinde kullanılması söz konusu olmaktadır. Dolayısıyla, kanun koyucunun gerekli düzenlemelerle bunu güçleştirici önlemler alması yerinde olacaktır.

2. Kişisel verilerin işlenmesine yol açan koruma tedbirlerinin ve delil değerlendirme yöntemlerinin CMK'da düzenlenmesinin önemi

Başta şüpheli olmak üzere kişilerin verileri üzerinde delil elde etmeye yönelik uygulanacak tedbirler CMK'da özel hükümlerle düzenlenmektedir. Bu özel düzenlemelerin varlığının sebebi, uygulanan yöntemlerin kişisel verilerin gizliliğinin yanı sıra diğer temel hak ve hürriyetlerine yönelik getirilecek sınırlamaların bazı güvenceleri haiz olması gerekmesindendir[292].

Burada önem taşıyan husus, sınırlayıcı tedbirlerin alınmasında hâkim, savcı veya kolluk makamlarının uyması gereken usulün, arkasında yatan insan haklarının korunması mantığı doğrultusunda belli bir metodoloji izlenerek bazı şartları içerecek şekilde düzenlenmiş olmasıdır. Çünkü koruma tedbirleri ve delil değerlendirme yöntemlerinin bazı ortak özelliklere ve şartlara sahip olması gerekmektedir. Bu noktanın tezimiz kapsamında öne çıkan en önemli gerekçeleri, özel hayatın gizliliğini ve kişisel verilerin korunması hakkının ihlal edilmemesidir.

Ayrıca, CMK'ya göre kişisel veriler üzerinde alınacak adli tedbirlerde suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması aranıyor olmasıdır. Dikkat edilmelidir ki PVSK'ya göre alınacak önleyici tedbirlerde makul şüphenin varlığı benzer yöntemler için yeterli olmaktadır. Dolayısıyla, kişisel veriler ile ilgili CMK güvencesinden mahrum bırakılarak kişisel verilerin işlenmesi kamu görevlilerine geniş takdir alanı bırakarak kişisel verilerin işlenmesini kolaylaştıran bu PVSK hükümlerinin düzeltilip değiştirilmesi gerekmektedir.

Önleyici amaçla elde edilen verilerin adli amaçlarla kullanılması kişisel verilerin işlenmesinde amaçla bağlılık ilkesine zıt olduğu gibi hiç şüphesiz hukuk güvenliğini de zedelemektedir. Keza adli faaliyetlerde bulunabilen kamu görevlileri önleyici olarak daha kolay elde ettikleri verileri kullanabilmektedirler. Bunu belirginleştiren en önemli örnek olarak kamusal alanda kameralı gözetlenmesinde kullanılan MOBESE yani Mobil Elektronik Sistem Entegrasyonu üzerinden bir değerlendirme yapılabilir. MOBESE,

[292] Bu konudaki detaylı açıklamalar için Dördüncü Bölüm(II)(A) başlığına bakılabilir.

bilindiği üzere temel gayesi trafik akışının kontrolü için oluşturulan ve kural ihlali yapan kişilere idari para cezası kesilmesinde delil sunan bir kameralı gözetim sistemidir. MOBESE dışında, iş yeri, alış veriş merkezleri, taksilerde, kreş ve okul gibi alanlarda da mevcut olan önleyici gözetleme sistemleri bulunmaktadır.

Önleyici amaçlı elde edilen bu veriler, kişilerin görüntüleri başta olmak üzere onların vücut bütünlüğü ve iletişim verileri gibi kişisel verilerini barındırmaktadır. Ayrıca bir bireye odaklanmayan fakat onu belirli kılabilecek her türlü veri de kişisel veri olacağı için unutulmamalıdır. Bu doğrultuda amaçla bağlılık prensibi çerçevesinde önleyici amaçla elde edilen kişisel verilerin sadece önleyici amaçlar çerçevesinde kullanılması gerekmektedir. Aksi halde, yani verinin işlenmeden önce belirtilen amaçlardan farklı amaçlar için kullanılması durumunda bu durum amaca bağlılık ilkesi açısından sorun teşkil etmektedir[293].

Fakat soruşturma sürecinin başlamasıyla önleyici tedbirlerle elde edilen veriler adli makamların da dâhil olduğu yargılama sürecinde işlenen suçu aydınlatma amacıyla kullanılabilmektedir. Böylece önleyici ve adli tedbirlerle elde edilme olarak ikiye bölünerek sınıflandırılan ayırım bu noktada son bulmakta, iç içe geçmektedir. Oysa Türk hukukunda çifte karakterli işlemlerle ilgili bir düzenleme olmadığından bu tarz verilerin hiçbir şarta bağlı olmaksızın adli süreçlerde kullanılmasının engellenmesi gerekmektedir[294]. Üstelik önleyici tedbirler sonucunda kişilerin verilerinin çoğu zaman onlardan habersizce elde ediliyor olması nedeniyle elde edilen verilerin ceza soruşturması açısından kural olarak hukuka aykırı delil statüsünde olacağına dikkat edilmelidir.

Doktrinde de bu doğrultuda, özellikle iletişimin tespiti kararlarında tedbir kararının verildiği tarihin öncesine ilişkin verilerin dosyaya delil olarak koyulmasının kural olarak mümkün olmadığı ifade edilmektedir[295]. Dolayısıyla, CMK'da yer alan güvencelerden bağımsız olarak kanunla düzenlenen önleyici tedbirler sonucu elde edilen delillerin bir

[293] Çekin, s. 48.
[294] Abanoz, Buket: Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu, İstanbul 2018, s. 38.
[295] Dülger, 2019, s. 331.

adli tedbir mahiyetinde olamayacağı sebebiyle soruşturma evresinde kullanılması mümkün değildir[296].

Bu gerekçelerle, koruma tedbirleri ve delil değerlendirme yöntemlerine hâkim olan güvencelerin önleyici tedbirler yoluyla bertaraf edilmesi sebebiyle önleyici amaçlarla elde edilen verilerin bir koruma tedbiriymişçesine ceza muhakemesinde kullanılabilecek delil niteliğinde olmayacağını düşünmekteyiz.

3. Farklı düzenlemelerdeki hükümlerin yetki kaynağı karmaşasına yol açması

Kişisel verilerin işlenmesi faaliyetlerinin dayandığı önleyici ve adli düzenlemeler arasında karışıklık mevcuttur. Bu durum kendisini, kullanılmakta olan yetkilerin birbirinden bağımsızlaşmaması noktasında kendisini göstermektedir. Diğer bir deyişle, somut olaya uygulanacak hükmün kanun mu yönetmelik mi olacağı belirsizliği yaşanmaktadır. Bunun bir sebebi, başta delil toplama işlemleri olmak üzere soruşturma evresinde kişisel verilerin işlenmesi hususunda sadece CMK değil, PVSK'da da hükümler bulunması; diğer bir sebebi ise Adli Kolluk Yönetmeliği'nin CMK'ya aykırı hükümler barındırıyor olmasıdır.

Aslında önleyici tedbirlerin PVSK'da ve adli tedbirlerin CMK'da olacak şekilde; CMK hükümlerinin detaylandırıldığı Adli Tedbir Yönetmeliği'nin de CMK'ya aykırı hüküm içermeyecek şekilde düzenlenmesi gerekirken somut olaylara uygulanacak hükmün tespitindeki muğlaklık uygulamada da karışıklıklara yol açmaktadır. Devletin bu noktada etkili ve dengeli kural koyma konusundaki pozitif yükümlülüğünü yerine getirmemesi elbette kişisel verilerin yer aldığı soruşturmalarda, müdahalede öngörülebilirlik unsurunu ihlal etmektedir. Bu da, AİHS m. 6'nın koruduğu adil yargılanma hakkı açısından ve m. 8'in koruduğu kişisel verilerin korunması açısından hukuka aykırılık teşkil etmektedir.

Dolayısıyla, kişisel verilerin işlenmesine dayanak olan bu düzenlemeler hem kurallar arasındaki yeknesaklığı bozmakta hem de kamu görevlilerine geniş takdir alanı bırakarak kişisel verilerin işlenmesini kolaylaştırmaktadır. Dolayısıyla olması gereken, kişisel verilerin işlenmesine ilişkin işleme yöntemlerinin ya sadece CMK'da yer alması ya da

[296] Aydın, Sedat Erdem: AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul 2015, s. 88.

her düzenlemede en az CMK düzenlemelerinin sahip olduğu güvenceleri içeriyor olmasıdır.

Üstelik adli tedbirlerle elde edilebilecek delillerin önleyici tedbirlerle elde edilerek soruşturmada delil niteliği kazandırılma çabası, hem bir bakıma kanun etrafından dolaşıldığını göstermekte hem de devleti vatandaşına tuzak kuran bir pozisyona düşürmektedir. Devleti polis devletine dönüştüren bu durumun demokratik toplum yapısı ve gereklilikleri ile bağdaşmamaktadır.

Olması gereken, koruma tedbirleri ve delil değerlendirme yöntemlerinin uygulanmasının temel amacı olan maddi gerçeğe ulaşılmasında insan haklarına ve hukuka aykırı yollardan sağlanması fikrinin hem mantıkî hem de hukukî açıdan mümkün olmayacağı ve olmaması gerektiği görüşünün hâkim olmasıdır[297]. Bu minvalde, PVSK'da yer verilen adli tedbir hükümlerinin CMK ile içerdiği güvenceler açısından ayrı ayrı karşılaştırılarak önleyici tedbirlerin adli tedbirlere dönüştürülmesinin engellenmesi önemlidir.

C. Bir Suçun İşlendiğini Öğrenen Cumhuriyet Savcısının Görev Ve Yetkileri

1. Soruşturma işlemleri açısından

Soruşturma, yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evreyi ifade etmektedir. İhbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez hemen işin gerçeğini araştırmaya başlayan Cumhuriyet savcısının görev ve yetkileri başta olmak üzere soruşturma işlemlerine ilişkin hükümler CMK m. 161 ila 169 arasında düzenlenmektedir. Buna göre Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adlî kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilmekte; suç ile ilgili sonuçlara varmak için bütün kamu görevlilerinden her türlü bilgiyi isteyebilmektedir.

Bu noktada kişisel veriler açısından belirtmek gerekir ki, bu yetki her ne kadar genel anlamda düzenlenmiş olsa bile mutlak bir yetki değildir. Bunun anlamı, başta kişisel veriler olmak üzere, Cumhuriyet savcısının yapabileceği her türlü araştırma ve isteyebileceği her türlü belgenin suç kapsamında olması ile sınırlanmış olmasıdır. Bu yüzden, bir suç şüphesi altında bulunan şüpheli ile ilgili kişisel veri içeren ve suçu

[297] Dülger, Murat Volkan: Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi), Ankara 2014, s. 40.

aydınlatma kabiliyeti bulunmadığı ortada olan hususların Cumhuriyet savcısınca araştırılmaması; çeşitli kurum ve kişilerden bilgi ve belge istenmemesi gerekir. Fakat bu hususların suçu aydınlatacağı düşünülürse de bu halde savcının kararında bunun gerekçesini de belirtmesi gerekiyor olmalıdır.

CMK m. 161(4)'te diğer kamu görevlileri de, yürütülmekte olan soruşturma kapsamında ihtiyaç duyulan bilgi ve belgeleri talep eden Cumhuriyet savcısına vakit geçirmeksizin temin etmekle yükümlü tutulmaktadır. Burada şunu ifade etmek gerekir ki, söz konusu görevliler Cumhuriyet savcısının talebini gözden geçirmeli ve suç ile bağlantısı olmayan kişisel verileri vermemelidir. Bunu yaparken, her ne kadar soruşturma evresi KVK Kanunu'nun istisnaları arasında sayılmış olsa bile, hem hakkın özüne yönelik hem de meşru bir sebep olmadan müdahale gerçekleşmekte olduğu gerekçesi ileri sürülebilir. Bu şekilde davrandıklarında görevlerini kötüye kullanma veya ihmallerinin söz konusu olmayacaktır. Aksine verileri paylaştıklarında konusu suç teşkil eden emrin icrası kapsamında TCK'da kişisel verilerle ilgili düzenlenen suçlardan sorumluluklarının meydana gelmesi dahi mümkün olabilecektir.

Öte yandan, soruşturma evresinde yapılan her soruşturma işleminin tutanağa bağlanması gerekmektedir[298]. Soruşturmanın yazılılığı ilkesinin bir yansıması olan bu hüküm doğrultusunda belirtmek gerekir ki, müdafi veya vekil sıfatıyla hazır bulunduğu işlemlerle ilgili tutanakta avukatın isim ve imzasına da yer verilmesi öngörülmektedir. Bu hüküm açısından ifade etmeliyiz ki, avukatın kişisel rızası varsa ismi yer alabilir fakat yoksa bunun yerine sicili numarası yazılması gerekir. Çünkü avukatın ismi bir kişisel veridir ve bu bağlamda bu şekilde korunması da soruşturma işlemlerini aksatacak bir durum da oluşturmayacaktır. Bu yargımız, CMK m. 169(4)'te belirtilen, tutanağın işleme katılan veya ilgisi bulunan kimselerin isimlerini içereceği hükmü için de geçerlidir. Keza aynı hassasiyeti taşıyan kanun koyucu CMK m. 169(7)'de, maddede sayılan suçlarla ilgili yürütülen soruşturmalarda, kolluk tarafından düzenlenen tutanaklara, ilgili görevlilerin açık kimlikleri yerine sadece sicil numaraları yazılacağını düzenlemektedir.

Ayrıca, kolluk görevlilerinin ifadesine başvurulması gerektiği hâllerde çıkarılan davetiye veya çağrı kâğıdı, kolluk görevlisinin iş yeri adresine tebliğ edileceği ve bu kişilere ait ifade ve duruşma tutanaklarında adres olarak iş yeri adresleri gösterileceği

[298] CMK, m. 169.

düzenlenmektedir. Burada amaç görevli kişilerin kendisi ve ailesinin can ve mal güvenliğini sağlamaya yönelik olduğundan, aynı usulü soruşturma sürecinde yer alan her bir kişi için kişisel verilerin korunması amacıyla genişletmenin önünde bir engel olmaması gerekir.

2. İddianame düzenleme açısından

İddianamenin düzenlenmesi ilişkin hükümler CMK m. 170 ila 174'de belirtilen kurallar arasında yer almaktadır. Bilindiği üzere, soruşturma evresi sonunda toplanan deliller, suçun işlendiği hususunda yeterli şüphe oluşturuyorsa; Cumhuriyet savcısı, m. 170(3)'e göre çeşitli unsurlara sahip olan bir iddianame düzenlemek zorundadır[299].

Kişisel veriler açısından bu madde üzerinde öne çıkan şu hususu belirtmek gerekir ki şüphelinin, müdafinin, maktul, mağdur veya suçtan zarar görenin, bunların varsa vekili veya kanunî temsilcisinin, ihbarda veya şikâyette bulunan kişinin kimliği eğer soruşturulan suç açısından kaçınılmaz surette gerekli ise açık olarak yazılmaktadır.

Bizim görüşümüze göre bunun yerine öncelikle ilgililerin kimlik numaraları gibi kişiyi doğrudan açıkça belirtmeyen fakat soruşturulması için yeterli imkân sağlayan tali yollara başvurulmalıdır. Aksi halde gerekli olmadığı halde kişilerin açık kimlik bilgileri dosyaya erişebilen ilgili ya da ilgisiz herkesçe öğrenilmektedir. Üstelik bu kişiler sır tutma yükümlülüğü altına olmayan kişiler de olabilmektedirler. Kanun'un bu düzenlemesi, başta özel hayatın gizliliği olmak üzere kişisel verilerin korunması hakkına yönelik orantısız ve sürekli bir müdahale teşkil etmektedir. Bu yüzden de soruşturma evresi işlemlerinin bütünsel olarak KVK Kanunu'nda istisna kapsamı içerisinde kaldığını savunarak iddianamenin bu şekilde düzenlenmesi mümkün olmamalıdır.

---

[299] İddianamenin içeriğine ilişkin unsurlar CMK m. 170(3)'te düzenlenmektedir:
"(3) Görevli ve yetkili mahkemeye hitaben düzenlenen iddianamede;
a) Şüphelinin kimliği,
b) Müdafii,
c) Maktul, mağdur veya suçtan zarar görenin kimliği,
d) Mağdurun veya suçtan zarar görenin vekili veya kanunî temsilcisi,
e) Açıklanmasında sakınca bulunmaması halinde ihbarda bulunan kişinin kimliği,
f) Şikâyette bulunan kişinin kimliği,
g) Şikâyetin yapıldığı tarih,
h) Yüklenen suç ve uygulanması gereken kanun maddeleri,
i) Yüklenen suçun işlendiği yer, tarih ve zaman dilimi,
j) Suçun delilleri,
k) Şüphelinin tutuklu olup olmadığı; tutuklanmış ise, gözaltına alma ve tutuklama tarihleri ile bunların süreleri, gösterilir."

Ayrıca kişisel verilerin korunması sürecinin getirdiği yenilikler çerçevesinde, iddianamede yer alan suç delilleri için de delil niteliğini kaybetmeyecek ölçüde anonimleştirilmesinin önem kazanmakta olduğunu ifade etmeliyiz. CMK m. 170(4)'te belirtildiği üzere, nasıl iddianamede yüklenen suçu oluşturan olayların mevcut delillerle ilişkilendirilerek açıklanması gerekli ise bizce mevcut delillerle ilişkilendirilemeyen olay ve kişisel verilerin iddianamede yer almaması da gerekmektedir. Keza burada soruşturmanın amacı dışında toplanan veriler bulunabilmektedir ki derhâl imha edilmemesi hali kural olarak suç teşkil etmektedir. Usulünce alınmayan karara binaen toplanan verilerin derhâl imhası üzerinde zaten bir tartışma söz konusu değildir. Böyle durumlarda disiplin ya da ceza hukuku hükümlerince işlemi gerçekleştirilmesinde rol oynayanların sorumluluklarına gidilebilecektir.

Öte yandan m. 171(5)'e göre, kamu davasının açılmasının ertelenmesine ilişkin kararlar, bunlara mahsus bir sisteme kaydedilmektedir. Bu kararların içerisinde herhangi bir kişiyi belirlenebilir kılan her türlü verinin kişisel veri olduğu üzerinde duraksama yaşanmamaktadır. Bu verilerin hukuka uygun kanuni süreler içerisinde muhafaza edildikten sonra imhası gereklidir. Ayrıca bu verilerin gizliliği esastır.

Bu madde bağlamındaki kayıtların, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak Cumhuriyet savcısı, hâkim veya mahkeme tarafından istenmesi halinde, sadece bu maddede belirtilen amaç için kullanılabileceği düzenlenmektedir. Buradaki amaç ise hakkında kamu davasının açılması ertelenen bir kişinin erteleme süresi içerisinde suç işlemesi halinde bu kayıtlara erişim sağlanmasıdır. Madde metninden anlaşılabilen farklı bir anlam da çıkmamakta olduğundan bahsedilen bu kayıtların bir başka amaçla ya da farklı bir dosya kapsamında kullanılması mümkün değildir. Erteleme süresi sona erdiği takdirde orantısız şekilde kaydedilmiş olan bu kayıtların da usulünce imha edilmesi gerekmektedir.

3. Kişisel verilerin toplanmasına karar verebilecek olan mercilerin veri sorumlusunun yükümlülüklerine tabi olması

Tezimizin önceki bölümlerinde belirttiğimiz üzere, kişisel verileri işleyen kişilerin veri sorumlusu olarak veri sorumluları siciline kayıt olmaları gerekmektedir. Soruşturma sürecinde CMK'da karar verme merci olarak kanunen yetkilendirilen hâkim, savcı ya da

kolluk görevlilerinin bu açıdan veri sorumlusu olarak görülebileceğini ifade etmek gerekir.

Her ne kadar veri sorumluları sicili daha çok özel hukuk tüzel kişilerinin sorumlulukları açısından düzenlenen bir husus olsa da bunun devlet tüzel kişiliği içerisinde hareket eden kişi ve kurumlar için de uygulanmasının mümkün olduğunu düşünmekteyiz.

Fakat bu halde, ne kişisel verinin işlenmesi talimatını veren her görevlinin ayrı ayrı olarak sicile kaydı ne de makamın sicile kayıtlarının pratik gerekçelerde söz konusu olmayacağı iddia edilebilir. Üstelik KVK Kanunu m. 28(2)'de kişisel veri işlemenin suç soruşturması için gerekli olması ve KVK Kanunu'nun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla bu sicile kaydın zorunlu tutulmayacağı belirtilmiştir.

Bizim görüşümüze göre, bu kişisel verilerin işlenmesine ilişkin genel ilkeler, soruşturma evresinde veri işleyen kişilerin sicile kayıtlı olmasını da gerektirir. Çünkü görevlilerin kişisel verilerin korunması gibi Türk hukukunda nispeten yeni düzenlenen bir alana ait kuralların gereğini yapacakları uzak bir ihtimaldir. Dolayısıyla, KVK Kanunu m. 16'nun soruşturma istisnası kapsamına alınması için bir neden bulunmamaktadır. Böyle bir durumda, görevli kişilerin eğitime tabi tutulup sertifika almaları da sağlanabilir.

Yine de CMK kapsamında kişisel verilerin delil olarak işlenmesi kararını veren hâkim, savcı ve kolluk görevlilerinin kayıt olma zorunluluğunun olmayacaksa eğer bu istisnanın özel bir kanuni düzenlemeyle yapılmasının gerekeceğini düşünmekteyiz. Ayrıca, başka bir fikir olarak kişisel verilerin işlenme kararını veren yargı görevlilerinin, KVK Kurumu'na bildirim yapma zorunluluğu da getirilebilir.

II. KİŞİSEL VERİLERİN SORUŞTURMA SÜRECİNDE İŞLENMESİ İLKELERİ

A. Türk Hukukunda Soruşturma Sürecine Hâkim Olan İlkeler

1. Genel olarak

Soruşturma evresine ilişkin ceza muhakemesi hükümleri CMK m. 90 ila 175 arasında düzenlenmektedir. Burada Türk hukukunda soruşturma sürecine hâkim olan ilkeler kaynağını insan haklarında bulmaktadır. Buna göre, insan haklarının pratikte gerçekleştirilebilmesi için ceza hukukuna ilişkin süreçlerde de devletin çeşitli

mekanizmalar sağlaması yönünde pozitif ve bu hakları ihlal etmemesi yönünde negatif yükümlülükleri bulunmaktadır.

Özellikle ceza muhakemesi kapsamındaki soruşturma evresinde bireyin özgürlüğüne, vücut bütünlüğüne ve özel hayatı gibi birçok temel insan hakkına yönelik idare tarafından müdahale edilebilmektedir. Bu müdahalenin ve elde edilen delillerin hukuka aykırı olmaması için alınacak tedbirlerin çizilen kanunî sınırlar içerisinde olması oldukça elzemdir. Bundan dolayı, ceza soruşturması sürecinde insan haklarına yönelik yapılmakta olan müdahalelerin tabi olduğu sınırların açık ve öngörülebilir bir usul çerçevesinde olması şarttır. İşte bu kısımda, söz konusu sınırları belirleyen ilkeler, kişisel verilerin korunması hakkı açısından açıklanmaktadır. İdare açısından hem pozitif hem de negatif yükümlülükler içeren bu ilkelerin hepsi adil yargılanma hakkı ile bağlantılıdır.

Öncelikle, tezimiz kapsamında soruşturma sürecinde hâkim olan en önemli ilkenin soruşturmanın gizliliği ilkesi olduğunu belirtmek gerekir. CMK m. 157(1)'de de düzenlenmekte olan gizlilik ilkesine göre, kanunun başka hüküm koyduğu hâller saklı kalmak ve savunma haklarına zarar vermemek koşuluyla soruşturma evresindeki usul işlemleri gizli tutulmalıdır. İnsan hakları açısından gizlilik ilkesi AİHS ve Anayasa'da düzenlenmekte olan adil yargılanma hakkına, özel hayatın gizliliği hakkına, kişisel verilerin korunması hakkına ve kişi dokunulmazlığı hakkı vb. haklara ve suç ve cezalara ilişkin esaslara dayanmaktadır. Gizliliği korumaktaki başarısız, kişisel özgürlük ve otonominin varlığı olumsuz etkileyecektir[300].

Gizlilikteki bir diğer önemli amaç soruşturma aşamasında elde edilen kişisel verilerin çeşitli kararlarla kovuşturma aşamasına geçilmemesiyle sonuçlanması halinde ortadan kaldırılma yükümlülüğüdür[301]. Bunun yanı sıra CMK m. 153'te de kendisi ile ilgili düzenleme olan bu ilkenin ihlali halinde TCK m. 258'de düzenlenen Göreve ilişkin sırrın açıklanması suçu meydana gelebileceğini belirtmek gerekir.

Tez kapsamında soruşturma sürecine hâkim olan ikinci önemli ilke soruşturmanın kurala bağlı olmayışı ilkesidir. Bunun anlamı, soruşturma evresinde araştırmaların nasıl

[300] Fleckenstein, Marilynn/Maury, Mary/Pincus, Laura/Primeaux, Pat: From the Universities to the Marketplace: The Business Ethics Journey: The Second Annual International Vincentian Conference Promoting Business Ethics, Berlin 2012, s. 28.

[301] Özellikle genetik inceleme sonuçlarının gizliliğine ilişkin CMK m. 80(2) hükmü ve fizik kimliğin tespitine ilişkin CMK m. 81(2) hükmü buna örnek verilebilir.

yapılacağı, hangi sıranın izleneceğinin düzenlenmemiş olup işlemlerin icrasının soruşturmayı yapan makamları takdirine bırakılmasını ifade etmektedir[302].

Fakat bu takdir marjının sınırsız olamayacağını belirtmek gerekir. Görevlilerin takdirleri çerçevesinde yapılan uygulamanın başta insan onurunun korunması olmakla birlikte, ceza muhakemesi ilkeleri, hukuk devleti ilkesi ve diğer temel hak ve hürriyetlere uygun olarak gerçekleştirilmesi şarttır[303]. Bu nedenle, tezimizin ilerleyen kısımlarında daha detaylı inceleyeceğimiz üzere, soruşturma evresinde kişisel verilerin korunması bahsinin hiçbir sınırlamaya tabi olmadan soruşturma mercilerinin takdirine bırakılmasının söz konusu olamayacağını belirtmemiz gerekmektedir.

Üçüncü ilke, soruşturmanın yazılılığı ilkesidir. Bu ilke, soruşturma sürecinde yapılan tüm işlemlerin yazılı olmasını sağlamaktadır. CMK m. 97 yakalama tutanağının ve m. 147 de ifade ve sorgu tutanağının yazılı olması gerektiğini açıkça düzenlemektedir. Yazılılık ilkesi sayesinde m. 148 kapsamında ifade alma ve sorguda yasak usullerle ifade alımının denetlenmesi imkânı sağlamaktadır. Ayrıca, soruşturma evresi sonucunda sunulan iddianame dosyası ve içeriğinin yazılı olarak kayıt altına alınmış olması sebebiyle kovuşturma makamlarının kişisel verilere erişimi oldukça kolaylaşmaktadır.

Dördüncü ilke, soruşturmanın dağınıklığı ilkesidir. Bu ilke soruşturmayı yapan asli makam olan savcının delillere erişiminde belli bir sıra izlemeden özgürce hareket etmesi ilkesidir. CMK m. 161(1)'de kaynağını bulan bu ilkeye göre Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adlî kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir; maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, bütün kamu görevlilerinden her türlü bilgiyi isteyebilir. Savcı bunu yaparken, emrindeki adlî kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür.

Bu ilke doğrultusunda gerçekleştirilme usulü savcılık ve kolluk görevlilerinin takdirine bırakılan soruşturma işlemleri için kanun ve yönetmeliklerde belirtilen usullere uymak zorunlu olduğundan soruşturmanın dağınıklığı ilkesinin mutlak bir ilke olduğundan bahsedilemez. Yargıtay da bir kararında, maddi gerçeğin araştırılması aşamasında kişisel

[302] Parlar, Ali/Çetin, Ahmet: Ceza Muhakemesinde Soruşturma Evresi Ve Uygulaması, İstanbul 2017, s. 71.
[303] Parlar/Çetin, s. 72.

ya da toplumsal değerlerin korunması zorunlu olduğundan hareketle delillerin serbestliği ilkesinin mutlak olmayıp delil yasakları olarak adlandırılan bir takım sınırlamalara tabi olabileceğini belirtmektedir[304]. O halde kişisel veri işleyen kamu görevlilerini sınırlayan kurallar soruşturmanın dağınıklığı ilkesine halel getirmemektedir.

Beşinci ilke, soruşturmanın kesikliği ilkesidir. Kesiklik ilkesi soruşturma işlemlerinin tek seferde yapılmamasını ifade etmektedir. Böylece suç delillerini araştırmak ve iddianame düzenlemekle görevli savcılık makamına süre açısından yeterli işlemleri yapabilmesinin imkânı verilmektedir. Soruşturma işlemlerinde kişi ya da mekânsal bir sınırlama olmayışını ifade eden dağınıklık ilkesi ile de oldukça yakın olan bu ilkeye göre zamansal açıdan savcılık makamının belli bir sınırlama olmadan işlemleri gerçekleştirilmesi amaçlanmaktadır.

Altıncı ilke, soruşturmanın kısa ve gecikmez olması ilkesidir. Bu ilke, şüphe altında bulunan kişi üzerindeki şüphenin ve alınmış olan koruma tedbirleri ve delil değerlendirme yöntemlerinin nihayete ermesini için soruşturma işlemlerinin derhâl ve gecikmeksizin yapılmasını ifade etmektedir. Ceza yargılaması suç ile uğraştığından medeni yargılamanın aksine delillerin önceden hazırlanması da mümkün olmamaktadır. Bu doğrultuda özellikle kişisel verilerin korunması açısından işlenmekte olan veriler üzerinde olduğu gibi diğer tedbirlerle elde edilen delillerin de sınırlı bir süreden sonra silinmesi, imha edilmesi vs. gibi nedenlerle yargılamanın en kısa sürede bitirilmesi gerekmektedir[305]. Bu açıdan özellikle kişinin özgürlüğüne yönelik doğrudan müdahalenin olduğu yakalama, gözaltı, ifade alımı ve tutukluluk tedbirlerinde kendisini gösteren bir ilkedir.

Anayasa m. 141(4)'te de yer verilen bu ilke doğrultusunda uygulanacak tedbirler için süreler bakımından kesin olan üst sınırlar kanunlarda belirtilmiştir[306]. Bu ilke doğrultusunda örneğin fizik kimliğin tespiti veya muayene ve genetik bilgilerin ya da

[304] Y. 16. CD, 21.04.2016, E. 2015/4672 K. 2016/2330, Erişim Tarihi: 2 Mart 2019, Kazancı İçtihat Bilgi Bankası.
[305] Yurtcan, Erdener: Ceza Yargılaması Hukuku, Ankara 2018, s. 74.
[306] Ayrıca, bu ilke doğrultusunda m. 94 uyarınca, yakalama emri üzerine soruşturma evresinde yakalanan kişi, en geç yirmi dört saat içinde yetkili hâkim veya mahkeme önüne çıkarılması gerekmektedir. Ayrıca CMK m. 95 uyarınca, şüpheli yakalandığında, gözaltına alındığında veya gözaltı süresi uzatıldığında, Cumhuriyet savcısının emriyle bir yakınına veya belirlediği bir kişiye gecikmeksizin haber verilmesi de gerekmektedir. Bir başka örnek olarak m. 101(4)'de belirtildiği üzere, tutuklama kararı verilmezse, şüphelinin derhâl serbest bırakılması gerektiği gösterilebilir.

iletişim verilerinin tespitine yönelik işlemden elde edilen bulguların takipsizlik kararına itiraz edilip de itiraz reddedilirse bu andan itibaren; itiraz edilmezse derhâl yok edilmesi gerekmektedir.

Yedinci ilke, soruşturmanın kamusallığı ilkesidir. Bu ilke suç işlendiği şüphesi varsa kamu makamlarınca doğrudan soruşturmaya başlanmasını ifade etmektedir. Bazı suç tiplerinde şikâyet aranıyor olsa bile, ihkakıhak yasağı çerçevesinde devletten başka hiçbir kişi ve kurumun ceza soruşturması yapma görevi ve yetkisi bulunmamaktadır. Diğer bir deyişle, yargı yetkisi hususunda devlet kendisine tabiri caizse paralel olan hiçbir oluşumu kabul etmez. Soruşturmaya başlama ve sürdürmede kuralın bu hususun devletin tekelinde olması nedeniyle devletin ajanlarının bu kamu görevini kendiliğinden yerine getirmesi gerekmektedir.

Sekizinci ilke, soruşturmanın kanuniliği ilkesidir. Bu ilkeye göre ilgili kamu makamları suç şüphesini öğrenmelerinden itibaren soruşturmaya başlamanın yanı sıra kanunen görevli oldukları tüm soruşturma kapsamındaki işleri yerine hukuka uygun olarak getirmekle yükümlü olmalarıdır. Bu yükümlülük gereğince gerçekleştiği iddia edilen suç ile ilgili şüpheli, mağdur ve diğer kişiler lehine ve aleyhine olabilecek kişisel veri içeren tüm delillerin kanuni sınırlar çerçevesinde toplanması gerekmektedir. Bu işle görevlendirilen kişilerin görevlerini yapmamaları yahut ihmal etmeleri halinde TCK'da belirtilen görevi kötüye kullanma suçlarının yanı sıra kişisel verilerin ihlali suçları meydana gelebilecektir.

Zikredilenlerin dışında, tezimiz bağlamında değerli olan iki önemli ilkeden daha bahsetmek gerekir. Bu ilkelerden ilki sınırlı yasallık ilkesi yani anayasal bir insan hakkını sınırlayan koruma tedbirleri ve delil değerlendirme yöntemleri düzenlemelerinin sınırsız olamayacağını ifade eder. İkincisi ise koruma tedbirlerinin geçmişe değil ileriye dönük uygulanması ilkesidir[307].

Sonuç olarak, soruşturmanın gizliliği ilkesi başta olmak üzere diğer ilkelerin, bütün suç soruşturmalarında kural olarak uygulanması gerekmektedir. Bu ilkelerin kişisel verilerin işlenmesi sürecinde de kişisel verilerin korunması açısından niteliğine uygun düştüğü

[307] Dülger, 2019, s. 333.

ölçüde özenle uygulanması verilerin soruşturma evresinde hukuka uygun olarak işlenmesi için oldukça önemlidir.

2. Kişisel verilerin korunması açısından

Türk hukukunda soruşturma sürecinde kişisel verilerin korunmasına yönelik hususların bir kül halinde düzenlendiği bir hüküm ne CMK'da ne de diğer yazılı hukuk kuralları arasında bulunmamaktadır. Bu konuda, CMK'da sadece bazı koruma tedbirlerine özel hükümler bulunmaktadır[308].

Fakat kişisel verilerin korunmasına ilişkin genel ilkelerin hukukun her alanında olduğu gibi soruşturma evresinde de yer alması gerekmektedir. Üstelik KVK Kanunu'nda soruşturma evresinin istisna kapsamında tutulmuş olması da KVK Kanunu'ndaki verilerin işlenmesi ilkelerinin soruşturmada uygulanarak kişisel verilerin korunmasına halel getirmeyecektir. Çünkü KVK Kanunu m. 28'in soruşturma işlemlerini tamamıyla kapsam dışında tutması hakkın özüne müdahale oluşturması nedeniyle hukuka aykırıdır. Keza yukarıda diğer gerekçelerle birlikte daha detaylı olarak gerekçelendirdiğimiz üzere kişisel verilerin işlenmesine ilişkin genel ilkelerin soruşturma evresinde kural olarak uygulanabilir olmalıdır[309].

Verilerin korunması hususunun kolluğun keyfine bırakılmaması için bu görev gelişen hızlı teknoloji karşısında gizliliğe ilişkin beklentileri karşılayacak şekilde donatılmamış olan yargı makamlarına değil değişen kamu davranışlarını ölçerek gizlilik ve kamu güvenliği dengesini kapsamlı olarak kurabilecek yasama organına verilmelidir[310]. Keza hâkimler, kendi kişisel hukuk anlayış ve görüşlerine uymasa bile kanunları uygulamakla mükelleftirler[311].

KVK Kanunu m. 4(2)'de kişisel verilerin işlenmesinde uyulması gereken ilkeler sayılmaktadır. Bu ilkeler;

---

[308] CMK m. 80(2) ve 81(2)'de kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde kişisel verilerin Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir.

[309] Daha fazla açıklama için tezin ikinci bölümünün (I)(D)(3)(d) başlığına ve (II)(M)(2) başlığına bakınız.

[310] Wagner, Stephen: "Stopping Police in Their Tracks: Protecting Cellular Location Information Privacy in the Twenty-First Century", Duke Law & Technology Review, 12, Kuzey Karolina 2013–2014, s. 202.

[311] Y. CGK, E. 2007/1-38 K. 2007/44 T. 20.2.2007, Erişim Tarihi: 6 Şubat 2019, Kazancı İçtihat Bilgi Bankası.

- işlemenin hukuka ve dürüstlük kurallarına uygun olması,
- doğru ve gerektiğinde güncel olması,
- belirli, açık ve meşru amaçlar için işlenmesi,
- işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması
- ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesidir.

Soruşturma evresinde kişisel verilerin işlenebileceğini belirten bir görüşe göre, kişilerin bu evrede kişisel verilerinin korunması hakkının ihlal edilmemesi ve ayrıca suçla ilişkisi olmayan kişilerin kişisel verilerinin korunması hakkı gözetilmelidir[312].

Dolayısıyla, soruşturma evresinde keyfi sebeple işlenen her veri, işlemenin hukuka ve dürüstlük kurallarına uygun olması ilkesi açısından hem hukuka aykırı delildir hem de kişisel verilerin korunması hakkının ihlal edilmesi anlamına gelmektedir. O halde, soruşturma evresinde uygulanacak koruma tedbirleri ve delil değerlendirme yöntemlerinin açık, belirli ve meşru bir amacın olduğunun iddia edilebilmesi için, düzenlemenin pozitif hukuk normları kadar insan haklarına ve evrensel hukuk ilkelerine uygun olmasını da gerektirmektedir[313].

Öte yandan, KVK Kanunu'nun 1996 yılı tarihli 95/46/EC sayılı Direktif'i baz alarak hazırlandığını daha önce ifade etmiştik. Fakat 2015 yılında Madde 29 Veri Koruma Çalışma Grubu, 95/46/EC sayılı Direktif'in soruşturma evresini kapsam dışı bırakan hükümlerinin idareye geniş yetki vermekte olduğunu ifade etmiştir. Bunun kişisel verilerin korunması hakkına müdahale oluşturacağı sebebiyle, soruşturma evresinde de kişisel verilerin işlenme ilkeleri, şartları ve ilgili kişinin haklarının uygulama alanı bulması gerektiğini belirtmiştir[314].

Bu doğrultuda, tezimizin genelinde sıklıkla değinmek olduğumuz üzere, her ne kadar KVK Kanunu'nun soruşturma evresine dönük olarak uygulanmayacağı istisna hükümlerinde belirtilmiş olsa da, soruşturma sürecinde işlenmekte olan verilerin saklama

[312] Akgül, s. 29.
[313] Dülger, 2019, s. 330.
[314] Madde 29 Veri Koruma Çalışma Grubu, 3211/15/EN WP 233 Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Adopted on 01 December 2015, s. 2 vd.

ve yok etme usulüne ilişkin olarak ilgili yönetmelik da bu yönetmelikteki hükümlerin uygulanabileceğini düşünmekteyiz. Bunun sebebi, soruşturma evresinin bütünsel olarak istisna kapsamına alınmış olması halinin kişisel verilerin korunması hakkına yönelik orantısız bir müdahale oluşturacağı ve hakkın özüne dokunabileceğidir. Aksi halde, soruşturma evresinde kişisel verilerin saklanması veya yok edilmesine yönelik uygulanacak bir yönetmelik de bulunmamaktadır.

Öte yandan, burada bahsedilen veri sorumluları daha çok özel hukuka tabi gerçek ve tüzel kişileri kapsamakta olduğundan kamu görevlilerin olan hâkim, savcı ve kolluk görevlilerinin aynı yükümlülüğü nasıl yerine getireceği tartışma konusu olabilecektir. Bizim görüşümüze göre, bu yönetmelik kapsamında belirlenmesi gereken verilerin imha politikası hükümleri doğrultusundaki detaylı usul ve kurallar, görevli ve yetkili idare kurumunca çıkarılmalıdır.

Sonuç olarak, soruşturma makamlarının soruşturma evresinde kişisel verilerin delil olarak toplanması sırasında hem soruşturma ilkelerine hem de kişisel verilerin işlenmesine ilişkin genel ilkelerin her birine uygun olarak hareket etmeleri gerekmektedir. Aksi halde hukuka aykırı bir işlemenin varlığı söz konusu olacaktır. Bunun sebebi, bizim görüşümüze göre, her ne kadar soruşturma evresinin KVK Kanunu'nda istisna kapsamına alınmış olsa da bu istisnanın sadece verilerin işlenme şartlarına ilişkin hükümleri kapsadığıdır. Bu yüzden, verilerin işlenmesine yönelik ilkeler yine de uygulanma fırsatı bulacaktır. Bu konuda kişisel verilerin koruma tedbirleri ve delil değerlendirme yöntemleri ile işlenmesi sürecinin bağımsız komisyonca denetlenmesi formülü düşünülmelidir. Yani denetim ve raporlama sayesinde komisyonca uygun bulunmayan verilerin soruşturma aşamasında kullanılmaması da bir çözüm olabilir[315].

KVK Kanunu'nun soruşturmayı istisna kapsamına alan hükmüne karşı bu gerekçeleri ileri sürmemizin nedeni, Anayasa'nın m. 90(5) hükmü doğrultusunda ilgili uluslararası belgelerin yürürlük kazanması sonucu hem uluslararası belgelerde sayılan hem de birazdan üzerinde duracağımız AİHM içtihatlarında belirtilen ilkelerin doğrudan yürürlükte uygulama alanı bulacak olmasıdır. Bu açıdan, KVK Kanunu'nun soruşturmaya ilişkin istisna hükmünün dar yorumlanması gerekmektedir. Buna göre,

[315] Dülger, 2019, s. 330.

alınacak olan her bir koruma tedbiri ve delil değerlendirme yöntemi içerisinde işlenmekte olan verilerin bu bağlamda korunması oldukça önemli ve gereklidir.

B. AİHM Kararları Işığında Belirginleşen İlkeler

1. Genel olarak

AİHM m. 8 ile ilgili önüne gelen başvurularda ihlal iddiası içeren somut olayı yorumlamaya geçmeden önce, m. 8(2) doğrultusunda olduğu ileri sürülecek olan müdahalenin yasal bir temelinin olması, meşru bir amaca yönelik olması ve demokratik toplumda gerekli olması unsurlarının gerçekleşip gerçekleşmediğini incelemektedir[316]. Zikredilen unsurlardan demokratik toplum gerekliliklerine uygunluk diğer unsurlardan daha öne çıkmakta olduğundan bundaki maksadın ne olduğunun daha fazla incelenmesi yerinde olacaktır.

Bu doğrultuda öncelikle AİHS m. 8'in anlamı içinde kişisel verilerin korunması hakkını güvence altına almak amacıyla her davanın kendine has gerçekliğinin dikkate alınması gerekmektedir. Bu noktada AİHM, kendisini nesnel bir ölçüt oluşturma zorunluluğu altında hissetmekte ve verdiği kararlarda bunu geliştirme ve uygulama gayreti içerisinde olduğu görülmektedir. Bu ölçütün ilkelerini ortaya çıkarabilmek için Mahkeme'nin vermiş olduğu değişik kararlara bakılmalıdır.

Buna göre, öncelikle demokratik toplum gerekliliklerine uygun bir müdahalenin m. 8(2)'de sayılan meşru sebepler doğrultusunda temelde zorlayıcı bir sosyal ihtiyaca cevap vermesi gerekmektedir[317].

İkinci olarak ise meşru amaç doğrultusunda yapılacak müdahalenin, hakkı orantılı olarak sınırlayan seviyede olması gerekmektedir[318].

[316] Örnek davalar için bakınız: Dragojević/Hırvatistan, Başvuru No: 68955/11, 15.01.2015, par. 78, Erişim Tarihi: 5 Şubat 2019; Roman Zakharov/Rusya, Başvuru No: 47143/06, Büyük Daire Kararı, 04.12.2015, par. 227, Erişim Tarihi: 18 Şubat 2019.
[317] Coster/Birleşik Krallık, par. 104; S. ve Marper/Birleşik Krallık, par. 101; Michaud/Fransa, Başvuru No: 12323/11, 06.12.2012, par. 120, Erişim Tarihi: 5 Nisan 2019; Campbell/Birleşik Krallık, Başvuru No: 13590/88, 25.03.1992 par. 44, Erişim Tarihi: 5 Nisan 2019.
[318] Sabanchiyeva ve Diğerleri/Rusya, Başvuru No: 38450/05, 06.06.2013, par. 131–132, Erişim Tarihi: 15 Nisan 2019.

Üçüncüsü ise, müdahaleyi haklı kılmak için ilgili ve yeterli gerekçelerin ulusal makamlarca sunulmasıdır[319].

Dördüncüsü ise, yapılacak müdahalenin devletlere tanınan takdir yetkisinin içerisinde kalıp kalmadığının her somut olay açısından ayrı ayrı incelenmesinin gerekli olmasıdır[320].

Bu genel ölçütler doğrultusunda da KVK kapsamında soruşturma evresinin istisna kapsamında tutulmuş olmasının uygun olması gerekeceği unutulmamalıdır.

Öte yandan, AİHM'in ceza yargılamalarındaki kanıt ve ispat konularına ilişkin içtihadına göre, bir delilin hukuka uygun olarak kullanılabilmesi için makul şüphenin ötesinde olması gerekmektedir. Makul şüphenin ötesinde olması ise delilin yeterince güçlü, açık ve diğer delillerle uyumlu çıkarımlardan veya aksi ispat edilmemiş fiili karinelerden oluşması anlamına gelmektedir[321]. Yine de AİHM, suçun işlendiğini gösteren makul şüphelerin varlığı konusunda, kendilerine sunulan delilleri değerlendirmek üzere daha iyi konumda olan yerel mahkemelerin değerlendirmesine daha çok önem vermektedir[322].

Fakat tüm bu süreç içerisinde, çıkan sonuca göre dava konusu olabilecek olaylarla ilgili olarak devletin lehine ya da aleyhine yönelik güçlü maddi karineler doğabilmektedir. Eğer bu karineler devlet aleyhine yönelik ortaya konulabiliyorsa ispat yükü ancak o zaman devlete düşmektedir. Örneğin *Gäfgen vs. Almanya* davasında AİHM, bir kimsenin sağlığı iyi durumdayken gözaltına alındığı halde, salıverildiği zaman yaralanmış olduğunun görülmesi halinde, bu yaraların nasıl oluştuğuna dair makul bir şekilde açıklama yapmanın devlete düştüğün ifade etmektedir[323]. Devletin bu noktada yapması gereken ise, kendisini haklı çıkarabilecek deliller getirmesi ve bu delillerin tatmin edici ve ikna edici olmasıdır[324].

Bununla birlikte AİHM, *Oleksandr Volkov/Ukrayna* davasında, usulle ilgili güvencelerin yeterli olup olmadığının belirlemede, ulusal hukukun disiplin soruşturmalarında herhangi

[319] Nada/İsviçre, Başvuru No: 10593/08, Büyük Daire Kararı, 12.09.2012, par. 181-185, Erişim Tarihi: 15 Nisan 2019.
[320] X/Finlandiya, Başvuru No: 34806/04, 03.07.2012, par 213, Erişim Tarihi: 25 Nisan 2019.
[321] Ramirez Sanchez/Fransa, Başvuru No: 59450/00, Büyük Daire Kararı, 04.07.2006, par. 117, Erişim Tarihi: 18 Nisan 2019.
[322] İrfan Güzel/Türkiye, Başvuru No: 35285/08, 07.02.2017, par. 87, Erişim Tarihi: 2 Nisan 2019; Klass ve Diğerleri/Almanya, Başvuru No: 5029/71, 06.09.1978, par. 49, Erişim Tarihi: 2 Nisan 2019.
[323] Gäfgen vs. Almanya, Başvuru No: 22978/05, Büyük Daire Kararı, 01.06.2010, par. 92, Erişim Tarihi: 3 Nisan 2019.
[324] Turan Çakır/Belçika, Başvuru No. 44256/06, 10.03.2009, par. 54, Erişim Tarihi: 4 Nisan 2019.

bir zaman sınırı olmaması sebebiyle disiplin makamlarının takdirini ucu açık hale getirmekte olduğunu ve bunun hukuki kesinlik ilkesini zedelediğini belirtmiştir[325].

Tezimiz kapsamında soruşturma evresinin KVK Kanunu'nun istisna kapsamında olması nedeniyle kişisel verilerin soruşturma evresinde kural olarak korunmamasının hukuka uygun olduğunu kanıtlama görevi AİHM'in önünde devlete düşmektedir. Belirtmek gerekir ki, devletin müdahalede ettiği somut olayların yorumlanmasında, daha çok Türk hukuk kuralları içesindeki işaret ettiğimiz istisna hükmü sebebiyle, yapısal problemlerin ortaya çıkması söz konusudur.

2. Avrupa kamu düzeni prensibi

AİHM vermiş olduğu bazı kararlarda, gerekçe olarak Avrupa'nın genel kamu düzeni kavramını kullanarak Avrupa Konseyine üye olan devletlerin oluşturmakta oldukları ortak kamu hukuku kurallarını ortaya koyacak şekilde bir asgari düzey tespiti yapmaktadır. Buna göre, AİHS'te yer alan bazı haklara yönelik müdahalelerde her ne kadar ülkelere takdir payı bırakılmış olsa da bu payın Avrupa'nın genel kamu hukuku sınırları içerisinde yer almasına özel önem verilmektedir.

Bu prensip doğrultusunda temel hak ve hürriyetlerin kullanılmasına yönelik belli bir standart oluşturmakta ve bu standart bazen hakka yönelik meşru müdahale sebebi teşkil edebilmekte bazen de AİHS'e uygun olarak yapılan müdahaleleri hukuka aykırı konuma getirebilmektedir. Hatta taraf devletlerde AİHS ile yeknesaklaşma amacıyla yapılmış olan kanuni düzenlemelerin önüne geçebilmekte, var olan kanunların AİHS kapsamında yer alan hakları yeterince koruyamaması sebebiyle hukuka aykırı olduğunu ifade edebilmektedir[326]. AİHM'in bu tavrında, AİHS'in izole edilmeden yaşayan bir belge olarak uluslararası hukukun genel ilkeleri ile uyumlu bir şekilde yorumlanmasını istemesi yatmaktadır[327].

Türkiye'nin AİHS'e taraf olması sebebiyle, Türk hukukundaki kişisel verilere ilişkin düzenlemelerin AİHS'in kişisel veriler ile ilgili kamu düzeni düzeyi çerçevesinde olması gerekmektedir. Aksi halde var olan kanunların bu açıdan AİHS ile bağdaşmayan bir

[325] Oleksandr Volkov/Ukrayna, Başvuru No: 21722/11, 09.01.2013, Erişim Tarihi: 7 Nisan 2019.
[326] Bayatyan/Ermenistan, Başvuru No: 23459/03, Büyük Daire Kararı, 07.07.2011, par. 9, Erişim Tarihi: 1 Nisan 2019.
[327] Nada/İsviçre, par. 169.

konumda olup insan hakları ihlallerine yol açacak bir seviyede olabileceğini belirtmek gerekir. Bu yüzden, AİHM'in kararlarının soruşturma evresinde kişisel verilerin korunması açısından Avrupa'nın genel kamu düzenini ortaya koyacak şekilde hangi seviyede olduğunun incelenmesi önemlidir. Soruşturma evresinin tamamen kapsam dışında bırakılmadığı görülürse, KVK Kanunu'ndaki istisna hükümlerinin soruşturma evresini tamamını kapsaması belki hâkimiyet tasarrufları açısından uygulanabilirliği savunulabilecek fakat bu durumun hukuka aykırı olduğu AİHM kararlarıyla gerekçelendirilmiş olacaktır.

Yaptığımız bu açıklamalardan sonra şimdi AİHM'in soruşturma evresinde kişisel verilerin işlenme şartlarına yönelik ilkelerini ortaya çıkarmaya ve bunları açıklamaya geçelim.

3. AİHM'in soruşturma evresinde kişisel verilerin işlenmesine yönelik ilkeleri

a) Genel olarak

Bu kısımda AİHM kararları ışığında AİHS'in ceza muhakemesine yönelik kişisel verilerin soruşturma evresinde hangi şartlar altında işlenebileceği ortaya konulmaya çalışılmaktadır. İlkelere geçmeden belirtmek gerekir ki devletin yalnızca negatif yükümlülükleri değil pozitif yükümlülükleri de incelenmektedir.

AİHM, kişisel verilerin korunmasının m. 8'de yer alan özel yaşam ve aile yaşamına saygı hakkının kullanılmasında büyük rol oynadığını, kişisel verilerin m. 8'de öngörülen güvencelere uygun olacak şekilde işlendiğine dair ulusal mevzuatta gerekli garantilerin yer almasının önemli olduğunu belirtmektedir[328]. Bu gerekli garantilerin iç hukukta düzenlenmesi, hakka yönelik müdahale ile korunan hak arasında makul bir dengenin olmasını gerektirecektir. AİHM'in de benimsemekte olduğu bu tavır, soruşturma evresinde AİHS'te yer alan bir hakka yönelik yapılacak bir müdahalenin hukuka uygun olabilmesi için orantılı olmasını ifade etmektedir.

Bu çerçevede her somut olayda makul dengenin kurulup kurulmadığını ayrı ayrı yorumlamakta olan AİHM'in yorumlarından çeşitli ilkeleri çıkarabilmek önem kazanmaktadır. Bu doğrultuda, hukuka uygun bir müdahalenin varlığından

[328] Gardel/Fransa, Başvuru No: 16428/05, 17.12.2009, par. 62, Erişim Tarihi: 5 Şubat 2019.

bahsedebilmek için hakka yönelik müdahalenin öncelikle meşru sebepler, kanunen düzenlenme ve demokratik toplum gerekliliğine uygun olma testlerinden sırasıyla geçmiş olması gerekmektedir. Aşağıda AİHM, yorumlarından çıkardığımız ilkeleri bu üç konu başlığı çerçevesinde ayrı ayrı değerlendirmekteyiz.

b) Meşru sebepler

Kişisel verilere yönelik AİHS m. 8 bağlamında bir işleme yapılmasında yapılan müdahalenin m. 8(2) göre meşru bir sebep teşkil edebilmesi için, ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması gerekmektedir. Burada sayılan sınırlama sebeplerinin Anayasa m. 20(3)'te sayılan sınırlama sebepleri üzerinde genişletici etkiye sahip olduğunu belirtmek gerekir.

AİHS m. 8(2)'de yer alan meşru sınırlama sebeplerinin varlığı halinde hakka yönelik sınırlama yapılması bu açıdan mümkündür. Sayılan bu sebepler doğrultusunda alınacak müdahale kararları da AİHS m. 8(2) anlamında uygun bir müdahale oluşturabilecektir[329]. Bu konu ile ilgili olarak *İrfan Güzel/Türkiye* davasında, AİHM, silah kaçakçılığı şüphelisi başvuranın telefon görüşmelerinin dinlemeye alınmasına izin veren ulusal mahkeme kararının, milli güvenlik ve kamu güvenliğinin korunması, düzenin korunması ve suç işlenmesinin önlenmesi gibi meşru amaçları orantılı olarak içerdiğini belirtmektedir[330].

AİHM, *Saint-Paul Luxembourg S.A./Luxembourg* davasında, bir gazetecinin yazdığı makalede üçüncü kişilerin kişisel verileri olan isimlerinin verilmesini, nispeten ciddi bir konunun bildirilmiş olmasından ötürü, suçun önlenmesi ve diğer kişilerin haklarının korunması hedeflerinin meşru sebep kıstasını yerine getirdiğini belirtmektedir[331]. Bu doğrultuda gerçek kimliğinin tespit edilmesini sağlamak ve olası bir suçun koşullarını açıklığa kavuşturmak için gazetecinin çalıştığı şirket binasına mahkemeden alınan arama ve el koyma kararı çerçevesinde zor kullanılarak girilmesini hukuka uygun bulunmuştur.

Öte yandan avukat-müvekkil gizliliği tarafından korunan elektronik mesajlardan oluşan elektronik verilerin aranması ve bu verilere el konulması ile ilgili *Vinci Construction ve*

[329] Klass ve Diğerleri/Almanya, par. 41; Dragojević/Hırvatistan, par. 78.
[330] İrfan Güzel/Türkiye, par. 77; Mahkemenin, telefon görüşmelerinin elde edilmesi konusunda genel esasları açıkladığı kararı için bakınız: Roman Zakharov/Rusya, par. 227-235.
[331] Saint-Paul Luxembourg S.A./Luxembourg, Başvuru No: 26419/10, 18.04.2013, Erişim Tarihi: 1 Mart 2019.

GTM Génie Civil et Services/Fransa davasında, delilleri elde etmedeki amacın hem ülkenin ekonomik refahı hem de düzenin korunması ve suç işlenmesinin önlenmesi menfaatleri açısından m. 8(2) kapsamında aranan meşru sebepleri yerine getirmekte olduğuna hükmetmiştir[332].

Özetle, AİHM kişisel verilerin ihlali iddiasıyla önüne gelen somut olaylarda, AİHS m. 8(2)'de sayılan meşru sebeplerin var olup olmadığı konusunda esnek bir tavır takınmaktadır. Eğer yerel hukukta kanuni düzenleme varsa kamu güvenliği, ulusal güvenlik ve düzenin korunması gibi taraf devletlerce ileri sürülecek meşru sebepleri devlet lehine geniş yorumlamaktadır. Mahkemenin vermiş olduğu ihlal kararlarının gerekçelerine bakıldığındaysa meşru sebebin yokluğundan değil demokratik toplum gerekliliklerinin sağlanmamasından ötürü verildiği dikkat çekmektedir.

c) Yasal düzenleme şartı

(1) Yasal düzenlemenin yokluğu

AİHS kapsamında yasal düzenleme şartının bir ayağı, temel hak ve hürriyetlere yönelik müdahalelerde dayanak olarak yasanın hükmünün var olmasıdır.

Hakka yönelik bir müdahalenin kanunla öngörülmüş olması, ulusal hukukun ve kamu gücünün AİHS m. 8 kapsamında yer alan haklara yönelik getirdiği keyfi sınırlamalara karşı koruma sağlamaktadır. Kişisel verilerle ilgili düzenlenmiş özel kanun olan KVK Kanunu'nda soruşturma evresindeki kişisel verilerin hiç korunmayacak şekilde düzenlenmiştir. Kişisel verilerin soruşturma evresinde işlenmesine yönelik güvenceler CMK ve ilgili diğer kanunlarda ise yer verildiği kadarıyladır. Buna karşılık, AİHM, yasal düzenleme eksikliğinin koruma tedbirleri üzerinde hem keyfi kararlara alınmasına hem de kamu denetiminin yokluğuna ve yetkinin kötüye kullanılma riskine yol açacağını belirmektedir[333]. Benzer gerekçeleri ileri sürdüğü *Elberte/Latvia* davasında AİHM, başvuranın yakını olan ölüden doku örneklerinin alınmasına yönelik idari usulün yasal

[332] Vinci Construction ve GTM Génie Civil et Services/Fransa, Başvuru No: 63629/10 60567/10, 02.04.2015, 11 Mart 2019.
[333] Copland/Birleşik Krallık, Başvuru No: 62617/00, 03.04.2007, par. 45, Erişim Tarihi: 4 Nisan 2019; Halford/Birleşik Krallık, Başvuru No: 20605/92, 25.06.1997, par. 49, 1 Mart 2019.

düzenlemeye sahip olmaması nedeniyle başvuranın kişisel verilerinin korunması hakkının ihlal edildiğine karar verilmiştir[334].

Yasal düzenlemenin yokluğunun ihlale yol açtığı *Oleksandr Volkov/Ukrayna* davasında AİHM, disiplin soruşturmasında verilecek yaptırım konusu fiillerin kanun ile düzenlenmiş sınırlarının olması gerektiğini ifade etmektedir. Bu davada mahkeme, meslekten ihraç edilen bir hâkimin usulünce yemin etmemesi sonucu meslekten atılması karşısında ilgili hukuku ve yapılan işlemi iki açıdan değerlendirmiştir. Önce yemin ihlali kavramının tutarlı bir yorumunu belirleyen hiçbir rehber ilke veya uygulamanın; sonra ise ihraç ile ilgili hükümlerin keyfi uygulanmasını önlemek için yeterli usul güvencelerinin var olup olmamasını araştırmıştır. Bu sebeple, ulusal hukukun disiplin suçları için uygun bir yaptırım çeşidi düzenlememiş oluşu ve bunların orantılılık ilkesine göre uygulanmasını sağlayacak kurallar geliştirmemiş olması nedeniyle bağımsız ve tarafsız denetim açısından güvenceler yeterli bulunmamıştır[335].

Dava konusunun kişisel verilerin saklanması ile ilgili olduğu *S. ve Marper/Birleşik Krallık* davasında AİHM, yasal düzenlemenin varlığını değerlendirirken sadece şeklen yasayla öngörülmenin ihlalin gerçekleşmemesi için yeterli olmadığını belirtmektedir. Buna göre mahkeme, kişisel bilgilerin soruşturma evresinde kullanılması ve muhafazası koşul ve yöntemleri konusunda ulusal hukuk hükümlerinin yeteri kadar detaylı olması gerektiğini ve bu tedbirlerin kapsamları ve uygulanmalarıyla ilgili açık ve detaylı kurallar belirleyen ve azami bazı şartlar koyan bir düzenlemenin varlığının çok önemli olduğunu belirtmektedir[336].

Öte yandan kişisel veriler ile ilgili tedbir kararlarına itiraz edilebilecek yasal düzenlemenin olmayışının da ihlal sebebi teşkil etmesi mümkündür. Bu açıdan, tedbire itiraz edilecek bir hukuk yolu mevcudiyetinin yokluğu, tedbire ilişkin olarak usulle ilgili güvencelerin ve etkin adli denetimin bulunmaması olarak anlaşılmaktadır[337].

---

[334] Elberte/Latvia, Başvuru No: 61243/08, 13.01.2015, 11 Mart 2019: Bu davada AİHM'in ısrarla altını çizdiği husus, kişisel verilere yönelik bir müdahalede hukuka uygun bir yasal düzenlemenin olmayışının idarenin yaptığı müdahalenin doğrudan idarenin geniş olan takdirine bırakılması sonucunu doğuracağını bunun da yasal düzenleme yokluğu sebebiyle hakka yönelik ihlal teşkil edeceğidir

[335] Oleksandr Volkov/Ukrayna, Başvuru No: 21722/11, 09.01.2013, 21 Mart 2019.

[336] S. ve Marper/Birleşik Krallık(Türkçe), Başvuru No: 30562/04 30566/04, Büyük Daire Kararı, 04.12.2008, Erişim Tarihi: 11 Nisan 2019.

[337] Brito Ferrinho Bexiga Villa-nova/Portekiz, Başvuru No: 69436/10, 01.12.2015, Erişim Tarihi: 13 Nisan 2019: Hâkim kararlarına itiraz yollarının incelendiği bu davada, avukat hakkında vergi kaçakçılığı

Tüm bu örneklerden yola çıkarak belirtmek gerekir ki Türk hukukunda soruşturma evresinde kişisel verilerin KVK Kanunu'nda getirilen güvencelerden istisna kapsamında olması sebebiyle yararlanamıyor olması problem teşkil etmektedir. Keza kişisel korunması ile ilgili her ne kadar yasal bir düzenlemeye sahip olsa da var olan istisna hükmü nedeniyle soruşturma evresinde uygulanacak bir yasal düzenleme bulunmamaktadır.

Bu durum, kişisel verilerin korunmasını hukuka aykırı olarak tamamıyla idarenin geniş takdirine, inisiyatifine ve insafına bırakmakta ve hukuk kuralları kişisel verilerin korunması hususunu kaderine terk etmektedir. Dolayısıyla Türk hukuku açısından, kamu görevlilerini kişilerin verilerini görüntülemekten ve işlemekten alıkoyacak yegâne unsur hukuka ve ahlaka adanmışlık olduğu görünmektedir[338].

KVK Kanunu kapsamında soruşturma evresinde hukuka aykırı olarak kişisel verilerin işlendiği ihbar edilecek özel bir şikâyet yahut itiraz makamı da bu bağlamda gerekli olmasına rağmen bulunmamaktadır. Dolayısıyla böyle bir durumda devlet, hakların korunmasındaki pozitif yükümlülüklerinden birisini yerine getirememektedir. Bu da aynı zamanda ortada yasal bir düzenleme olmadığı için kişilerin bu hakkı nasıl kullanacaklarını öngörememelerine yol açmaktadır.

Bizim görüşümüze göre söz konusu istisna hükümleri m. 8 bağlamında kişisel verilerin korunması hakkına yönelik yapısal bir aykırılık söz teşkil etmektedir. Türkiye'den AİHM önüne gidecek ilgili bir başvuruda m. 8(2)'de aranmakta olan yasal düzenleme şartına uymama nedeniyle ihlal kararının verilmesi ihtimali oldukça gerçekçi görünmektedir.

(2) Var olan yasal düzenlemelerin nitelikleri

AİHM, ulusal kanunların hukuk devletini oluşturan ilkelere uygun olacak şekilde yeterli koruma sağlayacak nitelikte olması gerektiğini belirtmektedir. Buna göre, kişisel verilerin

nedeniyle başlatılan soruşturmada sır tutma yükümlülüğü bağlamındaki gizliliğin kaldırılması için hâkime talepte bulunulmuştur. Fakat hem bu tedbir kararının alınması ve uygulanmasında şüpheli avukatın katılımı olmaksızın işlemlerin yürütülmesi hem de mesleki gizliliğin kaldırılması ile ilgili Avukatlar Birliğine danışılması gerektiği öngörülürken bu yollara somut olayda hiç başvurulmamıştır. Avukatın iç hukuk yargılamalarında başvuruları yasal şartlar sebebiyle sürekli kabul edilemez bulunarak reddedilmiştir.

[338] Akkaraca Köse, Melike (Tennis, Bradley T./Nuno Gomes de Andrade, Norberto/Stylianou, Konstantinos K./Anthopoulos, Haralambos/Tsiftsoglou, Anna/Akrivopoulou, Christina M./Güngör, Hasan Atilla/Contartese, Cristina/Suarez, Christopher A./Desierto, Diane A./Monteleone, Shara/Casarosa, Federica/Pina, Pedro/Ni Lonedain, Nora/Tzanou, Maria/Stan, Grigore-Octav/Pateraki, Anna): Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices, New York 2010, s. 72.

önleme ve adli amaçlarla kullanılmasında, kişisel verilerin korunması yolundaki ulusal hukukun sağladığı garantilere yönelik ihtiyaç özel hayatın gizliliğine ilişkin olması gereken güvencelere göre daha fazladır[339]. Dolayısıyla kanunların bu işleme faaliyetleri ile ilgili hükümlerinin hakkı ihlal etmeyecek düzeyde koruyucu niteliklere sahip olması gerekmektedir.

Kanunda olması gereken öngörülebilirlik koşulunun yerine getirilebilmesi gerekmektedir. Bu yönden kanunun, herkese karşı, hangi durumlarda ve hangi koşullarda kamu gücünün alabileceği tedbirlere yetkili olduğunu bildiren açık ifadeler içermesi gerekmektedir[340].

Ayrıca, var olan kanunların keyfiliğe mahal bırakmayacak nitelikte olması da şarttır. Bu doğrultuda, kanuna uygun alınmamış bir arama kararına yönelik itirazın hiçbir gerekçe gösterilmeden reddedilmesinin incelendiği *Gutsanovi/Bulgaristan* davasında, AİHM iki hususa dikkat çekerek m. 8'in ihlal edildiği kararını vermiştir.

Buna göre, birinci olarak soruşturmayı yapan kişilerin, başvuranların evinde bulmayı ve el koymayı düşündükleri soruşturmayla ilgili olan belge ve eşyalar belirlenmeden suçla ilgili olmayan kişisel verilerin de içerisinde bulunduğu özel eşya, belge ve bilgilerin toplanmasını hukuka aykırı bulmuştur. Çünkü tedbirin uygulanmasından önce suç ile irtibatlı ve orantılı bir müdahale oluşturacak bir hâkim kararı alınmamış ve söz konusu tedbirin geriye dönük incelemesi hukuka uygun olarak yerine getirilmemiştir.

İkinci olarak ise, ceza soruşturması beş ay önce başladığı için, soruşturmayı yürütenler, aramayı gerçekleştirmeden önce mahkeme kararı için başvurabilme imkânları olduğundan gecikmesinde sakınca bulunan bir halin varlığı iddiası muteber görülmemiştir. Dolayısıyla, usulde soruşturmayı yürüten yetkililerce gücün kötüye kullanılması riskini önlemeye yönelik yeterli güvencelerin alınmadığı sonucuna ulaşan AİHM, keyfiliğe karşı gerekli korumanın sağlanmadığı bu gibi olaylarda kişilerin haklarına yönelik müdahalenin yasayla öngörülmüş nitelikte olmayacağını belirtmektedir[341].

[339] S. ve Marper/Birleşik Krallık, par.103.
[340] Copland/Birleşik Krallık, par. 46; Halford/Birleşik Krallık, par. 49; Malone/Birleşik Krallık, par. 67.
[341] Gutsanovi/Bulgaristan, Başvuru No: 34529/10, 15.10.2013, Erişim Tarihi: 15 Mart 2019.

Sonuç olarak, eğer var olan kanunlar görevlilere keyfi davranmalarına imkân tanıyor ya da takdir yetkisini oldukça geniş tutuyorsa, o halde var olan düzenlemelerin niteliklerinin kanun ile öngörülme şartını sağlayacak düzeyde olduğunu iddia etmek pek mümkün değildir.

d) Demokratik toplumda gereklilik

(1) Genel olarak

Demokratik toplumda gereklilik incelemesinde, hakka yönelik getirilen sınırlamanın yasal olarak düzenlenmesi ya da meşru sebep doğrultusunda gerçekleştirilip gerçekleştirilmediğine bakılmamaktadır. Sadece bu sınırlamanın somut olayda korunan hak karşısında makul bir orantı teşkil edip etmediğini incelenmesi ifade etmektedir. Bu gereklilik hususunu hemen hemen önüne gelen her başvuruda değerlendirmeye alan AİHM, somut vakalardaki işlemlerin demokratik toplumdaki gerekliliği açısından orantılı bir müdahale olup olmadığını değerlendirmektedir. Somut olaylar karşısında verdiği değişik kararlarla da dinamik içtihadını oluşturmaktadır[342].

AİHM'in kişisel verilerin korunmasını içeren dava konularında verdiği kararlarından yola çıkarak bu noktayı çeşitli başlıklar altında toplamaya çalışarak aşağıda değerlendirmekteyiz.

(2) Takdir yetkisinin sınırlı olması gerekliliği

AİHM'in kişisel verilerin korunması hususunda demokratik toplum gereklilikleri üzerinde yorumlarında göze çarpan ilk önemli nokta, hakka yönelik müdahaledeki takdirin sınırlanması ölçütüdür. Her ne kadar devletlere sözleşmenin uygulanmasında takdir payı bırakmış olsa da incelemekte olduğu davalarda devletlerin bu takdir yetkisi sınırsız değildir. Davalar üzerinden gelişmekte olan takdir yetkisinin sınırlı olması ilkesinin bu özelliği yaşayan bir sözleşme olduğu belirtilen AİHS'in mantığına da uygundur. Takdir yetkisinin genişliği faaliyetin niteliğine ve sınırlamaların amacına bağlı olarak olaydan olaya değişebilmektedir. AİHM, özellikle bir şahsın varlığı veya kimliği

[342] Sher ve Diğerleri/Birleşik Krallık, Başvuru No: 5201/11, 20.10.2015, par. 172, Erişim Tarihi: 16 Mart 2019; Robathin/Avusturya, Başvuru No. 30457/06, 03.07.2012, par. 43, Erişim Tarihi: 17 Mart 2019.

ile ilgili önemli bir konu söz konusu olduğu zaman, devlete bırakılan takdir yetkisinin genel olarak sınırlı olacağını belirtmektedir[343].

Bir gözetim tedbirinin uygulanması hususundaki kanunun takdir yetkisinin kapsamını ve uygulanmasına ilişkin koşulların kişiye keyfîliğe karşı uygun bir koruma sağlayacak düzeyde yeterli açıklıkla tanımlanıyor olması gerekir[344]. Bu yüzden hakkı sınırlayan ulusal kanunların taşıması gereken şekli özelliklerin yanı sıra maddi özelliklerin varlığına dikkat edilmelidir. Aynı zamanda bu kanunlara dayanan idarenin takdir yetkisi sonucu yapılan müdahalenin uygun ve etkin güvencelerin varlığını içerisinde barındırması gerekir. Aksi halde demokratik düzeni tehdit eden sonuçların dahi ortaya çıkması söz konusu olabilecektir. Bu açıdan AİHM'e göre, davanın mahiyeti, alınacak tedbirlerin süresi, gerekçeleri, bu tedbirlere izin verecek, onları yerine getirecek ve kontrol edecek yetkili makamların, bu tedbirlere karşı iç hukukta öngörülen başvuru yolunun varlığı ve bunların hukuka uygun olmaları şarttır[345].

Öte yandan, kişisel verilerin gizliliği hakkına yönelik bir müdahalenin takdir payı içerisinde olduğunun iddia edilebilmesi için bunun demokratik bir toplumda gereklilik kıstasının yerine getirmesi şarttır. Bu doğrultuda özellikle hakka yönelik bir müdahalede aranan amaçlara daha az kısıtlayıcı araçlarla ulaşılmasının mümkün olup olmadığını tespit edilerek, izlenen meşru amaçlarla orantılı olmasını sağlaması gerekmektedir[346].

Dolayısıyla, soruşturma evresinde kişisel veriler ile ilgili alınacak tedbirlerde her zaman hakka daha az müdahale eden bir tedbir öncelikli olması gerekir. Aksi halde orantısız bir müdahalenin varlığı sebebiyle kararın alınmasına ilişkin idarenin takdirinin olduğu ileri sürülemeyecek, alınan karar ve elde edilen deliller hukuka aykırı olacaktır. Bu doğrultudaki *M.K./Fransa* davasında AİHM, şüpheli bir kişiden alınan parmak izinin kişi ceza almadığı halde 25 yıl boyunca depolanma sisteminde kalmasının kişilerin kişisel verilerin korunması hakkına demokratik bir toplumda gereklilikleri açısından orantısız

[343] Gardel/Fransa, par. 60–61.
[344] Cevat Özel/Türkiye, Başvuru No: 19602/06, 07.06.2016, par 31, 21 Mart 2019; Roman Zakharov/Rusya, par. 230.
[345] İrfan Güzel/Türkiye, par. 85.
[346] İrfan Güzel/Türkiye, par 86; Roman Zakharov/Rusya, par. 260.

bir müdahale anlamına geleceğini belirterek Devlet'in konuyla ilgili takdir hakkının sınırını aştığını ifade etmektedir[347].

PVSK'da parmak izi verilerinin depolanmasının 80 yıl olarak düzenlenmiş olması bu karara göre oldukça orantısız olduğundan açıkça hukuka aykırı olduğuna dikkat edilmelidir.

Son olarak, sağlık verilerinin toplanması işlemini değerlendirdiği *L.H. vs. Litvanya* davasında AİHM, meşru sebep olarak sağlık tedavisi veya sağlık hizmetlerinin sunulması ve yönetilmesi bakımından gerekliliğin ileri sürülmesine rağmen, uygulanabilir kanunların yetkili makamlara verilen takdir payının sınırını ve bu takdir payının nasıl kullanılacağını yeterince açık bir şekilde belirlemediği sebebiyle hakkın ihlal ediğini tespit etmiştir[348].

O halde sonuç olarak kamu görevlilerinin takdir yetkisini sınırlayan ve usule tabi tutan kanuni düzenlemeler var olmalıdır. Bu düzenlemeler çerçevesinde kişisel verilerin gizliliği hakkına daha az müdahale eden yöntem var ve yeterliyse ilk bu tedbir alınmalıdır. Alınan bu tedbirler gerekçelendirilmeli ve bu gerekçelere itiraz edebilecek iç hukuk yolları bulunmalıdır.

(3) Amaçla orantılı olma ilkesi

(a) Amaçla orantılı tedbir kararının seçilmesi ve alınması

Amaçla orantılı olma ilkesinin ilk görünümü olan uygun tedbirin seçilmesi ve kararın alınması, meşru amaç doğrultusunda kanundaki düzenlemeye dayanarak usulünce alınan tedbirin elde edilmesi umulan amaç doğrultusunda orantılı bir tedbir olması anlamına gelmektedir. Diğer bir deyişle, soruşturma evresinde alınan tedbirin suçu aydınlatma amacını yerine getirecek şekilde suç ile ilgili delilleri elde etmeye uygun bir tedbir olmasıdır. Suçun her türlü delille kanıtlanabilecek oluşunun soruşturma makamlarına geniş takdir yetkisi tanıdığı gerçeği karşısında, kişisel verilerin nasıl korunacağını ortaya koymak bu noktada önem kazanmaktadır.

Amaçla orantılı olma ilkesi, soruşturma evresinde delil elde etme yollarına başvurmadan önce bunların değerlendirilmesini ve daha elverişli delil elde etme yoluna başvurulması

[347] M.K./Fransa, Başvuru No: 19522/09, 18.04.2013, Erişim Tarihi: 13 Şubat 2019.
[348] L.H. vs. Litvanya, Başvuru No: 52019/07, 29.04.2014, Erişim Tarihi: 18 Mart 2019.

zorunluluğu getirmektedir. Başlatılan bir soruşturma kapsamında hedefe alınan kişinin gerçek ismini öğrenmek maksadını aşacak düzeyde alınan ölçüsüz koruma tedbiri ihlal kararı verilmesine sebebiyet vermiştir[349]. Mahkeme, *X/Finlandiya* davasında, bir kişinin rızası hilafına gerçekleştirilen tıbbi bir müdahalenin onun özel hayatına saygı hakkına ve özellikle de fiziksel bütünlük hakkına yönelik doğrudan bir müdahale oluşturduğunu kabul etmektedir[350]. Dolayısıyla, soruşturma evresinde şüpheli veya mağdur üzerinde delil elde etme amacıyla uygulanacak tedbirler orantılı olmalı, öncelikle alternatif yollara başvurulmalıdır.

AİHM, *Uzun/Almanya* davasında ise birkaç ay için uygulanmış ve başvurucunun haklarına sadece şüphelinin arabasında bulunduğu zamanlarda dokunmuş olan GPS sistemiyle yapılan takibi incelemiştir. Şüpheli ile ilgili somut olaydaki soruşturmanın çok ağır suçlarla ilgili olması sebebiyle özel hayata daha az müdahale eden başka soruşturma yollarının daha az etkili olacağını ifade eden AİHM, başvurucunun bir başka şüphelinin soruşturulması kapsamında GPS sistemiyle takip edilmiş olmasının demokratik bir toplumda gereklilikleri ile bağdaştığını düşünmektedir[351]. Buna göre, amaçla orantılı olan tedbiri seçmede tedbirin etkili olması unsuru önem kazanmaktadır.

Öte yandan sıkça ihlallerle karşılaşılmakta olduğundan arama kararlarının çeşidinin yanı sıra kapsamının genişliğinin de amaçla orantılı olması gerekmektedir. Bu hususta AİHM'e, demokratik toplum gereklilikleri ile örtüşen ölçülü bir arama kararının sahip olması gereken unsurlar aramanın bir hâkim tarafından verilen bir karara dayanması ve bu kararın da makul şüpheye dayanmasıdır. Ayrıca, kararın kapsamının makul bir şekilde sınırlı olması ve aramanın mesleki gizliliğe tabi belgelerin alınmasında bağımsız bir gözlemci eşliğinde yapılması diğer unsurları oluşturmaktadır[352]. Bunun dışında, kolluk

[349] Saint-Paul Luxembourg S.A./Luxembourg, Başvuru No: 26419/10, 18.04.2013, Erişim Tarihi: 5 Nisan 2019: Bu davada, kimliği belirlenemeyen şüpheli olduğu düşünülen kişinin ismindeki benzerlik nedeniyle buna dayanarak soruşturmayı yürüten hâkimin makaleyi yazan kişinin kimliğini teyit etmek üzere daha elverişli bir tedbire başvurmadan doğrudan kişinin çalıştığı gazete binasına yönelik arama ve el koyma kararı vermesi ve bu kararın uygulanması hakka yönelik müdahalenin gereksiz ve orantısız olmasına yol açmış olduğu belirtilmiştir.

[350] X/Finlandiya, Başvuru No: 34806/04, 03.07.2012, par. 212, Erişim Tarihi: 10 Nisan 2019.

[351] Uzun/Almanya, Başvuru No: 35623/05, 02.09.2010, 1 Mart 2019.

[352] Sher ve Diğerleri/Birleşik Krallık, par. 172; Robathin/Avusturya, par. 44; Wieser ve Bicos Beteiligungen GmbH/Avusturya, Başvuru No: 74336/01, 16.10.2007, par. 57, Erişim Tarihi: 1 Mayıs 2019.

kuvvetleri tarafından yapılacak bir aramanın dayanağı olan kararda el konulması mümkün olan nesne listesinin mümkün olduğunca belirli olması da gerekmektedir[353].

Görüldüğü üzere, soruşturma makamlarının alabileceği daha uygun yöntemlerin mevcut olup olmadığına bakılmaksızın kişinin haklarına yönelik daha ağır müdahaleler teşkil edecek tedbirlerin alınması işlemi hukuka aykırı olmasına yol açmaktadır. *Dragojević/Hırvatistan* davasında, doğrudan gizli teknik takip gibi ağır bir yönteme başvurulması AİHM tarafından keyfi bir uygulama olarak değerlendirilmiştir. Bunun gerekçesi ise, kamu görevlilerine verilen takdir yetkisinin kapsamı ve kullanım şekli bakımından ulusal düzenlemelerin hem yeterince açık olmaması gerçeği hem de olası suiistimal bakımından yeterli tedbirleri güvenceye alınmaması sebebiyle telefonun dinlenmesi için verilen emir ve yapılan denetim tedbirinin amaçla orantılı olmayışı sebebiyledir[354].

(b) Alınan tedbir kararının uygulanmasının amaçla orantılı olması

Amaçla orantılı olma ilkesinin ikinci görünümü, tedbir kararının alınmasında değil, alınan hukuka uygun tedbir kararına göre yapılacak uygulamada orantının olmasıdır. Soruşturma sürecinde kişisel verilere yönelik yasal zemine sahip olarak uygulanacak tedbir kararı suç ile ilişkilendirilecek şekilde özelleştirilmiş ve sınırlandırılmış olmalıdır. Dolayısıyla, iç hukuk kurallarının soruşturma sırasında toplanabilen kişisel verilerin kapsamını sınırlandırması gerekmektedir.

Bu konudaki *Copland/Birleşik Krallık* davasında AİHM, ulusal hukukta işverenlerin, çalışanlarının, telefon, elektronik haberleşme ve internet kullanımlarını denetleyebilecekleri durumları düzenleyen kuralların varlığının öneminin altını çizerek bununla ilgili bir araştırma yapmıştır. Akabinde, kanunun somut vakadaki koleji, yükseköğretim görevini yerine getirmek için gereken tüm tedbirleri alması amacıyla genişçe yetkilendirilmiş olmasını hukuk devleti açısından orantısız bulmamıştır[355].

Belirtmek gerekir ki AİHM'in bu görüşü hatalıdır. Çünkü, verilerin korunmasına yönelik dengeli bir müdahalenin varlığından bahsedebilmek için hakka müdahale eden tedbirlerde kişilere sağlanan güvencelerin varlığı esastır. Kanuni düzenlemelerde

[353] Sher ve Diğerleri/Birleşik Krallık, par. 174.
[354] Dragojević/Hırvatistan(Türkçe), Başvuru No: 68955/11, 15.01.2015, Erişim Tarihi: 18 Mart 2019.
[355] Copland/Birleşik Krallık, par. 47.

uygulanacak tedbirlerin düzenlenmiş olması şüphesiz uygulanacak tedbiri başlı başına hukuka uygun hale sokmaz. Bu tedbirlerin de orantılı olması gerekir.

Bu doğrultuda, AİHM daha sonraki bir kararında bu görüşünden vazgeçmiş ve dengeli bir müdahalenin varlığı için daha detaylı inceleme yapmıştır. *L.H. vs. Litvanya* davasında, soruşturma sürecinde başvuranın geriye dönük yedi yıllık döneme ait sağlık verilerinin, ayrım gözetilmeksizin ve bu verilerin belirleyici, alakalı ve soruşturmanın amacına uygun olup olmadığı değerlendirilmeksizin toplanmasını ölçüsüz bulmuştur[356].

Dolayısıyla görece yeni olan kararında AİHM artık kişisel verilere yönelik uygulanacak işleme faaliyetlerinin amaç doğrultusunda orantılı olmaları gerektiğine hükmetmiştir. AİHM'in bu yorumuna göre, kişisel verilerin korunması hakkına yönelik uygulanacak tedbirlerin amaçla orantılı olması kuraldır.

Öte yandan, terör faaliyetlerinde alınacak arama kararının uygulanmasında kapsamın geniş olması mümkündür. Örneğin, aramada el konulacaklar listesinin belirli olmaması da bu bağlamda kabul edilebilir görünmektedir. Bu konuyla ilgili *Sher ve Diğerleri/Birleşik Krallık* davasında AİHM, çok sayıda yaşamın risk altında olduğu geniş çaplı bir terör saldırısının iddiaları karşısında, saldırının amaçlanan mahiyeti veya hedeflerine ilişkin belirli bilgilerin mevcut olmaması, birden çok şüphelinin bulunması, kodlu dil kullanılması gibi unsurların varlığı ve durumun aciliyeti nedeniyle daha geniş koşullara tabi olan bir aramayı haklı kılabileceğini belirtmektedir[357].

Bizim görüşümüze AİHM'in buradaki yorumu devletlere geniş takdir yetkisi tanıyor olması nedeniyle hatalıdır. Kişisel verilerin işlenmesi ile ilgili hali hazırdaki düzenlemeler zaten kamu görevlilerine terör suçları söz konusu olduğunda geniş yetkiler vermektedir. Olması gereken, AİHM'in ideal hukuk doğrultusunda bu yetkileri sınırlayıcı ve hakkın özüne müdahale etmeyi engelleyici ilkeleri üreterek denge kurmasıdır. Aksi halde kamu görevlilerine verilecek geniş yetkiler kişisel verilerin terör bahane gösterilerek hukuka aykırı olarak kolayca işlenmesine yol açacaktır. Şüphesiz AİHM'in bu tavrı çeşitli suiistimallere yol açarak verilerin korunması hakkına yönelik müdahaleleri artıracaktır.

[356] L.H. vs. Litvanya, Başvuru No: 52019/07, 29.04.2014, 1 Mart 2019.
[357] Sher ve Diğerleri/Birleşik Krallık, par. 174.

(4) Kişisel verilerin işlenmesinde süre şartı olması ilkesi

Kişisel verilerin işlenmesinde süre şartının olması masumiyet karinesi gereği oldukça önemlidir. Süre sınırının olmaması ya da süre bittikten sonra hala verilerin tutuluyor olması veri sahibinin istemeyeceği verilerle ilişkilendirilmesine yol açmaktadır. Günümüzde verilerin işlenmesinin tüm süreç boyunca hukuka uygun olduğuna ilişkin yaygın bir kanı olması, suçlarla mücadelede veri bankalarının önemi doğrultusunda kişisel verilerin oldukça kolay işlenebilmesi ile alakalıdır.

Gerçekten de, kişisel verilerin suç işlenmesini önleme amacı karşısında elde edilmesi kişilerin haklarına yönelik hafif ve ulaşılmaya çalışılan meşru amaçla orantılı olabileceği iddia edilebilir. Çünkü çeşitli suçlardan elde edilen kişisel verilerin uzun süre muhafaza edilmesi yine suçun önlenmesi ve aydınlatılması ile ilgili amaçlar doğrultusundadır. Ayrıca muhafaza edilen bu veriler ile suç mahalliden alınacak DNA verilerinin karşılaştırılarak suç şüphelisinin yakalanması imkânının yokluğu durumunda, sadece elde kalan birbirinden bağımsız verilerin işlenen suçların aydınlatılması noktasında hiçbir işe yaramayacağı da ileri sürülebilir.

Dolayısıyla, çok geniş bir veri tabanına sahip olmanın ağır suçlara karşı mücadelede çok büyük avantajlar sağlayacağı önemli bir gerekçe olabilir. Fakat AİHM, aşağıda açıkladığımız sebeplerle bu görüşün karşısında durmakta, kişisel verilerin suçlarla mücadele anlamında da olsa süre sınırı konusunda oldukça geniş yetkilerle işlenmesini hakka yönelik orantısız bir müdahale olarak hukuka aykırı görmektedir.

Buna göre öncelikle, kişisel verilerin kaydedilmesinde bu kayıt işleminin amaca uygun olarak yapılması şarttır. Ayrıca, bu işlemin orantılı yani aşırı olmamasını ve teşhis imkânı veren verilerin kaydedilme amacına uygun olan süreyi aşmamasını sağlayacak şekilde iç hukuk kurallarının olması gerekmektedir[358]. AİHM'in bu konudaki yorumlarında kişisel verilerin korunmasına yönelik belli bir standart belirlemek amacıyla sıklıkla Avrupa Konseyi Verilerin Korunması Sözleşmesi'nin hükümlerine atıfta bulunması dikkat çekmektedir.

Bunun dışında, yine verilerin saklanmasında süre konusunun tartışıldığı *S. ve Marper/Birleşik Krallık* davasında, AİHM, şüpheliden alınan parmak izleriyle DNA

[358] Gardel/Fransa, par 63.

verilerinin, kişi hakkındaki ceza soruşturması takipsizlik veya beraatla sonuçlansa bile, zaman sınırlaması olmadan muhafaza edilemeyeceğini belirtmektedir[359]. Buradaki gerekçe ise, ilgili ve ailesi için büyük bir öneme sahip yegâne genetik bir kod olarak, hücre verilerindeki kişisel bilgilerin çokluğu ve niteliği ve DNA profilinin kişiler arasındaki mevcut akrabalık bağlarını ortaya çıkarmayı ve ilgilinin etnik kökeni hakkında bilgi edinmeyi sağlayan bir araç olmasıdır. Dolayısıyla, suç işlediklerinden şüphelenilen ancak henüz mahkûm olmamış olan kimselerin soruşturma evresi boyunca rızası olmadan böyle bir tedbirin olağan olmayan uzun sürelerle muhafazası, demokratik toplum gereklilikleri açısından kabul edilebilir görülmemiştir. Bu karara etki eden önemli faktör ise, Avrupa Konseyi'nin ilgili belgelerinden ve diğer sözleşmeci devletlerin yürürlükteki hukuk ve uygulamalarından çıkan anahtar ilkelere doğrultusunda, verilerin muhafazasının özellikle polis sektörü söz konusu olduğunda verilerin toplanmasının zaman sınırlı olması gerekmekte olmasıdır.

Elde edilen kişisel verilerin saklanmasında süre sınırının olmasına ilişkin *M.K./Fransa* davasında AİHM, adli yöntemlerle elde edilen kişisel veri içeren parmak izlerinin sadece belli bir süre ile depolanabileceğini aksi halde hukuka aykırı bir işlemenin vuku bulacağını belirtmektedir. Buna göre, veri toplama ve kayıt altında tutma usullerinin kişiler açısından öngörülebilir olacak şekilde düzenlenmesi, aksi halde belli bir usul ve süre sınırlaması olmaksızın verilerin saklanmasına izin vermenin hakkı yönelik uygulanacak tedbirin açıkça aşırı ve gereksiz olacağı görüşündedir[360]. Türk hukukunda da PVSK'da yer alan parmak izinin depolanmasına ilişkin hükümler 80 yıl gibi bir muhafaza süresi öngörmekte olduğundan içerisinde problemler barındırmaktadır.

Kanunen muhafaza etme süresi bittikten sonra verilerin silinmesi artık kişiler tarafından talep edilebilecek bir haktır. Bu konudaki *Gardel/Fransa* davasında AİHM, verilerin muhafazasında mahkûmiyetin sona ermesinden itibaren başlayan sürenin üst sınırının otuz sene olmasının sorun çıkartabilecek nitelikte görmüştür[361].

Belirtmek gerekir ki, verilerin silinmesi için veri sahiplerinin talep yükümlülüğü altına bırakılmaları doğru değildir. Çünkü hakka müdahale edenin devlet olduğu

[359] S. ve Marper/Birleşik Krallık(Türkçe), Başvuru No: 30562/04 30566/04, Büyük Daire Kararı, 04.12.2008, Erişim Tarihi: 19 Mart 2019.
[360] M.K./Fransa, Başvuru No: 19522/09, 18.04.2013, 21 Mart 2019.
[361] Gardel/Fransa, par. 68–70.

düşünüldüğünde müdahale sebebini ortadan kaldıran sürenin sona ermiş olması olgusu karşısında ilgili verilerin imha edilmesi yükümlülüğünün devlette olması gerekmektedir.

Keza AİHM, terör suçları ile ilgili başından soruşturma geçen bir kişinin cezalandırılmamasına rağmen isminin terör ile ilgili tutulan listelerde yer alması sebebiyle burada devletin kişiye yönelik mümkün olan en kısa sürede bildirim yapması gerektiğini belirtmektedir. Böylece kişinin isminin listede olması sebebiyle mahrum kaldığı haklarını kullanmada engelleri kaldırabilme imkânı oluşmuş olmaktadır[362].

Aycaguer/Fransa davasında ise AİHM, kişisel verilerin polisiye amaçlarla otomatik olarak işlenmesinde daha fazla korunma olması gerektiğini; iş hukuk kurallarının gerekli süre ve amaçlar dışında yasaya aykırı olarak verilerin işlenip depolanmasını engelleyici hukuk kuralları olmasının gerektiğini; ve aynı zamanda depolanmış verilerin silinmesinin talep edilebileceği uygun mekanizmaların kurulmasının devletin yükümlülüğünde olduğunu belirtmiştir[363].

Segerstedt-Wıberg and Others/İsveç davasında ise, birden fazla başvuranın durumlarını ayrı ayrı inceleyen AİHM, bir davacının taleplerini reddederken, diğerlerininkini kabul etmiştir. Buna göre, terör ilişkili eylemlerle doğrudan veya dolaylı olarak var olan bağlantıları sebebiyle polis kayıtlarında depolanmakta olan kişisel verilerinin silinmesi talep edilmiştir. Mahkeme, terörle mücadeleyi kişisel verilerin korunması hakkına müdahalede meşru sebep olarak kabul etmiştir. Verilerin depolanmaya devam ettiği 2002 yılına ait davada AİHM, 1990 yılındaki bomba tehditleri ile bağlantılı verilerinin ilgili ve yeterli olması sebebiyle verilerin depolanmasının suçun önlenmesi sebebiyle hukuka uygun olduğuna vermiştir.

Fakat, ikinci başvuranın 1967 yılında siyasi bir buluşmaya katılması bilgisinin depolanması için meşru sebep kıstasının karşılanmasında eski olması sebebiyle ilgili ve yeterli bulmamıştır. Bir diğer başvuranın 1969 yılında polise karşı şiddetli direnmesine ilişkin verilerinin depolanmasını da aynı sebeple kişisel verilerin korunması hakkına müdahalede orantısız bulmuştur.

[362] Nada/İsviçre, par. 91; Sayadi ve Vinck/Belçika(Birleşmiş Milletler İnsan Hakları Komitesi), Başvuru No: 1472/2006, 22.10.2008, par. 125, Erişim Tarihi: 7 Şubat 2019.
[363] Aycaguer/Fransa, Başvuru No: 8806/12, 22/06/2017, par. 38.

Diğer başvuranların sosyal ve hukuki düzeni şiddetle değiştirmeyi içerdiği iddia edilen bir programa sahip olan bir partiye üye oldukları bilgisinin, söz konusu partinin şiddetle olan alakasının kanıtlanamaması üzerine bu bilginin depolanmasının hakka yönelik orantısız olduğunu belirtmiştir[364].

Dolayısıyla verilerin imhası ve kişinin diğer hakları konusunda devlet, pozitif yükümlülüğünü kişinin talebi çerçevesinde değil kendiliğinden sağlama yükümlülüğü altında olmalıdır. Bu pozitif yükümlülük, soruşturma evresinde kişisel verilerin işlenmesinde süre sınırı belirleyen düzenlemeler yapmayı da beraberinde gerektirecektir. Türk hukukunda kişisel verilerin işlenme süreleri ile ilgili açık düzenlemelerin yokluğu sebebiyle kanun koyucunun etkili düzenleme yapması öncelikli önem arz etmektedir.

(5) Sır tutma yükümlülüğü açısından kişisel veriler korunması

(a) Meslek sırrı kapsamında kişisel verilerin korunması

Meslek sırrı kapsamındaki verileri avukat-müvekkil gizliliği üzerinden ele almaktayız. AİHM bu konuda verdiği kararlarda meslek sırrı kapsamında kişisel verilerin işlenmesine yönelik bazı özel güvencelerin olması gerektiğini belirtmektedir.

Bir avukat ile müvekkili arasındaki tüm iletişim verileri ve mesleki sır kapsamında yer alan tüm belgeler m. 8'in koruması altındadır. Buna göre, avukat-müvekkil arasında müvekkile ait kişisel bilgiler başta olmak üzere tüm verilerin avukatın sır tutma yükümlülüğü nedeniyle üçüncü kişilerle paylaşılması kural olarak yasaktır. AİHS açısından, bir avukat ile müvekkili arasındaki yazışmaya el konulmasının[365] ya da bir avukatın telefonunun dinlenmesinin[366] m. 8'in getirdiği güvencelere uygun olarak yapılması gerekmektedir.

Soruşturma evresinde alınan karar doğrultusunda sır tutma yükümlülüğü kaldırılabilmekte olduğundan kanuni güvencelerin verilmesi kaydıyla bu bilgilerin işlenmesi mümkün olabilmektedir. Fakat AİHM müvekkil-avukat gizliliğine yönelik yapılacak bir müdahaleyi zorlaştırmak isteyen bir bakış açısıyla değerlendirmektedir. Buna göre, *R.E./Birleşik Krallık* davasında, avukatların müvekkilleri ile yaptıkları

[364] Segerstedt-Wıberg and Others/İsveç, Başvuru No: 62332/00, par. 90, 91.
[365] Schönenberger ve Durmaz/İsviçre, Başvuru No: 11368/85, 20.06.1988, par. 28, Erişim Tarihi: 6 Şubat 2019.
[366] Kopp/İsviçre, Başvuru No: 23224/94, 25.03.1998, par. 74, Erişim Tarihi: 5 Şubat 2019.

görüşmelerin denetlenmesinin diğerlerine göre oldukça yüksek derecede ihlal teşkil ettiği kararını vermiştir. Gerekçe olarak ise, savunma hakkının avukatlar ve müvekkilleri arasındaki görüşmelere artırılmış koruma sağladığını ileri süren AİHM, iletişimin dinlenmesi kararlarının verilmesinde bu özel hususa önem verilmemesinin ihlale yol açabileceğini belirtmektedir[367].

Dolayısıyla, hakka yönelik müdahale kararının gerekçesinde yapılacak teknik tanımdan ziyade yapılan müdahalenin seviyesi belirleyici faktör olmaktadır. Ayrıca bu yargı, amacı ne olursa olsun avukat ile müvekkilleri arsındaki mesleki bağlamdaki kapsamı içerisinde yer alan tüm iletişim verileri için geçerlidir[368].

Yine bu doğrultudaki *Vinci Construction ve GTM Génie Civil et Services/Fransa* davasında, şirketlerin belirli çalışanlarının avukat-müvekkil gizliliği kapsamında olan belgeleri de dâhil olmak üzere çok sayıda elektronik belgesine soruşturma makamlarınca el konulmuştur. AİHM, soruşturmayla ilgilisi bulunmayan ve özellikle avukat-müvekkil gizliliği kapsamındaki belgelere el konulmasını önleyememiş olan devletin, veri sahiplerine yönelik itiraz etme ve yapılan işlemlerin hukuka uygun olduğuna ilişkin somut ve etkin bir inceleme yaptırma imkânı sunmak zorunda olduğu belirtmiştir[369].

Bunun dışında AİHM, m. 8 bağlamında mesleki sır kapsamında gizli tutulması gereken müvekkil ile ilgili bilgilerin suç içermesi halinde idari makamlara bildirim yapma yükümlülüğü getirilerek avukatların ikilemde bırakılması ile ilgili *Michaud/Fransa* davasında, sır tutma kuralına böyle bir istisna getirilemeyeceğini belirtmektedir. Buna göre, ülke hukuk kuralları arasındaki çatışma nedeniyle avukat ya müvekkilinin iletişiminin gizliliğine aykırı davranmak ya da kendisini barodan kaydının silinmesine kadar gidebilecek disiplin cezaları tehdidi altına girmektedir.

AİHM, ihbar yükümlülüğü getiren hükmün hukuka aykırı olduğunu, keza avukatın m. 8 kapsamında güvence altına alınan müvekkilleriyle profesyonel iletişimine saygı gösterilmesi hakkına yönelik sürekli bir müdahale oluşturduğunu belirtmektedir[370].

[367] R.E./Birleşik Krallık, Başvuru No: 62498/11, 27.10.2015, 15 Mart 2019.
[368] Niemietz/Almanya, Başvuru No: 13710/88, 16.12.1992, par. 32, 22 Mart 2019; Campbell/Birleşik Krallık, par. 46–48.
[369] Vinci Construction ve GTM Génie Civil et Services/Fransa, Başvuru No: 63629/10 60567/10, 02.04.2015, 1 Şubat 2019.
[370] Michaud/Fransa, par. 92.

Ayrıca, avukatların böyle bir yükümlülük altında bırakılmaları, aynı zamanda avukatların özel hayatlarına saygı haklarına da müdahale oluşturabilecektir çünkü özel hayat kavramı, mesleki veya ticari faaliyetleri de içine alacak şekilde geniş yorumlanmaktadır[371].

Öte yandan önüne gelen davalarda AİHM, şüpheli ile bilgi verilmemesinin yani sır tutma yükümlülüğünün mutlak olmadığını da ifade etmektedir[372]. O halde, sır tutma yükümlülüğü adaletin tecelli etmesi için oldukça önemli olsa bile dokunulmaz değildir.

Sır tutma yükümlülüğü kurumunun özellikle uyuşturucu ticaretinin veya demokrasi için büyük tehlike oluşturan uluslararası terörizm faaliyetlerinin finanse edilmesinin perdelenmesi amacıyla kullanılması şüphesi halinde bilgi ve belgelerin gizliliğine yönelik müdahalenin kapsamı geniş olması mümkündür[373].

Ayrıca, avukatların mesleki sır tutma yükümlülükleri çerçevesinde öğrendikleri bilgi ve belgelerin dışında, avukatın vekâlet yetkisi sayesinde müvekkilinin talimatları doğrultusunda suç teşkil eden faaliyetleri yapmasının sır tutma yükümlülüğü kapsamında kalması mümkün değildir.

Bu doğrultuda, önüne gelen somut olayda AİHM, kara para aklanmasına yönelik danışmalık yapan avukatın müvekkilleri ile birlikte suç işlemekte olduğu gerçeği karşısında müvekkile ait bilgilerin sır tutma yükümlülüğü kapsamında mütalaa edilemeyeceğini belirtmektedir[374].

AİHM'in bu görüşüne kısmen katılmadığımızı belirtmekte isteriz. Çünkü suç işlediği şüphesi somut olgularla ortaya koyulmamış olaylarda avukat-müvekkil gizliliğinin kaldırılmasına kapı aralanmaktadır.

---

[371] Niemietz/Almanya, par. 29; Michaud/Fransa, par. 91.
[372] Mor/Fransa, Başvuru No 28198/09, 15.12.2011, Erişim Tarihi: 3 Mart 2019.
[373] Grifhorst/Fransa, Başvuru No: 28336/02, 26.02.2009, par. 93, Erişim Tarihi: 2 Mart 2019.
[374] Michaud/Fransa, par 121, 127: Mahkemeye göre söz konusu bu işlemler avukat tarafından suç kapsamında olduğu bilinmek kaydıyla, mesleki faaliyetleri çerçevesinde müvekkilleri adına ve onların hesabına mali veya gayrimenkul işlemleri olabileceği gibi ticari fon alım satımı; müşteriye ait para, tahvil ve diğer aktifleri yönetmek; banka, tasarruf ya da tahvil hesabı açılması veya sigorta sözleşmesi düzenlenmesi; şirket kurulması için gereken katkının sağlanması; şirketlerin oluşturulması veya yönetimi ilgili olarak müvekkillerine yardım ettiklerinde söz konusu olmaktadır.

(b) Arama ve el koyma tedbirlerinin uygulandığı avukat bürolarında kişisel verilerin korunması

Avukat bürolarında yapılacak arama ve el koyma kararları ile ilgili olarak AİHM'in çeşitli kararlarından yola çıkarak belirtmek gerekir ki, bir avukatın ev veya bürosunda yapılan aramalar[375] ile el koymalar[376] AİHS m. 8 kapsamında ele alınmaktadır.

Avukat ve müvekkil arasındaki kişisel veri içeren haberleşmenin denetimi ve avukat bürolarında yapılacak arama ve el koyma kararlarında diğer kararlara göre özel hayatın ve kişisel verilerin korunmaya daha fazla önem atfedilmekte olduğunu yukarı belirtmiştik. Bu yüzden bu verilerin adi belgelere göre imtiyazlı bir statüye sahip olduğu ifade edilebilir.

Gerçekten de, iç hukukun bir avukatın bürosunun aranması olasılığını öngörmesinde, iç hukukta özel güvenceler yürürlüğe koyulduğu müddetçe bu AİHS'e engel oluşturmamaktadır[377]. Bu doğrultuda avukatın bürosundaki aramanın baro başkanı huzurunda gerçekleşmiş olması dikkate alınmakta ve bu şartın usulle ilgili özel bir güvence olduğu değerlendirilmektedir[378]. Hatta *Xavier Da Silveira/Fransa* davasında AİHM, özellikle konutunda arama yapılan bir avukatın bu güvenceden yararlanmaması nedeniyle m. 8'in ihlal edildiğine karar vermiştir[379].

AİHM'in bu tavrının gerekçesi ise öncelikle, avukatların meslek sırrına yönelik sınırı aşan bir müdahale riskinin gerçekleşmesi halinde adaletin iyi işlemesi üzerinde olumsuz etkileri olabileceğidir[380].

İkinci gerekçesi ise, sır tutma yükümlülüğünün avukat ile müvekkili arasındaki güven ilişkisinin temelini oluşturmasıdır[381].

---

[375] Roemen ve Schmit/Lüksemburg, Başvuru No 51772/99, 25.02.2003, Erişim Tarihi: 1 Nisan 2019; André ve Diğerleri/Fransa, Başvuru No: 18603/03, 24.07.2008, Erişim Tarihi: 12 Nisan 2019; Xavier Da Silveira/Fransa, Başvuru No: 43757/05, 21.01.2010, Erişim Tarihi: 13 Nisan 2019.
[376] Wieser ve Bicos Beteiligungen GmbH/Avusturya; Michaud/Fransa, par 117.
[377] André ve Diğerleri/Fransa, par. 42–43.
[378] Roemen ve Schmit/Lüksemburg, par. 69.
[379] Xavier Da Silveira/Fransa, par. 37, 43.
[380] Wieser ve Bicos Beteiligungen GmbH/Avusturya, par. 65–66; Niemietz/Almanya, par. 37; André ve Diğerleri/Fransa, par. 41.
[381] André ve Diğerleri/Fransa, par. 41; Xavier Da Silveira/Fransa, par. 36.

Üçüncü gerekçesi ise, avukatın savunmasını yüklendiği kişilere haberleşmelerinin gizli kalacağını garanti edemez pozisyona düşecek olmasının temel demokratik bir unsur olan mesleğini yerine getirememesine yol açacak olmasıdır[382].

Ayrıca avukatın görevini yapmasının engellenmesi söz konusu olduğundan, adil yargılanma hakkının ihlalinin gündeme gelmesi de bu durumda oldukça olasıdır.

(6) Bağımsız denetleyici organın varlığı şartı

Kişisel verilerin korunmasında demokratik toplum gerekliliklerini sağlayan bir diğer ölçüt, bağımsız denetleyici bir organın varlığı şartıdır.

AİHM'e göre, bağımsız denetimi sağlayacak bir kurumun sahip olması gereken belli ölçütler bulunmalıdır. Bunlardan bir tanesi idarenin faaliyetlerini yönlendirecek bir mekanizmanın devletin takdir payını genişletmeyecek şekilde kamunun çıkarları ile özel çıkarlar arasında adil bir denge kuracak bir yapıda olmasıdır[383].

Denetleyici bir organın varlığı ve bağımsız niteliği kişisel verilerin korunması hukukunun ulusal hukukça benimsenmesi ve geliştirilmesi hususunda dengeli bir müdahale sağlama yükümlülüğünün bir parçası olması sebebiyle önem taşımaktadır. Çünkü elektronik sistemlerin yaygınlaşması sonucunda kişisel verilerin korunması hukukunun teknolojinin gelişmesi ile teknik bir alana doğru gittikçe daha fazla uzmanlaşma ihtiyacı söz konusu olmaktadır. Bu teknik boyutu özümsemiş olarak yeterliliği sağlayabilecek kişilerin görevlendirileceği bir kurum, gelişen şartlara göre kişisel verilerin dengeli olarak nasıl korunacağı hususunda yol gösterici olabilecektir.

Ayrıca, soruşturma evresinde kişisel verilerin işlenmesi ile ilgili doğrudan rol alabilecek bir kurumun eksikliği de Türk ceza muhakemesi sürecinde hissedilmektedir. Keza KVK Kurulu idari yapıda Adalet Bakanlığı ilişkili bir kurumun kurulu olarak bağımsız bir yapı içerisinde değildir. Bu kurulun soruşturmalara müdahale etmesi yürütmenin bağımsız yargıya karışması anlamına geleceğinden fonksiyon gaspına söz konusu olabilecektir. Zaten gelinen noktada kişisel verilerin hukuka uygun ve güvenli olarak işlenebilmesi için

[382] Michaud/Fransa, par. 118.
[383] S. ve Marper/Birleşik Krallık(Türkçe), Başvuru No: 30562/04 30566/04, Büyük Daire Kararı, 04.12.2008, Erişim Tarihi: 13 Nisan 2019.

bağımsız bir denetçi organın muhakeme sürecine dâhil edilmesi önem arz etmekte olduğundan 2016/680/EU sayılı Direktif'te de bu kuruma yer verilmiştir.

C. Soruşturma Evresinde Verilerin İşlenmesine Hâkim Olan İlkeler ve İlgili Kişinin Hakları

1. Genel olarak

Kişisel verilerin işlenme yöntemlerine geçmeden önce, tezin bu kısmında buraya kadar belirttiğimiz verilerin soruşturma evresinde işlenmesine yönelik gerek AK gerekse AB belgeleri referanslı kaynaklarda belirginleşmiş olan ilkeleri ve ilgili kişinin haklarını ortaya koymaktayız.

Buna göre öncelikle, ceza hukukundaki hukuka uygunluk sebeplerinin verilerin işlenmesinde de geçerli olduğunu ifade etmek gerekir. Bu doğrultuda, ilgilinin rızası, üstün kamusal veya özel yarar, kanunun verdiği yetkinin kullanılması, amirin emri ve hakkın icrası soruşturma evresinde kişisel verilerin işlenmesine kaynaklık eden sebeplerdir.

Akabinde, bu sebeplerin çerçevesinde soruşturma evresinde kişisel verilerin işlenmesine, kişisel verilerin korunmasına ilişkin genel ilkelerin uygulanacağını düşünmekteyiz. Aksi halde hakkın özüne bir müdahale teşkil edileceğini yukarıda belirtmiştik. Ayrıca uygulanmaması için hiçbir hukuki ve teknik gerekçe de bulunmamaktadır. Bu doğrultuda zikredeceğimiz ilkelere uygun olarak elde edilmeyen bulguların Anayasa m. 37 uyarınca delil niteliğinde olmayacağını ifade etmek gerekir.

2. Soruşturma evresinde verilerin işlenmesine hâkim olması gereken ilkeler

a) Verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi

Kişisel verilerin soruşturma evresinde işlenmesine ilişkin uygulanacak olan genel ilkelerden birincisi, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesidir[384].

Bu ilkeye göre, soruşturma evresinde işlenen verilerin veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenmesi gerekmektedir. Kanunun gerekçesinde de

[384] KVK Kanunu m. 4(2)(a), GDPR m. 5(1)(a) ve 2016/680/EU sayılı Direktif m. 4(1)(a)'da yer almaktadır.

belirtildiği gibi, veriyi işleyenler, işlemede belirtilen amaç dışında, başka amaçlarla veri işlemeleri halinde, bu fiillerinden dolayı sorumlu olacaklardır[385].

Amacın meşru olması, veriyi işleyenin işlediği verilerin, işleme amacıyla bağlantılı ve gerekli olması anlamına gelmektedir. Bu ilkenin bir uzantısı GDPR m. 6(3)'te yer alan işleme faaliyetinin yasal güvenceye dayanıyor olmasıdır[386]. Bu şartın alternatifi ise GDPR m. 6(1)(a)'da düzenlenen kişinin kendi kişisel verilerin kullanımının kapsamını belirleme hususudur. Bu, veri sahibinin bir ya da daha fazla sayıda spesifik amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi anlamına gelmektedir.

Bu ilke doğrultusunda verilerin saklanması ve yok edilmesi usulü ile ilgili olarak Kişisel Verileri Koruma Kurumu tarafından 28.11.2017 tarihinde 30224 sayılı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik çıkarılmıştır. Her ne kadar yönetmeliğin daha çok özel sektör içindeki veri sorumlularına yönelik düzenlenmiş ve Yönetmelik m. 2'de bu yönetmelik hükümlerinin; KVK Kanunu m. 7 uyarınca veri sorumluları hakkında uygulanacağı belirtilmiş olsa da soruşturma süreci boyunca işlenmekte olan kişisel verilerin imhasına yönelik de uygulama alanı bulacağı düşünmekteyiz.

Keza bu bağlamda süreç içerisinde veriyi işleyen hâkim, savcı veya kolluk görevlilerinin veri sorumlusu gibi sorumlu tutulabileceğine ilişkin görüş ve gerekçelerimizi tezimizin birinci kısmında değerlendirmiştik. Aksi halde, Türk hukukunda soruşturma evresindeki kişisel verilerin saklanması ve yok edilmesi usulünü düzenleyen bir özel bir

---

[385] 6698 sayılı Kanun Gerekçesi, s. 8.

[386] Buna göre, işleme amacı yasal dayanakta belirlenmeli veya her işleme açısından kamu yararı hedefini karşılayan düzeyde gözetilen meşru amaçla orantılı olmalıdır. Öte yandan, yasal güvence bulunmaması halinde GDPR m. 6(4)'te zikredilen şartların sağlanması gerekir.
İşleme faaliyetinin hukuka uygunluğu ile ilgili hüküm GDPR m. 6(4)'te düzenlenmektedir:
"Kişisel verilerin toplanma amacı dışında bir amaca yönelik olarak yapılan işleme faaliyetinin veri sahibinin rızasına veya 23(1) maddesinde atıfta bulunulan hedeflerin güvence altına alınmasına yönelik olarak demokratik bir toplumda gerekli ve ölçülü bir tedbir teşkil eden bir Birlik veya üye devlet kanununa dayanmaması durumunda, kontrolör, başka bir amaca yönelik işleme faaliyetinin kişisel verilerin asıl toplanma amacına uygun olup olmadığını değerlendirmek üzere, bunun yanı sıra aşağıdaki hususları dikkate alır:
(a) kişisel verilerin toplanma amaçları ile planlanan diğer işleme amaçları arasındaki herhangi bir bağlantı;
(b) veri sahipleri ve kontrolör arasındaki ilişki başta olmak üzere kişisel verilerin toplandığı bağlam;
(c) 9. madde uyarınca özel kategorilerdeki kişisel verilerin işlenip işlenmediği veya 10. madde uyarınca mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenip işlenmediği başta olmak üzere kişisel verilerin mahiyeti;
(d) planlanan diğer işleme faaliyetlerinin veri sahiplerine olası yansımaları;
(e) şifreleme veya takma ad kullanımı da dâhil olmak üzere uygun güvencelerin bulunması."

düzenlemenin eksikliği söz konusu olacaktır. Bugün bu konuda kanunlarda sadece bazı tedbirlere ilişkin hakkı koruyucu özel hüküm düzenlemeleri bulunmaktadır.

Yönetmelik m. 5 uyarınca veri sorumluları siciline kayıt olmakla yükümlü olan veya olmayan veri sorumlularının, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlülüğü vardır. Bu bağlamda soruşturma evresinde kişisel verilerin işlenmesi talimatını veren kişi ve makamların da somut her vakada bu yükümlülük altında olmaları verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi açısından gerekli olduğunu düşünmekteyiz[387].

b) Amaca bağlılık-Amaçla sınırlanma ilkesi

İkinci ilke, amaca bağlılık veya diğer bir deyişle amaçla sınırlanma ilkesidir[388]. Bu ilkeye göre, kişisel veriler soruşturma evresinde açık ve meşru amaçlara yönelik olarak toplanmalıdır. Bu amaçlara uygun olmayan bir şekilde işlenmemelidir. Bu kuralın istisnası kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla işleme faaliyetleridir. Dolayısıyla, soruşturma evresinde yapılan işleme faaliyetleri amaçla bağlı ve sınırlı olmalıdır.

CMK m. 139'da bu ilkenin bir görünümü olarak gizli soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgilerin, ilgili ceza soruşturması dışında kullanılamayacağı ve suçla bağlantılı olmayan kişisel bilgiler derhâl yok edileceği düzenlenmiştir. Ayrıca

---

[387] Kişisel veri saklama ve imha politikasının kapsamı hükmü Yönetmelik m. 6'da düzenlenmektedir:
"(1) Kişisel veri saklama ve imha politikası asgari olarak;
a) Kişisel veri saklama ve imha politikasının hazırlanma amacına,
b) Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına,
c) Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarına,
ç) Kişisel verilerin saklanmasını ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaya,
d) Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere,
e) Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere,
f) Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına,
g) Saklama ve imha sürelerini gösteren tabloya,
ğ) Periyodik imha sürelerine,
h) Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe, ilişkin bilgileri kapsar."

[388] KVK Kanunu m. 4(2)(ç), GDPR m. 5(1)(b) ve 2016/680/EU sayılı Direktif m. 4(1)(b)'da yer almaktadır.

bu ilke, veriyi işleyenin veri işlemedeki amacının somut olayda özelleştirilmesini de kapsamaktadır[389].

Öte yandan, amaca bağlılık ve orantılılık ilkesinin bir sonucu olarak kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde soruşturma görevlileri tarafından uymaları gereken kurallar varlığı esastır. Bu açıdan, KVK Kanunu'ndaki genel ilkeler ile veri güvenliğine ilişkin alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket edilmesi zorunlu olmalıdır.

c) Daha az müdahale eden yöntemin uygulanması ilkesi

Üçüncü ilke, kişisel verilerin korunması hakkına daha az müdahale eden yöntemin uygulanmasıdır. Buna göre, kişisel verilerin soruşturma evresinde işlenmesinde, alınacak koruma tedbirleri ve delil değerlendirme yöntemlerinden kişisel verilerin korunması hakkına daha az müdahale eden tedbir seçilmelidir[390].

Soruşturma evresinde elde edilecek deliller arasında hiyerarşik bir ilişki olmadığından hangi tedbirin daha az müdahale teşkil edeceğinin hukuk kurallarınca belirtilmesi gerekmektedir. Aksi halde her somut olayda farklılaşan bir uygulama ortaya çıkacaktır. Bu noktada yüksek mahkeme kararları yol gösterici olacaktır. Bizim görüşümüze göre, diğer tedbirlere kıyasla vücut ve cinsel dokunulmazlığa yönelik alınacak tedbirlerin sıralamada daha sonraya bırakılması yerinde olacaktır.

d) Orantılılık (veri minimizasyonu) ilkesi

Dördüncü ilke, tedbir sonucu elde edilecek verilerin miktarı konusunda orantılılık (veri minimizasyonu) ilkesidir[391]. Bu ilkeye göre, soruşturma evresinde işlenen veriler, işlendikleri amaçlarla ilgili yeterli, yerinde ve gerekli olanla sınırlanmalıdır. Dolayısıyla, tedbir kapsamında kişisel verilerin gizliliği hakkına yönelik müdahalenin dengeli

[389] Von Grafenstein, Maximilian: The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation, Berlin 2018 s. 649.
[390] KVK Kanunu m. 4(2)(ç), GDPR m. 5(1)(c) ve 2016/680/EU sayılı Direktif m. 4(1)(c)'de yer almaktadır. Ayrıca bu konuda AİHM'in dikkat çekici yorumları için bakınız: İrfan Güzel/Türkiye, par 86.
[391] KVK Kanunu m. 4(2)(ç), GDPR m. 5(1)(c) ve 2016/680/EU sayılı Direktif m. 4(1)(c)'de yer almaktadır.

olmasını sağlama amacı güden bir ilkedir. Keza koruma tedbirlerin geçici olma özelliği bulunmaktadır[392]. Bağdaşan bu ilke ve özellik arasında doğal bir bağ bulunmaktadır.

Fakat uygulamada soruşturma evresinde kişisel verilerin işlenmesi üzerinde alınacak tedbirlerin yasal düzenlemelere sahip olmaması, uygulamada hangi tedbirin hangi miktarda alınacağını, ne kadarının depolanacağını ve ne kadarının işleneceğini belirsiz bırakmaktadır[393]. Söz konusu eksiklik kişisel verilerin hukuka aykırı olarak işlendiğini göstermektedir. Bu çerçevede işlenmekte ve depolanmakta verilerin ceza muhakemesinde de hukuka aykırı delil sınıfına girmesi gerekmektedir.

e) Verilerin doğruluğu ve güncelliği ilkesi

Beşinci ilke, soruşturma evresinde elde edilen veya işlenmekte olan verilerin doğruluğu ve güncelliğinin sağlanması ilkesidir[394]. Bu ilke soruşturma evresinde işlenmekte olan kişisel veriler üzerinde düzeltme, engelleme ve itiraz hakkının garanti altına alınmasını sağlamaktadır. İşlenen verilerin doğru olması, gereken şekilde ve güncel tutulması anlamına gelmekte olduğundan verilerin hukuka uygun depolanmasını destekleyen bir ilkedir.

İşlendikleri amaçlar göz önünde tutularak, bu ilke doğrultusunda doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmalı, kanuni düzenlemelerde ilgili makul tüm adımlar atılmalıdır. Bu doğrultuda, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin Yönetmelik m. 7'ye göre, genel ve hassas nitelikli kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi düzenlenmiştir.

Dolayısıyla, hakkındaki soruşturma kovuşturma aşamasına geçmeden sonlanan şüphelilerin verilerinin resen ya da şüphelinin talebi üzerinde imha edilmesi gerekmektedir. Bu, kişisel veriler üzerinde düzeltme hakkı ilkesinin bir sonucu olan verilerin doğruluğu ilkesinin gereğidir.

---

[392] Duran, Gökhan Yaşar: "Ceza Muhakemesinde Gözlem Altına Alınma (CMK m. 94)", Ceza Hukuku Dergisi, 13, 38, Ankara 2018, s. 98.
[393] Eijkman, Quirine: "Access to Justice for Communications Surveillance and Interception: Scrutinising Intelligence-Gathering Reform Legislation", Utrecht Law Review, 14, Utrecht 2018, s. 119.
[394] KVK Kanunu m. 4(2)(b), GDPR m. 5(1)(d) ve 2016/680/EU sayılı Direktif m. 4(1)(c)'de yer almaktadır.

f) Sınırlı süre saklanması ilkesi

Altıncı ilke, alınan tedbirler sonucu elde edilen kişisel verilerin sınırlı süre saklanması ilkesidir[395]. Bu ilkeye göre, soruşturma evresinde kişisel veriler yalnızca işlenme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan bir şekilde tutulmalıdır. Gerekçede belirtildiği üzere, bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilmelidir. Terör suçlarının önlenmesi gibi kamu yararı amacıyla elde edilen verilerin daha uzun süre saklanabilmesi bu ilke açısından mümkündür.

Depolanan kişisel verilerin dönemsel olarak sınırlı zaman süreçleri içerisinde gözden geçirilmesi ve silinmesinin hukuk kurallarında sağlanması gerekmektedir[396]. Bu doğrultuda örneğin, Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği m 19(1)(f) uyarınca trafik bilgilerini geçmişe dönük olmak üzere 2 yıl boyunca muhafaza edilmesi doktrinde kişisel verilerin gereğinden fazla sistemde tutulmasına yol açması sebebiyle hukuka aykırı bulunmaktadır[397].

g) Veri güvenliği (bütünlük ve gizlilik) ilkesi

Yedinci ilke, veri güvenliğini (bütünlük ve gizlilik) sağlamak için tedbir alınması ilkesidir[398]. Bu ilke, kişisel verilerin güvenliğini sağlamak amacıyla verilerin soruşturma evresinde yetkisiz veya yasa dışı işlemesine, kazara kaybına, imha edilmesine ve tahribe karşı gerekli teknik ve hukuki korunma tedbirlerinin alınmış olmasını ifade etmektedir. Bu bağlamda, veri korunması ile gizliliğin farklı anlamları ifade ettiği de unutulmamalıdır[399]. AB metinlerinde bu ilkeye yer verilmesine rağmen, KVK

[395] KVK Kanunu m. 4(2)(d), GDPR m. (5)(1)(e) ve 2016/680/EU sayılı Direktif m. (5)(1)(e)'de yer almaktadır.
[396] 2016/680/EU sayılı Direktif, m. 5.
[397] Dülger, 2019, s. 331.
[398] GDPR m. 5(1)(f) ve 2016/680/EU sayılı Direktif m. (5)(1)(f)'de yer almaktadır.
[399] Ruslijanto, Patricia Audrey (Saputra, Pramana Yoga/Wibowo, Dimas Wahyu/Cahyandari, Dewi/Silfiah, Rossa Ilma/Rohman, Fatkhur/Affandi, Luqman/Suryani, Dhebys/Handayani, Emi Puasa/Arifin, Zainal/Virdaus, Saivol/ Fadloli, Sri Nurkudri/Sulasari, Ayu/Hadiyantina, Shinta/Ramadhan, Nandaru/Mundzir, Hudriyah/Hadiwinata, Khrisna/ Muslim, Hairus Shobib/Fadloli, Abdul Chalim/Fadloli Nurkudri, Widaningsih/Santyaningtyas, Ayu Citra/Soeradji, Elvi/Batubulan, Kadek Suarjuna/Novitasari, Ane Fany/Suryadi, Satrio Binusa/Ellion, Handry Argatama/Setyowadi, Dewi/Sri Hudiarini, Rokiyah/Soraya, Joice): International Conference Call for Paper Personal Data Protection in Digital Era, Malang 2018, s. 127.

Kanunu'nda kanunun daha eski norm olan 95/46/EC sayılı Direktif'i temel alarak düzenlenmesi nedeniyle yer almayan bir ilkedir.

Veri güvenliğini ilkesini sağlaması amacıyla Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Yönetmelik m. 7'de, veri sorumlusu, kendi kurum veya kuruluşunda, KVK Kanunu hükümlerinin uygulanması ve verilerin silinme ve imhasına ilişkin normların uygulanmasını sağlamak amacıyla gerekli denetimleri yapmakla veya yaptırmakla yükümlü tutulmuştur. 2016/680/EU sayılı Direktif'in GDPR'la hemen hemen aynı ilkeleri içermekte olması sebebiyle bu ilke çerçevesinde hâkim, savcı ve kolluk amirlerinin gerekli denetimleri yapmalı ve bundan sorumluluğunun söz konusu olmalıdır.

Aynı şekilde, veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri başkasına açıklayamamakta ve işleme amacı dışında kullanamamaktadırlar. Bu yükümlülük görevden ayrılmalarından sonra da devam etmektedir. Bu da sır tutma yükümlülüğü ilkesinden dolayıdır. Buna göre, soruşturma evresinde şüpheli ya da bir başkası hakkında kişisel verilere vakıf olan görevlilerin görevlerinden sonra da devam edecek olan sır saklama yükümlülükleri bulunmakta ve vakıf olunan bilgiler işleme amacı dışında kullanma imkânı olmamaktadır.

Öte yandan, bu ilke doğrultusunda Anayasa Mahkemesi, yürütülen soruşturma dosyasında yer alan verilerin mağdurların kişisel verisi olması durumunda isteyen her şüpheli ve avukatına verilmemesini savunma hakkının kısıtlamayacağını belirtmiştir[400]. Dolayısıyla bu ilke sadece soruşturmayı yürüten görevliler için değil üçüncü kişileri de kendisine tabi duruma getirmektedir. Bunun dışında verilerin bütünlüğü ve gizliliği ilkesini destekleyici olarak diğer hukuki metinlerinde bulunmayan ve 2016/680/EU sayılı Direktif'te de ilk defa getirilen veri ayrımı ilkesi bulunmaktadır[401].

Bu ilkeye göre, soruşturmada verileri işlenen şüpheli, mağdur, tanık gibi farklı veri öznelerinin verileri birbirinden ayrı kategoriler içerisinde tutulması gizliliği sağlanması adına önemlidir. KVK Kanunu'nda yer almayan bu iki ilkeye de, soruşturma evresinde

[400] Başvuru No: 2014/14061, Karar Tarihi: 08.04.2015, Erişim Tarihi: 1 Nisan 2019.
[401] 2016/680/EU sayılı Direktif, m. 6.

işlenen kişisel verilerin etkin bir biçimde korunabilmesi ve AB müktesebatıyla uyum sağlanması için Türk hukukunda yer verilmesinin altını çizmek gerekmektedir.

h) Hesap verilebilirlik ilkesi

Sekizinci ilke ise, veri işleyicileri ve kontrolörlerinin işlemekte oldukları veriler üzerinde hesap verebilirliği ilkesidir[402]. Bu ilkeye göre, kişisel verileri işlenmesinden sorumlu olanlar, kişisel verilerin işlenmesine ilişkin ilkelere uygun davranmakla ve istendiğinde bunlara uygun davrandıklarını göstermekle yükümlüdürler.

KVK Kanunu'nun güncel ihtiyaçlara cevap veren bir yapıda olmaması sebebiyle bu ilke açısından da gerekli hükümlerin kanuna eklenmesi gerekli ve önemlidir. Aksi halde soruşturma evresinde işlenmekte olan kişisel verilerin güvence altına alındığı düşüncesinin dayanaklarından biri eksik kalacaktır.

3. Kişisel verilerin soruşturma evresinde işlenmesine ilişkin ilgili kişinin hakları

a) Genel olarak

Kişisel verilerin soruşturma evresinde işlenmesi ile ilgili ilkeler kısmının son bölümünde, verileri işlenen ilgili kişilerin sahip olduğu haklara yer vermenin önemli olduğunu düşünmekteyiz. Türk hukukunun kişisel verilerin korunması bağlamında meri kurallar ve bunun pratiğe dökülmüş hali açısından, alması ve geliştirmesi gereken belli bir mesafe olsa da hali hazırda düzenlenen haklar çerçevesinde gelinen mesafeyi göstermek gerekmektedir.

Dolayısıyla bu bölümde çoğunlukla adil yargılanma hakkından kaynaklanmak üzere, hem AİHM kararlarında hem de CMK'da soruşturmada yer alan kişilerin kişisel veriler ile ilgili haklarının düzenlendiği hükümlere yer vermekteyiz.

Bu noktada ifade etmek gerekir ki, soruşturma evresinde yer alan şüpheli/sanık, mağdur ve kişisel verisi işlenen diğer kişiler açısından soruşturma işlemleri ile ilgili olarak farklı hükümler bulunmaktadır. Fakat biz ilgili kişinin hakları kısmı başta olmak üzere tezimizin genel olarak tüm kapsamında, bu kişilerin hepsini ilgili kişi başlığı altında toplamaktayız. Çünkü kişisel verilerin korunmasında temel alınan husus, verinin niteliğidir. Yani koruma kişinin niteliğine göre değil, verinin özelliğine göredir. Bu

[402] GDPR m. 5(2) ve 2016/680/EU sayılı Direktif m. 4(4)'te yer almaktadır.

açıdan, verisi işlenen bir kişi varsa koruma kişinin niteliğinden önce verinin işlenmesi sebebiyle gündeme gelecektir. Bu yüzden, TCK m. 135'te kişisel verilerin kaydedilmesi suçunda verilerin işlenmesinde ilgili kişinin değil verinin niteliği nitelikli hal olarak düzenlenmiştir. Verinin hukuka aykırı olarak işlenmesine yönelik yaptırım içeren diğer meri hükümlerde de kişinin niteliğine göre bir ayırıma gidilmemektedir. Ayrıca kişisel verilerin korunmasına ilişkin tüm belgelerde de verisi işlenen kişiyi ifade eden olarak "ilgili kişi" tanımlar içerisinde yer almaktadır.

Bu gerekçeler çerçevesinde, hem bu kısım hem de tez genelinde esas yönelim olarak şüpheli/sanık, mağdur, tanık, kolluk görevlileri vs. hakkında ilgili kişi üst başlığını kullanmaktayız. Soruşturma evresinde kişinin niteliğinin ayırt edilmesi gerekiyorsa, bu kişilerden örneğin mağdurun daha fazla korunmasının gerekli olduğunu düşündüğümüz yerlerde bu yönde bir ayrıma da dikkat ettiğimizi de belirtmek isteriz.

İlgili kişinin haklarını düzenlediğimiz bu kısım içerisinde, haberdar edilme hakkı, susma hakkı, unutulma hakkı ve etkili bir soruşturma yapılmamasına itiraz hakkı yer almaktadır. Bu hakların dışında, bir kişinin genel hükümler çerçevesinde veri sahibine bildirim, veriye erişim, doğrulama ve sınırlama hakkı, verilerin silinmesi, sınırlanması ve doğrulanması hakkı, hassas verilerin özel olarak korunmasını talep etme hakkı, denetim makamına şikâyette bulunma hakkı ve hukuka aykırı işlemeden doğan tazminat hakkı gibi, asıl haklara bağlı hakların varlığını da zikretmek gerekir.

Belirtilen bu hakların kişilere kanuni güvence sağlayacak şekilde yürürlükte olmaları gerekmektedir. Güvence sağlayacak kanunların ise, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Aksi halde Anayasa m. 20(3)'te yer verilen hak güvenceden bağımsız bir hale getirilmiş olacaktır[403].

b) Haberdar edilme hakkı

Soruşturma evresinde kişisel verilerin korunması yönünden haberdar edilme hakkının görünümü, veri sahibine verilerin işlenmekte olduğu hakkında bildirim yapılmasını ifade etmektedir. KVK Kanunu m. 10'da veri sorumlusunun aydınlatma yükümlülüğü olarak yer almaktadır[404].

[403] E. 2014/149, K. 2014/151, KT: 02.10.2014, RG. 29223, 01.01.2015, Erişim Tarihi: 11 Nisan 2019.
[404] Veri sorumlusunun aydınlatma yükümlülüğü KVK Kanunu m. 10'da düzenlenmektedir:

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Yönetmelik m. 7'de de, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve KVK Kurul'una bildirmekle yükümlü tutulmuştur.

GDPR m. 32'de düzenlenen işleme güvenliği uyarınca, bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesi kesinse gereksiz gecikmeye mahal vermeden denetim makamına[405] ve veri sahibine bildirmesi gerekmektedir[406]. 4982 sayılı Kanun m. 21(2)'ye

---

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

[405] Kişisel veri ihlalinin denetim makamına bildirilmesi hükmü GDPR m. 33'te düzenlenmektedir:
"1. Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması haricinde, kontrolör, gereksiz gecikmeye mahal vermeden ve uygun olması halinde, ihlalden haberdar olduktan itibaren en geç 72 saat içerisinde, kişisel veri ihlalini 55. madde uyarınca yetkin denetim makamına bildirir.
Denetim makamına yönelik bildirimin 72 saat içerisinde yapılmadığı hallerde, bu bildirimle birlikte gecikme sebeplerine de yer verilir.
2. İşleyici, bir kişisel veri ihlalinden haberdar olduktan sonra, herhangi bir gecikmeye mahal vermeden, kontrolöre bildirimde bulunur.
3. 1. paragrafta atıfta bulunulan bildirimde en azından:
(a) uygun olduğu hallerde, ilgili veri sahibi kategorileri ve yaklaşık sayısı ile ilgili kişisel veri kaydı kategorileri ve yaklaşık sayısı da dâhil olmak üzere kişisel veri ihlalinin mahiyeti açıklanır;
(b) veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgileri iletilir;
(c) kişisel veri ihlalinin olası sonuçları açıklanır;
(d) uygun olduğu hallerde, kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dahil olmak üzere kişisel veri ihlalinin ele alınması için kontrolör tarafından alınan veya alınması önerilen tedbirler açıklanır.
4. Bilgilerin aynı zamanda sağlanmasının mümkün olmadığı hallerde ve ölçüde, bilgiler gereksiz herhangi bir ek gecikmeye mahal verilmeksizin aşamalı olarak sağlanabilir.
5. Kontrolör kişisel veri ihlallerini kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirir. Bu belgelendirme denetim makamının bu maddeye uyumluluğu doğrulamasını sağlar."

[406] Kişisel veri ihlalinin veri sahibine iletilmesi hükmü GDPR m. 34'te düzenlenmektedir:
"1. Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, kontrolör kişisel veri ihlalini gereksiz bir gecikmeye mahal vermeden veri sahibine iletir.
2. Bu maddenin 1. paragrafında atıfta bulunulan veri sahibine ilişkin bildirimde kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanır ve en azından 33(3) maddesinin (b), (c) ve (d) bentlerinde atıfta bulunulan bilgiler ve tedbirlere yer verilir.
3. Aşağıdaki koşulların herhangi birinin yerine getirilmesi durumunda, 1. paragrafta atıfta bulunulan veri sahibine ilişkin bildirim gerekmez:
(a) kontrolörün uygun teknik ve düzenlemeye ilişkin koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirler başta olmak üzere bu tedbirlerin kişisel veri ihlalinden etkilenen kişisel verilere uygulanmış olması;

göre ise, kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgelerin, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabileceği ifade edilmektedir.

Bu maddede sayılan haber verilme şartı, haberdar edilme hakkının bir görünümüdür. Bu madde hükmünün soruşturma evresinde işlenmekte olan kişisel verilerin korunmasına yönelik genişletici olarak uygulanmasında bir engel bulunmamaktadır.

GDPR m. 12 ve 2016/680/EU sayılı Direktif m. 12'ye göre bu bildirim, öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak veri sahibine yapılmalıdır. GDPR m. 13 uyarınca bildirimin kapsamı ise, veriyi işleyenin kim olduğu, planlanan işlenme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı; gözetilen meşru menfaatler ve kişisel verilerin alıcıları veya alıcı kategorilerinden ibarettir[407].

Öte yandan bu noktada, haberdar edilme hakkı gibi haber alma hakkına da değinmek gerekir. Anayasa m. 74'e ve 4982 sayılı Bilgi Edinme Hakkın Kanunu'na göre herkes bilgi edinme hakkına sahiptir. Bu sebeple, idari teşkilat içindeki tüm kurum ve kuruluşlar, kural olarak her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak zorundadırlar(m. 5). Ayrıca, bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idarî ve teknik tedbirleri almakla yükümlüdürler. 4982 sayılı Kanun'un uygulanmayacağı istisna hükümleri de bulunmaktadır. Bunlardan adli soruşturmaya ilişkin istisnaya göre, açıklanması veya zamanından önce açıklanması hâlinde suçların soruşturulması tehlikeye düşürecek ve yargılama görevinin gereğince yerine getirilmesini engelleyecek nitelikteki bilgi veya belgeler bu kanun kapsamı dışında tutulmaktadır[408].

(b) kontrolörün 1. paragrafta atıfta bulunulan veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alması;
(c) bildirimin ölçüsüz bir çaba gerektirecek olması. Bu durumda, bunun yerine, veri sahiplerinin aynı etkililikle bilgilendirildiği kamuya yönelik bir bildirim veya benzeri bir tedbir uygulanır.
4. Kontrolörün hâlihazırda kişisel veri ihlalini veri sahibine iletmemiş olması durumunda, denetim makamı, kişisel veri ihlalinin yüksek bir riske sebebiyet verme olasılığını değerlendirdikten sonra, kontrolörün bu bildirimi yapmasını şart koşabilir veya 3. paragrafta atıfta bulunulan koşullardan herhangi birinin yerine getirilmesine karar verebilir."

[407] Bilgiler ve kişisel verilere erişim ile ilgili olarak, GDPR Madde 13'te Veri sahibinden kişisel verilerin toplandığı hallerde sağlanacak bilgiler ve GDPR Madde 14'te Kişisel verilerin veri sahibinden alınmadığı hallerde sağlanacak bilgiler düzenlenmektedir.

[408] Adlî soruşturma ve kovuşturmaya ilişkin bilgi veya belgeler hükmü BEHK m. 20'de düzenlenmektedir: *"Açıklanması veya zamanından önce açıklanması hâlinde;*
a) Suç işlenmesine yol açacak,

Elbette ki, gizli yürütülen bir soruşturma kapsamında kişiye kişisel verilerinin işlendiğinin bildirilmesi pek mantıklı görünmemektedir. Fakat bu şekilde alınacak tedbirlerin yer aldığı adli sürecin AİHM'e göre etkin olması yani tedbire ilişkin yetkinin kötüye kullanmaya karşı etkin güvencelerin varlığını gerektirmektedir[409]. Zira istihbarat toplama gibi gizli yürütülen faaliyetlerde bildirimin yapılmaması işin gereğidir. Aksi halde faaliyet sürecinin, alanının ve süreç içerisinde rol alan görevlilerin açığa çıkmasına rol açabileceği sebebiyle zarar verebilecektir. Fakat soruşturma sona erdikten sonra bu bildirimin yapılmasının önünde bir engel bulunmamaktadır.

Bu doğrultuda, veri sahiplerine yönelik, en geç gözetim tedbirleri kaldırıldıktan sonra olmak üzere kısıtlamanın amacına zarar vermeyecek bir anda haberdar etmek gerekmektedir[410]. Ayrıca, haberdar edilme hakkının özel hukuk referanslı amaçlarla düzenlenmiş olduğu argümanı da ileri sürülebilir. Fakat soruşturmada bu hakkın hiç uygulanmamasına yol açan bu argüman da kısırdır çünkü kişisel verilerin korunması hakkının insan hakları kapsamında korunuyor olması sebebiyle esas olan hakkı belirtip sınırlarını çizmektir. Bu yüzden hali hazırdaki kanunda haberdar edilme hakkının soruşturma sürecinde uygulama alanı hiç bulmayacak şekilde düzenlenmesinin yerine orantılı bir düzenlemenin yapılması gerekmektedir.

Soruşturma evresinde işlenmekte olan kişisel veriler ile ilgili bildirimleri kişisel verileri işleyen makamın yapması uygun düşer. 2016/680/EU sayılı Direktif'te kontrolör hakkında düzenlenen hükümlere benzer olarak, veri işleyen makamın kişisel verilerin elde edildiği anda adil ve şeffaf bir işleme sağlanması için kişisel verilerin saklanacağı sürenin bildirilmesi öngörülmektedir.

Ayrıca işleme faaliyetinin kısıtlanmasını talep etme ya da işleme faaliyetine itiraz etme hakkı başta olmak üzere ilgili kişinin sahip olduğu haklara ilişkin bilgiler bildirimde yer almalıdır. Eğer kişisel veri, veri sahibinden elde edilmemişse, verinin işlenme olduğu

---

b) Suçların önlenmesi ve soruşturulması ya da suçluların kanunî yollarla yakalanıp kovuşturulmasını tehlikeye düşürecek,
c) Yargılama görevinin gereğince yerine getirilmesini engelleyecek,
d) Hakkında dava açılmış bir kişinin adil yargılanma hakkını ihlâl edecek,
Nitelikteki bilgi veya belgeler, bu Kanun kapsamı dışındadır.
4.4.1929 tarihli ve 1412 sayılı Ceza Muhakemeleri Usulü Kanunu, 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu, 6.1.1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu ve diğer özel kanun hükümleri saklıdır."

[409] Cevat Özel/Türkiye, par. 33; Klass ve Diğerleri/Almanya, par. 57; Roman Zakharov/Rusya, par. 234.

[410] Cevat Özel/Türkiye, par. 34; Roman Zakharov/Rusya, par. 287.

bilgisi veri sahibine en geç verilerin kaydedilmesi anında ya da eğer verilerin işlenmesi önceden planlanmışsa en geç işleme anına kadar yapılmalıdır[411].

Sonuç olarak, haberdar edilme hakkı, kanunun istisnaları arasında sayılmaması sebebiyle soruşturma evresinde uygulama alanı bulacaktır. Fakat bildirim yükümlülüğünün soruşturma evresini de kapsayacak şekilde yani ilgili kişinin kişisel verileri işlendiği takdirde bunun hassaten bildirilmesini öngören şekilde düzenlenmesi hakkın güvencelerini sağlamak adına önemlidir.

Keza AİHM de verinin hassas olup olmadığına bakılmaksızın kişisel veri niteliği taşıyan her veri ile ilgili yapılacak işleme faaliyetinin kişiye kesinlikle bildirilmesinin gerekli olduğunu belirtmektedir[412].

Doktrinde, CMK m. 135 uyarınca iletişimi denetlenen kişilerin işlemleri sonrasında geri bildirim yapılmalı ve bu bildirim hem fiilen dinlenen şahsa hem de hat sahiplerine yönelik olması savunulmaktadır[413].

Dolayısıyla, kişinin soruşturma evresinde kişisel verilerinin işlenmekte olduğunu öğrenmesi kişisel verilerin korunması hakkının bir görünümüdür. Bu doğrultuda, kişisel verilerin soruşturma evresinde işlenmesi halinde başta veri öznesi olmak üzere verinin elde edilmesi sırasında dolaylı olarak verilerine temas edilen kişilere de bildirim yapılması gerekir. Aksi düzenlemelerin varlığı ya da var olan güncel durum gibi düzenlemenin hiç olmayışı kişilerin hakkını tatbik edememesine yol açacağından, yapılacak orantılı düzenlemelerle hukuka aykırı bu durumun bir an önce giderilmesi taraftarıyız.

c) Susma hakkı

Susma hakkı kişinin kendisine yöneltilen soruları cevaplamayarak sessiz kalmasıdır. Ceza hukukunda susmak ikrar etme anlamına gelmez. Bu açıdan aleyhe delil vermeme ilkesi çerçevesinde ifade sırasında hangi konuda olursa olsun bir kişi suç ile ilgili bir bilgi vermekten kaçınabilir. Bu yüzden susma hakkı mutlak bir hak olarak düşünülebilir.

---

411 Varela, Alberto Arufe: Employment Privacy Law in the European Union: Human Resources and Sensitive Data, Cambridge 2003, s. 176.
412 M.N. ve Diğerleri/San Marino, Başvuru No: 28005/12, 07.07.2015, 1 Şubat 2019.
413 Gül/Alagöz, s. 164.

Fakat susma hakkının kullanılamayacağı yerler olabilecek midir? Örneğin, ifadesi alınacak olan kişinin kimliğini ibraz etmemesi ve adı da dâhil hiçbir beyanda bulunmaması söz konusu olabilir. Bu durum aleyhe delil vermeme ilkesinin bir görünümü olarak aleyhe kişisel veri vermeme hakkının olup olmayacağı sorularını beraberinde getirmektedir.

Susma hakkının kişisel veriler yönünden değerlendirdiğimizde şunu belirtmek gerekir ki eğer kişinin beyanı kişisel bir veriyi içeriyorsa kişi bunu söylememe konusunda daha rahat davranabilmelidir. Özellikle ifade ve sorgunun tarzına ilişkin hükümlerin düzenlendiği CMK m. 147 uyarınca, ifade verenin veya sorguya çekilenin kişisel ve ekonomik durumu hakkında bilgi alacağının düzenlenmiş olması karşısında kişinin susma hakkını kullanabiliyor olması gereklidir. Çünkü söz konusu veriler kişisel veri içermektedir.

Bunun ifade alımında aranan amaçla uyuşmaması sebebiyle kanuni usul olarak belirlenmesi bizce makul değildir. İşte bu gibi esasen yürütülen soruşturma ile doğrudan bağlantılı olmayan verilerin gereksizce toplanıyor olması hatalı bir tutum teşkil etmektedir. Dolayısıyla bu çerçevede, var olan kanuni düzenlemelerin kişisel verilerin gizliliği hassasiyetini taşıyacak düzeyde tekrar değerlendirilmesinde fayda bulunmaktadır.

d) Unutulma hakkı

Unutulma hakkı, kişinin daha çok sosyal medyaya bıraktığı veriler olmak üzere dijital ortamda girdi sağladığı verilerin silinmesini talep etme hakkıdır. Diğer bir deyişle, unutulma hakkı, kişinin kendisi hakkında sanal âlemde yer alan her türlü eksik ve yanlış bilginin düzeltilmesini ve kişinin kendi hak sahibi olduğu internete alanında yayınlanmamasını isteme hakkını ifade etmektedir[414]. Bu yönüyle, kişisel verilerin depolanmasının zıttıdır.

Unutulma hakkının konusu, işlenme tarihinde hem hukuka uygun hem de hukuka aykırı olan verileri kapsamanın yanı sıra yalnızca interneti kapsamaktadır[415]. Unutulma hakkının düzenlemelerde yer almaya başlıyor olmasının önemli bir yönü, her şeyi

[414] Henkoğlu, s. 108; Ayözger Öngün, s. 46.
[415] Yavuz, Can: İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı, Ankara 2018, s. 56.

kaydeden fakat hiçbir şeyi unutmayan ve bu yönüyle insan beyninden farklı bir yapıda olan ağ(web) üzerinde kişisel verilerin korunabilmesi amacıyla gerekli adımların atılabiliyor olmasıdır[416]. Burada adımlardan kasıt ise, hukuka aykırı olarak verileri hafızasında kayıtlı tutmakta olan ağların hukuk düzleminde şekillendirilmesi, hukuka aykırı kayıtların depolanmasının önüne geçilmesidir.

Unutulma hakkı KVK Kanunu'nda düzenlenmemektedir. Fakat benzer bir hüküm olarak KVK Kanunu m. 7'de, işlenmesini gerektiren sebeplerin ortadan kalkması halinde verilerin silinip anonim hale getirileceği düzenlenmektedir.

GDPR'da ise unutulma hakkı ilk defa ayrı bir maddede düzenlenmiştir. Her ne kadar silme hakkı dijital platform ile sınırlanmamış olsa bile, GDPR m. 17'nin başlığında unutulma hakkı, silme hakkı ile eş anlamlı olarak kullanılmıştır.

2016/680/EU sayılı Direktif'te ise unutulma hakkı düzenlenmemiştir. Fakat m. 16'da kişisel verilerin silinmesi, sınırlanması ve doğrulanması düzenlenmiştir. Madde kapsamında verilerin genel olarak silinmesi ele alınmakta olduğundan, sanal ortamda unutulma hakkı çerçevesindeki verilerin silinmesi talep edilebilecektir.

Temel dayanağı amaçla bağlılık ilkesi olan unutulma hakkı, veri denetleyicisini, başvuran kişinin kişisel verilerini silmesi ve verinin daha fazla yayılmasını durdurması hususunda yetkilendirmekte ve görevlendirmektedir[417].

Avrupa Adalet Divanı'nın bu konudaki bir kararına göre, AB vatandaşlarının unutulma hakkı olduğu bir gerçektir fakat bu gerçeklik Avrupa sınırlarını aşarak AB'yi dünya polisliğine soyundurmaya varacak şekilde evrensel hukukî koruma sağlayamamaktadır. Dolayısıyla daha çok dijital veri bankaları üzerinde tatbik edilen bu hak sadece Avrupa sınırları içerisinde söz konusu olarak söz konusu hakkın kullanımına yapay bir sınır çekilmektedir.

Soruşturma evresinde kişisel verileri işlenen kişilerin, amaçla bağlılık ve sınırlı süre saklanma ilkesi uyarınca unutulma hakları olduğunu belirtmek gerekmektedir. Buna göre

[416] Gutwirth/Leenes/de Hert, s. 204.
[417] Daha fazla açıklama için ikinci bölümün (I)(D)(3)(c) kısmına bakınız.

kişilerin sanal verileri süresiz ya da uzun uzadıya süreler boyunca işlenmesi ve depolanması hukuka aykırıdır.

e) İtiraz ve tazminat hakkı

Soruşturma evresinde orantılı bir biçimde işlenmeyen kişisel verilerin varlığı söz konusu olmakta ise bu işleme yönelik itiraz hakkının olması gerekmektedir.

GDPR m. 21 ve 2016/680/EU sayılı Direktif m. 56'da düzenlenen itiraz hakkına göre, veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı soruşturma evresini kapsamaktadır.

Bu maddede veri işleyenin, veri sahibinin menfaatlerinden, haklarından ve özgürlüklerinden ağır basan işleme faaliyetlerine yönelik olarak zorlayıcı meşru gerekçeler göstermediği sürece kişisel verileri işleyemeyeceği güvence altına alınmıştır. Dolayısıyla, bu gerekçeler ileri sürülerek verilerin işlenmesine soruşturma evresinde dahi itiraz edilebilecektir.

AİHM'e göre kişisel verilerin ihlal edildiği ile ilgili itirazlarda, itiraz incelemesi yapacak makamların incelemesi sadece kanunda bahsedilen şekli özellikleri açısından değil ayrıca işlemin gerçekleştiği fiili koşulların da inceleme kapsamında yer alması gerekmektedir.

Bu konu ile ilgili *Vinci Construction ve GTM Génie Civil et Services/Fransa* davasında AİHM, hâkimin soruşturma görevlilerinin el koyduğu belgelerin bir avukatın yazışmalarını içerdiğinin farkında olmasına rağmen itirazı sadece şeklen incelediği için yapılan el koyma işlemlerinin izlenen meşru hedefle orantısız olduğuna hükmetmiştir[418].

Tazminat hakkı ise KVK Kanunu m. 11(1)(ğ)'de zikredilmiştir. Kanun m. 28(2)'de tazminat talebinin soruşturma evresinde kanuna aykırı olarak işlenmesi halinde zararın giderilmesinin talep edilebileceğini düzenlemektedir. O halde, bu yönden hakkın tatbikinde bir engel bulunmamaktadır.

[418] Vinci Construction ve GTM Génie Civil et Services/Fransa, Başvuru No: 63629/10 60567/10, 02.04.2015, 21 Şubat 2019.

DÖRDÜNCÜ BÖLÜM:

KİŞİSEL VERİLERİN SORUŞTURMA EVRESİNDE KORUMA TEDBİRLERİ VE DİĞER DELİL DEĞERLENDİRME YÖNTEMLERİ İLE İŞLENMESİ

I. GENEL OLARAK

Tezimizin bu kısmında, CMK m. 74 ve devamında düzenlenen soruşturma evresinde delil toplamaya ilişkin hükümler değerlendirilmektedir.

Kişisel verilerin soruşturma evresinde işlenmesine yol açan CMK'da yer alan koruma tedbirleri düzenlemeleri ve diğer delil değerlendirme yöntemleri hükümlerine bakıldığında kanun koyucunun hepsine karşı ortak bir tavır takınmakta olduğu dikkat çekmektedir.

Buna göre, kanun koyucu, bu düzenlemelerle aslında kişisel verilere yönelik her türlü müdahalede, müdahalenin kişinin onurunu dikkate alınması gerektiğini göstermektedir. Bu doğrultuda, hâkim kararı olmaksızın veya kişinin sağlığına zarar veriliyorsa şüphelinin vücudundan örneklerin alınamamakta ve elde edilen veriler hiçbir biçimde kullanılamamaktadır[419].

Ayrıca belirtmeliyiz ki bizim buradaki amacımız elbette ki tüm süreci bütün yönleri ile ortaya koymak değil, ilgili hukuk kurallarındaki hükümleri kişisel verilerin korunması ilkeleri açısından değerlendirmektir. Dolayısıyla, genel ya da özel nitelikli kişisel verilerin soruşturma evresinde işlenmesine sebep olacak her işlemin yapılması, her ne kadar KVK Kanunu m. 28'deki istisnadan yararlanmakta olsa da bu işlemlerin en azından genel ilkelere uyması gerektiğini yukarıda belirtmiştik.

Bu bakış açısından hareketle, tezimizin ana eksenini oluşturan bu kısımda, öncelikle suç sonrasında delil elde etmek amacıyla kişisel verilerin adli tedbirlerle elde edilme yöntemleri değerlendirilmektedir. Akabinde ise alınan koruma tedbirlerinin ve delil değerlendirme yöntemlerinin uygulanması sırasında işlenmekte olan kişisel veriler ve en

[419] Mahmutoğlu, Fatih Selami. 2009. "Ceza ve Ceza Yargılama Hukukunda Özel Yaşam." Türkiye Barolar Birliği Özel Yaşamın Gizliliği Paneli, Ankara, 18 Ekim 2009, s. 108.

son olarak soruşturma evresinde kişisel verilerin işlenmesiyle sonuçlanan diğer hükümler değerlendirilmektedir.

II. SORUŞTURMA EVRESİNDE KİŞİSEL VERİLERİN KORUMA TEDBİRLERİ VE DELİL DEĞERLENDİRME YÖNTEMLERİ İLE ELDE EDİLMESİ

A. Genel Olarak

Suç sonrasında delil elde amacıyla alınacak bütün tedbirler, adli tedbir niteliğinde olup kural olarak CMK'da düzenlenmektedirler[420]. Bu yöntemlerin, temel hak ve hürriyetleri sınırlandırmakta olmaları sebebiyle Anayasa m. 13 uyarınca kanun ile düzenlenmeleri gerekmektedir.

Söz konusu yöntemler, CMK'da Koruma Tedbirleri olarak anılan CMK m. 90-140 hükümlerinde yer almaktadır. Ayrıca, Gözlem Altına Alınma, Muayene, Keşif ve Otopsiye ilişkin hükümlerin düzenlendiği m. 74 ve devamındaki hükümler koruma tedbiri başlığı altında düzenlenmediğinden bunların koruma tedbiri olup olmadığı tartışmalıdır. Esasen, delilden sanığa gitmeyi mümkün kılan bilimsel deney elde etme yöntemleri olmaları sebebiyle bunlar da birer modern koruma tedbirleridir[421]. Ayrıca bu tedbirler birer delil değil, delil değerlendirme yöntemleridir. Yani bu yöntemlerin sonucu ile delilin kendisi elde edilmeyip, var olan delillerin değerlendirme rapor sonucu olarak ortaya çıkmaktadır. Bu karışıklığı aşabilmek ve tüm yöntemlerin hepsini ifade edebilmek adına, koruma tedbirleri ve delil değerlendirme yöntemlerini ifadesini kullanmaktayız.

B. Soruşturma Evresinde Alınacak Koruma Tedbirlerinin ve Delil Değerlendirme Yöntemlerinin Ortak Özellikleri

Koruma tedbirleri, "*ceza muhakemesinin gereği gibi yapılabilmesi veya hükmün infazının mümkün kılınması amacıyla muhakeme sürecinde başvurulabilen ve hükümden önce,*

[420] CMK atfıyla özel hükümler getirmek amacıyla da Tanık Koruma Kanunu gibi kanunlarda da özel hükümler yer almaktadır.
[421] Parlar/Çetin, s. 238.

gerektiğinde zor kullanmak suretiyle bazı temel hak ve özgürlüklere geçici müdahaleyi gerektiren işlemlerdir"[422].

Kanun koyucunun benimsemekte olduğu sistemli tavır doğrultusunda bütün adli tedbirler bazı şartlara bağlı olarak alınabilmektedir. Koruma tedbirlerinin ön şartları olarak nitelenen bu şartlar gecikmede tehlike bulunması, haklı görünüş ve orantı bulunmasıdır[423]. Bazı yazarlar bu ön şartlara, suç şüphesinin bulunması ve kanunu düzenlemenin varlığını da eklemektedir[424].

Kanunla düzenlenme şartı, koruma tedbirleri ve delil değerlendirme yöntemlerini uygulanmasıyla temel hak ve hürriyetlere müdahale ediliyor olması dolayısıyladır. Bu yüzden kanuni düzenlemeye dayanmadan elde edilen veriler ve deliller hukuka aykırı olmaktadırlar. Bu sebeple, bir kişi hakkında bir önleme başvurulabilmesine olanak tanıyan bir kanuni kural olmadan o önlemin uygulanması mümkün değildir[425].

Tüm koruma tedbirlerinin amacı, sanığın muhakeme sürecinde hazır bulunmasını, delillerin korunmasını ve verilecek hükmün yerine getirilmesini sağlamaktır[426]. Somut olayda uygun düştüğü ölçüde koruma tedbirleri bu amaçlar doğrultusunda işlevini yerine getirmektedir. Bu yönüyle koruma tedbirleri ve delil değerlendirme yöntemleri esasen zorlayıcı tedbirler olup bunların uygulanabilmesi için ilgilinin rızası aranmamaktadır[427].

Bunun dışında, koruma tedbirleri ve delil değerlendirme yöntemlerinin bazı ortak özellikleri bulunmaktadır. Bu özellikler yöntemlerin geçici olması, araç olması, zorlama niteliğinin olması ve ihtiyari olmasıdır[428]. Bir görüşe göre bunlara, görünüşte haklılık, ölçülülük ve bir karara dayanması özellikleri de eklenmelidir[429].

Koruma tedbirleri ve delil değerlendirme yöntemlerinin geçici olması, alınan tedbir kararı süresince tedbirlerin uygulanmasını, muhakeme süresi ve dışında uygulanmamasını ifade

---

[422] Şahin, s 263.
[423] Centel, Nur/Zafer, Hamide, Ceza Muhakemesi Hukuku, İstanbul 2018, s. 357-358; Yenisey, Feridun/Nuhoğlu, Ayşe: Ceza Muhakemesi Hukuku, Ankara 2018, s. 301-302.
[424] Ünver, Yener/Hakeri, Hakan: Ceza Muhakemesi Hukuku, Ankara 2018, s. 302-304.
[425] Yurtcan, s. 316.
[426] Centel, Nur/Zafer, Hamide, s. 355.
[427] Toroslu, Nevzat/Feyzioğlu, Metin: Ceza Muhakemesi Hukuku, Ankara 2018, s. 251.
[428] Centel, Nur/Zafer, Hamide, s. 356; Ünver/Hakeri, s. 300-301.
[429] Şahin, Cumhur: Ceza Muhakemesi Hukuku I, Ankara 2017, s. 269-270.

eder. Bu sınırlama gereklidir çünkü bireyin başta özgürlüğü olmak üzere çeşitli temel haklarının kısıtlanmasına sürekli katlanması beklenemez.

Araç olma ise, tedbirlerle elde edilen delillerin maddi gerçeğe ulaşma yolunda araç olmasını ve sağlıklı bir muhakeme ve aşamalarının gerçekleşmesini ifade eder. Bu yönden kişiye yönelik tedbirlerin uygulanmasında da orantılılığa hizmet etmektedir.

Zorlama niteliği, uygulanan yöntemlerin hepsinde kişiden cebirle delil elde etmeye yönelimin olmasını ifade eder. Her ne kadar telekomünikasyon yoluyla yapılan iletişimin denetlenmesi gibi yöntemlerde ise zor unsuru olmamakla birlikte kişisel verilerin gizliliği ve diğer belirli temel hak ve hürriyetlere kamu gücü kullanılarak açıkça müdahale edilmektedir. Yöntemlerin ihtiyari olması ise, soruşturmanın dağınıklığı ilkesi ile yakından ilgili olup, yöntemlerin uygulanmasının zorunlu olmayıp, somut olay içerisinde işin gereğine uygun düştüğü ölçüde yöntemlerin uygulanmasıdır.

Öte yandan, CMK'da yer alan bu tedbirlerden bazıları diğer kanunlarda da adli amaçlı olarak düzenlenmektedir. Bunlardan özellikle soruşturma evresinde alınabilecek şekilde düzenlemenin varlığı kimi zaman tedbirin niteliği üzerinde karışıklığa yol açabilmektedir. Örneğin, durdurma ve kimlik sorma PVSK m. 4/A'da[430] ve Adlî ve Önleme Aramaları

[430] Durdurma ve kimlik sorma hükümleri PVSK m. 4/A'da düzenlenmektedir:
"Polis, kişileri ve araçları;
a) Bir suç veya kabahatin işlenmesini önlemek,
b) Suç işlendikten sonra kaçan faillerin yakalanmasını sağlamak, işlenen suç veya kabahatlerin faillerinin kimliklerini tespit etmek,
c) Hakkında yakalama emri ya da zorla getirme kararı verilmiş olan kişileri tespit etmek,
ç) Kişilerin hayatı, vücut bütünlüğü veya malvarlığı bakımından ya da topluma yönelik mevcut veya muhtemel bir tehlikeyi önlemek, amacıyla durdurabilir.
Durdurma yetkisinin kullanılabilmesi için polisin tecrübesine ve içinde bulunulan durumdan edindiği izlenime dayanan makul bir sebebin bulunması gerekir. Süreklilik arz edecek, fiilî durum ve keyfilik oluşturacak şekilde durdurma işlemi yapılamaz.
Polis, durdurduğu kişiye durdurma sebebini bildirir ve durdurma sebebine ilişkin sorular sorabilir; kimliğini veya bulundurulması gerekli diğer belgelerin ibraz edilmesini isteyebilir.
Durdurma süresi, durdurma sebebine esas teşkil eden işlemin gerçekleştirilmesi için zorunlu olan süreden fazla olamaz.
Durdurma sebebinin ortadan kalkması halinde kişilerin ve araçların ayrılmalarına izin verilir.
Polis, durdurduğu kişi üzerinde veya aracında silah veya tehlike oluşturan diğer bir eşyanın bulunduğu hususunda yeterli şüphenin varlığı halinde, kendisine veya başkalarına zarar verilmesini önlemek amacına yönelik gerekli tedbirleri alabilir. Bu amaçla kişinin üzerindeki elbisenin çıkarılması veya aracın, dışarıdan bakıldığında içerisi görünmeyen bölümlerinin açılması istenemez. Ancak, el ile dıştan kontrol hariç, kişinin üstü ve eşyası ile aracının dışarıdan bakıldığında içerisi görünmeyen bölümlerinin aranması; İçişleri Bakanlığı tarafından belirlenecek esaslar dâhilinde mülki amirin görevlendireceği kolluk amirinin yazılı, acele hâllerde sonradan yazıyla teyit edilmek üzere sözlü emriyle yapılabilir. Kolluk amirinin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Bu fıkra kapsamında yapılan araç aramalarına ilişkin olarak kişiye, arama gerekçesini de içeren bir belge verilir.

Yönetmeliği m. 27'de[431] hem önleyici hem de adli mahiyette düzenlenmiştir. Dolayısıyla, veri elde etme yöntemleri üzerinde önleyici ve adli tedbirlerin karılması ve CMK'da

Bu Kanun ve diğer kanunların verdiği görevlerin yerine getirilmesi sırasında, polis tarafından gerekli işlemler için durdurulan kişiler ve araçlarla ilgili hükümler saklıdır.
Polis, görevini yerine getirirken, kendisinin polis olduğunu belirleyen belgeyi gösterdikten sonra, kişilere kimliğini sorabilir. Bu kişilere kimliğini ispatlamaları hususunda gerekli kolaylık gösterilir.
Belgesinin bulunmaması, açıklamada bulunmaktan kaçınması veya gerçeğe aykırı beyanda bulunması dolayısıyla ya da sair surette kimliği belirlenemeyen kişi tutularak durumdan derhâl Cumhuriyet savcısı haberdar edilir. Bu kişi, kimliği açık bir şekilde anlaşılıncaya kadar gözaltına alınır ve gerekirse tutuklanır. Gözaltına ve tutuklamaya karar verme yetkisi ve usulü bakımından 5271 sayılı Ceza Muhakemesi Kanunu hükümleri uygulanır.
Kimliğinin tespiti amacıyla tutulan kişiye, kimliği tespit edildikten sonra ve talepte bulunması halinde, bu amaçla tutulduğuna ve tutulma süresine dair bir belge verilir. Kişinin kimliğinin belirlenmesi durumunda, bu nedenle gözaltına alınma veya tutuklanma haline derhâl son verilir.
Nüfusa kayıtlı olmadığı için kimliği tespit edilemeyen kişilerin nüfusa kayıtlarının temini için gerekli işlemler yapıldıktan sonra, 5 inci maddeye göre fotoğraf ve parmak izi tespit edilerek kayda alınır.
Kimliği tespit edilemeyen kişinin yabancı olduğunun anlaşılması halinde, 5682 sayılı Pasaport Kanunu ve 5683 sayılı Yabancıların Türkiye'de İkamet ve Seyahatleri Hakkında Kanun hükümlerine göre işlem yapılır."

[431] Durdurma, durdurma sonrası kontrol ve arama işlemleri Adlî ve Önleme Aramaları Yönetmeliği m. 27'de düzenlenmektedir:
"Kolluk, kişileri ve araçları;
a) Bir suç veya kabahat işlenmesini önlemek,
b) Suç işlendikten sonra kaçan faillerin yakalanmasını sağlamak, işlenen suç veya kabahatlerin faillerinin kimliklerini tespit etmek,
c) Hakkında yakalama emri ya da zorla germe kararı verilmiş olan kişileri tespit etmek,
ç) Kişilerin hayatı, vücut bütünlüğü veya mal varlığı bakımından ya da topluma yönelik mevcut veya muhtemel bir tehlikeyi önlemek, amacıyla durdurabilir.
Durdurma yetkisinin kullanılabilmesi için, "umma" derecesinde makul şüphe bulunmalıdır. Somut emarelerle desteklenen şüphe bulunmadan, süreklilik arz edecek, fiilî durum ve keyfilik oluşturacak şekilde durdurma işlemi yapılamaz.
Kolluğun durdurma yetkisini kullanabilmesi için tecrübesine ve içinde bulunulan durumdan edindiği izlenime dayanarak, kişinin bir suç işleyeceği veya işlediği hususunda veya kişinin silâhlı olduğu ve hâlen tehlike yarattığı konusunda makul bir sebebin bulunması gerekir.
Kolluk, görevini yerine gerekirken, kendisinin kolluk görevlisi olduğunu belirleyen belgeyi gösterdikten sonra durdurduğu kişiye durdurma sebebini bildirir; şüpheye yol açan davranışları ve durdurma sebebine ilişkin sorular sorabilir; kimliğini veya bulundurulması gerekli diğer belgelerin ibraz edilmesini isteyebilir.
Kişi, kimliğine ilişkin olanlar hariç, sorulan sorulara cevap vermekle yükümlü değildir. Durdurma yetkisinin kullanılmasına neden olan şüphe, yapılan açıklamayla veya herhangi bir şekilde ortadan kalkarsa, kişilerin gitmesine ve araçların ayrılmalarına izin verilir.
Durdurma süresi, durdurma sebebine esas teşkil eden işlemin gerçekleştirilmesi için zorunlu olan süreden fazla olamaz.
Durdurma üzerine aşağıdaki işlemler yapılır:
a) Durdurulan kişi üzerinde giysilerinden herhangi birisi çıkarılmaksızın, yoklama biçiminde bir kontrol yapılır. Bu işlem sonucunda, kişide silâh bulunduğu sonucunu çıkarmaya yeterli şüphe meydana gelirse, memur kendiliğinden silâh ve diğer suç eşyası araması yapabilir.
b) Yoklama sureyle kontrol, kişinin cinsiyetinde bulunan görevli tarafından yapılır.
c) Yapılan kontrolün konusu ve sebepleri ilgiliye açıklanır.
ç) Bir kişinin veya aracın durdurulma süresinin, şartlara göre makul olması ve kontrol için ayrılan süreyi aşmaması gerekir.
d) Yoklama sureyle kontrol, kişiye en az sıkın verici şekilde yapılır.
e) Yapılan kontrolün neticesinde suça ilişkin iz, eser, emare ve delil elde edilirse, kişi yakalanır.
f) Uyuşturucu gibi belirli bir şeyin, kişinin herhangi bir yerinde gizlendiği düşünülüyorsa, daha geniş çaplı kontrol yapılabilir.

sağlanan güvencelerden uzaklaşılarak kolluk amirinin yazılı emri yeterli görülebilmesi aşağıda gösterilmekte olduğu üzere verilerin hukuka uygun olarak işlenmesinde çeşitli problemlere yol açabilecektir.

C. Koruma Tedbirleri Ve Delil Değerlendirme Yöntemlerine İlgili Kişinin Rıza Vermemesi Problemi

Bu konuda öncelikle ifade etmek gerekir ki, kişisel verilerin soruşturma evresinde adli yöntemlerle işlenme yolları esasen hiç kimsenin kendisi veya belirli derecede yakınları aleyhine delil vermeye zorlanmaması ilkesiyle çatışmaktadır.

Kanunun verdiği bu yetki çerçevesinde kişinin rızası hilafına vücudu üzerinden delil elde edilmekte ve bu deliller de sıklıkla kişisel verileri içermektedir. Bu noktada delil elde edilen kişinin, bu ilke çerçevesinde delil vermeye zorlanmasına aktif katılımının hukuka uygun bulunup, kişinin delil alınması için pasif davranışa zorlanmasının[432] hukuka aykırı bulunması, hukuken yeterli bir ölçüt olamayacağı düşünülmektedir[433].

Bunun gerek soruşturma makamları gerekse şüpheli/sanık tarafından suiistimale açık olduğu ve muhakeme amacına aykırı uygulamalara neden olabileceği nedeniyle bunun

---

g) Yoklama sureyle kontrol, kişinin veya aracın ilk durdurulduğu yerde veya o yerin yakınında, mümkün olduğu kadar başkalarının göremeyeceği tarzda yapılır. Başka yere götürülerek kontrol yapılamaz.
ğ) Makul sebebi oluştuğu takdirde, daha geniş kapsamlı kontrol yapılması için, kolluk aracından veya yakındaki kapalı bir yerden yararlanılabilir.
h) Kontrolden sonra talep üzerine olay yerinde derhâl bir tutanak düzenlenir.
Kolluk, durdurduğu kişi üzerinde veya aracında silâh veya tehlike oluşturan diğer bir eşyanın bulunduğu hususunda yeterli şüphenin varlığı halinde, kendisine veya başkalarına zarar verilmesini önlemek amacına yönelik gerekli tedbirleri alabilir. Bu amaçla kişinin üzerindeki elbisenin çıkarılması veya aracın, dışarıdan bakıldığında içerisi görünmeyen bölümlerinin açılması istenemez. Ancak el ile dıştan kontrol hariç, kişinin üstü ve eşyası ile aracının dışarıdan bakıldığında içerisi görünmeyen bölümlerinin aranması; İçişleri Bakanlığı tarafından belirlenecek esaslar dâhilinde mülki amirin görevlendireceği kolluk amirinin yazılı, acele hâllerde sonradan yazıyla teyit edilmek üzere sözlü emriyle yapılabilir.
Arama emrinde aşağıdaki hususlara açıkça yer verilir:
a) Aramanın sebebi,
b) Aramanın konusu ve kapsamı,
c) Aramanın yapılacağı yer, tarih ve emrin geçerli olacağı süre,
ç) Aramanın yapılacağı kişinin açık kimliği ile aracın plaka, marka ve modeli.
Kişinin üstü ve eşyası ile aracının aranmasında 28 ve 29 uncu maddelerde belirlen usuller uygulanır.
Arama sırasında elde edilen ve adlî soruşturma ve kovuşturmalarda kullanılabilecek bilgi, bulgu ve şüpheliler hakkında bu Yönetmelikteki ilgili hükümler uygulanır.
Kolluk amirinin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Yapılan araç aramalarına ilişkin olarak kişiye, arama gerekçesini de içeren bir belge verilir.
Bu maddede yazılı işlemler gece de yapılabilir."

[432] Örneğin, alkol ölçümü için kişinin ölçüm cihazına üflemek zorunda bırakılması aktif katılım; kişiden alkol ölçümü için zor kan alınması pasif katılımdır.

[433] Ünver/Hakeri, s. 71.

yerine yasal sınırlar içerisinde uygulanacak adli yöntemlerin, delil vermeye zorlanmama ilkesinin istisnası olarak kabul edilmesi daha gerçekçi bir çözüm olabilecektir[434]. Tartışma bir yana, uygulamada yine de kişinin direnmesi halinde söz konusu zorlama fiilinin insan onurunu ihlal etmeyecek şekilde yapılması gerekir.

D. Koruma Tedbirleri Ve Delil Değerlendirme Yöntemlerinin Çeşitleri

1. Kişi hürriyeti ve güvenliğine müdahale eden yöntemler ile kişisel veri elde edilmesi

a) Yakalama ve gözaltı yolu ile kişisel veri elde edilmesi

Yakalama ve gözaltına ilişkin hükümler, CMK'da m. 90 ila 99 arasında düzenlenmektedir. Suçun işlenmesi ile başlayan bu süreç, şüphelinin sulh ceza hâkimi tarafından verilecek tutuklama veya serbest bırakılma kararı ile son bulmaktadır. Bu süreç içerisinde şüpheli konumundaki bireylerin kişisel verileri çeşitli yollardan işlenmeye maruz kalmaktadır. Yakalama ve gözaltı yöneldikleri değerler açısından özgürlüğe yöneliktir[435].

Bu konuda bazı maddeleri özel olarak değerlendirmek gerektiğinden, öncelikle gözaltı işlemlerinin denetimine değinmek gerekir. Bu hususun düzenlenmekte olduğu CMK m. 92'ye göre, gözaltına alınan kişilerin bulundurulacakları nezarethaneleri, varsa ifade alma odaları, bu kişilerin durumları, gözaltına alınma neden ve süreleri, gözaltına alınma ile ilgili tüm kayıt ve işlemleri Nezarethaneye Alınanlar Defterine kaydedilmektedir. Bu kayıtlar kişisel verileri pek tabi içermektedirler.

Dolayısıyla, bu verilerin kaydedilmelerine sebep oldukları işlem sona erdiği takdirde silinmesi veya anonimleştirilmesi gerekmektedir. Keza bu verilerin depolanmasında artık bir kamu düzeni sebebinin varlığından bahsedilemez. Aksi halde, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine, amaca bağlılık-amaçla sınırlanma ilkesine, verilerin doğruluğu ilkesine ve sınırlı süre saklanma ilkesine aykırılık meydana gelebilecektir.

İkinci nokta, bir suç şüphesi ile yakalanan veya gözaltına alınan şüphelinin bulunduğu bu statüye ilişkin bilgilerin artık onun kişisel verileri arasında yer aldığıdır. Dolayısıyla,

[434] Ünver/Hakeri, s. 72.
[435] Centel, Nur/Zafer, Hamide, s. 355.

soruşturma işlemleri için gerekli makamlara yapılacak bildirimin dışında başka kişilere bu durumun bildirilmesi kişisel verilerin korunması açısından hüküm ifade etmektedir. Buna göre, her ne kadar şüphelinin yakınlarına haber verilmesi ceza muhakemesine egemen olan adil yargılanma ilkesinden doğan bir hak olsa da, şüphelinin bu hakkı kullanmak istememesi de mümkündür.

Bunu soruşturma evresinde şüpheliye yönelik yapılan tüm çağrı evraklarının tebliğine ilişkin sorunsal üzerinden açıklarsak, tebligat zarflarının üzerinde kişinin yakınları tarafından görülecek şekilde şüpheliye ilişkin suç ile ilgili verilerin yazmaması gerektiğini belirtmek gerekmektedir. Çünkü her ne kadar bu kişiler, şüphelinin yakınları veya aynı yerde yaşamakta olduğu kimseler olsalar bile şüpheli kişinin iradesi soruşturma verilerinin hiç kimse ile paylaşılmaması yönünde olabilir. Aksini savunmanın tutarlı gerekçelerinin olması da pek mümkün görünmemektedir. Keza bir kişiye ait soruşturma verilerinin -ki bu sadece zarfın üzerinde suç tipinin yazması bile olabilir- başkaları tarafından öğrenilmesinde kamu düzenine ilişkin bir menfaat söz konusu olamaz. Fakat bu verilerin başkalarınca öğrenilmesi -ki şüpheli bu verilerin hiç kimse tarafından öğrenilmesini istemiyor olabilir- hem şüphelinin masumiyetlik karinesi ile hem de şahsilik ilkesi ile bağdaşmamaktadır.

Dolayısıyla, olması gereken kişinin soruşturmaya ilişkin statüsünü diğer insanlara duyurmak değil, bunu ya şüphelinin iradesine bırakmak ya da gizli tutmaktır. Bu minvalde, yakalanan veya gözaltına alınanın durumunun yakınlarına bildirilmesinin düzenlenmekte olduğu CMK m. 95 doğrultusunda Cumhuriyet savcısının emriyle şüphelinin bir yakınına veya belirlediği bir kişiye gecikmeksizin haber verilmesi konusunda şüphelinin rızasının alınması gereklidir. Bu durum, yakalanan veya gözaltına alınan yabancı ise, yazılı olarak karşı çıkmaması halinde, durumu, vatandaşı olduğu devletin konsolosluğuna bildirilmesi halinde de geçerlidir.

Her iki durumda da esas alınması gereken husus hiç şüphesiz şüphelinin iradesidir. Çünkü kişinin yakınlarına ya da vatandaşı olduğu konsolosluğa yapılacak bildirim şüphelinin kişisel durumuna ilişkin bir veridir. Bu verilerinin bireylerin iradesinden bağımsız olarak bildirilmesi hukuka aykırılık teşkil edecektir. Ayrıca, bu bildirimi zorunlu tutan bir kamu düzeni sebebi de olmadığından resen bildirim de söz konusu değildir. Aksi bir uygulama

halinde verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine aykırılık vuku bulacaktır.

Üçüncü nokta, soruşturmada yazılılık ilkesinin bir sonucu olarak kişiye yönelik yapılan yakalamanın tutanağa bağlanmasıdır. CMK m. 97'de düzenlenen bu hükme göre, bu tutanağa yakalananın, hangi suç nedeniyle, hangi koşullarda, hangi yer ve zamanda yakalandığı, yakalamayı kimlerin yaptığı, hangi kolluk mensubunca tespit edildiği, haklarının tam olarak anlatıldığının açıkça yazılması gerekmektedir.

Kanunun verdiği bu yetkiye dayanılarak tutulan bu tutanakta, öncelikle tutanağın tutulma amacının sınırları aşılmamalıdır. Bunun tezimiz açısından anlamı, suç ile ilgisi bulunmayan şüpheliye ait kişisel verilerin tutanağa yazılması problemidir. Amaca bağlılık-amaçla sınırlanma ilkesi ve orantılılık (veri minimizasyonu) ilkesi gereğince bu verilerin kesinlikle yakalama tutanağında yer almaması gerekmektedir.

Son olarak belirtmek gerekir ki, CMK m. 99'da, gözaltına alınan kişilerin bulundurulacakları nezarethanelerin maddî koşulları, şüphelinin hangi görevlinin sorumluluğuna bırakılacağı, sağlık kontrolünün nasıl yapılacağı, gözaltı işlemlerine ilişkin kayıt ve defterlerin nasıl tutulacağı, gözaltına alınmanın başlangıcında ve bu tedbire son verildiğinde hangi tutanakların tutulacağı ve gözaltına alınan kişiye hangi belgelerin verileceği ile kolluk tarafından gerçekleştirilen yakalama işlemlerinin yürütülmesinde uyulacak kuralların, Yakalama, Gözaltına Alma ve İfade Alma Yönetmeliği hükümlerinde gösterileceği düzenlenmektedir.

Bu yönetmelik hükümlerinin ve yakalama ve gözaltı sürecinde kişinin üst aramasına ilişkin hükümlerin, kişisel verilerin korunması hususunda yukarıda ele aldığımız ilkelere ve ilgili kişinin haklarına uygun olması gerekmektedir.

b) İfade alma yolu ile kişisel veri elde edilmesi

CMK m. 145 ila 148 hükümlerinde ifade ve sorguya ilişkin kurallar düzenlenmektedir. Bu hükümler delil elde etme amacı doğrultusunda düzenlenmese de ifadenin delil değerinde bir etki gücüne sahip olduğundan bu kısımda yer vermeyi uygun bulmaktayız.

Keza ifade, delillere ulaşma soruşturma evresinde şüphe kesinleştirmeyi sağlayacak olan delile ulaşma aracıdır[436].

İfade, bir suç işlediği yönünde şüphe altında olan kişiye yönelik yüklenen suç hakkında soruşturma evresinde savcı karşısında açıklama yapması ve kendisini savunmasının istenmesidir. Yakalama, Gözaltına Alma ve İfade Alma Yönetmeliği m. 4'e göre, şüphelinin kolluk görevlileri veya Cumhuriyet savcısı tarafından soruşturma konusu suçla ilgili olarak dinlenmesi olarak tanımlanmaktadır. Bu işlemin mahkeme karşısında gerçekleşmesi ise sorguyu ifade etmektedir.

İfade ve sorguda, öncelikle şüpheli veya sanığın kimliği saptanır. Şüpheli veya sanık, kimliğine ilişkin soruları doğru olarak cevaplandırmakla yükümlüdür. İfade ve sorgunun tarzının düzenlendiği CMK m. 147 ve ifade almanın esaslarının düzenlendiği Yönetmelik m. 23'e göre, ifade verenin veya sorguya çekilenin kişisel ve ekonomik durumu hakkında da bilgi alınmaktadır. Her ne kadar kanuni düzenleme bu şekilde olsa da suç ile bağlantısı olmayan fakat o kişiyi belirlenebilir kılan her türlü kişisel ve ekonomik durumu yansıtan verinin kişisel verilerin korunması kapsamındaki ilkelere tabi olacak şekilde alınması gerekmektedir. Çünkü her suçun şüpheli veya sanığın ekonomik durumu ile bağlantısı olmayabilir ya da kişi bu bilgilerini vermek istemiyor olabilir.

Dolayısıyla muhakeme sürecine bir katkısı olmayacak bu verilerin alınmasında hukuki bir menfaat bulunmamakta olduğundan bunun kanuni bir zorunluk haline getirilmesi hatalıdır. Verilerin öğrenilmesinde bir zorunluluk varsa kişisel verilerin korunması hususundaki ilkelere uyulması kaydıyla zaten bu veriler hali hazırda kanuni usuller çerçevesinde öğrenilip elde edilebilmektedir. Zorunluluk bulunmuyorsa bu verilerin alınmaması yahut kişisel durumu yansıtan verilerin kişinin iradesine bırakılması gerekmektedir. Kişinin kendi rızasıyla vermek istediği hallerde ise öncesinde kişiye bu açıdan bilgi vermesi gereken sınırlı çerçevenin varlığı hatırlatılıp kişi aydınlatılmalıdır.

Öte yandan, her ne kadar kişiye yönelik ifade ve sorgu sırasında susma hakkı tanınmış olsa da, kişinin açıklamakla yükümlü tutulduğu kimliğini açıklamayıp susması halinde ne olacağı belirsizdir. Bir görüşe göre, susma hakkı, sadece isnat edilen suç hakkında açıklamada bulunmamayı kapsamakta olduğundan kişi, kimliğe ilişkin soruları doğru

[436] Aksoy İpekçioğlu, Pervin: "Gözaltında Alınan İfadenin Önemi ve Delil Değeri", Ankara Üniversitesi Hukuk Fakültesi Dergisi, 57/3, Ankara 2018, s. 54.

olarak cevaplandırmak zorundadır[437]. Başka bir görüşe göre ise, kimliğini bildirmemek fiili Kabahatler Kanunu m. 40'ta yaptırıma bağlandığından hukuk düzenince yaptırıma bağlanmış bir fiil hukuka uygun sayılamayacaktır[438].

Elbette ki kişinin fiziki olarak hâkim kararı olmadan diğer yollarla tespite zorlanması beklenemez. Kamu gücünü karşısında bulan ve kişisel verilerini ifade etmek zorunda kaldığını düşünen kişiye, kişisel verilerini ifade etmesinin istemiyor ise gerekli olmadığının belirtilmesi de bir çözüm olarak düşünülebilir. Üretilmiş hukuki bir çözümün olmayışı nedeniyle dolayısıyla, kanun koyucunun bu soruna eğilmesi gerekmektedir.

Ayrıca, CMK m. 147'de ifade ve sorgu işlemlerinin kaydında, teknik imkânlardan yararlanılır hükmü düzenlenmektedir. Burada teknik imkânlar ifadesinin ne olduğu belirsizdir. Yönetmelik m. 23'e de bu hüküm aynen aktarılmış fakat teknik imkânlar ifadesi açıklanmamıştır. Kişisel verilerin korunması açısından, ifade ya da sorgu veren kişinin sesinin kaydedilmesi, fotoğrafının çekilmesi ya da sürecin kayda alınması bu madde bağlamında akla gelen ilk hallerdir. Dolayısıyla kanun koyucunun buradaki muradını açmamış olması ve kişilerin sahip olduğu güvenceleri belirtmemiş olması kanunu bireyler açısından açık ve öngörülebilirlikten uzak kılmaktadır.

Bunun dışında, yine CMK m. 147 ve Yönetmelik m. 23'te, tutanağa bağlanan ifade sonucunda tutanakta bu işlemler sırasında hazır bulunan kişilerin isim ve sıfatlarının yazılmasının gerektiği düzenlenmektedir. Bizim görüşümüze göre bu tutum hatalıdır. Çünkü her ne kadar belli bir düzen için işlemi yapan görevlilerin tespiti açısından açık kimliklerinin belirtilmesi gerekli görülebilecek olsa da bunun yerine görevli kişilerin memur sicil numaraları yazılması da pek tabi mümkündür. Böylece hem işlemi yapan kişinin kim olduğu kolaylıkla yine saptanabilir hem de işlemi yapan kişinin kim olduğuna dair verileri işlenmemiş ve tutanağa erişimi olan diğer kişilere ifşa edilmemiş olur. Aksi halde görevli kişilerin kişisel verilerinin suç yargılaması gibi hassas konularda onlara zarar verebilecek kişilerce öğrenilmesi sonucunu doğurmaktadır ki bu durumda görevlilerin kendileri ve aileleri tehlikeye atılmaktadır.

---

[437] Arıcan, Mehmet: "Ceza Muhakemesi Hukukunda İfade Alma ve Sorgu", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 17/1, İzmir 2009, s. 52.

[438] Ömeroğlu, Ömer: "Ceza Muhakemesinde Şüpheli ve Sanığın Fizik Kimlik Tespiti", Türkiye Barolar Birliği Dergisi, 115, Ankara 2014, s. 71.

Keza birçok suçlu ve hükümlü, uğradıkları yaptırımlardan ötürü doğrudan kamu görevlilerini sorumlu tutmaktadır. Oldukça yaygın bir şekilde kamu görevlilerine karşı, gördükleri iş sebebiyle suç işlenmektedir. Dolayısıyla bu verilerin işlenmesinde öne sürülen kamu düzeni gerekçesinin orantılı bir şekilde uygulanmaması sebebiyle kamu görevlilerinin kimliklerini ifşa ederek tehlikeye atan bu uygulamadan vazgeçilmesi gerekmektedir. Bu orantılılık (veri minimizasyonu) ilkesinin gereğidir.

Son olarak belirtmek gerekir ki, CMK m. 153'e göre, müdafi, soruşturma evresinde dosya içeriğini inceleyebilir ve istediği belgelerin bir örneğini harçsız olarak alabilir. Müdafinin diğer hakları bu maddenin devamında açıklanmaktadır. Dolayısıyla müdafi, gerekli olması sebebiyle doğrudan şüpheli veya sanık ile ilgili kişisel verilere vakıf olmaktadır. .

Yakalama, Gözaltına Alma ve İfade Alma Yönetmeliği m. 22'ye göre, soruşturmanın amacını tehlikeye düşürebilecek ise müdafinin dosya içeriğini incelemesi veya belgelerden örnek alması, kısıtlanabilmektedir. Fakat bu kısıtlama yakalanan kişinin veya şüphelinin ifadesini içeren tutanağı kapsamamaktadır. Burada kısaca müdafi avukatın sır tutma yükümlüğü altında olduğundan bahsetmek gerekmektedir. Avukatlık Kanunu m. 36'ya göre, avukatların, kendilerine tevdi edilen veya gerek avukatlık görevi, gerekse, Türkiye Barolar Birliği ve baro organlarındaki görevleri dolayısıyla öğrendikleri hususları açığa vurmaları yasaktır. Bu yüzden, müdafinin de bu yükümlülüğe uyması gerekmekte, öğrendiği kişisel verileri üçüncü kişilerle her ne sebeple olursa olsun paylaşmamalıdır. Aksi halde müdafinin hem disiplin hem de cezai sorumluluk gündeme gelebilecektir. Fakat bu verilerin anonimleştirilmesi halinde ve paylaşılması ilgili kişi belirli kılmayacak bir halde ise paylaşılmasında hukuka aykırılık bulunmamaktadır.

c) Tanık ve beyanı üzerinden kişisel veri elde edilmesi

(1) Genel olarak

Tanık, kendisine karşı yürütülmeyen bir ceza soruşturmasında, olay hakkında beş duyusu ile edindiği algılamaları ifadesiyle açığa vuran kişidir[439]. Soruşturma evresinde işlenmekte olan kişisel veriler tanık açısından özellik göstermektedir. Tanığa ilişkin hükümlere CMK m. 46 ila 61 arasında yer verilmektedir.

[439] Y. CGK, E. 2013/1-251 K. 2013/454 T. 12.11.2013, 19 Şubat 2019, Kazancı İçtihat Bilgi Bankası.

Ayrıca ceza muhakemesinde tanıklık görevi sebebiyle korunmaları zorunlu olan kişilerin korunması amacıyla alınacak tedbirlere ilişkin esas ve usulleri düzenlemek amacıyla Tanık Koruma Kanunu çıkarılmıştır. Bu tedbirin uygulanabilmesi için tanığın kendisinin veya yakınlarının hayatı, beden bütünlüğü veya mal varlığı ağır ve ciddi tehlike içinde bulunması temel şarttır.

Bunun dışında, Tanık Koruma Kanunu'nun ilgili maddelerine dayanarak çıkarılan Cumhuriyet Başsavcılıkları ve Mahkemelerce Alınacak Tanık Koruma Tedbirlerine İlişkin Esas ve Usuller Hakkında Yönetmelik'te de bazı önemli hususlar bulunmaktadır. Yönetmelik dayandığı kanunun kapsamını kişi yönünden genişleterek tedbirlerle ilgili hükümlerinin, muhbir için de uygulanacağını belirtmektedir.

Düzenlemelerin bütünü açısından ifade etmek gerekir ki hem tanığın verdiği beyan hem de tanık koruma kapsamında elde edilen herhangi bir kişiyi belirlenebilir kılan veriler kişisel veri niteliğindedir. Bu yüzden, tanığa ilk önce sorulacak hususlar ve tanığın korunması başta olmak üzere tanığa ilişkin hükümler açısından soruşturma evresinde verilerin işlenmesine hâkim olan ilkeler açısından öne çıkan noktaları ortaya koymak önem kazanmaktadır.

(2) Tanık ifadesinin kapsamı ve alınış usulü açısından

Bu doğrultuda ilk olarak belirtmek gerekir ki, CMK m. 58'e göre, tanığa, ilk önce adı, soyadı, yaşı, işi ve yerleşim yeri, iş yerinin veya geçici olarak oturduğu yerin adresi, varsa telefon numaraları sorulmaktadır. Gerekirse tanıklığına ne dereceye kadar güvenilebileceği hakkında hâkimi aydınlatacak durumlara, özellikle şüpheli veya mağdur ile ilişkilerine dair sorular yöneltilmektedir. Burada şunu kesin olarak vurgulamak gerekir ki tanığın ceza muhakemesindeki önemi, delil hükmünde olacak bir beyan vermesi ve bu beyanın da olayı aydınlatmasıdır. Bunun dışında, tanığın şahsına ait bilgilerinde ceza muhakemesine yönelik bir katkısı beklenmemelidir.

Dolayısıyla, duruşmada tanığa sorularak adı, soyadı, yaşı, işi ve yerleşim yeri, iş yerinin veya geçici olarak oturduğu yerin adresi, varsa telefon numaralarının öğrenilmesi, kural olarak somut vakaların aydınlanmasına yönelik bir katkı yapmamaktadır. Aksine, bu bilgiler verilirken dosyaya erişimi olan bütün üçüncü kişilerce bu bilgilerin öğrenilmesine

sebep olunmaktadır. Ki bu verilerin öğrenilmesi kişilerin can ve mal güvenliğini tehlikeye atabileceği göz ardı edilemeyecek sosyal bir fenomendir.

Maddede sayılan bu veriler bir kişiyi belirlenebilir kıldığı için hiç şüphesiz kişisel veridirler. Böyle olmayan veriler de zaten özel hayat verisidirler. Bu sebepten ötürü T.C. kimlik numarası gibi kişiyi dolaylı yoldan ayırt edilebilir kılan veriler muhakeme sürecinde yetecektir. Zaten yargılamada kullanılacak adli sicil özetleri, sanığın kişisel ve ekonomik bilgilerin yer aldığı belgelerin duruşmada okunması eğer bu belgeler delil niteliğini haizse CMK m. 209 uyarınca zorunlu olacaktır.

Dolayısıyla daha fazla kişisel verilerin öğrenilmesi kişisel verilerin soruşturma evresinde işlenmesine yönelik istisna hükmünü orantısız bir şekilde genişletilmesine yol açarak soruşturmanın asıl amacından uzaklaştırmaktadır. Bu durum ise, soruşturma evresinde verilerin işlenmesine hâkim olan ilkelerden verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, amaca bağlılık-amaçla sınırlanma ilkesi ve orantılılık (veri minimizasyonu) ilkesine aykırı teşkil etmektedir.

Tanık ifadesinin alınış usulü, tanığa söylenecek şeyler ve sorulacak sorulara ilişkin olarak CMK m. 59'a göre, tanık dinlenmeden önce hakkında tanıklık yapacağı olayla ilgili olarak mahkeme başkanı veya hâkim tarafından kendisine bilgi verilmekte ve hazır olan sanık tanığa gösterilmektedir. Sanık hazır değilse kimliği açıklanmaktadır. Konuşurken sözü kesilmemesi gereken tanığa, tanıklık edilen konuları aydınlatmak, tamamlamak ve bilgilerinin dayandığı durumları gereğince değerlendirebilmek için ayrıca soru yöneltilebilmektedir.

Bu hükümlerin kişisel verilerin korunması açısından değerlendirdiğimizde belirtmemiz gerekir ki, tanığın kimlik ve adres bilgileri doğrudan kişisel veri iken tanıklık konusu olay ve tanıklığa ilişkin beyanlar bilgiler dolaylı kişisel verilerdir. Şüphesiz bu veriler doğrudan olmasa bile kişisel verilere ilişkin koruma ilkeleri çerçevesinde korunmalıdırlar.

Ayrıca tanığa yöneltilecek suçu aydınlatmaya yönelik olmayan ve kişisel veri içermekte olan soru ve cevapların sorulup cevaplanması mahkemece engellenmelidir. Şayet bu engellenmez ise kişisel veriler duruşma tutanağına kayıt edilmemelidir. Böylece hem beyanın alınma anına hem de dosyaya erişimi olan ilgisiz üçüncü kişilerce kişisel verilerin

öğrenilmesi engellenmiş olacaktır. Suçtan bağımsız kişisel verilerin üçüncü kişilerce öğrenilmesinin ceza muhakemesine bir katkısı olmadığından, aksi bir durumda kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine, orantılılık (veri minimizasyonu) ilkesine ve amaca bağlılık-amaçla sınırlanma ilkesine aykırılık söz konusu olacaktır.

Tanıkların dinlenmesi sırasındaki görüntü veya sesler kayda alınabilmektedir[440]. Ancak hem mağdur çocukların hem de duruşmaya getirilmesi mümkün olmayan ve tanıklığı maddî gerçeğin ortaya çıkarılması açısından zorunlu olan kişilerin tanıklığında bu kayıt zorunlu tutulmaktadır. Ayrıca Tanık Koruma Kanunu'nda tanık ile ilgili alınabilecek koruma tedbirlerinde, tanığın kimlik ve adres bilgilerinin kayda alınıyor olması ve sesinin, görüntüsünün ve diğer bilgi ve belgelerin değiştirilebiliyor olması sebebiyle tanığın kişisel verileri işlenmektedir[441].

Tanığın kaydının görüntülü veya sesli olarak kaydedilmesindeki zorunluluk değerlendirildiğinde ise amaç bir delil elde etme uğraşı olması sebebiyle ifadelerin yazıya geçirilmiş olması halinde de bu maksat hâsıl olacaktır. Bu yüzden, tanığın kişisel verisi olan görüntüsü ve sesinin alınmasının zorunlu tutulmuş olması, kişisel verilerin

---

[440] CMK, m. 52(3).

[441] Tanık koruma tedbirleri hükmü Tanık Koruma Kanunu m. 5'te düzenlenmektedir:
"(1) Bu Kanun kapsamında bulunanlar hakkında uygulanabilecek tanık koruma tedbirleri şunlardır:
a) Kimlik ve adres bilgilerinin kayda alınarak gizli tutulması ve kendisine yapılacak tebligatlara ilişkin ayrı bir adres tespit edilmesi.
b) Duruşmada hazır bulunma hakkına sahip bulunanlar olmadan dinlenmesi ya da ses veya görüntüsünün değiştirilerek özel ortamda dinlenmesi.
c) Tutuklu veya hükümlü olanların durumlarına uygun ceza infaz kurumu ve tutuk evlerine yerleştirilmesi.
ç) Fizikî koruma sağlanması.
d) Kimlik ve ilgili diğer bilgi ve belgelerin değiştirilmesi ve düzenlenmesi:
1) Adlî sicil, askerlik, vergi, nüfus, sosyal güvenlik ve benzeri bilgi ve kayıtlarının değiştirilmesi ve düzenlenmesi.
2) Nüfus cüzdanı, sürücü belgesi, pasaport, evlilik cüzdanı, diploma ve her türlü ruhsat gibi resmî belgelerin değiştirilmesi ve düzenlenmesi.
3) Taşınır ve taşınmaz mal varlığıyla ilgili haklarını kullanmasına yönelik işlemlerin yapılması.
e) Geçici olarak geçimini sağlama amacıyla maddî yardımda bulunulması.
f) Çalışan kişinin iş yerinin ya da iş alanının değiştirilmesi veya öğrenim görenin devam etmekte olduğu her türlü eğitim ve öğretim kurumunun değiştirilmesi.
g) Yurt içinde başka bir yerleşim biriminde yaşamasının sağlanması.
ğ) Uluslararası anlaşmalara ve karşılıklılık ilkesine uygun şekilde, geçici olarak başka bir ülkede yerleştirilmesinin sağlanması.
h) Fizyolojik görünümün estetik cerrahi yoluyla veya estetik cerrahi gerektirmeksizin değiştirilmesi ve buna uygun kimlik bilgilerinin yeniden düzenlenmesi.
(2) Bu maddede yazılı olan tedbirlerden biri veya birkaçı aynı anda uygulanabilir. Bununla birlikte aynı sonuç daha hafif bir tedbir ile elde edilebiliyor ise bu durum da göz önünde tutulur.
(3) Bu madde hükümlerine göre uygulanacak koruma tedbirlerinin esas ve usulleri yönetmelikte gösterilir."

korunmasına yönelik orantılılık (veri minimizasyonu) ilkesi ve daha az müdahale eden yöntemin uygulanması ilkesine aykırı bir müdahale teşkil etmektedir. Dolayısıyla, olması gereken görüntü ve ses alınmadan kayıt işleminin yapılmasıdır. Keza ifadede öğrenilmek istenen ifade verenin görüntüsü ve sesi değildir.

(3) Tanık koruma tedbiri kararı açısından

Cumhuriyet savcısı tarafından verilen tanık koruma tedbiri kararlarının isteminde mutlaka gerekçe gösterilmeli ve karara dayanak olabilecek hukukî ve fiilî nedenlere de yer verilmelidir[442]. Dolayısıyla, bu gerekçe içerisinde hangi kişisel verilerin hangi sebep ve şartla işlenmekte olduğuna ilişkin açıklama yapılması amaca bağlılık-amaçla sınırlanma ilkesi açısından gerekli olduğunu düşünmekteyiz.

Koruma kararının düzenlenmekte olduğu Yönetmelik m. 9'a göre, kararda tanık koruma tedbirlerinden biri veya birkaçının aynı anda uygulanabileceği öngörülmektedir. Aynı sonuç daha hafif bir koruma tedbiri ile elde edilebiliyorsa veya tedbirlerden birinin uygulanması aynı anda bir başka tedbirin uygulanmasını da zorunlu kılıyorsa, karar sürecinde bu hususlar da nazara alınacağı düzenlenmektedir. Dolayısıyla, daha az müdahale eden yöntemin uygulanması ilkesinin uygulama alanı bulduğunu belirtmek gerekmektedir.

(4) Tanıktan elde edilen delilin sadece ilgili davaya münhasır olma zorunluluğu açısından

Hem CMK hem de TKK'da elde edilen delillerin ilgili ceza muhakemesinde kullanılabileceği belirtilmektedir. Bu durumun verilerin amaca bağlılık-amaçla sınırlanma ilkesine uygun olduğu düşünülebilir. Fakat bunun sadece ilgili davada kullanılması şeklinde daraltıcı bir hüküm olarak düzenlenmesi kişisel verilerin korunmasına yönelik daha olumlu bir yaklaşım sunacaktır. Aksi halde var olan düzenlemeden, her ilgili ceza muhakemesinde kullanılabilir anlamı da çıkabilmektedir.

Ki Yönetmelik m. 19(5)'te, Cumhuriyet savcısı veya mahkemece verilen tanık koruma kararları ile diğer tutanak ve belgelerin, tanık hakkında yürütülen bir başka soruşturma veya kovuşturma konusu suçla ilgili olması hâlinde, diğer adlî mercilere gönderilebileceği belirtilerek kişisel veriler paylaşılması öngörülmektedir.

[442] TKK, m. 6.

Fakat bu verilerin farklı bir suçta kullanılabilmesi kişisel verilerin işlenmesinde amaçla bağlılık ilkesi ile bağdaşmamaktadır. Ayrıca bu durum TKK m. 10(3)'e de aykırıdır[443]. Belirtmek gerekir ki hem taleplerin hem de kararların muhafaza edilmesi kişisel verilerin depolanması anlamına geldiğinden kişisel verilerin korunması ilkelerine uygun olması gerekmektedir[444]. Dolayısıyla, Yönetmelik hükmü kişisel verilerin korunmasına yönelik ölçüsüz bir müdahale teşkil ettiğinden orantılılık (veri minimizasyonu) ilkesine, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine ve amaca bağlılık-amaçla sınırlanma ilkesine aykırılık teşkil edecektir.

(5) Delillerin depolanması, imhası veya anonimleştirilmesi açısından

TKK m. 8'de tanıkların şahsî hâllerinin eski hale getirilmesi halinde bunun şekli, süresi, sonuçları vb. işlemler ile diğer esas ve usuller yönetmelikte gösterileceği hükme bağlanmış olsa da kişisel verilerin imhasına ilişkin bir hüküm yer almamıştır. Hatta kişisel verilerin imhası, silinmesi ve anonimleştirilmesine ilişkin hükümler ne kanununda ne de yönetmelikte düzenlenmemiş olduğundan şu anda hakka yönelik orantısız ve öze dokunan bu yüzden de hukuka aykırı bir durum söz konusudur. Bu sebeple TKK kapsamında kişisel verileri işlenen ve saklanan kişilerin verilerinin ne olacağı belirsizdir.

Dolayısıyla bu açıdan var olan hükümlerin, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, orantılılık (veri minimizasyonu) ilkesi ve sınırlı süre saklanma ilkesine aykırı olduğu ortadadır. Hukuka aykırı bu durumu ortadan kaldırabilmek için kanun koyucunun pozitif yükümlülüğü çerçevesinde gerekli düzenlemeleri yapması gerekmektedir.

(6) Tanığa ilişkin hükümlere hâkim olan gizlilik ilkesi açısından

Tanık Koruma Kanunu'n hâkim olan temel ilke gizliliktir. Kanun m. 10'da, tanığın gerçek kimlik ve adres bilgileri ile koruma kararının ayrı bir kartonda muhafaza edileceği ve

---

[443] Zikredilen TKK m. 10(3) hükmü şu şekildedir:
"… (3) Cumhuriyet savcısı, mahkeme veya hâkim tarafından bu Kanunda belirtilen işlemlerle ilgili olarak bir zabıt kâtibi görevlendirilir. Tanık koruma tedbirlerinin uygulanmasına ilişkin karar ve diğer belgeler, soruşturma evresinde Cumhuriyet başsavcılığınca, kovuşturma evresinde mahkemece bu kararlara mahsus yerlerde gizlilik esaslarına uygun olarak saklanır. Cumhuriyet başsavcılığınca veya mahkemece tanık koruma tedbirinin uygulanmasına ilişkin verilen karar ve diğer belgeler, soruşturma veya kovuşturma konusu suç dışında başka bir makam veya mercie gönderilemez. …"

[444] Depolama ile ilgili Yönetmelik'te farklı örnekler de bulunmaktadır. Bakınız m. 11(8), (9), (10), m. 13(2), 14(2), 15(4), 16(5),

saklanmaya ilişkin esas ve usullerin yönetmelikte gösterileceği düzenlenmektedir[445]. Bu hususun özellikle incelenmesi gerekmektedir keza burada kişisel verilerin saklanarak depolanması söz konusudur.

Yönetmelik m. 12(4) uyarınca, tanığın duruşma salonu dışında telekonferans, video konferans veya diğer sesli ya da görüntülü iletişim araçları ile özel bir ortamda dinlenmesi sırasında sesi veya görüntüsü değiştirilebilmektedir. Bu hâlde kimliğinin doğrulanabilmesi bakımından tanığın gerçek ses ve görüntüsü de kaydedilmektedir. Tanığın korunmasına yönelik talepler, kararlar ve diğer tüm belgeler, özel bir kasada saklanmak üzere Cumhuriyet başsavcılığı veya mahkemelerce tutulan ilgili kartonda gizlilik esasları çerçevesinde muhafaza edilmektedir.

TKK m. 18'de ayrı bir hüküm olarak düzenlenen gizlilik kuralı açısından gizliliğin tedbir sona erdikten sonra da devam edeceğini belirtmek gerekir. Hatta koruma kararlarının alınmasında ve uygulanmasında yer alan kişiler, bu görevleri nedeniyle öğrendikleri bilgileri görev sona erdikten sonra da açıklayamamaktadırlar. Kişisel verilere ilişkin

---

[445] Kimlik ve adres bilgilerinin gizlenmesi tedbiri hükmü Yönetmelik m. 11'de düzenlenmektedir:
"(1) Cumhuriyet savcısı veya mahkeme tarafından korunmasında zorunluluk bulunduğu re'sen veya istem üzerine belirlenen tanıkların kimlik ve adres bilgileri gizli tutulur.
(2) Tanığın kimlik ve adres bilgilerinin gizli tutulmasında zorunluluk bulunduğunun kolluk birimleri tarafından belirlenmesi hâlinde, durum vakit geçirilmeksizin ilgili Cumhuriyet savcısına bildirilir ve bu konuda bir karar verilinceye kadar tanığın kimlik ve adres bilgilerinin açığa çıkmasını engelleyecek her türlü tedbir alınır.
(3) Cumhuriyet başsavcılığı veya mahkemeye yapılacak olan kimlik ve adres bilgilerinin gizli tutulmasına ilişkin talepler, tanık koruma defterine kaydedilir ve uygun görülmesi hâlinde tanık için yeni bir kod isim ve adres belirlenmesine karar verilir. Bu karar ile ekli yeni kimlik ve adres bilgilerine ilişkin tutanak, ilgili Cumhuriyet savcısı veya hâkim ile görevli zabıt kâtibince imzalanarak tanık koruma kartonunda gizlilik esasları çerçevesinde muhafaza edilir.
(4) Tanığın soruşturma veya kovuşturma evrelerindeki beyanlarının tamamı koruma kararında belirtilen kod isimle tutanaklara kaydedilir ve sonraki tüm işlemlerin de bu isimle yürütülmesi sağlanır.
(5) Tanığın çağrılması, Cumhuriyet savcısı veya mahkeme tarafından tanığın gösterdiği veya re'sen belirlenecek bir adrese ilgili koruma veya kolluk birimi marifetiyle yapılır.
(6) Talebinin bulunması ve uygun görülmesi hâlinde tanığa telefon, telgraf, faks veya elektronik posta gibi araçlardan yararlanılmak suretiyle de çağrı yapılabilir.
(7) Çağrı için belirlenen adres, telefon veya diğer iletişim bilgilerinin herhangi bir nedenle değişmesi hâlinde, bu durum kararı veren merci ile kolluk veya koruma birimine derhâl bildirilir.
(8) Cumhuriyet savcısı veya mahkemeye gönderilen evraktaki tanığın gerçek kimlik ve adres bilgileri, koruma kararındaki bilgilerle değiştirilir ve ihtiyaç hâlinde kolluktaki beyanlarının bir sureti hiçbir adres bilgisi içermeyecek şekilde sadece kod isimle soruşturma veya kovuşturma dosyasına konulur.
(9) Cumhuriyet savcısı veya mahkemece düzenlenen tutanaklar ile verilen kararların içeriğinde kimlik ve adres bilgisi gizlenen tanığın beyanlarına yer verilmesi gereken durumlarda, ilgili tutanak veya kararda tanığın kod ismi dışında hiçbir kimlik ya da adres bilgisine yer verilmez.
(10) Kimlik ve adres bilgilerinin gizli tutulmasına karar verilen tanığın, bu karar öncesinde aynı olay sebebiyle kollukta alınmış ifadeleri olduğunun anlaşılması hâlinde, evrak aslı ve varsa suretleri, mevcut kayıtlara şerh verildikten sonra kollukta hiçbir evrak kalmayacak şekilde ilgili Cumhuriyet savcısı ya da mahkemeye gizlilik esasları çerçevesinde teslim edilir ve evrak ilgili kartonunda saklanır."

gizliliğin sağlandığı hukuka uygun bir işlemenin varlığı için soruşturma evresinde kişisel verilerin korunmasına ilişkin garantiler yer almalıdır. Bu doğrultuda, soruşturma evresinde Cumhuriyet başsavcılığınca yapılacak bu işlemlerle kişisel veri barındıran bu hususlarla ilgili hükmün var olması, veri güvenliği(bütünlük ve gizlilik) ilkesi açısından olumludur.

(7) Diğer hususlar

TKK m. 11'e göre, tanık koruma biriminde çalışan personel için geçici kimlik düzenlenebilmekte veya bunu sürdürebilmesi için belge verilebilmektedir. Bu belgelerin, tanığın korunması ile gözetilen kamu yararı veya somut diğer olgular da dikkate alınarak, soruşturma konusuyla orantılı ve amaca uygun olarak kullanılabileceği düzenlenmektedir.

İfade etmek gerekir ki bu veriler, ilgili kamu görevlilerinin kişisel verisi olduğundan verilerin işlenmesi prensipleri doğrultusunda koruma kapsamında yer almalıdırlar. Ayrıca kanunun amaca uygunluğu açıkça ifade etmesi sebebiyle verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi ve amaca bağlılık-amaçla sınırlanma ilkesi doğrudan uygulama alanı bulacaktır.

Yönetmelik m. 19(6)'ya göre, koruma kararları ve diğer belgeler, talep hâlinde hiçbir sınırlamaya bağlı olmaksızın Tanık Koruma Kurulu'na gönderilmektedir. Bu hüküm kişisel verilerin korunması açısından dengeli değildir. Son olarak belirtmek gerekir ki, TKK m. 15 uyarınca imzalanacak mutabakat metninin kişisel verilerin korunması ilkelerine uygun olmasına dikkat edilmelidir.

Kanun ve yönetmelik birlikte düşünüldüğünde belirtmek gerekir ki, kişisel verilerin korunmasına ilişkin ilke ve hakların yer aldığı yeterli düzenlemeler maalesef Türk hukukunda düzenlenmemiştir. Ayrıca, soruşturma evresinin tamamen KVK Koruması kapsamından çıkarılmış olması sebebiyle hassas veriler ile ilgili tanık açısından sır tutma yükümlülüğü altında bulunan kişilerin davranışlarına yönelik hangi normun uygulanacağı akıllarda soru işaretlerine yol açabilecektir.

Bunun dışında son olarak CMK m. 62 ila 73 hükümlerinde düzenlenen bilirkişiye ilişkin kurallara değinmek gerekir. Buna göre kanunda aksi düzenlenmediği müddetçe tanıklara ilişkin hükümler bilirkişiler hakkında da uygulanacağından tanık ile yaptığımız yorumlar

bilirkişi açısından da geçerlidir. Buna göre bilirkişi raporunda bir kişiyi belirlenebilir kılan ve soruşturma konusu suç ile bağlantılı olmayan kişisel verilerin anonimleştirilmesi kaydıyla yer alabileceğini belirtmek gerekmektedir. Fakat soruşturma evresinde verilerin işlenmesine hâkim olan ilkeler ve ilgili kişinin hakları doğrultusunda düzenlemelerin güncellenmesi ve detaylandırılması gerekmektedir.

2. Vücut ve cinsel dokunulmazlığa müdahale eden yöntemler ile kişisel veri elde edilmesi

a) Gözlem altına alınma yöntemi ile kişisel veri elde edilmesi

CMK m. 74'te gözlem altına alınmaya ilişkin hükümler düzenlenmektedir. Buna göre, fiili işlediği yolunda kuvvetli şüpheler bulunan şüpheli veya sanığın akıl hastası olup olmadığını, akıl hastası ise ne zamandan beri hasta olduğunu ve bunun, kişinin davranışları üzerindeki etkilerini saptamak için resmî bir sağlık kurumunda gözlem altına alınmasına karar verilmektedir.

Yargılamanın durmasına sebep olan bu kararı, soruşturma evresinde sulh ceza hâkimi vermektedir. Gözaltı kararından ve beden muayenesi tedbirinden tamamen farklı olan bu tedbir kararının alınmasından önce uzman hekimin bu yönde önerisinin olması gerekmektedir. Ayrıca bu karar öncesinde yine Cumhuriyet savcısının ve müdafinin dinlenmesi de şarttır. Bir görüşe göre bu tedbire ilişkin kararın verilmesinde CMK m. 100/1 hükmü kıyasen uygulanmalı ve verilecek ceza ve güvenlik tedbirleri ile orantılı değilse ilgili makamın bu yönde bir karar vermemesi gerekmektedir[446].

Kişisel verilerin korunması açısından belirtmek gerekir ki, verilerin nasıl elde edileceği, işleneceği ve paylaşılacağına ilişkin bu tedbir açısından herhangi bir düzenleme mevcut değildir. Fakat gözlem altında olan süreç içerisinde elde edilecek verilerin özel hayat verisi olmasının yanı sıra bir kişiyi belirli kılabilecek verilerin olması halinde bu verilerin kişisel veri olacağı üzerinde şüphe yoktur.

Dolayısıyla kişisel verilerin korunması kapsamındaki ilkelere dayanan güvencelere sahip olması gerekmektedir. Bu yüzden, kişisel veriler üzerinde gizlilik kararı bulunmalı ve

[446] Keçelioğlu, Elvan: "Ceza Muhakemesi Hukukunda Gözlem Altına Alma", Ankara Barosu Dergisi, 3, Ankara 2015, s. 239.

soruşturulan suç kapsamı içerisinde yer almadığı takdirde ya anonimleştirilmeli ya da imha edilmelidir. Bu gereklilik amaçla bağlılık ilkesinin bir sonucudur.

b) Şüpheli, sanığın veya mağdurun beden muayenesi ve vücudundan örnek alınması yöntemleri ile kişisel veri elde edilmesi

(1) Genel olarak

CMK m. 75'de şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınmasına ilişkin hükümler düzenlenmektedir. Buna göre, bir suça ilişkin delil elde etme amacıyla şüpheli veya sanık üzerinde iç beden muayenesi yapılması ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınması mümkündür. Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik m. 3'e göre iç beden muayenesi, kafa, göğüs ve karın boşlukları ile cilt altı dokularının incelenmesini ifade etmektedir.

CMK m. 75 ve Yönetmelik m. 4 uyarınca şüpheli/sanık üzerindeki müdahalede sadece kişinin sağlığına açıkça ve öngörülebilir zarar verme tehlikesinin bulunmaması gerekmektedir. Buna ilişkin karar, Cumhuriyet savcısı veya mağdurun istemi sonucu hâkim veya mahkeme tarafından resen verilmektedir. Gecikmesinde sakınca bulunan hâllerde ise Cumhuriyet savcısı tarafından resen karar verilebilmektedir fakat bu karar mahkemece onaylanmazsa hükümsüz kalmakta ve elde edilen deliller kullanılamamaktadır. Ayrıca üst sınırı iki yıldan daha az hapis cezasını gerektiren suçlarda iç beden muayenesi işlemi yapılamamaktadır. Bu suçlarda dış beden muayenesi yapılabiliyor olsa da kişiden kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınamamaktadır.

CMK m. 76'da ise bu sefer mağdurun beden muayenesi ve vücuttan örnek alınmasına ilişkin hükümler düzenlenmektedir. Buna göre, bir suça ilişkin delil elde etmek amacıyla, mağdurun vücudu üzerinde dış veya iç beden muayenesi yapılabilmesine veya vücudundan kan veya benzeri biyolojik örneklerle saç, tükürük ve tırnak gibi örnekler alınabilmektedir. Yönetmelik m. 3'e göre, dış beden muayenesi, vücudun dış yüzeyi ile kulak, burun ve ağız bölgelerinin gözle ve elle yapılan yüzeysel tıbbî incelemesini ifade etmektedir.

Bu işlemin temel koşulu kişinin sağlığını tehlikeye düşürmemek ve cerrahî bir müdahalede bulunmamaktır. Bu işleme ilişkin karar, Cumhuriyet savcısının istemiyle ya da re'sen hâkim veya mahkeme tarafından verilmektedir. Gecikmesinde sakınca bulunan hâllerde ise Cumhuriyet savcısı tarafından resen karar verilebilmektedir fakat bu karar mahkemece onaylanmazsa hükümsüz kalmakta ve elde edilen deliller kullanılamamaktadır.

Burada m. 75'ten farklı olarak dış muayene de yapılabileceğine dikkat edilmelidir. Yine başka bir fark olarak, olarak mağdur üzerinde cerrahî bir müdahalede bulunmak mümkün değilken, şüpheli/sanık üzerinde bu işlem kural olarak yasaklanmamıştır.

Alınan örneklerin kişisel sağlık verisi olarak hassas veri olduğu üzerinde şüphe bulunmamaktadır. Bu tedbirler ile kişi delil vermeye zorlandığından temel hak ve hürriyetlere yönelik muayene ve örnek alımına ilişkin hükümlerin yönetmelikle değil kanunla düzenlenmesi gerekmektedir[447].

Üstelik CMK m. 75'te şüphelinin/sanığın muayenesi ve örnek alımı için karar alınması gerektiği açıkça hükme bağlanmış ve rıza bir istisna olarak düzenlenmemişken, Yönetmelik m. 18(3)'de şüpheli/sanığın rızasının varlığı halinde karar alınmadan da alınmasına gerek olmadığına yer verilmesi hakkın kanunla değil yönetmelikle sınırlandığını göstermektedir. Anayasal bir hak olan kişisel verilerin gizliliğine yönelik bu sınırlamanın kanunla yapılmaması nedeniyle Anayasa m. 13 hükmüne aykırı bir durum ortaya çıkmaktadır. Aynı zamanda bu çerçevede, kişilerin yetkili merci kararı olmaksızın kendi rızaları çerçevesinde alacakları beden muayenesine ilişkin raporların soruşturma açısından uzman mütalaası hükmünde olacağı, hukuka uygunluk sebebi olarak ilgilinin rızasının varlığı sebebiyle TCK m. 287'de düzenlenen genital muayene suçunun oluşmayacağı belirtilmektedir[448].

CMK m. 76(4)'e göre, tanıklıktan çekinme sebepleri ile muayeneden veya vücuttan örnek alınmasından kaçınılabilmektedir. Yönetmelik m. 10 uyarınca da, çocuk ve akıl

[447] Apiş, Özge: "Ceza Muhakemesi Hukukunda Şüpheli/Sanığın Beden Muayenesi ve Vücudundan Örnek Alınması", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 18/1, İstanbul 2012, s. 292.

[448] Eroğlu, F. 2009. *Beden Muayenesi Ve Vücuttan Örnek Alma Suretiyle Elde Edilen Delillerin İspat Değeri*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Yeditepe Üniversitesi, Sosyal Bilimler Enstitüsü, s. 54.

hastasının çekinmesi konusunda kanunî temsilcisi karar vermektedir. Eğer kanunî temsilci şüpheli veya sanık ise bu konuda hâkim tarafından karar verilmektedir. Ancak, bu hâlde elde edilen deliller davanın ileri aşamalarında şüpheli veya sanık olmayan kanunî temsilcinin izni olmadıkça kullanılamayacaktır.

Bir görüşe göre, çocuğa ait hassas verilerin işlenmesinde çocuğu korumak için mümkün olan her yol göz önünde bulundurulmalı ve hem verilerinin gizliliği hem de çocuğun verileri üzerinde kendi kararını verebilmesi için on sekiz yaşından sonra öğrenebileceği şekilde güvence sağlanmalıdır[449].

Belirtmek gerekir ki şüpheli/sanık için sadece iç; mağdur için ise iç ve dış beden muayenesinin düzenlenmekte olduğu CMK m. 75 ve 76 hükümleri kapsamında şüpheli, sanık ve mağdurdan elde edilecek tüm veriler kişisel veridir. Dahası bu veriler, hassas nitelikli sağlık verisi sınıfına girmekte olup daha fazla koruma altına alınmaktadırlar. Bu doğrultuda, orantılılık ilkesi gereğince beden muayenesi sonucunda elde edilecek kişisel verilerin soruşturma evresine yapacağı katkı ile verilecek zararın arasında yararın zarardan daha fazla olması gerekmektedir[450].

Bunun dışında, Yönetmelik m. 9'da çocuğun soy bağının araştırılmasına ilişkin bir hüküm düzenlenmektedir. Buna göre, çocuğun soy bağının araştırılmasına gerek duyulması hâlinde, bu araştırmanın yapılabilmesi için, mağdurun ve diğer kişilerin beden muayenesi ve bu kişilerin vücudundan örnek alınmasına ilişkin hükümlere göre karar alınması gerekli olduğu belirtilmiştir. Bu doğrultuda elde edilecek verilerin çocuğun ırkı ya da etkin kökenine ilişkin olacağından bu verilerin de hassas veri olabileceğini belirtmek gerekir.

Son olarak, Yönetmelik m. 10'a göre, tanıklıktan çekinme sebepleri ile muayeneden veya vücuttan örnek alınmasından kaçınılabileceği düzenlenmektedir. Tanıklıktan çekinme sebeplerinin belirlenmesi hususunda CMK'nın ilgili hükümlerinin uygulanacak olmasının yanı sıra çocuk ve akıl hastasının çekinmesi konusunda kanunî temsilcisi karar verecektir. Çocuk veya akıl hastasının, tanıklığın hukukî anlam ve sonuçlarını

[449] Thompson, Ross A. (Institute of Medicine, Division of Health Care Services, Committee on the Role of Institutional Review Boards in Health Services Research Data Privacy Protectio): Protecting Data Privacy in Health Services Research, Washington 2001, s. 168.
[450] Eroğlu, F., s. 47.

algılayabilecek durumda olması hâlinde, görüşü de alınmaktadır. Kanunî temsilci de şüpheli veya sanık ise bu konuda hâkim tarafından karar verileceği ancak, bu hâlde elde edilen deliller davanın ileri aşamalarında şüpheli veya sanık olmayan kanunî temsilcinin izni olmadıkça kullanılamayacağı belirtilmektedir.

İfade etmek gerekir ki, bu son hüküm suiistimale açıktır. Söz konusu veriler çocuğun kişisel verileri olacağından kanuni temsilcinin olaya tam bağımsızlıkla ve çocuğun menfaati açısından yaklaşması gerekmektedir.

(2) Kişinin muayeneye yahut örnek alınmasın rıza göstermemesi problemi

Adli soruşturma altında olan bir kişinin kendisi aleyhinde delil vermeye zorlanmaması insan hakları gereğincedir. Fakat delil toplama süreci boyunca şüpheli ve mağdur üzerinden suçun aydınlatılması için kendi vücudundan delil alınması gerekli görülebilmektedir. Bu gereklilik sebebiyle, kendisinden delil elde edilecek kişinin katlanma yükümlülüğü doğmaktadır.

Katlanma yükümlülüğü, suç delillerinin ele geçirilmesi amacıyla kişilerin temel hak ve özgürlüklerine müdahale yapılması zorunluluğuna yönelik kişilerin karşı koymamasını ifade eder[451].

Kişilerin rızaları aleyhine delil vermeye zorlanması ise tartışma konusudur. Bazı yazarlar, kişiler üzerinde tatbik edilen yöntemlerle temel hak ve hürriyetlerinin kısıtlanmasını, kısıtlamanın kanunen yapılması ve meşru sebeplere hizmet etmesi nedeniyle hukuka uygun bulmaktadır. Karşıt görüşteki yazarlar ise, kişiden cebren delil niteliğindeki verilerini elde etmenin insan onuru ile bağdaşmayacağını belirtmektedirler. Bazı yazarlar ise, kanunen meşru sebepler çerçevesinde yapılacak sınırlamada orantılılığa ve insan onuruna dikkat edilmesi kaydıyla temel hak ve hürriyetlere istisna getirilebileceğini belirtmektedirler.

Bu doğrultuda, Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik m. 18'de şüpheli, sanık veya mağdurun beden muayenesi yapılmasında ilgili kişi olarak rızaları düzenlenmiştir. Buna göre, kanun

[451] İnci, Z. Özen: "Şüpheli ve Sanığa Rağmen Bir Ceza Muhakemesi Hukuku Mu? Şüpheli ve Sanığın Ceza Muhakemesi İşlemlerine Katlanma Yükümlülüğü ve Bu Yükümlülüğün Sınırları Hakkında Düşünceler", Hacettepe Hukuk Fakültesi Dergisi, 7/2, Ankara 2017, s. 122.

gereği şüpheli sanık veya diğer kişilerin aydınlatılmış olmalarına rağmen muayene yapılmasına ya da örnek alınmasına rıza vermemeleri hâlinde, kararın infazı için ilgilinin muayenesini veya vücudundan örnek alınmasını sağlamak üzere ilgili Cumhuriyet başsavcılığınca gerekli önlemler alınacağı hüküm altına alınmıştır[452].

İfade etmek gerekir ki zikredilen gerekli önlemlerle neyin kastedildiği anlaşılmamaktadır. Bu doğrultuda kişinin narkoz etkisi altında iken genital muayeneye tabi tutulması gibi rıza dışı örneklerle karşılaşılabilecek oluşu hem insan onuruna aykırı olması hem de hatalı sonuçların ortaya çıkacak olması sebebiyle eleştirilmekte, bunun yerine rızanın verilmediği durumlarda ikinci bir hâkim kararı alınarak tedbirin uygulanma zorunluluğunun bir kez daha gözden geçirilmesi önerilmektedir[453].

Ayrıca beden muayenesi ve vücuttan örnek alınmasına verilecek rızanın ceza muhakemesi açısından tartışmalı olduğunu da ifade etmek gerekir. Öncelikle CMK'nın ikili bir ayırım yaptığımı belirtilmelidir. CMK, şüpheli/sanık söz konusu olduğunda rızayı aramamakta ve hâkim veya savcı kararını yeterli görmektedir. Burada rıza olsa bile hâkim ve savcı kararına gereksinim söz konusudur[454].

Fakat mağdur bakımından ise öncelikle rıza aranmakta olup rızanın yokluğu halinde hâkim ve savcı kararı ile beden muayenesi ve vücuttan örnek alınmasını mümkün kılınmaktadır. Her ne kadar mağdurun rızası hilafına muayeneye tabi tutulması ikinci bir mağduriyete yol açabileceği düşünülecek olsa da, delil vermemesi için tehdit edilen mağdurların muayeneye razı olmadığı durumlarda söz konusu olabilecektir. Bu noktada bir görüşe göre, mağdurun rızası olmasa bile hâkim ve ya savcı kararıyla kişinin bedeni üzerine muayene suretiyle delil elde edilmesine olanak tanımak gerekmektedir[455].

---

[452] İlgilinin rızasına ilişkin hükümler Yönetmelik m. 18'de düzenlenmektedir:
"Mevzuatta aranan tüm koşulların gerçekleşmiş olmasına ve şüpheli sanık veya diğer kişilerin bu konuda aydınlatılmış olmalarına rağmen muayene yapılmasına ya da örnek alınmasına rıza vermemeleri hâlinde, kararın infazı için ilgilinin muayenesini veya vücudundan örnek alınmasını sağlamak üzere ilgili Cumhuriyet başsavcılığınca gerekli önlemler alınır.
Mağdurun rızasının varlığı hâlinde bu işlemlerin yapılabilmesi için Yönetmeliğin 7 nci ve 8 inci maddeleri uyarınca karar alınmasına gerek yoktur. Bir suçun aydınlatılmasını sağlamak amacıyla, şüpheli, sanık ve diğer kişilerin kendiliğinden başvurarak rıza göstermeleri hâlinde, soruşturma evresinde Cumhuriyet savcısının istemi, kovuşturma aşamasında ise hâkim veya mahkeme kararıyla tıbbî muayeneleri yapılabilir ya da vücutlarından örnek alınabilir."
[453] Yenisey/Nuhoğlu, s. 624.
[454] Ünver/Hakeri, s. 279.
[455] Ünver/Hakeri, s. 280.

Her iki halde de rızanın yokluğu durumunda, aleyhe delil vermeme ilkesine aykırı olarak, kişilerden cebren örnek alınmakta yani kişilerin verileri işleme tabi tutulmaktadır. Beden muayenesi tıbbi bir müdahale olup, elde edilen veriler kişiyi tanımlanabilir kılıyorsa hassas nitelikli kişisel sağlık verisi niteliğinde olup daha fazla korunmaya muhtaç olmalarıdır. Bazı yazarlara göre, Anayasa'ya göre kişinin vücuduna rızası olmaksızın müdahale edilmemesine kanunla istisna getirilebileceği mümkün olduğundan, kişinin rızası hilafına yapılan muayene ve elde edilen delil niteliğindeki veriler hukuka uygundur[456].

c) Moleküler genetik incelemeler yöntemi ile kişisel veri elde edilmesi

CMK m. 78'e göre, şüpheli, sanık veya mağdur üzerinde yapılacak iç veya dış muayene işlemleri ile elde edilen örnekler üzerinde, soy bağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması hâlinde moleküler genetik incelemeler yapılabilmektedir. Moleküler genetik incelemeler yapılmasına ise sadece hâkim karar verebilmektedir.

Belirtmek gerekir ki, bu madde kapsamında elde edilecek tüm moleküler inceleme verilerinin hassas nitelikli kişisel veri olacağı şüphesizdir. Keza Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik m. 14'te, örnekler üzerinde yapılan inceleme sonuçlarının kişisel veri niteliğinde olduğu belirtilmektedir. Dolayısıyla, kişiden alınan örnekler üzerinde amaçla bağlılık ilkesi gereğince öngörülen amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır.

Öte yandan, maddenin ikinci fıkrasına göre, moleküler biyolojik incelemeler kime ait olduğu belli olmayan beden parçaları üzerinde de yapılabilmektedir. Söz konusu parçaların kimin olduğu bilinmediğinden bu nesneler üzerinde yapılacak inceleme sonucunda bir kişiyi ayırt edici bilgi verdiği takdirde bu bilgi ve parça da kişisel veri statüsüne girecektir. İnceleme sonucu bir kişiyi belirli kılmıyorsa o halde alınan bu anonim örnekler üzerinde, ilgili amaç doğrultusunda işleme yapılabilir fakat bu amaçlar dışında tespitler yapılmasına yönelik incelemeler de yasaktır.

Ayrıca, CMK m. 79(2)'ye göre yapılacak incelemeler için bilirkişi olarak görevlendirilecek kişiler, teknik ve teşkilât bakımından uygun tedbirlerle yasak moleküler

[456] Ünver/Hakeri, s. 280.

genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdürler. İncelenecek bulgu, bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilmesi gerekmektedir. Burada kanun koyucu moleküler verilerin hassaslığı sebebiyle ek güvenceler getirmiş, veri sahibinin kimliğinin gizlenmesini gerekli görmüştür.

Bu doğrultuda, Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik m. 14'te de bulgular üzerinden moleküler genetik analizler için izole edilen DNA örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edileceği düzenlenmiştir. Bu, amaca bağlılık-amaçla sınırlanma ilkesi ve sınırlı süre saklanma ilkesinin bir gereğidir.

Bilirkişi açısından son olarak, yine m. 14'te moleküler genetik incelemelerin özel kalıtsal karakterler hakkındaki açıklamayı içermediği bilinen kromozom bölgesi ile sınırlı kalmasına özen gösterileceği düzenlenmiştir. Burada da amaca bağlılık-amaçla sınırlanma ilkesi, daha az müdahale eden yöntemin uygulanması ilkesi ve orantılılık (veri minimizasyonu) ilkesinin göz ardı edilmediği görülmektedir.

Öte yandan, Türkiye'de hali hazırda yürürlükte olan DNA bankasına ilişkin bir kanun olmadığından DNA verilerinin depolanacağı bir bankanın varlığından bahsedebilmek mümkün değildir. Yasal korumanın yokluğu sebebiyle, kişi hak ver hürriyetlerini ihlal etmeyecek özel bir düzenleme yapılmasının ve ayrıca bu konuda bir üst etik yapılanmasının gerekli olduğu belirtilmektedir[457]. Ayrıca bu gereklilik, kişinin kimliğini tespite yarayan DNA gibi yasal veri tabanlarının bulunmaması nedeniyle özellikle kolluğun delile ulaşmak için çok zaman harcamaması ve bunun da soruşturma dosyasına yansımaması için de geçerlidir[458].

Bu konudaki kuralları düzenleyen fakat yürürlüğe henüz girmemiş olan DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı bulunmaktadır. Tasarı m. 5'e göre, DNA analizi, CMK çerçevesinde vücuttan kim olduğunu tespit etmek amacıyla, hukukî

[457] Aslanova, Kemale (Bozkurt Yüksel, Armağan Ebru/Bak, Başak/Yüksel, Sera Reyhani): Futurist Hukuk, İstanbul 2018, s. 60.
[458] Karabulut, Ferhat/Karapazarlıoğlu, Ersin/Tosun, Hamza: Ceza Muhakemesinde Delil Kavramı ve Kovuşturma Sürecinde Hâkimlerin Delil Algısı", Türkiye Barolar Birliği Dergisi, 120, Ankara 2015, s. 413.

ve fiilî sebeplerle kimliği tespit edilemeyen kişiler ile vücut parçalarından ve ölmüş kişilerden alınan biyolojik örnekler üzerinde yapılabilecektir.

Bu Tasarı m. 8 hükmüne göre ise, banka bünyesinde kayıtlı olan DNA profillerinden soruşturmada gerçeğin ortaya çıkarılabilmesi veya kimlik tespiti amacıyla yararlanılabilecektir. Tasarı m. 10'da bu doğrultuda soruşturma evresinde kim olduğunu tespit etmek amacı ile vücut parçalarından ve ölmüş kişilerden alınan biyolojik örnekler üzerinde yapılan işlem sonuçlarının ilgili adli merciine yollandıktan sonra hemen imha edileceği düzenlenmektedir. Tasarı m. 10(2)'ye göre ise, bir suç sebebiyle olay yerinden alınan biyolojik örnekler üzerinde yapılan DNA analiz sonuçları en az beş yıl saklanacaktır. Bu bilgiler, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilecektir.

Dolayısıyla bu açıdan kişi cezaya mahkûm olduğu takdirde DNA bilgilerinin depolanmasında alt sınır belirlenmesinde karşın üst sınır belirlenmemektedir. Doktrinde, CMK'daki tedbirlerin sınırlı olarak uygulanmakta oluşu sebebiyle özellikle beraat hali ve diğer hallerin ayrılması ve bir suçtan beraat eden kişinin herhangi bir verisinin tutulmaması gerektiği belirtilmektedir[459].

Ayrıca belirtmek gerekir ki, hem CMK m. 80 hem de Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik m. 14(2) düzenlemesi uyarınca, mahkûmiyet kararı verilmesi halinde inceleme sonuçlarının yok edilmesi zorunluluğu bulunmamaktadır. Masumiyet karinesini zedeleyen bir düzenleme olmasının yanı sıra buradan çıkarılacak anlam aslında ülkemizde DNA bankalarının kurulmuş olduğudur[460]. Çünkü DNA'ya ilişkin hassas veriler hiçbir işleme ilkesi ve sınırına tabi olmadan ilgili hükümlerin getirilmemiş olması sebebiyle oluşturulan belirsizlik sayesinde depolanmaktadır.

Hiç şüphesiz bu durum kişisel verilerin korunması hakkına yönelik orantısız ve haksız bir müdahaleyi teşkil eder. Bu konuda verilerin depolanmasına ilişkin olarak kanuni düzenlemeler yapılmalı ve depolanacak verilerin tasnifine, depolanması kriterlerine, kayıt altında kalacağı sürelere, veriler üzerinde yapılabilecek işlemlere ve bu işlemlerin

[459] Küzeci, s. 436.
[460] Parlar/Çetin, s.775.

kimlerin hangi sürelerle sahip olacakları yetkiler ile yapabileceklerine ilişkin detaylı hükümler yer almalıdır.

Bu açıdan kişisel verilerin korunmasına ilişkin genel ilkeler, DNA verilerinin saklanmasında uygulama alanı bulmalı ve bu doğrultuda amaçla bağlılık ilkesi ve masumiyet karinesi saklama politikalarına hâkim olmalıdır. Çünkü veri bankalarının kurulma sebebindeki amaç adli olayların aydınlatılmasına yardımcı olmaktır. Fakat ceza veya güvenlik tedbirlerine mahkûmiyet ya da düşme kararı verildikten sonra bu bilgiler saklanacak olursa amacın dışına çıkılmış olur[461]. Ayrıca, sürenin uzunluğu sebebiyle verilerin doğruluğu, sınırlı süre saklanma ve ölçülülük ilkeleri ihlal edilmiş olacaktır.

d) Fizik kimliğin tespiti yöntemi ile kişisel veri elde edilmesi

(1) Genel olarak

CMK m. 81'de düzenlenen fizik kimliğin tespiti, şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntülerinin kayda alınması işlemidir.

Fizik kimliğin tespiti bağlamında madde hükmü açısından önemli olan bir nokta şüphelinin işlediği şüphesi altında olduğu suçun aydınlığa kavuşturulabilmesi için fiziksel kimliğinin teşhisinin gerekli olması şartıdır. Buna göre, kişisel veri işleme amaçlarının savcılık tarafından bir veri sahibinin teşhis edilmesini gerektirmemesi veya artık buna gerek kalmaması halinde savcılık kişiyi teşhis etmek üzere ek bilgi tutmak, elde etmek veya işlemek zorunda değildir[462].

Bir diğer önemli nokta ise, bu tedbirin uygulanabilmesi için üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suç şüphesi ve Cumhuriyet savcısının emrinin

---

[461] Aydın, s. 105.

[462] Teşhis gerektirmeyen işleme faaliyeti hükmü GDPR m. 11'de düzenlenmektedir:
"1. Bir kontrolörün kişisel veri işleme amaçlarının kontrolör tarafından bir veri sahibinin teşhis edilmesini gerektirmemesi veya artık buna gerek kalmaması halinde, kontrolör yalnızca bu Tüzük'e uygunluk sağlamak amacıyla veri sahibini teşhis etmek üzere ek bilgi tutmak, elde etmek veya işlemek zorunda değildir.
2. Bu maddenin 1. paragrafında atıfta bulunulan hallerde, kontrolörün veri sahibini teşhis edecek bir konumda bulunmadığını gösterebilmesi durumunda, kontrolör, mümkün olması halinde, veri sahibini bu durumdan haberdar eder. Bu durumlarda, 15 ila 20. maddeler, veri sahibinin bu maddeler kapsamındaki haklarını kullanmak amacıyla teşhis edilmesine olanak tanıyan ek bilgiler sağlaması haricinde, uygulanmaz."

gerekmekte olmasıdır. Fakat üst sınırın iki yıl ya da daha fazla belirlenmiş olması, esasen kişisel verilerin korunması açısından bir anlam ifade etmemektedir. Keza TCK'da düzenlenen suçların çoğunun üst sınırı iki yıl ya da daha fazladır.

(2) Elde edilen verilerin büyük ölçüde hassas nitelikli kişisel veri olması

Fizik kimliğin tespiti işleminde kişisel verilerin korunması açısından öne çıkan bazı hususlar bulunmaktadır. Bunlardan birincisi, bu işlem sonucu elde edilecek tüm verilerin, bir kişiyi doğrudan belirlenebilir kılacak olan veriler olması sebebiyle bu verilerin kişisel veri ve bazı verilerin de hassas veri kapsamında olacağıdır.

Bu doğrultuda kişisel verilerin korunmasına ilişkin genel ilkeler başta olmak üzere verilerin işlenme şartlarına dair güvencelere haiz olması gerekmektedir. Doktrinde, temel hak ve özgürlüklerle çok yakın ilişkiye sahip olan benzersiz nitelikteki parmak izi gibi verilere ilişkin kayıtların tutulmasının kişisel verilerin korunması ilkelerine tabi olması gerektiği belirtilmektedir[463].

(3) Sadece suç ile bağlantılı tespit işlemlerinin yapılması gerekliliği

İkinci öne çıkan husus, iddia edilen suç bağlamında tespitin sadece o suça özgülenerek yapılması ve verilerin işlenmesidir. Aynı zamanda şüpheli veya sanığın kimliğini tespit edecek verilerin iddia edilen suçun aydınlatılmasında delil olabilecek nitelikle olması lazımdır. Diğer bir deyişle, suçla bağlantılı olmayan kimlik verilerinin işleme kapsamına alınmaması gerekir. Aksi halde, bireyin vücut bütünlüğüne yönelik orantısız bir müdahale söz konusu olur.

PVSK m. 5'e göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, CMK kapsamında alınanlara özgü aynı sisteme kaydedilerek saklanmaktadır. Ancak, parmak izinin hangi sebeple alındığı ve alınma amacı sisteme kaydedilmemekte olduğundan verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, amaca bağlılık ilkesi ve orantılılık (veri minimizasyonu) ilkesi ihlal edilmektedir. Dolayısıyla kişisel verilerin korunması amacı doğrultusunda buna ilkelerin yer aldığı kanuni düzenlemelerin yapılması yerinde olacaktır.

[463] Küzeci, s. 432.

(4) Soruşturma sürecinde kullanılan önleyici amaçla edinilmiş kişiler verilerin saklanması ve imhasına ilişkin orantılı düzenlemelerin eksikliği

Üçüncü olarak öne çıkan husus önleyici amaçlı bir tedbirle elde edilen ama soruşturma sürecinde kullanılan kişisel veriler hakkındadır. PVSK m. 5 hükmüne göre, parmak izinin ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle sisteme kaydedilebileceği belirtilmektedir.

Bununla birlikte, Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'unda kuruma alınma ve kayıt işlemlerinin düzenlendiği m. 21(3)'e göre de hükümlülerin parmak ve avuç içi izleri alınmaktadır. Ayrıca hükümlülerin fotoğrafları çekilmekte, kan grupları, vücutlarının dış özellikleri ve ölçüleri belirlenmektedir. Kayıt altına alınan söz konusu bilgiler hükümlünün kişisel dosyasında veya elektronik ortamda saklanmaktadır.

Bir görüşe göre ise m. 5'in bu haliyle, hemen hemen herkesin parmak izini kayıt altına almayı öngörmekte olduğundan buradaki amaç adli bir tedbirden ziyade alınan genel bir önlem niteliğindedir[464]. Keza hem önleyici amaçla elde edilen, hem adli amaçla elde edilen hem de infaz hukuku çerçevesinde elde edilen kişisel veriler bu bağlamda tek bir sisteme kaydedilmektedir[465]. Elde etme ve kullanma amaçları yönünden farklılık arz eden bu üç durumun, kendi alanları ile ilgili bağımsız sistemlere sahip olması zikredilen karmaşayı ve problemlerin çözümüne yardımcı olacaktır. Yani, elde edilen parmak izlerinden önleyici olarak elde edilenler önleyici nitelikli sisteme, adli olarak elde edilenler adli nitelikli sisteme ve infaz hukukunca elde edilenler de infaz niteliğine sahip sisteme kaydedilmelidir.

PVSK m. 5'te ayrıca sisteme kayıtlı olan parmak izi ve fotoğrafların, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silineceği düzenlenmiştir.

Seksen yıl, AİHM'in kişisel verilerin depolanabileceği süreler ilgili yorumları başta olmak üzere, uluslararası hukuk normları açısından da kabul edilecek düzeyde değildir. Âdeta bir insanın ömrü boyunca kişisel verilerinin depolanmakta olduğunu ifade etmektedir. Bu yüzden kanuni düzenleme AİHM içtihadıyla çelişmektedir. Biz, bu

[464] Küzeci, s. 438.
[465] Ünver/Hakeri, s. 286.

sürelerin kişisel verilerin korunması hakkının özüne dokunacak düzeyde ölçüsüz olması sebebiyle sınırlı süre saklanma ilkesine ve amaca bağlılık ilkesine aykırı olduğu görüşündeyiz.

Üstelik depolanmakta olan verilerin hangi depolama sistemi ve programı çerçevesinde yapılacağı da belirsizdir. Keza bu noktada elde edilen verilerin depolanmasına ilişkin meri kuralları manzumesi bulunmamaktadır. O sebeple, veri ayrımı yapılmadan, bu verilere hangi sürelerle ve hangi platformlar üzerinden kimlerin erişip, kimlerin düzenleyebileceği belirsizdir. Bu noktada bizim görüşümüze göre yapılması gereken, öncelikle verilerin kaydedildiği tek sistem önleyici, adli veya infaz hukukuna yönelik olarak bölünüp özelleştirilmelidir. Aynı zamanda yukarıda zikrettiğimiz belirsiz bırakılan hususları tamamlayıcı adımlar mevzuatta düzenlenmelidir.

Aksi halde, gerekli olmadığı halde bu tedbir kayıtları tutulmaya devam edilirse, o halde bu kayıtlar üzerinden elde edilen delillerin de hukuka aykırı delil olacağı unutulmamalıdır.

(5) Soruşturma sürecinde elde edilen kişilerin verilerinin depolanması ve imhasına ilişkin orantılı düzenlemelerin eksikliği

Dördüncü olarak öne çıkan husus, şüpheli veya sanık niteliğinden kurtulan kişilerin bu işlem kapsamda elde edilen delillerinin imha edilmesinin gerekli olmasıdır. Buna göre, söz konusu verilerin hemen imha edilmesi ve ayrıca farklı sistemlerde depolanmaması gereklidir. Maddede belirtildiği üzere, bu tespit sonucu kayıtların, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilmesi gerekmektedir.

Danıştay da bir kararında, şüphelinin parmak izi ve fotoğraf kaydının alınmasına neden olan suça ilişkin kesinleşmiş beraat, takipsizlik veya suçluluğu ortadan kaldırıcı bir belgenin bulunmaması halinde kayıtların silinmesinin talep edilebileceğini ifade etmiştir[466].

[466] D. 10. D, 17.11.2009, E. 2008/10561, K. 2009/9766, 11 Şubat 2019, Kazancı İçtihat Bilgi Bankası.

Fakat Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik m. 17'ye göre, mahkûmiyet kararı verilmesi hâlinde elde edilen verilerin kolluk tarafından, diş izlerinin ise bu işlemi yapan sağlık kuruluşu tarafından arşivleneceği belirtilmektedir.

İfade etmek gerekir ki, hükümde arşiv süresi belirtilmemesi sınırlı süre saklanma ilkesine, mahkûmiyet sonrasının ne olacağı belirtilmemesi açısından da amaca bağlılık-amaçla sınırlanma ilkesine aykırılık teşkil etmektedir. Dolayısıyla kişisel verilerin korunması amacı doğrultusunda bu verilerin depolanmasına ilişkin orantılı sürelerin ve işlemlerin belirtildiği hükümlerin hazırlanması gerekmektedir.

e) Ölünün kimliğini belirleme ve adlî muayene ve otopsi yöntemleri ile kişisel veri elde edilmesi

CMK m. 86'da ölünün kimliğini belirleme ve adlî muayeneye ilişkin hükümler düzenlenmektedir. Buna göre, engelleyici sebepler olmadıkça ölü muayenesinden veya otopsiden önce ölünün kimliği her suretle ve özellikle kendisini tanıyanlara gösterilerek belirlenmekte ve elde edilmiş bir şüpheli varsa, teşhis edilmek üzere ölü ona da gösterilebilmektedir. Bu işlemin, Cumhuriyet savcısının huzurunda ve bir hekim görevlendirilerek yapılması şarttır.

CMK m. 87'de ise otopsiye ilişkin hükümler yer almaktadır. Buna göre, otopsi cesedin durumu olanak verdiği takdirde, mutlaka baş, göğüs ve karnın açılması işlemini ifade etmektedir. Bu işlemin, Cumhuriyet savcısının huzurunda biri adlî tıp, diğeri patoloji uzmanı veya diğer dallardan birisinin mensubu veya biri pratisyen iki hekim tarafından yapılması gereklidir.

Hem ölünün kimliğini belirleme ve adlî muayene hem de otopsi sonucunda ölen kişiye ilişkin olarak onu belirlenebilir kılan bazı veriler elde edilmektedir. Ceset hukuken bir kişi değildir. Dolayısıyla, ceset üzerinde elde edilecek verilerin kişisel veri olarak nitelenmemesi gerekmekte olduğu doktrinde ifade edilmektedir[467].

Bu bağlamda, ölü üzerinde yapılacak işlemlerin kişisel verilerin korunması açısından gündeme gelmesi pek mümkün görünmemektedir. Fakat ceset üzerinde elde edilecek

[467] Şimşek, s. 123.

verilerin, kişinin ölmeden önceki kişilik varlığına işaret ettiği yönleri bulunmaktadır. Örneğin, o kişinin ailesi açısından hangi aileye mensup olduğu, vücut özelliklerinin nasıl olduğu, yediği içtiği şeylerin ne olduğu gibi.

Bu açıdan bizim düşüncemize göre, kişinin ölmeden önce sahip olduğu diğer temel hak ve hürriyetlerinin yanı sıra özel hayatın gizliliği ve kişisel verilerinin korunması hakkı açısından da sahip olduğu verilerin korunması gereklidir. Her ne kadar cesedin kişisel verisi olmasının mümkünatı olmasa da kişinin ölüm anına kadar sahip olduğu ve gizli kalması gereken verilerinin öldükten sonra da koruma kapsamında olması gerekir. Kişi ceset halini aldıktan sonra artık yeni ve güncel kişisel veri edinemez ve veri öznesi olamaz. Fakat ölüm anına kadar olan kısmının korunması gerekir. Burada artık verisi korunan bir ceset değildir, cesedin ölüm öncesi olduğu kişidir. Sonuçta kişisel verilerin korunmasını kişinin ölümüne kadar sınırlayan bir hüküm de bulunmamaktadır.

Öte yandan, ölü üzerindeki işlemler sonucunda ölünün yakınına ait kişisel veriler de elde ediliyor olabilir. Ölü üzerinden diğer kişileri tanımlayan verilerin kişisel veri olması hasebiyle, yine bu yönden de kişisel verilerin korunması kapsamında olacağına dikkat edilmelidir. Bu konunun özelinde kişisel verilerin korunmasına ilişkin gereklilikler açısından hukuki hükümlerin nasıl düzenleneceğine ilişkin tartışmaların eksikliği hissedilmektedir[468].

f) Vücut ve cinsel dokunulmazlığa müdahale eden zikredilen yöntemlerin tamamı hakkında ortak değerlendirmemiz

Kanun koyucu CMK m. 80'de, 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçlarının, kişisel veri niteliğinde olduğunu açıkça ifade etmektedir. Bu veriler, amaçla bağlılık ilkesi gereğince başka bir amaçla kullanılamazlar; gizlilik ilkesi gereğince de dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemezler.

Bu bilgilerin, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde

[468] Turan, s. 206.

Cumhuriyet savcısının huzurunda derhâl yok edilmesi ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilmesi hükme bağlanmıştır.

Bu doğrultuda öncelikle ifade etmek gerekir ki, amaca bağlılık-amaçla sınırlanma ilkesi açısından delil toplama amacıyla elde edilen bu kısımdaki verilerin, işlenen suç ile bağlantılı olması şarttır. Belirsiz veya henüz belirli olmayan amaçlarla verilerin toplanarak depolanması ne amaca bağlılık ne de kişisel verilerin korunması hakkına yönelik en az müdahalede bulunması ilkesine uygun düşmeyecektir[469].

İkincisi, belli bir suç kapsamında elde edilen kişisel veri içeren deliller, amaçla bağlılık ilkesi gereğince elde edildiği suç kapsamının dışında başka bir suçun ispatlanmasında kullanılmamalıdırlar[470]. Zaten CMK m. 80(1) uyarınca örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamayacağı ve dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemeyeceği düzenlenmektedir.

Üçüncüsü, yeterinden fazla örnek alınması da orantılılık (veri minimizasyonu) ilkesi açısından müdahaleyi hukuka aykırı hale getirebilir. Üstelik alınan verilerin doğruluğu ve sınırlı süre saklanma ilkesi gereğince soruşturma için gerekli süreyi aşan düzeyde depolanmaması da gerekmektedir. Bu doğrultuda, elde edilen verilerin CMK m. 80(2) ve 81(2) uyarınca Cumhuriyet savcısının huzurunda derhâl yok edileceği hükme bağlanmıştır.

Doktrinde bir görüşe göre verilerin imhası sonradan yeni bir inceleme gerekebileceği sebebiyle sakıncalı olup imha yerine muhafaza yolu seçilmelidir[471]. Elbette ki bu görüş kişiden tekrar tekrar veri alınmasını engellemek istemesi sebebiyle verilerin depolanmasını makul görmektedir. Fakat Türk hukukunda verilerin depolanmasına uygulanacak kapsamlı bir düzenleme söz konusu olmadığı için bu görüşe katılmadığımızı belirtmek isteriz. Çünkü, uygulanacak kuralların yokluğunda depolanan verilerin oldukça uzun süreler boyunca muhafaza edilmesi, verilere erişim ve düzenleme yapabilecek

[469] Höfelmann, Elke, Das Grundrecht auf informationelle Selbstbestimmung anhand der Ausgestaltung des Datenschutzrechts und der Grundrechtsnormen der Landesverfassungen, Frankfurt am Main 1997, s. 62 (ŞİMŞEK, s. 126'den naklen)
[470] Aygün, A. "Beden Muayenesi ve Vücuttan Örnek Alma," Dergipark.org.tr Erişim Tarihi: 6 Nisan 2019 https://dergipark.org.tr/download/article-file/271158, s. 68.
[471] Ünver/Hakeri, s. 277.

kişilerin kimlerin olabileceğinin belirsizliği gibi bir çok sorunsal bulunmakta olup bunların çözülmeden depolanması kişisel verilerin korunması hakkına yönelik orantısız bir müdahale teşkil edebilecektir.

Dördüncüsü, bu bölümde elde edilen verilerin sıklıkla hassas veri kategorisi içerisinde yer alacağından ötürü, KVK Kanunu m. 6(3) uyarınca bu verilerin ilgilinin açık rızası olmadan kural olarak işlenememesi gerekir. Fakat soruşturma evresinde delil etme amacıyla bu verilerin işlenmesi gerekeceğinden kanun koyucunun çatışan bu durumu dengeleyici bir kanuni düzenleme yapması gerekmektedir.

Bunun dışında dikkat edilmelidir ki, m. 75(2)'te iç beden muayenesi yapılabilmesi veya vücuttan kan veya benzeri biyolojik örnekler alınabilmesi için müdahalenin, kişinin sağlığına zarar verme tehlikesinin bulunmaması gerektiği belirtilmektedir.

Hatırlatmalıyız ki hem KVK Kanunu'nun bütününe hâkim bir prensip hem de hakkın doğasından kaynaklanan bir unsur olarak kişisel verilerin işlenmesinde bireyin iradesi esas alınmaktadır. Dolayısıyla, her ne kadar uygulamada suiistimal edilebileceği tehlikesini öngörmemize rağmen, bizim görüşümüze göre kişinin sağlığına zarar verme tehlikesi bulunsa bile şüpheli veya sanığın açık rızası varsa örnek alınabilmesi tartışılabilmelidir. Keza m. 76(2), mağdurun rızasının varlığı halinde, bu işlemlerin yapılabilmesi için mahkeme kararı alınmasına gerek olmadığını belirterek mağdurun iradesini belirleyici nitelikte olduğunu göstermektedir.

Unutulmamalıdır ki, nasıl kişisel verilerin korunması koruma talep edilebilecek bir haksa kişisel verilerin ifşa edilmesi de kural olarak müdahale edilmemesi gereken bir özgürlüktür. Bu noktada kişinin kendi kaderini tayin etme hakkı ile insan onurunun korunması amacıyla kişinin kendisine karşı korunması fikri yarışacaktır.

Bunun yanı sıra, kişinin verilerin işlenmesine rıza vermemesi halinde, kişisel çıkarlarının üst konumda bulunan kişi/kurum karşısında tehlikeye girmemesi gerekir. Çünkü kişi çeşitli çıkarlarının zedelenmemesi ve karşı tarafla olan ilişkisinin bozulmaması adına aslında rıza vermeyeceği bir konuda razı olduğunu beyan edebilir. Bu durumun önlenmesi adına hukuk kuralları detaylandırılabilir ve kişinin rızası kabul edilmeyebilir. Bir diğer

önemli husus da verilen rızanın içeriğinin açık olması ve şüpheye yer bırakmayacak derecede kesin olmasıdır[472].

Soruşturma evresinde ilgili kişi olarak verisi işlenen şüpheli/sanık veya mağdurun vermiş olduğu rızanın özellikle bu yönden aranan şartı sağlıyor olması gerekir. Çünkü verisi işlenen kişilerin karşısında meşru güç kullanma tekeline sahip kolluk bulunmakta olup, kişi heyecan, bilgisizlik, korkutma, hile ve aklının çeldirilmesi gibi sebeplerle verilerinin işlenmesine rıza gösterebilir. Bu noktada yapılması gereken, kişinin rızasının geçerli kabul edilmesi için müdafi/avukat yardımı almış olmasının ve kendisine verilerinin işlenmesi halinde lehine/aleyhine doğabilecek hususların anlatılmasının hükme bağlanmasıdır.

Öte yandan, CMK m. 89'da yer alan zehirlenme şüphesi üzerine yapılacak işleme de değinmek gerekir. Bu hüküm uyarınca, organlardan parça alınırken görünen şekli ile organın tahribatı tanımlanmaktadır. Her ne kadar organın kişisel veriye haiz nitelikte olamayacağı düşünülebilir olsa da, somut olaya uygun düştüğü ölçüde bir kişiyi dolaylı yoldan da olsa tanımlanabilir kılabilir. O halde kişisel verilerin işlenmesine ilişkin güvencelere sahip olması gerekir.

Son olarak kanun koyucunun vücut ve cinsel dokunulmazlığa müdahale eden koruma tedbirleri ve delil değerlendirme yöntemleri konusunda CMK ve ilgili düzenlemelerde detaylı düzenlemeler yapması gerekmektedir. Bu doğrultuda soruşturma sürecinde vücut ve cinsel dokunulmazlığa müdahale edilerek elde edilen delillerin işlenmesine yönelik düzenlemelerde, işlemenin veya işleme kategorilerinin amaçları yer almalıdır.

Ayrıca, kişisel veri kategorilerinin yanı sıra kötüye kullanım veya yasa dışı yollarla erişim veya aktarımın engellenmesine yönelik güvenceler de belirtilmelidir. Bununla birlikte işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanabilir güvenceler; veri sahiplerinin hakları ve özgürlüklerine yönelik riskler ve kısıtlama amacına halel getirmemesi durumunda veri sahiplerinin bilgi alma hakkının tüm soruşturmaya hâkim olması gerekmektedir.

3. Arama ve el koyma yöntemleri ile kişisel veri elde edilmesi

[472] Küzeci, s. 232.

a) Kişisel veri elde edilmesi amacıyla arama kararı alınması

CMK m. 116'ya göre, soruşturma evresinde şüphelinin üstü, eşyası, konutu, iş yeri veya ona ait diğer yerler yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa aranabilmektedir[473].

CMK m. 119'da düzenlenmekte olan arama kararını, kural olarak hâkim, istisna olarak gecikmesinde sakınca bulunan hâllerde ise Cumhuriyet savcısının vermesi gerekmektedir. Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri yine arama yapabilmektedirler. Kolluk amirinin yazılı emri ile yapılan arama sonuçları Cumhuriyet Başsavcılığına derhâl bildirilmektedir. Ayrıca, konutta, iş yerinde ve kamuya açık olmayan kapalı alanlarda aramanın, kolluk amirinin yazılı emri ile yapılması mümkün değildir.

Öte yandan, PVSK m. 9'da da önleme aramasına ilişkin hükümler düzenlenmektedir. Buna göre, Polis, tehlikenin veya suç işlenmesinin önlenmesi amacıyla kişilerin üstlerini, araçlarını, özel kâğıtlarını ve eşyasını aramakta, alınması gereken tedbirleri ve suç delillerini koruma altına almaktadır.

Üst araması, vücuda ve özel hayata yönelik bu hakları sınırlayan bir tedbirdir[474]. Usulüne göre verilmiş sulh ceza hâkiminin kararı veya bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hâllerde mülkî âmirin vereceği yazılı emir gereklidir. Arama talep yazısında, arama için makul sebeplerin oluştuğunun gerekçelerinin yanı sıra önleme aramasının yapılabileceği yerlere ilişkin çeşitli hükümlere yer verilmektedir.

Kişisel verilerin korunması açısından arama kurumuna ilişkin hükümler değerlendirildiğinde bazı hususlar ortaya çıkmaktadır.

Bunlardan birincisi, hemen yukarıda değindiğimiz üzere polise önleyici arama yetkisinin verildiği maddenin ilk fıkrasında alınması gereken tedbirlerin alınacağı şeklinde bir düzenleme söz konusudur. Her ne kadar düzenleme böyle olsa da ortada yer alan alınacak

[473] Adli arama ve kapsamı hükmü Adlî ve Önleme Aramaları Yönetmeliği m. 5'te düzenlenmektedir: *"Adlî arama, bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için bir kimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak konutunda, işyerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında, eşyasında, aracında 5271 sayılı Ceza Muhakemesi Kanun ile diğer kanunlara göre yapılan araştırma işlemidir."*

[474] Centel, Nur/Zafer, Hamide, s. 355.

tedbirler konusunda belirsiz nedeniyle bu tedbirlerin ne olacağının ve sınırlarının belirtilmesi daha uygun olurdu.

Kanunun bu şekilde düzenlenmemesi sebebiyle bu tedbirlerin ne olacağı hususunda kolluğa çok geniş yetki verildiği ortadadır. PVSK'da düzenlenen bu yetkilerin, koruma tedbirlerine ilişkin CMK'da yer alan güvenceleri sağlıyor olması gerekmektedir. Geniş yetkinin varlığı ve gerekli düzenlemenin yokluğu sebebiyle bu durum kişisel verilerin soruşturma evresinde işlenmesine hâkim olan bütün ilkeleri ihlal ediyor durumda olduğu belirtmek gerekir. Sonuçta kolluğun temel görevi hukuk gücünü kişileri disipline etmek için kullanmak değil kişilerin temel hak ve hürriyetlerini savunmaktır[475].

Aynı zamanda Adli ve Önleme Aramaları Yönetmeliği m. 8(f) ile kolluğa, ilgilinin rızası halinde adli arama yapma yetkisi verilmişti. Daha sonra bu hüküm iptal edilmiş olsa da bu noktada oluşabilecek suiistimalleri engellemek adına belirtmek gerekir ki, rızanın varlığı kadar rızanın niteliği de önemlidir. Bir görüşe göre, rıza beyanının niteliği, kişinin rıza verirken herhangi bir baskıya maruz kalmaması yani kişinin iradesinin özellikle dikey ilişkinin söz konusu olduğu hallerde olmak üzere serbest ve özgür bir zihinsel etkinliğinin ürünü olmalıdır[476].

İptale konu olan söz konusu hüküm, Danıştay 10. Dairesi tarafından verilmişti. Bu karara daha sonra idare tarafından itiraz edilmesi üzerine, Danıştay İdari Dava Daireleri Kurulu, iptal kararını onamıştır[477].

Danıştay 10. Dairesi birinci gerekçe olarak, adli aramalarla kişinin Anayasal hakları olan özel hayatın gizliliği ve konut dokunulmazlığı haklarının sınırlandırılmasında Anayasa'nın sınırlama sebeplerini açıkça belirtmesine rağmen, ilgilinin rızasına yer vermemesini göstermiştir.

İkinci gerekçe olarak ise, ilgilinin rızasına, adli amaçlı aramanın düzenlendiği CMK'da da kanun koyucunun birey ile kolluk arasındaki güç dengesizliğinin ilgilinin rızasını sakatlayabileceği endişesiyle yer verilmediği ileri sürülmüştür. Daireye göre bu düzenleme ile söz konusu hakların, mümkün olduğunca yargı yerlerince verilen kararlarla

[475] Bloom, Robert M./Dewey, Erin: "When Rights Become Empty Promises: Promoting an Exclusionary Rule That Vindicates Personal Rights", Irish Jurist, 46, Dublin 2011, s. 70.
[476] Küzeci, s. 233.
[477] D. İDDGK, E. 2007/2257, K. 2012/1117, 14.9.2012, Kazancı İçtihat Bilgi Bankası.

sınırlanması esasının benimsendiğini göstermektedir. Danıştay İdari Dava Daireleri Genel Kurulu da Danıştay 10. Dairesi'nin bu gerekçelerini haklı bulup, başvuruyu reddetmiştir. Bu yüzden, yönetmeliğin ilgilinin rızasına ilişkin hükmü kaldırılmış olup, önleyici amaçla yapılacak olan adli aramalarda ilgilinin rızası hukuken geçerli değildir. Dolayısıyla aynı gerekçeler çerçevesinde başta arama olmak üzere, vücut ve cinsel dokunulmazlığa ilişkin adli müdahaleler ve diğer koruma tedbirleri ve delil değerlendirme yöntemleri üzerinde de ilgilinin rızasının somut olay çerçevesinde bir kez daha değerlendirilip, ilgili kişinin çıkarı yönünde karar alınması isabetli olacaktır.

Doktrinde bir görüşe göre adli yöntemlerle kişinin rızası hilafına yönelik müdahaleler kanunlar ve yönetmeliklerde detaylı hükümlerle düzenleninceye kadar orantılılık ilkesi çerçevesinde özellikle karar veren merci yanında uygulamacıyı da sınırlandıran ölçütler getirilmelidir[478].

İkincisi, CMK m. 119(2)'de düzenlenen, arama karar veya emrinde aramanın nedenini oluşturan fiil, aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya, karar veya emrin geçerli olacağı zamanın süresi açıkça gösterilmek zorunda oluşudur. Buna göre, kararda zikredilen unsurların açıkça gösterilmekte oluşu, kişisel verilerin korunmasına ilişkin ilkelerden amaca bağlılık-amaçla sınırlanma ilkesi ve orantılılık (veri minimizasyonu) ilkesi uyumludur.

Üçüncü husus, CMK m. 119(3)'te, arama tutanağına işlemi yapanların açık kimlikleri yazılacağı belirtilmekte oluşudur. Aramayı yapan görevlilerin kimliklerinin yazılmasının sebebi şüphesiz aramanın usulünce yapılmaması halinde sorumluluğuna gidilecek kişilerin belirlenmesi içindir. Fakat bizim görüşümüze göre görevlilerin doğrudan açık kimliklerini yansıtan verilerin yazılmasının yerine açık olmayan fakat görevlileri belirli kılabilecek sicil numarası gibi verilerin yazılması gerekli ve yeterlidir. Aksi halde görevlilerin kişisel verilerine yönelik orantısız bir müdahaleden bahsedilebilir. Çünkü gerekli olmadığı halde görevlilerin kişisel verileri açıkça alenileştirilmektedir.

Aynı şekilde, CMK m. 119(4)'te, Cumhuriyet savcısı hazır olmaksızın konut, iş yeri veya diğer kapalı yerlerde yapılacak aramada o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulacağı hükme bağlanmaktadır. Burada da aramaya katılacak komşuları

[478] Ünver/Hakeri, s. 274.

belirlemeyi sağlayacak açık kimliklerinin yazılması yerine T. C. Kimlik numaralarının kayda alınmasının yeterli olması gereklidir. Güncel haliyle bu husus, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, daha az müdahale eden yöntemin uygulanması ilkesi, orantılılık (veri minimizasyonu) ilkesi, veri güvenliği(bütünlük ve gizlilik) ilkesi ve amaca bağlılık-amaçla sınırlanma ilkesine aykırıdır. Dolayısıyla bu madde bağlamındaki uygulamaların zikredilen ilkeleri dikkate alarak bu yönde gelişmesi taraftarı olduğumuzu belirtmek isteriz.

Son olarak belirtmek gerekir ki, arama kararı kapsamında m. 120 ila 122 uyarınca yapılan işlemler sonucu elde edilen materyaller ve belgelerin ilgili suç kapsamında olması gerekmektedir. Soruşturma sürecine katkı sağlamayan kişisel verilerin amaçla bağlılık ilkesi gereği bu kapsamda yer almaması gerekir. Ayrıca ve bunlar içerisinde yer alan kişisel verilerin yalnızca suçla bağlantılı olan kısımlarının ölçülü olarak işlenmesi gerekir ki gereken miktarın aşılması da orantılılık (veri minimizasyonu) ilkesinin ihlaline yol açacaktır.

Dolayısıyla, bahsettiğimiz bu hususlarda yapılacak değişiklerle artacak olan hassasiyetler sonucu kişisel verilerin korunması hakkı ve koruma ilkeleri doğrultusunda olumlu adımlar atılmış olacaktır. Ayrıca, kanunda yazılı hallerin haricinde veya zikrettiğimiz ilkeler doğrultusunda hükümlerin yeniden düzenlenmesi halinde de bu ilkelere aykırı olarak bir kimsenin üzerini aramak için emir veren yahut bizzat arayan kamu görevlisi TCK m. 120 uyarınca haksız arama suçunu işlemiş olacaktır.

b) El koyma kararı ile kişisel veri elde edilmesi

(1) Genel olarak

El koyma, Adli ve Önleme Aramaları Yönetmeliği, m.4'te tanımlanmaktadır. Buna göre el koyma, suçun veya tehlikelerin önlenmesi amacıyla veya suçun delili olabileceği veya müsadereye tâbi olduğu için, bir eşya üzerinde, rızası olmamasına rağmen, zilyedin tasarruf yetkisinin kaldırılması işlemini ifade etmektedir. El koyma, zilyetliğe yönelik olan bir koruma tedbiridir[479].

[479] Centel, Nur/Zafer, Hamide, s. 355.

CMK m. 127'e göre, el koyma kararını vermeye hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yetkisi bulunmaktadır. Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri, el koyma işlemini gerçekleştirebilmektedir. Hâkim kararı olmaksızın diğer iki şekilde yapılan el koyma işlemlerinin, yirmi dört saat içinde görevli hâkimin onayına sunulması şarttır. Hâkim'in kırk sekiz saat içinde onaylamadığı kararlar kendiliğinden kalkmaktadır.

CMK m. 127(2)'ye göre, kolluk görevlisinin açık kimliği, el koyma işlemine ilişkin tutanağa geçirilmektedir. Arama kararındaki görevlilerin kimliğinin yazılış şeklinde bahsettiğimiz hususlar burada da geçerlilik kazanmaktadır. Buna göre kolluk görevlisinin açık kimliği yerine sicil numarası gibi onu sadece ilgilisine belirleyici kılan bir verinin yazılması gerekmektedir.

Burada el koyma kurumuna ilişkin CMK'da düzenlenmekte olan hükümleri soruşturma evresinde kişisel verilerin işlenmesine dair ilkeler açısından değerlendirmek önem kazanmaktadır. Bu doğrultuda aşağıda beş farklı el koyma çeşidini ayrı ayrı incelemekteyiz. Ölçülülük ilkesinin bir gereği olarak hakka müdahalede en hafif müdahale teşkil edecek yol ve yöntemin seçilmesi gerektiği unutulmamalıdır[480].

(2) Eşya veya kazancın muhafaza altına alınması ve bunlara el konulması yöntemi ile kişisel veri elde edilmesi

El koyma çeşitleri arasından birinci olarak eşya veya kazancın muhafaza altına alınması ve bunlara el konulmasına ilişkin hükümleri değerlendirmekteyiz. CMK m. 123'e göre, ispat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan mal varlığı değerleri muhafaza altına alınabilmektedir. Yanında bulunduran kişinin rızasıyla teslim etmediği bu tür eşyalara el konulabilmektedir.

Kişisel verilerin korunması açısından belirtmek gerekir ki, suç kapsamında soruşturma evresinde el konularak muhafaza altına alınan ve bir kişiyi belirlenebilir kılan herhangi bir nesne kişisel veridir. Bu doğrultuda, amaca bağlılık ilkesi uyarınca el konularak muhafaza alınacak şeylerin sadece suçla bağlantılı olmalı ve orantılılık açısından da gerek

[480] Şen, Ersan/Eryıldız, H. Sefa: El koyma, Ankara 2017, s. 35.

olmadığı halde kişisel verilerin çeşit ve miktar olarak elde edilmesinin önüne geçilmelidir.

Bu iki husus, kişisel verilerin soruşturma evresinde işlenmesine ilişkin ilkelerle irtibatlıdır. Bu yüzden, aksi yönde bir tedbir, amaca bağlılık-amaçla sınırlanma ve orantılılık (veri minimizasyonu) ilkesine doğrudan ihlal etmektedir. Daha az müdahale eden yöntemin uygulanması ilkesi ve verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine de dolaylı yoldan aykırılık meydana gelmiş olacaktır.

(3) El konulamayacak mektuplar ve belgeler üzerinde kişisel veri elde edilememesi

El koyma çeşitleri arasından ikinci olarak değerlendirmekte olduğumuz, CMK m. 126'da yer alan el konulamayacak mektuplar ve belgelere ilişkin hükümlerdir. Bu hükme göre, şüpheli ile CMK m. 45 ve 46'ya göre tanıklıktan çekinebilecek kimseler arasındaki mektuplara ve belgelere; bunlar bu kimselerin nezdinde bulunduğu müddetçe el konulamamaktadır.

Bu noktada belirtmeliyiz ki, bu madde kapsamında el konulamayacak mektup ve belgeler düzenlenmekte olduğundan bu maddeye soruşturulan suç ile ilgili olmayan ve kişisel veri içeren belgelere de el konulamayacağı hükmü eklenmelidir. Böylece, kişisel verilerin korunmasındaki verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, amaca bağlılık-amaçla sınırlanma ilkesi ve orantılılık (veri minimizasyonu) ilkesine uygun bir düzenleme yapılmış olacaktır.

(4) Taşınmazlara, hak ve alacaklara el koyma yöntemi ile kişisel veri elde edilmesi

El koyma çeşitleri içinde üçüncü olarak değerlendirmekte olduğumuz, CMK m. 128'de taşınmazlara, hak ve alacaklara el koymaya ilişkin hükümlerdir. Buna göre, soruşturma konusu suçun işlendiğine ilişkin olmak üzere şüpheliye ait olan taşınmazlara, ulaşım araçlarına, her türlü hesaba, her türlü hak ve alacaklara, kıymetli evraka, ortaklık paylarına ve diğer mal varlığı değerlerine el konulabilmektedir. Fakat öncelikle suçtan elde edildiğine dair somut delillere dayanan kuvvetli şüphe sebebi bulunması gerekmektedir. Ayrıca somut olarak belirlenen değerlerin başka bir kişinin zilyetliğinde bulunması işlemin yapılmasını engellememektedir.

Belirtmek gerekir ki bu el koyma kararı kapsamında el konulacak değerlerin arasında, suç delilleri ile irtibat kurulamayan kişisel veriler koruma kapsamında olmalıdır. Örneğin, bu

madde kapsamında bir banka hesabına el koymak mümkündür fakat somut delillerin işaret etmediği aynı şahsa ait aynı bankadaki başka hesaplar varsa bunlara aynı karar kapsamında el konulamamalıdır. Aksi halde hem kişisel verilerin ihlali söz konusu olur hem de ölçülü hareket edilmiş olunmaz. Bu da, verilerin işlenmesinde amaca bağlılık-amaçla sınırlanma ilkesi ve orantılılık (veri minimizasyonu) ilkesine aykırılık teşkil eder.

Öte yandan bu kanun kapsamında ilgili müdürlüklere yapılacak el koyma bildirimlerinin müdürlükteki herkes tarafından değil sadece işlemi gerçekleştirecek kişiler tarafından gerçekleştirilmesi gerekir. Bu doğrultuda yapılacak her el koyma kararı için dosyada gizlilik kararı da alınmasının daha iyi koruma sağlayacağı aşikârdır. Bu durum verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi ve veri güvenliği(bütünlük ve gizlilik) ilkesi ile irtibatlı ve gereklidir.

Son olarak söz konusu kararın ilgili gerçek kişiye tebliğ edileceği hüküm altına alındığından belirtmek gerekir ki bu tebliğin şüphelinin kendisine ve eğer kendisinin muvafakati varsa yakınlarına da yapılabilir. Ayrıca yalnızca tebliğ zarfının kapalı olması yeterli olmaz, bunun dışında zarfın dış yüzeyinin mümkünse ilgili kişinin adı da dâhil anonimleştirilmesi gereklidir. Çünkü kişinin ceza soruşturmasına ilişkin tüm bilgileri onu belirlenebilir kıldığı ölçüde kişisel veridir ve kişinin ailesi başta olmak üzere yakınında bulunanların bu durumu öğrenmeleri Amaca bağlılık-amaçla sınırlanma ilkesi gereğince şart değildir.

(5) Postada el koyma yöntemi ile kişisel veri elde edilmesi

El koyma çeşitleri arasından dördüncü olarak değerlendirmekte olduğumuz, CMK m. 129'da düzenlenen postada el koymaya ilişkin hükümlerdir. Buna göre, suçun delillerini oluşturduğundan şüphe edilen ve gerçeğin ortaya çıkarılması için soruşturma ve kovuşturmada adliyenin eli altında olması zorunlu sayılıp, posta hizmeti veren her türlü resmî veya özel kuruluşta bulunan gönderilere el konulabilmektedir. Buna ilişkin karar, hâkim tarafından veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından vermektedir. Kanunun lafzından anlaşıldığı üzere yalnızca fiziki postaya ilişkin el koyma hükümleri düzenlenmektedir. Bu doğrultuda elektronik postaya ilişkin hükümler telekomünikasyon yoluyla yapılan iletişim denetlenmesi (CMK m. 135-138) hükümlerinde incelenecektir.

CMK m. 129(2)'ye göre, el koyma işlemini yerine getiren kolluk memurları, bu gönderilerin içinde bulunduğu zarfları veya paketleri kural olarak açamazlar. Fakat el koyma kararı veya emrinin CMK m. 129(3)'te sayılan suçlarla ilgili olarak verilmesi halinde gönderilerin bulunduğu zarf veya paketler, Cumhuriyet savcısının talimatıyla kolluk memurları tarafından açılabilir. Postadaki zarf ve paketlerin kendisi kişiyi belirli içeriği ise belirlenebilir kılacağından sadece Cumhuriyet savcısının el koyma kararı zarfların açılmasını kapsamamalıdır. Bu yüzden, Cumhuriyet savcısının talimatında zarfın açılmasının özellikle belirtilmesi gerekir. Bu, daha az müdahale eden yöntemin uygulanması ilkesi gereği doğrultusundadır.

Maddenin diğer fıkralarında, soruşturma ve kovuşturmanın amacına zarar verme olasılığı bulunmadıkça, alınmış tedbirlerin ilgililere bildirilmesi ve açılmamasına veya açılıp da içeriği bakımından adliyenin eli altında tutulmasına gerek bulunmadığına karar verilen gönderilerin, hemen ilgililerine teslim olunacağı düzenlenmektedir. Kişisel veriler açısından da belirtmek gerekir ki postanın bizzat kendisi bir kişisel veridir. Ayrıca postada yer alan her türlü materyal ve yazı bir kişiyi belirlenebilir kıldığı ölçüde kişisel veri kabul edilebileceğinden yürütülen soruşturma kapsamındaki suç ile ilgili olmaması halinde bu verilere el konulmaması gerekmektedir. Bunun dışında, söz konusu kişisel verilerin illa ki şüpheliye yönelik olması gerekmez, bir başka kişiye de ait olabileceği akıldan çıkarılmamalıdır. Bu yargılarımız, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi ve amaca bağlılık-amaçla sınırlanma ilkesine dayanmaktadır.

(6) Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma yöntemi ile kişisel veri elde edilmesi

El koyma çeşitleri arasında beşinci olarak bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koymaya ilişkin hükümleri değerlendirmekteyiz. CMK m. 134'e göre, herhangi bir suç dolayısıyla yapılan soruşturmada, şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilebilmektedir.

Bu kararın verilebilmesi için somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka bir surette delil elde etme imkânının bulunmaması hallerinin birlikte varlığı şarttır. Bu şartlardan birinin eksikliği halinde bu karar verilemez. Bu karar kural olarak

hâkim tarafından verilebilir. İstisnai olarak ise gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından da verilebilmektedir. Fakat bu halde hem yirmi dört saat içinde hâkim onayına sunulmalı hem de hâkim bu kararı en geç yirmi dört saat içinde onaylamalıdır. Kanuna göre, tüm bu usule herhangi bir aykırılıkta çıkarılan kopyaların ve çözümü yapılan metinlerin derhâl imha edilmesi gerekmektedir. Bu düzenleme verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi çerçevesindedir.

CMK m. 134(2)'ye göre, bilgisayar, bilgisayar programları ve bilgisayar kütüklerine el konulabilmesi için bu araç ve gereçlerdeki şifrenin çözülememesinden dolayı sisteme girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması şartının gerçekleşmesi gerekmektedir. Bu şartlar seçimliktir. El koymanın amacı ise çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi içindir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazların gecikme olmaksızın iade edilmesi gerekmektedir. Aksi halde, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine, amaca bağlılık-amaçla sınırlanma ilkesine ve daha az müdahale eden yöntemin uygulanması ilkesine aykırılık söz konusu olacaktır.

Maddenin devamındaki fıkralarda, bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılacağı ve alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verileceği ve bu hususun tutanağa geçirilerek imza altına alınacağı düzenlenmektedir.

Ayrıca maddeye göre, bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilmesi mümkündür. Burada, kopyası alınan verilerin kâğıda yazdırılarak, bu hususun tutanağa kaydedilmesi ve ilgililer tarafından imza altına alınması gerekmektedir.

Kanuni düzenleme bu olmakla birlikte, esasen sistemdeki tüm verilerin kâğıda yazılarak kayda alınması pek mümkün olmadığından bilgisayarın hash değeri alınmaktadır. Bu değer bilgisayar verilerinin alındığı andaki durumunun âdeta aynadaki görüntüsü gibi eşsiz rakamlara dökülerek yedeklenmesi suretiyle veri bütünlüğünü sağlamaktadır[481].

[481] Özen, Muharrem/Özocak, Gürkan: "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi", Ankara Barosu Dergisi, 1, Ankara 2015, s. 53.

Buradan hareketle kişisel verilerin korunması açısından belirtmek gerekir ki, burada el koyulan bilgisayar verileri ve hash değeri doğrudan veya dolaylı olarak bir kişiyi belirli yahut belirlenebilir kıldığı ölçüde kişisel veridir. Bir kişiyi belirli kılmıyor olsa bile özel hayat verisi olduğu su götürmez bir gerçektir. Dolayısıyla, bu veriler incelenirken gerekli sayıda yetkili tarafından ve gizli olarak incelenmesi ve bu verilerin soruşturmanın dışına taşacak şekilde alenileştirilmemesi amaçla bağlılık ve orantılılık ilkesi gereğince şarttır. Soruşturma ile bağlantısı olmayan tüm verilerin dosya kapsamına bile alınmadan imha edilmesi gerekmektedir. Bu da veri güvenliği(bütünlük ve gizlilik) ilkesi gereğincedir.

Son olarak belirtmemiz gerekir ki, şüpheli ile tanıklıktan çekinebilecek kişiler arasındaki iletişimi sağlayan ve kişisel veri barındıran belgelerin delil olarak toplanma imkânının olup olmadığı hususu belirsizdir. Bunun sebebi bizim görüşümüze göre kanunda düzenlenmesi gerekirken eksik bırakılan hususlardan biri olmasıdır. Bu yüzden el konulabilecek verilerin işleme ilkelerine dayanan sınırlarının belirtilmesinin şart olacağı görüşündeyiz.

Bu konuyu içeren bir davada Yargıtay, bilgisayar sistemlerinin birbirlerine bağlanabilme özelliklerinden dolayı verilerin, dolaylı şekilde bağlantılı olduğu başka bir sistemde bulunabileceğinden hareketle aramanın verilerin gerçekte bulunduğu yeri içine alacak biçimde genişletilmesini dengeli bir müdahale olarak yorumlamıştır[482]. Bizim görüşümüze göre bu yargı eksiktir. Çünkü bu şekilde geniş kapsamlı bir müdahale ile çok daha fazla verinin elde edilmesine imkân tanınmaktadır. Bu bağlamda, kurallara tabi olmadığı müddetçe idareye tanınan geniş yetkinin tatbiki hem hakka yönelik orantısız bir müdahale teşkil edecek hem de somut olayların yorumlanmasında yargının işini zorlaştıracaktır.

4. Gizli soruşturma yöntemleri ile kişisel veri elde edilmesi

a) Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi yöntemi ile kişisel veri elde edilmesi

Soruşturma evresinde telekomünikasyon yoluyla yapılan iletişimin denetlenmesi ve teknik araçlarla izlemeye ilişkin alınacak koruma tedbiri hükümleri, CMK m. 135 ve

[482] Y. CGK, E. 2017/16-956 K. 2017/370 T. 26.9.2017, Kazancı İçtihat Bilgi Bankası: Yüksek Mahkeme bu görüşünde Avrupa Konseyi Siber Suç Sözleşmesi/Açıklayıcı Rapor, No:187'ye atıfta bulunmaktadır.

devamında düzenlenmektedir. Bununla birlikte, PVSK Ek m. 7'de polisin bilişim suçlarına ilişkin olarak önleyici amaçlarla adli tedbirler alabileceğinden bahsedilmektedir[483].

Buna ek olarak 2007 yılında yürürlüğe giren fakat tüm hükümleri Adalet Bakanlığının bu konuda yönetmelik çıkarma yetkisi olmaması sebebiyle iptal edilen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Yönetmeliği'nde de önemli hükümler bulunmaktadır[484].

Aşağıda ilgili koruma tedbirleri açısından çeşitli hükümler, kişisel verilerin soruşturma evresinde korunmasına ilişkin ilkeler ve ilgili kişinin hakları açısından değerlendirilmektedir.

(1) CMK hükümleri açısından

(a) Genel olarak

İletişimin denetlenmesi, bir insan hakkı olan haberleşme hürriyetine kamu otoritelerinin gerekçeli müdahale etmesi anlamına gelmektedir. Anayasa m. 22'de belirtildiği üzere herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Daha önce de açıkladığımız üzere, haberleşme özgürlüğü kişisel veriler ile doğrudan ilişkilidir. Bu yüzden iletişimin denetlenmesine yönelik alınan koruma tedbirlerinin haberleşme özgürlüklerinin yanı sıra kişilerin kişisel verilerin korunması hakkına da dokunmaktadır.

---

[483] PVSK Ek m. 7 düzenlemesine göre: *"Birinci fıkrada belirtilen görevlerin yerine getirilmesine yönelik olarak, 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçlar ile bilişim suçlarının işlenmesinin önlenmesi amacıyla hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürünün, Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanının veya bilişim suçlarıyla sınırlı olmak üzere bilişim suçları ile ilgili daire başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen veriler tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç kırk sekiz saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhâl kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir."*

[484] Danıştay Onuncu Dairesinin 09.03.2017 tarihli ve Esas No:2012/1001; Karar No:2017/1361 sayılı kararı ile Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin iptaline karar verilmiştir.

Haberleşmenin özgürlüğü açısından daha çok öne çıkan bu tedbirlerin hakka yönelik müdahalesinin kanun ve yönetmelikle sınırlanmış olması bir açıdan kişisel verilerin korunmasını sağlamaktadır. Gerçekten de, bu hak kendi özel koruma alanlarında özellikle kişilik hakkında getirdiği koruma boyutuyla kişinin kişisel verilerinin korunması hakkına da hizmet etmektedir[485]. Çünkü bu gibi haklar için anayasada özel sınırlama sebepleri öngörülmüşken, kişisel verilerin korunması ile ilgili olarak m. 20(3)'de özel sınırlama sebepleri sayılmamakta, bu husus daha aşağı bir norm olan kanuna bırakılarak verilerin korunması hukukunu zayıflatmaktadır.

Öte yandan, CMK m. 135 ila 138 arasında adli bir tedbir olarak telekomünikasyon yoluyla yapılan iletişimin denetlenmesine ilişkin hükümler düzenlenmektedir. Bunlardan CMK m. 135'te düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınmasına ilişkin kurallara göre, şüphelinin telekomünikasyon yoluyla iletişimi dinlenebilmekte, kayda alınabilmekte ve sinyal bilgileri değerlendirilebilmektedir[486]. Bunun için m. 135(8)'de sayılan katalog suçlar içerisinden bir suçun işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı yeterlidir.

CMK'nın 135.maddesine göre yapılan bu tedbir geçmişe dönük olarak değil, geleceğe dönük olarak yapılabilmektedir[487]. Ayrıca kuvvetli şüphe sebeplerinin somut delillere dayanması gerekir. Üstelik başka suretle delil elde edilmesi imkânının bulunmaması da şarttır. O halde öncelikle diğer delil elde etme yollarına başvurulmalı, bu yolların tüketilmesinde sonra veya bu yolların tüketilmesinde bir yarar görülmemesi üzerine bu madde bağlamında delil elde etme yoluna gidilmesi gerekmektedir. Bu şekilde, bu

---

[485] Şimşek, s. 153.

[486] İptal edilen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik m. 4'te iletişimin dinlenmesi ve kayda alınması, sinyal bilgisi ve sinyal bilgilerinin değerlendirilmesi tanımlanmaktadır:
"... e) İletişimin dinlenmesi ve kayda alınması: Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri ifade eder.
...
h) Sinyal bilgisi: Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi,
ı) Sinyal bilgilerinin değerlendirilmesi: İletişimin içeriğine müdahale niteliğinde olmayıp yetkili makamdan alınan karar kapsamında sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemlerini ifade eder."

[487] Y. 16. CD, 24.04.2017, E. 2015/3 K. 2017/3, 11 Şubat 2019, Kazancı İçtihat Bilgi Bankası.

tedbirin alınmasında mutlak bir zorunluluğun bulunması şartı da verilen kararda sağlanmış olmaktadır.

Fakat bu koşulun başka bir koruma tedbirine başvurulduğu sırada telekomünikasyon yoluyla yapılan iletişimin denetlenmesinin uygulanamayacağı şeklinde dar yorumlanmaması gerektiği belirtilmektedir[488]. İkincil bir yöntem olmasının bir diğer sonucu da, elde edilen delil niteliğindeki verilerin, delilin soruşturmaya bağlılığı ilkesi çerçevesinde kural olarak sadece o suç kapsamında işlenebilmesidir[489].

Şüphelinin telekomünikasyon yoluyla iletişimi dinlenmesinin, kayda alınmasının ve sinyal bilgileri değerlendirilmesinin dışında, zikredilen maddeye 2014 yılında eklenen 6. fıkraya göre, iletişimin tespitine[490] ilişkin hükümler düzenlenmiştir. Her iki tür işleme ilişkin kararların alınmasındaki kural, hâkimin karar vermesidir. Gecikmesinde sakınca bulunan hâllerde ise hâkimin onaylaması şartıyla Cumhuriyet savcısının kararıyla da bu işlem yapılabilmektedir. Kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodu ve tedbirin süresi belirtilmesi şarttır. Bu, verilerin işlenmesine ilişkin amacın sınırlanması ilkesi doğrultusundadır. Bu tedbir açısından m. 135(8)'de sayılan katalog suçların soruşturmaya konu olması gerekmediğinden, her suç için uygulanabilmektedir.

Bunun dışında, CMK m. 135(3)'d göre, şüphelinin tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kural olarak kayda alınamadığından, kayda alma gerçekleştikten sonra bu durumun anlaşılması hâlinde alınan kayıtlar derhâl yok edilir. İstisna olarak ise, tanıklıktan çekinme hakkı olan şahısların da suç işleme şüphesi altında olması halinde bu tedbire başvurulabilecektir. Tanıklıktan çekinme hakkı sahiplerinin yanı sıra iletişimin denetlenmesi yasak olan ve özel usullere tabi olan başka kişiler de bulunmaktadır. Bunlar, başta avukatlar olmak üzere, milletvekilleri, kamu görevlileri, yabancılar ve MİT

[488] Aydın, s. 80.
[489] Yenisey/Nuhoğlu, s. 450.
[490] İptal edilen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik m. 4'te iletişimin tespiti tanımlanmaktadır:
"... f) İletişimin tespiti: İletişimin içeriğine müdahale etmeden, iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri ifade eder."

görevlileridir[491]. Bu doğrultuda şüpheli veya sanığa yüklenen suç dolayısıyla suç şüphelisi olmayan müdafinin bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında, m. 135 hükmü uygulanamaz.

Kararların yerine getirilmesinin ve iletişim içeriklerinin yok edilmesinin düzenlendiği CMK m. 137(3)'e göre, m. 135 doğrultusunda verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da hâkim onayının alınamaması halinde, ilgili kayıtların Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilmesi gerekmektedir.

Dolayısıyla, kişisel verilerin sistemlerde bu belirtilen süreyi aşacak şekilde kayıtlı durması ya da başka veri sistemlerine kayıt edilmesi hukuka aykırıdır hatta TCK m. 135'te düzenlenen kişisel verilerin kaydedilmesi suçu işlenmiş olur. Doktrinde bir görüşe göre, bu madde hükmü, beraat veya mahkûmiyet durumunda nasıl davranılacağını da içerecek biçimde daha geniş düzenlenmelidir[492]. Bu eksiklik elde edilen verilerin ne kadar saklanacağının düzenlenmemesi nedeniyle de eleştirilmektedir[493].

Ayrıca m. 137(4) uyarınca tespit ve dinlemeye ilişkin kayıtların yok edilmesi hakkında ilgilisine tedbirin nedeni, kapsamı, süresi ve sonucu ile ilgili bilgi verileceği düzenlenmesine rağmen sinyal bilgilerinin değerlendirilmesi tedbiri bildirim kapsamına alınmamıştır. Bir görüşe göre, muhataba bildirim sinyal bilgilerinin değerlendirilmesi bakımından da söz konusu olmalıdır[494]. Bunun varlığı bizce kişisel verisi işlenen ilgili kişinin haberdar edilme hakkı gereğincedir.

Bu noktada ilgilinin rızası açısından bir değerlendirme önem taşımaktadır. İlgilinin rızası ceza hukukunda hukuka uygunluk sebebi olarak sayılmakta olduğundan, ilgilinin rızası halinde karar alınmadan uygulanacak iletişimin denetlenmesinde hukuka aykırılık olmayacaktır. Fakat ilgilinin rızasının her durumda hukuka uygunluğu sağlayamayacağını belirtmek gerekir. Bu noktada doktrinde ikili bir ayrıma gidilerek hangi durumun hukuka uygun olacağı belirtilmektedir. Buna göre, telefonun banda kaydedilmesi dışında sadece dinlenmesine rıza gösterilmesi halinde verilen rıza hukuka

[491] Gül/Alagöz, s. 158.
[492] Gül/Alagöz, s. 164.
[493] Aydın, s. 84.
[494] Şahin, s. 367.

uygunluk sebebi olacaktır. Fakat hat sahibinin telefon konuşmasının banda kaydedilmesine rıza göstermesi halinde ise rızanın geçersiz sayılması savunulmaktadır[495].

Son olarak, tesadüfen elde edilen deliller konusunu işlemek de gerekir. İletişimin denetlenmesi sırasında yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan fakat katalog içerisindeki suçlardan birinin işlendiği şüphesini uyandırabilecek bir delile tesadüfi delil denmektedir[496]. Tesadüfen delil elde edildiğinde derhâl Cumhuriyet savcılığına bildirilir. Bir görüşe göre, delilin bizzat Cumhuriyet savcılığınca muhafaza altına alınması yükümlülüğü kanuna eklenmelidir[497].

Kişisel verilerin korunması hükümleri açısından belirtmek gerekir ki tesadüfen elde edilen delillerin doğrudan kişisel veri olması yahut kişisel veri içermesi halinde, m. 138'de yer alan usule uyulmasının yanı sıra kişisel verilerin korunmasına ilişkin ilkeler doğrultusunda da davranılması gerekir.

Dolayısıyla, bir kişiyi belirlenebilir kılacak kişisel veri içeren tesadüfi delillerin, öngörülen amaç doğrultusunda amaca bağlılık ilkesi gereğince koruma altına alınmasına ve gizliliğine azami dikkat edilmelidir. Söz konusu delillerin katalog içerisindeki suçlardan birinin işlendiği şüphesini uyandırabilecek nitelikle olması ve bu şüphenin de gerekçelendirilmesi şarttır.

Ayrıca bu madde bağlamında, doğrudan katalog kapsamında sayılan suçların işlendiği hususunda şüphe oluşmayan delil niteliğindeki kişisel verilerin yanı sıra söz konusu delillerden bağımsız kişisel verilerin koruma kapsamına alınması gerekmektedir. Aksi halde, koruma altına alınabilecek delillerde ölçüsüz ve orantısız bir müdahale söz konusu olabilir. Bu halde müdahalenin hukuku uygunluk sebebi olan kanunun verdiği yetkinin dışına çıkılarak orantılılık (veri minimizasyonu) ilkesi ihlal edilmiş olur.

---

[495] Yenisey/Nuhoğlu, s. 446: Burada belirtilen görüşe göre, görüşmenin banda kaydedilmesine verilecek rıza StGB m. 201(1) aykırı olacağından geçersiz sayılması gerektiği ileri sürülmüştür.

[496] Tesadüfen elde edilen deliller hükmü CMK m. 138'de düzenlenmektedir:
"(1) Arama veya elkoyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.
(2) Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, 135 inci maddenin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir."

[497] Gül/Alagöz, s. 164.

(b) Kişisel verilerin korunması açısından

CMK m. 135 hükmünün, kişisel verilerin korunmasına ilişkin ilkeler açısından öncelikle belirtmek gerekir ki bu işlem süreci içerisinde hangi iletişim verilerinin kişisel veri olabileceği üzerinde belirsizlik yaşanmamalıdır. Tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodu ve tedbirin süresi bir kişiyi belirlenebilir kıldığı ölçüde kişisel veridir.

Ayrıca, CMK m. 135 kapsamında elde edilecek her bir verinin, bir kişi veya kişileri belirlenebilir kılmakta olan iletişim bilgi ve verilerini içerdiği ölçüde kişisel veri olacağı unutulmamalıdır. Kendisi bir kişisel veri olan e-postaların açılıp içeriği de bu kapsamdadır. Bu tedbirle elde edilen kişisel verilerin, kişisel verilerin korunması ilkelerine tabi olması doğal olandır.

İkincisi, alınan tedbirlerle kişisel verilere yönelik bir müdahale teşkil etmekte olduğundan bu müdahalenin kişisel verilerin korunması ilkeleri açısından orantılı ve delil toplanma amacına yönelik olması gerekmektedir. Bu yüzden, m. 137(2) uyarınca metin haline getirilecek iletişim verileri içerisinde suçla ilgili olmayan kişisel verilerin bu metin içerisinde yer almaması gereklidir. Ayrıca, CMK m. 135(4)'e göre, iletişimin tespiti, dinlenmesi, kayda alınması, sinyal bilgilerinin değerlendirilmesi veya mobil telefonun yerinin tespitine en fazla iki ay için karar verileceği ve bu sürenin bir aydan fazla olmamak üzere bir defa daha uzatılabileceği düzenlenmektedir. Fakat bu süre, örgüt faaliyeti çerçevesinde işlenen suçlarla ilgili olarak, hâkim tarafından bir aydan fazla olmamak toplam üç ayı geçmemek üzere müteaddit defa uzatılabileceği düzenlemiştir.

Burada, alınacak tedbir süreleri boyunca kişisel verilerin işlenmesinde sınırların aşılmamasına dikkat edilmelidir. Aksi halde özellikle verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, amaca bağlılık-amaçla sınırlanma ilkesi, daha az müdahale eden yöntemin uygulanması ilkesi ve orantılılık (veri minimizasyonu) ilkesi ihlal edilmiş olacaktır.

Üçüncüsü, bu tedbirlerle elde edilen verilerin işlenme ve depolanma şartları ile ilgilidir. İptal edilen iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi işlemlerinin düzenlendiği Yönetmelik m. 9 hükmüne göre, elde edilen veriler arşivlenmekte, alt veri taşıyıcılarına nakledilebilmekte ve bu işlemler tutanağa kaydedilmekteydi. Zaten yeterli olmayan bu hükmün iptali ve yeni yönetmelik

çıkarılmaması sebebiyle, gizli soruşturma yöntemleriyle elde edilen verilerin depolanması ve imhasına yönelik işlemlerin nasıl gerçekleştirileceği belirsizdir. Bu durum öngörülebilirliği engellemesi sebebiyle hukuka aykırı olduğundan bir an önce giderilmesi şarttır. Aksi halde sadece kanun kapsamında yapılacak işleme faaliyetleri kamu görevlilerine geniş takdir yetkisi vermeye devam edecektir.

Bunu gidermek adına getirilecek yeni hüküm kapsamındaki her bir hususun verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, amaca bağlılık ilkesi, daha az müdahale eden yöntemin uygulanması ilkesi, orantılılık (veri minimizasyonu) ilkesi, verilerin doğruluğu ilkesi, veri güvenliği(bütünlük ve gizlilik) ilkesi ve hesap verilebilirlik ilkesi doğrultusunda güvence sağlayan açıklayıcı hükümlerle donatılması gereklidir. Ayrıca, yine gizlilik ilkesi gereğince, iletişimin denetlenmesinin gizliliğinin ihlali hem TCK m. 285 uyarınca soruşturmanın gizliliğinin ihlalini hem de kişilerin ses ve görüntülerinin yetkisiz olarak nakledilmesi sebebiyle de TCK m. 286'nın ihlali gündeme gelebilecektir. Bunun dışında başta kolluk görevlileri olmak üzere gizlilik herkes için söz konusu olup bunun ihlali halinde TCK m. 132 ve m. 137 deki suçlar oluşabilecektir[498].

Dördüncüsü, şüphelinin takibatına devam edilmemesi halinde, tespit ve dinlemeye ilişkin kayıtların CMK m. 137(3) uyarınca imhasına ilişkindir. Buna göre, imha hükümleri tedbir kararının uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da Cumhuriyet savcısı tarafından verilen kararın hâkim tarafından onaylanmaması hâlinde devreye girmektedir. İmhası söz konusu olan kayıtlar, Cumhuriyet savcısının denemi altında en geç 10 gün içinde yok edilmektedir. İmha işlemleri yakma, silme, kırma, kıyma vb. şeklinde olabilmektedir.

CMK m. 137(4)'e göre, tespit veya dinlemeye ilişkin kayıtların yok edilmesi hâlinde, soruşturmanın sona ermesinden ibaren en geç 15 gün içinde Cumhuriyet başsavcılığı tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgilisine yazılı olarak bilgi vermesi hüküm altına alınmaktadır. Bu hükmün, soruşturma evresinde kişisel verilerin işlenmesine ilişkin haberdar edilme hakkı doğrultusunda olduğunu belirtmek gerekir.

[498] Yenisey/Nuhoğlu, s. 447.

Fakat alınan koruma tedbiri sonucu elde edilen verilerin, kovuşturmaya yer olmadığına dair karar verilmesi ya da hâkim onayının alınamaması hali dışında bu madde açısından imha edilmemekte olduğu dikkat etmek gerekir. Bu doğrultuda, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinin de verilerin imhası kapsamına alınması gerekmektedir. Aksi halde, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi, amaca bağlılık-amaçla sınırlanma ilkesi, verilerin doğruluğu ilkesi ve sınırlı süre saklanma ilkesine düzenleme var olmaya devam edecektir.

Tüm bu sebeplerden ötürü, verilerin imhasına ilişkin diğer düzenlemelerin ve işlemlerin, kişisel verilerin korunmasındaki genel ilkelerden sınırlı süre saklanma ilkesi, verilerin doğruluğu ilkesi ve amaca bağlılık ilkesi açısından ve unutulma hakkı ile uyumlu olarak yeniden düzenlenmesi gerekmektedir.

Beşincisi, Yönetmelik m. 10(1)'de, CMK m. 135'e aykırı olarak verilen kararlara karşı itiraz edilebileceğinin düzenlenmişken, yönetmeliğin iptali sebebiyle, kişisel verilerin korunmasına ilişkin itiraz hakkının burada uygulama alanı bulamamakta olmasıdır. Keza CMK'da bu yönde bir düzenleme bulunmamaktadır. KVK Kanunu'nun soruşturma evresini kapsam dışı tutmasına rağmen bu maddelerin varlığı, önceleri soruşturma evresinde de kişisel verilerin bir nebze olsun korunmakta olduğunu göstermekteydi. Fakat yönetmeliğin iptali ile veri sahibi hakları açısından müspet olarak değerlendirilecek bu hükümlerin ortadan kalmasına yol açmıştır.

(2) PVSK açısından

PVSK Ek m. 7(2)'ye göre, polis de telekomünikasyon yoluyla yapılan iletişimi denetleyebilmektedir. Buna göre, bilişim suçlarının işlenmesinin önlenmesi amacıyla hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürünün, İstihbarat Dairesi Başkanı'nın veya bilişim suçları ile ilgili daire başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen veriler tespit edilebilmekte, dinlenebilmekte, sinyal bilgileri değerlendirilebilmekte ve kayda alınabilmektedir.

PVSK Ek m. 7(4)'te, tedbir kararının içeriğine ilişkin hükümler düzenlenmekte ve tedbir kararının terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak

gerekli görülmesi halinde, hâkim tarafından üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebileceği belirtilmektedir[499].

Bize göre, ortada kişisel verilerin işlenmesi bahsi söz konusu olduğundan sadece nedenlerin belirtilmesi yeterli değildir. İleri sürülen nedenlerin hukuka uygun olması ve ileri sürülen nedenler çerçevesinde yapılan işlemenin verilerin işlemesine yönelik genel ilkelere uygun olması gerekmektedir. Ayrıca kanun hükmünde sürelerin kararın verildiği tarihten mi yoksa tedbirin alındığı tarihten mi uygulanmaya başlayacağının muğlak bırakılması sebebiyle bir eleştiri de bulunmaktadır[500].

Ayrıca, Adlî görev ve yetkiler başlıklı PVSK Ek m. 6'nın son hükmüne göre, polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirmek zorunda tutulmaktadır. Burada yapılan işlemin hiçbir kararı gerektirmediğine ve sadece yetkili başsavcılığın tespiti amacıyla yapılmakta oluşuna dikkat edilmelidir.

Bunun dışında, PVSK Ek m. 7(7)'ye göre, madde kapsamında yürütülen faaliyetler çerçevesinde elde edilen kayıtlar emniyet ve asayişi sağlamak üzere Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine alınacak önleyici ve koruyucu tedbirler amacı dışında kullanılamamaktadır.

Önemle belirtmek gerekir bu fıkrada birbiriyle tezat iki yargı bulunmaktadır. Buna göre, hem amaçla bağlılık ilkesinin yer verilmesi nedeniyle önleyici-adli ayrımı yapılmakta hem de buradan önleyici amaçlı elde edilen verilerin, adli amaçlı olarak kullanılabileceği anlamı da çıkmaktadır. Bu yüzden hüküm bir yandan amaca bağlılık ilkesine uymakta diğer yandan uymamaktadır.

---

[499] PVSK Ek m. 7(4) düzenlemesine göre:
"Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları, ilgili internet bağlantı adresi veya bağlantıyı tesbite imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usûlle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir."
[500] Center, Nur/Zafer, Hamide: Ceza Muhakemesi Hukuku, İstanbul 2018, s. 475.

Bu durum verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine ters olduğundan bu ikiliğin bozularak önleyici amaçlı elde edilen verilerin, adli amaçlı olarak kullanılamayacağı hükmü getirilmelidir. Ayrıca, elde edilen bilgi ve kayıtların saklanmasında ve korunmasında ise gizlilik ilkesi geçerli olduğu düzenlenmiş olduğundan Veri güvenliği (bütünlük ve gizlilik) ilkesine uyumlu bir düzenlemenin varlığından bahsedilebilecektir.

PVSK açısından son olarak bir hükme daha değinmek gerekmektedir. Kayıp çocukların araştırılmasının düzenlendiği m. 13/A'ya göre, kaybolan çocukların bulunması amacıyla, polis, kayıp çocuğa ait veya başkasına ait olmakla birlikte kayıp çocuk tarafından kullanılan her türlü banka hesap hareketlerini talep edebilir, telekomünikasyon yoluyla iletişimini denetleyebilir ve sinyal bilgilerini değerlendirebilir.

Tedbir kararı, en çok bir ay için verilebilir; ancak bu süre, bir defaya mahsus olmak üzere bir ay daha uzatılabilir. Bu tedbir sulh ceza hâkiminin kararı veya gecikmesinde sakınca bulunan hallerde derhâl mahkemenin onayına sunulmak şartıyla mülki idare amirinin yazılı veya sonradan yazılı hale getirilmek üzere sözlü emri ile yapılabilmektedir.

Belirtmek gerekir ki bu tedbir esasen adli bir tedbir olarak CMK kapsamında yer alması daha doğrudur. Keza suç şüphesi altında adli bir vaka üzerine harekete geçilmektedir. Hali hazırda CMK'da bunun ile ilgili düzenleme olması sebebiyle önleyici mahiyette teknik araçlarla inceleme yapıp kişisel verilerin işleniyor olması hem önleyici-adli tedbir mantığına terstir hem de kişisel verilerin korunmasını dolambaçlı hale getirebilecektir.

Görüldüğü üzere, telekomünikasyon yoluyla iletişime ilişkin adli tedbirlere benzer olarak kişisel verilerin işlenmesine yönelik önleyici tedbirlerin yetkilendirildiği hükümler yer almaktadır. Böylece, kolluk makamlarına yargı mercileriyle bağlantılı olarak CMK'da düzenlenen koruma tedbirlerini alabilme salahiyeti verilmektedir. Uygulamada bu hükümlerin de kişisel verilerin korunmasına ilişkin genel ilkeler doğrultusunda gerçekleştiriliyor olmasına dikkat edilmelidir. Çünkü iletişimi denetleme yetkisinin kontrolsüz bir şekilde idari makamlara tanınması bizatihi korunmak istenen değerleri ortadan kaldırabilecek sonuçlar doğurabilir.

Anayasa Mahkemesi'nin bir kararında da belirttiği üzere, bu kapsamda verilecek yetkinin öncelikle kapsamı ve sınırları belli olması gereğinin yanı sıra yetkinin kötüye

kullanılmasını önleyecek ya da kötüye kullanımın zararlarını telafi edecek etkili denetim mekanizmalarının hukuk sisteminde öngörülmesi gerekmektedir[501].

(3) Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi yöntemi hakkında genel değerlendirmemiz

Mevzuattaki hükümlerde görüldüğü üzere kanun koyucu düzenlemekte olduğu iletişimin denetlenmesine ilişkin hükümlerde kişilerin kişisel verileri ile kamu düzeni arasında bir denge oluşturmaya çalışmaktadır. Bu doğrultuda, kişisel verilerin korunması hakkına getirilen sınırlamalarla kişisel iletişim verilerinin soruşturma evresinde işlenebilmektedir.

Fakat mevzuatta hali hazırda olduğu gibi kişisel verileri bu tedbirlerin uygulanması safhasında soruşturma evresinde yeterince korumamakta olan bu hükümlerin değiştirilmesi gerekmektedir. Bu doğrultuda, bu kısımda zikredilen koruma tedbirleri ile ilgili eleştiriye açık bazı hususları öne çıkarmak ve önerilerde bulunmak gerekmektedir.

Birincisi, CMK ve zikredilen kanunlardaki tedbir türlerine, uygulamada yapılmakta olan bazı işlemlerin de eklenmesidir. Buna göre, korumanın kapsamını geliştirmek amacıyla bu tedbirlere, iletişim ortamına girilmesi, iletişimin okunması, izlenmesi veya herhangi bir şekilde elde edilmesi lafzı eklenmelidir[502]. Çünkü uygulamada hali hazırda aynı maddeye dayanmak suretiyle bu işleme faaliyetleri gerçekleştirilmektedir. Bu faaliyetler işin gereği zaten uygulama alanı bulduğundan kanuni düzenlemede yer alması önemlidir.

İkincisi, tedbirlerin uygulanmakta olduğu katalog suçlarının kişisel verilerin korunmasına ilişkin yeterli hassasiyeti gözetecek şekilde düzenlenmemiş olmasıdır. Bir görüşe göre katalog suçları kapsamına kişisel verilerle ilgili suçlar da eklenerek verilerin korunması güvence altına alınmalıdır[503]. Böylece, başka türlü delil elde edilmesinin güç olduğu iletişim araç ve ortamlarının suç aracı olarak kullanılmasının önüne geçilmiş olunacaktır.

Her ne kadar özgürlükçü amaçla ileri atılmış olsa bile bu görüşü benimsemek mümkün değildir. Çünkü söz konusu tedbirler katalog suçlarla sınırlı olarak alınabilmektedir. Eğer kişisel verilerle ilgili suçların bu kataloğa eklenmesi söz konusu olursa verilerin soruşturma evresinde basit şüpheyle dahi işlenmesine imkân tanıyacaktır. Hiç şüphesiz

[501] E. 2014/122, K. 2015/123, KT: 30.12.2015, RG. 29640, 01.03.2016, 17 Şubat 2019.
[502] Gül/Alagöz, s. 164.
[503] Gül/Alagöz, s. 164.

polis devletini çağrıştıran bu sonuç hukuk güvenliğini tehlikeye atacağından demokratik toplum gerekliliklerileyle bağdaşmayacaktır.

Başka bir görüşe göre ise, m. 135'te öldüğünden şüphe edilen ya da bir suç neticesinde özgürlüğünden mahrum bırakıldığı değerlendirilen kişilerin sinyal bilgilerinin değerlendirilebileceğine dair bir hüküm bulunmamaktadır. Dolayısıyla, bu kişilerin kişisel verilerini işlenmesinde kanuni düzenlemenin açıkça bu hususu gözetmemiş olması alınacak koruma tedbirinin kanuni dayanağının olmadığını gösterir. Böyle bir durumda alınacak tedbirin kanunilik şartı sağlanmadığından ötürü hukuka aykırı olacağı ve bu durumu ortadan kaldıran özel bir düzenleme ihtiyacının olduğu belirtilmektedir[504]. Verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi gereğince biz de kişisel verilerin yeterli seviyede korunabilmesi için düzenlenme yapılması taraftarıyız.

Üçüncü olarak belirtmek gerekir ki, her ne kadar KVK Kanunu m. 28'ine göz yumması sebebiyle dolaylı olarak hukuka uygun görünse bile, kolluk görevlilerine önleyici olarak iletişimin denetlenmesi olanağının sağlanması eleştiriye açıktır. Yukarıda zikredilen kanunlarda kişisel verilerin korunmasına ilişkin ilkeler ve kişilerin talep edebilecekleri haklara ilişkin düzenlemeler büyük ölçüde yer almamaktadır. Örneğin, bu maddelerde hukuka aykırı tedbirler için tazminat maddesinin düzenlenmesi nedeniyle hüküm getirilmesi bir ihtiyaçtır[505]. Bu durum, kişisel verilerin korunması hukuku açısından önemli eksikliğe yol açmaktadır. Dolayısıyla, kişisel veriler alanındaki evrensel ilkelere aykırı olması sebebiyle düzenlemelerin bu haliyle hukuka aykırı olduğu belirtilmektedir[506].

Ayrıca, burada önemle üzerinde durmak gerekir ki sayılan bu tedbirler önleyici amaçlı olarak uygulanmakta ve CMK açısından kolluk olarak nitelendirilebilecek olan daire başkanlarının emri ile de yapılabilmektedir. Fakat bu tedbirlerin düzenlendiği CMK'da, adli amaçlı olarak alınması halinde hâkim veya savcı kararının gerekeceği düzenlenmiş ve fakat kolluk amirlerine böyle bir yetki tanınmamıştır. Dolayısıyla, zikredilen tedbirlerin alınması önleyici olursa gecikmesinde sakınca bulunan halin varlığında

[504] Gül/Alagöz, s. 164.
[505] Gül/Alagöz, s. 163.
[506] Dülger, 2019, s. 329.

CMK'daki tedbirin alınmasına göre daha kolay bir şekilde kolluk tarafından dahi alınabilecektir.

Üstelik CMK'ya göre alınacak adli tedbirlerde suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumu aranmakta iken PVSK'ya göre alınacak önleyici tedbirlerde bu şartlar aranmamaktadır. Bu durum kişisel verilerin korunması açısından hem daha az müdahale eden yöntemin uygulanması ilkesine aykırıdır hem de kanunun etrafından dolaşılmasına açık olduğunu göstermektedir.

Bu noktada, tezimizin önceki kısımlarında zikredilen kişisel verilerin soruşturma evresinde korunmasına ilişkin ilke ve haklara yönelik düzenlemenin yer alması gerektiğini, aksi halde işlemelerin hukuka aykırı olacağını ifade etmek gerekir[507]. Keza Anayasa Mahkemesi de adli tedbirlerde aranan sıkı şartların önleyici tedbirlere de hakkın korunması adına sirayet etmesi gerektiğini belirtmektedir[508].

b) Gizli soruşturmacı görevlendirilmesi yöntemi ile kişisel veri elde edilmesi

Gizli soruşturmacının düzenlenmekte olduğu CMK m. 139'a göre, soruşturma konusu olan m. 139(7)'de sayılan katalog suçlardan biri için işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebeplerinin bulunması halinde kamu görevlileri gizli soruşturmacı olarak görevlendirilebilmektedirler. Soruşturmacı kamu görevlisinin kimliği değiştirilebilmektedir. Bu madde bağlamında yapılacak görevlendirme kararı hâkim tarafından verilmektedir. Bunun için kişisel verilerin korunmasında daha az müdahale eden tedbire başvurma ilkesi gereğince başka surette delil elde edilememesi gerekmektedir.

Kişisel verilerin korunması ilkeleri açısından gizli soruşturmacının görevlendirilmesi hükmü yorumlandığında bazı hususlar öne çıkmaktadır. Bunlardan birincisi, soruşturmacının sahip olduğu kişisel verilerin, ilgili Cumhuriyet Başsavcılığında muhafaza edilmekte oluşudur. Buradaki veriler ve soruşturmacının kimliği, görevinin sona ermesinden sonra da veri güvenliği (bütünlük ve gizlilik) ilkesi gereğince gizli tutulmaktadır. Bu doğrultuda, gizli soruşturmacının gerçek verilerinin yanı sıra

[507] Daha fazla açıklama için üçüncü bölümün (II)(D) başlığına bakınız.
[508] Başvuru No: 2013/6367, 10.12.2015, 10 Şubat 2019.

soruşturmacı sıfatı gereği aldığı kimlik verilerinin kişisel verilerin korunması hükümlerinden yararlanacağını belirtmek gerekir.

İkincisi, soruşturmacının faaliyetleri ile ilgilidir. Buna göre, CMK m. 139(4) doğrultusunda gizli soruşturmacı, faaliyetlerini izlemekle görevlendirildiği örgüte ilişkin her türlü araştırmada bulunmak ve bu örgütün faaliyetleri çerçevesinde işlenen suçlarla ilgili delilleri toplamakla yükümlü tutulmaktadır. Burada da gizli soruşturmacının toplayabileceği delillerin amaca bağlılık-amaçla sınırlanma ilkesi ve orantılılık (veri minimizasyonu) ilkesi gereğince ancak bu örgütün faaliyetleri çerçevesinde işlenen suçlarla ilgili olması gerektiği gözlerden kaçırılmamalıdır.

Dolayısıyla, her ne kadar faaliyetlerini izlemekle görevlendirildiği örgüte ilişkin her türlü araştırmada bulunmakla yükümlü tutulmuş olsa bile, gizli soruşturmacının örgütle ilişkili kişilere ait olan fakat suçla bağlantılı olmayan kişisel verileri toplaması orantısız bir müdahale teşkil edecektir.

Üçüncüsü, CMK m. 139(6)'ya göre soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgilerin, görevlendirildiği ceza soruşturması ve kovuşturması dışında kullanılamayacağının hüküm altına alınmasıdır. Ayrıca suçla bağlantılı olmayan kişisel bilgilerin derhâl yok edilmesi gerektiği de düzenleme içerisinde yer almaktadır.

Verilerin imhasına ilişkin olarak, iptal edilen Yönetmelik m. 29'a göre, gizli soruşturmacı tedbirinin kullanılması sonucunda suç işlendiğine ilişkin bilgi elde edilmemişse, elde edilen tüm veriler, kovuşturmaya yer olmadığına dair karar verilmesinden sonra Cumhuriyet savcısı ve sorumlu kolluk görevlisi tarafından, toplam süre 10 günü geçmemek kaydı ile imha edilmekteydi. Yönetmelik iptal edildiği için, bu 10 günlük sürenin de artık uygulama alanı bulmaması yani verilerin derhâl imha edilmesi gerekir.

Dördüncüsü, gizli soruşturmacı, soruşturma süreci içerisinde kişisel suçla bağlantılı olmayan kişisel bilgileri topladığında soruşturmacının cezai sorumluluğuna gidilmiyor oluşudur. Çünkü kanun derhâl yok edilmesi kaydıyla suçla bağlantılı olmayan kişisel bilgiler toplanabileceğini ifade etmektedir. Elbette soruşturmacı kanunun çizdiği bu yetkiyi aşıp keyfi müdahalelerde bulunmamalıdır. Çünkü suçla bağlantılı olmayan kişisel bilgiler imha edilse bile gizli soruşturmacı başta olmak üzere süreç içerisinde yer alanlar

hassas verileri bile öğrenebilmektedirler. Dolayısıyla bu bilgilerin ifşa edilmemesi gerekmektedir.

Her ne kadar belgeler imha edilerek bir daha kimsenin bu bilgileri öğrenmemesi sağlanmaktaysa da görevli kişinin zihninden bu bilgilerin nasıl silineceği ya da silinmesinin gerekip gerekmediği ayrı bir problem teşkil etmektedir. Bu doğrultuda bir görüşe göre, veri sahibinin korunması için elde edilen verilerin hangi kısmının kullanılacağı ile ilgili bağımsız bir makam eliyle yapılacak önleyici bir denetim anayasal hakların korunması için bir gerekliliktir[509]. Bizim görüşümüze göre, tezin ilk kısımlarında kişisel veri ve sır arasındaki ayrımı yaparken de belirttiğimiz üzere, bu veriler sır kapsamında olmalı ve sırra ilişkin getirilecek yeni düzenlemeler kapsamında korunmalıdır.

Beşincisi, kişisel verilerin korunmasına hâkim olan genel ilkelerin sınırlayıcı etkisi sebebiyle, örgütün suçla bağlantısı olmayan faaliyetleri çerçevesinde işlenen suçlarla ilgili delilleri toplanırken de kişilere ait kişisel verilerin toplanmaması gerekmektedir.

Esasen uygulamada toplama işi soruşturmacıya bırakıldığı için hangi delillerin toplanacağı onun takdirine bırakılmaktadır. Bu yüzden verilerin işlendikten sonra imha ediliyor olması veri güvenliği(bütünlük ve gizlilik) ilkesi ve hesap verilebilirlik ilkesi açısından yeterli güvenceyi sağlamamaktadır.

Elbette bir delilin kendisi veya içeriğinin kişisel veri içermesi halinde bu onun delil olarak toplanmasını engellemez. Fakat ölçüsüz davranıldığı takdirde orantılılık (veri minimizasyonu) ilkesi gereği toplanan delillerin hukuka uygunluğundan bahsedilemeyeceği gibi ceza kanunları açısından suç işlendiği de ileri sürülebilecektir.

Bizim görüşümüze göre, soruşturmacının hiçbir ilke ve sınıra tabi olmadan masumiyet karinesinden hala yararlanmakta olan şüphelinin kişisel verilerini kendi takdirince toplayabilmesine yol açan düzenlemeler tutarsız ve orantısızdır. Bu konuda, Türk hukukunda kişisel verilerin korunmasına ilişkin soruşturma evresine uygulanacak meri kuralların yokluğu sebebiyle bu konuda boşluk söz konusudur.

c) Teknik araçlarla izleme yöntemi ile kişisel veri elde edilmesi

[509] Kanadoğlu, s. 90.

Teknik araçlarla izlemeye ilişkin hükümler CMK m. 140'ta düzenlenmektedir. Buna göre, CMK m. 140(2)'da yer alan suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebepleri bulunması halinde şüphelinin kamuya açık yerlerdeki faaliyetleri ve iş yeri teknik araçlarla izlenebilmekte, ses veya görüntüsü kayda alınabilmektedir. Bu işlem teknik araçlarla izleme olarak tanımlanmaktadır.

Burada izlemeden maksat, belirli bir süre devam eden ve kişilerin hareket veya ilişkilerinin görüntülenmesi ya da yaptıkları konuşmalarının tespiti amacını güden işlemlerdir. Kişilerin izlenmesini, dinlenmesini kimi zaman da seslerinin kaydedilmesini kapsayan bu işlemler, cihazlı takipler, şebek takipler, suiistimalle takipler ve akustik dinlemeler olarak dört şekilde yapılmaktadır[510]. Tedbirin kapsamı açısından belirtmek gerekir ki kişilerin işledikleri suçların delil, iz, emare ve eserlerinin tespiti maksadıyla yapılmış bireysel saptamalar izleme sayılmamaya devam etmelidir[511].

Teknik araçlarla izleme kararının hâkim tarafından verilmesi gerekmektedir. Fakat gecikmesinde sakınca bulunan hâllerde sunulan kararın hâkim tarafından onaylanması kaydıyla Cumhuriyet savcısı tarafından da verilebilmektedir. Hâkim onayına süresinde sunulmaması veya hâkim tarafından aksine karar verilmesi hâlinde kayıtların derhâl imha edilmesi gerekmektedir.

Bu tedbirde kişisel verilerin korunmasına ilişkin ilkeler açısından öne çıkan bazı dikkate değer noktalar bulunmaktadır. Bunlardan birincisi, bu tedbirin kişinin kamuya açık yerlerdeki faaliyetlerini kapsamakta olduğundan kişinin kişisel verileriyle ilgili üç alan teorisinin çekirdek alanı hariç diğer iki alanında yer alan kişisel verileri içermesinin yüksek ihtimal olmasıdır. Kişinin kamuya açtığı verilerinin işlenmesinde kural olarak bir sakınca olmasa da bu tedbirin belli bir kişiyi odağa alınacak şekilde gerçekleştirilmemesi gerekmektedir.

---

[510] Gül/Alagöz, s. 162.

[511] Tedbirin kapsamı hükmü iptal edilen Yönetmelik m. 17'de düzenlenmektedir:
"(1) Teknik araçlarla izlemeye ait talep ve kararlar aynı soruşturmayla ilgili olmak üzere birden fazla kişiyi kapsayabilir.
(2) Karar süresince, izlenecek kişilerin iş yeri veya kamuya açık yerlerdeki tüm faaliyetleri izlenebilir, görüntülenebilir ve kayda alınabilir. Kişilerin konut olarak kullandığı yerlerde teknik araçlarla izleme yapılamaz.
(3) İzlemeden maksat, belirli bir süre devam eden ve kişilerin hareket veya ilişkilerinin görüntülenmesi ya da yaptıkları konuşmalarının tespiti amacını güden işlemlerdir.
(4) Kişilerin işledikleri suçların delil, iz, emare ve eserlerinin tespiti maksadıyla yapılmış bireysel saptamalar izleme sayılmaz."

Bu maddede düzenlenen yetki ile ise belli bir kişi odağa alınması hedeflenmektedir. Kanunun verdiği yetki olduğundan hukuka uygunluk sebebidir. Elbette bu uygunluk sebebi, maddede belirtilen amacın dışına çıkmamalı ve işleme faaliyeti ölçülü miktarda olmalıdır. Öte yandan, üç alan teorisinin çekirdek kısmının yani kişinin mahrem verilerinin bu madde bağlamında işlenememesi gerekmektedir. Zaten kanun koyucu da bu benimsemiş olmalı ki bu madde hükümlerinin kişinin konutunda uygulanamayacağını düzenlemektedir.

İkinci olarak belirtmek gerekir ki, elde edilen delillerin maddede sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamayacağını düzenlemekte olduğundan kanun koyucu hem amaçla bağlılık ilkesine uymakta hem de kişinin masumiyetlik karinesinin ihlal edilmesinin önüne geçmek istemektedir.

Üçüncüsü, veri güvenliği(bütünlük ve gizlilik) ilkesi uyarınca bu tedbir için verilen kararların tutanakla Cumhuriyet başsavcılığına teslim edilmesi ve mahkeme kaleminde kalan suretin gizli tutulması için ilgili hâkim tarafından gerekli tedbirlerin alınmasıdır.

Bu doğrultuda iptal edilen Yönetmelik m. 15(4)'te söz konusu kararların tedbir süresince değişik iş kartonuna takılmayacağı ve tedbirin sona erdiği öğrenildiğinde ilgili kartonuna ilave edileceği düzenlenmekteydi. Ayrıca gizliliğe verilen önem sebebiyle m. 15(5)'de bütün bu işlemler sırasında gizliliğe uyulur denilerek bu husus vurgulanmaktaydı. Bu hükümlerin kişisel verilerin soruşturma evresinde bütünlüğü ve gizliliği ilkesi çerçevesinde yeniden uygulama bulacak şekilde yürürlüğe girmesi, verilerin işlenmesi ilkeleri doğrultusunda atılacak olumlu bir adım olacaktır.

Dördüncüsü, bu tedbir, başka suretle delil elde edilememesi hâlinde alınabilecek olacağından kişisel verilere daha az müdahale eden yöntemin uygulanması ilkesi burada da uygulamadadır. Bu yüzden iptal edilen Yönetmelik m. 16'da, teknik araçlarla izlemeye ilişkin talep ve kararlarda, başka suretle delil elde edilmesi imkânının bulunmadığı hakkındaki açıklama, bilgi veya belgelerin yer alması gerektiği de öngörülmüştür.

Bu doğrultuda, kişisel verilerin gizliliğine ilişkin güvence sağlamak açısından kişilerin görüntülerinin yalnızca izlenmesi yeterli ise ayrıca bunların kayıt altına alınmasına gerek

yoktur[512]. Verilerin korunmasına yönelik müspet bir düzenleme olması sebebiyle tekrardan yürürlüğe girmesi gereken hükümlerdendir.

Beşincisi, orantılılık (veri minimizasyonu) ilkesi açısından hükümlerin değerlendirilmesidir. Öncelikle iptal edilen Yönetmelik m. 16 uyarınca tedbir talebi ve kararı kapsamı içerisinde teknik araçlarla izleme süresinin belirtilmesi gerektiği düzenlenmekteydi. Akabinde, iptal edilen Yönetmelik m. 20(2)'ye göre, teknik araçlarla izlemeye en fazla dört haftalık süre için karar verilmekte ve gerektiğinde bir defaya mahsus olmak üzere dört haftadan fazla olmamak kaydıyla uzatılmaktaydı.

Buraya kadar ki düzenlemeler orantılılık açısından olması gerektiği gibi olduğundan tekrardan yürürlüğe girmesi gerekmektedir. Aksi halde, verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesine, amaca bağlılık-amaçla sınırlanma ilkesine ve orantılılık (veri minimizasyonu) ilkesine aykırılık teşkil edeceğinde olması gereken verilerin korunmasını sınırlayacak müdahalenin dengeli olmasını sağlayacak hükümlerin düzenlenmesidir.

III. KİŞİSEL VERİLERİN SORUŞTURMA EVRESİNDE İŞLENMESİNE İLİŞKİN DİĞER KURUMLAR

A. Genel Olarak

CMK'da koruma tedbirleri arasında düzenlenmeyen fakat soruşturma evresinde kişisel verilerin korunması hukuku açısından değer ifade eden diğer hükümler de bulunmaktadır. Ayrıca bu hususlara ilişkin olarak çeşitli özel kanun, yönetmelik ve yönergeler de çıkarılmaktadır.

Bu kısımda bu hususlara ilişkin hükümler soruşturma evresinde kişisel verilerin işlenmesine ilişkin ilkeler açısından değerlendirilmektedir. Bu doğrultuda, öncelikle uzlaştırmaya ilişkin hükümler olmak üzere adli sicile ve adli bilişime ilişkin noktalar yorumlanmaktadır.

B. Uzlaştırmada Kişisel Veriler

[512] Küzeci, s. 432.

Uzlaştırmaya ilişkin hükümler CMK m. 253 ila 255 arasında düzenlenmektedir. Soruşturma sürecine ilişkin uzlaşma hükümlerinin düzenlenmekte olduğu m. 253'te katalog halinde sayılan suçlarda savcılık tarafından şüpheli ile mağdur veya suçtan zarar gören gerçek veya özel hukuk tüzel kişisinin uzlaştırılması girişiminde bulunulmaktadır.

CMK m. 253(15)'e göre, uzlaşma müzakereleri sonunda uzlaştırmacı bir rapor hazırlayarak kendisine verilen belge örnekleriyle birlikte uzlaştırma bürosuna vermektedir. Uzlaşmanın gerçekleşmesi halinde, tarafların imzalarını da içeren raporda, ne suretle uzlaşıldığı ayrıntılı olarak açıklanmaktadır. CMK m. 253(20)'e göre ise, uzlaştırma müzakereleri sırasında yapılan açıklamalar, herhangi bir soruşturma ve kovuşturmada ya da davada delil olarak kullanılamamaktadır.

Tüm bu kurallar çerçevesinde, kişisel veriler açısından belirtmek gerekir ki uzlaşma raporunda yer alan kişisel veriler bağlı bulunduğu soruşturma da dâhil hiçbir yargılamada delil olarak ileri sürülememesi gerekmektedir. Ayrıca, bu uzlaşma raporu içerisinde de suçtan bağımsız olan kişisel veriler yer almamalıdır. Aksi halde, uzlaştırma süreci kapsamında verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi ve amaca bağlılık-amaçla sınırlanma ilkesi açısından kişisel verilerin korunmasının ihlali gündeme gelebilecektir.

C. Adli Sicil Kanunu

5352 sayılı Adli Sicil Kanunu kesinleşmiş ceza ve güvenlik tedbirlerine mahkûmiyete ilişkin bilgilerin otomatik işleme tâbi bir sistem kullanılarak toplanmasına, sınıflandırılmasına, değerlendirilmesine, muhafaza edilmesine ve gerektiğinde en seri ve sağlıklı biçimde ilgililere bildirilmesine dair usul ve esasları belirlemektedir.

Bu doğrultuda, Türk mahkemeleri tarafından vatandaş veya yabancı hakkında verilmiş ve kesinleşmiş mahkûmiyet hükümleri adlî sicile kaydedilip Adalet Bakanlığı Adlî Sicil ve İstatistik Genel Müdürlüğündeki Merkezî Adlî Sicil'inde tutulmaktadır.

Soruşturma evresi açısından iki husus öne çıkmaktadır. Birincisi, soruşturma evresinde verilen kararların kanunda kural olarak ne kaydedilecek ne de kaydedilmeyecek belgeler arasında sayılmıyor oluşudur[513]. İstisna olarak m. 6'da kamu davasının açılmasının

[513] Adlî sicile kaydedilecek bilgiler hükmü Adil Sicil Kanunu m. 4'te düzenlenmektedir:

ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararlar, ancak bir soruşturma ile bağlantılı olarak mahkeme, hâkim veya Cumhuriyet Başsavcılığı tarafından istenmesi halinde verilmek üzere kaydedileceği belirtilmiştir.

"(1) Türk mahkemeleri tarafından vatandaş veya yabancı hakkında verilmiş ve kesinleşmiş mahkûmiyet hükümleri adlî sicile kaydedilir. Bu bağlamda;
a) Hapis cezaları ile ilgili olarak;
1. Hapis cezasına mahkûmiyet kararı,
2. Koşullu salıverilme kararı,
3. Koşullu salıverilmede denetim süresinin uzatılmasına ilişkin karar,
4. Koşullu salıverilme kararının geri alınmasına dair karar,
5. Hapis cezasının infazının tamamlandığı hususu,
b) Hapis cezasının ertelenmesi halinde;
1. Denetim süresi,
2. Denetim süresinin yükümlülüklere uygun veya iyi halli olarak geçirilmesi dolayısıyla cezanın infaz edilmiş sayıldığı hususu,
3. Ertelenen hapis cezasının infaz kurumunda çektirilmesine ilişkin karar
c) Adlî para cezası ile ilgili olarak;
1. Adlî para cezasına ilişkin mahkûmiyet hükmü,
2. Adlî para cezasının ödenmek suretiyle infaz edildiği hususu,
3. Adlî para cezasının tazyik hapsi suretiyle kısmen veya tamamen infaz edildiği hususu,
4. Adlî para cezasının tazyik hapsinden sonra kalan kısmının ödenmek suretiyle infaz edildiği hususu,
d) Kısa süreli hapis cezasına seçenek yaptırıma mahkûmiyet halinde;
1. Kısa süreli hapis cezasına seçenek yaptırım olarak, adlî para cezasına mahkûmiyet veya güvenlik tedbiri uygulanması hükmü,
2. Kısa süreli hapis cezasına seçenek yaptırım olarak hükmedilen güvenlik tedbirinin gereklerinin yerine getirilmemesi dolayısıyla hapis cezasının infazına ilişkin karar,
3. Kısa süreli hapis cezasına seçenek yaptırım olarak hükmedilen güvenlik tedbirinin değiştirilmesine ilişkin karar,
e) Belli hakları kullanmaktan yoksun bırakılma ile ilgili olarak;
1. Kasten işlenen bir suç nedeniyle hapis cezasına mahkûmiyetin kanunî sonucu olarak yoksun kalınan haklara cezanın ertelenmesi dolayısıyla getirilen istisnaya ilişkin karar,
2. Mahkûmiyet hükmüyle bağlantılı olarak verilen, belli bir hak ve yetkinin kullanılmasının veya belli bir meslek veya sanatın icrasının yasaklanmasına ya da sürücü belgesinin geri alınmasına ilişkin karar,
f) Türk vatandaşı hakkında yabancı mahkemeden verilmiş ve kesinleşmiş olan mahkûmiyet kararının Türk hukuku bakımından doğurduğu hak yoksunluklarına ilişkin olarak Cumhuriyet savcısının istemi üzerine mahkemece verilen karar,
g) Ceza mahkûmiyetini bütün sonuçlarıyla ortadan kaldıran şikayetten vazgeçme veya etkin pişmanlık dolayısıyla verilen karar,
h) Ceza zamanaşımının dolduğunun tespitine ilişkin karar,
i) Genel veya özel affa ilişkin kanun; özel affa ilişkin Cumhurbaşkanlığı kararı,
j) Askerî Ceza Kanununa göre verilmiş mahkûmiyet kararlarındaki ferî cezalar,
k) Akıl hastalığı nedeniyle hükmedilen güvenlik tedbirlerine ilişkin kararlar,
Adlî sicile kaydedilir.
(2) Kanun yararına bozma veya yargılamanın yenilenmesi sonucunda verilen mahkûmiyet hükmü ya da eski hükümde değişiklik yapan tüm hüküm ve kararlar açısından da birinci fıkra hükümleri uygulanır.
(3) Kanun gereği olarak gerçek kimliği saklı tutulan kişilerin adlî sicil ve arşiv kayıtlarına ilişkin usul ve esaslar yönetmelikle düzenlenir."

Adlî sicile kaydedilmeyecek bilgiler Adli Sicil Kanunu m. 5'te düzenlenmektedir:
"(1) Türk mahkemeleri tarafından verilmiş olsa bile;
a) Disiplin suçlarına ve sırf askerî suçlara ilişkin mahkûmiyet hükümleri,
b) Disiplin veya tazyik hapsine ilişkin kararlar,
c) İdarî para cezasına ilişkin kararlar,
Adlî sicile kaydedilmez."

Maddenin ikinci fıkrasındaki özel hükme göre, karşılıksız yararlanma suçunda etkin pişmanlıktan yararlanması dolayısıyla şüpheli, sanık veya hükümlü hakkında verilen kararların adlî sicilde on beş yıl süreyle bunlara mahsus bir sisteme kaydedileceği hüküm altına alınmaktadır.

Bu açıdan belirtmek gerekir ki, zikredilen süre, suçun yaptırımının en fazla üç yıl olduğu düşünüldüğünde ziyadesiyle fazladır. Bu yüzden, soruşturma evresinde verilerin işlenmesine hâkim olan ilkelerden amaca bağlılık-amaçla sınırlanma ilkesini, orantılılık (veri minimizasyonu) ilkesini ve sınırlı süre saklanma ilkesini ihlal etmektedir.

İkinci husus, arşiv bilgilerinin soruşturma evresinde Cumhuriyet başsavcılıkları, hâkim veya mahkemeler tarafından diğer davalarda kullanılmak üzere istenebiliyor olmasıdır[514]. Bu doğrultuda bir suça ilişkin soruşturma kapsamında adlî sicil ve arşiv kayıtlarında; Mahkeme, hâkim ve Cumhuriyet Başsavcılığı doğrudan doğruya, kolluk ve diğer kamu kurum ve kuruluşları Adalet Bakanının onayı ile sorgulama yapabilmektedirler[515].

Adli sicil belgesinde yer alan kayıtlar doğrudan ya da dolaylı olarak bir kişiyi belirleyen ya da belirlenebilir kıldığı ölçüde kişisel veri olacaktır. Bu yüzden bu verilerin soruşturma evresinde işlenmesine hâkim olan ilkeler ve ilgili kişinin hakları doğrultusunda yeterli güvencelere haiz olması gerekmektedir. Bu doğrultuda, veri güvenliği(bütünlük ve

---

[514] Arşiv bilgilerinin istenmesi hükmü Adli Sicil Kanunu m. 10'da düzenlenmektedir:
"(1) Arşiv bilgileri;
a) Kullanılış amacı belirtilmek suretiyle, kişinin kendisi veya vekâletnamede açıkça belirtilmiş olmak koşuluyla vekili,
b) Bir soruşturma veya kovuşturma kapsamında Cumhuriyet başsavcılıkları, hâkim veya mahkemeler,
c) Yetkili seçim kurulları,
d) Özel kanunlarda gösterilen hallerde ilgili kamu kurum ve kuruluşları, Tarafından istenebilir.
(2) Kanunda açıkça belirtilmediği takdirde, kişi hakkında alınacak bir karar veya yapılacak bir işlemle ilgili olarak, bir yakınının adlî sicil ve arşiv kayıtları istenemez ve bu bilgiler, kişiyi herhangi bir haktan yoksun bırakmak için dayanak olarak kullanılamaz.
(3) On sekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir."

[515] Adlî sicil ve arşiv kayıtlarında sorgulama yetkisi verilmesi hükmü Adli Sicil Kanunu m. 13'te düzenlenmektedir:
"(1) Bir suça ilişkin soruşturma ve kovuşturma kapsamında adlî sicil ve arşiv kayıtlarında;
a) Mahkeme, hâkim ve Cumhuriyet Başsavcılığı doğrudan doğruya,
b) Kolluk ve diğer kamu kurum ve kuruluşları Adalet Bakanının onayı ile
Sorgulama yapabilirler.
(2) Kamu kurum ve kuruluşları, mevzuatın adli sicil ve arşiv kaydı alınmasını öngördüğü hallerde, Adalet Bakanlığının belirleyeceği usul ve esaslar çerçevesinde ilgili kişiler hakkında adli sicil ve arşiv kayıtlarında sorgulama yapabilirler. Gerçek kişiler de kendileriyle ilgili adli sicil ve arşiv kayıtlarını, Adalet Bakanlığının belirleyeceği usul ve esaslar çerçevesinde ve güvenli kimlik doğrulama araçlarını kullanarak sorgulayabilir, sonucu fiziki veya elektronik ortamda merciine verebilirler."

gizlilik) ilkesi uyarınca kanun m. 11'de adlî sicil ve arşiv bilgileri gizli olacağı ve bu bilgilerin görevlilerce açıklanamayacağı düzenlenmektedir.

Bu minvalde, m. 8'de adli sicil bilgilerini verebilecek merciler gösterilmektedir. Bu mercilerde görevli kişiler, yetkisi olmayan kişilere adli sicil bilgisini vermesi durumunda TCK m. 137'deki suçun faili olabilecektir[516].

Ayrıca, amaca bağlılık-amaçla sınırlanma ilkesi uyarınca bu Kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamayacağı da hükme bağlanmaktadır. Buradan hareketle verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi için diğer ilkelerin de kanuna eklenmesi gerekmektedir.

D. Adli Bilişim

Adli bilişim, bir bilgisayarda veya iletişim aygıtındaki silinmiş veya var olan elektronik delille ilgili yapılan araştırmayı ifade etmektedir. Adli bilişimde görevlendirilmiş uzmanlar sayesinde bilişim ile ilgili bulgular incelenmekte ve suçu aydınlatılmasında kullanılan deliller arasında önemli bir yer alabilmektedir. Bilgisayar delillerini muhafaza etme, tanımlama, sonuç çıkarma ve belgeleme ile uğraşan görevliler bir bakıma bilgisayar disk sürücüleri üzerinde otopsi yapmaktadırlar[517].

Adli bilişim daha çok bilgisayar diskleriyle uğraşmakla beraber aslında bütün elektronik delillerin çözümü için adli bilişime başvurulmaktadır. Dolayısıyla, yüzden ceza yargılamasında delillerin elde edilmesi ve değerlendirilmesi amacıyla adli bilişime sıklıkla müracaat edilmektedir[518].

Kişisel verilerin soruşturma evresinde işlenmesine hâkim olan ilkelerin adli bilişim sürecinde uygulanmasını engelleyici bir sebep bulunmamaktadır. Fakat ilgili koruyucu düzenlemelerin yokluğu söz konusudur. Bu doğrultuda kişisel veri olan veya içeren delillerin korunabilmesi için verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi uyarınca gerekli düzenlemelerin yapılması şarttır.

Bu düzenlemelerde, amaca bağlılık-amaçla sınırlanma ilkesi, daha az müdahale eden yöntemin uygulanması ilkesi, orantılılık (veri minimizasyonu) ilkesi, verilerin doğruluğu

[516] Bayraktar, s. 635.
[517] Karagülmez, Ali: Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara 2014, s. 490.
[518] Karagülmez, s. 490.

ilkesi, sınırlı süre saklanma ilkesi, veri güvenliği(bütünlük ve gizlilik) ilkesi ve hesap verilebilirlik ilkesi ve ilgili kişinin hakları doğrultusunda işin gereğine uygun düştüğü ölçüde dengeli ve yeterli güvencelerin sağlanması gerekir.

E. Tazminat İstemi

Soruşturma sürecinde alınan hukuka aykırı koruma tedbirleri sebebiyle hakları ihlal edilen kişilerin tazminat isteminde bulunma hakkı vardır[519]. Buna göre, soruşturma sürecinde tezimizin yöntemler kısmında belirtmekte olduğumuz her bir kanuna aykırılık hali için veri öznesi olan kişiler, maddî ve manevî her türlü zararlarını, Devletten isteyebilmektedirler.

Bu talebin, karar veya hükümlerin kesinleştiğinin ilgilisine tebliğinden itibaren üç ay ve her hâlde karar veya hükümlerin kesinleşme tarihini izleyen bir yıl içinde yapılması gerekmektedir[520].

---

[519] Koruma tedbirleri nedeniyle tazminat istemi hükmü CMK m. 141'de düzenlenmektedir:
"(1) Suç soruşturması veya kovuşturması sırasında;
a) Kanunlarda belirtilen koşullar dışında yakalanan, tutuklanan veya tutukluluğunun devamına karar verilen,
b) Kanunî gözaltı süresi içinde hâkim önüne çıkarılmayan,
c) Kanunî hakları hatırlatılmadan veya hatırlatılan haklarından yararlandırılma isteği yerine getirilmeden tutuklanan,
d) Kanuna uygun olarak tutuklandığı hâlde makul sürede yargılama mercii huzuruna çıkarılmayan ve bu süre içinde hakkında hüküm verilmeyen,
e) Kanuna uygun olarak yakalandıktan veya tutuklandıktan sonra haklarında kovuşturmaya yer olmadığına veya beraatlerine karar verilen,
f) Mahkûm olup da gözaltı ve tutuklulukta geçirdiği süreleri, hükümlülük sürelerinden fazla olan veya işlediği suç için kanunda öngörülen cezanın sadece para cezası olması nedeniyle zorunlu olarak bu cezayla cezalandırılan,
g) Yakalama veya tutuklama nedenleri ve haklarındaki suçlamalar kendilerine, yazıyla veya bunun hemen olanaklı bulunmadığı hâllerde sözle açıklanmayan,
h) Yakalanmaları veya tutuklanmaları yakınlarına bildirilmeyen,
i) Hakkındaki arama kararı ölçüsüz bir şekilde gerçekleştirilen,
j) Eşyasına veya diğer mal varlığı değerlerine, koşulları oluşmadığı halde el konulan veya korunması için gerekli tedbirler alınmayan ya da eşyası veya diğer mal varlığı değerleri amaç dışı kullanılan veya zamanında geri verilmeyen,
k) Yakalama veya tutuklama işlemine karşı Kanunda öngörülen başvuru imkânlarından yararlandırılmayan, Kişiler, maddî ve manevî her türlü zararlarını, Devletten isteyebilirler.
(2) Birinci fıkranın (e) ve (f) bentlerinde belirtilen kararları veren merciler, ilgiliye tazminat hakları bulunduğunu bildirirler ve bu husus verilen karara geçirilir.
(3) Birinci fıkrada yazan hâller dışında, suç soruşturması veya kovuşturması sırasında kişisel kusur, haksız fiil veya diğer sorumluluk hâlleri de dâhil olmak üzere hâkimler ve Cumhuriyet savcılarının verdikleri kararlar veya yaptıkları işlemler nedeniyle tazminat davaları ancak Devlet aleyhine açılabilir.
(4) Devlet, ödediği tazminattan dolayı görevinin gereklerine aykırı hareket etmek suretiyle görevini kötüye kullanan hâkimler ve Cumhuriyet savcılarına bir yıl içinde rücu eder."
[520] Tazminat isteminin koşulları CMK m. 142'de düzenlenmektedir:

Kişisel verilerin hukuka aykırı olarak ihlal edildiği kesinse, burada ifade etmek gerekir ki kişinin kişilik hakkı ihlal edilmektedir. Özel hukuk açısından TMK m. 24'e göre, hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilmektedir.

Kişisel verilerin ihlali kişilik hakkı ihlali olduğundan, CMK m. 141 uyarınca tazminat talebi reddedilen kişiler, bu hükümlere dayanarak hukuk mahkemelerinde dava açabilmeli diye düşünmekteyiz. Ayrıca eğer verilerin ihlali idarenin kolluğundan sadır olmuşsa, hakkın ihlali sebebiyle idari yargıda tam yargı davası da açılabilir.

Bizim görüşümüze göre, soruşturma sürecinde kişisel verileri hukuka aykırı olarak işlenen kişiler, bu maddeye göre istemde bulunabilmelidirler. Hukuka aykırılık çoğu zaman soruşturma evresinde verilerin işlenmesine hâkim olan ilkeler ve hakların kanuni düzenlemelerde yer almaması dolayısıyla olabilecektir.

"(1) Karar veya hükümlerin kesinleştiğinin ilgilisine tebliğinden itibaren üç ay ve her hâlde karar veya hükümlerin kesinleşme tarihini izleyen bir yıl içinde tazminat isteminde bulunulabilir.
(2) İstem, zarara uğrayanın oturduğu yer ağır ceza mahkemesinde ve eğer o yer ağır ceza mahkemesi tazminat konusu işlemle ilişkili ise ve aynı yerde başka bir ağır ceza dairesi yoksa en yakın yer ağır ceza mahkemesinde karara bağlanır.
(3) Tazminat isteminde bulunan kişinin dilekçesine, açık kimlik ve adresini, zarara uğradığı işlemin ve zararın nitelik ve niceliğini kaydetmesi ve bunların belgelerini eklemesi gereklidir.
(4) Dilekçesindeki bilgi ve belgelerin yetersizliği durumunda mahkeme, eksikliğin bir ay içinde giderilmesini, aksi hâlde istemin reddedileceğini ilgiliye duyurur. Süresinde eksiği tamamlanmayan dilekçe, mahkemece, itiraz yolu açık olmak üzere reddolunur.
(5) Mahkeme, dosyayı inceledikten sonra yeterliliğini belirlediği dilekçe ve eki belgelerin bir örneğini Devlet Hazinesinin kendi yargı çevresindeki temsilcisine tebliğ ederek, varsa beyan ve itirazlarını on beş gün içinde yazılı olarak bildirmesini ister.
(6) İstemin ve ispat belgelerinin değerlendirilmesinde ve tazminat hukukunun genel prensiplerine göre verilecek tazminat miktarının saptanmasında mahkeme gerekli gördüğü her türlü araştırmayı yapmaya veya hâkimlerinden birine yaptırmaya yetkilidir.
(7) Mahkeme, kararını duruşmalı olarak verir. İstemde bulunan ile Hazine temsilcisi, açıklamalı çağrı kâğıdı tebliğine rağmen gelmezlerse, yokluklarında karar verilebilir.
(8) Karara karşı, istemde bulunan, Cumhuriyet savcısı veya Hazine temsilcisi, istinaf yoluna başvurabilir; inceleme öncelikle ve ivedilikle yapılır.
(9) Tazminat davaları nedeniyle Avukatlık Asgari Ücret Tarifesi gereğince hesaplanan nisbî avukatlık ücreti ödenir. Ancak, ödenecek miktar Tarifede sulh ceza hâkimliklerinde takip edilen işler için belirlenen maktu ücretten az, ağır ceza mahkemelerinde takip edilen davalar için belirlenen maktu ücretten fazla olamaz.
(10) Tazminata ilişkin mahkeme kararları, kesinleşmeden ve idari başvuru süreci tamamlanmadan icra takibine konulamaz. Kesinleşen mahkeme kararında hükmedilen tazminat ile vekâlet ücreti, davacı veya vekilinin davalı idareye yazılı şekilde bildireceği banka hesap numarasına, bu bildirimin yapıldığı tarihten itibaren otuz gün içinde ödenir. Bu süre içinde ödeme yapılmaması halinde, karar genel hükümler dairesinde infaz ve icra olunur."

Bunun gibi kişisel verilerin korunması hakkına yönelik orantısız ve ölçüsüz uygulanan tedbirler sebebiyle de söz konusu olabilecektir. Sonuçta var olan kanuni düzenlemeler uluslararası belgelerdeki standartlarla aynı durumda değildir.

Bu görüşümüzün temel dayanağı KVK Kanunu'ndaki istisna hükmünün soruşturma evresini doğrudan doğruya ve tamamen KVK Kanunu kapsamında tutarak âdeta kişisel verilerin bu evrede korunmamasını öngören kronik problemdir. Yapılan bu düzenlemenin kapsamının genel ve istisnasız olması nedeniyle bu kanun hükmü aslında insan hakları kapsamında korunan kişisel verilerin korunması hakkına yönelik sürekli bir ihlal niteliğindedir. Bu yüzden, hakkında koruma tedbirleri alınan şüphelilerin dosyaları üzerinde yapılacak işleme faaliyetleri sonucu büyük olasılıkla kişisel verilerin korunması hukukuna aykırı olacaktır.

Keza kanunun kendisi veri sorumlusu sayılabilecek olan hâkim, savcı ve kolluk görevlilerini bu konuda yönlendirmemekte âdeta verileri hukuka aykırı olarak işlemelerine fırsat oluşturmaktadırlar.

KVK Kanunu'nun hukuka aykırı işlemelere izin veren güncel durumu sebebiyle, kişisel verilerin işlendiği her soruşturmada verilerin korunmasına yönelik orantısız müdahalenin varlığı söz konusu olacaktır.

Dolayısıyla CMK m. 141 uyarınca kişilerin tazminat talep edebilmeleri mümkündür. Bu yüzden, var olan ihlal sebebiyle tazminatın talep edilmesine KVK m. 28 karşıt bir gerekçe teşkil edip engel olamaz diye düşünmekteyiz.

SONUÇ

Anayasa m. 20(3)'te güvence altına alınan kişisel verilerin koruması hakkının tesisi için özel olarak hazırlanan 6698 sayılı Kanun, 2016 yılında yürürlüğe girmiştir. İlgili uluslararası düzenlemeler ve daha çok 95/46/EC sayılı Direktif doğrultusunda hazırlanan bu kanun kapsamında yer alan hükümler, kişisel verilerin insan hakları kapsamında korunmasını güvenceye alma amacını gütmektedir. Bu alanda düzenlenen ilk kanun olması ve verilerin korunmasını belli şartlara tabi tutması sebebiyle veri işleyicileri için de oldukça önem taşımaktadır. Her ne kadar doktrin ve uygulamada korumanın özel hukuk boyutu daha çok çalışılmakta olsa da, korumanın kamu hukukuna bakan yönünün de ele alınması, istenen korumayı sağlaması adına çok önemlidir.

Tez kapsamında başta AB belgeleri olmak üzere uluslararası belgeler ve yerel hukuk kuralları üzerinde yapılan detaylı incelemeler sonucunda kişisel verilerin korunmasıyla ilgili bazı noktalar öne çıkmıştır. Öncelikle verilerin genel mahiyetiyle korunması hususunda, korunmaya değer olacak verilerin sadece kişisel veri teriminin kapsamında yer alan veriler olacağı fikrine ulaşılmıştır. Akabinde, aralarındaki çok güçlü ilişkiye rağmen kişisel verilerin korunması hakkının özel hayatın gizliliği hakkından farklı bir insan hakkı olmaya eğilimli olduğu anlaşılmıştır. Ayrıca kişisel verilerin korunması hakkı, diğer temel hak ve hürriyetler ile birbirlerine karşılıklı koruma sağlamakta oldukları analiz edilmiştir.

Tezin asıl yazılma gayesi olan kişisel verilerin soruşturma evresindeki işlenmesine karşı bir insan hakkı olarak korunması hususunda çok önemli çıkarımlara ulaşılmıştır. Bunlardan birincisi ve belki de en önemlisi, verilerin korunması hakkının gerekçelerinin kanun koyucu tarafından eksik anlaşılmasıdır. Şöyle ki, AB kişisel veriler mevzuatında uygulanmakta olan 2016/679/EU sayılı GDPR, KVK Kanunu'nun dayanağı olan 95/46/EC sayılı Direktif'te olduğu gibi soruşturma evresinde kişisel verilerin işlenmesini kapsam dışı bırakmaktadır. Fakat bu soruşturma işlenmelerinin yapılabilmesi için soruşturmanın gizliliği ve işin doğası gereği gibi sebeplerle değildir. Çünkü soruşturma evresine uygulanması amacıyla aynı gün 2016/680/EU sayılı Direktif çıkarılmış, bu Direktif'te kişisel verilerin korunmasının ceza hukuku boyutu düzenlenmiştir. Kanun koyucunun bu farkı göz ardı etmesiyle kişisel verilerin soruşturma evresinde koruma kapsamında olmaması sonucuna ulaşılarak delil elde etme amacıyla yapılan tüm işleme

faaliyetleri idarenin takdirine bırakılmaya devam etmiştir. Oysa yapılanması gereken soruşturma evresinde kişisel verilerin işlenmesi sonucuyla irtibatlı olan ilgili CMK, kanun ve yönetmelik hükümlerinin yeniden düzenlenmiş olmasıydı.

Ortaya çıkan ikinci sonuç, kanunun soruşturma evresini koruma kapsamı dışında bırakıyor olmasının hakkın özüne müdahale teşkil edeceğidir. Anayasal bir hak olarak kişisel verilerin korunması amacıyla getirilen KVK Kanunu'nun soruşturma evresini tamamen kapsamına almaması, bu evrede hakkın hiç kullanılamıyor olmasına yol açmaktadır. AB ülkelerinde 2016/680/EU sayılı Direktif doğrultusunda kişisel veriler soruşturma evresinde koruma kapsamına alınabiliyorken, bu imkânın Türk hukukunda olmama AİHM kararlarında da gösterildiği üzere demokratik toplum gereklilikleri ile bağdaşmaz. Dolayısıyla olması gereken eğer soruşturma evresinde kişisel verilerin hiç uygulanmayacak şekilde KVK Kanunu'nun getirdiği güvencelerin kapsam dışı bırakılıyorsa, ya istisna hükümlerinin kaldırılması ya da bu alana uygulanacak kapsamlı bir düzenlemenin yapılmasıdır.

Ortaya çıkan üçüncü sonuç, tüm kişisel veri koruma belgelerinde yer aldığı gibi KVK Kanunu içerisinde de yer verilen veri işlenmesine hâkim olan ilkelerin, istisna hükmünün varlığına rağmen uygulama alanı bulabilecek olmasıdır. Kanun istisna hükmünde KVK Kanunu hükümlerinin soruşturma evresi işlemlerine uygulanmayacağı belirtmekte olmasına karşın genel ilkeler kişisel verilerin korunması hususunun olmazsa olmazları, temel yapı taşları olması sebebiyle yine de uygulama alanı bulacak olmasıdır. Keza kişisel verilerin korunması amacıyla getirilen bir kanunda belirtilen temel ilkelerin hiçbir şekilde uygulanmayacak olmaması kanunun neden getirildiğini sorgulatacaktır. Üstelik eğer veriler ilkeler doğrultusunda işlenmeyecekse, kanun, gerekli korumayı sağlaması için taşıması gereken maddi özelliklerden uzak olacaktır. Bu yüzden, kanun emretse yahut kişinin rızası olsa bile kişisel verilerin işlenmesi ilkelerine her halde uyulması şart olmalıdır.

Tezimiz bağlamında ortaya çıkan dördüncü sonuç ise, soruşturma evresinde delil elde etme amacıyla kişiler yahut nesneler üzerinde yapılan işlemlerin kişisel verilerin işlenmesi sınıfına girecek olmasına karşın bu sürece uygulanacak kapsamlı kurallar bütününün Türk hukukunda düzenlenmiş olmamasıdır. Kamu gücü kullanılarak işlemekte verilerin korunmasına yönelik CMK ve diğer ilgili hukuk kurallarında sadece

birkaç madde de yer verilerek kişisel verilerin soruşturma evresinde korunamayacağı aşikardır. Verili hukuk kurallarının olmayışı zorluğunu aşabilmek için uluslararası belgeler ve doktrinden yararlanılarak soruşturma evresinde kişisel verilerin işlenmesinin ilkeleri ve ilgili kişilerin hakları kapsamlı bir araştırma sonucu ortaya çıkarılmıştır. Tezimiz bağlamında oldukça önemli olduğu düşündüğümüz bu parametreler çerçevesinde öngörülebilir her bir işleme faaliyeti için dikkat edilmesi gereken hususlar ve öneriler, muhtemel kanun değişikliği açısından bir fikir vermesi amacıyla yorumlanmıştır.

Bu noktada varılan sonuç bize göstermektedir ki soruşturma evresinde kişisel verilerin işlenmesine yönelik başta CMK ve PVSK olmak üzere Türk hukukunun kapsamlı değişikliğe ihtiyaç duymaktadır. Bu doğrultuda, ortaya koyduğumuz ilkeler ve hakların CMK içerisinde "Soruşturma Evresinde Kişisel Verisi İşlenen Mağdur, Şüpheli Veya İlgili Kişinin Hakları" başlığıyla bir maddede düzenlenmesi, kişisel verilerin soruşturma evresinde korunmasına yönelik güvence sağlayacaktır. Bu doğrultuda yapılacak değişiklikler ile, soruşturma sürecinde delillerin işlenmesinde, işlemenin veya işleme kategorilerinin amaçları; kişisel veri kategorileri; kötüye kullanım veya yasa dışı yollarla erişim veya aktarımın engellenmesine yönelik güvenceler belirtilmelidir. Ayrıca, işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanabilir güvenceler; veri sahiplerinin hakları ve özgürlüklerine yönelik riskler ve kısıtlama amacına halel getirmemesi durumunda veri sahiplerinin kısıtlamayla ilgili bilgi sahibi olma hakkının soruşturmaya hâkim olmasının sağlanması gerekmektedir.

Sözün özü, kişisel verilerin korunması için getirilen KVK Kanunu, uygulanabilirlik alanını sınırlayan diğer hükümler sebebiyle kişisel verilerin korunmasına hizmet edememektedir. Bunun sonucu ise kanunun soruşturma evresinde tamamıyla uygulanmaması ve kişisel verilerin serbestçe işlenmeye devam edilmesidir. Oysa GDPR ve 2016/680/EU sayılı Direktif bu alanı korumasız bırakmak bir yana özel hükümlerle düzenlemektedir. Bu eksiklik yüzünden Türkiye hala Avrupa Birliği nazarında veri koruması açısından güvensiz ülke listesinde yer almaktadır. Her ne kadar Alo 198 Veri Koruma hattı ile vatandaşa bilgi ve danışma hizmeti verilerek veri korumasına ilişkin farkındalık artırılmaya çalışıyor olsa da, kanun koyucunun yeterli farkındalıkla gerekli kanuni düzenlemeleri yapmadığı müddetçe kişisel verilerin soruşturma evresinde hukuka

aykırı olarak işlenmeye devam edeceği bir gerçektir. Bu sebeple, bir an önce CMK ve KVK Kanunu'nda tez boyunca gerekçeli olarak ortaya konulan unsurlar çerçevesinde değişikliklerin yapılması gerektiğini düşünmekteyiz. Aksi halde kişisel verilerin soruşturma evresinde işlenmesinde yeterli hukuki güvencenin yokluğu, önemli hak ihlallerini ortaya çıkararak hukuk güvenliğini tehlikeye atmaya devam edecek ve kişisel veriler soruşturma evresinde insan hakları kapsamında korunamayacaktır.

KAYNAKÇA

Doktrin Kaynakları

Abanoz, Buket: Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu, İstanbul 2018.

Akdağ, Hale: Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013.

Akgül, Aydın: Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014.

Akıncı, A. N. 2019. *Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti.* Uzmanlık Tezi, Ankara: T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Sektörler ve Kamu Yatırımları Genel Müdürlüğü.

Akipek, Jale/Akıntürk, Turgut/Ateş, Derya: "Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, İstanbul 2018.

Akkaraca Köse, Melike (Tennis, Bradley T./Nuno Gomes de Andrade, Norberto/Stylianou, Konstantinos K./Anthopoulos, Haralambos/Tsiftsoglou, Anna/Akrivopoulou, Christina M./Güngör, Hasan Atilla/Contartese, Cristina/Suarez, Christopher A./Desierto, Diane A./Monteleone, Shara/Casarosa, Federica/Pina, Pedro/Ni Lonedain, Nora/Tzanou, Maria/Stan, Grigore-Octav/Pateraki, Anna): Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices, New York 2010.

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

Aksoy İpekçioğlu, Pervin: "Gözaltında Alınan İfadenin Önemi ve Delil Değeri", Ankara Üniversitesi Hukuk Fakültesi Dergisi, 57/3, Ankara 2018.

Akyürek, Güçlü (Bayraktar, Köksal/Keskin Kiziroğlu, Serap/Yıldız, Ali Kemal/Zafer, Hamide/Aksoy Retornaz, Eylem/Evik, Ali Hakan/Sınar, Hasan/Altunç, Sinan/Aytekin İnceoğlu, Asuman/Erman, Barış/Eroğlu Erman, Fulya): Özel Ceza Hukuku - Cilt III - Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar (TCK m. 106-140), İstanbul 2018.

Alston, Philip/Bustelo, Mara/Heenan, James: The EU and Human Rights, 1999 New York.

Apiş, Özge: "Ceza Muhakemesi Hukukunda Şüpheli/Sanığın Beden Muayenesi ve Vücudundan Örnek Alınması", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 18/1, İstanbul 2012.

Arıcan, Mehmet: "Ceza Muhakemesi Hukukunda İfade Alma ve Sorgu", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 17/1, İzmir 2009.

Arpacı, Abdülkadir: Kişiler Hukuku (Gerçek Kişiler), İstanbul 2000.

Aslanova, Kemale (Bozkurt Yüksel, Armağan Ebru/Bak, Başak/Yüksel, Sera Reyhani): Futurist Hukuk, İstanbul 2018.

Aşıkoğlu, Şehriban İpek: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul 2018.

Ayan, Mehmet/Ayan, Nurşen: Kişiler Hukuku, Konya 2015.

Aydın, Sedat Erdem: AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul 2015.

Aygün, A. "Beden Muayenesi ve Vücuttan Örnek Alma," Dergipark.org.tr Erişim Tarihi: Nisan 2019 https://dergipark.org.tr/download/article-file/271158,

Ayözger Öngün, A. Çiğdem: Kişisel Verilerin Korunması Hukuku, İstanbul 2019.

Başalp, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Ankara 2004.
Bayraktar, Köksal(Akyürek, Güçlü/Keskin Kiziroğlu, Serap/Yıldız, Ali Kemal/Zafer, Hamide/Aksoy Retornaz, Eylem/Evik, Ali Hakan/Sınar, Hasan/Altunç, Sinan/Aytekin İnceoğlu, Asuman/Erman, Barış/Eroğlu Erman, Fulya): Özel Ceza Hukuku - Cilt III - Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar (TCK m. 106-140), İstanbul 2018.
Bennett, Colin J.: Regulating Privacy: Data Protection and Public Policy in Europe and the United States, New York 1992.
Berg, M. van den/Kwant, P.O/Graff, P. de/Slewe, T: Mass Surveillance : What are the risks for the citizens and the opportunities for the European information society? What are the possible mitigation strategies? Part 2 Technology foresight, options for longer-term security and privacy improvements, Brüksel 2015.
Birtek, Fatih: Haberleşmenin Gizliliğini İhlal Suçları (TCK m. 132), Ankara 2013.
Bloom, Robert M./Dewey, Erin: "When Rights Become Empty Promises: Promoting an Exclusionary Rule That Vindicates Personal Rights", Irish Jurist, 46, Dublin 2011.
Bostancı Bozbayındır, Gülşah: "Avrupa Birliği Ceza Hukukunda 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, 2, İstanbul 2018.
Bozkurt Yüksel, Armağan Ebru: Bulut Bilişimde Kişisel Verilerin Korunması, Ankara 2016.
Brouwer, Evelien Renate: The Other Side of Moon: The Schengen Information System and Human Rights : a Task for National Courts, Brüksel 2008.
Bük, Alaattin: Bilişim Alanında Kişisel Verilerin Korunması, Ankara 2018.
Caruana, Mireille M.: "The Reform of the EU Data Protection Framework in The Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement", International Review of Law, Computers & Technology, 2017.
Centel, Nur/Zafer, Hamide: Ceza Muhakemesi Hukuku, İstanbul 2018.
Centel, Nur/Zafer, Hamide/Çakmut, Özlem: Kişilere Karşı İşlenen Suçlar, İstanbul 2017.
Çekin, Mesut Serdar: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul 2018.
Develioğlu, Hüseyin Murat: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017.
Dinç, Güney. 2009. "Uluslararası Belgeler Açısından Özel Yaşam." Türkiye Barolar Birliği Özel Yaşamın Gizliliği Paneli, Ankara, 18 Ekim 2009.
Duran, Gökhan Yaşar: "Ceza Muhakemesinde Gözlem Altına Alınma (CMK m. 94)", Ceza Hukuku Dergisi, 13, 38, Ankara 2018.
Dülger, Murat Volkan: Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi), Ankara 2014.
Dülger, Murat Volkan: Kişisel Verilerin Korunması Hukuku, İstanbul 2019.
Eijkman, Quirine: "Access to Justice for Communications Surveillance and Interception: Scrutinising Intelligence-Gathering Reform Legislation", Utrecht Law Review, 14, Utrecht 2018.
Erem, Faruk: "Ceza Hukukunda Meslek Sırrı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, 1, Ankara 1943.
Eroğlu, F. 2009. *Beden Muayenesi Ve Vücuttan Örnek Alma Suretiyle Elde Edilen*

Delillerin İspat Değeri. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Yeditepe Üniversitesi, Sosyal Bilimler Enstitüsü.
Fehér-Polgár, Pál/Németh, Zsolt. 2016. "Safety Consciousness of the Mobile Phone Users." 11th IEEE International Symposium on Applied Computational Intelligence and Informatics, Timişoara, 12-14 Mayıs 2016.
Finn, Rachel L./Wright, David/Jacques, Laura: Study on Privacy, Data Protection and Ethical Risks in Civil Remotely Piloted Aircraft: Final Report, Brüksel 2014.
Flaherty, David: Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, North Carolina, 2014.
Fleckenstein, Marilynn/Maury, Mary/Pincus, Laura/Primeaux, Pat: From the Universities to the Marketplace: The Business Ethics Journey: The Second Annual International Vincentian Conference Promoting Business Ethics, Berlin 2012.
Fong, Adrian: "The Role of App Intermediaries in Protecting Data Privacy", International Journal of Law and Information Technology, 25, Oxford 2017.
Gioioso, Kaylie: "Small Companies, Big Breaches: Why Current Data Protection Laws Fail American Consumers in Cases of Third-Party Hacking", Journal of Business & Technology Law Proxy, 10, Maryland 2016.
Gutwirth, Serge/Leenes, Ronald/de Hert, Paul: Reforming European Data Protection Law, Dordrecht 2015.
Gürocak, İsmail: Türk Ceza Kanununda Haberleşmenin Gizliliğini İhlal Suçları, Ankara 2015.
Gözler, Kemal: Anayasa Hukukunun Genel Teorisi, Bursa 2011.
Gül, İbrahim/Alagöz İsmail: Kişisel Verilerin Korunmasına Yönelik İhlaller(Dinlemeler) ve Uluslararası Düzenlemeler, Ankara 2016.
Gür, İkbal: Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Ankara 2010.
Gürsel, İlke: İşçinin Kişisel Verilerinin Korunması Hakkı, Ankara 2016.
Hatemi, Hüseyin/Kalkan Oğuztürk, Burcu: Kişiler Hukuku (Gerçek Kişiler-Tüzel Kişiler), İstanbul 2014.
Hava, Y. F. 2016. *Türk Dış Politikasında TİKA Bağlamında Yumuşak Güç Kullanımı Ve Balkanlar*. Yayınlanmamış Yüksek Lisans Tezi, Çanakkale: Çanakkale Onsekiz Mart Üniversitesi, Sosyal Bilimler Enstitüsü.
Hayes, Darren R.: A Practical Guide to Computer Forensics Investigations, New Jersey 2014.
Helvacı, Serap: Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul 2001.
Henkoğlu, Türkay: Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015.
Hert, Paul/Papakonstantinou, Vagelis: "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection Of İndividuals", The Computer Law & Security Review, 28, İngiltere 2012.
Hervey, Tamara/McHale, Jean: Health Law and the European Union, Cambridge 2004.
Hildebrandt, Mireille/Gutwirth, Serge: Profiling the European Citizen: Cross-Disciplinary Perspectives, Berlin 2008.
İnci, Z. Özen: "Şüpheli ve Sanığa Rağmen Bir Ceza Muhakemesi Hukuku Mu? Şüpheli ve Sanığın Ceza Muhakemesi İşlemlerine Katlanma Yükümlülüğü ve Bu Yükümlülüğün Sınırları Hakkında Düşünceler", Hacettepe Hukuk Fakültesi Dergisi, 7/2, Ankara 2017.
Kanadoğlu, Korkut. 2009. "Türkiye Cumhuriyeti Anayasasında Özel Yaşam" Türkiye

Barolar Birliği Özel Yaşamın Gizliliği Paneli, Ankara, 18 Ekim 2009.
Karabulut, Ferhat/Karapazarlıoğlu, Ersin/Tosun, Hamza: Ceza Muhakemesinde Delil Kavramı ve Kovuşturma Sürecinde Hâkimlerin Delil Algısı", Türkiye Barolar Birliği Dergisi, 120, Ankara 2015.
Karagülmez, Ali: Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara 2014.
Keçelioğlu, Elvan: "Ceza Muhakemesi Hukukunda Gözlem Altına Alma", Ankara Barosu Dergisi, 3, Ankara 2015.
Keser Berber, Leyla: Çevrimiçi Davranışsal Reklamcılık(Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014.
Korkmaz, İbrahim: Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara 2017.
Köse Aysun, Melike: Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135), Ankara 2018.
Küzeci, Elif: Kişisel Verilerin Korunması, Ankara 2019.
Lubin, Asaf: "We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance", Chicago Journal of International Law, 18/2, Şikago 2018.
Mahmutoğlu, Fatih Selami. 2009. "Ceza ve Ceza Yargılama Hukukunda Özel Yaşam." Türkiye Barolar Birliği Özel Yaşamın Gizliliği Paneli, Ankara, 18 Ekim 2009.
Murray, Andrew: Information Technology Law The Law and Society, 2016 Oxford.
Ni Lonedain, Nora (Tennis, Bradley T./Nuno Gomes de Andrade, Norberto/Stylianou, Konstantinos K./Anthopoulos, Haralambos/Tsiftsoglou, Anna/Akrivopoulou, Christina M./Güngör, Hasan Atilla/Contartese, Cristina/Suarez, Christopher A./Desierto, Diane A./Monteleone, Shara/Casarosa, Federica/Pina, Pedro/ Akkaraca Köse, Melike/Tzanou, Maria/Stan, Grigore-Octav/Pateraki, Anna): Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices, New York 2010.
Oğuz, Habip. 2014. "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum." Çağ Üniversitesi Elektronik Ticaret Hukuku Sempozyumu, Tarsus, 25 Nisan 2014.
Oğuzman, M. Kemal/Seliçi, Özer/Oktay-Özdemir, Saibe: Kişiler Hukuku (Gerçek ve Tüzel Kişiler), İstanbul 2015, s. 154.
Oturaklı, Alper(Karaduman, Şebnem S./Karayazgan, Ahmet/Esatoğlu, Yahya Tekin/Süzel, Cüneyt): Sigorta Hukukunun Bazı Güncel Sorunları, İstanbul 2017.
Ömeroğlu, Ömer: "Ceza Muhakemesinde Şüpheli ve Sanığın Fizik Kimlik Tespiti", Türkiye Barolar Birliği Dergisi, 115, Ankara 2014.
Özbek, Veli Özer/Kanbur, Mehmet Nihat/Doğan, Koray/Bacaksız Pınar/Tepe, İlker: Türk Ceza Hukuku Genel Hükümler, Ankara 2018.
Özbek, Veli Özer/Kanbur, Mehmet Nihat/Doğan, Koray/Bacaksız Pınar/Tepe, İlker: Türk Ceza Hukuku Özel Hükümler, Ankara 2018.
Özbudun, Ergun: "Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği", Ankara Hukuk Fakültesi Ellinci Yıl Armağanı 1925-1975, Ankara 1975.
Özen, Muharrem/Özocak, Gürkan: "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi", Ankara Barosu Dergisi, 1, Ankara 2015.
Öztan, Bilge: Medeni Hukukun Temel Kavramları, Ankara 2014.
Parlar, Ali/Çetin, Ahmet: Ceza Muhakemesinde Soruşturma Evresi Ve Uygulaması, İstanbul 2017.
Pollack, Michael C.: "Taking Data", The University of Chicago Law Review, 86, Şikago

2019.
Posadas, Dalmacio V. Jr.: "The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption." Gonzaga Law Review, 53, Washington 2017.
Ramage, Sally: Privacy-Law of Civil Liberties, Nebraska 2007.
Rodrigues, Roberto J./Wilson, Petra/Schanz, Stephen J.: The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases, Washington 2001.
Ruslijanto, Patricia Audrey (Saputra, Pramana Yoga/Wibowo, Dimas Wahyu/Cahyandari, Dewi/Silfiah, Rossa Ilma/Rohman, Fatkhur/Affandi, Luqman/Suryani, Dhebys/Handayani, Emi Puasa/Arifin, Zainal/Virdaus, Saivol/ Fadloli, Sri Nurkudri/Sulasari, Ayu/Hadiyantina, Shinta/Ramadhan, Nandaru/Mundzir, Hudriyah/Hadiwinata, Khrisna/ Muslim, Hairus Shobib/Fadloli, Abdul Chalim/Fadloli Nurkudri, Widaningsih/Santyaningtyas, Ayu Citra/Soeradji, Elvi/Batubulan, Kadek Suarjuna/Novitasari, Ane Fany/Suryadi, Satrio Binusa/Ellion, Handry Argatama/Setyowadi, Dewi/Sri Hudiarini, Rokiyah/Soraya, Joice): International Conference Call for Paper Personal Data Protection in Digital Era, Malang 2018.
Sarıusta, K. 2018. *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması.* Yayınlanmamış Yüksek Lisans Tezi, Gaziantep: Gaziantep Üniversitesi, Sosyal Bilimler Enstitüsü.
Serdar, İlknur: Radyo ve Televizyon Yoluyla Kişilik Hakkının İhlali ve Kişiliğin Korunması, Ankara 1999, s. 41.
Sert, Şeyma: Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara 2019.
Solomon, Julie/Berman Jacquelin: Tools for Building Culturally Competent HIV Prevention Programs, New York 2008.
Sırabaşı, Volkan: İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Ankara 2007.
Şahin, Cumhur: Ceza Muhakemesi Hukuku I, Ankara 2017.
Şen, Ersan: Özel Hayatın Gizliliği ve Korunması, İstanbul 1996.
Şen, Ersan: Yeni Türk Ceza Kanunu Yorumu, İstanbul 2006.
Şen, Ersan/Eryıldız, H. Sefa: El koyma, Ankara 2017.
Şimşek, Oğuz: Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008.
Taştan, Furkan Güven: Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul 2017.
Thanaraj, Ann: "Studying Law in a Digital Age: Preparing Law Students for Participation in a Technologically-Advanced Multidisciplinary and Complex Professional Environment", Nottingham Law Journal, 27/2, Nottingham 2018.
Thompson, Ross A. (Institute of Medicine, Division of Health Care Services, Committee on the Role of Institutional Review Boards in Health Services Research Data Privacy Protectio): Protecting Data Privacy in Health Services Research, Washington 2001.
Toroslu, Nevzat/Feyzioğlu, Metin: Ceza Muhakemesi Hukuku, Ankara 2018.
Turan, Metin: Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Ankara 2017.
Uncular, Selen: İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara 2014.
Ünver, Yener/Hakeri, Hakan: Ceza Muhakemesi Hukuku, Ankara 2018.
Van Ooik, Ronald/Vandamme, Thomas: European Basic Traties, Deventer 2013.
Varela, Alberto Arufe: Employment Privacy Law in the European Union: Human Resources and Sensitive Data, Cambridge 2003.

Velidedeoğlu, Hıfzı Veldet: Türk Medeni Hukuku, İstanbul 1963.
Von Grafenstein, Maximilian: The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation, Berlin 2018.
Yurtcan, Erdener: Ceza Yargılaması Hukuku, Ankara 2018.
Wacks, Raymond: Privacy: A Very Short Introduction, Oxford 2015.
Wagner, Stephen: "Stopping Police in Their Tracks: Protecting Cellular Location Information Privacy in the Twenty-First Century", Duke Law & Technology Review, 12, Kuzey Karolina 2013–2014.
Yavuz, Can: İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı, Ankara 2018.
Yılmaz, Sabire Sanem: Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Ankara 2017.
Zafer, Hamide: Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK m. 132-134), İstanbul 2010.

Mahkeme Kararları

AİHM Kararları
André ve Diğerleri/Fransa, Başvuru No: 18603/03, 24.07.2008.
Amann/İsviçre, Başvuru No: 27798/95, Büyük Daire Kararı, 16.02.2000.
Aycaguer/Fransa, Başvuru No: 8806/12, 22.06.2017.
Bărbulescu/Romanya, Başvuru No: 61496/08, Büyük Daire Kararı, 05.09.2017.
Bayatyan/Ermenistan, Başvuru No: 23459/03, Büyük Daire Kararı, 07.07.2011.
Benedik/Slovenya, Başvuru No: 62357/14, 24.04.2018.
Brito Ferrinho Bexiga Villa-nova/Portekiz, Başvuru No: 69436/10, 01.12.2015
Cevat Özel/Türkiye, Başvuru No: 19602/06, 07.06.2016.
Campbell/Birleşik Krallık, Başvuru No: 13590/88, 25.03.1992.
Copland/Birleşik Krallık, Başvuru No: 62617/00, 03.04.2007.
Coster/Birleşik Krallık, Başvuru No: 24876/94, Büyük Daire Kararı, 18.01.2001.
Delfi AS/Estonya, Başvuru No: 64569/09, Büyük Daire Kararı, 16.06.2015.
Dragojević/Hırvatistan, Başvuru No: 68955/11, 15.01.2015.
Dragojević/Hırvatistan(Türkçe), Başvuru No: 68955/11, 15.01.2015.
Elberte/Latvia, Başvuru No: 61243/08, 13.01.2015.
Gäfgen vs. Almanya, Başvuru No: 22978/05, Büyük Daire Kararı, 01.06.2010.
Gardel/Fransa, Başvuru No: 16428/05, 17.12.2009.
Grifhorst/Fransa, Başvuru No: 28336/02, 26.02.2009.
Gutsanovi/Bulgaristan, Başvuru No: 34529/10, 15.10.2013.
Halford/Birleşik Krallık, Başvuru No: 20605/92, 25.06.1997.
İrfan Güzel/Türkiye, Başvuru No: 35285/08, 07.02.2017.
Klass ve Diğerleri/Almanya, Başvuru No: 5029/71, 06.09.1978.
Kopp/İsviçre, Başvuru No: 23224/94, 25.03.1998.
L.H. vs. Litvanya, Başvuru No: 52019/07, 29.04.2014.
M.K./Fransa, Başvuru No: 19522/09, 18.04.2013.
M.N. ve Diğerleri/San Marino, Başvuru No: 28005/12, 07.07.2015.
Malone/Birleşik Krallık, Başvuru No: 8691/79, 02.08.1984.
Michaud/Fransa, Başvuru No: 12323/11, 06.12.2012.
Mor/Fransa, Başvuru No 28198/09, 15.12.2011.
Nada/İsviçre, Başvuru No: 10593/08, Büyük Daire Kararı, 12.09.2012.
Niemietz/Almanya, Başvuru No: 13710/88, 16.12.1992.

Oleksandr Volkov/Ukrayna, Başvuru No: 21722/11, 09.01.2013.
Oy ve Oy/Finlandiya, Başvuru No: 931/13, Büyük Daire Kararı, 27.06.2017.
Peck/Birleşik Krallık, Başvuru No: 44647/98, 28.01.2013.
R.E./Birleşik Krallık, Başvuru No: 62498/11, 27.10.2015.
Ramirez Sanchez/Fransa, Başvuru No: 59450/00, Büyük Daire Kararı, 04.07.2006.
Robathin/Avusturya, Başvuru No. 30457/06, 03.07.2012.
Roemen ve Schmit/Lüksemburg, Başvuru No 51772/99, 25.02.2003.
Roman Zakharov/Rusya, Başvuru No: 47143/06, Büyük Daire Kararı, 04.12.2015.
S. ve Marper/Birleşik Krallık, Başvuru No: 30562/04 ve 30566/04, Büyük Daire Kararı, 04.12.2008.
S. ve Marper/Birleşik Krallık(Türkçe), Başvuru No: 30562/04 30566/04, Büyük Daire Kararı, 04.12.2008.
Sabanchiyeva ve Diğerleri/Rusya, Başvuru No: 38450/05, 06.06.2013.
Saint-Paul Luxembourg S.A./Luxembourg, Başvuru No: 26419/10, 18.04.2013.
Segerstedt-Wıberg and Others/İsveç, Başvuru No: 62332/00.
Schönenberger ve Durmaz/İsviçre, Başvuru No: 11368/85, 20.06.1988.
Sher ve Diğerleri/Birleşik Krallık, Başvuru No: 5201/11, 20.10.2015.
Sodan/Türkiye, Başvuru No: 18650/05, 02.02.2016.
Turan Çakır/Belçika, Başvuru No. 44256/06, 10.03.2009.
Uzun/Almanya, Başvuru No: 35623/05, 02.09.2010.
Vinci Construction ve GTM Génie Civil et Services/Fransa, Başvuru No: 63629/10 60567/10, 02.04.2015.
Wieser ve Bicos Beteiligungen GmbH/Avusturya, Başvuru No: 74336/01, 16.10.2007.
X/Finlandiya, Başvuru No: 34806/04, 03.07.2012.
Xavier Da Silveira/Fransa, Başvuru No: 43757/05, 21.01.2010.

Anayasa Mahkemesi Kararları

Bireysel Başvurular:
Başvuru No: 2013/6367, 10.12.2015.
Başvuru No: 2013/2941, 11.05.2016.
Başvuru No: 2014/7256, 27.02.2019.
Başvuru No: 2014/14061, 08.04.2015.

İptal Davaları:
E. 2010/40, K. 2012/8, KT: 19.01.2012, RG. 28579, 06.03.2013.
E. 2011/141, K. 2013/10, KT: 10.01.2013, RG. 28865, 28.12.2013.
E. 2013/84, K.2014/183, KT: 04.12.2014, RG. 29294, 13.03.2015
E. 2014/149, K. 2014/151, KT: 02.10.2014, RG. 29223, 01.01.2015.
E.2014/180, K.2015/30, KT: 19.3.2015, RG. 29321, 09.04.2015.
E. 2014/122, K. 2015/123, KT: 30.12.2015, RG. 29640, 01.03.2016.
E. 2015/61, K. 2016/172, KT: 02.11.2016, RG. 29913, 09.12.2016.
E. 2015/76, K. 2017/153, KT: 15.11.2017, RG. 30325, 07.02.2018.
E. 2016/125, K. 2017/143, KT: 28.09.2017, RG. 30310, 23.01.2018.

Danıştay Kararları

D. 5. D, E. 2013/5342, K. 2013/9525, 10.12.2013, Kazancı İçtihat Bilgi Bankası.
D. 10. D, 26.5.2015, E. 2011/7001 K. 2015/2573, Lexpera Hukuk Bilgi Sistemi.

D. 10. D, 17.11.2009, E. 2008/10561, K. 2009/9766, Kazancı İçtihat Bilgi Bankası.
D. İDDGK, E. 2007/2257, K. 2012/1117, 14.9.2012, Kazancı İçtihat Bilgi Bankası.

Yargıtay Kararları

Y. 4. HD, 10.4.2008, E. 2007/9966 K. 2008/5096, Kazancı İçtihat Bilgi Bankası.
Y. 12. CD, 05.09.2018, E. 2018/2571 K. 2018/7821, Kazancı İçtihat Bilgi Bankası.
Y. 12. CD, 13.01.2014, E. 2013/9043 K. 2014/151, Kazancı İçtihat Bilgi Bankası.
Y. 14. CD, 8.12.2014, E. 2013/5239 K. 2014/13911, Kazancı İçtihat Bilgi Bankası.
Y. 16. CD, 24.04.2017, E. 2015/3 K. 2017/3, Kazancı İçtihat Bilgi Bankası.
Y. 16. CD, 21.04.2016, E. 2015/4672 K. 2016/2330, Kazancı İçtihat Bilgi Bankası.
Y. CGK, E. 2007/1-38 K. 2007/44 T. 20.2.2007, Kazancı İçtihat Bilgi Bankası.
Y. CGK, E. 2013/1-251 K. 2013/454 T. 12.11.2013, Kazancı İçtihat Bilgi Bankası.
Y. CGK, E. 2013/10-468 K. 2014/268 T. 20.5.2014, Kazancı İçtihat Bilgi Bankası.
Y. CGK, E. 2017/16-956 K. 2017/370 T. 26.9.2017, Kazancı İçtihat Bilgi Bankası.

Diğerler Kaynaklar

Avrupa Birliği Komisyonu, 2016. *2016 Türkiye Raporu SWD(2016) 366 nihai*. Erişim Tarihi: Ocak 2019 https://www.ab.gov.tr/files/pub/2016_ilerleme_raporu_tr.pdf.

Avrupa Birliği Komisyonu, 2018. *2018 Türkiye Raporu SWD(2018) 153 nihai*. Erişim Tarihi: Ocak 2019 https://www.ab.gov.tr/siteimages/birimler/CEB/commission_country_reports/2018/2018_turkiye_raporu_tr.pdf.

Birleşmiş Milletler İnsan Hakları Komitesi, Sayadi ve Vinck/Belçika, Başvuru No: 1472/2006, 22.10.2008.

EU GDPR Portal. Şubat 2019 https://eugdpr.org/the-regulation/

Madde 29 Veri Koruma Çalışma Grubu, *16/EN WP 237, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), Adopted on 13 April 2016.* Erişim Tarihi: Nisan 2019, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=56068.

Madde 29 Veri Koruma Çalışma Grubu, *16/EN WP 240 Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016.* Erişim Tarihi: Nisan 2019, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.

Madde 29 Veri Koruma Çalışma Grubu, *1806/16/EN WP 239 Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector, Adopted on 8 June 2016*. Erişim Tarihi: Nisan 2019, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.

Madde 29 Veri Koruma Çalışma Grubu, *3211/15/EN WP 233 Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Adopted on 01 December 2015.* Erişim Tarihi: Nisan 2019,

https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=56082.
Margaret R. 2009. “Deperimeterization.” Techtarget.com. Erişim Tarihi: Nisan 2019 https://searchsecurity.techtarget.com/definition/deperimeterization.
Türk Dil Kurumu Büyük Türkçe Sözlük. 2019. “Kişisel” Erişim Tarihi: Mart 2019 http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK. GTS.5c979f3cbbb49733853275; “Veri” Erişim Tarihi: Mart 2019 http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK. GTS.5c97a2f190afa3.80189263.
Türk Dil Kurumu Sözlükleri, 2019. “Sır” Erişim Tarihi: Ağustos 2019 https://sozluk.gov.tr/?kelime=sir.

ÖZ GEÇMİŞ

Kişisel Bilgiler

Adı Soyadı	: Muhammet Sefa Mutlu
Doğum Yeri ve Tarihi	: Kadıköy 04.08.1993

Eğitim Durumu

Lisans Öğrenimi	: Kadir Has Üniversitesi Siyaset Bilimi ve Kamu Yönetimi (2017) Kadir Has Üniversitesi Hukuk Fakültesi (2018)
Yüksek Lisans Öğrenimi	: Kadir Has Üniversitesi Kamu Hukuku Bölümü (2017- …)
Bildiği Yabancı Diller	: İngilizce

İş Deneyimi

Çalıştığı Kurumlar ve Tarihleri: Reşit Hukuk Bürosu, (2019-...)

İletişim

Telefon	: 0533 334 46 29
E-posta Adresi	: muhammedsefamutlu@gmail.com