

**BİR GÖZETİM TEKNİĞİ OLARAK KAPALI DEVRE KAMERALARIN
KULLANILMASI VE KİŞİSEL VERİLERİN KORUNMASI**

CANBERK YILDIZ

NİSAN 2022

**BİR GÖZETİM TEKNİĞİ OLARAK KAPALI DEVRE KAMERALARIN
KULLANILMASI VE KİŞİSEL VERİLERİN KORUNMASI**

**BAHÇEŞEHİR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
YÜKSEK LİSANS TEZİ**

CANBERK YILDIZ

**SOSYAL BİLİMLER ENSTİTÜSÜ ÖZEL HUKUK TEZLİ YÜKSEK LİSANS
DERECESİ İÇİN GEREKLİ ÇALIŞMALAR YERİNE GETİRİLMİŞTİR**

NİSAN 2022



BAHÇEŞEHİR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZ ONAY FORMU

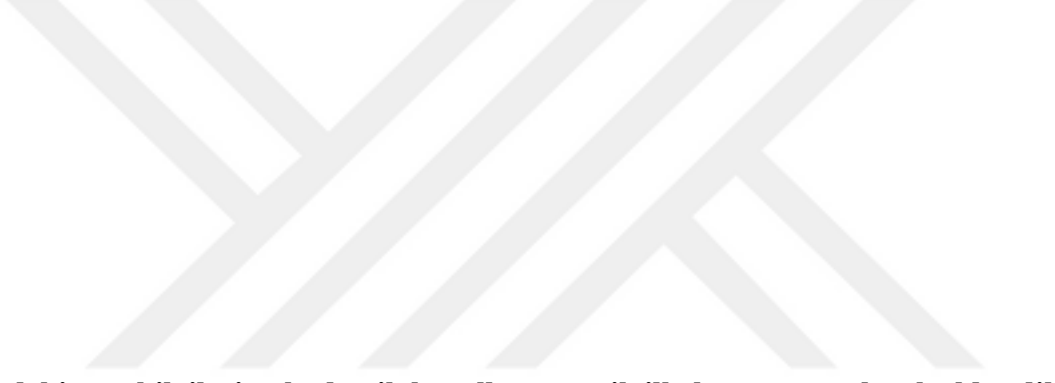
Program Adı:	Özel Hukuk Tezli Yüksek Lisans Programı
Öğrencinin Adı Soyadı:	Canberk YILDIZ
Tezin Adı:	Bir Gözetim Tekniği Olarak Kapalı Devre Kameraların Kullanılması ve Kişisel Verilerin Korunması
Tez Savunma Tarihi:	26/04/2022

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğu Lisansüstü Eğitim Enstitüsü tarafından onaylanmıştır.

Prof. Dr. Ahmet ÖNCÜ
Enstitü Müdürü

Bu Tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

	Ünvanı, Adı Soyadı	İmza
Tez Danışmanı:	Dr. Öğr. Üyesi Elif KÜZECİ EROL	
2. Üye :	Dr. Öğr. Üyesi Mehmet Sinan ALTUNÇ	
3. Üye :	Dr. Öğr. Üyesi Evrim AKGÜN	



Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim.

Ad, Soyad : Canberk YILDIZ
İmza :

Bir Gözetim Tekniđi Olarak Kapalı Devre Kameraların Kullanılması ve Kişisel Verilerin Korunması

Özet: Bu çalışma kapsamında; kapalı devre kamera sistemlerinin günümüzdeki hızlı teknolojik ilerlemeler ile birlikte farklı alanlarda kullanılmaya başlanması bireylerin özel hayatlarının gizliliğinin ve kişisel verilerinin korunmasına etkileri aktarılmıştır. Uygulamada Kişisel Verilerin Korunması Kanunu’nun getirdiğı düzenlemelere riayet edilmesi bilhassa gözetleyenlerin keyfi ya da ölçsüz davranışlarının önüne geçilmesini sağlamıştır. Nitekim bu Kanun, gözetim ilişkisindeki zayıf taraf olan bireyin mağduriyetinin azaltılmasına yardımcı olmuştur. “Gözetim Kavramı, Gözetimin Tarihsel Gelişimi ve Kapalı Devre Kamera Sistemleri” başlığını taşıyan birinci bölümde, gözetim kavramının ne olduğı, tarihsel süreç içerisinde gözetim faaliyetlerinin ne şekillerde ifa edildiğı, farklı sosyo-ekonomik kuramlar içerisinde gözetim faaliyetlerinin nasıl kullanıldığı, teknolojik gelişmelerle birlikte nasıl gözetim toplumuna dönüşüldüğü ve kapalı devre kamera sisteminin tanımı ve unsurları ortaya konulmuştur. İkinci bölümde ise kapalı devre kameralar özelinde gözetimin nasıl yapıldığı, bu teknik dahilinde yapılan gözetimin kanuni dayanağının ve amacının ne olduğı vurgulanarak, kamuya açık ve kapalı alanlardaki ya da farklılık arz eden diğer alanlardaki gözetime dair farklı uygulamalara değinilmiştir. Son olarak, çalışmamızın üçüncü bölümünde kapalı devre kameralar ile gözetlenenlerin kişisel verilerinin korunmasına dair Türk hukuk sistemi içerisinde bir değerlendirme yapılmış ve karşılaştırmalı hukukta yer bulan mevzuat, uygulama ve başta Avrupa İnsan Hakları Mahkemesi kararları olmak üzere diğer yargı kararlarından dikkat çeken ve tarafımıza bu yönde yol gösterebilecek hususlar ortaya konularak, ülkemizde yerleşmesi gereken düzenlemeler hakkında görüş bildirilmiştir.

Anahtar Kelimeler : Kapalı Devre Kamera, Kamera, CCTV, Closed Circuit Television, Kişisel Veri, Kişisel Verilerin Korunması, Özel Yaşam, Özel Yaşamın Gizliliğinin Korunması.

Implementation of Closed Circuit Television Cameras as a Surveillance Technique and Protection of Personal Data

ABSTRACT : Using of closed-circuit camera systems in different areas within the framework of today's rapid technological acceleration and the difficulty of avoiding surveillance activities relating this surrounding activities and the importance of protecting the privacy of individuals' private lives and personal data has been conveyed in the scope of this study. In practice, by complying with the regulations brought by the Law on the Protection of Personal Data, it could be possible to prevent permissive or disproportionate behavior of the surveillant for a individual monitored. Indeed, Law on the Protection of Personal Data facilitates reducing victimization for the individual, who has not equal mechanism to defend themselves in the surveillance relationship. The first chapter titled, "The Concept of Surveillance, Historical Development of Surveillance and the CCTV ", explains what the concept of surveillance is, the execution of surveillance activities in the historical process, how surveillance activities are used in different socio-economic theories, how we have turned into a surveillance society with technological development are growing constantly, besides the definition and components of the CCTVs. In the second part, different implementations of surveillance in public and non-public areas or in other areas that differ are mentioned, by emphasizing how the surveillance is applied in particular for closed circuit cameras and the legal basis and purpose of the surveillance decided within this technique. The third and final section assesses Turkish legal system regarding the protection of the personal data of those who are monitored with closed circuit cameras. Addition to that issues that draw attention from the legislation of comparative law, practice and other judicial decisions, especially the decisions of the European Court of Human Rights which deemed to guide us in this direction and opinions were expressed about the regulations that should be adapted in Turkish legal system.

Keywords : Closed Circuit Television, CCTV, Camera, Personal Data, Protection of data, Data Protection, Private life, Protection of the private life, Respect for private life.

*Bu alıřmanın meydana gelmesinde desteęini esirgemeyen
Sayın E. Yücel Hocam'a*

İÇİNDEKİLER

KISALTMALAR	x
-------------------	---

GİRİŞ

BİRİNCİ BÖLÜM

GÖZETİM KAVRAMI, GÖZETİMİN TARİHSEL GELİŞİMİ VE KAPALI DEVRE KAMERA SİSTEMLERİ

I. Gözetim Kavramına Genel Bir Bakış ve Gözetimin Tarihi	1
A. Gözetim Kavramı	1
B. Gözetimin Tarihçesi	2
C. Farklı Sosyo – Ekonomik Kuramlar Çerçevesinde Gözetim	6
1. Bürokrasi ve Gözetim.....	6
2. Disiplin ve Gözetim.....	7
II. Teknolojik Gelişim ve Gözetim Uygulamaları	10
A. Gözetim Toplumu ve Teknolojik Gelişim	10
B. Gözetim Uygulamaları	28
1. Panoptikon.....	28
2. Süper Panoptikon	31
3. Sinoptikon	34
4. Banoptikon	35
C. Panoptikon Dışındaki Gözetim : Nano Teknoloji	37
III. Kapalı Devre Kamera Sistemi Tanımı, Unsurları ve Teknik Açıdan	
İncelenmesi.....	42

İKİNCİ BÖLÜM

BİR GÖZETİM TEKNİĞİ OLARAK KAPALI DEVRE KAMERALARIN KULLANILMASI

I. Kapalı Devre Kamera Sistemlerinin Hukuki Niteliği	49
II. Kapalı Devre Kamera Sistemleri Vasıtasıyla Yapılan Gözetimin Kanuni Dayanağı...	62
A. Devlet Tarafından Yapılan Gözetim	62
B. Özel Teşebbüsler ve Üçüncü Kişiler Tarafından Yapılan Gözetim	70

III. Kapalı Devre Kamera Sistemlerinin Kullanımının Amaçları	75
A. Suçun Önlenmesi ve Adaletin Sağlanması Amacı.....	76
B. Güvenliğin Sağlanması Amacı.....	80
C. Denetim Sağlama Amacı.....	81
D. Gözetleme Amacı.....	82
IV. Kapalı Devre Kamera Sistemlerinin Kullanım Alanları	82
A. Kamusal Alanlarda Kapalı Devre Kamera Sistemlerinin Kullanımı	87
1. Kolluk Faaliyetlerinde Kapalı Devre Kamera Sistemlerinin Kullanımı	87
2. Yerel Yönetim Faaliyetleri Kapsamında Kapalı Devre Kamera Sistemlerinin Kullanımı.....	96
3. Diğer Kamuya Açık Alanlarda Kapalı Devre Kamera Sistemlerinin Kullanılması	104
B. İşyerinde Kapalı Devre Kamera Sistemlerinin Kullanımı	108
C. Kamuya Açık Olmayan Yerlerde Kapalı Devre Kamera Sistemlerinin Kullanımı	119

ÜÇÜNCÜ BÖLÜM

KAPALI DEVRE KAMERALAR İLE GÖZETLENENLERİN KİŞİSEL VERİLERİNİN KORUNMASI

I. Türk Hukuk Sisteminde Kapalı Devre Kameralar İle Gözetlenenlerin Kişisel Verilerinin Korunması.....	124
A. Kişisel Verilerin Anayasal Düzlemde Korunması	124
B. Kişisel Verilerin Korunması Kanunu Kapsamında Gözetlenenlerin Kişisel Verilerinin Korunmasını İsteme Hakkı.....	134
1. KVKK Kapsamında Kapalı Devre Kamera Kayıtlarının Hukuki Niteliği.....	139
2. Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı	140
3. KVKK Kapsamında Gözetlenenlerin Kişisel Verilerinin Korunmasına İlişkin Hükümler.....	147
a. Gözetlenenlerin Kişisel Verilerinin İşlenmesinin Kanuni Dayanağı	147
b. Gözetlenenlerin Kişisel Verilerinin İşlenmesinde Temel İlkeler	148
c. Gözetlenenlerin Kişisel Verilerinin İşlenmesi Koşulları.....	158
4. Kişisel Verilerin Korunması Kanunu Kapsamında Gözetlenenlerin Hakları	170
5. İstisnalar	176
C. Özel Nitelikli Kişisel Veri Sayılan Kapalı Devre Kamera Görüntüleri	179

1. Özel Nitelikli ve Özel Nitelikli Olmayan Kapalı Devre Kamera Görüntülerinin Ayrımı	179
2. Özel Nitelikli Kapalı Devre Kamera Görüntülerinin Korunmasına İlişkin Tedbirler	184
3. Termal Kamera Görüntülerinin Kamu Sağlığı Amacıyla Kullanılmasının Değerlendirilmesi	187
II. Karşılaştırmalı Hukukta Kapalı Devre Kameralar İle Gözetlenenlerin Kişisel Verilerinin Korunması.....	191
A. Karşılaştırmalı Hukukta Kapalı Devre Kameralarla Gözetimde Kişisel Verilerin İşlenmesi	191
B. Yapay Zeka ve Kapalı Devre Kameralar	205
C. Tasarımda Gizlilik ve Kapalı Devre Kameralar	209
D. Kapalı Devre Kamera Verilerine Erişim Hakkı	212
E. Avrupa İnsan Hakları Mahkemesi ve Yerel Mahkeme İçtihatları Işığında Kapalı Devre Kameralar ile Gözetim	217
SONUÇ	229
KAYNAKÇA.....	230

KISALTMALAR

a.g.e.	: Adı geçen eser
a.g.i.	: Adı geçen internet sitesi
a.g.m.	: Adı geçen makale
AB	: Avrupa Birliđi (European Union – EU)
ABAD	: Avrupa Birliđi Adalet Divanı (Court of Justice of the European Union CJEU)
AİHM	: Avrupa İnsan Hakları Mahkemesi (The European Court of Human Rights)
AİHS	: Avrupa İnsan Hakları Sözleşmesi, Roma 4 Kasım 1950 (Convention for the Protection of Human Rights and Fundamental Freedoms)
AK	: Avrupa Konseyi (The Council of Europe)
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
AYM	: Anayasa Mahkemesi
AYMK	: Anayasa Mahkemesi Kararı
b.n.	: Başvuru Numarası
BDSG	: Bundesdatenschutzgesetz (Federal Veri Koruma Yasası-Almanya)
bkz	: Bakınız
BM	: Birleşmiş Milletler
C.	: Cilt
CCTV	: Close Circuit Television (Kapalı Devre Televizyon)
CJEU	: Avrupa Birliđi Adalet Divanı (Court of Justice of the European Union)
çev.	: Çeviren
der.	: Derleyen
diğ.	: Diğerleri
E.	: Esas sayısı
EDPL	: European Data Protection Law Review, Oxford University Press (Avrupa Veri Koruması Hukuk Dergisi, Oxford Üniversitesi Yayınları)
EİHB	: Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi, Paris 10 Aralık 1948 (The Universal Declaration of Human Rights-UDHR)
GVKT	: Genel Veri Koruma Tüzüğü
Haz.	: Hazırlayan

HD	: Hukuk Dergisi
HHFD	: Hacettepe Hukuk Fakültesi Dergisi
ILO	: The International Labour Organisation, UN (Birleşmiş Milletler Uluslararası Çalışma Örgütü)
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
İş K.	: 4857 sayılı İş Kanunu
CÜ	: Cumhuriyet Üniversitesi
K.	: Karar sayısı
KHK	: Kanun hükmünde kararname
k.t.	: Karar tarihi
KVKK	: 6698 sayılı 24 Mart 2016 tarihli Kişisel Verilerin Korunması Kanunu
m.	: madde
no.	: numara
par.	: paragraf
PVSK	: 2559 sayılı 4 Temmuz 1934 tarihli Polis Vazife ve Salahiyet Kanunu
PVK	: Polis Vücut Kamerası
RFID	: Radio Frequency Identification (Radyo Frekanslı Tanımlama)
RG.	: Resmi Gazete
s.	: Sayfa
S.	: Sayı
s.y.	: Son yararlanma
t.	: Tarih
TCK	: 5237 sayılı 26 Eylül 2004 tarihli Türk Ceza Kanunu
vb.	: ve bunun gibi
vd.	: ve devamı
Y.	: Yıl
Yarg.	: Yargıtay
YHGK	: Yargıtay Hukuk Genel Kurulu

GİRİŞ

Kişisel verilerin korunması hukuku son yıllarda tüm dünyada olduğu gibi ülkemizde de değer kazanmıştır. Bireyin gözetlenmesi ihtiyacı eskiden olduğu gibi bugün de insanlık için ayrı bir önem ifade etmektedir. Ancak gözetimin sadece insan odaklı olduğunu söylemek doğru olmayacaktır. Gözetim insan dışındaki diğer varlıkları da konu alan bir faaliyetler bütünü olmakla birlikte, insana yönelen gözetimin diğerine nazaran daha sık yapıldığı söylenebilir. Bu faaliyetlerin gerçekleştirilmesi için kullanılan teknikler yıllar içerisinde değişim göstermiştir. İçinde bulunduğumuz dijital çağda bireylerin gözetlenmesi eskiye göre çok daha kolaydır. Bu durumu gözetleyenler açısından olumlu, gözetlenen bireyler açısından ise olumsuz olarak değerlendirebiliriz. Gözetim faaliyetleri yıllar önce insan üzerinde yapılırken, günümüz dünyasında insan ile birlikte gerçekleştirilmektedir. İnsanlar sürekli olarak cep telefonları, bilgisayarları, tabletleri ve diğer kişiselleştirilmiş teknoloji icatları ile ilgili olmaya başlamışlardır. İşyerinde ayrı evde ayrı bilgisayarlara sahip olan insanlar, akıllı ev sistemleri sayesinde içinde yaşamını sürdürdüğü dört duvar arasında bile dijital çağa geçiş yapmış bulunmaktadır.

Yukarıda bahsedilen gözetim faaliyetlerinin gerçekleştirilmesinde kapalı devre kamera sistemleri gibi sürekli görüntüleme araçlarından da yararlanılmaktadır. Kapalı devre kameraların kullanıldığı gözetim sistemlerinde yapay zeka ve nesnelerin interneti teknolojisinin kullanılmasıyla birlikte insan tarafından bu gözetim faaliyetlerine harcanan emek ve zaman azalmıştır. Bu durumun insan yaşamını olumlu yönde etkilediğini söylemek mümkündür. Ancak bu işleyiş süreçlerinde kişisel verilerin korunması açısından bireylerin bireysel mahremiyetlerinin tehlikeye girmesi söz konusu olduğundan tüm bu faaliyetlerin hukuki düzenlemeler doğrultusunda ayrıntılı olarak değerlendirilmesi gerekmektedir.

Bir deyim olan “bir görüntü bin söze bedeldir” tabiri genel olarak kamera kayıtlarının neden bizim için önemli olduğunu ortaya koysa da bu tezin konusunun neden özellikle kapalı devre kamera sistemleri olarak belirlendiğini açıklamamız önemlidir. Kapalı devre kamera sistemleri çalışmamızın ilerleyen bölümlerinde açıklandığı üzere, kısaca video kameralar ile toplanan görüntü kayıtlarının aynı sisteme entegre olan video görüntüleme cihazına aktarıldığı dışarıya kapalı sistemler olarak tanımlanmaktadır. Yani bu sistemler aracılığıyla toplanan görüntüler bireysel ya da ticari amaçla video kaydı olarak bunu üçüncü kişilerin görüntülenmesine sunan diğer faaliyetlerden ayrılmaktadır. Tez çalışmamız bu bakımdan sınırlı tutulmuştur. Ayrıca bu sistemler güvenlik ve suçun önlenmesi gibi amaçlarla günlük yaşantı içinde yoğun ve kuşatıcı olarak kullanılmaktadır. Bir bireyin günlük yaşantısında, iş hayatında ya da özel hayatında kendisi ile ilgili değerlendirmelerde bulunduğu görülebileceği gibi bu kimsenin ailesi, yakınları ya da diğer üçüncü kişiler tarafından da o kimse hakkında farklı şeyler söylenebilecektir. Kişinin kendi hakkındaki değerlendirmeleri ya da diğer kişilerin onun hakkındaki söylemlerine tezat teşkil eden bir fotoğraf ya da video kesiti mevcut görüşleri kolaylıkla değiştirebilecektir. Çünkü bir video kesitini gören insan, o kesite ait zaman diliminde aynı yerde bulunmamış olmasına rağmen o anın bilgisine kameranın gözleri ile vakıf olma imkanına sahiptir. Bu bakımdan geçerlilik konusunda çok önemli bir değere sahip olan bireylere ait kamera görüntülerinin bu önemli özellikleri nedeniyle hukuka uygun olarak işlenmesi, saklanması, korunması ve en sonunda da imha edilmesi gerekmektedir. Bu işlemlerin hukuka uygun olarak yapılıp yapılmadığının tespitine yönelik normatif düzenlemeler çeşitli hukuk kaynaklarında yer buluyor olsa bile, bu çalışma esas olarak Kişisel Verilerin Korunması Kanunu temel alınarak hazırlanmıştır.

BİRİNCİ BÖLÜM

GÖZETİM KAVRAMI, GÖZETİMİN TARİHSEL GELİŞİMİ VE KAPALI DEVRE KAMERA SİSTEMLERİ

I. Gözetim Kavramına Genel Bir Bakış ve Gözetimin Tarihi

A. Gözetim Kavramı

Temel amacı bireylerden bilgi edinme ve sınıflandırma olan gözetim faaliyetleri, teknolojinin gelişmesi ile birlikte farklı hallere bürünerek karşımıza çıksa da aslında yeni bir kavram değildir. Gözetim (surveillance), hakkında veri toplananları etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel veri toplanması ve işlenmesidir¹.

Gözetim sözcüğü ilk defa 18. yüzyılın sonlarına doğru bir bireyin hareketlerinin yakından izlenmesi anlamında kullanılmaya başlamakla birlikte² en genel şekliyle, bir ya da daha fazla kişinin hareketlerinin veya iletişiminin sistemli olarak araştırılması ya da izlenmesi olarak tanımlanabilir³. Gerçekleştirilen gözetim faaliyetinin birey hakkında bilgi edinmenin yanında, edinilen bu bilgilerin sınıflandırılması amacına hizmet ediyor olması gereklidir. Bu nedenle bireylerin bilgileri sınıflandırma amacı olmadan sadece birbirlerini izlemeleri bu kapsama girmeyecektir.

Gözetimin hedefi olan bireylere ait kişisel veri, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu durumda kişinin internet geçmişi, biyometrik verileri, DNA kodları ve kişiye ait kapalı devre kamera görüntüleri gibi bir gerçek kişiye ait tüm kişisel verilerin gözetimin konusunu oluşturabileceğini söylemek mümkün olabilir.

Tez çalışmamızın bu bölümünde gözetim kavramını gözetimin tarihsel gelişimini açıklayacağımız için belirtmemiz gerekir ki gözetim olgusunun doğduğu dönemdeki toplum ile günümüz toplumunda farklı gözetim teknikleri kullanılmaktadır. Bugün kullandığımız

¹ David LYON, Gözetlenen Toplum, Günlük Hayatı Kontrol Etmek, çev. Gözde Soykan, Kalkedon, İstanbul 2006, s.13.

² Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul 2020, s. 624.

³ Roger CLARKE, "Dataveillance: Delivering '1984'", 9 Şubat 1993, <http://www.rogerclarke.com/DV/PaperPopular.html> (s.y. 8 Şubat 2022)

teknolojilerin bir çoğunun dayanağı olan bilgisayar teknolojilerinin gözetim tekniklerin gelişmesinde ve çeşitlenmesinde önemli bir rolü bulunmaktadır.

Gözetim, 18. yüzyılda belirli fiziksel duvarlar içinde hiçbir şeyi kaçırmayan mükemmel göz vasıtasıyla sadece ve ancak her şeyi sürekli olarak görmeye dayalı olarak yürütülebiliyordu. Foucault'un, "...Ledoux 'un Arcet-Senans'ı inşa ederken hayal ettiği budur: Daire biçiminde düzenlenmiş olan ve hepsi de içe doğru açılan binaların merkezinde yüksek bir bina, tüm yönetsel, asayişe ve gözetime ilişkin, denetimin ekonomisine ilişkin ve itaat ile çalışmaya teşvikleri sağlayan dinsel işlevleri kendi bünyesinde toplayacaktır; bütüne emirler buradan gelecek; tüm faaliyetler burada kaydedilecek ve yargılanacaktır..." diyerek belirttiği üzere⁴ geçmişte kullanılan dairesel mimariler gibi ütöpik tekniklerin yerini artık zaman ve mekan tanımayan bilgisayarlar ve yapay zeka almıştır.

İnsan doğası gereği başkası hakkındaki bilgiye merak duymaktadır. Başkasına ait olanın bilinmesi geçmişte olduğu gibi bugün de güç sayılmaktadır. Bireyler hakkında bilgi toplama ve bunları işleme yani gözetleme faaliyetlerinin neredeyse medeniyetin kendisi kadar eski olduğunu söyleyebiliriz. Fakat günümüzde kullanılan gözetim kavramı modernitenin geliş ve modern devletin ortaya çıkması ile birlikte bugünkü halini almıştır⁵.

B. Gözetimin Tarihçesi

Sanayi devrimi ve beraberinde getirdiği sosyal ve kültürel etkilerden biri olan insanların bir arada yaşamaları 18. yüzyıldan itibaren özellikle İngiltere ve Batı Avrupa' da bireylerin özel yaşamlarının gizliliğini gündeme getirmiştir. Bireylerin şehir hayatında sosyal ilişkiler kurması, fabrikalarda birlikte çalışması gibi gündelik değişimler ve bu değişimler karşısında özel yaşamın gizliliği hakkını koruyan yeni düşünceler ortaya çıkmıştır⁶.

Gözetim olgusu dünden bugüne çeşitli yaklaşımlar çerçevesinde incelenmesine rağmen, sosyal bilimlerde kabul görmesi Michael Foucault sayesinde olmuştur. Foucault, iktidarın sosyal kontrol mekanizmalarını Ortaçağ'dan moderniteye uzanan değişimi bağlamında ele

⁴ Michel FOUCAULT, Hapishanenin Doğuşu, Gözetim Altında Tutmak ve Cezalandırmak, çev. Mehmet Ali Kılıçbay, İmge Kitabevi, Ankara 2019, s.260.

⁵ Elif KÜZECİ, Kişisel Verilerin Korunması, Onikilevha Yayıncılık, İstanbul 2021, s. 21.

⁶ A.g.e., s.22.

almaktadır⁷. Modernite kavramı Giddens’a göre, yaklaşık olarak 17. yy’dan itibaren Avrupa’da ortaya çıkan ve az ya da çok tüm dünya çapında etkili hale gelen sosyal yaşam ve örgütlenme tarzları olarak ifade edilmiştir⁸. Ortaçağ’ın sona ermesiyle gelişmeye başlayan ve sanayi devrimi ile Batı Avrupa’da hız kazanan modernite, bugünkü modern devletin ortaya çıkmasına sebep olmuştur. Modern devlet ise devleti oluşturan bireyler hakkında bilgiye ihtiyaç duymaktadır. Bu ihtiyacın birden fazla nedeni bulunabilir: Merkezi yönetimi sağlamak, güçlendirmek, sosyal devlet ilkesi gereği yurttaşların refahının sağlanması, sağlık planlamalarının yerine getirilmesi ya da güvenliğin sağlanması bunlardan bir kaçını oluşturmaktadır⁹.

Modern devletin yurttaşları hakkında tutmakta olduğu kayıtları esas olarak üçe ayırabiliriz. 1) *Yönetisel Kayıtlar* : Yurttaşların yönetim birimi ile bir işlem yapması sonucu oluşturulan kayıtlar: kimlik belgesi düzenlenmesi, pasaport başvurusu, vergi beyanı verme, adres bilgisi değişikliği bildirimi vb. 2) *Haber alma ve istihbarat faaliyetleri sonucunda oluşturulan kayıtlar* : Polisin topladığı bilgiler, soruşturma faaliyetleri vb. 3) *İstatistiki faaliyetler sonucu oluşturulan kayıtlar*: Nüfus sayımı, anket, saha araştırmaları vb. gibi faaliyetler sonucunda oluşturulmuş kayıtlardır. Bu kayıtların oluşturulması açısından gözetim faaliyetleri büyük önem taşımaktadır¹⁰.

İnsanların kullanmış oldukları araç ve gereçler gibi üretim teknikleri de farklı dönemlerde değişiklik göstermiştir. Modernleşme sürecinin başında tarım toplumunda yaşayan insan makineleşme ve fabrikalaşma gibi gelişmeler ile birlikte sanayi toplumunun ortaya çıkışına şahit olmuştur. Sanayi toplumu kavramı ilk olarak makinelerin üretim faaliyetlerinde kullanıldığı büyük fabrikaları aklımıza getirirse de soyut açıdan toplumun kültürünün, kurumlarının ve gelişiminin endüstriyel üretim süreçleri tarafından belirlendiği bir toplum türünü ifade etmektedir¹¹. Günümüzde endüstriyel faaliyetlerin sanayi toplumunun başlangıcında olduğundan daha geniş ölçüde yapıldığını ve daha gelişmiş araçların bu faaliyetlerde kullanıldığını söyleyebiliriz. Ancak bugünün toplumunu sanayi toplumu olarak adlandırmak yerine bilgi toplumu olarak adlandırmamız daha doğru olacaktır. Çünkü içinde

⁷ Cengiz DERDİMAN, Nihal TATAROĞLU, “Devlet Gözetimi İle İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri”, İnÜHFD, C.7, S.1, Y. 2016, s. 252.

⁸ Steven LOYAL, The Sociology of Anthony Giddens, Pluto Press, Virginia 2003, s. 115.

⁹ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 23.

¹⁰ A.g.e., s. 24.

¹¹ Gordon MARSHALL, A Dictionary of Sociology, <https://www.encyclopedia.com/social-sciences-and-law/sociology-and-social-reform/sociology-general-terms-and-concepts-80> (s.y. 8 Şubat 2022)

yaşadığımız bu dönemde küreselleşmenin de etkisiyle sanayi toplumundan bilgi toplumuna geçiş yaşanmıştır¹². Bilgi ve iletişim teknolojilerindeki gelişim sonucunda asıl üretim aracı bilgi haline gelmiş, çeşitli iş kollarında hammadde olarak kullanılmaya başlanmıştır.

Nitekim bir bilgi toplumu içerisinde yaşadığımız göz önüne alındığında bilgiye yönelik ihtiyacın ve talebin önceki dönemlere göre çok daha fazla açıktır. Örneğin, yapay zeka teknolojilerinin farklı algoritmaların geliştirilebilmesi için büyük veri setlerine ihtiyaçları vardır. Ancak bu şekilde büyük veri kümeleri kullanılarak doğru analizlere ulaşabileceklerdir. Bununla birlikte Dülger tarafından, yapay zekanın kişisel verilerin korunması hukuku açısından bir takım sorunlara sebep olduğu da belirtilmiştir. İlk sorun büyük veriye ihtiyaç duyulması sebebiyle tüm kişisel verilerin veya mümkün olan en çok miktardaki verinin toplanması ya da bir araya getirilmesidir. Bununla birlikte hali hazırdaki verilerin daha fazla öğrenmeye ve analize konu olarak veriden veri türetilmesine dair süreçlerin sakıncalı olduğu söylenebilmektedir. Üçüncü bir sorun ise belirli bir veri işleme faaliyetinde elde edilmiş olan verilerin, başlangıçta bilinmeyen ve çok çeşitli amaçlar için işlenebilmesi, yapay zekanın öngörülemezlik özelliği sebebiyle verinin işleme amaçlarının yerinden kurgulanmasının söz konusu olması ya da amaçla sınırlı veri işleme ilkesine aykırı davranılmasıdır. Son olarak ise giderek daha fazla otomatik karar alma mekanizmasına yer verilmesi bu teknolojinin doğurduğu sakıncalardan biri olarak görülmektedir¹³.

Bilgi toplumu istediği bilgiye ulaşmak açısından ise çok farklı kanalları değerlendirmektedir. Bugün dünyadaki en çok yaşayan insan nüfusuna sahip olan Çin’de yer alan en bilinen gözetim aracı 626 milyon yüz tanıma teknolojisi barındıran kamera ile yürütülen bir gözetim ağıdır¹⁴. Bu sistem Çin hükümetine bireyleri tanıma ve izleme imkanı tanımakla birlikte, sistemin sürdürülebilirliğinin sağlanması amacıyla en az beş adet ayrı veri platformu kurulmuş olup, bu platformlar hem birbirleri ile veri alışverişinde bulunurlar hem de bir bütün olarak ülkenin sosyo-kredi sistemini desteklemektedirler¹⁵. Bu sosyo-kredi sistemi Çin

¹² Faruk KOCACIK, “Bilgi toplumu ve Türkiye”, C.Ü. Sosyal Bilimler Dergisi, C. 27, S. 1, Y.2003, s.2.

¹³ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 675.

¹⁴ Birleşik Krallık genelinde faaliyetine devam eden kamera sayısı yaklaşık 6 milyon adettir. IHS Markit tarafından yürütülen araştırmaya göre, 2021 yılı sonunda yaklaşık 1 milyar adet kameranın gözetim faaliyetlerinde kullanılıyor olacağı öngörülmektedir. Çin ile Amerika Birleşik Devletleri kişi başına düşen kamera sayısı açısından birbirleri ile yarışmaktadır. Bkz. Michael, KWET, The Rise of Smart Camera Networks, and Why We Should Ban Them, The Intercept, Police are using cameras at private businesses and homes, along with AI, to expand their video surveillance — raising privacy concerns. January 27 2020, 8:53 p.m., <https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/> (s.y. 15 Kasım 2021)

¹⁵ Lizie RETTINGER, “The Human Rights Implications of China’s Social Credit System”, Journal of High Technology Law, C. 21, S. 1, 2021, s. 11.

vatandaşlarının alım güçleri ya da finansal durumları ile doğrudan ilgilidir. Görüldüğü üzere Çin örneğinde devlet, veri toplama ve kullanma amaçları arasındaki geçişkenliği kullanarak, ihtiyacı olan bilgiyi ilgili kanallara aktarmaktadır.

Modern devletin yurttaşlarına karşı olan sorumluluklarını yerine getirme safhasında bilgiye ihtiyaç duyduğu bir gerçektir. Ancak bilgiye ihtiyaç duyan sadece merkezi yönetim olarak kalmamaktadır. Kamu gibi özel sektör aktörleri de karlılıklarını ve verimliliklerini artırmak için müşterilerinin, çalışanlarının, hedef kitlelerinin kişisel bilgilerine ihtiyaç duymaktadır. Kamu ve özel sektörün benzer faaliyetleri farklı amaçlar için gerçekleştirdikleri açıktır. Özel sektörün amacı verimliliğini arttırarak karlılığını yükseltmek; modern devletin amacı ise bilgi güvenliğini sağlamak, ulusal egemenlik ve refah düzeyini artırmak olarak karşımıza çıkmaktadır¹⁶. Öte yandan, kamu ve özel sektörün kişilere ait bilgiyi işlemesi açısından benzerlikler bulunmaktadır. Örnek vermemiz gerekirse, Türkiye’ de kamu hizmetlerinin tek bir noktadan ve farklı kanallardan entegre olarak sunumunu hedefleyen E-Devlet Kapısı 18 Aralık 2008 tarihinde 22 farklı hizmetle faaliyete geçmiştir. 2010 yılı sonunda ise sistem üzerinden verilen hizmetlerin sayısı 246’ya yükselmiştir. Öte yandan, aynı dönem içerisinde kullanıcı sayısında önemli artışlar gerçekleşmiştir. 2010 yılının sonunda 1.950.000 olan kayıtlı kullanıcı sayısı, 2011 yılının Mayıs ayı başında 7.140.000 sayısına ulaşmıştır¹⁷. Kamu hizmetlerinin daha etkin ve etkili sunulmasının yanı sıra yurttaşların sunulan bu hizmetlere daha kolay ulaşmasının sağlanması aslında birer müşteri olarak değerlendirildikleri izlenimi yaratabilir. Bu sisteme entegre edilen kamu kurum ve kuruluşları yurttaşlar için verdikleri hizmetler kapsamında kişisel veri işlemektedirler. Bununla birlikte, özel sektör aktörü olan bir bankayı ele aldığımızda ise bankanın müşterilerinin çeşitli hesap işlemlerini yapmak, kredi kullandırmak ve diğer bankacılık hizmetlerinden müşterilerini yararlandırmak ya da faaliyetlerinin promosyonunu yapmak amaçlarına istinaden müşterilerine ait kişisel verileri tıpkı E-Devlet Kapısı’na benzer internet bankacılığı şubeleri aracılığıyla işlemekte olduğunu görebilmekteyiz. Burada gerek kamu gerek ise özel sektör aktörünün hedefi müşteri memnuniyetinin sağlanmasıdır¹⁸. Ayrıca her iki aktörün de yurttaşların kişisel verilerini işleme sürecinde Kişisel Verilerin Korunması Kanunu’na tabi oldukları görülmektedir¹⁹. Bu

¹⁶ Elif KÜZECİ, Kişisel Verilerin Korunması, s.25.

¹⁷ T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı, DPT Yayın No: 2826, Bilgi Toplumu İstatistikleri, Haziran 2011, s.77.

¹⁸ Elif KÜZECİ, Kişisel Verilerin Korunması, s.25.

¹⁹ “Kanunun 2. maddesinde Kanunun kapsamı belirlenmektedir. Buna göre Kanun, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır. Kanunda, özel hukuk tüzel kişileri

doğrultuda da kişisel verilerin etkin korunması için hem kamu hem de özel sektör tarafından benzer veri koruma tedbirlerinin alınması gerekli olmaktadır.

C. Farklı Sosyo – Ekonomik Kuramlar Çerçevesinde Gözetim

1. Bürokrasi ve Gözetim

Modernite dediğimiz kavram çalışmamız içerisinde daha önce de açıklandığı üzere, hem bir tarihsel süreci (modern çağ) hem de Rönesans sonrasındaki aydınlanma ile 17 ve 18. yüzyıldaki akıl çağında ortaya çıkan belirli sosyo-kültürel normlar, tutumlar ve uygulamalar topluluğunu ifade etmektedir²⁰. Gözetimin, modernite ile gelişimi farklı düşünürlerin konuya başka açılardan yaklaşımlarına sebebiyet vermiştir. Düşünürlerin bir kısmı gözetim olgusunu ekonomik bir yaklaşımla sınıf ilişkileri veya bilimsel yönetim temelinde incelemiştir. Bir kısmı düşünürler gözetimin kültürel ve felsefi boyutlarını incelerken, bazı düşünürler ise gözetimi ulus-devlet ve moderniteyle ilişkilendirerek özgürlükler sorunu olarak görmüşlerdir²¹.

Burada hem Karl Marx hem de Max Weber'in gözetimin bürokrasi ile olan ilişkisi üzerinde durduğunu görmek mümkündür. Bürokrasinin tam olarak neyi ifade ettiğinin bilinmesi bu değerlendirme açısından önemlidir. Bürokrasi kavramı İngilizcede “bureau²²” (belirli bir konuda bilgi sunan organizasyon ya da ofis) kelimesinden türemiş olup, 18. yüzyıldan itibaren de memurların çalıştığı devlet dairesi, ofis ve büro gibi, devlete ait çalışma alanlarını nitelendirmekte kullanılmaktadır²³. Ancak bu tanımdan destek alarak bürokrasinin salt devlet kurumlarından oluştuğunu söylemek zordur. Bazı yazarlar bürokrasinin ticari teşebbüsleri de kapsadığı yönünde görüş bildirmişlerdir²⁴. Weber'in aşağıda kısaca ifade etmeye çalıştığımız bürokrasi anlayışı da bu kapsayıcılığı kabul etmektedir.

ile kamu hukuku tüzel kişileri bakımından bir ayrım yapılmamıştır. Bu nedenle, Kanunda öngörülen usul ve esaslar hem özel kuruluşlar hem de kamu kuruluşları bakımından uygulanacaktır.” Bkz. KVKK, 2. madde gerekçesi.

²⁰ Bkz. yuk. s.13.

²¹ Uğur DOLGUN, Enformasyon Toplumundan Gözetim Toplumuna, Ekin Kitabevi, Ankara 2005, s. 73.

²² Kavramın İngilizce karşılığı için bkz. <https://www.oxfordlearnersdictionaries.com/definition/english/bureau?q=bureau> (s.y. 12 Şubat 2022)

²³ Hasan ACAR, “Kamu Güvenliğinin Sağlanmasında Weberyen Bürokrasi ve Hiyerarşi Kavramı”, Uluslararası Yönetim İktisat ve İşletme Dergisi, C. 14, S. 3, 2018, s. 671.

²⁴ Daniel J. SOLOVE, The Digital Person: Technology and Privacy in the Information Age, New York University Press, 2004, s. 38.

Gözetimi, emek ve sermaye arasındaki mücadelenin bir ögesi olarak gören Karl Marx’a göre, fabrikalardaki işçilerin izlenmesi, temelinde sermaye adına yönetsel denetimin sürdürülmesi için bir araçtır. Bununla birlikte Weber’e göre, modern toplum değişken bir yapıdadır. Weber burada Marx’tan farklı olarak, görüşünün temeline ekonomiyi değil teknolojik gelişimi almıştır. Marx’ın “el değirmeni bize feodalizmi, buharlı makineler kapitalizmi verdi” savı, Weber’in bakış açısına göre ekonomik değil, teknolojik bir önermeyi ifade etmektedir²⁵. Weber’in modern toplumunda kitlesel, karmaşık ve değişken topluluğun örgütlenmesi, ancak toplumsal yaşamın her alanına yönelik rasyonel planlama, örgütlenme, siyaset yapma ve denetleme yapılması suretiyle mümkün olabilecektir. Bu ise sadece rasyonel yönetsel bir araç vasıtasıyla yani “modern bürokrasi” ile sağlanabilecektir²⁶.

Weber’in “modern bürokrasi”si, sadece devlet mekanizmaları dahilinde var olan bir bürokrasi değil, devlet mekanizmalarının yanı sıra modern ticaret işletmelerini, modern orduyu da kapsayacak şekilde, modern toplumun büyük ölçekli örgütlenmelerinin yönetiminin sosyal bir biçimidir. Kamu ya da özel bütün bu modern örgütlerin bürokrasi içerisinde verimli uygulama arayışı ise veri saklama ve çağırma araçları geliştirilmesi sonucunu doğurmaktadır. Bürokratik faaliyet çerçevesinde kamu çalışanları da bir makine dişlisi gibi mekanikleşerek adeta makinenin bir dişlisi haline gelmektedirler. Bu durum insanın kendi yarattığı bir sistemin mahkumu olmasına sebebiyet verebilir²⁷.

Diğer bir yönden Habermas ise, bu düzeni (gözetimi) bir itaat kafesine benzeterek özgürlüğün kaybı olarak nitelendirmektedir²⁸. Habermas’a göre; kültür, kişilik ve sosyal iletişim ağlarını kapsayan alan ile devlet ve ekonomiye hakim bürokratik sistem birbirinden ayrılmaktadır. Bu görüşe göre, bürokratik alandan bireyin kültür, kişilik ve sosyal iletişim alanına yapılacak her müdahale toplumsal yaşamı tehdit olarak algılanabilecektir.

2. Disiplin ve Gözetim

Gözetim olgusunun dünden bugüne çeşitli yaklaşımlar çerçevesinde incelenmesine rağmen, sosyal bilimlerde kabul görmesi Michel Foucault sayesinde olduğunu daha önce

²⁵ Anthony GIDDENS, Siyaset, Sosyoloji, ve Toplumsal Teori, Toplumsal Düşüncenin Klasik ve Çağdaş Temsilcileriyle Hesaplaşmalar, İstanbul 2017, s. 76.

²⁶ Elif KÜZECİ, Kişisel Verilerin Korunması, s.26.

²⁷ A.g.e., s.26.

²⁸ Jürgen, HABERMAS, İletişimsel Eylem Kuramı, çev. Mustafa Tüzel, Alfa Yayınları, İstanbul 2019, s. 938.

vurgulamıştık. Foucault’a göre, gözetim bürokratik örgütlenmenin sınırlarını aşan, toplumun geneline yayılan geniş bir disiplin bağlamında değerlendirilmelidir²⁹.

18. yüzyılın sonunda Avrupa’ da ortaya çıkan “disiplinci iktidar”, insanlardan daha çok şey almak için terbiye etme amacı taşımakta, bunu ise şiddete veya bedensel cezaya başvurarak değil, bireylere belli öznellik biçimleri dayatarak yapmaktadır³⁰. Disiplinci iktidarın yukarıdaki hedeflerini gerçekleştirmesi için ideal kurum ise Jeremy Bentham’ın 19. yüzyılda hazırladığı bir hapisane mimarisi planı yani “panoptikon” dur. Panoptikon, her ne kadar bir mimari biçim olsa bile, özelde bir yönetim biçimi olarak görülebilir³¹. Foucault tarafından panoptikon mimarisinin sadece hapisane için geçerli olmadığı, bununla birlikte bu yönetim biçiminin fabrika ve okullarda da uygulanabileceği belirtilmiştir³².

Panoptikon gerçek bir bağımlı olma durumu yaratmaktadır hatta öylesine bir ortam yaratmaktadır ki, hayali bir ilişkiden mekanik olarak doğmuş olsa bile mahkumu iyi davranmaya, deliyi sakın olmaya, işçiyi çalışmaya, öğrenciyi özenli olmaya, hastayı tedaviye zorlamaya sevk ederken, tüm bunlar için güç kullanmayı gerektirmez³³.

Panoptikon fiziksel olarak şu şekilde tanımlanmıştır: “ Çevrede halka şeklinde bir bina, merkezde bir kule, bu kulenin halkanın iç cephesine bakan geniş pençeleri vardır, çevre bina hücrelere bölünmüştür, bunlardan her biri binanın bütün kalınlığını kat etmektedir, bunların biri içeri bakan ve kuleninkilere karşı gelen, diğeri de dışarı bakan ve ışığın hücreye girmesini sağlayan ikişer pencereleri bulunmaktadır. Bu durumda merkezi kuleye tek bir gözetmen ve her bir hücreye tek bir mahkum, bir deli, bir hasta, bir işçi veya bir okul çocuğu kapatmak yeterlidir. Geriden gelen ışık sayesinde, çevre binadaki hücrelerin içine kapatılmış küçük silüetleri olduğu gibi kavramak mümkündür³⁴.”

Bentham’ın tasarladığı mimari sistemin, Foucault tarafından bütün toplumda yer alan daha geniş bir disiplin kuramı çerçevesine oturtulduğunu söylememiz mümkündür. Foucault

²⁹ Elif KÜZECİ, Kişisel Verilerin Korunması, s.28.

³⁰ Michel FOUCAULT, Hapishanenin Doğuşu, s. 255.

³¹ A.g.e., s.304; Michael FOUCAULT, Büyük Kapatılma, çev. I. Ergüden & F. Keskin, Ayrıntı Yayınları, İstanbul 2000, s. 135; Abdurrahman, SAYGILI, Mikro-İktidarın Bir Fiziği: Hapishane, AÜHFD, C. 53, S.2, Y. 2004, s.189.

³² Elif KÜZECİ, Kişisel Verilerin Korunması, s. 28.

³³ Michel FOUCAULT, Hapishanenin Doğuşu, s. 299

³⁴ A.g.e., s. 296.

adeta Bentham'ın panoptikon tasarımına ışık tutmaktadır. Gözetime daha kapsayıcı ve geniş bir açıdan bakan Foucault'dan gözetimin sosyal yapısına ilişkin daha çok şey öğrenmek mümkün olmaktadır.

Açıklamaya çalıştığımız bu sistemde mahkum veya tutuklunun önünde onu sürekli olarak gözetleyen kule merkezi, iktidarı temsil eder. Bununla birlikte mahkum merkezden gelen bakışların sürekliliği nedeniyle kendisinin gözetlenip gözetlenmediğini bilmemekte fakat gözetlendiğinden sürekli olarak şüphe duymaktadır. Böylelikle; gözetlenenler, gözetleyenlerin ne zaman kendilerini gözetlediklerini bilmedikleri için de davranışlarını sınırlamak ve her an gözetleniyormuş gibi davranışları sınırlama durumunu içselleştirmek zorunda kalmaktadırlar³⁵. Tam da bu noktada kapalı devre kameralar ile gerçekleştirilen gözetim faaliyetlerine değinmemiz gereklidir. Gerçekten de günümüzde kapalı devre kamera ile izleme faaliyetleri bireyleri dört bir yandan çevrelemiştir. Birey evde, işyerinde, okulda, trafikte ya da yolda sürekli olarak izlenmektedir. O halde yukarıdaki önermenin aynısının kapalı devre kameralar ile gözetlenen insanlar açısından da geçerli olacağı söylenebilecektir.

Foucault tarafından yapılan tanıma göre “modern toplum, disipliner bir toplumdur”. Bu modern toplumlarda iktidar, insanların toplumsal normlara riayet etmelerini sağlamak için onları sürekli daha fazla gözetler. Toplumu oluşturan bireylerin hareketleri belgelenip sınıflandırılarak kayıt altına alınır. Bu şekilde kayıtlanan tüm bilgiler temelinde iktidarla ilişkilidir³⁶. Belki de buradan çıkarılacak en önemli sonuç şudur: “Modern devlet verimliliği arttırmak ve hedeflerini gerçekleştirmek için kişisel verilere gereksinim duyar”³⁷. İzlediği amaçlara göre kişisel verileri elde eden, toplayan, saklayan, değiştiren, dönüştüren, aktaran ve kamu gücünü kullanan modern devlet yönetimi; tüm toplumsal sistem içerisinde “en güçlü bilgi tekeli” haline gelmiştir.

Dikkat edilmesi gereken bir diğer nokta da bilgiye ihtiyaç duyanın toplumsal sistemlerden sadece kamu erkinin olmadığıdır. Diğer toplumsal sistemlerden olan kapitalist işletmeler de bilgiye ihtiyaç duymaktadırlar. Hem devlet hem de kapitalist işletmelerin iktidar

³⁵ Abdurrahman SAYGILI, s. 189.

³⁶ David LYON, Elektronik Göz, çev. Dilek Hattatoğlu, Sarmal Yayınevi, İstanbul, 1997, s. 44 .

³⁷ Elif KÜZECİ, Kişisel Verilerin Korunması, s.29.

sağlamak için bilginin gücüne duydukları bu gereksinim ve bağımlılık, bilgi toplumunun nasıl modern dönemin bir bileşeni olduğunu ortaya koymuştur³⁸.

Çalışmamızın ilerleyen bölümlerinde değineceğimiz üzere³⁹; günümüz koşullarında, enformasyon teknolojilerinde yaşanan gelişmeler ile birlikte gözetim duvarlar, hapishaneler, kapalı mekanlar ve sınırlara dayandırılmaktan çıkarak, toplumsal yaşamın her alanına sirayet etmiştir. Örneğin; kapalı devre kameralar, telefon kayıtlarının dinlenmesi, GPS teknolojileri ve kredi kartı hareketleri gibi teknolojik araçlarla gözetim yapılmaktadır. Açıkça görüldüğü üzere tüm bunlar bizi, gözetim toplumunda yeni bir denetim biçimi olan “süper panoptikon”a götürmektedir.

II. Teknolojik Gelişim ve Gözetim Uygulamaları

A. Gözetim Toplumu ve Teknolojik Gelişim

Gözetim toplumu gibi kavramlar içinde bulunduğumuz modern dünyada bütün yaşam tarzımızın gözetim ile çevrelendiğine dikkat çekmektedir⁴⁰. 20.yüzyıl teknolojisindeki gelişmeler ve elektronik gözetim vasıtalarındaki artışla birlikte, gözetim uygulamaları ileri teknoloji tabanlı prosedürler ve tekniklerden oluşan bir boyuta geçiş yaparak, geçmişteki benzer uygulamalardan farklılaşmıştır. Gözetimin bilgisayarlar aracılığı ile yapılıyor olması ve elektronik veri tabanlarının veri depolama alanları olarak kullanılması, bu dönüşümü gözler önüne sermektedir. Bu dönüşümün belki de en büyük özelliği bilginin çoğaltılmasıdır. Farklı veri tabanlarının birbiriyle iletişim kurması sayesinde bilginin çoğaltılmasının önü açılmıştır⁴¹. Burada bahsedilen değişim; sosyal, yönetsel ve siyasal kararlar ile teknolojik gelişmelerin birbirlerini etkilemeleri sonucunda meydana gelmiştir⁴².

Gözetim toplumu, bilgi toplumu ya da Toffler’in deyimiyle üçüncü dalga⁴³ denilen süreçte asıl önemli olanın “bilgi” olduğu açıkça görülmektedir. Diğer bir deyişle, gözetim toplumunda gözetimdeki gelişmeye öncülük eden birinci araç bilgidir. Bilginin hangi vasıtalar

³⁸ A.g.e., s.29.

³⁹ Bkz. s. 25. vd.

⁴⁰ David LYON, Gözetim Çalışmaları, Genel Bir Bakış, çev. Ali Toprak, Kalkedon, İstanbul 2013, s. 45.

⁴¹ Efe, BAŞTÜRK, Panoptikon’ dan Post Panoptikon’ a Gözetimin Soykütüğü (Doktora Tezi), Ankara 2016, s. 271.

⁴² Colin J. BENNETT, Regulating Privacy, Data Protection and Public Policy in Europe and the United States, Cornell University Press, ABD 1992, s. 21’den naklen Elif KÜZECİ, Kişisel Verilerin Korunması, s. 31.

⁴³ Alvin TOFFLER, Üçüncü Dalga, çev. Selim Yeniçeri, Koridor Yayıncılık, İstanbul 2018, s.84.

üzerinden elde edildiği zamana bağlı olarak değişmiştir. Ancak bilgiye erişim araçları değişse bile bilgi toplumu içerisinde verilerin korunması her zaman önemli olmuştur.

19. yüzyıl öncesine kadar kamu erki tarafından kişilere ilişkin olarak az sayıda ve sınırlı alanlarda kayıt tutulduğunu görmekteyiz. Bu dönemde iktidar ve kilise arasında güçlü bir bağ bulunmaktadır. Örneğin; Hristiyan toplumlarda tutulan kayıtların kiliseler tarafından tutulduğunu görmek bizi şaşırtmamaktadır⁴⁴. Daha sonrasında ise bilgisayar teknolojileri ve veri bankalarının kullanılması, gözetim ve modernitenin paralel olarak gelişmesine sebebiyet vermiştir.

Gözetimdeki gelişmenin araçlarından bir tanesi olan bilgisayarlar, verilerin toplanmasını, işlenmesini, saklanmasını, aktarılmasını ve birbirleri ile ilişkilendirmesini hızlandırmış, kolaylaştırmış, yaygınlaştırmış ve ucuzlaştırmıştır⁴⁵. Günümüzde herkesin evinde kişisel kullanım amacıyla en az bir tane bulunan bilgisayar, 1950’li ve 1960’lı yıllarda sadece devlet tekelinde kullanılan, neredeyse bir oda büyüklüğünde yer tutan bir sistemdir. Bu karmaşık sistemler aynı zamanda maliyetleri nedeniyle sadece devletler ve büyük şirketlerde bulunabilmekteydi⁴⁶.

Hükümetler tarafından toplanan büyük miktardaki verilerin büyük veri bankalarında tutulması bireylerin bu güç karşısında korkmalarına sebebiyet vermiştir. Bu büyük veri birikimlerinin içerisinde kullanışlı olanların çekip çıkarılmasına olanak tanıyan “veri madenciliği”nin gelişmesi de işte bu sebeple olmuştur. Veri madenciliği faaliyeti bir analiz sürecini ifade etmekte olup, amacı veri kümeleri içerisinde yer alan daha önceden tespit edilmemiş kalıpları ortaya çıkarmaktır⁴⁷. Bu faaliyetler sonucunda elde edilen sonuçlar bazı durumlarda veriler (değişkenler) arasındaki ilişkiyi ortaya çıkarır ve böylece verileri işleyen tarafa mevcut verilere dayanarak bireylerin bilinmeyen özellikleri hakkında çıkarımlar yapmasına olanak tanır⁴⁸. Hem devlet kurumlarının hem de özel teşebbüslerin günümüzde veri

⁴⁴ Daniel J. SOLOVE, s. 13.

⁴⁵ Arthur R. MILLER, The Assault on Privacy, Computers, Data Banks, and Dossiers, The University of Michigan Press, ABD 1971, s. 216.

⁴⁶ Harry HENDERSON, Privacy in the Information Age, Facts of File, ABD, 2006, s. 13.

⁴⁷ Pauline T. KIM, "Data Mining and the Challenges of Protecting Employee Privacy under U.S. Law", Comparative Labor Law & Policy Journal, C. 40, S. 3, Y. 2019, s. 406.

⁴⁸ Ayrıca veri madenciliğinden elde edilen sonuçların kullanılmasındaki takdirin veri işleyen tarafa ait olduğu, başlangıçta ele alınan veri ile sonradan türetilen veri arasındaki bağlantının ne ölçüde doğru olduğunun ve isabetliliğin bu hususta önemli olduğu vurgulanmıştır. Bkz. Giovanni, COMANDE, "The Rotting Meat Error: from Galileo to Aristotle in Data Mining", European Data Protection Law Review (EDPL), C. 4, S. 3, Y. 2018, s. 273.

madenciliği faaliyetleri yürüttükleri görülmektedir⁴⁹. Youtube içerisinde yer alan videolar çoğunluğun doğrudan erişimine açık olduğu üzere kapalı devre kamera sistemlerinden elde edilen videolardan farklı bir alanda değerlendirilebilir. Bu sebeple tez konumuz ile doğrudan bağlantılı olmasa da bu internet sitesinde yer alan video kayıtları üzerinde yapılan veri madenciliği çalışmalarının da var olduğunu belirtmemiz gerekir. 2017 yılında gerçekleştirilen bir araştırmada ifade edildiği üzere “henüz Youtube’un zengin video veri seti üzerinde sistematik ve devamlı olarak tarama yaparak veri toplayacak ve işleyecek bir mekanizma” geliştirilememiştir⁵⁰.

Yukarıda da ifade ettiğimiz üzere gözetim toplumu içinde Devlet geniş ölçekli gözetim faaliyetleri gerçekleştirmektedir. Bu denklemin karşı tarafında yer alan gözetlenen bireyler ise aciz ve korunmaya muhtaç konumda yer almaktadırlar. İngiltere’de faaliyet gösteren bir aktivist grup “Surveillance Chess” adı verilen projeyi hayata geçirmiştir. Bu proje kapsamında birden fazla lokasyonda yer alan Closed Circuit Television (kapalı devre televizyon) sistemlerini hackleyerek, kameralar aracılığıyla gözetleyenlere; “Satranç oynayalım mı?” mesajı içeren görüntüler göstermişlerdir. Bu eylem CCTV’lerin gerektiğinde izleyenlere bir ilah gücü vermesine rağmen, çok kolay bir şekilde de ele geçirilip tanrı gücündekileri bir anda çaresiz bırakabilecek nitelikte aletler olduğunu bizlere göstermektedir⁵¹. Bu görüntüleri izleme fırsatına sahip olan bireyler bir anlık da olsa rollerin değiştiğini görebilmektedir. Böylelikle gözetlenen bireyin farkındalığı oluşmaktadır. Sürekli gözetim altında bulunanlar monitör odalarına girip, kendilerinin gözetleyenler karşısında ne kadar da aciz ve güçsüz görüldüğünü gördüklerinde de buna benzer bir algının oluştuğunu söylemek mümkündür⁵².

Kişisel veriler kilise kayıtlarından, yakınların hatıralarından ya da başka bir takım kurumların tozlu raflarında yer alan dosyalardan hızlı bir şekilde bilgisayar ortamlarına aktarılmaya başlanmıştır. Yine bu dönemde; hukukçuların, kamunun ve çeşitli düşünürlerin, yaygınlaşan bilgisayar kullanımının bireylerin özel yaşamı üzerinde yaratabileceği tehlikelerin

⁴⁹ Christopher SLOBOGIN, “Government Data Mining and the Fourth Amendment”, The University of Chicago Law Review, C. 75, S. 1, Y. 2007, s. 5.

⁵⁰ Zifeng, TIAN, “A Robust Framework for Mining You Tube Data” , Theses, Dissertations and Capstones, Marshall Digital Scholar, Marshall University, S. 1129, Y. 2017, s.5.

⁵¹ Surveillance Chess, <http://chess.bitnik.org/> (s.y. 10 Şubat 2022)

⁵² Smita KHERIA, D. Mac SITHIGH, Judith RAUHOFER, Schafer BURKHARD, “CCTV Sniffing”: Copyright and Data Protection Implications, S. 2013/2, CREATE Working Papers, Y. 2013, s.2.

üzerine eğildiğini görmekteyiz⁵³. Bu durum teknolojik gelişmelerin getirdiği bir zorunluluk olarak karşımıza çıkmaktadır.

Bu teknolojik gelişmeler ayrıca enformasyonun taşıyıcılardan bağımsız olarak dolaşımında olabildiği ve bireylerin fiziksel hareketlerinin bu bakımdan pek de önemli olmadığı yeni toplum düzenini beraberinde getirmiştir. Dijital dünyada bedenlerden ziyade bedenlerin üzerinden toplanan verilerin geçerliliği söz konusudur⁵⁴. Yaşadığımız toplumda bir verinin en kolay ve en ucuz şekilde işlenmesini sağlayan teknolojik araç hala bilgisayarlardır. “Veriler, yalnız sayıların ve isimlerin ötesinde DNA kodları, fotoğraflar ve ses kayıtlarına kadar uzansa da gözetlemenin gerçekleşebilmesini sağlayan teknolojiler bilgisayar gücü içerir⁵⁵”. Modern gözetlemenin gelişimini sağlayan teknoloji ve paralelinde gelişmekte olan bilgisayarlarla yapılan gözetim, modern yaşamın da olmazsa olmazıdır⁵⁶.

Eski çağlarda insanlara ait doğrudan bakışlar yoluyla yapılan gözetim, yeni yüzyılda makineler ve bilgisayarlar tarafından yapılmaktadır. Teknolojik gelişimin sebebiyet verdiği bu yeni gözetim, “bilgi, analiz, birleşim ve iletişim” gibi etmenlerin makineler aracılığıyla birbirlerine bağlanmasından ibarettir. Kredi kartı ya da telefon veri tabanları gibi özel sektöre ait veri tabanları da bireyler hakkında tümleşik profiller oluşturulmasını sağlamaktadır. Bu özel şirketler söz konusu profil oluşturma faaliyetlerini olumsuz anlamda, devlet tekeline bırakmamaktadır. Bu faaliyetlerin yürütülmesinde özel sektör ile kamu sektörünün omuz omuza çalıştığı görülmektedir. Dijital siciller ya da profiller üç tür bilgi akışı üzerinde oluşturulmaktadır⁵⁷. Bireylere ait veriler: 1) Özel sektör kuruluşları arasında 2) Kamu kurumu ile özel sektör kuruluşu arasında 3) Özel sektör kuruluşu ile kamu kurumu arasında aktarılmaktadır. Bireylere ait eğitim bilgileri, mali bilgiler, sağlık bilgileri, tüketim geçmişleri, davranış biçimleri, ikamet bilgileri gibi verilere bilgisayar sistemleri tarafından kolaylıkla ulaşılabilmektedir. Dolayısıyla elde edilen bu verilerin, görevleri birbirinden bağımsız ve yerleri birbirinden uzak kamusal ya da özel örgütler arasında paylaşımı kolaylaşmış olmaktadır⁵⁸.

⁵³ Elif KÜZECİ, Kişisel Verilerin Korunması, s.34.

⁵⁴ Zygmunt BAUMAN, Küreselleşme, Toplumsal Sonuçları, çev. Akın Emre Pilgir, Ayrıntı Yayınevi, İstanbul 2020, s. 28.

⁵⁵ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 35.

⁵⁶ David LYON, Gözetlenen Toplum, s .13.

⁵⁷ Daniel J. SOLOVE, s. 3.

⁵⁸ David LYON, Elektronik Göz, s .120.

Gözetimdeki gelişmenin önemli araçlarından bir diğeri internettir. Birbirinden farklı veri tabanları arasında uzaktan paylaşım, ilişkilendirme ve birleştirme olanağı sağlayan internet ve internetle bağlantılı diğerk teknolojilerin (world wide web, e-posta, sosyal medya ağları vb. gibi) kullanımının yaygınlaşması ile gözetimde yeni bir çağ başlamıştır. İnternetin birinci neslinden (Web 1.0) ikinci nesline (Web 2.0) geçişten sonra bugün üçüncü neslin (Web 3.0) gelmiş olduğu kabul edilmektedir⁵⁹. Anlamlı web dönemi olarak ifade edebileceğimiz bu sistemde internet içerisinde yer alan her bir bilgi anlamlandırılmaktadır. Nitekim bu yeni internet çağının iki temel unsuru bulunduğunu görmekteyiz. Bunlardan birincisi, bilgilerin insanlar ve bilgisayarlar tarafından anlaşılabilmesi için kaynakların anlamsal bakımdan etiketlenmesidir. İkinci unsurun ise bu kaynaklarla çalışabilen ve onlardan yeni bilgiler çıkarabilen akıllı servislerin geliştirilmesi olduğunu görmekteyiz⁶⁰.

Henüz kesin bir tanımı olmayan internetin dördüncü nesli (Web 4.0) fikri ise gelişmeye devam etmektedir. Belirttiğimiz üzere sınırları kesin şekilde belirlenmiş özelliklere ya da kesin bir tanıma sahip olmayan bu nesilde insan ve makinelerin simbiyotik (iki canlının tek bir organizma gibi hareket etmeleri suretiyle oluşturdukları ilişki olarak ifade edilse de taraflardan birinin yaşayan bir organizma olmadığı aşıkardır. Kanımızca bu terimle ifade edilmek istenen birlikte hareket etme kabiliyetidir.) bir ilişki dahilinde sisteme katılabilmeleri söz konusu olabilecektir⁶¹. Daha basit bir ifade ile makinelerin web içeriklerini okuyacak kadar akıllı hale, insan beynine eş değer seviyeye gelmeleri hedeflenmektedir. Bu kurgu çerçevesinde oluşturulmak istenen dördüncü nesil internet çok yüksek zeka seviyesindeki etkileşimlerden oluşan devasa bir ağı temsil edecektir.

İnternetin ilk versiyonundan günümüze kadar birçok değişim yaşandığını söylememiz mümkündür. Günümüzün internet ağı diğerk iletişim teknolojilerinin birçoğunun özelliğini doğrudan içerisinde bulundurmaktadır. İnternet üzerinden televizyon izlemek, gazete okumak, bir başkasıyla sesli ve görüntülü olarak konuşmak, geniş topluluklar ile bir araya gelerek toplantılar gerçekleştirmek, konferanslar ya da seminerler vermek mümkündür. Tüm bu faaliyetlerin aynı zamanda fiziksel anlamda bir araya gelmeye gerek kalmadan hallediliyor

⁵⁹ George, BOUCHAGIAR, "Privacy and Web 3.0: Implementing Trust and Learning from Social Networks", Review of European Studies, C. 10, S. 4, Y. 2018, s. 16.

⁶⁰ A.g.m. s. 17.

⁶¹ Sareh AGHAEI, International Journal of Web & Semantic Technology (IJWest), C. 3, S. 1, Y. 2012, <http://www.airccse.org/journal/ijwest/ijwest.html> (s.y. 10 Şubat 2022)

olması internetin kullanımını fazlasıyla arttırmıştır⁶². Bu artan sayı içerisinde çok geniş bir kitleye sahip sosyal medya platformu kullanıcıları da yer almaktadır.

Lessig’e göre, internet ortamında yaptığımız her şey aslında bir veri üretmektedir. Üretilen ya da bir internet gezintisi sırasında arkamızda bıraktığımız bu veriler ticari aktörler açısından kamusal aktörlere göre çok daha değerlidir⁶³. Bunun sebebi ise üretilen verinin niteliğidir. Şöyle ki; kamusal aktörlerden biri olan devlet, çoğu zaman sadece koyulan hukuk kurallarına uyulup uyulmadığını, özel sektör aktörleri ise internet kullanıcılarının gezinti sırasında bıraktığı tüketim alışkanlıklarını umursamaktadır. Özel sektör aktörleri için burada asıl hedeflenen, kullanıcının para harcamasının sağlanmasıdır. Bir kullanıcı bilgisayar başına geçip herhangi bir konu hakkında arama yaptığında, henüz kendisi bile farkına varmadan hakkındaki bilgileri dışarıya göndererek, verilerinin veri tabanlarında toplanmasına sebep olmaktadır.⁶⁴

İnternet ortamında verilerin elde edilmesi iki şekilde tezahür etmektedir. Bunlardan birincisi internet siteleri vasıtasıyla bir kişiye ait bilginin doğrudan ve açıkça kişinin kendisinden toplanmasıdır. Bir internet sitesine girişte, bu siteyi kullanabilmek için kayıt olunması ve bir takım bilgilerin verilmesi gerekiyorsa durum böyledir⁶⁵. Bunun dışındaki ikinci yol ise; kişiden bilginin gizlice edinilmesi durumudur. Yukarıdaki açıklanan birinci durumda, kişiden veri açıkça istenerek alınırken, ikinci durumda kullanıcının bilgisi ve onayı olmadan verisi gizlice alınmaktadır⁶⁶. İkinci durumun en bilindik örneği çerez dediğimiz tarayıcı durum bilgisi içeren dijital ufak ebatlı dosyaların kullanımınıdır⁶⁷.

⁶² “Global digital population as of January 2021”, Statista, <https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20January%202021%20there,the%20internet%20via%20m> (s.y. 12 Şubat 2022). Bu demografik çalışmaya göre, Ocak 2021 tarihi itibarıyla dünya çapında 4.66 milyar aktif internet kullanıcısı bulunmaktadır. Yine aynı çalışmada ifade edilen sonuca göre, yaklaşık 4.2 milyar sosyal medya kullanıcısı bulunur. Önceki 10 yılın başı olan 2010 yılı sonunda bu rakamın 2 milyar kişinin biraz üzerinde olduğu tespit edilmiştir. (Ayrıntılı bilgi için bkz. <https://www.itu.int/net/itunews/issues/2010/10/04.aspx> (s.y. 12 Şubat 2022)). Bu durum internet erişiminin son on yıl içerisinde iki kat arttığını göstermektedir. Dikkat çekici önemli bir diğer nokta ise genel erişim içerisinde sosyal medya kullanımının büyüklüğü hakkında bizlere önemli bir bilgi vermesidir.

⁶³ Lawrence LESSIG, Code Version: 2.0, Basic Books, New York 2006, s. 216.

⁶⁴ Harry, HENDERSON, s.4

⁶⁵ Daniel J. SOLOVE, s. 23.

⁶⁶ Elif KÜZECİ, Kişisel Verilerin Korunması, s 37.

⁶⁷ Eva Rose RAHİM, “Information Security In The Internet Age”, İsmail NORISWADI, Edwin Lee YONG CIEH (Ed.), Beyond Data Protection, Strategic Case Studies and Practical Guidance, Springer Books, Y. 2013, s. 176.

Çerez (cookie) ”kullanıcının ziyaret ettiği web siteleri tarafından oluşturulan ve Üstün Metin Transfer Protokolü (Hyper Text Transfer Protocol – HTTP) kapsamında aktarımı gerçekleşen küçük dosyalardır⁶⁸”. Bu dosyalar, bir kullanıcının herhangi bir web sitesinde gezinirken web sunucusu tarafından oluşturularak, kullanıcının web tarayıcısı tarafından bilgisayarına yerleştirilen küçük veri bloklarıdır. Çerezler kullanıcının gezindiği internet sayfaları hakkında bilgi sahibi olma fırsatı sunarak bireylerin davranışları ve hareketleri hakkında bilgi sunar ve birey hakkında profil oluşturulmasını sağlayabilir⁶⁹.

Çerez kullanımı dışında mevcut internet ağı içerisinde kullanılan birçok yeni teknolojik gelişme bulunmaktadır. Örneğin bunlardan biri internet üzerinden kullanılan makine çevirisinin (machine translation) kullanımıdır. Metinlerin kaynak dillerinden hedeflenen başka bir dile otomatik olarak çevrilmesini ifade eden dil işleme etkinliği olarak tanımlanan bu etkinlikler, çevirilerin anlam ve bağlam açısından gereken yeterliliği sağlaması için tasarlanan yapay zeka araştırmalarından da yararlanmıştır⁷⁰. Günümüzde, Google ve Microsoft başta olmak üzere birçok özel şirket internet ağı üzerinden bu hizmeti kullanıcılarına ücretsiz bir şekilde sağlamaktadır.

İnternetin gelişimi yukarıda da değindiğimiz üzere; sosyal medya platformlarının hem sayılarını artırmış hem de bunlarla doğru orantılı olarak kullanıcı sayılarını yükseltmiştir⁷¹. Bazı kullanıcıların bu platformlara bilgisayarlar üzerinden ya da çoğunlukla mobil cihazlarından günde 10 defadan fazla girdikleri görülmektedir. Bazı araştırmacılara göre, bu durum bireyin kendi bilgisini paylaşmasına dair aldığı güçlü hazzın sağladığı motivasyondan kaynaklanmaktadır⁷². Bireyler adeta bu güçlü haz karşısında mahremiyetini korumak yerine toplum tarafından tanınır olmayı seçmektedir. Sosyal medya dahil tüm internet platformunun kullanımının bu kadar artmış olması, yukarıda açıkladığımız şekilde internet üzerinden yapılan gözetimin de doğru orantılı bir şekilde artmasına sebep olduğundan ayrı bir önem arz etmektedir.

⁶⁸ Hüseyin Can AKSOY, Mesut HALICIOĞLU, AB ve Türk Hukukunda Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme, Kişisel Verileri Koruma Dergisi, C.3, S.1, Y. 2021. s.63.

⁶⁹ A.g.m. s. 61-88.

⁷⁰ Elif KÜZECİ, Sayısal Fil, Bilişim Teknolojileri, Devlet ve Hukuk Kesişiminde Bir İnceleme, İnkılap Kitabevi, İstanbul 2021, s. 110.

⁷¹ Bkz. yuk. d.n. 69, s. 25.

⁷² George, BOUCHAGIAR, s. 23.

Yukarıda değindiğimiz Web 3.0 aynı zamanda Metaverse bakımından da önemlidir. Bu iki sistemin arasındaki bağlantıyı Metaverse ve Web 3.0 stratejisti Cathy Hackl'in şu açıklaması ile anlamak daha kolay olabilir. Hack'e göre, "Web 1.0 kullanıcılarının internet aracılığıyla bilgiye ulaşmış, Web 2.0 sosyal medya aracılığıyla insanları bir araya getirmiştir. Web 3.0 ile birlikte Metaverse ise insanları, yeri ve diğer şeyleri bir araya getirmektedir"⁷³. Bu bağlamda; 2021 yılının sonlarına doğru ilan edilen Metaverse'in ne olduğunu açıklamak yerinde olacaktır.

Siber alan denilen internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler dahil olmak üzere, bağımsız bilgi teknolojisi altyapıları ve yerleşik veriler ağından oluşan bilgi ortamının bulunduğu küresel etki alanı aynı şekilde Metaverse için de geçerliliğini korumaktadır⁷⁴. Metaverse bu alanda bulunan teknoloji ile nasıl iletişime geçeceğimiz ile ilişkilidir⁷⁵. Bu teknolojinin tanıtım sürecinde de çoğunlukla gösterildiği üzere, Metaverse içerisinde bahsedilen iletişimin çoğunlukla sanal gerçeklik⁷⁶ üzerinden sağlanacağı söylenebilecektir. Ancak bu dijital evrenin içine girebilmek için sanal gerçeklik ya da artırılmış gerçeklik cihazlarına ihtiyaç bulunması gibi bir zorunluluk bulunmaz. Bireyler doğrudan bilgisayarları ve mobil cihazları aracılığıyla da bu evrene dahil olabileceklerdir.

Her gelişen teknolojinin beraberinde bir takım problemleri de getirmesi doğaldır. Bu evrende işlenen suçların nasıl nitelendirileceği ya da hukuki yaptırım sonucuna bağlanıp bağlanmayacağı önemli bir sorun olarak karşımıza çıkabilir. Filozof Morgan Luck 2009 tarihli bir makalesinde bu konuyu oyuncunun yaşadığı ikilem olarak nitelendirmiştir. Yani sanal gerçeklikte yaşanan bir ölümün, bir satranç oyununda bir piyonun alınmasından pek de farklı

⁷³ Into The Metaverse, Powering the development of the future internet 3.0: themetaverse, <https://www.wired.com/sponsored/story/into-the-metaverse/> (s.y: 14 Şubat 2022)

⁷⁴ Marco MAYER, Niccolo de SCALZI, Luigi MARTINO, Iacopo CHIARUGI, International Politics in the Digital Age: Power Diffusion or Power Concentration?, XXVIIth SISP CONFERENCE, University of Florence, 12-14 Eylül 2013, s. 8.

⁷⁵ Eric RAVENSCRAFT, What Is the Metaverse, Exactly?, <https://www.wired.com/story/what-is-themetaverse/> (s.y. 04 Şubat 2022)

⁷⁶ "Virtual Reality" (VR) kavramı aslında "bir bilgisayar tarafından üretilen, gerçek bir yeri veya durumu temsil ediyor gibi görünen bir dizi görüntü ve ses bütünü" olarak tanımlanmıştır. Bkz. <https://dictionary.cambridge.org/tr/s/ingilizce/virtual-reality> (s.y: 13 Şubat 2022). Bununla birlikte yapay gerçekliğin duyuşal deneyim açısından bir gün sınırsız bir etkiye sahip olan son platform ("final platform") olduğu ifade edilmiştir. Bkz. Lisa MESSERI, The Man, the Myth, and the Metaverse, <https://www.wired.com/story/theman-the-myth-and-the-metaverse/> (s.y. 14 Şubat 2022). Ayrıca metaverse içerisinde kullanılan teknolojik iletişim yöntemlerinden bir diğeri ise artırılmış gerçeklik (augmented reality ya da AR) teknolojisidir. Artırılmış gerçeklik, gerçek dünyada bulunan nesnelerin bilgisayar tarafından oluşturulan farklı duyuşal bilgiler (görsel, işitsel, dokunsal, koku alma) dahilinde gerçek dünya gerçekliği benzeri etkileşim sağlayan bir deneyimdir. Patrick SCHUEFFEL, The Concise Fintech Compendium, Friborg: School of Management Fribourg 2017, https://www.researchgate.net/publication/322819310_The_Concise_Fintech_Compendium (s.y. 13 Şubat 2022)

bir durum yaratmadığı söylenebilir. Keza bir çok oyunda öldürmek fiili ödüllendirilmekte ve hatta oyuncular bundan zevk duymaktadırlar⁷⁷. 1982 yılında bir atari oyunu olarak piyasaya çıkan Custer's Revenge adlı oyun içerisinde bir görev Amerikan yerlisi bir kadının cinsel tacizini emretmekteydi. Bu görev sanal dünya da bile bir çok kişi tarafından ahlaki yönden sorunlu görülmüştür⁷⁸. 2012 yılında Hollanda Yüksek Mahkemesi tarafından verilen bir kararda iki genç bir başka gence ait sanal tılsımı çaldıkları gerekçesiyle cezalandırılmışlardır. Mahkemenin buradaki gerekçesi Runescape adlı bu oyundaki sanal tılsımın elde edilmesi için harcanan zaman ve çaba nedeniyle gerçek bir değere haiz olmasıdır⁷⁹. Bu gibi durumların Metaverse içerisinde yaşanacağı düşünüldüğünde, çare olarak bu fiilleri gerçekleştirilenlerin sanal evrenden yasaklanması ya da bu fiilleri gerçekleştirenlere para cezası müeyyidesi getirilmesi düşünülebilir. Metaverse evreninin bu gibi sorunları beraberinde getirdiği açıktır. Sistemin kullanımının artmasına bağlı olarak insanların sürekli olarak bu sanal evrende geçirecekleri zamanın fazlalığı öngörüldüğünde kendilerinden toplanan verilerin miktarının da artacağı aşıkardır. Nitekim gözetim faaliyetlerinin gerçekleştirilebileceği yeni bir evren yaratılmış olmaktadır.

İnternetin gelişiminin gözetim teknikleri açısından önemli olduğuna yukarıda değinmiştik. Günümüz teknolojilerinden biri olan blokzinciri teknolojisi niteliği gereği kamuya açık veri tabanları (*DLT ya da Digital Ledger of Transactions*) üzerinden faaliyetlerine devam etmekte ve bireyin tüm işlemleri takip edilebilmektedir. Özellikle Covid-19 pandemi sürecinde evlere kapanılan dönemde gelişimi büyük bir ivme kazanan kripto para evrenine ve arkasındaki devasa blokzinciri (blockchain) teknolojilerine de değinmemiz de yerinde olacaktır.

Pandeminin ilk günlerinde yaklaşık olarak 7.300 \$ üzerinden fiyatlanan Bitcoin, bir yıl sonunda yüzde 640 oranında değerini artırırken bu kripto para biriminin maliyeti 46.800 \$ olmuştur⁸⁰. Peki pandemi süreci ile bu yükseliş arasında doğrudan bir ilişki var mıdır? Bu

⁷⁷ Morgan LUCK, "The Gamer's dilemma: An analysis of the arguments fort he moral distinction between virtual murder and virtual paedophilia", Ethics and Information Technology, S.11, Y. 2009, s. 34.

⁷⁸ David CHALMERS, What Should Be Considered a Crime in the Metaverse, <https://www.wired.com/story/crime-metaverse-virtual-reality/> (s.y. 14 Şubat 2022)

⁷⁹ Arno R. LODDER, "Dutch Supreme Court 2012: Virtual Theft Ruling a One-Off or First in a Series?", Journal of Virtual Worlds Research, C. 6, S. 3, Y. 2013, s. 1-12.

⁸⁰ Diğer kripto para birimlerine göre pazarda işlem hacmi daha yüksek olan Bitcoin (Bkz. <https://coinmarketcap.com/>, (s.y. 14 Şubat 2022)) tüm zamanların en yüksek değeri olan 61.374,28 \$'a 2021 yılının Ekim ayında ulaşmıştır. [https://www.statista.com/statistics/326707/bitcoinpriceindex/#:%0B~:text=Bitcoin%20BTC%2FUSD%20price%20history%20up%20until%20February%2017%2C%202022&text=i%20coin%20\(BTC\)%20price%20again%20reached,Apri%202021%20and%20November%202021](https://www.statista.com/statistics/326707/bitcoinpriceindex/#:%0B~:text=Bitcoin%20BTC%2FUSD%20price%20history%20up%20until%20February%2017%2C%202022&text=i%20coin%20(BTC)%20price%20again%20reached,Apri%202021%20and%20November%202021) (s.y. 14 Şubat 2022)

soruya olumlu cevap vermemiz mümkündür. Nitekim kripto para birimlerinin dünyanın herhangi bir yerinden alınıp satılabilmesi, salgına bağlı kapanmalarda hareket kabiliyetleri kısıtlı olan bireylerin yatırım taleplerini bu para birimlerine yönlendirmelerine sebep olmuştur.. Yükselen talepler ise eş zamanlı olarak maliyetlerin artmasına sebebiyet vermiştir. Ayrıca yatırımcıların merkez bankalarının ya da siyasi karar alıcıların pandemi sürecinde pazara müdahalesinden korkmaları da bu merkeziyetsiz para birimlerine olan yönelimi pekiştirmiştir⁸¹.

Buna karşılık diğer bir yönden ise kripto para birimlerinin yasal olmayan aktivitelerin finansmanında kullanılıyor olması gibi olumsuz iddialar da bulunmaktadır. Hatta bazı ülkelerin bu konuda yasaklamalar getirmiş olduğu da görülmektedir⁸². Bir araştırmaya göre hukuka aykırı sayılan bu işlemlerin hacminin, toplam piyasadaki işlem hacminin yaklaşık olarak yüzde 3'üne tekabül ettiği ortaya koyularak, bunun dışındaki işlemlerin doğrudan kripto para birimi borsaları arasında yapıldığı ifade edilmiştir⁸³. Tüm bu açıklamalar ışığında küçük ölçekli sayılabilecek yasa dışı faaliyetler sebebiyle bu denli gelişmekte olan, merkeziyetsiz ve şeffaf bir ekonomi ekosisteminin ve arkasındaki blokzinciri teknolojisinin eldeki veriler göz önüne alındığında yasaklanması için yeterli olmadığını söyleyebiliriz. Nitekim yukarıda bahsi geçen çalışmada da ortaya konulduğu üzere, bu ekosistemin bir bütün olarak yasa dışı faaliyetlerin destekleyicisi olduğu ve tamamen bu amaca hizmet ettiği gibi bir anlam çıkmamaktadır.

Yükselen kripto para trendi dışında dikkat çekici olan bir diğer husus ise bu finansal enstrümanların arkasındaki teknoloji olan blokzinciri teknolojisidir. Blokzinciri kavramı temel olarak işlemlerin kaydedildiği ve paylaşıldığı bir kayıt veri tabanını ifade etmektedir. Bu sistemde işlemlerin kayıtlarını tutan blokların kronolojik olarak ve sıralı şekilde bir zincire doğrusal olarak bağlanması söz konusudur. Blok zinciri ekosistemi içerisinde merkezi olmayan eşler arası (peer to peer) bir ağ bulunmakta olup, bu ağ içerisindeki düğümlerin eşleşmek üzere

⁸¹ Hadar Y. JABOTİNSKY, Roe SAREL, "How the Covid-19 Pandemic Affected the Cryptocurrency", Columbia Law School's Blog on Corporations and The Capital Markets, Marc 2021, <https://clsbluesky.law.columbia.edu/2021/03/26/how-the-covid-19-pandemic-affected-the-cryptocurrencymarket/> (s.y. 19 Şubat 2022)

⁸² Çin, Katar, Mısır, Irak vb. gibi bir takım ülkeler kripto para birimi kullanımını yasaklamışlardır. Bkz. Marco QUIROZ-GUTIERREZ, "Crypto is fully banned in China and 8 other countries", <https://fortune.com/2022/01/04/crypto-banned-china-other-countries/> (s.y. 19 Şubat 2022)

⁸³ Betsy VERECKEY, "Bitcoin: Who owns it, who mines it, who's breaking the law", MIT Management Sloan School, <https://mitsloan.mit.edu/ideas-made-to-matter/bitcoin-who-owns-it-who-mines-it-whos-breaking-law> (s.y. 19 Şubat 2022)

birlikte çalışması sağlanmaktadır⁸⁴. Düğümler arasında bir eşlenme sağlandığı anda doğruluğu kesinleşen işlem kamuya açık bir veri tabanına kayıtlanmaktadır. Böylelikle burada bahsedilen eşlenme (consensus) özelliği blokzinciri üzerindeki işlemlerin katılımcıların çoğunluğu tarafından doğrulanabilir olmasını sağlamaktadır. Böylelikle sistemin şeffaflığı sağlanmış olur⁸⁵. Ayrıca kripto para ekosisteminde, blokzincir alt yapısını kullanmayan kripto para birimlerinin de olduğunu söylemek mümkündür⁸⁶.

Bu teknolojinin kripto para ekosisteminde kullanımının dışında, farklı kullanım alanları bulunmaktadır. Örnek vermemiz gerekirse siber güvenlik çözümlerinin geliştirilmesinde, bulut tabanlı hizmetlerin sunulmasında, akıllı sözleşmelerin kurulmasında⁸⁷, akıllı şehirlerin dizayn edilmesinde ve yönetilmesinde (akıllı sağlık uygulamaları, yönetim gereksinimlerinin tespitinde analiz amaçlı, akıllı araçlar ve ulaşım sistemlerinin işletilmesinde vb.) bu teknolojilerden yararlanılmaktadır⁸⁸. Aynı zamanda, bazı bankaların yüksek hızlı, düşük maliyetli ve kripto para birimlerindeki çift harcama problemlerini ortadan kaldıran dijital dönüşüm uygulamalarını blokzinciri teknolojisi dahilinde geliştirmeye çalıştıkları uygulamalarla çözmeye çalıştıkları görülmektedir⁸⁹.

Bazı ülkeler gelişen teknolojiyi değerlendirerek para basma ve yönetme yetkilerini kullanmak suretiyle kendi dijital para birimlerini oluşturup gelişen kripto para birimi pazarına yönelen sermayeye alternatif yaratmaya çalışmaktadırlar⁹⁰. Bu ülkelerin merkez bankalarının

⁸⁴ Yun Joo AN, Paul Moon Sub CHOI, Seth H. HUANG, "Blockchain, Cryptocurrency, and Artificial Intelligence in Finance", P. M. S. CHOI, S. H. HUANG (Ed.), Fintech with Artificial Intelligence, Big Data, and Blockchain, Springer, 2021, s. 4.

⁸⁵ A.g.m. s. 4.

⁸⁶ Örneğin; IOTA adı verilen ve nesnelerin interneti teknolojisine entegre olarak çalışan kripto para biriminin kullandığı altyapı (Tangle) blokzinciri teknolojisinden belirli yönler açısından farklıdır. Bu farklılığın temel sebebi nesnelerin interneti teknolojisinin kullanılmasına bağlı olarak işlem maliyetlerinin kesinlikle sıfıra indirgenmesinin zorunlu görülmesidir. Blokzinciri teknolojisinde bu tarz işlem maliyeti (Bitcoin ya da Ethereum'da) öngörülürken, Tangle sisteminde bu yönde bir işlem maliyeti bulunmamaktadır. Blokzincirinin bu özelliğini gören Tangle geliştiricileri nesnelerin interneti teknolojisine tam olarak bağlı bir dünyada milyarlarca IOT cihazı ve verileri ancak yerleşik altyapının işlemleri ücretsiz yapması koşuluyla işlevsel olabileceğini düşünerek bu yeni sistemi hayata geçirmişlerdir. Serguei POPOV, "IOTA; Feeless and Free", IEEE Blockchain Technical Briefs, January 2019, <https://blockchain.ieee.org/technicalbriefs/january-2019/iota-feeless-and-free> (s.y. 20 Şubat 2022)

⁸⁷ Gurinder SINGH, Vikas GARG, Pooja TIWARI, "Introduction to Blockchain Technology", R. AGRAWAL, N. GUPTA (Ed.), Transforming Cybersecurity Solutions Using Blockchain, Springer, 2021, s. 5 v.d.

⁸⁸ Rayan M. NOUH, Dhananjay SINGH, "Introducing Blockchain for Smart City Technologies and Applications", Dhananjay SINGH, Navin Singh RAJPUT (Ed.), Blockchain Technology for Smart Cities, Springer, 2020, s. 4. v.d.

⁸⁹ Lissa L. BROOME, "Banking on Blockchain." North Carolina Journal of Law & Technology, C. 21, S. 1, Y. 2019, s. 178.

⁹⁰ Marcelo M. PRATES, "Money in the Twenty-First Century: From Rusty Coins to Digital Currencies.", Ohio State Business Law Journal, C. 15, S. 1, Y. 2021, s. 222.

Uluslararası Ödemeler Bankası (Bank for International Settlements) öncülüğünde gerçekleştirdikleri çalışmaya ait rapora göre, kripto para birimlerinde olduğunun aksine merkez bankalarına ait dijital para birimleri merkeziyetsiz bir yapıya sahip değildir. Bu para birimlerinin merkez bankaları tarafından kontrol ediliyor olması ya da rezerv karşılıklarının bulunması gibi unsurlar halkın paraya olan güvenini artırarak finansal istikrarı sağlayacaktır⁹¹. Bu özelliği ile merkez bankalarına ait dijital paralar, kripto para birimlerinden ayrılmaktadır. Merkez Bankaları Dijital Para Birimi (CBDC) bir kripto para sisteminde olduğu gibi blokzinciri alt yapısını kullanmaktadır⁹². Netice itibariyle istisnai olarak oluşturulan prototipler ya da Bahamalar gibi nispeten küçük ekonomiler dışında büyük ölçekli bir ekonomik düzlem içerisinde kullanılan ilk CBDC, Çin hükümeti tarafından çıkarılan Dijital Yuan olmuştur⁹³. Kanımızca CBDC’lerin kripto paraların yerini alması çok kolay görünmemektedir. Bilhassa kripto para birimlerinin arzının sınırlı olması, merkeziyetsiz yapıya sahip olmaları, bu para birimleri üzerinde doğrudan devlet kontrolünün olmaması (hükümetlerin kripto para birimlerini doğrudan takip ve kontrol yetkisi olmasa da alım-satım işlemlerinde vergilendirmeyi düzenlemesi ya da borsalara ilişkin düzenlemeler getirmesi söz konusu olabilecektir) gibi nedenlerle kripto para birimlerinin CBDC’lere göre daha fazla talep edilen tarafta yer alacağı söylenebilir.

Hem genel anlamda blokzinciri teknolojisinin hem de kripto para birimleri hareketlerinin tamamen kamuya açık olmalarının sonucu bir anlamda şeffaflılığı sağlarken diğer yönden de bireyin bu ekosistem içerisindeki hareketlerinin tamamının takip edilebilirliğini beraberinde getirmektedir. Bu sistem içerisinde mahremiyetin korunması

⁹¹ Raporun oluşturulmasına katkıda bulunan merkez bankaları arasında Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England ve Board of Governors Federal Reserve System ve Bank for International Settlements bulunmaktadır. Bkz. Central bank digital currencies: executive summary, September 2021, <https://www.bis.org/publ/othp42.pdf> (s.y: 19 Şubat 2022)

⁹² Diğer özellikleri bakımından bu dijital paralar: 1) Ön ödemeli banka kartlarında saklanan banka mevduatlarından farklı olarak merkez bankası ile para kullanıcısı arasındaki bir aracının bulunmadığı, doğrudan bu parayı ihraç eden merkez bankasının sorumluluğunda olan, 2) Bankaların merkez bankasında tuttukları elektronik rezervlerden farklı olarak sadece seçilmiş kişilerin ya da kurumların değil herhangi bir kişinin ya da kuruluşun kullanımına açık olan, 3) Nakit paradan farklı olarak fiziksel bir formda bulunmayan bunun yerine elektronik şekilde var olan paralardır. Bkz. Marcelo M. PRATES, s. 223.

⁹³ James T. AREDDY, China Creates Its Own Digital Currency, a First for Major Economy, <https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy11617634118> (s.y. 19 Şubat 2022) Türkiye’nin ise Merkez Bankası’nın Dijital Türk Lirası geliştirme çalışmalarını Aselsan, Havelsan ve Tübitak-Bilgem ile ikili mutabakat zaatları imzalamak ve “Dijital Türk Lirası İşbirliği Platformu” oluşturarak bu örnekler arasına girdiği görülmektedir. Merkez Bankası’nın projenin birinci faz sonuçlarını ilgili testlerin tamamlanması sonrasında 2022 yılında açıklayacağı kamuya duyurulmuştur. Bkz. Türkiye Cumhuriyeti Merkez Bankası, “Merkez Bankası Dijital Türk Lirası Ar-Ge Projesi Hakkında Basın Duyurusu”, S. 2021-40, 15/09/2021, <https://www.tcmb.gov.tr/wps/wcm/connect/7afe5eab-0a8f-4a85-9e2790f2d41f225f/DUY2021-40.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-7afe5eab-0a8f-4a85-9e27-90f2d41f225f-nLF8y.z> (s.y: 19 Şubat 2022)

oldukça önemlidir. Örneğin; Bitcoin ile maaş alınan bir senaryo içerisinde bitcoin ile kira ödemesi ya da herhangi bir alışveriş yapılırsa hem ev sahibi hem de ödeme alan üçüncü kişi tarafından kiracı ya da tüketicinin ne kadar maaş aldığı bilgisine erişebilecektir. Buradaki kripto para biriminin miktar ve kimden kime iletildiğine dair bağlantı bilgisi Bitcoin'in çalışması için gerekli olduğu için herkesin erişimindedir. Bu nedenle özellikle finansal gizlilik ve kişisel verilerin korunmasına yönelik olarak bir takım adımların atıldığını görmekteyiz⁹⁴.

Daha önce yapay zekanın kapalı devre kamera sistemlerinde kullanıldığını belirtmiştik. Hatta bu teknolojinin insan hayatını kolaylaştırıcı olumlu etkilerine de kısaca değinmiştik. Ancak bu değerlendirmenin dışında yapay zeka ve robotik alanındaki gelişmelerin istihdam ve çalışan maaşları üzerindeki olumsuz etkilerini ortaya koyan çalışmaların da olduğunu ifade etmemiz gerekir⁹⁵.

Akademik çevrenin, özel teşebbüslerin ya da kamu kurumlarının bu teknolojiye yönelik artan ilgilerine rağmen yapay zekanın genel geçer, standart bir tanımı bulunmamaktadır. Yapay zekanın, insan zekasından yola çıkarak tanımlanmaya çalışıldığı görülmektedir. Bu bakımdan yapılan birçok tanımın insan gibi davranan veya zeka gerektiren eylemleri gerçekleştirebilen makinelerle atıfta bulunduğunu görebiliriz⁹⁶. Yıllar içerisinde bu tanımın standart hale getirilmesine dair yapılan çalışmalar sonucunda Avrupa Komisyonu tarafından Yapay Zeka Stratejilerinin belirlenmesi hususunda görevlendirilen Yüksek Deneyim Grubu⁹⁷ (HLEG ya da “ High-Level Expert Group”) 2019 yılında yapay zeka için bir tanımlamada bulunmuştur. Bu bakımdan yapay zeka sistemleri kendilerine verilen karmaşık hedefler için gerçekleştirilebilecek en iyi eyleme karar vermek amacıyla, çevreden toplanan verileri

⁹⁴ Kripto para kullanımının yarattığı bu çekincelerin giderilmesi için yaratılan çözümlerden bir tanesi Liquid Network adı verilen bir yan zincirdir. Bkz. Faruk TERZİOĞLU, Bitcoin'de Mahremiyet, 26.09.2019, <https://blokzincir.bilgem.tubitak.gov.tr/bzcalistay/bzcalistay2/documents/sunum/Faruk%20Terzio%C4%9Flu.pdf> (s.y: 20 Şubat 2022). Çünkü kaydedilen her işlemde göndericinin ve alıcının adresleri bulunduğundan , işlemler, kullanıcının hesap bakiyesi, işlem türü ve sıklığı gibi detaylar bu adresleri bilen herkes tarafından serbestçe izlenebilir. Bkz. Blokzincirlerde Güvenlik ve Mahremiyet Raporu, Tübitak Bilgem Blokzinciri Araştırma Laboratuvarı, Nisan 2020, s. 20.

⁹⁵ Elif KÜZECİ, Sayısal Fil, s. 132; Daron ACEMOĞLU, Pascual RESTREPO, “ Robots and Jobs : Evidence From US Labor Markets”, Journal of Political Economy, C. 128, S. 6, 2020, <https://economics.mit.edu/files/19696> (s.y: 20 Şubat 2022)

⁹⁶ Sofia SAMOILI, Montserrat LOPEZ-COBO, Emilia GOMEZ, Giuditta De PRATO, Fernando MARTINEZ-PLUMED, Blagoj DELIPETREV, “AI Watch Defining Artificial Intelligence, Towards an operational definition and taxonomy of artificial intelligence”, Publications Office of the European Union, Luxembourg Y. 2020, s.7.

⁹⁷ Bu grubun yapay zekaya ilişkin uygulamaları etik, hukuki ve sosyal açılardan değerlendirdiği ve ileriye ilişkin gelişen teknolojilere dair önerilerde bulunduğu çalışmaları olmakla birlikte, ekip akademik çevrelerden katılanlar da dahil 52 farklı temsilciden oluşmaktadır. Bkz. a.g.e., s. 8.

yorumlamak, akıl yürütmek veya bu verileri işlemek suretiyle fiziksel ya da dijital boyutta hareket eden ve insanlar tarafından tasarlanmış yazılım ya da donanım sistemleridir⁹⁸. Kapalı devre kamera sistemlerinde yapay zekanın kullanılmasının örneklerini anlık yüz tanımlama sistemlerinde, polis vücut kameralarında ya da insan hareketlerini algılayan ve kayda geçen özel tekniklerin bulunduğu diğer kapalı devre kamera sistemlerinde görebilmekteyiz. İlerideki bölümlerde bu işleyişin nasıl olduğu ve bu iç içe geçmiş kullanımlar sırasında mahremiyetin korunması açısından nelere dikkat edilmesi gerektiğini ayrıca açıklayacağız.

Yukarıda farklı konular üzerinden açıklanan teknolojik gelişmeler, gözetim etkinliklerinde farklı araçların kullanılmasını da beraberinde getirmiştir. Gözetim araçlarının sürekli ve hızlı bir şekilde değişmesi nedenleriyle bazı yazarlar “kişisel bilgi gizliliğinin günümüzde tanınımının yapılamayacağı” anlamına geldiğinden bahsederler. Tansuğ, “Eskiden özel yaşamının gizliliğini –ev, beden, haberleşme, onur...- ihlal eden eylemleri tanımlamak kolayken, bilgi çağında, “kişisel bilgilerin gizliliğini ihlal eden”leri tanımlamak çok zor bir hale gelmiştir. Çünkü hızla gelişen teknoloji, her geçen gün yeni bir araç sunuyor...” derken, aslında bir gerçeği çarpıcı şekilde gözler önüne sermektedir⁹⁹.

1940’lı yıllardan bu yana kullanılan kapalı devre kamera sistemi teknolojileri günlük hayatın izlenmesi ve kaydedilmesi amacıyla kullanılan sistemlerdir¹⁰⁰. Özellikle şehirlerde bu sistemlerden kaçınabilme olanağı neredeyse hiç bulunmamaktadır. Günümüz toplumlarında cadde ve mağazalarda sürekli olarak görmeye alıştığımız “kesintisiz video gözetlemesi” uyarılarını, otoyollardaki hız kontrol kameralarını ve benzeri sistemleri düşündüğümüzde, gözetlemenin daha geniş alanlara yayıldığını, merkezden bağımsızlaştırıldığını ve şehrin ayrılmaz bir parçası haline geldiğini görmekteyiz. Şehir yaşamının bu ayrılmaz ögesi hemen hemen tüm kamusal alanlar dahil çeşitli bölgelerin ve mekanların gözetlenmesinde kullanılarak günümüz modern gözetim anlayışının en göze çarpan uygulaması haline gelmiştir. Bu teknolojiyi sadece kamu alanlarını gözetleyen ve verileri kaydeden bir sistem olarak değil, “gözetlenenlerin bulunduğu tüm alanları ve edimselleştirdiği tüm davranışları bir araya getirerek haritalayan bir montaj-teknik olarak düşünmek” mümkündür¹⁰¹.

⁹⁸ A.g.e., s. 18.

⁹⁹ Avniye TANSUĞ, “AB’ nin Yeni Ekonomik Silahı: “ Veri Saklama Hukuku”, Bilişim Hukuku, Der. Mete Tevetoğlu, Kadir Has Üniversitesi Yayınları, İstanbul 2006, s. 536.

¹⁰⁰ Clive NORRIS, Mike MCCAHL, David WOOD, “The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space”, Surveillance&Society, C.2, S.2/3, Y. 2004, s. 118.

¹⁰¹ Efe BAŞTÜRK, s. 277.

Şehirleri birer kamusal düzen ve güvenlik mekanı olarak tasavvur edip, onları bu özellikleri nedeniyle görünür kılmak çağımıza özgü bir durum değildir. Yunan düşüncesinde düzenli şehir, karmaşayı dışarıda tutmanın bir yolu olarak betimlenmiştir. Aristo ve Platon “şehirlerin desenleri ve alansal düzenlemeleri, toplumun nasıl olması gerektiğinin aynadaki yansımasıdır” söyleminde bulunarak tam olarak şehirlerin düzenliliğine dikkat çekmektedirler. 17. Yüzyılda Paris’te polis teğmeni La Reynie, şehirde yaşayanların şehirden dışarı çıkmaları durumunda güvenliklerini sağlamak amacıyla 6500 adet fener kurdurtmuş ve bu sayede Paris bir ılık şehri haline gelmiştir¹⁰².

Castells’e göre ise içinde yaşadığımız şehir, her ne kadar bir yer vasfında olsa da aynı zamanda bir süreci de ifade etmektedir¹⁰³. Ona göre günümüz kentleri; “bilgi şehirleri” başka bir ifadeyle gözetleme şehirleridir. Bu bakımdan görüntülemenin süreklileştirilmesi ve görünür olan her şeyin veri olarak kaydedilmesi söz konusudur¹⁰⁴.

Teknolojinin yukarıda da aktardığımız büyük ölçüdeki gelişiminden önce şehirde gözetleme demek, sokak ışıkları ve fiziksel mimari aracılığıyla nöbet tutmak ve çarpıklıkları önlemek demek iken gelişmiş şehirde ise bu kavram, bütün bireyler hakkında kamera görüntüleri de kullanarak elektronik etiketler tutmak anlamına gelmektedir¹⁰⁵. Örneğin, 1999 yılında Londra’nın Newham bölgesinde görüntüsüne giren yüzleri aktif olarak tarayan Mandrake adlı yüz tanıma sistemi faaliyete geçirilmiştir. Bu sistem günde 24 saat faaliyette olup, 140 adet sabit ve 11 adet mobil kamera aracılığıyla entegre olduğu dijital veri bankası görüntülerini karşılaştırmış ve yaklaşık 600-1000 aralığında suçlunun yüz tespitini gerçekleştirmiştir¹⁰⁶. Sistemin ortaya çıkışındaki temel amaç bölgede gerçekleşen ırkçı saldırıların faillerinin tespitinin sağlanmasıdır¹⁰⁷. Netice itibariyle Mandrake’nin doğuş amacına başarılı olarak hizmet ettiği söylenebilir.

Teknoloji sadece yeni gözetim araçlarının icat edilerek kişisel verilerin bunlar tarafından işlenmesini sağlamamıştır. Aynı zamanda eskiden beri var olan birtakım verilerin

¹⁰² David LYON, Gözetlenen Toplum, s. 104.

¹⁰³ Manuel CASTELLS, Ağı Toplumunun Yükselişi, ABD 1996, s. 386’dan naklen: David LYON, Gözetlenen Toplum, s. 114

¹⁰⁴ Efe BAŞTÜRK, s. 277

¹⁰⁵ David LYON, Gözetlenen Toplum, s. 114.

¹⁰⁶ Stephen GRAHAM, The Fifth Utility, Sage Journals, C. 29, S. 3, 2000, s. 47.

¹⁰⁷ David LYON, Gözetlenen Toplum, s. 117.

işlenmesini ve sınıflandırılmasını da mümkün hale getirmiştir. Bu bakımdan, DNA verileri önemli bir örnektir. Gen parçalarından oluşan DNA, en genel tanımıyla kalıtımın moleküler temelidir¹⁰⁸. Her bireyin tam anlamıyla eşsiz olan DNA verisi, hem bireyi diğer bireylerden tam olarak ayırmaya yaradığı için hem de kalıtsal özellik taşıdığı için kişisel verilerin korunması açısından çok önemlidir¹⁰⁹.

Yukarıda bahsedilen gözetim teknolojilerinin dışında her gün kullandığımız cep telefonları, GPS veri sağlayıcıları gibi günlük hayatımızın vazgeçilmezi haline gelmiş teknolojiler de bulunmaktadır. Örneğin, cep telefonları telefonların ve dolayısıyla kullanıcılarının ne zaman ve nerede olduğuna ilişkin olarak zaman ve konum bilgilerini doğrudan servis sağlayıcılarına gönderebilmektedir. Keza sürücüsüz taşıt örneğinde de otomobil firmalarının araçlar üzerinden araç sahiplerinin konum bilgilerine doğrudan eriştiklerini görebiliyoruz. Örnekler ilk bakışta çok masum görünebilir, fakat madalyonun diğer yüzüne bakıldığında otomobil firması her saniye her dakika müşterisinin nerede olduğunu biliyorsa, bunu veri tabanına aktarıp üçüncü kişilere mesela grup şirketlerine aktarıyorsa, müşteri aleyhinde bir profil oluşturulamayacağının garantisi verilebilir mi?

Teknolojik gelişmelerin ve bilgisayar sistemlerinin, gözetimin merkezinde konumlandırıldığı bu yeni dönemde, bilgisayarlar sadece veri depolama görevi yürütmemektedirler. Bilgisayarlar ayrıca farklı verilerin birleştirildiği, analiz ve sentez yapabilen bir aygıtlardır. Günümüzde, bilgisayarın bu işlevlerinin daha çok kullanılmaya başlanması ise gözetimin artık veri gözetimi (dataveillance) haline gelmiş olması nedeniyledir¹¹⁰. Anderson ise özellikle Google'ın yüz tespit, yüz tanıma, fotoğraf asistanı (stories) özellikle bünyesinde barındırdığı görüntü algılayıcılar, sokak görüntüsü uygulaması Street view, sürücüsüz taşıtlar ya da diğer otonom robotik icatlar ve geniş veri bankaları

¹⁰⁸ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 42.

¹⁰⁹ Biyometrik teknolojiler 21. yüzyılda gözetim teknolojilerinin ulaşmış olduğu en ileri seviyeyi temsil etmektedir. Bireylerin bedenleri üzerinden; parmakları, gözleri, retina taraması vb. ya da biyolojik özellikleri üzerinden; DNA, kan grubu, kalp ritmi vb. üzerinden kimlik oluşturulması tekniğine biyometrik teknoloji diyebiliriz. Daha teknik bir tabir ile biyometrinin, “kişileri birbirinden ayıran ölçeklenebilir psikolojik ve davranışsal karakteristiklerin, kimlik tespitinde kullanılan bilgisayar kontrollü sistemler” olarak tanımlandığını görmekteyiz. Bkz. Uğur DOLGUN, Biri Bizi Gözetliyor, Kutu Yayınları, İstanbul 2019, s. 163; 11 Eylül’ den sonra bireylerin kimliklerini tespit etmek amacıyla kullanılan dijital görüntüleyici teknolojilerinin yerine, biyometrik teknolojiden faydalanılmaya geçilmiştir. Artık günümüzde biyometrik çipli pasaportlar neredeyse tüm ülkeler tarafından kullanılmaktadır. Biyometrik teknoloji bu açıdan, ülke sınırlarında, havalimanlarında kullanılmak için geliştirilen ve kimlerin içeri girmeye izinli olduğu hususunda bilgi sağlamaktadır. Bkz. Efe BAŞTÜRK, s. 283.

¹¹⁰ Efe BAŞTÜRK, s. 275.

sayesinde insanları çevreleyen bir ekosistem olduğunu; veri gözetiminden Google gözetimine (googleveillance) doğru bir geçiş yaşandığını belirtmiştir¹¹¹. Burada örnekler arasında saydığımız sürücüsüz taşıtlar ya da benzer teknolojiyi kullanan kendi kendine giden arabalar (self-driving cars) açısından son dönemdeki gelişimlerini göz önüne alarak ayrı bir parantez açmak mümkündür.

Sürücüsüz taşıtların kullanılması elbette ki günlük yaşantımızı ve otomobil sektörünün dinamiklerini baştan ayağa değiştirecektir. Ancak bu sistemlerin kullanılmasının belirli açılardan sorunlu olduğu alanlar da bulunmaktadır. Bunlardan birincisi bu sistemleri üreten hükümetlerin ya da üreticilerin ahlaki ve etik değerlendirmeler açısından otonom araçların nasıl programlanacağına karar vermelerinin zorunlu olmasıdır¹¹². Fakat bu araçların sürüş sırasında karşılaşacakları ikilemlerle baş etmelerini sağlayacak programın oluşturulması oldukça güçtür. Örnek olarak gösterebileceğimiz bir senaryoda sürücüsüz araç içerisinde seyahat edildiğini düşünelim. Bu seyahat sırasında sürücüsüz aracımız tam virajı almasından sonra yakın mesafede karşıdan karşıya geçen çocuk çocuklarla dolu bir yaya geçidine yaklaşmaktadır. Fren yapmasına rağmen yol üzerinde bulunan aşırı kum birikintisi nedeniyle araç yola yeterli ölçüde tutunamamaktadır. İşte tam bu aşamada yapay zeka devreye girerek bir takım muhtemel sonuçları hesaplamaya girişecektir. Aynı şeritte kalıp fren yapmaya devam ederse yüzde 90 oranla çocuklara çarpacak ve en azından 3 çocuğun ölümüne sebebiyet verilecektir. Yapay zekanın bu çocukları korumak için aracı uçuruma doğru yönlendirmesi ve araç içerisindeki kişileri feda etmesi söz konusu olmalı mıdır? Gerçekten de günümüz sürücüsüz araç sistemleri bu gibi senaryolara istinaden (yaya ve diğer araçlar ile) çarpışmadan kaçınmaya yönelik olarak programlanmaktadır¹¹³. Peki burada feda edilmesi gerekli olan değer, kişi ya da kişiler hangi kriterlere göre belirlenecektir?

Etik açıdan doğru olanın araç içerisindeki iki kişinin, üç çocuğun ölmemesi için feda edilmesi olacağı söylenebilir. Nicelik dışında nitelik itibarıyla da değerlendirme yapılması, genç bireylerin yaşlı olanlara karşı korunacak olması da düşünülebilir. Ancak bu yöndeki değerlendirmeler çoğunlukla kişisel eğilimleri yansıtmakta olup belirli oranda bir bencillik

¹¹¹ Steve F. ANDERSON, *Technologies of Vision: The War Between Data and Images*, The MIT Press, ABD 2017, s. 108.

¹¹² Anthony NELSON, "Smart Transportation Systems: Sustainable Mobilities, Autonomous Vehicle Decision-Making Algorithms, and Networked Driverless Technologies." *Contemporary Readings in Law and Social Justice*, C. 12, S. 2, Y. 2020, s. 25.

¹¹³ Eric SCHWITZGEBEL, "Should Your Driverless Car Kill You Others May Live?" , *A Theory of Jerks and Other Philosophical Misadventures*, MIT Press, ABD 2019, s. 76.

içerdiği söylenebilir. O halde yapılması gereken aslında kullanılacak olan algoritmaları gün ışığına çıkarmak, açıkça ve detaylı olarak incelemek ve kamuoyu nezdinde üretici, kullanıcı, hükümet temsilcileri dahil tüm tarafların katılımıyla tartıştıktan sonra yolcu güvenliği ve diğer unsurlar yönelik riskler arasındaki kabul edilebilir bir dengenin ortaya konulmasıdır¹¹⁴.

İkinci husus ise bu taşıtların bireylerin mahremiyetlerini sınırlandırdığı yönündeki olumsuzluklardır. Bu taşıtlar bulundurdukları bir çok gelişmiş sensör ile çevrelerinden sürekli olarak veri toplamaktadırlar. Toplanan bu konum verileri ya da şehir sakinlerinin hareket bilgileri sürücüsüz aracın yazılımı tarafından depolanmakta ve analiz edilmektedir. Bir kere bireylerin kamuya açık tüm alanlarda verilerinin sürekli olarak toplanması, bu fiziksel gözetimi çoğunlukla bir özel teşebbüsün gerçekleştirmesi, bu gözetim faaliyeti için ek bir alt yapıya ihtiyaç bulunmaması, kullanıcı olmayan bireylere bu veri toplama faaliyeti hakkında herhangi bir bilgilendirme yapılmaması ve kendilerine seçim yetkisi verilmemesi bireysel mahremiyete yönelik ihlallere sebebiyet verebilecek uygulamalardır¹¹⁵. Bu çalışmada sürücüsüz araçların veri toplama faaliyetlerinin genele yayılmasının (her yerde bulunabilirliğinin) CCTV'lere benzediği vurgulanmıştır. Ancak CCTV'lerden farklı olarak bu araçlar kurulum gerektirmeden gözetimin sınırlarını yasal olarak sürülmesine izin verilen tüm halka açık yolları kapsayacak şekilde genişletebilir¹¹⁶. Nitekim CCTV gözetimi ancak yeni bir kamera alt yapısının belirli bir alana kurulması ile başlayabilecektir. Bu durum gerçekleştirilecek gözetimin ölçüsünü fazlasıyla genişlettiği için bu sistemlerin veri koruma açısından detaylı değerlendirilmesi bir zorunluluk olarak karşımıza çıkmaktadır.

Her geçen gün daha fazla genişleyen, yaygınlaşan, ucuzlayan bilişim teknolojileri içerisinde, elektronik vasıtalar aracılığıyla verilerimizin toplanması kayıtların yalnızca elle tutulduğu zamana göre kolaylaşmış ve bilgilere ulaşma yolları çeşitlenmiştir. Bu durum aslında gözetimin de değiştiğini gözler önüne sermektedir. Yeni gözetim irade dışıdır, emek yoğunluğuna değil, sermaye yoğunluğuna bağlıdır ve merkezileştirilmiş kendini denetlemeyi içermektedir. Ayrıca toplumu oluşturan belirli bireyler yerine herkesi hedeflemekte olup daha yaygın ve yoğundur. Bu yeni gözetim ile tarihsel süreçte izlenimlediğimiz devletin disiplin

¹¹⁴ A.g.e., s. 77.

¹¹⁵ Cara BLOOM, Joshua TAN, Lujio BAUER, "Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles, Proceedings of the Thirteenth Symposium on Usable Privacy and Security, 2017, s. 357, https://www.ftc.gov/system/files/documents/public_comments/2017/11/00046-141905.pdf (s.y. 21 Şubat 2022)

¹¹⁶ A.g.i, s. 357.

araçları da değişmiştir. Fiziksel duvarlar yerine çipler, kelepçeler yerine uzaktan izleme aygıtları, zorlama yerine yönlendirme teknikleri kullanılmakta olup tüm bunlar bir bütün olarak topluma etki edebilme yetisine sahiptir. Yukarıda özelliklerini saydığımız bu yeni gözetim, bireyi her yönden kuşatmış bir gözetim uygulamasını ifade eden “Panoptikon” sistemine çok benzemektedir.

B. Gözetim Uygulamaları

Gözetim kavramının tam olarak neyi karşıladığının ya da asıl amacının ne olduğunun yanında ne şekilde gerçekleştirildiği de çalışmamız bakımından oldukça büyük bir öneme sahiptir. Bu bölümde sırasıyla gözetim uygulamalarından Panoptikon, Süper Panoptikon, Sinoptikon ve Banoptikon’u ele alacağız.

1. Panoptikon

Panoptikon ideal biçime getirilmiş olan bir iktidar mekanizmasının diyagramıdır, her tür engelden, dirençten veya sürtüşmeden arınmış olan işleyişi, saf bir mimari ve optik sistem olarak sunabilmektedir. Bedenleri mekana yerleştiren, bireyleri sınıflandıran, hiyerarşik örgütlenmeyi, iktidar merkezlerini ve kanallarını düzenleyen panoptik sistem, bir iktidarın araçlarını ve müdahale biçimlerini tanımlama tarzıdır¹¹⁷.

Bentham’ın Panoptikon’u bir mimari yapı olarak betimlediği görülmektedir¹¹⁸. Ancak panoptikonun bu şekilde betimlenmesi, onun sadece mimari bir biçim olarak ele alınmasına sebep olmamalıdır. Panoptikon, mimari bir biçim olmasının yanında aynı zamanda bir yönetim biçimidir. Bir başka deyişle, bireylerin üzerine doğrudan etki eden, insan zihnine iktidar verme şeklidir. Bu bağlamda panoptikonun mimari yapıdan çok daha kapsamlı, iktidarlar tarafından yapılacak her türlü zorlamanın uygulanma tekniği olduğunu söyleyebilmemiz mümkündür. Foucault buna ilişkin olarak, “ Bir ödevin veya bir hal ve gidişin dayatılmasının söz konusu olduğu bir birey çoğulluğunun bulunduğu her seferinde panoptikon uygulanabilir.”, demiştir¹¹⁹.

¹¹⁷ Michel, FOUCAULT, Hapishanenin Doğuşu, s. 303.

¹¹⁸ Jeremy BENTHAM, Catherine PEASE-WATKIN, Simon WERRET, Barış ÇOBAN, Zeynep ÖZARSLAN, Panoptikon: Gözün İktidarı, çev. Barış Çoban & Zeynep Özarslan, 3. Baskı, Su Yayınevi, İstanbul 2019, s. 9.

¹¹⁹ Michel, FOUCAULT, Hapishanenin Doğuşu, s. 303.

Bu mimaride yaratıcısı olan Jeremy Bentham'ın bir ilkesi saklıdır; "İktidarın görünür ama varlığının kanıtlanmazlığı ilkesi". Bentham tarafından ayrıntılı olarak açıklanan bu sistemde öyle bir düzen sağlanmıştır ki, mahkumlar ne zaman gözetlendiklerini bilememektedirler. Panoptikon yapıda gözetlenen mahkumlar sürekli olarak görünürlerken, buna karşılık gözetleyenler sürekli olarak görünmezdirler¹²⁰. Nitekim biz panoptisizmi, Bentham'ın hapishane mimarisinden doğan bir gözetim toplumu teorisi olarak tanımlayabiliriz¹²¹.

Bentham'ın Panoptikon'u, gerek felsefe gerek ise sosyoloji alanlarında gözetim, disiplin, bağlılık ve kontrol kavramlarını bir araya getirmiştir. Bu bağlamda, onu sadece bir mimari olarak değil aynı zamanda bir zorlama tekniği olarak düşündüğümüzde, günümüz toplumunda yaşayan her bir bireyi, hareketleri merkezi iktidar tarafından kontrol edilen bir mahkuma benzetebiliriz. . Bu doğrultuda, modern toplumda yaşayan insanlar olarak kendimize "Yaşadığım bu dünyada hareketlerime karar vermekte özgür müyüm?" sorusunu yönelttiğimizde vereceğimiz cevap bu benzetmenin yerinde olup olmadığını belirleyeceğini söyleyebiliriz.

George Orwell'in "1984" adlı romanı Bentham'ın ceza politikasına¹²² odaklanan gözetleme kavramından farklı olarak, toplumla ilgili gözetleme kavramına dikkat çeker. Orwell, hayal ürün olan bu distopik dünyada toplum gözetiminden duyduğu korkuyu, iktidarın (büyük birader) Okyanusya yurttaşları üzerinde uyguladığı baskıcı eylemlerinde dışa vurmaktadır¹²³. Büyük birader o kadar baskıcıdır ki Okyanusya vatandaşları sadece sokaklarda, meydanlarda veya iş yerlerinde izlenmezler, her yurttaşın evinde kendisini gözetleyen bir televizyon bulunur. Büyük birader kesintisiz olarak yurttaşların hareketlerini ve hatta düşüncelerini izlemektedir¹²⁴.

¹²⁰ Abdurrahman SAYGILI, s. 189.

¹²¹ Anne BRUNNON-ERNST, Beyond Foucault: New Perspectives on Bentham's Panopticon, TY Book, ABD 2012, s. 16.

¹²² Jeremy Bentham'ın çalışmaları "1952 yılında Baumgart tarafından "temel önemdeki konu olmadığı iddiasıyla" çalışma alanının dışında bırakılmasına karşın, 1980'li ve 1990'lı yıllarda ilgi merkezi haline geldi. "Bentham'ın Hapishanesi" (1993) adlı eserinde Janet Semple, İngiltere 'nin 19.yüzyıl başındaki politik düşünce çerçevesinde Panoptikon'un gelişimini ortaya koymuştur. Benzer şekilde Ignatieff (1978), Evans (1982), Foucault (1975) ve daha birçok düşünür Bentham'ın Panoptikonu' nun İngiliz ceza tarihindeki önemi" üzerinde durmuşlardır. Jeremy BENTHAM, Catherine Pease-Watkin, Simon WERRET, Barış ÇOBAN, Zeynep ÖZARSLAN, s. 87.

¹²³ Kevin D. HAGGERTY, Richard V. ERICSON, "The Surveillant Assemblage", British Journal of Sociology C. 51, S. 4, Y. 2000, s. 610.

¹²⁴ George ORWELL, 1984, 3. Basım, çev. Celal Üster, Can Yayınları, İstanbul 2019.

Bentham ve Orwell'in yanı sıra Foucault'nun da panoptikona ilişkin değerlendirmeleri oldukça faydalıdır. Foucault'un "Hapishane'nin Doğuşu" adlı eseri Bentham'ın "Panoptikon"u üzerine kuruludur¹²⁵. Fakat buradaki panoptikonun amacı gözetim yoluyla disiplini sağlamaktır. Foucault'ya göre bu disiplin, panoptikon sayesinde kendiliğinden sağlanmakta olup yöneten tarafından yaptırım uygulanmasına gerek kalmamaktadır. Panoptik mimari içinde gözetlenenler, kesintisiz olarak izlendikleri için bu gözetim sırasında işleyecekleri suçlar veya kabahatlerden dolayı cezalandırılabilirliklerini bildiklerinden, adeta bu disiplini içselleştirerek, suç veya kabahat işlemekten çekinmektedirler.

Foucault gerçekten de panoptikonun belirli açılardan modernitenin aynası olduğunu bizlere gösteren önemli çalışmalarda bulunmuştur. Ona göre disiplin, davranışı ve güdülenmeyi değiştirmek için "ruh"u kontrol etmeye yarayan bir anahtardır¹²⁶.

Gandy ise toplum gözetiminde üç temel eylemin yer aldığı bir panoptik sistem fikri ortaya çıkarmıştır. Panoptik sistemdeki rollerinden bağımsız olarak toplumu oluşturan bireylerin ya da grupların kişisel bilgilerinin toplanması, işlenmesi ve paylaşılması (aktarılması) sistemi meydana getirmektedir. Bu sistem elde edilen bilgiler dahilinde bireyleri sınıflandırmaya dayanmaktadır. Geniş bir alana yayılan ve süreklilik arz eden toplum gözetimi, kolay bir şekilde bireyler hakkında profiller oluşturarak, onları sınıflandırarak ortaya çıkan sonuçların yönetsel amaçlar için kullanılmasını sağlayacaktır¹²⁷.

Panoptikon devlet tarafından en alt düzeyde mahkumların en üst düzeyde ise toplumun kontrolünün sağlandığı bir kurallar bütünüdür ancak günümüzde, modern devlet ve yeni gözetim anlayışıyla gelişim göstererek toplumsal yaşamın her alanında yer almaya başlamıştır. Bu durum özellikle üç tekniğin gelişmesine paralel olarak yaşanmıştır. İlk olarak CCTV'ler gündelik yaşamda, sokaklarda, otobanlarda, alışveriş merkezlerinde (AVM'lerde), işyerlerinde kısacası gün içinde bulunan çoğu kamusal ve özel alanda yer alarak, bireylerde kendilerini sürekli olarak gözetleniyormuş izlenimi yaratmaktadır. Bir diğer teknolojik gözetim aracı ise, tüketiciyi odak noktası alan gözetim araçlarıdır bunlara örnek olarak; kredi kartları, sadakat

¹²⁵ Jeremy BENTHAM, Catherine Pease-Watkin, Simon WERRET, Barış ÇOBAN, Zeynep ÖZARSLAN, s. 7.

¹²⁶ Zygmunt BAUMAN, David LYON, Akışkan Gözetim, çev. Elçin Yılmaz, Ayrıntı Yayınevi, İstanbul 2018, s. 67.

¹²⁷ Oscar H. GANDY, The Panoptic Sort. A Political Economy of Personal Information, Oxford University Press, Oxford Scholarship Online, 2021, s. 29. <https://oxford.universitypressscholarship.com/> (s.y. 30 Mart 2022)

kartları, bireylerin alışveriş geçmişlerine ilişkin verilerinin toplanması ve işlenmesini gösterebiliriz. Bu gözetim tekniğinde gözetimin, gözetlenen birey ile gözetleyen tam anlamıyla bir işbirliği yaparak gerçekleştirildiğini söyleyebiliriz. Lyon “Tezgahın ardındaki kişinin bize telefon numaramızı, sürücü ehliyet numaramızı veya posta kodumuzu neden sorduğu ya da bir makinenin işlemini tamamlayabilmek için neden bizden daha fazla bilgi talep ettiğini sormaktansa, bu işte bize faydası olacak bir yön olduğunu varsayıyoruz”¹²⁸ ifadesinde bulunarak tüketicileri, kendilerinden istenileni aşırı bir gönüllülük içinde vermelerinden ötürü eleştirmektedir. Son olarak ise, internet ve uydular vasıtasıyla yapılan gözetimin klasik panoptikonu değiştirdiğini söyleyebiliriz¹²⁹. Bu yeni teknolojilerin ortaya çıkmasına olanak verdiği gözetim uygulaması süper panoptikon olarak da tanımlanır.

2. Süper Panoptikon:

Günlük yaşamları içerisinde kapalı devre kameralarla birbirlerini sürekli olarak izleyen, internet ortamında her hareketi takip edilebilen ve post-modern dönemde izleniyorum öyleyse varım algısıyla sosyal medyada özel hayatını paylaşan, GPS veya telefon teknolojisi ile bulunduğu yer saniye saniyesine belli olan bir bireyin, artık klasik panoptikon dışına çıktığını söyleyebiliriz.

Klasik panoptikon aslında artık sadece çeperlerde, özellikle de şehirlerde yoksulların, toplumdan dışlanmışların bulunduğu yerlerde söz konusudur¹³⁰. 21. Yüzyılda etrafımızı saran panoptikon sistemi, “süper panoptikon”¹³¹ ya da “siber panoptikon”¹³² olarak tanımlanır. Bu panoptik uygulamaların farklı gözetim teknikleri sayesinde çeşitli faaliyetlerde kullanıldığını görmekteyiz. Güvenliğin tesisi amacıyla parmak izlerinin, DNA kayıtlarının ve sabıka kayıtlarının tutulması, işyerlerinde CCTV’lerle yapılan gözetim, internet gözetimi ya da

¹²⁸ Zygmunt BAUMAN, David LYON, s. 142. Örneğin, mağaza zincirleri ya da havayolu firmalarının sıklıkla kullandığı sadakat kartları bakımından yapılan bir araştırmaya göre, insanların sadakat kartları kullanımı ile profil çıkarma arasındaki bağlantıları hiç bilmedikleri ya da bilmelerine rağmen umursamadıklarını ortaya koymuştur. Ayrıca bkz. Jason PRIDMORE, Loyalty Cards in the United States and Canada, Elia Zureik vd. (Haz.), Surveillance, Privacy and the Globalization of Personal Information, Montreal; McGill-Queen’s University Press, ABD 2010, s. 299.

¹²⁹ Jan KIETZMANN, Ian ANGELL, “Panopticon Revisited”, Communications of the ACM, C.53, S. 6, Y. 2010, s. 138.

¹³⁰ Zygmunt, BAUMAN, David LYON, s. 74.

¹³¹ Mark POSTER, The Second Media Age, Polity Press, Büyük Britanya 1995, s. 86.

¹³² Elif KÜZECİ, Kişisel Verilerin Korunması, s. 58; Shawn C. HELMS, “Translating Privacy Values with Technology”, Boston University Journal of Science and Technology Law, C.7, Y. 2001, s. 292.

tüketim alışkanlıklarının kaydedilmesi amacıyla çerezlerin izlenmesi bu faaliyetlerden bazılarıdır¹³³. Günümüzdeki gözetim faaliyetleri ve veri toplama teknikleri gerçekten de panoptik bir sistem oluşturmakta fakat bu panoptik sistem bazı açılardan Bentham'inkinden ayrılmaktadır.

Yönetmelik iktidarın merkezdeki bir kuleden mahkumları gözetlediği klasik panoptikon bu açıdan tam anlamıyla merkezde yoğunlaşan bir gözetimi ifade etmekte idi. ancak teknolojiye gelişmeler ile bugün içinde bulunduğumuz panoptikonda gözetleyen sadece merkezi iktidar değildir. Bireyler aynı zamanda özel kuruluşlar tarafından da izlenmektedir¹³⁴. CCTV'lerin güvenliğin sağlanması amacıyla, hem devlet tarafından örneğin MOBESE sistemiyle hem de özel şirketler tarafından kullanıldığını görebiliriz.

Ayrıca yine klasik panoptikonda bulunan “gözetleyenlerin görünmezliği” ilkesine göre, merkezi kuleden gelen ışığı görmesi sonucunda mahkum kule tarafından izlendiğini düşünür ancak ne zaman izlenip ne zaman izlenmediğini bilemediğinden dolayı mahkumda sürekli olarak izlendiği bu nedenle davranışlarına her zaman dikkat etmesi gerektiği şeklinde bir algı oluşmaktaydı. . Sonuç olarak mahkum ya da birey panoptik sistemin temel amacı olan kendisinden bekleneni yapmayı bir şekilde içselleştirerek davranışlarına yansıtmaktadır.

Panoptik yapı 21. yüzyılda bilişim teknolojileri zeminine oturtulmuştur. Bireylere ait kişisel veriler çoğu zaman kendilerine haber verilmeden, farkındalıkları ya da bu süreçlere ilişkin aydınlatılmaları sağlanmadan ve izinleri alınmaksızın toplanmaktadır. Günümüzde bu tarz kuşatıcı panoptik faaliyetlerle birçok alanda örneğin işyerinde, yolda, okulda ya da diğer alanlarda sıklıkla karşılaşmak mümkündür. Daha önceki bölümlerde yer yer değindiğimiz üzere; sürücüsüz arabalar, internetin kullanımı, metaverse ya da DNA'larımızın işlenmesine dair örneklerde olduğu gibi sürekli olarak gerçekleştirilen, sistematik ve birçok alana yayılan bir siber gözetimden bahsedilmesi mümkündür. Bu süper panoptik sisteme hizmet eden gözetim araçlarından bir tanesi de şüphesiz CCTV'lerdir. .

Avrupa ve Amerika'da yaşanan bir takım teknolojik gelişmelerin CCTV'ler gibi uzun zamandır hayatımızda bulunan sistemlerin çok ötesinde bulunduğu söylenebilir. Bu gelişmeler kapsamında yoğun gözetimin maddesel alandan siber alana geçtiği belirtilmekte olup, öğretilde

¹³³ David LYON, Elektronik Göz, s. 98.

¹³⁴ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 59.

gerçek süper panoptikonun siber alanda (bilhassa world wide web kastedilmiştir) hüküm sürdüğü yönünde tartışmalarda bulunulmuştur¹³⁵. Ancak belirtmek isteriz ki internetin gelişimi kadar gözde olmasa da CCTV kameralarının kullanım kolaylığı, teknolojiadaki gelişmeyle ucuzlamaya başlaması ve keza internet protokolünü kullanan kapalı devre kamera sistemlerinin de internete ve bulut veri tabanları sistemlerinin gelişimi ile paralel gelişmesi CCTV'leri de süper panoptik gözetim uygulamalarının merkezine konumlandırmaktadır.

Yukarda ifade ettiğimiz klasik panoptikon mimarisinde hapisane içerisinde bulunan mahkum üzerinde sürekli gözetlendiğine dair bir algı yaratıldığını böylelikle mahkumu kendisi hakkında bilgi toplandığına inandıran devletin amacına ulaştığını görmekteydik. Ancak bu yoğun bilgi toplama faaliyeti ne ölçüde hukuka uygun olacak, bunun da değerlendirilmesi gerekmektedir. Burada gözetimin en kolay örneklediği ve uygulandığı hapisane sistemi içerisinde bir örnek verecek olursak, Hudson Palmer'a karşı davasında¹³⁶, bir mahkumun cezaevindeki hareketlerinin izlenmesi bakımından hücresinde sürekli yoğun gözetim altında tutulmasına gerek olup olmadığı üzerinde durulmuştur. Mahkeme tarafından hakkında hapis cezası hükmedilen bir sanığın, hapisanede bulunduğu sürece mahremiyetinin azalacağına, gardiyanların mahkumların nerede ve nasıl yaşadıklarını sürekli olarak kontrol etme gücüne sahip olduklarını, her detayı gözetleme ve düzenleme yetkileri olduğunu belirterek, mahkumların mahremiyetlerinin gizliliğinin diğer anayasal haklara kıyasla daha az önemli görülmemesi gerektiğini ve bu kişilerin mahremiyetlerinin korunmasının önemli olduğunu belirtmiştir. Bu bakımdan cezaevleri Anayasa'nın uygulanma sınırlarından demir bir perde ile ayrılmış olarak görülemez¹³⁷. Örneğin, bir mahkumun üzerinin soyularak aranması özel yaşama müdahale kapsamında değerlendirilir ve aşırı, ölçüsüz, taciz boyutunda, hukuki meşruluktan yoksun ya da alakasız ise Anayasa'ya aykırı olduğu söylenebilir. Yani süper panoptik bir sistemde bile gözetimin bir takım sınırlandırmalara tabi olduğunu söylememiz mümkün olacaktır.

Daha genel anlamda baktığımızda ise yeni gelişen teknolojiler aracılığıyla sürekli olarak gözetim yapan devlet karşısında, bu kimselerin korunmasının gerekli olduğu

¹³⁵ Emanuel Gregory, BOUSSIOS, "Termination or Accountability? The Controversy over the United States Use of Cyberintelligence." Polish Quarterly of International Affairs, C. 25, S. 2, Y. 2016, s. 36.

¹³⁶ Bkz. Hudson Palmer'a karşı, 468 U.S. 517, k.t. 03 Temmuz 1984.

¹³⁷ Jennifer A. BROBST, The Metal Eye: Ethical Regulation of the State's Use of Surveillance Technology and Artificial Intelligence to Observe Humans in Confinement, California Western Law Review, C. 55, S. 1, Y. 2018, s. 48.

mahkemelerin gözünden kaçmamaktadır¹³⁸. Ancak yine de bu görüşe karşı olan mahkeme kararları da bulunmaktadır. Bu kararlarda devletin gerçekleştirdiği gözetim bakımından “sadece gözetimin zarar vermeyeceği”nden söz edildiğini görebilmekteyiz¹³⁹. O halde burada birey ve devletin karşı karşıya geldiğini söylemek yerinde olacaktır. Kaldı ki bu durum sadece devletin bireyi belirli bir alana kapattığı hapisanede gerçekleşen gözetim için değil tüm mecralarda gerçekleştirilen süper panoptik diğer gözetim faaliyetleri için de geçerlidir. Kural olarak, her yurttaş, yurttaşlığından kaynaklanan yükümlülüklerinin yanında bir takım temel hak ve özgürlüklere de sahiptir. Devletin vatandaşlarına salt insan olmalarından dolayı sahip olduğu bir takım haklarını kullanabilmeleri için sunması gereken bir takım pozitif yükümlülükler bulunmaktadır. Bunlar daha özel düzlemde anayasalarda ya da farklı uluslararası sözleşmelerde bulunabilecektir. Sonuç olarak devletin, vatandaşların ve çevresinin güvenliğinin sağlanması için bir takım faaliyetlerde bulunması zorunludur. Fakat bireyin devlet tarafından güvenlik sebebi gerekçe gösterilerek sürekli olarak gözetim altında tutulması bireyin temel haklarını ihlal edeceği ölçüde, bu gözetim faaliyetlerinin durdurulması gerekmektedir.¹⁴⁰

3. Sinoptikon :

Sinoptikon aslında bir gözetim kavramıdır. Bu kavram gözetim çalışmalarına Thomas Mathiesen tarafından dahil edilmiştir. Mathiesen’e göre, panoptikon az sayıda bireyin çok sayıda bireyi daha doğrusu toplumu gözetlemesi fikri temelinde oluşmuş olmakla birlikte, sinoptikon bunun tam tersi olacak şekilde toplumun az sayıda bireyi gözetlemesi anlamına gelmektedir¹⁴¹. Mathiesen, Foucault’u, panoptikon kavramını incelerken televizyon gibi çok önemli bir kitle iletişim aracını dikkate almamış olması nedeniyle eleştirir. Mathiesen’e göre, “milyonlarca insanı bir araya getirme özelliği olan ve hepsinin aynı anda yaratılan bir azınlığa hayranca bakışın nasıl inşa olduğunu¹⁴²” incelemeyen Foucault, içinde bulunduğu dönemin koşullarını dikkate almamıştır.

Panoptikon ve Sinoptikon birbirinden tamamen farklı iki sistem değil, birlikte gelişmelerini sürdüren sistemlerdir. Sinoptikon’da bireyler kendi isteklerine değil ancak iktidarın onlara sunduklarına ulaşabilirler. Burada önemli bir konumda bulunan televizyon ya

¹³⁸ A.g.m., s. 51.

¹³⁹ Neil M. RICHARDS, The Dangers of Surveillance, Harvard Law Review, C. 26, S. 7, Y. 2013, s. 1934.

¹⁴⁰ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 60.

¹⁴¹ Thomas MATHIESEN, The Viewer Society, Theroetical Criminology, C.1, S.1, 1997, s. 215.

¹⁴² A.g.m., s. 215.

da benzer kitle iletişim araçları birer gözetim aracı olarak kullanılırlar. Kısacası, Sinoptik sistemde gözetim faaliyetleri, başta televizyon ve iktidar güdümlü medya sayesinde toplumu oluşturan bireylerin zihinlerini ve bedenlerini sürekli olarak kontrol altına tutmaktadır. Böylelikle bireylerin dolaylı ve sürekli olarak gözetim altında olduğunu söylememiz mümkündür.

4. Banoptikon:

Banoptikon kavramı ilk defa Didier Bigo tarafından ortaya atılmış olup Jean-Luc Nancy'nin Agamben tarafından geliştirilmiş “ban” (yasak) fikri ile Foucault'un “panoptikon” düşüncesini birleştiren Bigo, profil çıkarma teknolojilerinin, belirli gözetim tekniklerine göre hangi birey gruplarına uygulanacağını belirleyen gözetim sistemine banoptikon demiştir¹⁴³.

Buradaki yasak fikrine kısaca değinmemiz gerekirse; Agamben'e göre hukuksal-kurumsal iktidar yasak olanı belirleme kudretine sahiptir. Bu yasak ile toplumdan dışlanan insan bir nevi hukukun şiddetine maruz kalmış yasaklı bir kişi konumunda bulunur. Ancak bu durum yasaklı bireyin hukuk kurallarının tamamen dışında bulunacağı anlamına da gelmeyecektir¹⁴⁴. Kastedilen içleyici bir dışlamanın öngörülmesidir¹⁴⁵. O halde banoptikon sisteminde panoptik gözetim dahilindeki kişiler hakkında profiller oluşturulduğunu ve yukarıda anlattığımız şekilde bazı bireylerin de (egemen iktidar tarafından risk kriterlerine göre değerlendirilerek) yasaklı kişi konumuna geldiklerini söylememiz mümkündür.

Banoptikon, “Azınlık Raporu” isimli filmde olduğu gibi henüz gerçekleşmemiş olaylarla ilgili veri akışını yönlendirmek için çalışmaktadır. Bu bakımdan yüksek teknoloji araçları vasıtasıyla profil çıkarma önemli bir unsurdur. Mattelart'a göre¹⁴⁶, yönetsel güç, banoptikon gözetimi risk oluşturan gruplara karşı oluşturmuştur. Dolayısıyla bu sistemde önemli olan panoptikondaki gibi gözetleneni içeride tutmak değil, istenilmeyeni dışarıda

¹⁴³ Zygmunt BAUMAN, David LYON, s.75.

¹⁴⁴ Amy O'DONOGHUE, “ Sovereign Exception: Notes on the Thought of Giorgio Agamben, <https://criticallegalthinking.com/2015/07/02/sovereign-exception-notes-on-the-thought-of-giorgioagamben/> (s.y: 22 Şubat 2022)

¹⁴⁵ Didem MUTLU, Mehmet ARI, Foucault ve Agamben Düzleminde Biyo-Politika, *Fiscaeconomia*, C. 4, S. 1, Y. 2020, s. 166.

¹⁴⁶ Armand MATTELART, Gözetimin Küreselleşmesi, Güvenileştirme Düzeninin Kökeni, çev. O. Gayretli & S. E. Karacan, Kalkedon, İstanbul 2012, s. 274.

tutmaktır. Bigo'nun bu kavramı oluştururkenki çıkış noktasının istenmeyen göçmenler olması bu amacı en görülebilir şekliyle okuyucuya göstermektedir¹⁴⁷.

Bu gözetim sisteminde bireyler tarafından hissedilen güvensizlik duygusu diğer sistemlerdekine nazaran daha fazladır. Enformasyon çağında yapılan rasyonel ayrımcılığın çoğunlukla ırksal profillerin çıkarılmasına yönelik olduğu görüldüğünde, bu faaliyetler nedeniyle haklarında olumsuz sonuç çıkarılanlara çok büyük çapta dezavantaj yaratacağı açıktır¹⁴⁸. Lyon'a göre, gözetleme teknolojileri bireyler açısından gerçekten de eşitsizlik yaratmıyorsa, kesinlikle var olan eşitsizlikleri güçlendirmekte ve hızlandırmaktadır¹⁴⁹.

Banoptikon gözetimi günümüzde iki şekilde yapılmaktadır. Bir tarafta bireyin hapsedilmesi, kapalı tutulması, diğer tarafta ise bireyin dışarda bırakılması söz konusudur. Burada her ne kadar bireyin hapsedilmesinden bahsedilse de gerçek bir hapisanede birey hakkında profil oluşturulması esas amaç olarak görülmez. Bu nedenle banoptikonun hapisanedeki gözetimden farklılaştığı söylenebilecektir. Bireyin belirli bir alanda kapalı tutulması ya da belirli bir alanın dışında tutulması toplumdan dışlanmasına neden olmaktadır. Örneğin; günümüzde Avrupa Birliği (AB)'nin sorunlarından biri haline gelen mülteci krizi konusunun, hem mülteciler hem de bu konudaki uygulamaları belirleyen karar mekanizması devletler açısından gün geçtikçe daha zor bir hale büründüğü söylenebilecektir¹⁵⁰. Bir mülteci kampında bulunmak aslında, kampın dışında yer alan dünyadan dışlanmak demektir. Yani istenmeyen bireyler konumunda olan mülteciler kapalı tutulmak suretiyle toplumdan dışlanmaktadır. Bauman¹⁵¹'in deyiimi ile “banoptikonun temel amacı atığın, değerli ürünlerden ayrılmasını ve çöplüğe gönderilmek üzere işaretlenmesini garantiye almaktır”. Bu ifadede bahsi geçen ayrıştırmanın yukarıda verdiğimiz örnekte gerçekleştiğini görmekteyiz. Bauman'ın bahsettiği “Atık” deyiimi burada faydanın karşıt anlamlısıdır. Atığın tek yaptığı şey gayet verimli bir biçimde kullanılabilecek olan mekanı kirletmek ve karıştırmaktır. Ancak burada ifade edilen değerlinin değersizden ayrılması ve çöplüğe gönderilmesi aynı zamanda

¹⁴⁷ Zygmunt BAUMAN, David LYON, s.77.

¹⁴⁸ Zygmunt BAUMAN, David LYON, s.81.

¹⁴⁹ David LYON, Gözetlenen Toplum, s. 134.

¹⁵⁰ “Özellikle Suriye iç savaşının sonuçlarından olan bu durum nedeniyle milyonlarca mültecinin, iç savaşın başlangıcından itibaren Türkiye, Ürdün ve Lübnan gibi Suriye'ye komşu ülkelerde misafir edilmelerinden dolayı Avrupa uzunca bir dönem bu sorunla yüzleşmedi. 2015 yılının başından itibaren mültecilerin Avrupa'ya doğru hareketlenmesiyle birlikte mülteci meselesi genelde AB'nin özelde ise onun önde gelen gücü Almanya'nın sorunu haline geldi.” Bkz. Enes BAYRAKLI, Kazım KESKİN, Avrupa'nın Mülteci Krizi, Akademik İncelemeler Dergisi, C. 12, S. 2, Y. 2017, s. 115 – 136.

¹⁵¹ Zygmunt BAUMAN, David LYON, s. 80.

kişisel verilerin sınıflandırılmasına ilişkin olarak da gündeme gelebilmektedir¹⁵². Sınıflandırılan kişisel veriler ile uygun gelir düzeyine sahip tüketicilere yönelik bir pazarlama faaliyeti yapılırken, diğer potansiyel tüketiciler ve kişisel verilerinin atık olarak görüldüğünü söyleyebiliriz. Sonuç olarak panoptik sistem sadece sınırlarda, güvenlik ve geçiş alanlarında bulunmamakta ve sadece belirli gruplara dezavantaj yaratmamakta, küreselleşen dünyada gelişen gözetim teknikleri sayesinde çok çeşitli yollarla bireyler hakkında profiller oluşturulmaktadır. Kredi kartı bilgileri, alkol, uyuşturucu alışkanlıkları, cinsel yönelim ya da biyometrik veriler gibi alanlarda oluşturulacak profiller bireyleri çevrelemektedir.

C. Panoptikon Dışındaki Gözetim : Nano Teknoloji

Geçtiğimiz çeyrek yüzyıl ile birlikte gündelik yaşantımıza, iş ve sosyal hayatımıza sayısız yeni teknolojiler ve yeni icatlar girmiştir. . Gerçekten de bilimsel çalışmaların ve icatların kümülatif olarak ilerlemesinin de etkisiyle, 2000 yılından sonra bundan önceki çeyrek asra göre bilim ve teknolojinin çok daha hızlı ilerlediğini görmekteyiz. Bu bilimsel yeterlilik yapay zeka , büyük veri (*big data*), blokzinciri, sanal gerçeklik, artırılmış gerçeklik, Web 4.0, Metaverse, kripto para birimleri, dijital paraların kullanımı, sürücüsüz taşıtlar ve özellikle sağlık teknolojileri açısından nöroteknoloji, sentetik biyoloji, nano cihazlar, yine ayrıca drone teknolojileri, bulut bilişim teknolojisi gibi çoğunu daha önce duymadığımız ya da bilim-kurgu filmlerinde görebildiğimiz teknolojileri hayatımıza katmıştır. Tüm bu teknolojiler arasında nano-teknoloji klasik gözetimi panoptikonda gerçekleştirilenin ötesine taşıdığı için gözetim teknikleri ve uygulamaları açısından çok büyük değere sahiptir.

Bir bilim alanı olarak nano-teknolojinin gelişimi 1980’li yıllarda vuku bulmuştur. Bu dönemdeki nano-teknoloji çalışmaları çoğunlukla, az sayıda atomdan mekanik aygıtlar yapılması yönündeki yaklaşımlardan ibarettir¹⁵³. Bu teknoloji ilk olarak nano-ölçü (nanoscale) düzeyinde başlamıştır. . Nano-ölçü dediğimiz kavram herhangi bir ölçü biriminin milyarda biri değerindedir.

¹⁵² Oscar GANDY, s. 71-116.

¹⁵³ Stephen, WOLFRAM, A Kind of Science, Wolfram Media Inc., Kanada 2002, s. 1193.

Nano-teknoloji ise kimya, fizik, malzeme bilimi veya mühendislik alanlarında yapılan bilimsel çalışmaların nano-ölçü düzeyinde yapılması anlamına gelmektedir¹⁵⁴. Bilim adamları yıllardır nano-ölçü düzeyinde çalışmalar yaparak, daha hızlı ve daha küçük depolama cihazları geliştirerek büyük depolama alanlarının külfetinden kurtulmak, hastalıkların tanı ve tedavisinde daha hızlı sonuçlar almak, yan etkilerin zararlarından kaçınmak amacıyla sağlık ve ilaç çalışmaları yapmak, daha dayanıklı, güçlü ve hafif aletlerin üretilmesi amaçlarıyla nano-ürünler ve teknolojiler üretmişlerdir. Bu teknoloji sayesinde kanserli hücrelerin tedavisinde, yan etkisi bulunan ilaçlar yerine nano-robotların kullanıldığı; cep telefonları ya da laptopları şarj etmek için hareket enerjisini elektrik enerjisine çeviren kıyafetlerin giyildiği bir döneme girmiş bulunuyoruz.

Nano-Teknoloji, bilgi teknolojileri ile diğer bir takım teknolojileri bünyesinde barındırır. RFID etiketleri (RFIDs), entegre devreler, nano-tozlar, biyo sensörler veya akıllı giysiler, akıllı kumaşlar ve akıllı yüzeyler gibi teknolojiler perakende, sağlık, taşımacılık, mağazacılık ve depolama sektörlerinde kullanıldığı gibi, ceza hukuku ve güvenlik alanlarında da kendilerine yer bulmuşlardır¹⁵⁵.

Nano-teknolojinin faydalarının yanında bir takım olumsuz sonuçları da bulunmaktadır. Bu nano-cihazlar sayesinde bireyler adeta küçük ölçekli birer veri tabanı haline gelmekte, birey üzerinden sürekli olarak gizli şekilde bilgi toplamak mümkün olmaktadır. Hal böyle olunca, bireylerin mahremiyetlerinin ve kişisel verilerinin korunması oldukça önem kazanmaktadır.

Nano-panoptisizm fikri ise, nano-teknoloji alanındaki gelişmelerin bir sonucu olarak Mehta tarafından ortaya atılmıştır. Nano-teknoloji ile birlikte gözetimin artık Panoptikon'un ötesine geçtiğini; bireyin CCTV sistemleriyle, telefonlarla, internet veya bilgisayarlarından alınan verileriyle gözetlenmesinin nano-teknoloji sonrasında giydiği kıyafetler, kullandığı veya taktığı çeşitli cihazlar ile kablosuz bir şekilde, bulunduğu yerden bağımsız olarak gözetlenmesine evrildiğini söyleyebiliriz.

¹⁵⁴ National Nanotechnology Coordination Office, Nanotechnology: Big Things from a Tiny World (Brochure), 16 Mart 2018.

¹⁵⁵ Jeroen van den HOVEN, Pieter E. VERMAAS, Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon, Journal of Medicine and Philosophy, S. 32, Y. 2007, s. 283.

Nano-teknoloji, CCTV sistemlerini de etkilemektedir. Bugün meta-lens diye tabir edilen ve nano-teknoloji sayesinde geliştirilmiş ultra ince, hafif, imalatı kolay ve ekonomik olan bir mercek türünün kameralarda kullanılması mümkündür. Bu özelliklerine ek olarak daha iyi performans göstermesi ve daha düşük enerji tüketimi sağlaması ile birlikte bu nano-lenslerin özellikle artırılmış gerçeklik, küçük ölçekli insansız hava araçları (mini-drones) için görüntü sağlama, sürücüsüz taşıt, tarıma odaklı robotik teknolojiler ve biyo-medikal sağlık uygulamalarında sıklıkla kullanılacak olması nedeniyle geleneksel optik lenslerin yerini alması da beklenmektedir¹⁵⁶. Nano-kameralar ise birtakım diğer nano bileşenlerden meydana gelen ve görüntüleri tespit eden, işleyen ve aktaran nano cihazlardır¹⁵⁷. Nano-kamerayı meydana getiren bileşenler nano-dedektörler, nano-lensler, nano-bellekler, nano-işlemciler, nano-antenler ve nano-bataryalardır.

Geleneksel CCTV sistemlerinde, yani belirli bir alana yerleştirilen kapalı devre sisteme bağlı bir kameranın bulunduğu sistemlerde bu yönde bir gelişim bina dışına, işyerine ya da diğer alanlara konumlandırılan CCTV'lerin çok küçük hale gelmesine sebebiyet verecektir. Eğer bu nano lensleri elde etmek maliyet olarak da iddia edildiği gibi ucuz olursa, CCTV'lerin sayıca artacağı ve gerçekleştirilen gözetimin daha yoğun hale geleceğini söyleyebiliriz. Bu durum ise nano-panoptisizmin uygulanma alanını daha da genişletecektir.

CCTV'ler dışında polis vücut kameraları (PVK) ve diğer taşınabilir kamera sistemleri de gözetim amaçlı olarak kullanılabilir. Örneğin; günümüzde kullanılmakta olan PVK'ların çoğu bir yaka kartı ebatındadır. Bireyler, polislerin taşıdıkları bu kartı (aydınlatmaya dair bir bilgilendirme yer alsın ya da yer almasın) görebilmektedirler. Bu taşınabilir kameraların ilerleyen dönemlerde nano boyutlara inmesi ihtimalinde bireylerin aleyhinde bilgilendirmeye dayanmayan bir veri işleme faaliyetinin yürütülmesi söz konusu olabilecektir.

Nitekim Princeton ve Washington Üniversiteleri tarafından gerçekleştirilen bir araştırma kapsamında kalın bir tuz tanesi boyutunda bir kamera geliştirilmiştir. Bu geliştiren kameranın eski benzerlerine göre çok daha net ve dağınık olmayan bir görüntü sağladığı da

¹⁵⁶ Mu K. CHEN, Yonfeng WU, Lei FENG, Qingbin FAN, Minghui Lu, Ting XU, Din P. TSAI, Principles, Functions, and Applications of Optical Meta-Lens, Advanced Optical Materials, C.9, S.4, Y. 2021, <https://onlinelibrary.wiley.com/doi/10.1002/adom.202001414> (s.y: 23 Şubat 2022)

¹⁵⁷ Jennifer SİMONJAN, Ian F. AKYILDIZ, Josep Miquel JORNET, Bernhard RİNNER, Nano-Cameras: A Key Enabling Technology for the Internet of Multimedia Nano-Things, NANOCOM, Rejkavik, İzlanda, 5-7 Eylül 2018

vurgulanmıştır. Bu aşırı küçük kameraların yukarıda aktardığımız şekilde gözetimde kullanılması dışında ayrıca insan vücudundaki sorunları tespit etmeye, hastalıkların teşhisine yönelik çalışmalarda da kullanılacağı belirtilmektedir¹⁵⁸.

Nano-teknolojiler açısından ayrıca RFID (Radio Frequency Identity Chip) teknolojisine değinmemiz gerekecektir. RFID kısaca bir otomatik tanımlama teknolojisidir. Mikroişlemci ile donatılmış bir etiket (tag) taşıyan nesne, bu etikette taşıdığı bilgiler ile hareketlerinin izlenebilmesine imkan vermektedir. RFID teknolojisini diğer otomatik tanımlama teknolojilerinden (Örn: barkod) ayıran bir takım özellikler bulunmaktadır¹⁵⁹. Örneğin, tamamen radyo frekansları kullanılarak bir RFID etiketinin üzerindeki veri değiştirilebilir, etikete veri yazılabilir, etiketteki veri benzer teknolojilere göre daha iyi şifrelenebilir. Yine bunlara benzer olarak, etiketin saklayabileceği kullanışlı veri miktarı, etiket dayanıklılığı, etiketin belirli bir mesafeden okunabilmesi gibi avantajları bulunmaktadır.

Önümüzdeki yıllarda sıklıkla duyacağımız bir kavram da “nesnelerin interneti” (internet of things – Iot) teknolojisidir. RFID etiketleri ve okuyucularını da barındıran bu ekosistemde makineler sürekli olarak birbirleriyle bilgi paylaşır, tabir-i caizse birbirleriyle konuşurlar. Sürekli olarak internete bağlı olan ve çeşitli nesnelere gömülü cihazların birbirleriyle ve farklı hizmet sağlayıcılarla küresel ölçekte etkileşime girmelerine olanak tanıyan bu ekosistem, farklı makinelerin ya da teknolojilerin birlikte daha etkili bir şekilde çalışabilmelerine olanak tanıyacaktır¹⁶⁰. RFID teknolojisinin CCTV’lerde kullanılmasının en bariz örneği CCTV kameralarının güvenlik amaçlarıyla bina girişlerine ya da diğer benzer alanlara yerleştirilmesi durumlarında görebiliyoruz. Bu şekilde kullanılan bir CCTV’ye entegre olan RFID eklentisi varsa, örneğin RFID etiketi olan kişi güvenli sayılarak işlenen görüntülerinin yapay zeka dahilinde doğrudan silinmesi ya da mozaikleştirilmesi söz konusu olabilir. RFID ile CCTV’lerin bir arada çalıştığı diğer bir örnek ise ürün yönetimi ve mağaza güvenliğinin sağlanması olabilecektir. Örneğin; RFID etiketi içeren bir ürünün ücreti ödenmeksizin mağaza dışına çıkarılması gibi bir durum söz konusu ise mağazadan çıkış anında RFID üzerinden tetiklenen CCTV’nin doğrudan buna ilişkin kayıt yaptığını görebiliriz. Ürünün

¹⁵⁸ Molly SHARLACH, Researchers Shrink Camera to the Size of a Salt Grain, Princeton University, <https://www.nanowerk.com/nanotechnology-news2/newsid=59252.php> (s.y: 23 Şubat 2022)

¹⁵⁹ Erkan M. YÜKSEL, Halim A. ZAIM, Otomatik Nesne Tanımlama Teknolojisi Olarak RFID ve RFID’ in Faydaları, s.1, https://www.emo.org.tr/ekler/c005118de912f94_ek.pdf (s.y. 12 Eylül 2021)

¹⁶⁰ Subhas Chandra MUKHOPADHYAY, Internet of Things: Challenges and Opportunities, Springer, 2014, s.1.

nerede olduğunu araştıran mağaza yetkilisi ise sadece ürün kodunu ara yüze girerek ilgili video kaydına ulaşma kolaylığına sahip olacaktır.

Şehirlerin yakın bir gelecekte makinelerin iletişim içinde olduğu, birbiriyle konuştuğu akıllı şehirler haline gelmesi kuvvetle muhtemeldir. Bu şehirler, makinelerin veri değiş-tokuşu yaptıkları ve bu temel üzerinde karar alabildikleri akıllı bir iletişim ağından oluşacaktır. Örneğin, bir elektrikli otomobil, akıllı alt yapısı sayesinde şarj istasyonu ile tamamen radyo frekansları ile konuşarak gerektiği kadar elektrik alabilir ya da evimizdeki makineler o günün kullanım verilerine dayanarak ev içerisindeki enerji tüketim miktarımızı dengeleyebilir, ayrıca trafikteki araç ve insan akışlarını izleyerek, yoğunluğun farklı yollara dağıtılmasını sağlayabilir¹⁶¹. Yine Tayvan'ın başkenti Taipei'de belirli alanlarda şehrin akıllı yönetiminin sağlanması için nesnelerin interneti kullanılmaktadır. Başka bir örnek olarak ise; Brezilya'da sayısı yirmi bini geçen öğrenciler akıllı uniformalar giymesini ve okul yönetiminin öğrencileri uniformalarındaki RFID çipleri üzerinden takip etmesini gösterebiliriz¹⁶². Kullanmakta olduğumuz pasaportlar hem biyometrik verilerimizi içermekte hem de bu içerisinde RFID çipleri bulunmaktadır.

RFID teknolojisinin günlük hayatı ve geleceğin akıllı şehirlerinin yönetimini kolaylaştıracağını faydalarının sadece belirttiklerimizle sınırlı kalmayacağını öngörmekteyiz. Yukarıdaki örneklerde değindiğimiz üzere özellikle perakende ve tedarik sektöründe, ham madde üzerine yerleştirecek RFID etiketleri ile üretim sürecinde hangi ürünlerin kimler tarafından kullanıldığı gibi veriler kayıt altına alınabilecek; stok takibi, hatalı ürünün ayıklanması, nakliye, teslimat, mal sayımlarının yapılması gibi işlemler insan gücü gerekmeden yapılabilecektir.

Bireyin giymiş olduğu bir kıyafete, ayakkabıya veya üretim bandındaki herhangi bir nesneye ya da trafikteki herhangi bir araca kendine has bir RFID etiketi entegre edildiğinde, birey, üzerinden veri elde edilen bir nesne haline gelmektedir. Böylelikle bireyler açısından nano-teknolojinin görünmez bir gözetim sistemi yaratması söz konusu olmaktadır. Bu sistemlerin bir takım dezavantajlı durumlar yaratması ise oldukça muhtemeldir. Örneğin; etiketli bir veri taşıyıcısının, toplumdaki hareketleri nedeniyle ayrımcılığa maruz kalması ya da

¹⁶¹ Subhas Chandra MUKHOPADHYAY, s. 82.

¹⁶² Jordan FRITH, A Billion Little Pieces: RFID and Infrastructures of Identification, The MIT Press, ABD 2019, s. 211.

uğraması söz konusu olabilecektir. pahalı ürünler satan bir mağazaya giren bir bireyin taşımakta olduğu etiket, bireyin tüketim geçmişi hakkında mağazaya bilgi verecek, bu durum bireyin orada hoş karşılanıp karşılanmayacağı hususunu etkileyebilecektir . Bu durum müşterinin kişisel verisinin hukuka aykırı olarak kullanıldığı ve özel hayatının gizliliğinin ihlal edildiği anlamına gelecektir¹⁶³. Bu bakımdan bireyin kendi verisinin geleceğini belirleme hakkı açısından ayrıca açık rızasının alınması, verinin ancak açık rıza sonrası işlenebileceği açıktır.

Bireylerin kişisel verilerinin korunması açısından nesnelerin interneti sisteminin yaratacağı sorunların göz ardı edilmemesi gereklidir. RFID etiketleriyle ham maddelerin, giydiğimiz kumaşların, kullandığımız aletlerin ve yüzeylerin içerisine yerleştirilen mikro ebattaki çipler her an her koşulda birey hakkında bilgi toplanması ve bunların bir başka yere aktarılması, depolanması anlamına gelebilecektir. . Bu açıdan, burada yapılan gözetimin sürekliliği yönünden diğer hiçbir gözetim tekniğine benzemediğini söylememiz mümkündür. Ayak izlerini hatırlayan halılardan, gün içerisinde nerelerde bulunduğuna dair bilgi veren ayakkabı tabanlarına kadar bu nano-panoptik sistem artık tamamen gelişmemiş, etrafı duvarlarla çevrili hapisane modelinden ayrılmıştır¹⁶⁴. Böylece bireyler panoptik sistemin merkezi sınırlarının dışına çıkabilseler de aslında nano-panoptik sistemden kaçamamaktadırlar.

Nano-lensler, nano-kameralar, RFID sistemleri ve bunlar gibi birçok farklı teknoloji hayatımız içerisine girmiş bulunmaktadır. Böylece kişisel verilerin korunması tartışmaları da maddenin kendisinden, bitlere ve baytlara doğru kaydıktan sonra maddenin en küçük yapı taşı olan atomuna yönelmiştir¹⁶⁵. Bunu şöyle anlatmamız mümkündür. Eskiden mahremiyet dediğimizde aklımıza gelenler ev, duvarlar ve perdeler iken sonraki dönemlerde mahremiyeti bilgisayar teknolojilerinde, bitlerde, baytlarda aradık. İçinde bulunduğumuz zaman diliminde ise mahremiyeti daha küçük yapı taşları arasında yani nano birimlerde aramaktayız.

III. Kapalı Devre Kamera Sistemi Tanımı, Unsurları ve Teknik Açıdan İncelenmesi

Kapalı devre kamera sistemi kameraların kurulu olduğu alanın denetlenmesini amaçlayan, kapalı bir alıcı sistem içerisinde belirli bir alanda görüntü kaydı yapan ve bunları

¹⁶³ Jeroen VAN DEN HOVEN, Pieter E. VERMAAS, s. 294

¹⁶⁴ A.g.m., s. 292.

¹⁶⁵ A.g.m., s. 293

aktaran sistemler olarak tanımlanmıştır¹⁶⁶. Bu sistem içerisinde, video kameralar ile toplanan görüntüler, sadece birlikte çalıştığı (kapalı bir sistem ya da devre içerisinde) sınırlı sayıdaki diğer bileşenlere (monitörlere) aktarılmaktadır. Görüntü kayıtları doğrudan üçüncü kişilerin erişimine sunulmamaktadır. Bu nedenle çalışmamız kapsamında video görüntülerinin toplandığı, işlendiği, aktarıldığı ya da benzeri işlemlere tabi tutulan video görüntü kayıt faaliyetlerinin değerlendirilmesi söz konusu değildir. Yukarıdaki nitelendirmede belirtilenin aksine, örneğin televizyon yayınları sınırlı sayıda bir monitöre değil daha geniş alanda tüm topluma yayın yapmaktadır. Kapalı devre kameralar bu yönden diğer görüntü kaydı alan ve aktaran sistemlerden ayrılmaktadır. Nitekim kapalı devre sistemlerin tersine açık devre kamera sistemleri gibi bir sistem bulunmamakla birlikte diğer sistemler (örneğin; bunun içerisinde bireysel telefonu ile çekim yapan kişiden canlı yayında tüm dünyaya yayın yapan bir haber kanalının yayını faaliyetleri bulunmaktadır) doğrudan tez konumuzun dışındadır.

Yukarıdakine benzer bir tanımda bu sistemlerin kapalı devre görüntü ve kayıt sistemlerini ifade ettiği belirtilmiştir. Genel olarak sistem bir veya birden fazla kameranın kullanılması yoluyla belirli bir bölgenin gözetlenebilmesi, elde edilen görüntülerin kayıt altına alınması ve video monitörlerinde görüntülenmesine olanak sağlamaktadır¹⁶⁷. Walter Bruch isimli bir Alman mühendis tarafından tasarlanan ilk kapalı devre kamera sistemi 1942 yılında, V-2 roketlerinin kalkışlarının izlenmesi amacıyla kullanılmıştır.

Teknik açıdan kapalı devre kamera sistemleri dört temel unsurun birleşimi ile meydana gelmektedir. Bunlar video kamera, güç ve iletişim kabloları, video kayıt cihazı, kontrol ve video görüntüleme (monitör ya da birden çok monitörün yer aldığı kumanda odaları) cihazıdır¹⁶⁸. Bu sistemlerin farklı amaçlar için kullanıldıkları görülmektedir. Isı algılayıcı kameralar kullanılarak görüntülenenenlerin aynı zamanda vücut ısılarının tespit edildiği, hareket sensörlü kameralarla hareketlerin tespit edildiği ya da gece görüşü özellikli kameralarla karanlık alanlarda bulunan insanların görüntülendiği kapalı devre kamera sistemleri bulunmaktadır. Farklı amaçlarla kullanılan tüm bu kamera sistemlerinin kameralar dışındaki bütün bileşenleri benzer özellik göstermektedir. Bu bileşenlerin ayrı ayrı değerlendirilmesi ve nasıl çalıştığının

¹⁶⁶ Jolanta IGNAC-NOWICKA, Visual Monitoring as a Tool in Industrial Security Engineering, Mape, C. 4, S. 1, Y. 2021, s. 108.

¹⁶⁷ Cüneyt AKINLAR, Yusuf OYSAL, Hüseyin POLAT, Efnan GÜNAL, Güvenlik Sistemleri, 1., Eskişehir 2012, s. 82.

¹⁶⁸ Cüneyt AKINLAR, Yusuf OYSAL, Hüseyin POLAT, Efnan GÜNAL, s. 86.

ortaya konulması konumuz için önem arz eden bir husustur. Bunun için ilk olarak CCTV'lerin dış dünyada en çok göze çarpan unsuru olan video kameralardan başlamak yerinde olacaktır.

Video kamera odaklanılan bir ışık görselini kamera lensi vasıtasıyla daha sonra bir monitör ekranına yansıtılması ya da kaydedilmesi için zamana bağlı olarak değişen bir elektronik video sinyaline dönüştürmektedir. Birden fazla aşamadan oluşan görüntünün sağlanması işlemi lensin ilgili alandan yansıyan ışığı toplamadıktan sonra kamera görüntü sensörüne yollamasıyla başlamaktadır. Sensör bu ışık görüntüsünü elektronik sinyallere dönüştürmekte, kamera elektroniği de sensörden gelen bu bilgileri işledikten sonra kameranın türüne göre video sinyallerini kablo vasıtasıyla, kablosuz ya da diğer transfer araçları dahilinde bir izleme monitörüne yollamaktadır. Sistemi daha iyi ifade etmek için şu örneği vermemizde sakınca yoktur. İnsan gözü sürekli olarak belirli bir görüntüyü eş zamanlı olarak takip eder. Buna karşılık video kameralar aynı görüntüyü deyimli yerindeyse nokta nokta taramakta ve aktarıldığı yerde yeniden oluşturulmaktadır. Bu açıdan kamera taramaları sayfanın bir köşesinden diğer köşesine hareketini tamamlayan bir daktilonun işleyişine benzetilmektedir¹⁶⁹. Tek renk, renkli ya da kızılötesi termal kameralar dahil tüm kamera çeşitleri bu şekilde görüntü toplamaktadır.

Video kameraların farklı çeşitleri bulunmaktadır. Bu farklı çeşitler analog kameralar, dijital kameralar, internet kameraları (IP kameralar), LLL (low light level) kameralar ve termal kameralar olarak karşımıza çıkmaktadır. 2000'li yıllara kadar neredeyse kullanılan tüm güvenlik kameralarının analog kameralardan oluştuğunu söylememiz mümkündür. Bu kameralar tek renk analog ve renkli analog kameralar olarak ikiye ayrılmaktadır. Daha sonraki dönemde ise dijital sinyal işleme (DSP) sistemlerinin entegre olmasıyla bu kamera türü yerini dijital kameralara bırakmaya başlamıştır. Yine buna paralel olarak analog kameralarda çalışan kayıt sistemleri olan VCR (Video Cassette Recorder)'ların yerini DVR (Digital Video Recorder) sistemleri almış, bu durum ise video kayıtlarına daha kolay erişim olanağı sağlamış ve maliyetleri azalmıştır¹⁷⁰.

Analog kamera sistemlerinin bir başka dezavantajı ise bu sistemlerde kameralar ile kayıt cihazı arasında kablo bulunması zorunluluğu, sınırlı sayıda kamera giriş sayısı olan kayıt

¹⁶⁹ Herman KRUEGLE, Frank ABRHAM, CCTV Surveillance: Analog and Digital Video Practices and Technology, Butterworth-Heinemann, ABD 2006, s. 109.

¹⁷⁰ A.g.e., s. 120.

cihazlarında fazla sayıda kamera kullanılmasının imkansız olması gibi durumlar geniş çaplı gözetim için analog sistemlerin kullanımını zorlaştırmaktadır. Dijital kameralar ise sensör, bilgisayar destekli dönüştürücü, dijital ID kamerası ve dijital video kaydedicisi unsurlardan oluşan ve işletim sistemi olarak dijital sinyal işlemcisi kullanan kameralardır. Dijital kameraların çözünürlük oranı analog kameralara göre çok daha fazladır¹⁷¹.

Teknolojinin gelişmesi ile birlikte karşımıza çıkan, yeni bir kamera türü de İnternet Protokolü (IP) kameralarıdır. Bu türde kameralar, kayıt ve monitörler bir yerel ağa veya internet gibi geniş çaplı bir internet protokolü (IP) ağına bağlanmaktadır. İnternet bağlantı ağı içerisinde (aynı bir web sayfası açmak, mail göndermek ya da dosya transfer etmek işlemlerinde olduğu gibi) veriler hedeflenen başka bir cihaza aktarılmaktadır¹⁷². Bu sistemde her kamera için ayrı bir kablo kullanılmasına gerek kalmayacağı için kullanımları daha kolaydır. Analog ve dijital kameraların bir arada kullanıldığı karma kapalı devre kamera sistemleri de bulunmakla birlikte, uzun vadede orta ve büyük çaplı kapalı devre görüntüleme sistemlerinin IP kameralar ve dijital sistemlerden oluşacağı öngörülmektedir¹⁷³. IP kameraların kullanımlarının artmasının yanı sıra yine son dönemde sıkça kullanılan, özellikle şirketler tarafından ucuz ve erişiminin kolay olması sebebiyle tercih edilen bulut veri tabanlarının bu kameralarla birlikte kullanımına sık rastlanılmaktadır.

Bulut teknolojisi ilk defa 1996 yılında bir MIT araştırma makalesinde internet ile bağlantılı olarak kullanılmıştır. Ancak popüler hale gelmesi 2006 yılında Google Ceo'su Eric Schmidt tarafından şirketin veri hizmetlerini sunucularda muhafaza etme stratejilerini açıklanması sırasında kullanılmasıyla olmuştur¹⁷⁴. Bulut teknolojisi kullanan kullanıcıların cihazlarında bir depolama donanımı ya da işlem gücünün bulunmasına gerek yoktur. Bunun yerine bu teknik altyapılar başka bir yerde yani bulutta bulunur. Böylelikle cihazların daha ince tasarımlarımla, daha hafif ve taşınması daha kolay şekilde üretilmesi sağlanmaktadır. Ancak yine de IP kameralar tarafından toplanan görüntülerin bulut temelli video depolama sistemine aktarılması hususunda bir takım güvenlik zafiyetlerinin oluşabilecek ve veri koruma yönünden

¹⁷¹ A.g.e., s. 120.

¹⁷² Steven J. MURDOCH, Ross ANDERSON, Tools and Technology of Internet Filtering, Ronald DEIBERT, John PALFREY, Rafal ROBOZINSKI, Jonathan ZITTRAIN (Ed.), Access Denied: The Practice and Policy of Global Internet Filtering, The MIT Press, ABD 2008, s. 57.

¹⁷³ Cüneyt AKINLAR, Yusuf OYSAL, Hüseyin POLAT, Efnan GÜNAL, s. 90.

¹⁷⁴ Ulrik Christian ANDERSEN, Bro Soren POLD, The Metainteface: The Art of Platforms, Cities, and Clouds, The MIT Press, ABD 2018, s. 121.

sorunlar gündeme gelebilecektir. Bu sistemlerin uygulamaya konulması konunun bu yönden de değerlendirilmesi önemlidir¹⁷⁵.

IP kamera sistemleri ile elde edilen video görüntüleri bazı maskeleyme teknikleri kullanılarak maskelenip (örneğin; kameralara yansıyan yüz bilgisi ya da araç plaka numarası maskelenmektedir) şifrelendikten sonra internet ağı içerisinde bulut sistemlerinde bu şekilde yedeklenmektedir. Böylelikle veri gizliliğine dair temel kaygılar bir ölçüde giderilmiş olacaktır¹⁷⁶. IP kamera ile bulut veri tabanı arasındaki veri akışına ilişkin maskeleyme ve şifreleme işlemleri nedeniyle bu sistemlerin diğer benzer kamera güvenlik sistemlerine göre daha güvenli hale geldiğini söyleyebiliriz.

Diğer bir kamera türü olan LLL (low light level) kameralar ise ışığın az olduğu ortamlardan görüntü toplayabilmek için tasarlanmıştır. Bu kamera türünde hedef alandaki ışık seviyesini yükseltmek için bir görüntü yoğunlaştırma aracı bulunmakta olup, böylelikle kameraların çok daha düşük ışıklı ortamlarda (yapay ışıklar, ay ışığı vb.) kullanılması mümkün olmaktadır. Bu kameraların içerdikleri görüntü yoğunlaştırıcılar, gece koşullarında binlerce kilometre uzaktaki nesnelerin görüntülenmesini sağlayabilmektedir¹⁷⁷.

Bir diğer kapalı devre kamera türü olan termal kızılötesi kameralar ise uzun dalgalı kızılötesi kullanmakta olup üretimleri diğer kamera sensörlerine göre daha zordur. Bu kamera türünde toplanan sensördeki piksel sayısı diğer türlere göre daha azdır ve daha düşük verimle çalışması mümkündür. Son dönemde bu sorunların ortadan kalktığı çok daha efektif termal kameraların üretildiği görülmektedir. Termal görüntüleme sistemleri sadece sıcaklık yaymakta olan nesnelerden dağılan ısıya tepki vermeleri nedeniyle vücut sıcaklıklarının tespiti hususunda kullanılmaktadır. Yine bununla birlikte katı hal kamera sensörlerinin (günümüzde kullanılan bir çok kamera bu sensörleri kullanmaktadır) görüntü toplamasına yarayacak bir görselin tespit edilemediği gece ya da ışısız ortamlarda gece görüşü amacıyla da kullanılmaktadır¹⁷⁸.

¹⁷⁵ Cengiz PAŞAOĞLU, Emel CEVHEROĞLU, Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması, Bilişim Teknolojileri Dergisi, C. 13, S. 2, Nisan 2020, s. 183-195.

¹⁷⁶ Choi Il KANG, Lee Hee JUNG, Bhum Cheol LEE, Cloud Based Video Storage System With Privacy Protection, 17th International Conference on Advanced Communication Technology (ICACT), 2015, s. 463.

¹⁷⁷ Herman KRUEGLE, Frank ABRHAM, s. 125.

¹⁷⁸ A.g.e., s.117.

Kapalı devre kamera sistemlerinin bir diğer unsuru video kayıt cihazıdır. Kayıt cihazları kameralar vasıtasıyla aktarılan görüntü verilerinin gün, saat, dakika, saniye ve salise bilgisi ile işaretlenerek depolanmasını sağlamaktadırlar. Teknolojinin gelişmesi ve analogdan dijitale doğru gelişmeyle, eskiden video kasetlerde tutulan kayıtlar artık sabit disklerle depolanmaya başlanmıştır. Bu durum hem depolanma alanlarında küçülmeye hem de maliyetlerin azalmasına sebebiyet vermiştir. Bireylerin kişisel verileri sayılan bu kayıtların ne kadar süre ile kayıtlı tutuldukları, başka ortamlara aktarım olup olmadığı ya da internet gibi açık tabanlı bir ortamda sistemin dışarıdan gelen müdahalelere ne kadar dayanıklı olduğu hususları ilerdeki bölümlerde incelenecektir.

Bir diğer unsur ise görüntüleme cihazları yani monitörlerdir. Bir kapalı devre kamera sisteminde kameralar tarafından elde edilen görüntülerin gösterildiği en az bir adet monitör bulunmaktadır¹⁷⁹. Bununla birlikte video görüntüleme cihazları yani monitörlerin de farklı çeşitleri bulunmaktadır. Video monitörleri tek renk monitörler, renkli monitörler, CRT (Cathode Ray Tube), LCD (Liquid Crystal Display), plazma ve bilgisayar ekranlarından oluşmaktadır¹⁸⁰. CRT monitörler maliyetleri daha düşük olan ve daha az enerji tüketiminde bulunan LCD, plazma ve OLED (Organic Light Emitting Device) gibi yeni monitör sistemleri karşısında artık kullanılmaz hale gelmiştir. Kameralardan gelen videoların görüntülendiği bu ekranlar, daha büyük çaplı organizasyonlarda yerini kontrol kumanda merkezlerine bırakmıştır. Örneğin, bir mağazadaki güvenlik kameralarının video kayıtlarının görüntülendiği sistem çoğu zaman o işyerinde kullanılan bir bilgisayar iken, şehir gözetim sistemlerinin (örn; Mobese) kumanda odaları bulunmaktadır. Kumanda merkezlerinin görüntüleri izledikleri alanlara eş zamanlı olarak müdahalede bulunabilmeleri için bir çok monitöre ses aktarımı sağlayan mikrofonların entegre edildiği de görülmektedir.

Teknolojinin gelişmesi ve teknolojiye erişimin kolaylaşmasıyla kapalı devre kameralar birçok alanda kullanılmaya başlanmıştır. Kullanılmasındaki temel amaç güvenliğin sağlanması olan bu sistemler sadece kamu binalarının önlerinde, askeri alanların sınırlarında, küresel ölçekli firmaların bina önlerinde değil, her evin önünde her işyerinde kullanılabilir hale gelmiştir. Kapalı devre kameralar artık şehir merkezlerinde, meydanlarda, sokaklarda, otobanlarda, parklarda, işyerlerinde, okullarda, hastanelerde, üniversitelerde, tren, metro ve

¹⁷⁹ Cüneyt AKINLAR, Yusuf OYSAL, Hüseyin POLAT, Efnan GÜNAL, s. 87.

¹⁸⁰ Herman KRUEGLE, Frank ABRHAM, s. 41.

tramvay istasyonlarında, havalimanlarında kullanılmaktadır. CCTV sistemlerinin bulunmadığı bir kamusal alan hayal etmek çağımızda imkansız gibi gözükmektedir.

Bunlara ek olarak kapalı devre kamera sistemlerinin sadece bir yere sabit olarak konumlanmak suretiyle çalıştıklarını anlamak yanlış olacaktır. Sabit konumlandırılan kameralar yanında, taşınabilir kameraların da gözetim amacıyla kullanıldıklarını görebilmekteyiz. Örneğin; gece bekçilerinin nöbetleri sırasında yakalarına yerleştirdikleri kameralar (yaka kameraları) ya da polislerin görevleri sırasında taktıkları vücut kameraları bunlardandır¹⁸¹.

İKİNCİ BÖLÜM

BİR GÖZETİM TEKNİĞİ OLARAK KAPALI DEVRE KAMERALARIN KULLANILMASI

Kapalı devre televizyon sistemlerinin günümüzde etrafımızı çevirdiği ve gerçekten de kendi mahremiyet alanımız olarak gördüğümüz evlerimizden dışarıya adımımızı atar atmaz büyük çaptaki bir kamera gözetiminin içinde yer aldığımız söylenebilir. Mağazalarda, alışveriş merkezlerinde, tramvay ve metro istasyonlarında, meydanlarda hem devletin hem de özel teşebbüslerin kameralar aracılığıyla bireyleri gözetledikleri ve bunu panoptik sistemdekine benzer şekilde, güvenliği sağlama ve insanları kurallara uygun davranmaya yönlendirme amaçlarıyla yaptıkları görülmektedir¹⁸².

Kamusal alanların neredeyse tamamında kapalı devre kameraların kullanıldığını görmekteyiz. Trafik kameraları (örneğin; Türkiye’de Mobese ve Elektronik Denetim Sistemi) trafikte araçların hızını izleyip kayıt altına alırken diğer birçok yerde, caddelerde, mağazalarda, özel okullarda, hastanelerde ve bankalarda kamera gözetimi yapılmaktadır. İnsanlar bu alanlarda gördükleri *“bu alan kapalı devre kamera kaydı ile 7/24 kayıt altına alınmaktadır”* şeklindeki uyarıları düşünmeden kabul etmektedirler ve bu gözetim araçlarından kaçış mümkün değildir¹⁸³. Günümüzün derinleştirilmiş ekranları eskiye göre gözetleyenlere çok daha geniş bir

¹⁸¹ Meghan E. HOLLIS, *Securitiy or Surveillance, Examination of CCTV camera usage in the 21st century*, CCTV Surveillance or Crime Prevention, Criminology & Public Policy, S. 18, Y. 2019, s.131.

¹⁸² Elif KÜZECİ, *Kişisel Verilerin Korunması*, s. 60.

¹⁸³ David LYON, *Gözetlenen Toplum*, s. 102.

görüş açısı sağlamakta olup, bireyler video görüntüleri üzerinden ekranlar vasıtasıyla tespit edilebilmekte ve bu tarz bir görüntüleme sistemi aynı zamanda bir kimlik tanımlama sistemine ya da en azından bir doğrulama prosedürüne bağlı olabilmektedir¹⁸⁴. Böylelikle gözetleyen kamusal otoritenin ya da özel hukuk tüzel veya gerçek kişinin gözetlenen kişi hakkında daha fazla bilgi sahibi olmaları mümkün olmaktadır. Bu bakımdan gözetimi gerçekleştirenlerin işlerinin kolaylaşacağını ifade etmek yanlış olmayabilir. Bu bölüm içerisinde kapalı devre kameraların gözetim tekniği olarak nasıl kullanıldıkları, bu kullanıma bağlı olarak değişen hukuki nitelikleri, kanuni dayanağının neler olduğu, hangi alanlarda ve hangi amaçlara yönelik olarak kullanıldığı gibi hususlarda açıklamalara yer verilmiştir.

I. Kapalı Devre Kamera Sistemlerinin Hukuki Niteliği

Kapalı devre kameraların kullanımlarının büyük ölçüde artmasında bu sistemlerin insanların ve malların güvenliğini sağlama açısından kullanılmaları etkili olmuştur. Güvenlik endüstrisi içerisindeki gelişmelere bağlı olarak 1960'lı yılların başında ilk olarak video görüntüleme sistemleri ile alarm sistemleri birleştirilmeye başlanmıştır. Birtakım şirketler (Motorola, Radio Corporation of America ve General Electric) bu dönemde başı çekmek suretiyle dönemin teknolojik sınırları dahilinde video kamera tüplerini sektörle buluşturmuşlar ve bu teknoloji 1990'lı yılların sonlarına kadar kullanılmıştır. İzleyen dönemlerde teknolojiye bağlı olarak video kayıt endüstrisi dijitalleşmiş ve özellikle uzaktan uzağa video aktarımlarının yapılması savunma sanayinde bir gereksinimi karşıladığı için bu video sistemlerinin internet altyapısına entegre edilmeleri sağlanmıştır¹⁸⁵.

Araç olarak kullanılan sistemler bu şekilde evrilirken, bunun karşılığında bu sistemlerin kullanılma amaçlarının (güvenlik, suçun önlenmesi ve adaletin sağlanması, denetim, eğitim vb.) çok fazla değişmediğini söylemek mümkündür. Bununla birlikte CCTV sistemlerinin hukuki nitelikleri ise amaca göre şekillenen kullanımlara bağlı olarak değişmektedir. O halde CCTV sistemlerinin nasıl kullanıldıklarının tasnifinin yapılması gerekir. Kapalı devre kamera sistemlerini hiçbir şekilde kayıt yapmayan sistemler, kayıt yapmayan fakat izleme yapan sistemler, hem kayıt hem izleme yapan sistemler ve yapay zeka ya da diğer teknolojik uygulamalar entegre edilmiş sistemler olarak ayırtmamız mümkündür.

¹⁸⁴ David LYON, Vesikalı Yurttaş , Gözetim Aracı Olarak Kimlik Kartları, çev. Barış Baysal, Kalkedon, İstanbul 2012, s. 137.

¹⁸⁵ Herman KRUEGLE, Frank ABRHAM, s.3.

Hiç bir şekilde kayıt yapmayan kameraların kullanıldığı sistemler tamamen gözetlenen tarafın algısını yönetmek amacıyla kullanılmaktadır. Bu sistem içerisinde daha sonra açıklayacağımız tüm diğer sistemlerden farklı olarak bir gözetleyen bulunmamaktadır. Aslında çalışmayan, sahte bir CCTV'nin bina dışında konumlandırılması böyledir. Yine de sahte CCTV kullanılarak yapılan gözetimin birey açısından zararlı olmadığı gibi bir kesinlik söz konusu değildir.

Bu sistemdeki kameralar gözetlenen bireyler tarafından her açıdan görülebilecek, hedef alanların en dikkat çekici noktalarına konumlandırılmaktadır. Elbette ki bu sahte CCTV'nin kullanılması ile herhangi bir kişisel verinin işlenmediğini söylemek mümkündür. Fakat daha sonraki bölümde aktaracağımız üzere özellikle özel yaşamın gizliliği ve Anayasa'da yer alan "Kişinin Hakları ve Ödevleri" başlığı altındaki en önemli temel haklardan bir tanesi olan "kişinin dokunulmazlığı, maddi ve manevi varlığını koruma ve geliştirme hakkı"nı göz önünde bulundurarak, bireylerin kendilerini geliştirmelerine ket vuran bir yönü olduğunu belirtmemiz yerinde olacaktır. Çünkü kameranın sahte olup olmadığını anlama gücüne sahip olmayan birey izlendiğini düşünerek belirli bir hareketi yapma ya da yapmama gibi iradesi dışında hareket edebilecektir¹⁸⁶.

Normalde CCTV sistemleri neredeyse her zaman kayıt araçları ile birlikte çalışmakta ve güvenlik personelleri ya da diğer gözetleyenler tarafından izlenmekte ve arka planda izlenen görüntülerin kayıt altına alınması sağlanmaktadır. Fakat bazı durumlarda kayıt ve muhafaza işlevi söz konusu olmaz ve sadece izleme gerçekleştirilir. Kayıt yapmayan ve izleme yapan kameralar olarak nitelendirdiğimiz bu sistemler çoğunlukla güvenlik gerekçeleri ile belirli alanların izlenmesi için kullanılan sistemlerdir. Bunlara örnek olarak havalimanlarına, alışveriş merkezlerine, stadyumlara ya da diğer kamusal alanlara girişlerde yer alan güvenlik personelinin önünde bulunan ve anlık gözetleme gerçekleştirilen ekranları vermemiz mümkündür.

Bu tür kapalı devre kamera sistemlerinin kişisel verilerin korunması açısından hem izleme hem de kayıt yapan kamera sistemlerine göre daha tercih edilebilir olduğunu söyleyebiliriz. Bu şekilde gerçekleştirilecek bir veri işleme faaliyetinin 6698 sayılı Kişisel

¹⁸⁶ Bkz. aşı., s. 139.

Verilerin Korunması Kanunu (KVKK)'nın genel hükümleri arasında yer alan verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesine ve veri işlemenin mümkün olduğunca azaltılması ilkesine uygun olduğu görülmektedir. Kayıt yapan kameralar ise işlenen verilerin aynı zamanda kaydedilerek daha fazla veri işlenmesine sebebiyet verebilecek ya da bu kayıtların ne kadar süre boyunca tutulacak olduğu ya da kimlerle paylaşılabilceği konularında verilerin korunmasına bağlı riskleri gündeme getirebilecektir. Kayıt yapmayan sadece izleme yapılan kameralar ile kayıt ve izleme yapılan kameralar arasında bir ayrıma da Avrupa İnsan Hakları Mahkemesi (AİHM) gitmiştir. AİHM'e göre, sadece izleme yapılan ve kayıt yapmayan kameraların Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesinde yer alan "Özel Hayata Saygı" hakkına daha az müdahale yaratacağı açıkça belirtilmiştir¹⁸⁷. Bu değerlendirme kameraların hukuki niteliğinin tespiti bakımından gerçekten büyük önem taşımaktadır.

Bir kapalı devre kamera sistemi dahilinde görüntülerin sadece izlemeye konu olması dışında eğer bu görüntüler kayıt altına da alınıyorsa, bu sistemleri hukuki yönden farklı nitelendirmemiz mümkün olacaktır. Nitekim veri işleyenler tarafından gerçekleştirilen veri işleme faaliyetleri de çeşitlenmiş olmaktadır. Verilerin izlenmesi ve kaydedilmesi işlemlerinin KVKK'nın 3. maddesine göre farklı veri işleme faaliyetleri olarak görüleceğini söylemek mümkündür. Madde metninde kişisel veriler için "*Kişisel verilerin...elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem...*" şeklinde belirtilen tüm işlemlerin ayrı ayrı birer veri işleme faaliyeti olarak görüldüğü belirtilmektedir. İşleme faaliyetlerinin çeşitlenmesi ve izleme dışında kayıt faaliyetinin de eklenmesi ölçülülük değerlendirmesi yapılmasını gerektirebilir. Yani kişisel verinin sadece izlenmesi yoluyla ulaşılmak istenen amaca erişim mümkün ise beraberinde kayıt yapılması durumunda bu veri işleme faaliyetinin ölçüsüz olarak gerçekleştirildiğini söylemek mümkün olabilecektir. Keza bireylerin video görüntülerinin anlık olarak bir kameradan herhangi bir ekrana yansıtılarak izlenmesi dışında, izlenen verilerin belirli bir konumda depolanması verilerin korunması bakımından alınması gereken teknik tedbirlerin alınıp alınmadığı sorusunu da gündeme

¹⁸⁷ Peter Alexander EARLS DAVIS, "Facial Detection and Smart Billboards: Analysing the 'Identified' Criterion of Personal Data in the GDPR", European Data Protection Law Review (EDPL), , C. 6, S. 3, Y.2020, s. 370. Bu değerlendirmeyi içeren kararlar için bkz. Pierre Herbecq and the Association "Ligue des droits de l'homme", Belçika'ya karşı, b.n. 32200/96, k.t. 14 Ocak 1998; Perry, Birleşik Krallık'a karşı, b.n. 63737/00, k.t. 17 Ekim 2003; Peck, Birleşik Krallık'a karşı, b.n. 44647/98, k.t. 28 Ocak 2003.

getirecektir. Verilerin kaydının tutulduğu alanların yetkisiz erişimlere karşı korunması gerekeceği gibi, ilgili mevzuatta öngörülen bir süre ya da işlendiği amaç için gerekli olan süre geçtikten sonra verilerin silinmesi gerekecektir.

Diğer kapalı devre kamera sistemleri dışında hem kayıt yapan hem de yüz tanıma ya da benzeri yapay zeka entegrasyonları kullanan kapalı devre kamera sistemleri de bulunmaktadır. Bu kamera sistemlerinin içerisine istenilen amaca yönelik olarak gelişmiş bir takım yapay zeka uygulamalarının konumlandırıldığını görmekteyiz. Örnek vermemiz gerekirse daha önce de belirttiğimiz gibi trafikte araç sayan, kişilerin belirli bir yere giriş çıkışını takip eden, keza sınır bölgelerindeki geçişleri izleyen kamera sistemleri daha önceki dönemlerde insanların gücünden faydalanılarak gerçekleştirilen gözetim faaliyetlerini otomatikleştirmiştir.

Bu tanıma uyan teknolojilerden bir tanesi insan hareketlerini takip eden (Human Pose Estimation) algoritmaların kurulu olduğu CCTV'lerdir. Burada bahsettiğimiz teknoloji aslında sinir ağları teknolojisi olarak da nitelendirilmektedir¹⁸⁸. Böylelikle bilgisayar sistemlerine yüklenen büyük veri setleri ve yapay zeka sayesinde insan hareketlerini tespit etme ve anlamlandırma mümkün olmaktadır¹⁸⁹. Kullanım alanlarına dair örnek vermek gerekirse, sınır güvenliklerinde yer alan kameralar, insan geçişini ya da araç geçiş sıklığını sayan kameralar bunlardandır.

İnsan hareketlerinin takibi son yıllarda çok daha fazla önem kazanmış ve bu teknolojiyi geliştirmeye yönelik çalışmalar hızlanmıştır. Buna karşılık kullanılan veriler bütünü ise analiz edilmesi zor bir hale bürünmüştür. Bu zorluğun ortadan kaldırılması için çalışmalar yapılmış, bu konuya ilişkin farklı çözümler geliştirilmiştir. Bu kapsamda fazla miktardaki farklı veriyi barındıran veri setlerinden anlamlı bir sonuç çıkarmak görevi yapay zekaya verilmiştir. Örneğin; Coco adı verilen bir uygulama iki yüz binden fazla fotoğraf ve 250.000 kişinin görüntüsünden oluşan bir veri seti üzerine kurulmuştur. Pose Track adlı bir diğer uygulama ise video kayıtlarını temel veriler olarak almakta ve veri seti içerisinde 66.0000 fazla tekli kare içeren 514 video kaydı barındırmaktadır¹⁹⁰. İnsanların göz hareketlerini, mimiklerini ya da el

¹⁸⁸ Benny PLATTE, Rico THOMANEK, Tony ROLLETSCHEKE, Christian ROSCHKE, Marc RITTER, "Person Tracking and Statistical Representation of Person Movements in Surveillance Areas", International Journal of Design, Analysis and Tools For Integrated Circuits And Systems, C. 7, S. 1, 2018, s. 21.

¹⁸⁹ A.g.m., s. 21.

¹⁹⁰ Bin XIAO, Haiping WU, Yinchun WEI, "Simple Baselines for Human Pose Estimation and Tracking", European Conference on Computer Vision, 2018, s. 10. Burada belirtilen çalışma temelinde ortaya konulan

ve kol hareketlerini tespit etmeye yönelik olarak yaratılan yazılımlar insan hareketlerinin takibindeki gelişmeyi ortaya koymaktadır. Bu yönüyle kamera gözetimi ile geçişin yasak olduğu sınırdan geçen bir bireyin tespiti dışında daha da ileriye gidilerek, yoğun stres altında gözlerini kaçırarak bir insanın ne ölçüde içinde bulunduğu ortamla zihinsel ya da duyuşsal olarak bağlantısının olup olmadığı ortaya konulabilecektir.

Kalabalık alanlarda bireylerin hareketleri ve yüzlerinin tespit edilmesi de benzeri uygulamaların işleme konulmasını gerektirmektedir. Brainwash projesinde kullanılan veri setinde insan yüzlerinin tespiti için kullanılan uygulama OverFeat bu bakımdan örnek olarak gösterilebilir¹⁹¹. Brainwash projesi San Francisco’da bulunan bir kafenin (Brainwash Cafe) ziyaretçilerinin üç gün boyunca kaydedilen fotoğraf görüntülerinden oluşan veriler bütününe bireylerin haberi ya da herhangi bir izneleri olmaksızın bir webcam (web kamerası) aracılığıyla kayıt altına alınması ile başlatılmıştır. Stanford Üniversitesi tarafından yürütülen bu projede toplanan görüntüler yüz tanıma sistemlerinin algoritmalarının beslenmesi amacıyla gözetim sektöründe, akademik, ticari ya da askeri amaçlarla kullanılmıştır. Veri seti toplamda 11.917 adet fotoğrafın bir araya gelmesinden oluşurken, 81.973 adet insan yüzü görüntülerde yer almıştır. Amerikan Savunma Bakanlığı’nın da desteği ile 2015 yılında tamamlanan çalışma veri setinin büyüklüğü itibarıyla önemli görülmekte olup, bu veri seti 2016 ve 2017 yıllarında ayrıca Çin Savunma Teknolojileri Ulusal Üniversitesi tarafından da kullanılmış, ardından üniversitenin dijital arşivlerinden kaldırılmıştır. Aradan geçen zaman göz önünde bulundurulduğunda günümüz itibarıyla veri setinin üniversitenin dijital arşivlerinden kaldırılmış olması yerinde bir hareket olmuştur. Bu durumun bireylerin mahremiyetlerinin korunması için gerekli olduğu değerlendirilebilir¹⁹².

Yapay zekanın videolardaki hareketleri tespit ederek, anomalileri tespit etmesinin mümkün olduğu görülmektedir¹⁹³. Gelecek dönemde ise yüzünde maske olan ve sadece kaşları görülen bir kimsenin, kaş özelliklerinden kimlik tespitinin gerçekleştirilmesi amaçlanmaktadır.

ve insan hareketlerinin takibinde başarılı olan uygulamaya ilişkin kod bilgisi bu internet sitesinde yer almaktadır. Bkz., https://github.com/NVIDIA-AI-IOT/trt_pose (s.y. 18 Ekim 2021)

¹⁹¹ İnsan hareketlerinin tespiti ve takibi teknik bakımından videoları oluşturan her bir kamera görüntüsünün parçalara ayrılması ve şifrelenmesinden sonra bu görüntülerin bir LSTM algoritması tarafından işlenmesi sayesinde gerçekleştirilir. Ayrıntılı bilgi için bkz. Russell STEWART, Mykhaylo ANDRILUKA, Andrew Y. NG, End-to-End People Detection in Crowded Scenes, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, s. 2331.

¹⁹² Brainwash projesi hakkında detaylı bilgi için bkz. <https://exposing.ai/brainwash/> (s.y. 02 Kasım 2021), <https://purl.stanford.edu/sx925dc9385> (s.y. 02 Kasım 2021)

¹⁹³ Joseph GEORGE, Sreelakshmi RAMCHANDRAN, Nezmi K. A. , Shreya NAIR, “Video Surveillance Using Deep Learning”, Journal of Critical Reviews, C.7, S. 9, 2020, s. 2949.

Şüphesiz bulunduğumuz dünyada bir insanın sadece kaç özelliklerinden bir şüpheliyi teşhis etmek çok zordur. Buna karşılık yapay zekanın bunu mümkün hale getirmesi, suçun önlenmesi ve güvenliğin sağlanmasında yapay zekanın gözetim tekniği olarak kullanımının ne kadar önemli olduğunu bizlere gösterir¹⁹⁴.

Yapay zekanın algılama, planlama, akıl yürütme, öğrenme, iletişim kurma, karar verme ve hareket etme yoluyla rasyonel olarak belirli bir hedefe ulaşan akıllı yazılımlar ya da bedenlenmiş robotlar olarak görülmesi mümkündür¹⁹⁵. Teknolojinin gelişmesi dahilinde geniş alanlarda yapay zeka ile otomatik gözetim yapılarak, belirli bir alandaki sorunlu davranışlar kolaylıkla tespit edilebilmektedir. Örneğin; alarm sistemlerinin çalıştırılması bakımından yapay zeka ve CCTV'ler birlikte çalıştırılabilir¹⁹⁶. Kapalı bir kapının açılması ya da yangın çıkması durumunda kapalı devre kameraya yerleştirilen yapay zeka algoritması dahilinde sorun tespit edilip, doğrudan müdahale sağlanabilecektir¹⁹⁷.

Avustralya'daki Swinburne Teknoloji Üniversitesi'nin kullandığı iCetana sistemi kampüste içerisinde kullanılmaktadır. Bu sistem kameralardan aldığı görüntü kayıtlarını yapay zeka dahilinde normal hareket şekilleriyle karşılaştırmakta ve anomalileri tespit etmektedir. Bu anomaliler kapsamına düşme, yumruklaşma gibi kampüste istenmeyen herhangi bir davranış girebilecektir¹⁹⁸. Nitekim normal şartlarda insanlar tarafından yapılan video izleme faaliyetlerinin tamamen otomatikleştirilmesi yani görüntüleme ve izleme faaliyetlerinin bilgisayarlar tarafından yerine getirilmesi, bir bilgisayarın gerçek zamanlı kimlik tespitine yönelik olarak insandan çok daha hızlı olduğu göz önüne alındığında, bu sistemlere yönelik olan talepleri artırabilir. Bir meydana gezen turistlerin güvenlikleri ya da şehirde yer alan risk

¹⁹⁴ A.g.m., s. 2955.

¹⁹⁵ Dan HUNTER, Mirko BAGARIC, Nigel STOBBS, "A Framework for the Efficient and Ethical Use of Artificial Intelligence in the Criminal Justice System", Florida State University Law Review, C. 47, S. 4, Y.2020, s. 755

¹⁹⁶ Bu örnekte alarm sistemlerinde yapay zekanın entegrasyonun olumlu olacağı düşünülebilir. Ancak geçmişte yaşanan bir takım kötü deneyimlerden bahsetmek de mümkündür. Örneğin; yüz tanıma teknolojilerinin 2006 yılında Almanya'da Federal Polis Bürosu tarafından kullanılmaya başlanmasıyla yanlış alarm oranlarında yaşanan yükselmeler polislik faaliyetlerinin efektif bir şekilde yerine getirilmemesine neden olmuştur. Bu sorunlar sistemin bekleneni vermemesine karşılık bireylerin gizliliğine müdahalede bulunduğu savının ileri sürülmesine neden olmuştur. Bkz. Norma MÖLLERS, Jens HÄLTERLEIN, "Privacy issues in public discourse: the case of "smart" CCTV in Germany", Innovation: The European Journal of Social Science Research, C. 26, S. 1-2, 2013, s. 60.

¹⁹⁷ Söz konusu anomalilere müdahalenin gerçekleştirilmesi açısından yapay zekanın "bedenlenmesi" hususu önem taşır. Fiziksel dünyada eylem halinde olan yapay zekanın "robotik" olarak tanımlanması mümkündür. Yapay zekanın fiziksel ortama uyum sağlayan robot bedenler içerisinde çalışması sosyal ortamda güçlü bir değişim yaratabilecektir. Bu husustaki değerlendirme için bkz. Elif KÜZECİ, Sayısal Fil, s. 143.

¹⁹⁸ Dan HUNTER, Mirko BAGARIC, Nigel STOBBS, s. 769.

bölgelerindeki tehditler anında gerçek zamanlı olarak tespit edilebilecek ve gerektiğinde önlenebilecektir. Ayrıca gözetim sırasında toplanan verilerin aynı sistemler aracılığıyla çok daha hızlı arşivlenmesi ve daha sonradan kullanılmak üzere bir veri tabanı oluşturması işlemleri, yapay zeka ile çok daha hızlı gerçekleştirilecektir. Özetle, gözetim ve yapay zeka eşleşmesi karşısında, insan ve gözetim teknolojileri artık zayıf bir eşleşme olarak görülmektedir¹⁹⁹.

Stanford Üniversitesi'nin Brainwash projesinin dışında diğer üniversitelerin de benzer yüz verisi tarama ve toplama faaliyetleri yürüttükleri görülmüştür. Duke Üniversitesi'nden araştırmacılar 2014 yılında kampüste yer alan 8 adet kamera üzerinden 2 milyondan fazla video görüntüsü toplamışlardır. Bu veri toplama çalışmaları kamuoyunda özellikle toplanan verilerin sınır ötesine aktarıldığı, yabancı devletler ve askeri aktörlerle paylaşıldığı gibi sebeplerle gerginlik yaratmıştır. Yapay zeka ile yüz tanıma sistemlerinin vazgeçilmezi olan yüz görüntüleri sadece üniversiteler tarafından yürütülen projelerde kullanılmamakta aynı zamanda özel şirketler de kendi amaçları doğrultusunda bu yönde çalışmalar gerçekleştirmektedirler²⁰⁰. Microsoft firması tarafından MSCeleb, IBM firması tarafından yapılan "Diversity in Faces" projeleri buna örnek olarak gösterilebilir²⁰¹.

Bu teknolojiyi kullanan diğer şirket olan Facebook'un yüz tanıma teknolojisi kullanarak dijital fotoğraf albümlerindeki kullanıcıların tanımlanmasına yönelik olarak Aralık 2010 tarihinde getirmiş olduğu yüz etiketleme özelliğinin kapatılacağı duyurulmuştur. Buna gerekçe olarak kullanıcıların mahremiyetleri bakımından endişelerini, hükümetin baskısını ve bu alandaki düzenleyici kuralları sebep gösteren şirket bu faaliyetlerde kullanılan bir milyar kullanıcının yüz taramalara verilerinin de silineceğini belirtmiştir. Şirketin 2019 yılında geçirdiği soruşturma sonucunda Federal Ticaret Komisyonu ile 5 milyar dolarlık rekor bir uzlaşmaya imza attığı, uzlaşmaya konu olan konulardan bir tanesinin de yüz tanıma

¹⁹⁹ Ray SURETTE, Haroon IDREES, Mubarak SHAH, "Enhancing Camera Surveillance Using Computer Vision: A Research Note", Policing: An International Journal, C. 41, S. 2, 2018, s. 263.

²⁰⁰ Facial Recognition Tech Is Growing Stronger, Thanks to Your Face, <https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html> (s.y. 05 Kasım 2021)

²⁰¹ IBM tarafından 2019 yılında yürütülen IBM Diversity in Faces projesi kapsamında bir milyon yetmiş bin adet fotoğraf arşivlenmiştir. Ayrıntılı bilgi için bkz., Michele MERLER, Nalini RATHA Rogerio FERÍS, John R. SMITH, Diversity in Faces, IBM Research AI, Nisan 2019, s. 2.; IBM tarafından yüz tanıma sistemlerinin daha isabetli ve adil çalışabilmesi için gerekli düzenlemelerin yapılması amacıyla gerçekleştirilen bu proje, kamuoyuna açıklanmasından sonra fotoğrafı ve biyometrik bilgileri rızası olmaksızın kullanılan bir kişi tarafından mahkeme önünde dava edilmiştir. Ayrıntılı bilgi için bkz. https://exposing.ai/ibm_dif/ (s.y.: 05 Kasım 2021)

teknolojilerine dair olduğu görülmüştür²⁰². Facebook'un en büyük dijital fotoğraf arşivine sahip şirketlerden biri olduğunu düşündüğümüzde, bireylerin yer aldıkları fotoğraflarda doğrudan etiketlenabiliyor olmalarının olumsuz birtakım sosyal etkileri olabilecektir. Ayrıca yüz tanıma teknolojilerinin uygulanmasına karar verip daha sonra bu uygulamadan vazgeçen ya da durduran başka büyük şirketlerde bulunmaktadır.

Almanya'da yapılan bir araştırma kapsamında üç gruba bölünen katılımcılarından birinci gruba standart CCTV gözetimi, ikinci gruba yapay zeka içeren CCTV gözetimi uygulanmış, üçüncü grup için ise herhangi bir gözetim faaliyetinde bulunulmamıştır. Çalışmanın sonucuna göre, yapay zeka içeren CCTV gözetimine maruz bırakılan grup diğerlerine göre daha fazla stres altında kalmış ve diğer gruplara kıyasen kameraların görüş alanlarından daha fazla kaçmaya çalışmalar ve kendilerine daha fazla çekidüzen vermişlerdir²⁰³. Yeni olan bu sistemlerin kurulması ve uygulamaya konulması insan hakları anlamında ve etik bir takım sorunları beraberinde getirebilir. Örneğin; havalimanı güvenliğinden geçmek üzere olan bir kimse bir anda arkasına dönüp koşmaya başladığında yapay zeka temelli bu yeni kamera sistemi bu hareketi bir tehlike olarak algılayabilir, çünkü algoritmasını besleyen veri setinde normal insan hareketinin bu olmayacağı yönünde bilgi barındırır. Fakat gerçek dünyada durum bu kadar kolay değildir. Yani bahsedilen kişinin aynı zamanda vedalaşmayı unuttuğu bir yakınına doğru koşuyor olması da ihtimal dahilindedir. Ancak bu görüşümüze karşıt olarak Alman Mahkemeleri tarafından verilen bir kararda ise yapay zeka içeren CCTV'nin geleneksel CCTV'ye göre hukuki yönden daha az müdahaleci olduğu belirtilmiştir. Mahkeme konuya ilişkin olarak “gizliliği ortadan kaldıran unsurun video görüntülerinin insanlar tarafından izlenmesi” olduğunu belirterek, bu nedenle akıllı kamera gözetiminin doğrudan insan gözetimine tercih edilebileceği ifade edilmiştir²⁰⁴.

Yüz tanımlama yazılımları kullanan kapalı devre kameralar için “*yüzleri kimliklere bağlamaktadır*” nitelendirmesini yapan Hodge'a göre, günümüzde bireylerin kimlikleri, bilgileri ya da rızaları olmaksızın bilgisayar ağında paylaşılmakta, dağıtılmaktadır²⁰⁵. Yüz tanımlama tekniği kullanan kameraların kullanımlarının kısıtlı olduğu zamanlar da

²⁰² Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System, <https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html> (s.y: 20 Ekim 2021)

²⁰³ Cornelius HELD, Julia KRUMM, Petra MARKEL, Ralf P SCHENKE, “Intelligent Video Surveillance”, in Computer, C. 45, S. 3, Y. 2012, s. 83.

²⁰⁴ A.g.m., s. 84.

²⁰⁵ Samuel J. HODGE, Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century, University of Cincinnati Law Review, C. 89, S. 1, Y. 2020, s. 58.

bulunmaktadır. Bu kısıtlılık görüntü kalitesinin zayıflığından, kameranın yüz açısını doğru yakalayamamasından ya da veri setinde yer alan ve eşleştirmeye yarayan fotoğrafların güncel olmamasından kaynaklanır. Bu yönde bir zayıflık sistemin etkililiğini azaltır ve sonucunda algoritmanın yapabileceği çok şey olmaksızın, yüz tanımlamada isabetsizliği beraberinde getirir. Buna ek olarak bu sistemin kullanılması sırasında karşılaşılabileceğimiz bir başka isabetsizlik durumu daha bulunmaktadır. Yapay zeka ile çalışan kapalı devre kamera sistemlerinin veri tabanlarının genel olarak beyaz erkek bireylerden oluşması nedeniyle bu sistemlerin azınlık gruplar, kadınlar ve genç yetişkin bireyler açısından daha az isabetli olduğu tespit edilmiştir²⁰⁶. Ayrıca bu isabetsizlikten etkilenen gruplardan biri olan çocukların yüz tanıma sistemlerine konu olarak alınmaları durumu söz konusu ise, daha farklı ve hassas bir muameleye tabi tutulmalarının şart olduğu söylenebilir²⁰⁷. Çoğunlukla ne yapacakları üzerinde takdir yetkileri bile olmayan bireyler olan çocuklar ve gençlerin, yüzlerinin yanlış okunması ya da değerlendirilmesi yaşamları üzerinde belirleyici etkiye sahip olabilecektir. Yeteri kadar korunamayan gençlerin kendilerini sürekli baskı altında hissetmeleri duygusal ve entelektüel gelişimleri açısından türlü olumsuzlukları beraberinde getirecektir. Özellikle çocuklar açısından bu teknolojinin hem ticari hem de kolluk amacıyla kullanılmasının yasaklanması değerlendirilmelidir²⁰⁸.

Burada bahsedilen isabetsizliğin yapay zekanın beslendiği büyük verinin içerdiği küçük verilerin niteliksiz oluşundan (burada kastedilen tek tek verilerin kalitesiz olması kesinlikle değildir, her veri kendi başına büyük bir anlama sahiptir. Ancak verilerin büyük bir veri seti haline getirilmesi ya da başka herhangi bir toplulaştırmaya uğraması söz konusu ise bu set halindeki verinin her zaman anlamlı olduğunu söylemek mümkün değildir. Günümüzde bir çok bilim dalı -veri bilimi, veri analitiği gibi- verilerin anlamlandırılması için çalışmaktadır) kaynaklandığı söylenebilecekse de karşıt yönden bakıldığında yapay zekayı gözetim faaliyetlerinden çıkarmak ve karar alma yetkisini insana bırakmak da bir takım sakıncaları beraberinde getirebilir. Çünkü büyük verinin gözetimde kullanılmasının potansiyel faydalarından biri de gözetimde takdir yetkisinin kullanılmasındaki sorunları ortadan kaldırmasıdır. Şöyle ki, büyük verinin kullanıldığı yapay zeka entegrasyonuna sahip yüz tanımlama sistemlerinden önce gözetim neredeyse tamamen insanın (kolluğun) becerilerine

²⁰⁶ Buna ilişkin gerçekleştirilen araştırmada siyah tenli kadınların cinsiyetlerini tanımlamak hususunda yaklaşık % 31 oranında bir hata payı olduğu görülmüştür. A.g.m., s. 62.

²⁰⁷ Lindsey BARRETT, “Ban Facial Recognition Technologies for Children - And for Everyone Else”, Boston University Journal of Science and Technology Law, C. 26, S. 2, Y. 2020, s. 285.

²⁰⁸ A.g.m., s. 285.

bağlı bir faaliyet olarak karşımıza çıkmaktaydı. Bu koşullar altında polislerin şüpheliyi tespit etmekte çoğunlukla kendi algılarına dayalı normatif yargıları ile hareket etmeleri, bir takım yanlış uygulamaları beraberinde getirebilecektir²⁰⁹. Örneğin, sosyo-ekonomik açıdan geri kalmış çevrelerde ırk ya da sınıfsal anlamda basmakalıp görüşler nedeniyle bazı insan gruplarına doğrudan şüpheli gözüyle bakıldığına şahit olabiliriz. Gerçekten de insan ya da yapay zeka arasında kararsız kalıp hangisinin bu sistemleri yöneteceği hususundaki değerlendirme gayet zordur ve bir açmaza neden olmaktadır. Ancak kanımızca gözetimi gerçekleştiren insan sayısının azaltılması, bu faaliyetlerin yapay zekaya bırakılması ve eğer ortaya çıkan sonuçlar gözetlenenler aleyhindeyse buna karşı etkin bir itiraz hakkı sunulması en uygun seçenek olarak görülmektedir.

Amerika’da bazı kanun koyucular eyaletler düzleminde yüz tanıma sistemlerine karşı sınırlamalar getirmiş, birtakım mahkeme kararlarında bu sistemlerin kullanılması sırasında alınacak koruma önlemleri ve taahhütlere değinilmiş olsa da Federal düzeyde geçerli olan özel bir yasa henüz ABD Senato’sundan geçmemiştir. Senatonun gündeminde olan bazı yasalar ise şunlardır: Algoritmik Güvenirlilik Yasası, Ticari Yüz Tanıma Gizliliği Yasası, Yüz Koruma Yasası. Buna ilaveten günümüzde FBI (Federal Soruşturma Bürosu) yüz tanıma teknolojilerini kullanırken iki yasal düzenlemeyi esas aldığı görülmektedir. Bunlardan birincisi 1974 tarihli Gizlilik Yasası, diğeri ise 2002 tarihli E-Hükümet Yasası’dır. Bu kanunlara göre FBI tarafından yürütülecek biyometrik çalışmalarda gizlilik etki değerlendirilmesi yapılması (bunu Avrupa Birliği Genel Veri Koruma Tüzüğü (GVKT) kapsamındaki etki değerlendirmelerine benzetmek mümkündür) ve Bilgilerin Şeffaf Uygulanması Kuralları’na (Fair Information Practices Principles) uygun davranılması gerekmektedir²¹⁰.

Yüz tanımlama teknolojileri aracılığıyla elde edilen delillerin kabul edilebilirliği ise tartışmalı bir konudur. Bu teknoloji yüz görüntülerinin dijital olarak karşılaştırılması suretiyle kimlik tespiti yapılmasını sağlar. Somutlaştırmak için suç işleyen bir kimseye ait görüntüler üzerinden yüz tanımlama teknolojisi ile kimlik tespiti gerçekleştirdiğimizi düşünelim. Mahkemenin elinde başka hiçbir kayıt olmamasına rağmen, bu yazılıma güvenilmesi sonucunda bir kimsenin suçlu ilan edilmesi mümkün müdür?

²⁰⁹ Elizabeth E. JOH, The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing, Harvard Law & Policy Review, C. 10, S. 1, Y.2016. s. 28.

²¹⁰ Samuel J. HODGE, s. 63.

Bazı mahkeme kararlarında bu teknolojiler vasıtasıyla elde edilen delillerin kesin delil olarak ele alınamayacağı belirtilmiştir. Bu delillerin kesin delil olarak görülmemesi yüz tanımlama teknolojilerinin yukarıda da değindiğimiz üzere yeteri kadar isabetli görülmemesinden kaynaklanır²¹¹. Bu görüşü destekleyen taraflar, Amerikan Ceza Muhakemesi alanında yerleşik olan Daubert standartları kapsamında da yüz tanımlama sayesinde elde edilen delillerin güvenilirliğinin sorgulanması ihtiyacından söz ederler²¹². Yine buna ilişkin olarak Amerikan Mahkemeleri tarafından verilen bir kararda, kolluk kuvvetlerinin yüz tanımlama teknolojisini şüphelilerin kimliklerinin belirlenmesi ya da elenmesinde tek kaynak olarak kullanamayacakları vurgulanmıştır²¹³. Dolayısıyla, yüz tanıma teknolojisinin kullanıldığı bir soruşturmada şüphelinin kimliğinin tespiti yönünde bir belirsizliğin olabileceği her halükarda göz önünde bulundurulmalı, yargı bölgesindeki hukuki kurallara bağlı olarak gerektiğinde keşif yapılarak olayın şahitlerine ya da doğru video kayıtlarına ulaşılmaya çalışılmalıdır.

İsabetsizlik açısından baktığımızda ise sadece yüz tanıma teknolojileri için değil, hareket tespitinde kullanılan her türlü yapay zekanın, bir takım suç niteliği taşıyan hareketlerin nispeten daha az görülmesi ve bu suçlara ilişkin öncü hareketlere ilişkin yeteri kadar veri ve dolayısıyla analiz bulunmamakta olması sebebiyle, hatalı sonuçlar sağlayabileceği göz önünde bulundurulmalıdır²¹⁴. Örneğin, caddede yürüyen bir kimsenin araçların kapı kollarını çekerek ilerlemesi bir öncü hareket olabilir. Bu hareket genel olarak hırsızlık ya da gasp suçlarının öncü hareketi olarak algılanmaktadır. Ancak bu fiilin gerçekleştirilmesi her zaman suç işlendiği anlamına gelmez. Bu gibi sorunların giderilmesi için hem bu davranış kodlarına hem de farklı çevre koşullarına ilişkin (kabalığın yoğunluğu, yağmur, fırtına gibi hava olayları) verilerin, bu yüz tanıma algoritmalarına tanıtılması ve sürekli olarak güncelleme sağlanması önemlidir²¹⁵.

²¹¹ A.g.m., s. 67.

²¹² Daubert standartları uzman bir bilirkişi ya da tanıgın bilimsel ifadelerinin mahkeme tarafından davada kullanılıp kullanılmayacağının belirlenmesine yarayan bir standarttır. Bu kapsamda dikkate alınması gereken hususlar şunlardır: 1) Söz konusu teori veya teknik test edilmeye elverişli midir? 2) Emsal değerlendirmesine ve karşılaştırmaya açık mıdır? 3) Bilinen ya da potansiyel hata oranı nedir? 4) İşleyişi sürdüren standartların var ve devamlı olması 5) İlgili bilim çevrelerinde benimsenip benimsenmediği? Bu soruların cevaplarına göre Daubert standartlarına uygun bir bilimsel tekniğin mahkemelerde delil olarak kullanılması mümkün olabilecektir. Amerikan Ceza Muhakemesi alanında kullanılan bu standart kapsamında yüz tanıma sistemlerinden elde edilen delillerin güvenilir olmadığı belirtilmektedir. Bkz. Daubert Merrel Dow Pharmaceuticals Inc.'e karşı, 509 US 697, k.t. 28/06/1993.

²¹³ People, Carrington'a karşı, b.n. 265888, k.t. 2 Şubat 2018.

²¹⁴ Ray SURETTE, Haroon IDREES, Mubarak SHAH, s. 298.

²¹⁵ A.g.m., s. 298.

Diğer taraftan yüz tanıma teknolojisi aracılığıyla alınan delillerin mahkemelerde kesin delil olarak kabul görebileceği yönündeki görüşü savunanların destek aldıkları mahkeme kararlarında ise özellikle iki yöne dikkat çekildiği görülmektedir²¹⁶. Birincisi veri tabanlarında yer alan fotoğrafların hükümete (ehliyet, işe giriş süreçleri, göçmenlik ya da diğer sebeplerle olabilir) gönüllü olarak verilmiş olmasıdır. İkincisi ise yüz tanıma teknolojilerine konu olan bireylerin makul bir mahremiyet beklentilerinin bulunması olarak görülmüştür²¹⁷. Buna karşıt olan görüşler de bulunmaktadır. Yani bireylerin kimliklerinin korunması açısından belirli bir ölçüde makul mahremiyet beklentilerinin olabileceği savunulmaktadır²¹⁸. Katz, Birleşik Devletler’e karşı kararında, ilk olarak bir bireyin yüz özelliklerinin topluma ifşa edilmesinin kimlik bilgilerini gönüllü olarak paylaştığı anlamına gelmediğine; ikinci olarak ise mahremiyet beklentisinin toplumda kabul gören sosyal normlara göre değerlendirilmesinin gerektiğine dikkat çekilmiştir²¹⁹. Sonuç olarak, bir bireye ait yüz görüntüsünün delil olarak kullanılmasına izin verilecek ise önce bireyin yüz tanımlamada kullanılan yüz görüntülerini rızasıyla verip vermediğine dikkat etmemiz gerekir. Akabinde ise bireyin yüz görüntüsünün bireysel mahremiyet alanında kaldığı görüldüğünden, temel hak ve özgürlüklere bir müdahalenin söz konusu olup olmadığının değerlendirilmesinin gerekeceğini söyleyebiliriz²²⁰.

Bu teknolojinin yukarıdaki değerlendirme haricinde de bir çok temel hak ve özgürlüğü etkilemekte olduğunu görmekteyiz. Başta ayrımcılığa uğramama hakkı, onurlu yaşama hakkı, özel ve aile hayatına saygı gösterilmesini isteme hakkı, toplanma ve gösteri yapma özgürlüğü, düşünceyi açıklama ve ifade özgürlüğü olmak üzere bir çok temel hak ve özgürlüğün bireylere sağlanması sırasında bu teknolojinin kullanılıyor olması, bu haklara belirli oranda bir müdahale sayılabilecektir. Yukarıda değindiğimiz üzere, yüz tanımlama teknolojisi farklı ten renklerine sahip bireyler arasında ayrımcılığa sebebiyet verebilecektir. Yine kişinin rızası alınmaksızın ya da vazgeçme şartı sunulmaksızın hakkında yüz bilgisi toplanması, bireyin onurlu yaşamı

²¹⁶ Birleşik Devletler, Dionisio’ya karşı, 410 U.S. 1, k.t. 22 Ocak 1973; Smith, Maryland’a karşı, 442 U.S. 735, k.t. 20 Haziran 1979.

²¹⁷ Birleşik Devletler, Knotts’a karşı yargılamasında, Yüksek Mahkeme arama kararı olmaksızın gerçekleştirilen gözetimin Anayasa’nın Dördüncü Değişikliği’nden doğan hakları ihlal etmediğine, çünkü davalının somut olayda meşru bir mahremiyet beklentisinin olamayacağına hükmetmiştir. Bkz. Samuel J. HODGE, s. 71. ; Aynı yöndeki diğer bir görüş açısından bkz. Benjamin J. GOOLD, Open to all? Regulating open street CCTV and the case for “symmetrical surveillance”, Criminal Justice Ethics, C. 25, S. 1, 2006, s. 7; İlgili karar için bkz. Birleşik Devletler, Knotts’a karşı, 460 U.S. 276, k.t. 2 Mart 1983.

²¹⁸ Samuel J. HODGE, s. 71.

²¹⁹ Katz, Birleşik Devletler’e karşı, 389 U.S. 347, 18 Aralık 1967.

²²⁰ Mahremiyet beklentisinin toplumda kabul gören sosyal normlara göre değerlendirilmesi açısından Amerika’da gerçekleştirilen araştırmaya göre, katılanların % 60’ı topluluğa karıştıklarında kimliklerinin gizli kalması gerektiğine, % 93’ü ise bilgilerinin kim tarafından alındığına dair bilgilendirme almaları gerektiğine inanmaktadır. Bkz. Samuel J. HODGE, s. 71.

açısından olumsuz etkiye sahip olabilecektir. Daha da ötesinde toplanma haklarını kullanmak isteyen bir grup insan, bu uygulamadan çekinerek ilgili toplantıya katılmaktan vazgeçiyor olabilir. Bu nedenle uygulamanın amaç, içeriği ve kapsamının çok iyi değerlendirilmesi zorunludur.

AB Temel Haklar Ajansı (European Union Agency For Fundamental Rights) tarafından yüz tanıma teknolojilerinin uygulanmasından önce dikkate alınması gereken bir takım unsurlar ve öneriler belirlenmiştir²²¹. Buna göre; öncelikle yüz tanıma teknolojilerinin kullanımını düzenleyen açık ve ayrıntılı bir yasal düzenleme yapılması gereklidir. Yüz görüntülerinin işlenmesinin ne zaman gerekli olacağı ve orantılı olup olmadığı belirlenirken, bu uygulamanın kullanım amacı bakılmalı ve yüz görüntülerinin otomatik işlemeye tabi tutulan kişiler açısından olumsuz sonuç doğurmasının engellenmesi için tedbirler göz önünde bulundurulmalıdır. Eğer uygulama herhangi bir temel hak ve özgürlüğün özüne müdahale etmiş sayılıyorsa, kesinlikle hukuka aykırı sayılacaktır²²².

Ayrıca kimlik doğrulaması amacıyla bir kimseye ait fotoğrafların eşleştirilmesi (bire bir eşleme) yapılacaksa bu faaliyetin; kimlik tespiti amacıyla yüz görüntüsünün belirli bir veri tabanı içindeki diğer görüntüler ile eşleştirilmesinden (bire karşı çok eşleme) tamamen ayrı sınıflandırılması gerekli olup, alınan önlemlerin ikinci faaliyet için daha üst düzey olması gereklidir. Çünkü bu durumda temel haklara müdahale riski daha yüksektir²²³. Canlı yüz tanımlama teknolojisi bakımından özgürlük kaygıları daha da artmaktadır. Bireyler yüz görüntülerinin bir izleme listesiyle eşleştirildiğinin farkında olmayabilirler, ayrıca bu anlık kayıtlar kontrollü bir ortamda çekilen yüz görüntülerine göre daha yüksek hata oranı verebilecek olduğundan sadece terörle ve ciddi suç türleriyle mücadele, kayıp ya da şüphelilerin tespitinde istisnai olarak kullanılmalıdır. Bunlara ek olarak yüz tanıma teknolojilerindeki isabet azlığının her daim göz önünde bulundurulması ve bu sisteme dayalı olarak muamele edilen herkese insan onuruna ve saygınlığına uygun şekilde davranılmalıdır.

²²¹ Facial Reconition Technology: Fundamental Rights Considerations in the context of Law Enforcement, European Union Agency For Fundamental Rights, <https://op.europa.eu/en/publication-detail/-/publication/0de97f99-10db-11ea-8c1f-01aa75ed71a1/language-en#> (s.y. 30 Şubat 2022)

²²² Michael O'FLAHERTY, "Facial Recognition Technology and Fundamental Rights". European Data Protection Law Review (EDPL), C. 6, S. 2, 2020, s. 172.

²²³ A.g.m., s 172.

Son olarak değinmemiz gerekir ki bu sistemler genelde kamu aktörleri ve kolluk mekanizmalarının kullanımına sunulmaktadır. Ancak Clearview²²⁴ örneğinde olduğu gibi tedarikçi bir özel şirket olabilmektedir. Hal böyle olunca hizmet sözleşmesi ya da teknik şartname vb. her ne ad altında olursa olsun kamu aktörlerinin özel şirketlerle yaptıkları sözleşmelerde temel haklar ve özgürlüklerin korunmasına yönelik taahhütler ve verilerin korunmasına ilişkin kurallar yer almalıdır. Aynı zamanda temel haklar etki değerlendirilmesi adı verilen bir etki değerlendirilmesinin de uygulamaya henüz başlanmadan önce yapılması çok yerinde olacaktır²²⁵.

II. Kapalı Devre Kamera Sistemleri Vasıtasıyla Yapılan Gözetimin Kanuni Dayanağı

A. Devlet Tarafından Yapılan Gözetim

Türkiye’de kapalı devre kameralarla gözetim denildiğinde aklımıza ilk olarak MOBESE (Mobil Elektronik Sistem Entegrasyonu) sistemi gelmektedir. Neredeyse tüm ülkeyi kapsayan ve birçok teknik takip sisteminin altyapısını birleştiren bu sistem, kolluk güçlerine suç ile mücadele konusunda büyük destek sağlamaktadır. Konuyu açıklamaya başlamadan önce hem MOBESE hem de KGYS (Kent Güvenlik Yönetim Sistemi)’nin aslında aynı sistemi ifade ettiğini söylememiz gerekmektedir.²²⁶ Bu nedenle her iki ifadenin çalışmamız içerisinde aynı sistemi nitelendirmek için kullanıldığını belirtmeliyiz. EGM tarafından yapılan tanıma göre, MOBESE (KGYS) kamu düzeni ve güvenliği ile kişilerin can ve mal emniyetinin korunması, suç işlenmesinin önlenmesi, trafik güvenliği ve kontrolünün sağlanması amacıyla meydan, karayolları, cadde, sokak ve park gibi kamuya açık alanlarda kurulan görüntüleme ve plaka tanıma sistemleri olarak tanımlanmıştır²²⁷.

²²⁴ *Clearview AI* (Artificial Intelligence) yüz tanımlama faaliyeti sunan ve Amerikan emniyet güçlerinin kullanımında olan bir yazılımdır. Kolluk kuvvetlerinin yüz tanımlama uygulamaları dahilinde gözetim faaliyeti yürütürken özel hukuk tüzel kişileri ile işbirliği yaptığını görebilmekteyiz.

²²⁵ Michael O’FLAHERTY, s 173.

²²⁶ Emniyet Genel Müdürlüğü (EGM) tarafından yayınlanan bazı yayınlarda bu gözetleme sisteminin MOBESE olarak ifade edildiği ya da toplumun genelinde alışageldik kullanımın bu yönde olduğu görülse de İçişleri Bakanlığı’nın, EGM’nin ve İl Emniyet Müdürlüklerinin resmi internet sayfalarında sistemin resmi adının “Kent Güvenlik Yönetim Sistemi” olarak belirtildiği görülmektedir. Nitekim Emniyet Genel Müdürlüğü Bilgi Teknolojileri Dairesi Başkanlığı Kuruluş, Görev ve Çalışma Yönetmeliğinin “Tanımlar” başlıklı 4’üncü maddesinde “MOBESE” ifadesine yer verilmemiş, ancak “KGYS” kısaltmasının açılımı olarak “Kent Güvenlik Yönetim Sistemi” ifadesine yer verilmiştir. Bkz. Civan BAŞAR, Devletin Kitlesel Gözetleme Araçlarının Özgürlükler ve Hukuk Güvenliği Üzerindeki Etkileri ile Bunların Yasal Dayanakları Üzerine Bir İnceleme, Türkiye Barolar Birliği Dergisi, S. 133, Y. 2017, s. 104.

²²⁷ KGYS ve PTS Projesi, Bilgi Teknolojileri ve Haberleşme Daire Başkanlığı, <https://www.egm.gov.tr/bilgiteknolojilerivehaberlesme/kgysvepts> (s.y. 2 Mart 2022) Aynı internet sitesi içerisinde PTS’lerden ise

Bu sistemler kamera ve radar cihazlarının kullanıldığı diğer bir takım alt bileşenlerden (“Bölge Görüntüleme Sistemi”, “Plaka Tanıma Sistemi”(PTS), “Hız Ölçüm Sistemi”, “Elektronik Denetleme Sistemi” (EDS) ve “ Mobil EDS” vb. gibi sistemlerdir.) oluşmaktadır. Bu alt bileşenler arasında ismini sıkça duyduğumuz ve özel olarak trafik güvenliğinin tesisine yönelik bir sistem olan EDS de bulunmaktadır. Trafik kuralı ihlallerinin önüne geçmek, kazaların engellenmesi ve can ve mal güvenliğinin sağlanması amaçlarına yönelik olarak kullanılan trafik takip sistemi olan EDS, Emniyet Genel Müdürlüğü, İl Emniyet Müdürlükleri veya POLnet entegrasyonu²²⁸ dahilinde yerel yönetimler tarafından kullanılmaktadır.

MOBESE’ler hem suç işlenmesinden önce hem de suç işlendikten sonra kullanılabilmektedir. Suçun işlenmesinden önce caydırıcılık, potansiyel kurban için güven duygusunun tesisi ve güvenlik görevlileri açısından da doğru davranma konusunda fayda sağlamakta olan bu sistemler, suç işlendikten sonra ise suçun aydınlatılması, faillerin tespiti ve yakalanması konusunda kolluk kuvvetlerine yardımcı olmaktadır²²⁹. Fakat, ister MOBESE ister KGYS olarak adlandırılın, mevcut durumda bu sistemlerin işleyişine dair kuralları, yani MOBESE’nin bir unsuru olan kameralar vasıtasıyla görüntü alınması, kaydedilmesi ve belirli bir süre muhafaza edilmesi ve bu görüntü verilerinin idari ve kolluk hizmetlerinin icrasında kullanılması konularını belirleyen herhangi bir yasal düzenleme bulunmamaktadır²³⁰.

Bu bakımdan, 5442 sayılı İl İdaresi Kanunu’nun 11. ve 32. maddeleri uyarınca illerde valilere, ilçelerde ise kaymakamlara suç işlenmesini önlemek için her türlü tedbiri alma yetkisi veren düzenlemenin MOBESE bakımından da uygulanmasının mümkün olduğu belirtilmiş olsa da, bu düzenlemeler doğrudan kamera takiplerinin usul ve esaslarına ilişkin olmadığından bu

kamera üzerinden aldığı araç fotoğrafını ve plaka karakterlerini tanımlama, tanımlanan karakterlerin veri tabanında yedeklenmesi ve istenen zaman diliminde plakası okunan araçların plaka bilgileri ve fotoğrafları ile beraber sorgulanmasını ve alarm üretilmesini sağlayan bir görüntü işleme teknolojisi olarak tanımlanmıştır.

²²⁸ Emniyet Teşkilatı tarafından yürütülen hizmetlere bilişim desteği vererek; görevin süratli, güvenilir ve etkin bir şekilde yerine getirilmesini ve vatandaşlarımızın zamanında, kaliteli ve kesintisiz olarak hizmet alabilmelerini sağlayan modern bir “Polis Bilgi Sistemidir”. PolNet Emniyet Teşkilatı iç otomasyon, ortak veritabanı ve vatandaş hizmet projesi olup, bu sistem ile bilgiye erişim amacıyla yapılan yazışmalar ve bu yazışmaların kaybettirdiği zaman ortadan kaldırılmış, birçok hizmet gerektiği gibi yapılmaya başlanmış ve etkinlik arttırılarak daha kaliteli hizmet verilmesi sağlanmıştır. Bkz. POLNet Nedir ?, Bilgi Teknolojileri ve Haberleşme Daire Başkanlığı, <https://www.egm.gov.tr/bilgiteknolojilerivehaberlesme/projeler/> (s.y. 20 Şubat 2022)

²²⁹ Cengiz DERDİMAN, Nihal TATAROĞLU, s. 256.

²³⁰ Civan BAŞAR, s. 114.

yöndeki beklentileri karşılamamaktadır²³¹. Nitekim bahsi geçen 5442 sayılı İl İdari Kanunu'nun 11. ve 32. maddeleri yetkililere sadece “belirli bir an için” ve “geçici nitelikte” yetki vermektedir. Bu durum izleme faaliyetinin de diğer kolluk tedbirleri gibi geçici, zorunlu ve ölçülü olarak yapılması anlamına gelir. Buna karşılık MOBESE'ler ile kamera kayıtlarının tutulması ve bireylerin hareketlerinin izlenmesi ise sürekli bir faaliyettir²³². Bu bakımdan ilgili kanuni düzenlemenin MOBESE'ler açısından uygulanabilirliği tartışmalıdır.

MOBESE sistemi kapsamında gerçekleştirilen faaliyetlerin usul ve esaslarının belirlenmesi kapsamında değerlendirilmesi gereken bir diğer yasal düzenleme ise, 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun Ek 7. maddesi olmaktadır. Bu düzenlemeye göre “*Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayiş sağlamaya, ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır.*” Fakat görüldüğü üzere, buradaki düzenleme de yine polise (ve jandarmaya) genel anlamda istihbarata yönelik bir takip yetkisi tanımaktadır. Bu yetkilerin geniş yorumlanarak, kamusal alanda herhangi bir suç soruşturması olmadan kamu görevlisine kamera ile gözetim yapma yetkisi verdiğinin söylenmesi uygun olmayacaktır. Keza, aynı maddenin devamında “*İstihbarat faaliyetlerinde, bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir*” denilerek, bu madde hükmünün uygulanmasının sadece bu kanunda belirtilen suçlarla ilgili olarak ve sadece hakim kararıyla söz konusu olabileceği vurgulanmıştır²³³.

Devlet görevlileri tarafından yapılan kapalı devre kamera gözetimin hukuki dayanağı olarak değerlendirilebilecek bir diğer kanun maddesi, 2918 sayılı Karayolları Trafik

²³¹ İlgili düzenleme 5442 sayılı İl İdaresi Kanunu'nun 11. maddesinde şu şekilde yer almaktadır: “*Madde 11- A) Vali, il sınırları içinde bulunan genel ve özel bütün kolluk kuvvet ve teşkilatının amiridir. Suç işlenmesini önlemek, kamu düzen ve güvenliğini korumak için gereken tedbirleri alır. Bu maksatla Devletin genel ve özel kolluk kuvvetlerini istihdam eder, bu teşkilat amir ve memurları vali tarafından verilen emirleri derhal yerine getirmekle yükümlüdür. B) Memleketin sınır ve kıyı emniyetini ve sınır ve kıyı emniyetiyle ilgili bütün işleri, yürürlükte bulunan hükümlere göre sağlar ve yürütür. C) İl sınırları içinde huzur ve güvenliğin, kişi dokunulmazlığının, tasarrufa müteallik emniyetin, kamu esenliğinin sağlanması ve önleyici kolluk yetkisi valinin ödev ve görevlerindendir. Bunları sağlamak için vali gereken karar ve tedbirleri alır.*” Aynı Kanun'un 32. maddesine göre ise, “*Madde 32 - A) Kaymakam, ilçe sınırları içinde bulunan genel ve özel kolluk kuvvet ve teşkilatının amiridir; B) Suç işlenmesini önlemek, kamu düzen ve güvenliğini korumak için gereken tedbirleri alır. Bu maksatla Devletin genel ve özel kolluk kuvvetlerini istihdam eder. Kanun, Cumhurbaşkanlığı kararnamesi ve diğer mevzuat ile Cumhurbaşkanınca alınmış bulunan karar ve tedbirlerin yürütülmesi için emirler verir. Bu teşkilat amir ve memurları kaymakam tarafından verilen emirleri derhal yerine getirmekle ödevlidir...*”

²³² Cengiz DERDİMAN, Nihal TATAROĞLU, s. 263.

²³³ A.g.m., s. 264

Kanununun 51. maddesidir. “Hız sınırlarına uyma” başlığını taşıyan maddenin ikinci fıkrasında “Hız ölçen teknik cihaz veya çeşitli teknik usullerle yapılan tespit sonucu Yönetmelikte belirlenen hız sınırlarını a) Yüzdeondan yüzde otuza (otuz dâhil) kadar aşan sürücülere 235 Türk lirası, b) Yüzdeotuzdan yüzde elliye (elli dâhil) kadar aşan sürücülere 488 Türk lirası, c) Yüzdeelliden fazla aşan sürücülere 1.002 TL idari para cezası verilir.” düzenlemesinin yer aldığı görülmektedir. Otoyollarda vatandaşların hareketlerini izleme konusunda yetki veren bu düzenleme, MOBESE ve diğer kamera gözetim araçlarının uygulamaya geçmesinden daha önce çıkarılmıştır²³⁴. Dolayısıyla, düzenlemenin yapıldığı tarihte hız tespitinde kullanılacak teknik araçtan kasıt hız radarı gibi sadece hız tespitine yönelik araçlar olduğundan ve kameralara ilişkin doğrudan bir düzenleme yapma amacı bulunmadığından, söz konusu uygulamaların hukuki dayanağını teşkil etmeyeceği de ortadadır. Bu amaç sonradan gelişmiş olsa bile yukarıda belirttiğimiz madde hükmünün lafzı gereği MOBESE’ler için kullanılması uygun olmayacaktır. Maddenin amacını gerçekleştirmek için elverişli olmadığından hız tespit kamerasıyla sürekli yapılacak bir izleme ölçüsüz olarak nitelendirilebilecektir.

Yukarıda belirttiğimiz kanun maddelerinin MOBESE faaliyetlerine uygulanmasında bir hukuka uygunluk değerlendirmesi yapacak olursak karşımıza üç kriter çıkacaktır. Bunlardan birincisi amaca uygunluk, ikincisi ise ölçülülüktür. Bu iki kriter dışında bir de görüntü kaydının alındığı yer konusunun önem teşkil ettiği görülmektedir. Son kriter üzerinden değerlendirmeye başlarsak kamera görüntülerinin kamuya açık alanda mı yoksa bireyin özel yaşam alanı sayılabilecek bir alındığının değerlendirilmesi yapılması bir zorunluluk olarak karşımıza çıkmaktadır.

MOBESE kameraları kamuya açık alanlarda kurulmuş olduklarından, gerçekleştirilen izleme ve kayıt faaliyetlerinin bireylerin kamuya açık alanlardaki görüntülerinden oluştuğu söylenebilecektir. Burada kamuya açık alanın fiziki olarak açık ya da kapalı bir mekân olup olmadığı önem arz etmemekte olup, bu alanın mülkiyeti bir kamu tüzel kişisine veya özel hukuk kişisine ait olabilir²³⁵.

²³⁴ A.g.m., s. 264

²³⁵ Tevfik Sönmez KÜÇÜK, Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı ile Önleyici Amaçla İzlenmesi, YUHFD, C. 15 , S. 1, Y. 2018, s. 70.

Ancak yukarıdaki yasal düzenlemelere bakıldığında örneğin; CMK md. 140'da olduğu gibi sadece kamuya açık alanlardaki görüntülerin kayıt altına alınacağına dair bir yasal düzenleme MOBESE'ler için bulunmamaktadır²³⁶. Bu bakımdan yasal olarak kaydın hangi alana yönelik yapılması gerektiği hususunda herhangi bir sınırlandırmaya gidilmediğini görmekteyiz. Bu durumda her ne kadar kamuya açık bir alanda kurulmuş da olsa doğrudan özel yaşam alanına çevrili bir MOBESE kamerasının bireyler hakkında görüntü kaydı alabilme ihtimali söz konusu olacaktır. Netice olarak bu durumu MOBESE faaliyetlerini düzenleyen açık ve belirli bir yasal düzenlemenin olmamasının olumsuz yanı olarak görmek mümkündür.

Gerçekleştirilen kamera görüntüsü toplama faaliyetini mevcut yasal düzenlemeler kapsamında değerlendirirken, bu görüntülerin toplanmasının ya da görüntüler üzerindeki diğer işleme faaliyetlerinin yasada belirtilen amaçları gerçekleştirmeye elverişli olup olmadığına da bakılması gerekecektir. Yani bu sistemler aracılığıyla elde edilen kamera görüntülerinin amaca uygun kullanılması gerekir. Kamuya açık alanlarda gerçekleştirilen MOBESE takibinin önleyici amaçla gerçekleştirilmesi gereklidir. Suçun işlenmesinin ve kamu düzeninin bozulmasının önlenmesi amacıyla gerçekleştirilmeyen nitelikte bir MOBESE takibinin mevcut düzenleme altında hukuka aykırı olduğu söylenebilir²³⁷.

Ölçülülük ise kamera görüntüsünün alınmasının amaca uygunluk bakımından, yani suç işlenmesini ve kamu düzeninin bozulmasını önlemek açısından elverişli ve gerekli olması anlamına gelmektedir²³⁸. Ölçülülük ilkesine üç yönden yaklaşmak mümkündür. İlk olarak bu görüntülerin suçun önlenmesi amacıyla kullanılmasının mutlaka gerekli olup olmadığı saptanmalıdır. Eğer bu yönde bir zorunluluk yoksa görüntüler kayda alınmamalıdır. Görüntülerin işlenmesi amacın gerçekleştirilmesi için zorunlu ise bu durumda amaca ulaşmak için gerekli olan en az miktarda görüntü kullanılmalıdır. Yine bunların dışında kamera gözetimine kıyasla daha az verinin işlendiği, daha az sınırlandırıcı bir araç kullanılarak suç işlenmesinin önlenmesi amacına ulaşılabiliriyorsa, bu daha az sınırlandırıcı aracın tercih edilmesi gerekmektedir²³⁹.

²³⁶ CMK'nın "Teknik Araçlarla İzleme" başlıklı 140'ıncı maddesi: "Madde 140: (1) Aşağıdaki suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir" Bkz. Ceza Muhakemeleri Kanunu.md. 140.

²³⁷ Tevfik Sönmez KÜÇÜK, s .70.

²³⁸ A.g.m., s .75.

²³⁹ A.g.m., s .76.

Gözetimin ölçülü olması gerektiğinden bahsettiğimizde, bu faaliyetlerin gerçekleştirilme süresi de büyük önem teşkil etmektedir. Örneğin, bir kimse hakkında çok sayıda CCTV görüntüsü alınması o kişinin geçmiş hareketleri hakkında kronolojik bir bilgi sağlamakta olup, gözetleyenlere bireyin yaşamına samimi bir pencereden dahil olma imkanı verir. Çünkü bireye ait konum bilgisi aynı zamanda o kişiye ait ailevi, siyasi, iş hayatı, dini tercihi ya da cinsel tercihi hakkında bilgi sağlamaktadır²⁴⁰. O halde devlet aktörlerinin MOBESE gözetimine bir de bu açıdan bakması gerekecek ve bu yönde gerekli tedbirleri alması lazım gelecektir. Eğer bir video kaydından devşirilen bu kadar fazla bilgi söz konusuysa, bunları ilk başta hiç almaması, gizleyerek ya da maskeleyerek alması, yetkisiz erişimleri önlemesi ve işlenmesinin gerekmediği ölçüde de derhal imhasını sağlaması gerekecektir.

Tüm bu değerlendirmelerimiz ışığında ülkemizde gerçekleştirilen MOBESE faaliyetlerinin doğrudan bireyin takibinde kullanılmasının hukuka aykırı olacağını söylememiz mümkündür. MOBESE ile görüntü kaydının alınması sadece suç işlemenin ve kamu düzeninin bozulmasının önlenmesi amacıyla yapılmak zorunda olduğundan, bu amaca uygun olmayan şekilde bir birey sürekli olarak takip edilmemelidir. Keza bu durumun aynı zamanda ölçüsüz bir veri işleme faaliyeti olduğu da söylenebilir. Bunlara ilaveten doğrudan özel bir yasayla düzenlenmeyen ve ölçüsüz sayılacak bir bireysel gözetleme faaliyetinin Anayasa’da düzenlenen “*Hukuk Devleti*” ilkesi ile de bağdaşmayacağı söylenebilir. Hukuk devleti içerisinde hukukun üstünlüğü şemsiyesi altında devlet organlarının bütün faaliyetlerinin hukuka uygunluğunun sağlanması önemli ve gereklidir²⁴¹. Mevcut yasal koşullar altında ise görüntü kaydının nasıl alındığı, kim ya da kimlere hangi amaçlarla aktarıldığı gibi hususlar düzenlenmemiş olduğundan, bu faaliyetlerin hukuka uygunluğunun değerlendirilmesi ve hukuka uygun olmayan işlemler için yaptırımın belirlenmesi hususunda yasal bir düzenleme ihtiyacı bulunmaktadır.

Burada ayrıca farklı bir ayrıma giderek MOBESE ile takip edilmek istenen bireyin herhangi bir birey olmadığı, kamuya mal olmuş bir kimse ya da siyasal bir figür olduğu durumu da ayrıca değerlendirmemiz önemlidir. Öncelikle söylememiz gerekir ki kamera görüntüleri eğer suçun işlenmesinin önlenmesi amacıyla kullanılmamışsa, yani bu amaçtan bağımsız bir gözetim gerçekleştiriliyorsa kamera görüntülerinin tespiti ve kaydedilmesi baştan itibaren

²⁴⁰ Emmanuel, A. P. JIMENEZ, The Fourth Amendment Limits of Facial Recognition at The Border, Duke Law Journal, C.70, S. 1837, Y. 2021, s. 1874.

²⁴¹ Civan BAŞAR, s. 120.

hukuka aykırı sayılmalıdır. İlâveten takip fiilinin mahiyeti gereği çoğunlukla belirli bir zaman aralığında gerçekleşmesi nedeniyle, süreç boyunca bu kişinin işlenen çok sayıda görüntü kaydı bulunacaktır. Bu durum görüntülenme faaliyetini ölçsüz hale getirecektir.

Buna ek olarak bazı durumlarda bireyin kamusal alanlarda dahi kendi mahremiyetine saygı duyulacağına ve korunacağına dair makul bir beklentiye sahip olduğu haller bulunabilir²⁴². Bu makul beklenti kamusal alanlarda görüntü kayıtlarının alınmasında herhangi bir birey için siyasal figüre göre çok daha yüksek olacaktır. Yani MOBESE'lere yansıyan görüntünün özel hayatına ilişkin olduğunun savunmasını birey, siyasi figüre kıyasla çok daha kolay yapabilecektir. Çünkü siyasi figürün özel yaşam alanı daha dar yorumlanmakta olup, bu kişilerin hayatları üzerinde kamunun bilgi almasının değerli olduğu vurgulanmıştır²⁴³. Aşağıda açıklayacağımız üzere, burada bireyin özel hayatının gizliliğinin korunmasının mı yoksa kamuya mal olmuş kişinin hayatından bilgi alma hakkının mı öncelikli olacağı tartışılabilir. Fakat, üçüncü kişilerin bu yöndeki bilgi alma haklarının bir üst paragrafta açıkladığımız hukuka aykırı olarak alınan kayıtlar açısından geçerli olmaması gerektiğini düşünmekteyiz. Aksi durumda takibin hedefi olan siyasi figürün özel hayatının gizliliğine önemli ölçüde bir müdahalenin gerçekleştiği söylenebilecektir.

Hem herhangi bir bireyin hem de siyasi figürün görüntü kayıtlarının tutuldukları elektronik ortamlar hakkında veri güvenliği tedbirlerinin alınmış olması da gerekecektir. Yine buna ek olarak MOBESE ile yapılabilecek gözetimin yukarıda sayılan mevcut yasal düzenlemeler kapsamında sadece kolluk otoritelerinin kullanımında olması sebebiyle, tüm kamera görüntülerinin yetkili makamlar nezdinde muhafaza edilmesi ve yasayla izin verildiği ölçüde aktarılması gereklidir. Yani MOBESE dahilinde elde edilen bireye ait bir görüntünün, kanun tarafından öngörülen istisnai durumlar haricinde ilgili kurum tarafından herhangi bir başka devlet kurumuna ya da herhangi bir özel kuruma aktarılmaması gereklidir. Bu yöndeki aktarımlar, paylaşımlar ya da çoğaltımların hukuka aykırı olacağı söylenebilir.

Yukarıda yer verilen hukuki düzenlemelerden hiçbirisi doğrudan MOBESE ile alınan görüntülerin işlenmesi, kaydedilmesi, muhafaza edilmesi ya da bu görüntülere kimlerin

²⁴² Bkz. aşı. s. 142.

²⁴³ Leyla Müjde KURT, Kamuya Mal Olmuş Kişi Kavramı, AÜHFD, C. 66, S. 3, Y. 2017, s. 593.

sonradan erişebileceği hususlarını direkt olarak düzenlememektedir²⁴⁴. Devletin kolluk organları tarafından yürütülen kamera gözetiminde alınan görüntülere kimlerin erişim sağlayabilecekleri, bu kişilerin ilgili görüntüleri hangi amaçla kimlere aktarabilecekleri, görüntülerin hangi ilkeler ışığında işlenebileceği ya da işlemenin amacına uygun ve ölçülü olup olmayacağı değerlendirilmesinin gerçekleştirilmesi açıkça bir yasal düzenlemeye bağlanmalıdır. Bu faaliyetlerin sınırlandırılması, hukuka aykırı bir kullanım için etkili hukuki çarelerin belirlenmesi ve devlet otoriteleri tarafından keyfi kullanımlarının önüne geçilmesi için belirttiğimiz yasal düzenlemenin yapılması biraz önce değindiğimiz hukuk devleti olmanın da bir koşulu olarak görülmektedir.

KVKK'nın yürürlüğe girmesiyle birlikte devlet eliyle yapılan kapalı devre kamera gözetiminin sınırlarının çizilmeye başlandığını söylememiz mümkündür. Kişisel veri sayılan kamera görüntülerinin artık bu Kanundaki sınırlamalara tabii olarak işlenebileceği, ölçülülük ilkesine aykırı işlemlerin hukuka aykırı olacağı ve kayıtların imhasının gerekmesi gibi konularda kamu gücünü sınırlandırılması söz konusu olabilecektir. Bu yönde MOBESE gibi yaygın bir gözetim sisteminin doğrudan KVKK ile düzenlenmesi yerine ayrı bir düzenlemeye tabi olması kanımızca gereklidir. KVKK'nın 4. maddesinde öngörülen kişisel verilerin işlenmesinin “kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilmesi” düzenlemesini bu kapsamda bir zorunluluk olarak görmemiz yerinde olabilir. Öğretide de buna paralel görüşler bulunmakta olup, bireyleri sokağa çıktıkları andan itibaren kayıt altına alan bu kamera sistemlerinin işleyişine ilişkin usul ve esasların düzenlendiği bir kanuni düzenlemeye ihtiyaç bulunduğu belirtilmektedir²⁴⁵. Gaul'e göre, CCTV sistemleri vasıtasıyla yapılacak gözetimin usul ve esaslarının kanunla düzenlenmesi gereklidir²⁴⁶. Eğer bu düzenleme yapılmaz ise bireylerin bu yoğun gözetim karşısında savunmasız bırakılmamaları için KVKK kapsamında ikincil düzenleme yapılması öngörülebilir. KVKK'nın “İstisnalar” başlıklı 28. maddesi doğrultusunda MOBESE'lerin faaliyetlerinin bu kanunun uygulanması alanına girip girmediği ise çalışmamızın ilerleyen bölümlerinde değerlendirilecektir²⁴⁷.

²⁴⁴ Burada belirtilen hususlarda EGM'den ve Jandarma Genel Komutanlığı (JGK)'ndan 4982 sayılı Bilgi Edinme Kanunu kapsamında bilgi istenmiş olup, ilgili kurumlardan gelen cevapların yeterli olmadığı ve belirtilen hususlarda veri işleme faaliyetlerinin nasıl gerçekleştiğine ışık tutmadığı görülmüştür. Bkz. Civan BAŞAR, s. 116.

²⁴⁵ Mustafa Bedri ERYILMAZ, Ceza Muhakemesi Hukuku Dersleri, 1. Baskı, Ankara 2012, s. 467.

²⁴⁶ Thomas GAUL, 2007, Untersuchung der verfassungsrechtlichen Anforderungen an Videoüberwachungsmaßnahmen des Staates im öffentlichen Raum mit und ohne biometrische Erkennungsverfahren unter besonderer Berücksichtigung der hermeneutischen Erkenntnismethoden im Verfassungsschutz, zur Erlangung der Würde eines doctor iuris der Juristischen Fakultät der Julius Maximilians Universität, Würzburg s. 183'ten naklen Cengiz DERDİMAN, Nihal TATAROĞLU, s. 262.

²⁴⁷ Bkz. aşa. s. 187.

B. Özel Teşebbüsler ve Üçüncü Kişiler Tarafından Yapılan Gözetim

Gözetimin küreselleşmesi ve teknolojiadaki hızlı gelişim ile birlikte kapalı devre kamera gözetiminde özel sektörün kamu gücü ile birlikte aktif rol aldığını gözlemlemekteyiz. Bir taraftan özel sektörün ya da vatandaşların, aslında kamu gücünden beklenen güvenliğin sağlanması için kapalı devre kamera sistemi kurulması süreçlerine mali olarak destek vermeleri söz konusuysa diğertaraftan da bu aktörlerin kendi kapalı devre kamera sistemlerini kurmaları ve gözetleyen konumunda bulunmaları söz konusu olabilecektir.

Dünya üzerindeki bir çok ülke tüketim, eğlence ve turizm için güvenli ve çekici yerler yaratılması amacıyla kapalı devre kameraların gücünden faydalanma yoluna gitmektedir. Hem kamu gücü hem de özel sektör, hem tüketicinin artması hem de turizmin geliştirilmesi için gerekli CCTV altyapısını birlikte kurmaya çalışmaktadır²⁴⁸. Gözetleyenin kamu değil de, özel teşebbüsler ya da toplumu oluşturan diğerbireyler olduğu durumda ise bu aktörler mağazalarda, işyerlerinde, kafelerde, apartmanlarda, bina girişlerinde kendi kapalı devre kamera sistemlerini faaliyete geçirmişlerdir. Ülkemizde bu alanlarda yapılan kapalı devre kamera gözetimleri için kamu kurum ve kuruluşlarından herhangi bir özel izin alınmamaktadır. Bu durum, devletin bu alanı düzenlemekte yetersiz kalması gibi bir durum yaratır ki oluşan boşluk bireylerin özel hayatlarının gizliliğini tehdit edebilir.

Özel teşebbüslerin ya da üçüncü kişilerin yaptıkları kamera gözetimine dayanak oluşturabilecek yasal düzenlemelerden biri 5442 sayılı İl İdari Kanunu'na 2018 yılında getirilen 9. maddenin (ç.) fıkrasıdır. Bu düzenleme, valilere Cumhurbaşkanlığı Kararnamesi ve diğertevzuatın verdiği yetkiyi kullanmak ve bunların getirdiği ödevleri yerine getirmek için genel emirler çıkarma ve bunları ilan etme yetkisi vermiştir. Buna benzer olarak, aynı Kanun'un 11. maddesinde de, valinin il sınırları içerisinde bulunan genel ve özel bütün kolluk kuvvet ve teşkilatlarının amiri olarak suç işlenmesinin önlenmesi, kamu düzeni ve güveninin korunması için gerekli tedbirleri alacağına ilişkin hüküm bulunmaktadır²⁴⁹. Valiler bu yetkilerini

²⁴⁸ David, LYON, Gözetlenen Toplum, s. 122.

²⁴⁹ 5442 sayılı İl İdaresi Kanununun 11. maddesinde şu şekilde yer almaktadır: “Madde 11 – A) Vali, il sınırları içinde bulunan genel ve özel bütün kolluk kuvvet ve teşkilatının amiridir. Suç işlenmesini önlemek, kamu düzen ve güvenliğini korumak için gereken tedbirleri alır. Bu maksatla Devletin genel ve özel kolluk kuvvetlerini istihdam eder, bu teşkilat amir ve memurları vali tarafından verilen emirleri derhal yerine getirmekle yükümlüdür. B) Memleketin sınır ve kıyı emniyetini ve sınır ve kıyı emniyetiyle ilgili bütün işleri, yürürlükte

kullanarak bulundukları illerde genel emir mahiyetinde kamu ve özel işletmelere güvenlik kameraları taktırma yükümlülüğü getirebilecektir²⁵⁰.

İçişleri Bakanlığı tarafından İstanbul Valiliği'ne gönderilen güvenlik kameralarına ilişkin yazıda²⁵¹, “Suç ve suçlularla mücadele kapsamında güvenlik kameraları kamu ve özel sektör tarafından etkin olarak kullanılmaktadır. Kent güvenlik yönetim sistemleri, plaka tanıma sistemleri, kamu binaları başta olmak üzere apartman, site ve işyerlerinde güvenlik kameraları ile 24 saat esasına göre kayıt yapmaktadır. Ayrıca Bakanlığımıza ilgili mevzuatla verilen suç ve suçlularla mücadele, kamu düzeni ve genel güvenliği sağlama görevi kapsamında ilgili genelge çerçevesinde şehir içi toplu ulaşım araçlarında da güvenlik kameraları bulunmaktadır.” denilmektedir. İlgili yazışma ile özel sektörün gerçekleştirdiği kamera gözetimine İçişleri Bakanlığı tarafından izin verildiği ve güvenlik kameralarının kullanımlarının ne kadar yaygın olduğu gibi tespitlerin yapılması mümkün olmuştur. Burada genel anlamda tüm işletmelere yönelik olarak verilen bir izinden bahsedilmektedir. Halbuki olması gereken, herhangi bir teşebbüsün işyerinde bu gözetim faaliyetini gerçekleştirmeden önce yerel yönetimlere ya da idareye başvurup özel bir izin almasıdır.

Bununla birlikte yine aynı yazıda, “Güvenlik kameraları tarafından kayıt altına alınan görüntülerin yetkisiz kişiler tarafından elde edilmesi, kullanılması ve ifşa edilmesinin önlenmesi, bunları kayıt altına alan kişi, kamu görevlisi, kamu, özel sektör, apartman, site yöneticileri ve ilgili esnafın sorumluluğundadır.” diye belirtilmiş olup, kameralarla gözetim yapanlara bir takım yükümlülükler yüklendiği görülmektedir.

Özel teşebbüslerin kapalı devre kameraları sistemlerini, bu sistemlerin önleyici ve caydırıcı niteliği haiz olmalarından dolayı meydana gelebilecek maddi veya manevi zararların sorumluluğundan kurtulmak üzere, serbest iradeleri ve ticari kararları dahilinde kullandıkları görülmektedir²⁵². Her ne amaca hizmet ederse etsin neticede özel teşebbüsler ya da üçüncü kişiler tarafından kapalı devre kamera sistemleri dayanaklarını kural olarak kanundan

bulunan hükümlere göre sağlar ve yürütür. C) İl sınırları içinde huzur ve güvenliğin, kişi dokunulmazlığının, tasarrufa müteallik emniyetin, kamu esenliğinin sağlanması ve önleyici kolluk yetkisi valinin ödev ve görevlerindendir. Bunları sağlamak için vali gereken karar ve tedbirleri alır...”

²⁵⁰ Cengiz DERDİMAN, Nihal TATAROĞLU, s. 266.

²⁵¹ İçişleri Bakanlığı İller İdari Genel Müdürlüğü'nün 30 Kasım 2018 tarih ve Alınacak Tedbirler Konulu Yazısı, <https://www.istesob.org.tr/wp-content/uploads/2018/12/214-Nolu-Genelge-Alinacak-TedbirlerHakkinda.pdf> (s.y: 28 Kasım 2021)

²⁵² Civan BAŞAR, s. 117.

almamakla birlikte kanundan doğan bir takım yetkiler dahilinde çıkarılan yazılar uygulamaya yön vermektedir. Bu duruma istisna olarak ise alışveriş merkezlerinde yapılan CCTV gözetimlerini vermemiz mümkündür.

Alışveriş merkezlerinde gerçekleştirilecek kamera gözetimi doğrudan Alışveriş Merkezleri Hakkında Yönetmeliğin 19. maddesinin 2. fıkrasında düzenlenmiştir. Bu düzenlemeye göre, AVM’lerde mevzuatta belirtilen alanlar ile sınırlı olarak kamera kaydı alınmasının sorumluluğu alışveriş merkezi yönetimlerindedir. Bu düzenleme tek olması nedeniyle önemli olsa da aslında gerçekleştirilecek kamera gözetiminin hangi alanda yapılacağı ve toplanan kayıtların ne kadar süreyle saklanacağı hususlarının dışındaki hususlar düzenlememekle birlikte CCTV’ler ile yapılacak gözetimin faaliyetlerinin düzenlenmesi açısından sınırlı olduğu söylenebilir.

Gerek özel teşebbüslerin gerekse de kamunun çalışanları, işyerlerinde bulundukları zaman dilimlerinde kameralar vasıtalarıyla devamlı olarak gözetim altında tutulmaktadır²⁵³. Bilhassa çalışanların performanslarının değerlendirilmesi amacıyla yapılan bu gözetimlerde, çalışanların izlenmesi ya da denetlenmesi gibi amaçlar doğrultusunda kişisel veri toplama yetkisi veren herhangi bir kanuni düzenleme bulunmamaktadır. Ancak bu husustaki veri işlemenin düzenlenmesi için örnek alınması gereken uluslararası bir takım çalışmaların olduğunu da vurgulamamız gerekir.

Uluslararası Çalışma Örgütü (UÇÖ, International Labour Office - ILO)’nün, çalışanların gizliliği ve işyerinde izleme ve gözetim konusunda²⁵⁴, çalışanların sağlık verilerinin gözetime konu edilmesi konusunda farklı rehberler hazırladığı görülmektedir²⁵⁵. Bu rehberlerden biri olan çalışanların gizliliği ve işyerinde izleme ve gözetim konusundaki rehber içerisinde, işyerinde gözetim hakkında (gözetim uygulamalarını açıkça işçiye bildirmenin gerekeceği, çalışanların yoğun şekilde gözetime çalışanın onuru ile bağdaşmadığı için itiraz

²⁵³ “Güvenlik hizmeti” başlıklı “MADDE 19 – (1) Alışveriş merkezinin otopark dahil her türlü bağlantı ve eklentileri ile giriş ve çıkışlarında 10/6/2004 tarihli ve 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuatı çerçevesinde özel güvenlik hizmeti sağlanır. (2) Alışveriş merkezinde bebek bakım odası ve tuvalet gibi niteliği itibarıyla kayıt altına alınması uygun olmayan alanlar dışındaki ortak kullanım alanları kamera ile kayıt altına alınır ve bu kayıtlar en az otuz gün süreyle saklanır. Bu kayıtların saklanmasıyla alışveriş merkezi yönetimi sorumludur.”

²⁵⁴ International Labour Office, Conditions of Work Digest, Workers’ privacy Part II: Monitoring and surveillance in the Workplace, C. 12, S.1, Y. 1993.

²⁵⁵ International Labour Office, Technical and Ethical Guidelines for Workers’ Health Surveillance, Cenevre 1998.

ettikleri, ayrıca diğerk bir itirazın da gözetimin uygulanış şekillerine yapıldığı) kapsamlı bilgi verilmiştir²⁵⁶.

Üçüncü kişiler tarafından yapılan kapalı devre kamera gözetiminden bahsettiğimiz için değinmemiz gereken konulardan bir tanesi de insansız hava araçları vasıtasıyla yapılan gözetimdir. İnsansız hava araçları (Drone), uçuşu esnasında üzerinde pilotu, uçuş ekibi ya da yolcusu bulunmayan hava taşıtı olarak tanımlanmaktadır²⁵⁷. Bir yüzyıl önce insan için tehlikeli görülebilen askeri görevlerin yerine getirilebilmesi için geliştirilen bu sistemler, günümüzde sadece askeri güvenlik amaçlarıyla kullanılmamaktadır. Bu amacın yanı sıra hava fotoğrafçılığı, ürün teslimi, tarımsal faaliyetlerin yerine getirilmesi, gözetleme ve kolluk faaliyetleri, bilimsel araştırmalar ve çeşitli altyapı hizmetlerinde kullanılmaktadır.

Tüm bu amaçların dışında sivil drone kullanımının da her geçen gün arttığını söylememiz mümkündür. Bu durumda gözetlenenlerin gözetleyen olduğu bir dünyaya doğru geçiş yapıldığını söylemek mümkün olabilir. Kaldı ki, Andres’e göre²⁵⁸, “eğer polislik faaliyetlerinde polis memurlarının vücut kamerası takmasına izin veriliyorsa, buna karşılık yurttaşlarında sivil drone kullanarak memurları gözetlemelerinin önerilmesi anlamsız değildir.” Yeni gelişen drone teknolojisi dahilinde çok hafif, küçük ebatlı ses kaydı dahi yapabilen cihazlar bireysel kullanımda bulunmaktadır. Bu durum hükümetlerin de yararına olacaktır. Hükümetler artık bir helikoptere kıyasla çok daha ucuz bir şekilde, genellikle bireyler farkına

²⁵⁶ ILO tarafından düzenlenen ve yürürlüğe konulan sözleşmelerdeki düzenlemeler, üye ülkeler tarafından onaylanırsa o ülke için bağlayıcı bir nitelik kazanmaktadır. Tavsiye kararları ise üye ülkeleri bağlayıcı gücü olmayan tamamlayıcı metinlerdir. Sözleşmeleri kabul etmiş olan ülkeler düzenli denetim (onaylanmış olan sözleşme kapsamında periyodik olarak ILO Uzmanlar Komitesine sunulan rapora istinaden yapılır) ve şikayete bağlı denetim olarak öngörülen iki farklı denetim mekanizması ile denetlenmektedir. Sözleşme ve tavsiye kararlarının uygulanması için eliyle yapılan bu denetimler neticesinde, ILO uygulamaya ilişkin aykırılıkları tespit ediyorsa bu durumu uluslararası kamuoyunun gündemine sunar. Özel paragrafa alınma adı verilen bu durum ILO denetim mekanizmasının en ağır yaptırımını olmaktadır. Bu denetim mekanizması ile birlikte değerlendirdiğimizde ILO’nun sözleşmelerine aykırı olan bir gözetim faaliyeti açısından doğrudan bir yaptırım uygulaması beklenmemeli, sözleşmeye aykırılığı tespit etme ve eleştiri getirme, akabinde de ortak bir çözüm gerçekleştirme şeklinde sonuç elde edilmesi beklenmelidir. Kaldı ki burada bahsedilen ihlale konu düzenleme bir rehber ise bunun yaptırımının daha sınırlı olacağı söylenebilir. Bkz. Ali Kemal SAYIN, ILO Normlarının ve Örgütün Denetim Mekanizmasının Türk İş Hukukuna Etkisi, Çalışma ve Sosyal Güvenlik Bakanlığı, Çalışma Dünyası Dergisi, C.1, S. 1, Temmuz – Eylül 2013, s. 11-34.

²⁵⁷ Bu araçlar bir yer destekli kontrol mekanizması ve iletişim sağlayıcı sistemin bir araya gelmesiyle oluşur. İnsansız hava araçları (drone) hakkında detay için bkz. Junyan HU, Alexander LANZON, “An innovativetri-rotor drone and associated distributed aerial drone swarm control”, Robotics and Autonomous Systems, S. 103, Mayıs 2018. s. 162-174.

²⁵⁸ Austin, CHOI-FITZPATRICK, The Good Drone-How Social Movements Democratize Surveillance, The MIT Press, ABD 2020, s. 134.

varmadan onlardan herhangi bir şekilde onay almadan gözetim faaliyetlerini yürütebiliyorlar²⁵⁹. Bu durum bireysel mahremiyet alanın fazlasıyla kısıtlandığı anlamına gelebilecektir.

Drone kullanmanın kanuni yönüne gelecek olduğumuzda, gözetim aracının etki alanı olan hava sahaları ve bunların bağlı oldukları kara ve su alanlarında²⁶⁰ geçerli olan hukuk kuralları önem kazanmaktadır. Türkiye’de İnsansız Hava Aracı (İHA) olarak nitelendirilen drone ile yasal olmayan uçuş gerçekleştirilirse, kolluk kuvvetleri tarafından müdahale gerçekleştirilmekte ve yasaya aykırı uçuşları gerçekleştirenler hakkında yasal işlem başlatılmaktadır²⁶¹. Türk Sivil Havacılık Kanunu kapsamında çıkarılan İnsansız Hava Aracı Sistemleri Talimatı’nın 18. maddesinde belirtildiği üzere, izin alınmadan ve risk analizi yapılmadan uçuşa yasak bazı bölgeler irtifaya bağlı olmaksızın havalimanlarında, en yakında bulunan pistin kenarından 9 km mesafeden yakın sahada, irtifaya bağlı olmaksızın çok kalabalık bölgeler ve kalabalık bölgeler üzerinde vb. uçuş yapılması yasaktır. Burada dikkat edilmesi gereken bir diğer kural olan aynı Talimat’ın 19. maddesinin (ç) bendinde drone uçuşlarının, insan ve yapılardan en az 50 metre uzaklıkta gerçekleştirilebileceği belirtilmiştir. Bu kuralın bireylerin mahremiyetiyle olan bağlantısı yadsınamaz ve yerinde bir uygulamadır. Ancak 50 metrelik mesafenin kamera yakınlaştırma özellikleri dikkate alınarak artırılması gerekliliği de gündeme gelebilecektir. Bireylerin bu yöndeki mahremiyet beklentilerini olumsuz etkileyebilecek bir husus da yerel yasa uygulayıcılarının yetki alanlarının hava sahalarına uzanıp uzanmadığını hakkındadır²⁶². Yani gizliliği ihlal eden bir drone müdahalesini şikayet eden bireye cevap veren yerel kamusal aktörün, havada gerçekleşmiş bir olayın kendi yetkisi alanında gerçekleşmediğini söyleme ihtimali bulunmaktadır.

Bu alandaki veri koruma kurallarını uluslararası ya da ulusal havacılık örgütlerinin mi yoksa ülkelerin kanun koyucularının ya da hükümetlerinin mi düzenlemesi gerektiğine dair bir bilinmezlik söz konusudur. Ülkemizde yukarıda bahsettiğimiz 50 metrelik yaklaşma

²⁵⁹ ByRon BARTSCH, James COYNE, Katherine GRAY, Drones In Society, Exploring The Strange New World Of Unmanned Aircraft, Routledge, Londra 2018, s. 81.

²⁶⁰ 14/10/1983 tarih ve 2920 sayılı Türk Sivil Havacılık Kanunu’nda yer alan ifadeye göre, “Türk Hava Sahası terimi”: Türkiye Cumhuriyetinin egemenliği altındaki ülke ile Türk karasuları üzerindeki sahayı ifade etmektedir.

²⁶¹ İstanbul Valiliği tarafından düzenlenen “Genel Emir” içerisinde, “Bahse konu Hava Araçlarının yasaklanan mahallerde izin alınmadan yapacakları uçuşların tespiti halinde; bu durum tutanağa bağlanarak Sivil Havacılık Genel Müdürlüğüne ve Valiliğimize bildirilecek olup, haklarında 5442 sayılı İl İdaresi Kanunu, 5326 sayılı Kabahatler Kanunu, 2920 sayılı Türk Sivil Havacılık Kanunu ve 5237 sayılı Türk Ceza Kanunu (TCK) hükümleri uyarınca yasal işlem yapılacaktır.” şeklinde belirtilmiştir. Bkz. <http://istanbul.gov.tr/kurumlar/istanbul.gov.tr/guncel/duyurular/insasiz-hava-araci-duyurulari/iha-gelen-emir.pdf> (s.y. 30 Şubat 2022)

²⁶² ByRon BARTSCH, James COYNE, Katherine GRAY, s. 82.

mesafesinin öngörülmesi dışında doğrudan bireylerin gizliliğini dikkate alan bir kanuni düzenleme hariç, bireylerin gizliliğini koruyan herhangi bir veri koruma kuralı bulunmamaktadır. Bununla birlikte, bireylerinin verilerinin korunmasına dair kaygıların çoğunlukla uluslararası düzlemdeki havacılık düzenleme otoritelerinin radarına girmediğini söylemek de mümkündür²⁶³. Sonuç olarak bu yönde yasal düzenlemenin doğrudan veri koruma hukuku içerisinde yer alması bir gereklilik olarak karşımıza çıkmaktadır.

İnsansız hava araçlarının özel teşebbüsler ya da diğer üçüncü kişiler tarafından kullanımının ya da diğer bir ifadeyle bu teknoloji araçlarının sivil kullanımlarının artmasının gözetlenenlerin gözetleyen olmaları sonucunu doğurduğunu yukarıda ifade etmiştik. Gözetlenenlerin gözetleyen olduğu bu akışkan gözetim dünyasında karşımıza çıkan bir başka örnek ise kitlesel kaynaklı gözetim (“crowdsourcing”) yöntemidir. Burada coğrafi olarak farklı alanlara dağılmış bireylerin kendi bilgisayarlarından, CCTV görüntülerini izlediği kitlesel kaynaklı bir gözetim söz konusudur. Yani burada gözetleyen artık toplumun kendisidir. İngiltere’de bu yönde farklı örnekler söz konusudur²⁶⁴. Örneğin; CrimeStoppers UK sitesinin içerisinde bilinen şüphelilerin bilgilerinin ve CCTV kayıtlarının bulunduğu profiller herkese açık olarak yayınlanmaktadır. Bu uygulama bir nevi “aranıyor!” duyurularının internet ortamında yer alan örnekleri gibidir.

Sonuç olarak ülkemizde meydanlarda, işyerlerinde, apartmanlarda, bina girişlerinde, sitelerde veya diğer alanlarda kapalı devre kameraların kullanılma oranlarının yüksekliği ve yaygınlığı göz önüne alındığında, yapılacak kanun veya ikincil düzenlemelerle ek düzenlenmeye konu olmasının ya da Kişisel Verileri Koruma Kurulu tarafından ilke kararı niteliğinde uygulama esasları getirilmesinin gerekli olduğu söylenebilir. Söz konusu gözetim faaliyetlerinin temel amacının güvenliğin sağlanması ve suç işlenmesinin önlenmesi olması, kamera ile izleme yönteminin zorunlu olması ve elde edilen verilerin saklanması ve aktarılması konularında yasal düzenlemelerin yapılması gözetlenenlerin temel hak ve özgürlüklerinin korunması açısından gereklilik arz etmektedir.

III. Kapalı Devre Kamera Sistemlerinin Kullanımının Amaçları

²⁶³ ByRon BARTSCH, James COYNE, Katherine GRAY, s. 82.

²⁶⁴ Burkhard SCHAFER, Crowdsourcing and Cloudsourcing CCTV Surveillance, Datenschutz und Datensicherheit, C. 37, S. 7, Y. 2013, s. 434.

Kapalı devre kamera sistemlerinin kullanılma amaçlarını dört farklı kategori altında inceleyeceğiz. Bu kategoriler aşağıdakilerden oluşmaktadır:

- 1) Suçun Önlenmesi ve Adaletin Sağlanması Amacı
- 2) Güvenliğin Sağlanması Amacı
- 3) Denetim Sağlama Amacı
- 4) Gözetleme Amacı

A. Suçun Önlenmesi ve Adaletin Sağlanması Amacı

Kapalı devre kameraların günümüzde bu kadar çok kullanılmasının en önemli sebebi suçun önlenmesi ve adaletin sağlanması amacına yönelik kullanılmalarıdır. Kameraların caydırıcılık unsuru olmasının yanı sıra, suç işlendiğinin fark edilmesini kolaylaştırması ve suç niteliği taşıyan görüntülerin kayıt altına alınarak suç delili olarak kullanılması çok önemlidir.

1993 yılından 1998 yılına kadar İngiltere’de suç oranlarının azaltılması amacıyla çoğunluğu kamu maliyesinden aktarılan yaklaşık 100 milyon sterlin kapalı devre kamera sistemlerine harcanmıştır²⁶⁵. Fakat bu büyük ölçekli harcamalara rağmen, kameraların suç azalttığına dair kesin ve güvenilir bir veri bulunmamaktadır²⁶⁶. Yine de aynı dönemde İngiliz kamu otoritelerinin topluma bu sistemlerin başarılarını anlatan açıklamalarda bulundukları görülmüştür²⁶⁷.

Kamu otoritelerinin taraflı söylemlerini bir kenara bırakacak olursak, kapalı devre kameraların suç oranlarını azaltmadaki başarılarını daha sistematik inceleme fırsatımız olabilir. Bu bakımdan incelenmesi gereken kameraların teknik bakımdan sadece çalışıyor olmaları değildir. Asıl değerlendirilmesi gereken “neden o bölgede işe yaradıkları” ya da “hangi bağlamlarla” çalıştıklarıdır. Çünkü ancak bu sorular düzgün sorabilir ve yanıtları doğru

²⁶⁵ Clive NORRIS, Jade MORAN, Gary ARMSTRONG, Surveillance, Closed Circuit Television and Social Control, Routledge, New York 2016, s.3.

²⁶⁶ Emma SHORT, Jason DITTON, “Does CCTV Affect Crime?”, CCTV Today, C. 2, S. 2, Y. 1995, s. 10-12.

²⁶⁷ 16 Nisan 1993 tarihli “The Guardian” da yer alan habere göre, Polis Baş Müfettişi Graham Pearson yapmış olduğu açıklamada, CCTV’ler sayesinde suç oranının daha önceki döneme göre %74 oranında azaldığını ifade etmiştir. Sonrasında “Independent”’in 6 Haziran 1994 tarihli haberine göre ise, polis tarafından alıkonulma oranlarının neredeyse üç katına çıkmış olduğu belirtilmiştir. Bkz. Clive NORRIS, Jade MORAN, Gary ARMSTRONG, s.175.

sınıflandırabilirsek, o takdirde bir bölgede suçu azaltan bir güvenlik kamerasının başka bir bölgede de kullanılabileceğine kanaat getirebiliriz.

Bununla birlikte, kamera gözetiminin suç oranlarına etkisini daha nesnel anlamda değerlendiren Skinns, Doncaster'da kullanılan kapalı devre kameraların suç oranını yüzde altı oranında düşürdüğünü ortaya koymuştur²⁶⁸. Ortaya konulan bu rakam, perde arkasında başka gerçekleri gizlemektedir. Bu gerçek suçun kamera olmayan alanlara ve şehir merkezinden ilçelere doğru yayılmasıdır. Gerçekten de kamera kaydı alınan alanlarda suç oranlarında düşüş yaşanırken, ilçelerde çok büyük sayılabilecek şekilde yüzde otuz birlik bir artış saptanmıştır.

Amerika'nın Milwaukee eyaletinde suçun yoğun yaşandığı bölgelere ve kalabalık kavşaklara yerleştirilen kameralar dahilinde yapılan gözetime dair bir çalışmaya göre, 2016 yılında Milwaukee Polis Departmanı ile Ulusal Adalet Enstitüsü bünyesinde kurulan Kent Enstitüsü birlikte çalışarak kentteki CCTV gözetimini geliştirmeye yönelik katı bir planı hayata geçirmeye başlamışlardır. Farklı etnik ve ırksal kökenlerden gelen insanların bulunduğu şehirde 2017 yılında 10.000 kişide 159,47 olarak hesaplanan suç gerçekleşme oranı, bu şehri ülkede 100.000 kişinin üzerinde insan yaşayan şehirler arasında suç oranı en yüksek yedinci şehir haline getirmiştir. Bununla birlikte bu istatistiklerin alt kırılımına bakıp sadece malvarlığına karşı işlenen suçları baz aldığımızda ise şehir doğrudan ilk üç şehir arasına yerleşmektedir²⁶⁹. Ortaya konulan sonuçlara göre, çalışmanın gerçekleştirildiği sırada şehirde suç işleme sayılarının azaldığı tespit edilmiştir. 2017 yılında 9,507 olarak tespit edilen şiddet suçu sayısı, bir yıl sonra 2018'de 8,416 adet ile sınırlı kalmış, bununla birlikte malvarlığına karşı işlenen suçlar da aynı süreçte 22,569'dan 17,699'a doğru bir azalma göstermiştir²⁷⁰. Bu çalışma kapsamında ortaya çıkan bir sonuç da CCTV'lerin daha fazla konumlandırıldığı kesişim alanları diye tabir ettiğimiz kavşaklarda ya da meydanlarda, CCTV bulunmayan yerlere kıyasla daha fazla suç işlendiğidir²⁷¹. Ancak bu durum kesişim alanlarının doğaları gereği daha fazla

²⁶⁸ Clive NORRIS, Jade MORAN, Gary ARMSTRONG, s.175.

²⁶⁹ 2007 yılında 15 CCTV kamerası ile yapılan gözetim 2011'e geldiğimizde sayı olarak 42'ye çıkarılmış olup, 40 farklı lokasyonda konumlandırılmıştır. 2020 yılı itibarıyla ise 24 tanesi yeni panoramik, 12 tanesi kaydırma, eğme ve yakınlaştırma özelliği bulunan PTZ kameralar ve 9 adet yeni otomatik araç plaka tanımlayıcı kameralar olmak üzere toplamda 87 kamera faaliyetine devam etmektedir. Bkz. Lily ROBIN, Bryce E. PETERSON, Daniel S. LAWRENCE, How Do Close-Circuit Television Cameras Impact Crimes And Clearances? An Evaluation of The Milwaukee Police Department's Public Surveillance System, Police Practice and Research, C. 22, S. 2, Y. 2021, s. 1174.

²⁷⁰ A.g.m., s. 1184.

²⁷¹ A.g.m., s. 1184.

kullanıldığı, daha fazla insanın bu alanları ziyarette bulunduğu göz önüne alındığında bu şekilde bir sonuç doğması yadsınamaz.

Toplumu oluşturan bireylere kameralar ile gözetim faaliyetlerinin “gökyüzündeki bir dostun gözü” olarak tanıtılması bu faaliyetlerin her geçen gün daha etkin olarak sürdürülmesine fayda sağlamıştır. Bu gözetim tekniği sadece suç oranlarını azaltmak konusunda değil, bunun yanı sıra suç ile karşılaşma korkusunun azalmasını da sağlamıştır²⁷². Kameraların güven veren koruyucu etkisi 90’lı yıllarda özellikle kadınlar açısından önemli bir gelişme olarak görülmüştür. Bununla birlikte şehirlerde kurulu CCTV kameralarının gün geçtikçe artması gözetleyenlerin işini zorlaştırmaya başlamıştır. Çok fazla sayıda kameranın monitörler aracılığıyla izlenmesi ve suç niteliğinde olan hareketlerin bu şekilde tespit edilmesi pratik olarak imkansız hale gelmiştir. Bu zorluk süreçten insan faktörünün çıkarılması gibi bir fikrin doğmasına sebebiyet vermiştir. Bu fikre göre, “ilgili durum” ya da “kritik durum” diye tabir edilen tetikleyici olguların gerçekleşmesiyle birlikte CCTV sistemi kayıt tutmaya başlayacaktır²⁷³. Açıkça belirtmek gerekir ki, CCTV kameralarının varsayılan hallerinde inaktif olarak kayıt tutmaması sadece aktif hale geldiklerinde kayıt tutmaları kişisel verilerin korunması ve bireylerin mahremiyetlerinin korunması açısından çok yerinde bir uygulamadır. Ancak buradaki soru kritik durumların nasıl tespit edileceğine yönelik olmaktadır. Burada gözetleyicilere yardımcı olacak bileşen daha önce de ifade ettiğimiz gibi yapay zeka olacaktır.

Kritik durumlar, işyerinde ve kamusal alanlarda yaşanacak örnekler bakımından ikiye ayrılarak kategorize edilmiştir. İşyerinde bu durumlar herhangi bir cezai soruşturmanın yürütülmesine sebebiyet verebilecek bir fiil olarak tanımlanırken, kamusal alanlarda belirli bir yere yetkisiz giriş, şiddet ya da taciz, saldırı vb. gibi fiiller kritik durum sayılabilecektir. Bu yöntem çerçevesinde oluşturulan hareket takip algoritması çerçevesinde ilgili fiillerin tespiti yapılabilecektir. Keza özellikle işyerinde gerçekleşebilecek olaylar açısından seslerin işlenmesi söz konusu olacak ve eğer bir takım tetikleyici anahtar kelimelerin (saldırgan, aşağılayıcı, onur kırıcı ya da uygunsuz nitelikteki kelimeler) kullanılması söz konusuysa yine kameralar faaliyetlerine başlayacaktır²⁷⁴.

²⁷² Clive NORRIS, Jade MORAN, Gary ARMSTRONG, s. 207.

²⁷³ Mrigank SHARAD, Robin Singh SIDHU, Smart Surveillance System for Detecting Interpersonal Crime, International Conference on Communication and Signal Processing (ICCSP), 2016, s. 2.

²⁷⁴ A.g.m., s. 3.

Şunu da belirtmemiz lazım, bu teknik video kayıtlarının geri dönüştürülebilecek şekilde şifrlenmesi ya da maskelenmesi yoluyla işlenmesinden daha güvenlidir. Çünkü sistem bahsedilen tekniklerden farklı olarak ilgi alanına girmeyen bireyleri kesinlikle tespit etmemektedir. Eğer ilgi alanına giren bir durum hakkında kayıt yapılıyorsa, kayıtlarda yer alan kişi zaten suç konusu gerçekleştiren bir kimse olacağından kimlik tespitinin yapılması gerekli olacaktır²⁷⁵.

İnsan faktörünün bu gözetim unsurlarından çıkarılması Avrupa Birliği (AB)'nde CCTV kullanımının fizibilite çalışmalarını hedef alan Indect projesi kapsamında da değerlendirilmiştir. Bu projenin temel amacı tüm bilgilerin yapay zeka temelli olarak işlenmesini ve anormal davranışların ya da şiddet fiillerinin otomatik olarak tespit edilmesini sağlayan bir sistem tasarlamaktır²⁷⁶. Suç, terörizm ve şiddet eylemleriyle ilgili potansiyel tehditlerin tespiti amacıyla bireylerin, nesnelerin ve kentsel alanların izlenmesi bu süreçler dahilinde kolaylaşacaktır. Buna göre, gözetim faaliyetlerinin insansız yapılabilmesi daha az iş gücünü gerektirmesi, diğer insanlar tarafından izlenme aktivitelerinin daha az olması nedeniyle mahremiyetin daha etkin korunması ve bunların beraberinde verilerin gizliliği bakımından sakıncalı olabilecek sonuçlar doğurabilen insan hatası faktörünün daha az olacağı göz önüne alınarak, projenin faydalı olabileceği yorumu yapılmıştır²⁷⁷. Keza bu uygulamaların insansız gerçekleştirilmesi uzun vadede ekonomik olarak da karlılığı artıran bir etken olarak görülmektedir²⁷⁸.

Suçun önlenmesi amacıyla kameralar vasıtasıyla yapılan gözetimde, menfaatler dengesinin iyi korunması gereklidir. Bu kapsamda, gözetim altında yer alan bireylerin özel yaşamlarına ve kişisel verilerinin korunması hakkına müdahale niteliğinde olan bir eylem bulurken diğer taraftan da yapılan gözetim ile suçun işlenmesi önlenmeye çalışılarak başka kişilerin hak ve özgürlükleri korunmaya çalışılmaktadır. Belirli koşullar altında, bireylerin kişisel verilerinin korunmasına karşılık kamu düzeninin korunması gerekliliği ön plana çıkmakta ve kameralarla gözetim yapılmaktadır.

²⁷⁵ A.g.m., s.2.

²⁷⁶ Mathias VERMEULEN, Rocco BELLANOVA, European “Smart” Surveillance: What's at Stake for Data Protection, Security and Human Rights, C. 23, S. 4, Y. 2013, s. 121.

²⁷⁷ Jennifer A. BROBST, s. 6.

²⁷⁸ A.g.m., s. 7.

“Almanya Federal Verilerin Korunması Kanunu 6b/1’in, video kameralarla yapılan izlemelerde menfaatler dengesi konusunda yön gösterici bir niteliği sahip olduğu belirtilmelidir. Bu hüküm gereğince kamuya açık alanların optik-elektronik araçlarla izlenmesi yalnızca kamusal bir görevin yerine getirilmesi; bir yere kimin girebileceğini belirleme hakkının icrası veya somut amacı tespit edilmiş meşru bir menfaatin gerçekleştirilmesi için gerekli olması ve ilgililerin güvence altına alınan menfaatinin üstün olması halinde mümkündür. 28.04.2017’te md.6-b’de yapılan değişiklikle spor, toplantı, eğlence ve alışveriş merkezleri ile park alanları gibi büyük ölçekli yapıların ya da taşıtların ve kamuya tahsis edilen demir, deniz ve kara yolu ulaşımında kullanılan büyük binaların video kamera ile izlenmesinde buralarda bulunan kişilerin yaşamlarının, sağlıklarının ve özgürlüklerinin korunması menfaatinin ayrı bir önem taşıdığı ve öncelikle korunması gerektiği kabul edilmiştir.”²⁷⁹

B. Güvenliğin Sağlanması Amacı

Kapalı devre kamera sistemlerinin kullanılma amaçlarından bir diğeri ise güvenliğin sağlanması amacı olarak karşımıza çıkar. Bu amacın suçun önlenmesi ile olan bağlantılı olduğu ortadadır. Zira aynı alanda suçun işlenmesi önleildiğinde güvenliğin de sağlandığı ifade edilebilir. Ancak bu amaç biraz daha uygulamaya bağlı olarak farklılaşmıştır. Burada önemli olan belirli bir alanın güvenliğinin sağlanmasıdır. Bu alan bir meydan, işletme, fabrika ya da ev olabilir.

Yerleşim alanlarının güvenliğinin sağlanması için kullanılan kapalı devre kameralar gözetleme yapılan alanlarda bireylerin mahremiyetinin tehlikeye girmesine yönelik bir takım sorunları beraberinde getirmektedir. Şehirlerde gerçekleştirilen kamera gözetiminin temel amacının kamu düzeninin ve toplumdaki güvenliğin sağlanması olduğunda belirli oranda bireysel gözetime izin verilmesi mümkündür. Ancak bu gözetimin ölçülü olması ve bir takım güvenlik tedbirleri dahilinde yapılması durumunda, gözetimin hukuka uygun olduğunu söyleyebiliriz.

Bu doğrultuda, kapalı devre kamera sistemlerinin bulunduğu güvenlik sistemlerinin tüm AB sınırları dahilinde belirli bir seviyeye getirilmesi açısından, veri güvenliği önlemlerini alan güvenlik sistemlerinin belirli bir sertifikasyonu gerektirdiği ve eğer bu standartları sağlamayan

²⁷⁹ Tefik Sönmez KÜÇÜK, s. 77.

bir güvenlik sistemi varsa bunun kullanılmaması gerektiği belirtilmiştir. CRISP adı verilen AB güvenlik projesinde hedeflenen belirli bir seviyeye getirilmiş ve sertifikalanmış güvenlik sistemleri ile AB vatandaşlarının güvenlik teknolojilerine güven duymasının sağlanmasıdır²⁸⁰.

CRISP projesinde hedeflenen diğer alt amaçlar ise CCTV sistemlerinin tasarım ve uygulamalarının daha şeffaf olarak yapılması, CCTV sistemleri üzerinde efektif kontrol sağlanması ve böylelikle uygulamada veri sahibi ilgili kişiler için bu sistemleri daha görünür yapma, gerektiğinde itirazlarını ya da erişim haklarını kullanmaya teşvik etme olmaktadır²⁸¹. Bu sistem her ne kadar yurttaş ve devlet arasında bir köprü gibi görülse de sonuç itibarıyla arka planda güvenlik endüstrisi aktörlerinin de yer aldığını unutmamak gerekir. Çünkü günün sonunda sertifikasyonu sağlayan aktörler tüm AB’de satışını yapabileceği bir güvenlik sistemine sahip olacak ve eğer doğru adımlar atılmazsa tekelleşme söz konusu olabilecektir.

Ayrıca kapalı devre güvenlik kameralarıyla çevrelenen herhangi bir alanda güvenliğin sağlanması işi teknik ekipmanlarla çok daha az sayıdaki insan gücü ile yapılabileceğinden avantaj sağlamaktadır. Bunu çok sayıda kamera az sayıda insan olarak ifade edebiliriz. Örneğin; büyük ölçekli bir fabrikaların güvenlik kontrol odasından izlendiği ve güvenlik ihlali yaşandığında ya da yaşanma riski tespit edildiğinde müdahale amacıyla güvenlik personellerinin ilgili alanlara yönlendirilmesi böyledir.

C. Denetim Sağlama Amacı

Kapalı devre kameralar, gözetleyenlerin gözetlenen bireyler üzerinde denetim kurmasını sağlayan araçlardır. Bu araçlar gözetim altındaki kişilerin belirli bir takım kurallara uyup uymadığını denetleyerek, bireyleri istenen davranışları gerçekleştirme hususunda disipline etmektedirler. Çalışmamızın önceki bölümünde ifade ettiğimiz üzere, gözetim belirli bir ölçüde bireyi disipline etmeyi ve onu belirli bir yola sokmayı hedefler, işte bu bakımdan kapalı devre kameraları da araç olarak kullanması mümkündür.

İşyerlerinde ve fabrikalarda çalışanların gerek performans değerlendirmesi gerekse de ne yaptıklarının gözetlenmesi bu amaca yöneliktir. Bununla birlikte, kamusal bir alan olmayan

²⁸⁰ Simone WURSTER, Irene KAMARA, Thordis SVEINSDOTTIR, *Certified Security Systems For Sustainable Cities of The 21st Century*, *ITU Kaleidoscope: ICTs for a Sustainable World*, 2016, s. 3.

²⁸¹ A.g.m., s. 2.

evlerde çocuk bakıcıları ve yardımcıları gözetlemeye ve denetlemeye yarayan, internet üzerinden veri aktarımı ile gözetleyenlerin anlık olarak gözetlemelerine izin veren kameralı sistemler de buna örnek olarak gösterilebilir²⁸². Ancak özellikle dikkat etmek gerekir ki, kameralar vasıtasıyla denetim amacına yönelik gözetimde, gözetleyenlerin denetim sağlama amacı ile gözetlenenlerin özel yaşamlarının gizliliğinin korunmasının arasındaki dengenin iyi değerlendirilmesi gereklidir.

D. Gözetleme Amacı

Kapalı devre kameraların gözetleme amacıyla kullanması, kamusal alanlarda bireylerin sergiledikleri davranışları ve faaliyetleri izleme ve çoğunlukla bu verilerin belirli başka amaçlar için kullanılması anlamına gelmektedir. Otoyollardaki trafiğin gözetlenmesi, MOBESE ya da EDS gibi sistemlerin kullanılması temelde bu amaca yönelik yapılan faaliyetlerdir. Gözetleme kavramı eskiden, somut bir kimsenin, başka bir kimse (çoğunlukla siyasi otorite) tarafından izlenmesi anlamına gelmekteydi²⁸³. Ancak enformasyon çağında izlenen somut birey olsa bile gözetleme faaliyetleri sonucunda kayıt altına alınan o bireyden elde edilen veriler olmaktadır. Bu nedenle, somut bireyin önemini yitirdiğini buna karşılık aynı oranda bireye ait kişisel verilerin önem kazandığını söylemek mümkün olabilir. Böylelikle gözetlemenin konusu da aynı şekilde somut olandan sayısal verilere doğru yön değiştirmiştir.

IV. Kapalı Devre Kamera Sistemlerinin Kullanım Alanları

Kapalı devre kamera sistemlerinin kullanımının yaygınlaşması şehirlerin gelişmesi ve daha karmaşık yapılar haline gelmesiyle olmuştur. Günümüz şehirlerini birbirine yabancı bireylerin bir araya gelerek oluşturduğu heterojen yapılar olarak tarif edebiliriz²⁸⁴. Bu heterojen yapılar içinde farklı etnik kökenlerden, sınıflardan, ırklardan, kültürlerden gelen insanlar yer almaktadır. Çoğu zaman şehirli her birey sosyo-ekonomik anlamda aynı şeyi hedefler: İnsan olmanın doğasında var olan kendini gerçekleştirebilmek arzusunu hayata geçirebilmek. Farklı geçmişlere sahip insanlar bu amaçlarını gerçekleştirebilmek için kentlerde yaşamayı seçmektedirler.

²⁸² Cüneyt AKINLAR, Yusuf OYSAL, Hüseyin POLAT, Efnan GÜNAL, s. 83.

²⁸³ David, LYON, Gözetlenen Toplum, s. 75.

²⁸⁴ Clive NORRIS, Jade MORAN, Gary ARMSTRONG, s.11.

Sosyal bir varlık olan insanın birlikte yaşama şekli, ortaya farklılıkların beslediği değişik görüşler ve çeşitlilikleri çıkarsa da aynı zamanda korku duygusunu beslemektedir. Çünkü birey kendisinden farklı olandan korkmaktadır. Ellin'e göre, yirminci yüzyılın sonlarında insanlar bu korkular sebebiyle, şehir yaşantısının sosyal güçlükleriyle yüzleşmek yerine daha çok içe kapanık, bölücü mimari projelere önem vermişlerdir²⁸⁵. Bu korkunun yönlendirmesiyle insanlar için güvenlik öncelikli bir konu haline gelmiş ve alınan tedbirlerle kentler birer kamusal düzen ve güvenlik yapılanmaları olmuştur.

Çağımızın gelişmiş enformasyon şehirleri aynı zamanda düzen, güvenlik ve gözetleme şehirleridir. Bu gözetleme daha önce bahsetmiş olduğumuz üzere modernite öncesinde şehir ışıklarıyla ve doğrudan nöbetçilerin gözleriyle yapılırken, artık kent yaşamının kameralar vasıtasıyla izlenmesi demektir. Dikkat etmemiz gereken nokta ise, eski tekniklerin tamamen ortadan kalkmamış olması, sadece yeni teknolojilerin gözetime katılmasıdır.

Kapalı devre video kameraların kullanımının gelişmesi açısından üç farklı etmen olduğunu söyleyebiliriz. Bunlar uzay-zaman ilişkisi, küreselleşme ve risk toplumunun ortaya çıkışıdır²⁸⁶. Kapalı devre video kamera sistemlerinin ortaya çıkmasıyla birlikte, video görüntülerinin gerçek zamanlı farklı mekanlar arasında aktarılabilmesi, kayıt altına alınması ve gelecekteki bir tarihte tekrar oynatılması imkanı doğmuştur. Böylelikle eski panoptik sistemin uygulanma alanı mekânsal ve zamansal anlamda genişletilmiştir. Küreselleşme ve beraberinde getirdiği ekonomik sonuçlar, kapalı devre kameraların gelişimi açısından önem taşımaktadır. Özellikle İngiltere' de pek çok şehir tüketim, eğlence ve turizm için güvenli ve çekici alanlar yaratmak amacıyla kapalı devre kameralardan yararlanmıştır. Sonuç olarak, karlılık peşindeki özel sektörün bu sistemin gelişmesinde payı oldukça büyüktür²⁸⁷.

Risk yönetimi açısından bakarsak, kenti yöneten yöneticinin kapalı devre kameralardan beklediği bir diğer netice sadece izlenen olayın kaydedilmesi değil, gözetlenenlerin hareketlerinin tahmin edilebilmesidir. Böylelikle gelecekte yaşanabilecek olaylar konusunda hazırlıklı olan yönetici oluşabilecek zararları en aza indirme konusunda avantaj sağlayacaktır.

²⁸⁵ Nan ELLIN, Korkunun Mimarisi, Princeton Architectural Press, New York 1997, s. 44'ten naklen David LYON, Gözetlenen Toplum, s. 116.

²⁸⁶ Clive NORRIS, Jade MORAN, Gary ARMSTRONG, s.11.

²⁸⁷ David, LYON, Gözetlenen Toplum, s. 121

1980’li yılların başında var olan ekonomik durgunluk sadece iş kuyruklarının uzamasına sebebiyet vermedi. Tüketici harcamalarındaki azalma uzun vadede şehirlerin alışveriş merkezleri tarafından çevrelenmesine de neden oldu. Şehir yöneticileri ise tüketicileri şehir merkezlerinde yer alan meydanlara, caddelere ve alışveriş alanlarına çekebilmek için bu alanları güvenilir hale getirmeye çalışmışlardır. Reeve’e göre, böylelikle kapalı devre kameralar kent merkezlerindeki kamusal alanların cazibe merkezi haline getirilmesinde bir araç haline gelmiştir²⁸⁸. Fakat kamusal alanda bulunan kameralar bununla sınırlı kalmamıştır. Gözetimin görünen yüzü kapalı devre kameralar evlerin etraflarında, işyerlerinde, alışveriş merkezlerinde hızla artarak çoğalmıştır.

Spor müsabakalarının yapıldığı alanlar, stadyumlar ve gösteri merkezleri de kentsel yaşamın kültürel öğeleridir. 1970’ler İngiltere’inde futbol stadyumlarının saha ile izleyicilerin ve rakip takım taraftarlarının bulunduğu alanlar yüksek demir tellerle birbirinden ayrılmaya başlanmıştır. 1 Mayıs 1982’de Londra derbisi diye adlandırılan Arsenal-Westham United karşılaşması sırasındaki olaylarda bir taraftar öldürülmüştür. Futbol ile ilgili şiddet uzun süre etkisini sürdürmüş, bunun neticesinde stadyumlar kör nokta kalmayacak derecede kapalı devre kameralarla donatılmıştır. 1998 yılı Dünya Kupası’ndan önce, 26 kişilik bir holigan grubu bir barda başka bir grupla kavga ettikleri gerekçesiyle polis tarafından göz altına alınmıştır. Olağan müdahale önlemleri yeterli olmayınca sis bombası bile kullanılan bu büyük kavgada, yaklaşık 60 kişi mahkeme karşısına çıkarılmış fakat Mahkeme barda yer alan kapalı devre kamera kayıtlarının aleyhte delil olmaya yeterli güce sahip olmadığı gerekçesiyle holiganları serbest bırakmıştır²⁸⁹.

Stadyumlar ve çevrelerinde kapalı devre kameraların kullanılmasının artması teknolojik gözetim araçlarının, daha önceki polis faaliyetlerine olan baskınlığını da gözler önüne sermektedir. Çünkü bu yeni gözetim, eskisi gibi sadece bireyin hareketine değil, bireyin dudak hareketlerine ya da basit jest ve mimiklerine indirgenmiş, çok daha detaycı, disipline edici bir gözetimdir. Bugün stadyumlarda sadece sahaya yabancı madde atanları tespiti yarayan sıradan kameraları değil; hakaret veya küfür içeren söz sarf edenlerin tespit edilebildiği ve hatta ısı algılayıcıları olan kamera sistemlerinin kullanıldığını görebiliriz. Bu gözetimin disipline edici olmasının sebebi ise bir kere kurallara uymadığı durumda bireyin yaptırımla karşılaşacağını

²⁸⁸ Clive NORRIS, Jade MORAN, Gary ARMSTRONG, s.69.

²⁸⁹ Andy NICHOLLS, Nick LOWLES, Hooligans 2: The M-Z of Britain's Football Hooligan Gangs, Milo Books, Birleşik Krallık 2007, Sunderland.

bilmesidir. Arsenal Futbol Kulübü karşı takım oyuncusuna su şişesi fırlatan bir taraftarını kapalı devre kamera sistemi vasıtasıyla tespit ederek hayat boyu stadyumuna almayacağını açıklamış ve gerekli cezayı kulüp olarak kendisi uygulamıştır. İngiltere Futbol Federasyonu ise bu tarz yaptırımların kulüpler tarafından uygulanmasının sevindirici olduğunu belirtmiştir²⁹⁰.

Bu yaygınlaşmanın bir nedeni de CCTV'lerin mevcut adalet mekanizması içerisinde suçun ve suçlunun tespit edilmesini kolaylaştırmasıdır. Çünkü kamera kayıtları kimin ne yaptığını açık bir şekilde ortaya koymaktadır. Önceki dönemlerde sadece şahitlerin görgüsü, itiraflar ya da yazılı dokümanlar ile sınırlı olan deliller, zamanla olay yeri izleri, vücut izleri, ayak izleri ve benzeri fiziksel kayıtları da kapsamına alarak teknolojik gelişmelerden payına düşeni almıştır. Şu anki süreçte ise parmak izlerinin analizi, yalan dedektörleri, DNA analizleri gibi daha güvenilir kanıtların sıklıkla kullanıldığını görmekteyiz. Bu yeni tekniklerin gelişimiyle birlikte olayların nasıl meydana geldiğine dair daha da kesin bilgilere ulaşabileceğiz. Ancak belirtilen tekniklerin bazıları sanıldığından daha az güçlü ya da tutarlı olsa da hukuk aktörleri tarafından bu kanıtların kesinliğine olması gerekenden fazla inanç duyulmaktadır. Bu duruma CSI etkisi de denilmektedir²⁹¹.

Geçtiğimiz yıllarda Florida'da bir hukuk profesörü evinin önünde gizemli bir şekilde öldürülmüştür. Bu olayın zanlıları bir halk otobüsünde, bir spor salonunun önünde, bir gişe ve ATM önünde yer alan kameralara yakalanmış ve bu hareketleri tamamen takip edilmiştir. Bir başka önemli örnek de 2013 yılında Boston'da meydana gelen bombalama olayının failinin Boston Maratonu'nun izleyicileri ve düzenleyicileri tarafından çekilen fotoğraflardan tespit edilmiş olmasıdır. Hükümet yetkilileri tarafından olaydan yalnızca üç gün sonra her iki şüphelinin kameralardan alınan görüntüleri çevreye asılabilmıştır²⁹². Bu örnekteki olayın

²⁹⁰ Arsenal escape FA action for coinh throat lingard- the second time they have avoided punishment for missile being launched from the crowd, <https://www.thesun.co.uk/sport/football/8357559/arsenal-escape-fa-action-coin-throw-lingard/> (s.y. 21 Ekim 2021)

²⁹¹ Jean R. STERNLIGHT, Justice in a Brave New World? Connecticut Law Review, C. 52, S.1, Y.2020, s. 223; CSI Etkisi ise, "...televizyon dizilerinde adli bilimsel yöntemlerin toplum üzerinde yanlış kanı ve inançlar oluşturabilecek şekilde abartılı bir biçimde kullanılması sonucunda ortaya çıkan etki..." olarak tanımlanmış olup, terim ilk kez 2002'de "CBS Early Show" ve "Time Magazine" içerisinde bir makalede yer almıştır. 2003 yılında Amerikan hukuk sözlüklerine dahil olmuştur. Ülkemizde ise 2010 yılında gösterime başlayan "Kanıt" dizisi bu etkiyi yaratan televizyon dizi örneklerinden bir tanesi olarak karşımıza çıkar. Bkz. Aylin YAKUPOĞLU, Can ÇALICI, Neylan ZİYALAR, "Suçların Aydınlatılmasında CSI Etkisi", Adli Tıp Bülteni, C. 21, S. 2, Y. 2016, s. 60.

²⁹² Samuel J. HODGE, s. 33.

çözümüne kavuşturulmasında kameraların gözetim amacıyla kullanılması, CCTV'lerin suçun ve suçluların tespiti açısından önemini bir kez daha gözler önüne sermiştir²⁹³.

Suçun önlenmesi ya da adaletin sağlanması amacına yönelik olarak bir kamera kaydını izlerken, bu kaydın içerdiği sekansı gözümüz ile görmüş kulağımız ile duymuş gibi yaşarız. Ancak bu kayıtlar her ne kadar objektif olarak değerlendirmeye çalışılsa bile aslında herkes izlediği görüntüyü kendi gözlerinden ve geçmiş deneyim değerlerinin süzgecinden geçirmektedir. Yüksek mahkeme yargıçları, polis arabası kamerasından gerçekleşen araç kovalamasını izlemiş ve polisin kendisine orantısız güç uyguladığına dair davalı iddialarını o video kaydını delil alarak değerlendirmişlerdir. Aynı kaydı izleyen 8 yargıç orantısız güç uygulandığına dair iddiaları geçersiz bulurken bazı hakimler ise farklı karara varmışlardır. Bu farklı görüşlerden yola çıkılarak yapılan araştırma da ise farklı geçmişlere sahip 1350 kişiye aynı olayı değerlendirmesi istenmiş bu araştırma neticesinde de aynı görüntüye ilişkin farklı kanaatlere varıldığı tespit edilmiştir. Gerek hakimler gerek katılımcılar açısından bir grubun diğerine kıyasla daha haklı olduğunu söylemek bu açıdan zordur. Araştırmalar, kişinin algısının geçmiş deneyim ve inançları doğrultusunda yönlendirildiğini göstermiştir²⁹⁴.

Yukarıdaki örnekleri değerlendirdiğimizde CCTV gözetiminin suçun önlenmesi ve adaletin sağlanması amacıyla kullanılmasının toplumun genelinde kabul gördüğünü söylememiz mümkündür. Bu durum aynı zamanda CCTV'lerin kullanımlarını da yaygınlaştırmıştır. Bu yönlerden desteklenmesi gereken bir uygulama olduğunu kabul edebiliriz. Fakat bu uygulama yasal düzenlemeler çerçevesinde ve ölçülü olarak yerine getirilmesine rağmen, yukarıdaki örnekte olduğu gibi delilleri değerlendirenlerin ön kabulleri nedeniyle bir olumsuzluk yaşanmaktaysa, görüntülerdeki bireylere buna karşı etkin itiraz yolları tanınması da gerekecektir.

Kapalı devre kameraların kullanım alanlarını 3'e ayırarak incelememiz mümkündür: (i) kamusal alanlarda kapalı devre kamera sistemlerinin kullanımı (ii) işyerinde kapalı devre kameraların kullanımı (iii) kamuya açık olmayan yerlerde kapalı devre kamera kullanımı.

²⁹³ Jean R. STERNLIGHT, s. 224.

²⁹⁴ A.g.m., s. 242.

A. Kamusal Alanlarda Kapalı Devre Kamera Sistemlerinin Kullanımı

1. Kolluk Faaliyetlerinde Kapalı Devre Kamera Sistemlerinin Kullanımı

İnsanların topluluk halinde yaşayabilmeleri için belli bir hukuksal düzenle birlikte huzur ve güvenliklerinin tesis edildiğinin bilincinde olmaları gereklidir. Toplum yaşamı için olmazsa olmaz bu düzen devlet tarafından oluşturulmalıdır. Bu düzen içerisinde bireylerin güvenlik, dirlik ve esenliğini sağlamak idarenin ve dolayısıyla devletin sorumluluğundadır. Devletin kamu düzenini sağlarken birey ile karşı karşıya gelmesine sık rastlanmaktadır. İdare tarafından kolluk faaliyetlerinin bireylerin temel hak ve özgürlüklerini sınırlayabildiği, buradaki sınırlandırmanın amacının ise kamu düzeninin sağlanması olduğu görülmektedir²⁹⁵.

İdare tarafından kamu düzeninin sağlanması, korunması ya da bu düzenin bozulması durumunda eski hale getirilmesi için bireysel ve toplumsal davranışların düzenlenmesi ve de toplum düzenine aykırı eylemleri kuvvet kullanarak önlemesi amacıyla oluşturduğu teşkilata, yürütülen faaliyete ve bu faaliyeti yerine getiren personele “kolluk” adı verilmektedir²⁹⁶. Kolluk sadece bir faaliyeti değil, bu faaliyeti yürütmekle görevli olan personeli de içeren daha geniş bir kavram olarak karşımıza çıkmaktadır²⁹⁷.

Kamu düzenini oluşturan unsurlar ise güvenlik, dirlik ve esenlik, genel sağlık ve genel ahlaktır²⁹⁸. Güvenlik, “*toplumun, onu oluşturan bireylerin, onların kişilik hakları ve insanlık onurlarının, kamusal ve kişisel malların, her türlü tehlike ve kazalardan korunması*” olarak tanımlanmaktadır²⁹⁹. Kapalı devre kameraların kullanılmasının bireyler açısından güven sağladığı bir gerçektir. Ancak güvenlik tesis etmesinin yanı sıra bu araçların kamu düzeninin diğer unsurlarını da koruduğu ve tesis etmeye yaradığı görülmektedir.

²⁹⁵ Turan YILDIRIM, Melikşah YASİN, Nur KAMAN, Eyüp ÖZDEMİR, Gül ÜSTÜN, Özge Okay TEKİNSOY, İdare Hukuku, 6. Baskı, On İki Levha, İstanbul 2016, s. 543.

²⁹⁶ Bahtiyar AKYILMAZ, Murat SEZGİNER, Cemil KAYA, Türk İdare Hukuku, 1. Baskı, Seçkin, Ankara 2009, s. 471.

²⁹⁷ Şeref A. GÖZÜBÜYÜK, Turgut TAN, İdare Hukuku, Genel Esaslar, 6. Baskı, Turhan Kitabevi, Ankara 2008, s. 746.

²⁹⁸ Turan YILDIRIM, Melikşah YASİN, Nur KAMAN, Eyüp ÖZDEMİR, Gül ÜSTÜN, Özge Okay TEKİNSOY, s. 546.

²⁹⁹ Bahtiyar AKYILMAZ, Murat SEZGİNER, Cemil KAYA, s. 473

Toplumsal gnlk hayatın akışını engelleyen her trl dzensizlik, ses ve grnt kirlilięi, karışıklık ve kargaşadan korunmasını ifade eden dirlik ve esenlik³⁰⁰ unsuruna ya da bireylerin ahlak anlayışlarının olumsuz olarak dışa yansımaları yani olumsuz davranışlarının, toplumun dzenini bozacak veya sarsacak nitelikte olduęu durumlarda genel ahlak unsuruna³⁰¹ aykırı fiiller olduęu sylenebilir. Dolayısıyla bu aykırı fiiller kamu dzeninin bozulmasına sebebiyet verebilir. O halde burada deęerlendirilmesi gereken husus kamu dzeninin bozulduęu ya da bu ynde bir tehdidin bulunduęu durumlarda kolluk CCTV'ler aracılığıyla gzetim yapabilecek midir?

Kolluęun faaliyetlerinin amacı kamu dzeninin korunması ve bozulan kamu dzeninin yeniden tesis edilmesidir. Bu amaca ynelik olarak gvenlięin saęlanması, konut dokunulmazlığının saęlanması, toplum yaşamını tehdit eden salgın ve bulaşıcı hastalıkların nlenmesi, toplumu oluşturan bireylerin toz, grlt, duman gibi dış etkenlerden korunması, evrenin korunması ve evreyi tehdit eden unsurların ortadan kaldırılması, toplumsal dzeni bozucu genel ahlaka aykırı davranışlara engel olunması, tarihi eser ve anıtların korunması gibi faaliyetler kolluęun yerine getirmekle ykml olduęu faaliyetlerden bazılarıdır. Kapalı devre kameraların kullanım amalarıyla neredeyse tamamen aynı olan bu faaliyetlerin hepsinde gzetim unsuru olarak CCTV sistemlerinin kullanılabilir. Yine bunlara ek olarak trafik akışının dzenlenmesi, sınır gvenliğinin ve ormanların korunması gibi kolluk faaliyetlerinin de CCTV sistemleri aracılığıyla yapılması imkanı bulunmaktadır.

Kolluk faaliyetleri lkemizde idari kolluk ve adli kolluk olarak ikiye ayrılmaktadır. İdari kolluk kamu dzenini, bozulmasından nce alınan tedbirler vasıtasıyla korumayı ifade ederken; adli kolluk ise, kamu dzeni bozulduktan sonra, suun faillerinin tespit edilmesi, su delillerinin bulunması ve bunların adli makamlara teslim edilmesi yoluyla bozulan kamu dzeninin yeniden saęlanmasını ifade etmektedir³⁰². İdari kolluk ve adli kolluk aynı teşkilat ve personel tarafından yerine getirilmekte olup, sadece ama ynnden birbirlerinden ayrıldıkları sylenebilir. İdari kolluk deyimini yerine "nleyici kolluk" deyiminin de kullanıldığđ grlmektedir³⁰³. Kapalı devre kamera sistemlerinin, her iki kolluk tr tarafından faaliyetleri kapsamında kullanıldığđ aıka grlmektedir.

³⁰⁰ A.g.e., s. 473

³⁰¹ A.g.e., s. 474

³⁰² A.g.e., s. 474.

³⁰³ Turan YILDIRIM, Melikşah YASİN, Nur KAMAN, Eyp ZDEMİR, Gl STN, zge Okay TEKİNSOY, s. 549.

Günümüzde uluslararası boyutta etkisini gösteren ve Dünya Sağlık Örgütü tarafından 30 Ocak 2020 tarihinde uluslararası kamu sağlığı sorunu ve 11 Mart 2020’de pandemi olarak kategorize edilen, Covid-19 pandemisi³⁰⁴ insanların, kamu sağlığı gerekçesiyle öngörülemeyen bir takım kısıtlamalara maruz kalmalarına sebebiyet vermiştir. Kriz dönemlerinde neredeyse tüm toplumlar birbirine benzer politikalar izler. Bir takım haklar askıya alınır, gözetim yoğunlaştırılır, bürokrasinin etki alanı genişler, sınırlar kapatılır, ticaret ulusal pazara yönelir, düzenlenir ya da tamamen son bulur³⁰⁵. Kamu düzeninin diğer bir unsuru olan genel sağlık, toplumu oluşturan bireylerin bulaşıcı ve yaygın hastalıklardan korunması ve insan yaşamının sağlıklı³⁰⁶ bir ortamda sürdürülebilmesidir³⁰⁷.

Burada güncel bir probleme değinmemiz gerekir. Kamu düzeninin bir başka unsuru olan genel sağlığın korunması açısından Covid-19 ile mücadeleye dair gerekli önlemlerin alınması zorunlu olarak görülebilir. Kamusal alanların özellikle havalimanlarının termal kameralar ile gözetlenmesi bu sebebe yönelik olarak yürütülen faaliyetlerden bir tanesidir. Salgın dönemlerinde bir takım temel hak ve özgürlüklerin kısıtlanması mümkün olarak gözükse de ilk olarak hakların özü itibariyle sınırlandırılmaya elverişli olup olmadığının tespiti gereklidir. Sınırlandırmaya elverişli haklar sadece bir takım şartlar altında sınırlandırılabilirken, yaşam

³⁰⁴ Preparing for Large-scale Community Transmission of Covid-19, Guidance for Countries and Areas in the WHO Western Pacific Region, World Health Organization, 28 Şubat 2020, s. 1; Dünya Sağlık Örgütü Genel Direktörü tarafından yapılan açıklamada, “11 Mart 2020 tarihi itibariyle 114 ülke genelinde 118,000’den fazla sayıda hasta bulunduğu ve 4,291 kişinin yaşamını yitirdiği, hala bir çoğunun hastanelerde tedavi görmekte olduğu belirtilmekle, içinde bulunulan durumun ciddiyeti sebebiyle Covid-19 uluslararası kamu sağlığı sorunu iken pandemi olarak kategorize edilmiştir”, WHO Director-General’s opening remarks at the media briefing on COVID-19, 11 Mart 2020, <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> (s.y. 28 Kasım 2021)

³⁰⁵ Astrid BROUSSELLE, Emmanuel BRUNET-JAILLY, Christopher KENNEDY, Susan D. PHILLIPS, Kevin QUIGLEY, Alasdair ROBERTS, Beyond COVID-19: “Five Commentaries On Reimagining Governance For Future Crises And Resilience”, Canadian Public Administration, C. 63, S. 3 , 2020, s. 371.

³⁰⁶ Gemalmaz’a göre, “AİHS sisteminde md.2 ve vakanın özelliğine göre md. 3 bağlamındaki “pozitif yükümlülük” kategorileştirilmesi vesilesiyle, ikinci kuşak haklardan addedildiği için Sözleşmede yer verilmemiş olan “sağlık hakkı” kavramı içinde mütalaa edilebilecek bazı edimlerin, Sözleşmeciler Devletlere yüklediğine” dikkat edilmektedir. “Avrupa İnsan Hakları Komisyonu’nun “İşiltan, Türkiye’ye karşı” davasında verdiği 22/05/1995 tarihli kabul edilmezlik kararında, Komisyon, Devletin (kişilerin) yaşamını korumak bakımından pozitif yükümlülüklerinin, hastanelerin hastaların yaşamını korumak için hastanelere yönelik gerekli düzenlemeleri yapmasını içerdiğini ortaya koymuştur.” Keza “Calvelli and Ciglio İtalya’ya karşı” kararında, Avrupa İnsan hakları Mahkemesi, Devletin, “kişinin yaşamını güvence altına almaya yönelik önlemler alması şeklindeki pozitif yükümlülüğünün “ kamu sağlığı alanına da uygulanır olduğunu” belirtmiştir. Bunun gibi “Makaratsız Yunanistan’a karşı” kararında belirtildiği üzere, “AİHS (m.2/1) hükmü çerçevesinde bireyin yaşamını tehlikeye düşüren hastalık riskine karşı onun yaşamını koruma şeklinde bir pozitif yükümlülüğün bulunduğu söylenebilir. Mehmet Semih GEMALMAZ, Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş, 7. Baskı, Legal, İstanbul 2010, s. 148.

³⁰⁷ Bahtiyar AKYILMAZ, Murat SEZGİNER, Cemil KAYA, s. 473.

hakkı ya da işkence ve diğer zalimane, insanlık dışı ya da aşağılayıcı muamele ya da ceza yasağı gibi bazı hakların herhangi bir şekilde sınırlandırılması mümkün değildir³⁰⁸.

Sınırlanılmaya elverişli haklar, hakların sınırlandırılması için öngörülen koşullar çerçevesinde sınırlandırılabilirler. Bununla birlikte, yapılacak sınırlamaların “sınırlamanın sınırı ölçütleri”ne uygun olarak yapılması yani hakkın özüne dokunmaması gereklidir³⁰⁹. Bu uygulamadaki sınırlandırmanın özel hayatın gizliliğine ilişkin olması nedeniyle Anayasa’nın 20. maddesinde yer alan “*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; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.*” hükmünün uygun düştüğü ölçüde uygulama bulacağı söylenebilecektir. Ancak buradaki sınırlandırma doğrudan bireylerin aranması ve el koymaya ilişkindir. Bununla birlikte yine aynı Anayasa maddesinin 3. fıkrasında “*Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir.*” denilmiş olmaktadır. Kişisel verilerin işlenmesine ilişkin bu özel sınırlandırma sebebinin uygulanabileceği mümkün gözükse de gerçekleştirilen uygulamanın kanuni bir düzenleme dayanmadığını söyleyebiliriz. Neticede, bahsi geçen Anayasal düzenlemelere riayet edilmeden yapılan her türlü sınırlandırmanın keyfi olarak yapıldığı ifade edilebilir.

Hakların sınırlandırılmasında diğer bir unsur, sınırlandırmanın “gerekliliği” ve “yasayla” yapılmasını ifade eden koşullardır. Ancak her ne kadar bir hakkı sınırlandırmak için sınırlandırma ölçütleri var olsa da sınırlandırma gerekli ve yasa ile yapılmışsa da bu sınırlandırmanın nerede durması gerektiğini ortaya koyan “sınırlandırmanın sınırını” belirleyen bir standart bulunmaktadır³¹⁰. Anayasa’nın 13. maddesinde belirtildiği üzere, “*Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve*

³⁰⁸ Mehmet Semih Gemalmaz, Ulusalüstü İnsan Hakları, s. 1638.

³⁰⁹ Mehmet Semih GEMALMAZ, Temel Belgelerde İnsan Hakları: Maddi Hukuk, İnsan Hakları Derneği Yayını, İstanbul 1996, s. 309-323.

³¹⁰ Mehmet Semih Gemalmaz, Ulusalüstü İnsan Hakları, s. 1634

ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.” Bu bakımdan sınırlandırmanın sınırı için iki standart bulunduğunu söyleyebiliriz. Yapılacak sınırlandırma demokratik toplum düzeni için gereklerine uygun olarak yapılmalı ve ayrıca sınırlandırmanın hakkın özüne dokunmuyor olması gerekmektedir. Dolayısıyla Covid-19 ve genel sağlık nedeniyle de olsa kişilerin özel yaşamlarının gizliliği hakkının sınırlandırılması her daim yukarıdaki koşullara bağlı olarak yapılabilecektir. Sonuç olarak, yapılacak sınırlandırmanın bireylerin haklarının özüne dokunmaması ve kanun ile yapılması gereklidir.

Son zamanlarda küresel düzlemde kolluk faaliyetleri kapsamında gerçekleştirilen gözetim, etki alanını genişletmeye başlamıştır. Özel teşebbüsler ve bireyler kendileri için gerçekleştirdikleri gözetim faaliyetlerini polis ağlarına entegre etmektedirler. Bunun kolluk (ya da yerel yönetimler) tarafından neden desteklendiği ise aslında her iki tarafında kazandığı kazançlı bir hamle olmasından kaynaklanır. Şöyle ki, kolluk tarafından gözetlenmesi düşünülen her alana kamera yerleştirerek bunları şehrin video yönetim sistemine bağlamak zor ve pahalı bir iştir. Bunun yerine işletmelerin ya da yerleşimcilerin kendilerine ait kameraları polis ağlarına bağladıkları görülmektedir. Bu işbirliğine bağlı gözetim ağı denilmektedir³¹¹. Amerika Birleşik Devletleri’nde yer alan Detroit bu şekilde bir işbirliğine ev sahipliği yapmaktadır. Yeşil Işık projesi adı verilen bu işbirliğine işletmeler satın aldıkları CCTV’leri doğrudan polis merkezindeki sisteme bağlamaktadırlar. Yurttaşların kameraların doğrudan polis ağına bağlı olduğunu gösterme konusunda ise kameraların yanına yeşil ışık yerleştirilir. Suç işlemenin engellenmesine yönelik olarak yurttaşlara verilen mesaj açıktır: “Polis seni izliyor!”

Gelişen teknoloji ile birlikte kolluk faaliyetleri kapsamında kullanılan bir başka kamera türü ortaya çıkmış ve dünya çapında polis güçlerinin ilgisini çekmiştir. Polis vücut kamerası (PVK) adı verilen bu kameralar çağdaş tekno-bürokratik düzlem içerisinde akıllı bir “uzman sistem” olarak tanımlanmaktadır. Bu kamera sistemlerinin standart kapalı devre kameralardan tek farkının herhangi bir yere monte edilmemiş olmaları ve sürekli olarak polisler tarafından taşınmaları gösterilebilir. Hatta bunlara küçük taşınabilir CCTV’ler diyebilmek

³¹¹ Michael KWET, The Rise of Smart Camera Networks, and Why We Should Ban Them, The Intercept, Police are using cameras at private businesses and homes, along with AI, to expand their video surveillance raising privacy concerns. January 27 2020, 8:53 p.m. <https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/> (s.y. 15 Kasım 2021)

mümkündür³¹². Ancak bu yeni uygulamanın attan önce araba yaklaşımı benimsenerek, henüz sınırları belirlenmeden ya da kullanılmasındaki ölçülülüğün değerlendirilmesine fırsat verilmeden polislik faaliyetlerinde kullanılmasının yanlış olduğu söylenebilir³¹³.

PVK'ların kolluk faaliyetlerinin güvenilirliğini artırdığı yönünde bir değerlendirme yapabiliriz. Çünkü bu kameralar kolluğun yurttaşlarla yüz yüze bulunduğu her faaliyete şeffaflık getirmektedir. Şeffaflık ise beraberinde toplumun kolluğa olan güveninin artmasını sağlamaktadır. Bu kameralar kolluğun orantısız (aşırı) güç kullandığını, yolsuzluğu, rüşveti ya da polisin hatalı davranışlarını ortaya çıkaracaktır. Burada sayılan sebepler yurttaşların PVK'ların kullanılmasını istemesine sebep olabilir, bununla birlikte polis otoriteleri de bu uygulamanın artırılmasından yanadır. Çünkü bu sistemler kolluk açısından da muhatabı oldukları ya da olabilecekleri dayanaktan yoksun şikayetlerden korunma kolaylığı sağlamaktadır³¹⁴. Olumlu olarak görülen bu özellik aslında tüm benzer kapalı devre kameraları açısından vurgulanmaktadır. Bu kameralar aracılığıyla elde edilen görüntüler sayesinde gerçek iddialar ile sahte ya da asılsız iddialar kolaylıkla ayrıştırılmakta ve bu da soruşturma sürelerinde ve iş yükü açısından tasarruf olarak görülebilmektedir³¹⁵.

Polis vücut kameraları görev başındaki polis memurlarının tüm mesai süreleri boyunca kayıt yapmakta ve görüntülerde yer alan şahısların yüz taramalarını yapıp milyonlarca fotoğrafla karşılaştırarak bu şahısların kimlik tespitlerini gerçekleştirmektedir. Sistem aslında o kadar kalitelidir ki görüntüye giren bir kimsenin kimlik tespiti ekranda belirip bu kişi bir kez etiketlendiyse, arkasını dönse bile etiketli olarak belirmeye devam eder. ABD'de düzenlenen bir gösteride bu kameralara yansıyan bir örnekte, kalabalığı dağıtan polis vücut kamerasında katılımcılar arasındaki bir kadının – yüzünün tanınmasını önlemek için Black Lives Matter yazılı bir bandana takmıştır – gösteriyi örgütleyen kişiye yumruk attığı tespit edilmiştir. Yüz görüntüleme sistemi yumruk atan kişinin yüzünün neredeyse yarısı kapalı olmasına rağmen kimlik eşleştirmesi yapabilmeyi başarmıştır. Sistem aynı zamanda eşlemeyle birlikte kadının Charlottesville'deki ikamet adresini de göstermektedir. Polis bu görüntüleri izledikten sonra adresine gidip yaklaşık bir saat içinde kadını kendi evinin önünde kaldırımda gözaltına

³¹² Bryce Clayton NEWEL, *Police On Camera: Surveillance, Privacy and Accountability*, Routledge, New York 2020, s.28.

³¹³ A.g.e., s.27.

³¹⁴ A.g.e., 51.

³¹⁵ Samuel J. HODGE, s. 33.

almıştır³¹⁶. Böylece uygulamanın polislik faaliyeti açısından faydalarını görebilmekteyiz. Ancak Amerika'nın Virginia eyaletindeki bazı polis departmanları tarafından kamusal protestolarda vücut kameralarının kayıt yapmalarının yasaklandığını görmekteyiz³¹⁷. Bu bağlamda kamera görüntülerinin kayıt altına alınmaması şüphelinin tespit edilememesine neden olacaktır.

Tüm bunlara yönelik olarak Guzik, *“bu teknolojinin insan zihninde bıraktığı objektiflik algısının kolluk faaliyetlerinin hareketlerine boyun eğme etkisi yaratabileceğine değinerek, polislere yöneltilecek şikayetlerin azalacak olmasının daha büyük bir endişe kaynağı olması gerektiğini ve azalan şikayetleri iyi görme eğilimine direnilmesinin yerinde olacağını”* belirtmektedir. Bu ifadeyi somutlaştırmak açısından şu şekilde bir örnek verilmesi mümkündür. Örneğin; polis memurları olay raporlarının yaşananlarla örtüşmesini sağlamak için video görüntülerini kullanabilirler. Bu durum memurların hatırladıkları gerçek ile yaşananlar arasındaki tutarsızlıkları azaltabilir. Sonuçta yurttaşlar ya da savunma avukatlarının yaşananlara itiraz etmeyecekleri ve bu hakkı kullanmalarının azalması ihtimali gündeme gelir. Keza günümüzde çoğunlukla kolluğun kendi aleyhine yapılan şikayetleri dikkate almakta gönülsüz olduğuna dair çok sayıda kanıt bulunmaktadır³¹⁸. Buna ek olarak, PVK'lar üzerinde hakimiyetlerinin de bulunduğu düşünüldüğünde yurttaşlar tarafından talep edilen kayıtların gösteriminin ertelenmesi ihtimali de söz konusu olacaktır³¹⁹. Yukarıdaki gibi bir durumda itiraz hakkının sık kullanılmaması o hakka dair hak bilincini giderek azaltır. Bu da zamanla ilgili hakkın artık korunamayacak olması anlamına gelir.

Kişisel verilerin korunması bağlamında bu kameralarının sürekli olarak kayıt yapıyor olması veri işlemenin ölçülülüğünün değerlendirilmesini gerektirir. Amerikan Sivil Özgürlükler Birliği'nin PVK'lar için yayınladığı bildiriye göre³²⁰, *“Güvenirlilik açısından vücut kameralarının ideal çalışma şekli, polis memurlarının mesailerinin başlangıcından sonuna kadar tüm süreyi kapsayacak şekilde hiçbir duraklama olmaksızın kaydedilmesi şeklinde olmalıdır. Ancak bu şekilde memurun görev başında bulunduğu sürede gerçekleştireceği görevi kötüye kullanma faaliyetlerini saklama ihtimalinin ortadan*

³¹⁶ Julian R. MURPHY, Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests. Washington and Lee Law Review Online, S. 75, Y. 2018, s. 3.

³¹⁷ A.g.m., s. 6.

³¹⁸ Bryce Clayton NEWEL, s. 59.

³¹⁹ A.g.e., s. 58.

³²⁰ Jay STANLEY, Police Body-Mounted Cameras: WithRight Policies in Place, a Win For All, Version 2.0, American Civil Liberties Union (ACLU) Policy, 2015, s.3.

kaldırılabilir. Buradaki sorun sürekli olarak kamera kaydı yapılmasının hem halk hem de memurlar için bir mahremiyet problemi doğurmasıdır.” Birliğin raporunda sürekli olarak yapılan gözetimin büyük bir gözetim faaliyeti olduğu da aynı zamanda vurgulanmıştır.

Yani polis memurlarının video kayıtlarını yönlendirememesi sağlanmalı ama aynı zamanda verilerin korunmasına yönelik olarak da kayıt işlemine bir limit getirilmesi gereklidir. Bu kameralara entegre edilecek bir otomatik tetikleyicinin çözüm olarak kullanılması mümkün olabilir. Örnek vermemiz gerekirse, kameralar seslerin yükseldiği durumda ya da belirli bir hareket algılayıcısının çalışması ile kayıt almaya başlayabilir. Polis otomobillerine bağlı kameraların sirenlerin ya da ışıkların çalışmasıyla birlikte kayda başlaması bu bakımdan örnek gösterilebilir. Bir diğer çözüm bu sistemlerin sadece yurttaş ile temas anında kullanılmasının sağlanması olarak görülebilir. Bu durumda özellikle memurların kendi aralarında yaptıkları konuşmalar kayıt altına alınmaz ve mahremiyetleri korunabilir. Son bir çözüm ise veri korumanın temel ilkelerinden biri olan toplandığı amaç için kullanılması gerekli olmayan verinin silinmesi veya imha edilmesinin sağlanmasıdır. Verinin imha süresi yıllarla değil haftalarla sınırlı olmalıdır. Daha uzun süre ile muhafazası gereken bir video kaydının işaretlenerek muhafazası sağlanabilir. Hangi durumlarda işaretleme yapılacağı ise şu şekilde belirtilmiştir: (i) güç kullanımı söz konusuysa, (ii) göz altına alma ya da yakalamalarda, (iii) Sözlü ya da yazılı şikayetlerin kayda alınması durumunda³²¹. Ayrıca bu teknolojinin Anlık Yüz Tanıma teknolojisi (AYT - Live Facial Recognition) içeren gelişmiş örnekleri de olduğunu da söylememiz gerekir.

Yeni bir başka teknoloji olan Anlık Yüz Tanıma teknolojisi polislerin kamusal alanlarda anlık olarak bireylerin yüz tanımlarını yapabildikleri bir görüntüleme sistemidir. AYT teknolojisi gelişmiş veri eşleme ve biyometrik veri işleme faaliyetleri yürütmekle birlikte CCTV'lere ya da plaka tanımlama araçlarına benzemekle birlikte örneğin, CCTV'lerden farklı olarak, yüz özellikleri üzerinden tanıma ve izleme faaliyetlerini otomatikleştirir ve belirli bir kişinin tanımlanmasında biyometrik verileri gerçek zamanlı olarak işler³²². Standart bir yüz tanıma teknolojisi içeren CCTV'den farklı olduğu nokta ise normal yüz tanıma teknolojilerinin tipik olarak kameraların kayıt altına aldığı yüz görüntüsü ile veri tabanında yer alan başka bir

³²¹ Örnek olarak, Washington Eyaleti için işaretlenen verinin saklanması süresi maksimum üç yıl olarak belirlenmiştir. Bkz. Jay STANLEY, s.6.

³²² Ben BRADFORD, Julia A. YESBERG, Jonathan JACKSON, Paul DAWSON, Live Facial Recognition: Trust And Legitimacy as Predictors of Public Support for Police Use of New Technology, The British Journal of Criminology, C. 60, S 6, Y. 2020, s. 1504.

görüntünün biyometrik eşlemelerinin yapması yani diğer bir deyişle bire bir işleme söz konusu iken, AYT'ler ise kameraların görüntüsüne giren her bir bireye ait biyometrik verinin otomatik olarak yakalar ve herhangi bir ayırım yapmadan kimlik tespiti yapar. Ardından kolluk kuvvetlerini ilgi alanlarına giren bir arananın bulunduğundan haberdar eder. Toplanan toplam verinin büyüklüğü göz önüne alındığında bu tekniğin kullanılması niteliği gereği belirli bir ölçüsüzlüğü beraberinde getirir³²³. Bu ölçüsüzlüğün veri koruma hukuku açısından doğurduğu sorunun giderilmesi açısından ise herhangi bir arama listesi ile eşleşmeyen ve fakat görüntülere girmiş oldukları için kayıtlanan biyometrik verilerin anında ortadan kaldırılacağı Londra Emniyeti tarafından teyit edilmiştir³²⁴. Eşleşme sağlanan kayıtlar en fazla otuz gün muhafaza edilmektedir.

Polislerin AYT'leri kullanmasının hukuki anlamda meşruluğunu ve bu alandaki mahremiyet kaygısına detaylı olarak yaklaşmak gerekmektedir. Bu yeni teknolojiye meşruluk kazandıran en büyük etken pek tabi ki güven etmeni olacaktır. Güven ve meşruluk birbiriyle bu yönden yakın bir ilişki içinde bulunur. Gücün uygun şekilde kullanıldığına güven duymak, gücün haklı olarak elde tutulduğuna inanmayı gerektireceğinden, polisin normatif olarak elindeki gücü uygun kullandığına inanıldığı bir durumda, aslında bu yetki ya da gücün kullanımına dair bir meşruluğun bulunduğu varsayılabilir³²⁵.

Bu yeni teknoloji tam anlamıyla bir biyometrik veri kontrol noktası olarak görülmekte olup, bireysel mahremiyete ya da sosyal bir norm olarak mahremiyete olan etkileri yadsınamaz. Yukardaki açıklamalarla bağlantılı olarak mahremiyet kaygılarının da bu yeni teknolojiye duyulan güvene ve meşruluğuna bağlı olarak değişebileceğini söylemek mümkündür. Yani polisin bu yeni aracı uygun ve ölçülü olarak, gerekli amaçlar dahilinde kullandığına güvenen birey bu faaliyetleri gözünde meşrulaştırır ve bu nedenle mahremiyet kaygısı bastırılmış olur³²⁶.

Bu teknoloji sadece aranan suçluların tespit edilmesi ve yakalanmasında değil, örneğin pazarlama ve tanıtım faaliyetlerinde de kullanılabilir. AYT sistemi görüntü alanına giren bir bireyi tespit edip, bu bireyin yaş, cinsiyet, etnik grup, kıyafet gibi bir takım özelliklerini

³²³ Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places, 18 Haziran 2021, s. 4, <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places20210618.pdf> (s.y. 11 Kasım 2021)

³²⁴ A.g.m., s. 1504.

³²⁵ A.g.m., s. 1506.

³²⁶ A.g.m., s. 1507.

tarayıp analiz ettikten sonra bu birey hakkında bir profil oluşturabilir. Eş zamanlı olarak beraberinde olan reklam panolarında oluşturulan bu profile göre bir reklam yansıtabilir³²⁷. Buna örnek olarak Londra'nın en işlek ve popüler kesişim noktalarından biri olan ve yılda yaklaşık 100 milyon insanın yürüyerek geçtiği Piccadilly Circus'a 2017 yılının Ekim ayında yerleştirilen yüksek çözünürlüklü reklam panoları, beraberindeki teknolojiyle birlikte inşaların yaşlarına, cinsiyetlerine ve hatta duygularına göre içerikleri yayalara sunmaktadır. Bu platformların yüz tanıma sistemleri kullanması bir takım mahremiyet tecavüzü iddialarını da beraberinde getirmiştir. Bu platformların tüm dünya çapında önde gelen üreticilerinden biri olan Quividi tarafından yapılan açıklamaya göre, sistemin kişilerin kimliklerinin tespitine yarayacak herhangi bir veri, bir video ya da görüntü kaydetmediği vurgulanmıştır. Quividi tarafından kullanılan algoritma video görüntülerini sadece bir an için işlemekte ve tüm işlenen veriler tamamen sistem içerisinde gerçek zamanlı olarak işlenmektedir³²⁸.

Yukarıdaki örnekte olduğu gibi biyometrik verilerin çok hızlı ve geniş çapta otomatik olarak toplanması, bireylerin verileri üzerindeki hakimiyetinin az olması, şeffaflığın azlığı, AYT sistemlerinin teknik kapasiteleri ve istatistiksel olarak tutarlılığı, ön yargı ve ayrımcılığa sebebiyet verme potansiyeli, arama listelerinin doğru bilgiyi barındırmama olasılığı ya da çocukların ve yardıma muhtaç yaşlıların zarara uğrama olasılıkları bakımından ayrı ayrı değerlendirme yapılması gereklidir³²⁹. Bu teknolojinin büyük ölçekli verileri nasıl işlediği görülmektedir. Ekranı kimin girdiğine dair bir sınırlandırma yapılmadığına göre herkes, kendisinden herhangi bir onay alınmadan ya da bilgisi olmaksızın verisi işlenen olabilir. Bu bakımdan bireylerin rıza göstermesi aranmayacaktır. Rıza alınmasının kullanılan sistemlerin nitelikleri gereği işin doğasına aykırı olacağını öngörebilmek mümkündür. Fakat en azından ilgili kişilerin süreçlere aktif bir şekilde katılmadıklarını göz önüne alarak veri işlemenin açık, gerekli, ölçülü ve şeffaf olarak yapılmasını sağlamalıdır.

2. Yerel Yönetim Faaliyetleri Kapsamında Kapalı Devre Kamera Sistemlerinin Kullanımı

19. yüzyılda açıldığı andan beri Londra Underground metrosunda intihar vakalarına sıklıkla rastlanılmaktadır. Sadece 2000-2010 yılı arasında toplam 643 kişi bu metro raylarına

³²⁷ Information Commissioner's Opinion, s. 18.

³²⁸ Peter Alexander EARLS DAVIS, s. 366.

³²⁹ Information Commissioner's Opinion, s. 19.

atlayarak intihar etme girişiminde bulunmuştur.³³⁰ Bu ve benzeri birtakım bireysel ya da toplumsal olayların, terörizm, şiddet, saldırı, alkol ve sigara kullanımı, yangın riski, yasak yerlere giriş, diğer güvenlik önlemlerine uyulmaması vb. gibi, önüne geçmek için kurulmuş bir görüntü işleme algoritması olan Cromatica, kapalı devre kameraların kullanılması ile izlenenlerin hareketlerini gözlemleyen ve izlenenlerin bir sonraki hareketlerini tahmin ederek sistemi kullananlara uyarı veren bir sistemdir³³¹.

Sistemde kullanılan algoritma sayesinde normal şartlar altındaki kalabalık akışlarının ölçülmesi, eğer bu akışta bir sorun varsa doğru yönlendirmenin sağlanması, aşırı yoğunluk, çok uzun sıralar gibi kalabalıkların oluşturduğu ya da bireylerin olağanüstü faaliyetlerinin tespit edilmesi sayesinde yöneticiler birçok sorunu daha meydana gelmeden çözebilme şansına sahip olmuşlardır. Sistemin en büyük getirisinin intiharların ya da diğer insanların hayatlarının korunması yönü olduğu söylenebilirse de Cromatica aynı zaman da kaza niteliği teşkil etmeyecek fakat yine de gözetlenmesi ve kontrol edilmesi gereken tüm potansiyel tehlikeli durumlar için önemlidir.

Londra'da 1990'lı yılların ortasında bile 14.000'in üzerinde CCTV kamerası bulunmaktadır³³². Hem dünyanın finans merkezlerinden biri hem de kalabalık bir başkent olan bu şehrin potansiyeli Cromatica gibi sistemlerin kullanılmasını gerektirebilir. Diğer dünya başkentleri gibi Londra'da da tüketim, eğlence ve turizm için güvenli ve çekici cazibe alanları yaratmak amacıyla kapalı devre kamera sistemlerinden yararlanılmıştır. Caddeler, sokaklar, meydanlar ve diğer kamusal alanlar yerel yönetimlerin sorumluluğu altındadır³³³. İlk bakışta, Cromatica gibi çözümleri bulmak her ne kadar yerel yönetimlerin sorunu gibi gözükse de bu gibi sistemlerin kurulması ve faaliyete geçmesinde özel sektörün de desteği aranmaktadır. Yerel yönetim ve özel sektör, şehirlerin gelişmesi, tüketimin artması ve turizmin gelişmesi için bu altyapıyı birlikte yaratmaya çalışmaktadırlar. 2018 yılında ise Londra dünya üzerinde güvenlik

³³⁰ Suicide Statistics (Freedom of Information request to Transport for London) , What Do They Know, Ekim - Kasım 2011, https://www.whatdotheyknow.com/request/suicide_statistics (s.y. 28 Kasım 2021)

³³¹ Louahdi KHOUDOUR, Jean Pierre DEPARIS, Jean-Luc BRUYELLE, F. CABESTAING, Didier AUBERT, Samia BOUCHAFA, Sergio A. VELASTIN, Maria Alicia VICENCIO-SILVA, M. WHERETT, Project Cromatica, International Conference on Image Analysis and Processing (ICIAP), C.2, Y. 1997, s. 761.

³³² İbrahim CERRAH, Bilişim Teknolojileri ve Etik, Bilişim Teknolojilerinin Güvenlik Hizmetlerinde Kullanımının “Etik Boyutu” ve “Sosyal Sonuçları”, Turkish Journal of Police Studies, C. 4, S. 1-2, Y. 2002, s. 149.

³³³ David, LYON, Gözetlenen Toplum, s. 121.

kameralarıyla en çok izlenen şehirlerden birisi haline gelmiştir. Örneğin; sadece bir mahalle olan Islington’da ilgili tarihte yaklaşık 180 adet kamera aktif olarak çalışmaktadır³³⁴.

Öte yandan Glasgow Şehir Konseyi’nin 2020 yılı için verdiği bilgilere baktığımızda, şehrin aktif olarak kayıt yapan 420 adet sabit kapalı devre kameranın yanında, yaklaşık 11 adet mobil kapalı devre kameranın şehirde istenmeyen davranışların tespiti için kullanıldığını görmekteyiz³³⁵. Kentsel gözetime ilk defa 32 adet kamera ile 1994 yılında başladığı Glasgow’da şehrin yöneticileri ve özel sektör temsilcileri şehirdeki suçu azaltmak ve bölgeyi daha güvenli bir yer haline getirmek için kapalı devre kameralar kurulması gerektiğini ve böylelikle şehirdeki turizmin artacağı ve ziyaretçi sayısının da yükseleceğini düşünerek ortak bir girişimde bulunmuşlardır. Aynı dönemde bölge halkı ve ziyaretçiler üzerinde yapılan araştırmaya göre, araştırmaya katılanların yüzde doksanı kapalı devre kameralarla şehir gözetiminin yapılmasını desteklemiştir³³⁶.

Ditton ise buna karşıt olarak, kapalı devre kameraların şehir merkezinde suç işlenmeyeceğine dair bir güvence oluşturmadığını, kapalı devre sistemlerinin kurulmasıyla şehir merkezini kullanan kişi sayısının fazla yükselmediğini ve bireylerin kendi güvenlikleriyle ilgili olarak hissettiklerinin aynı olduğuna dikkat çekmiştir. Ditton’un Glasgow üzerinde yaptığı bu çalışmaya göre, kameraların getirdiği tek yenilik, kamera kurulan alanlarda bireylerin suçun kurbanı olma korkularının azalmış olmasıdır³³⁷.

Bu kapsamda bakıldığında bir diğer açıklanması gereken husus da “istenmeyen ya da sinir bozucu davranışlar”ın tam olarak neyi ifade ettiğidir. Kapalı devre kamera sistemleri vasıtasıyla şehrin sorunlu bölgeleri tespit edilebilir. Toronto Emniyet Müdürlüğü şehrin sorunlu bölgelerini sadece suç işleme oranı yüksek olan bölgeler değil, aynı zamanda istenmeyen ya da sinir bozucu davranışların gözlendiği yerler olarak tanımlamaktadır³³⁸. Şehir merkezleri ve turizm alanlarında suç işlenmesi bile gerekli önlemlerin alınması ve dışarıdan gelen insanların her açıdan kendilerini güvende hissetmeleri gerekmektedir. Böylelikle kapalı devre kamera

³³⁴ Robert DRAPER, They Are Watching You and Everything Else on the Planet, National Geographic, (Şubat 2018), <https://www.nationalgeographic.com/magazine/2018/02/surveillance-watching-you/> (s.y. 17 Ekim 2021)

³³⁵ Glasgow City Council, Mobile CCTV, <https://www.glasgow.gov.uk/article/23765/Mobile-CCTV> (s.y. 20 Ekim 2020)

³³⁶ Nicholas R. FYFE, Jon BANNISTER, City Watching: Closed Circuit Television Surveillance in Public Spaces, The Royal Geographical Society (with the Institute of British Geographers), C. 28, S. 1, Y. 1996, s. 40.

³³⁷ David, LYON, Gözetlenen Toplum, s. 121

³³⁸ David, LYON, Gözetlenen Toplum, s. 127.

sistemleri suçu önleme amacından daha da çok belirli bir ekonomik alanın kalkınmasını sağlamaktadır.

Ayrıca kamuya açık özel alanlarda yapılan gözetim sonucu ortaya çıkan bir diğer ekonomik sonuç da suç oranlarının azalmasıyla birlikte suçtan dolayı uğranılan zararın da çok büyük ölçüde azalması olarak karşımıza çıkmaktadır. Bournemouth’da 47 adet kamera ile faaliyete geçen gözetim sistemi mala zarar verme suçlarında azalmaya neden olarak Ağustos 1986’da £220,000 olan zararın sadece bir yıl içinde £36,000’a düşmesini sağlamıştır³³⁹. Aradaki maddi farka bakıldığında, neden bugüne kadar gelen süreç içerisinde kapalı devre kamera sistemlerinin İngiltere genelinde bu kadar fazla desteklendiği anlaşılabilecektir.

Sadece Londra ya da Birleşik Krallık’ın diğer bölgelerinde değil, diğer şehirlerde de benzer uygulamaların hayata geçirildiğini söylememiz mümkündür. Seattle ve New York’ta yapılan yerel düzenlemelerin ayrıntılarına baktığımızda, bu düzenlemelerin amaçlarının üçe ayrıldığını görmekteyiz. İlk olarak federal düzlemdeki anti-terör faaliyetlerinde yerel polisin rolünün ortaya konulmasının gerekmesidir³⁴⁰. Aslında bu itici gücün 11 Eylül olaylarından sonra tüm Amerika’da var olduğunu söyleyebiliriz. İkinci olarak, aşağıda detaylı olarak bilgi vereceğimiz akıllı şehirler ve bu şehirlerde işlenen büyük ölçekli akışkan verilerin açık bir şekilde dağıtımının düzenlenmesi ihtiyacı olarak karşımıza çıkar. Son olarak ise yerel polis teşkilatlarına yönelik reformların gerçekleştirilmesi ihtiyacını sayabiliriz³⁴¹.

Ülkemiz sınırları içerisinde ise kapalı devre kameraların genel kamu teşkilatı içerisinde hem merkez yönetimi hem de yerel yönetimler tarafından kullanıldığını görmekteyiz. Uygulama açısından yerel yönetim faaliyeti gösteren belediyelerin yurttaşların isteklerine ve ihtiyaçlarına cevap vermeleri çoğunlukla daha kolay olmaktadır. Türkiye’de yerel yönetimler daha nitelikli hizmet sunmak amacıyla kent ihtiyaçlarına yönelik olarak kentin farklı bölgelerine kapalı devre kamera sistemleri kurmaktadır³⁴².

³³⁹ Stephen GRAHAM, Jon BROOKS, Dan HEERY, “Towns on the Television: Closed Circuit TV Surveillance In British Towns and Cities”, Electronic Working Paper No. 17, <https://www.ncl.ac.uk/mediav8/apl/files/guru-ewp/ewp17.pdf> s. 6, (s.y. 28 Kasım 2021)

³⁴⁰ Ira S. RUBINSTEIN, Privacy Localism, Washington Law Review, C. 93, S. 4, Y. 2018, s. 1966.

³⁴¹ A.g.m., s. 1967.

³⁴² Civan Başar, s. 106.

İstanbul Büyükşehir Belediyesi (İBB) tarafından yönetilen “Ulaşım Yönetim Merkezi”nde Akıllı Ulaşım Sistemleri olarak adlandırılan uygulama dahilinde kentte meydana gelen anlık trafik akışı 24 saat gerçek zamanlı olarak izlenmektedir³⁴³. Yine İBB tarafından EDS ve Mobil EDS’ler kapsamında kırmızı ışık ihlalleri, emniyet şeridi ihlalleri, tramvay yolu ihlal tespiti gibi faaliyetler gerçekleştirilmektedir. Bunun haricinde İstanbul Fatih Belediyesi, “Güvenli Parklar” projesi kapsamında çocukların ve ailelerin güvenliklerinin tesisi için belediye sınırları içerisindeki parkları toplamda 242 adet kamerayla 7 gün 24 saat izlemektedir³⁴⁴. Bu görüntüler Belediye’ye ait tek bir merkezde toplanmaktadır. Yukarıdakilere ek olarak uzun zamandır İBB’nin gündeminde olan bir başka konu ise ticari taksilere yerleştirilecek kameralardır³⁴⁵.

Belediyeler tarafından elde edilen bu görüntülerin talep halinde özel hukuk kişilerine verilip verilmeyeceği ise bir başka önemli noktadır. Özel hukuk kişisi belediyedeki görüntüye erişmek istiyorsa adli mercilere başvurmakla (örneğin; suç şikayetinde bulunmakla) yükümlüdür. İlgili görüntülerin doğrudan adli merciler tarafından talep edilmesi gerekli olduğunu söyleyebiliriz. İlgili özel hukuk kişinin talebini değerlendiren adli merci bu kayıtları belediyeden talep edebilir. Bu talebin hukuki dayanağını PVSK’nın Ek 6. maddesi oluşturmaktadır³⁴⁶. Belediye tarafından ilgili talebin alınması üzerine personel tarafından

³⁴³ Trafik Yönetim Sistemleri, Ulaşım Yönetim Merkezi, <https://uym.ibb.gov.tr/hizmetler/trafik-yonetim-sistemleri>, (s.y. 5 Mart 2022)

³⁴⁴ “Güvenli Parklar” projesi hakkında bkz. <https://www.fatih.bel.tr/tr-TR/parklarimizin-guvenligini-arttirmaya-devam-ediyoruz-8345> (s.y. 5 Şubat 2022)

³⁴⁵ İBB Meclisi kararına göre, 15 bin adet takside zorunlu kamera uygulamasına geçilecek olup, bu kameralar vasıtasıyla taksilerin iç kısımları gözetlenerek canlı görüntüler Taksi Yönetim Merkezi’ne aktarılacaktır. Yeni kurulan ve 85 denetim personelinin bulunduğu bu merkezden 15 bin taksi ile 7 bin minibus ve taksi dolmuş izlenecektir. Bkz. “Karar verildi! İstanbul’da 15 bin taksiye kamera”, <https://www.hurriyet.com.tr/gundem/15-bin-taksiye-kamera-41896672> (s.y. 5 Mart 2022) EGM’nin taksilerde kamera kaydının yapılmasını zorunlu kılan genelgesi bu yöndeki çalışmaları hızlandırmıştır. Ancak bu uygulamanın beraberinde getirdiği özel hayatın gizliliğine dair kaygılar bir takım itirazları da beraberinde getirmiştir. İlgili EGM Genelgesinin iptali ve yürütmesinin durdurulması için İstanbul Barosu Başkanlığı tarafından Ankara 17. İdare Mahkemesi’nde dava açılmıştır. Bkz. “Taksilerde Ses ve Görüntü Kaydı Yargıya Taşındı”, <https://www.istanbulbarosu.org.tr/HaberDetay.aspx?ID=12625> (s.y. 05 Şubat 2022) Bu gibi mahremiyet kaygılarına istinaden önce bu faaliyetler dahilinde ses kaydı yapılmayacağını açıklayan İBB, son olarak ise kamera kayıtlarının doğrudan aktarılmayacağını, aktarımın güvenlik ile ilgili bir uygunsuzluk bulunduğu hallerde yapılacağını ifade etmiştir. Görüntüler belirli bir süre taksi içerisindeki kayıt sisteminde kalacak ve sürenin bitmesiyle birlikte otomatik olarak imha edilecektir. Bkz. <https://tuhim.ibb.gov.tr/haberler/haber-taksi/> (s.y. 5 Mart 2022)

³⁴⁶ PVSK’nın “Adli görev ve yetkiler” başlıklı Ek 6. maddesinin (4.) fıkrasında belirtildiği üzere, “Bir suç işlendiği veya işlenmekte olduğu bilgisini edinen polis, olay yerinin korunması, delillerin tespiti, kaybolmaması ya da bozulmaması için acele tedbirleri aldıktan sonra el koyduğu olayları, yakalanan kişiler ile uygulanan tedbirleri derhal Cumhuriyet savcısına bildirir ve Cumhuriyet savcısının emri doğrultusunda işin aydınlatılması için gerekli soruşturma işlemlerini yapar.” Yine aynı maddenin 7. ve 8. maddelerine göre “Polis, suçun delillerini tespit etmek amacıyla, Cumhuriyet savcısının emriyle olay yerinde gerekli inceleme

sadece belirtilen zaman aralığı ile sınırlı olarak bir araştırma yapılarak görüntüler işlenir. Bu sınırlandırmanın veri korumanın genel ilkelerinden ölçülülük ve amaca uygunluk ilkesini karşıladığı söylenebilir³⁴⁷. Ayrıca görüntüler başlangıçta talepte bulunan ilgili özel hukuk kişisine teslim edilmemektedir ki bu da verilerin yetkisiz üçüncü kişilerden korunmasının sağlanması açısından bir veri koruma tedbiri olarak önemlidir.

Yerel yönetimler tarafından gerçekleştirilen gözetim faaliyetlerine ilişkin ele alınması gereken bir diğer konu akıllı şehirlerde gerçekleştirilen gözetimdir. Akıllı şehirler sosyal yaşamın getirdiği bir çok zorluk karşısında harekete geçme amacının sonucu olarak, insanların toplumsal yaşamda karşılaştıkları sorunlara çözüm olarak doğmuştur. Daha iyi bir teknoloji ve veri analizi tekniklerinden yararlanmak koşuluyla, günümüzün sorun merkezi olan her büyük şehir daha efektif bir akıllı şehre dönüştürülebilir³⁴⁸. Hem teknolojik anlamda gelişmiş hem de sürdürülebilir bu yeni şehir modellerinde dijital teknolojiler önde geldikleri için sürekli devam eden bir gözetim gerçekleştirildiği söylenebilir. Hal böyle oluna akıllı şehirde yönetim sorunlarından en temelini bireysel mahremiyetin kaybı olacağı iddia edilmektedir³⁴⁹. Akıllı şehirlerin varlığı sebebiyle karşımıza çıkacak mahremiyet problemleri şunlardan oluşmaktadır: (i) anlamlı rızanın azlığı, (ii) kamu ilişkilerinde toplanan kişisel verilerin yönetimi, (iii) altyapı ve verilerin özelleştirilmesi, (iv) nesnelerin interneti teknolojisi aracılığıyla verilerin farklı amaçlarla kullanılması, (v) bulut teknolojileri sayesinde verilerin muhafaza edilmesi³⁵⁰. Bu sorunların hepsine getirilebilecek kusursuz bir çözüm bulunmamakla birlikte, bireylerin özel hayatlarına olan saygının ve mahremiyetlerinin korunması ile kamu yararı amacına yönelik olarak verilerin işlenmesi faaliyetleri arasında bir dengenin kurulmasının gerekli olacağı ifade edilmiştir³⁵¹.

ve teknik araştırmaları yapar, delilleri tespit eder, muhafaza altına alır ve incelenmek üzere ilgili yerlere gönderir.”; “Olay yeri dışında kalan ve o suça ilişkin delil elde edilebileceği yönünde kuvvetli şüphe sebebi bulunan konut, işyeri ve kamuya açık olmayan kapalı alanlarda yapılacak işlemler için Ceza Muhakemesi Kanununun arama ve el koymaya ilişkin hükümleri uygulanır.”

³⁴⁷ “Toplu Ulaşım Hizmetleri Müdürlüğü Kamera Görüntü Talep İşlemleri İçin İzlenecek Adımlar”, <https://tuhim.ibb.gov.tr/haberler/toplu-ula%C5%9F%C4%B1m-hizmetleri-mueduerlue%C4%9Fue-kamera-goeruentue-talep-%C4%B0%C5%9Flemeleri-%C4%B0%C3%A7in-%C4%B0zlenecek-ad%C4%B1mlar/> (s.y. 6 Şubat 2022)

³⁴⁸ John Wagner GIVENS, Debra LAM, "Smarter Cities or Bigger Brother? How the Race for Smart Cities Could Determine the Future of China, Democracy, and Privacy", *Fordham Urban Law Journal*, C. 47, S. 4, Y. 2020, s. 836.

³⁴⁹ Iria GIUFFRIDA, *Smart Cities and Sustainability: A New Challenge to Accountability?* Symposium Issue: Sustainability in the City, *William & Mary Environmental Law and Policy Review*, C. 45, S. 3, Y. 2021, s. 765.

³⁵⁰ Lilian EDWARDS, “Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective”, *European Data Protection Law Review (EDPL)*, C. 2, S. 1, Y.2016, s. 41 vd.

³⁵¹ John Wagner GIVENS, Debra LAM, s. 845.

Akıllı şehirde toplanan veriler için kasıtlı ya da kasıtsız veri ihlalleri her zaman söz konusu olabilecektir. Bu bakımdan AB Hukuku içerisinde yer alan veri korumaya ilişkin yasal düzenlemelerin akıllı şehirlerde ortaya çıkabilecek bir takım mahremiyet sorunlarına (İot teknolojileri, büyük veri ve bulut sistemler vb.) karşı nasıl kullanılabilceği tartışılmaktadır³⁵². Benzer çalışmaların bulunduğu Amerika’da ise, Amerika Federal Ticaret Komisyonu’nun (FTC) 2015 yılındaki raporunda nesnelerin interneti teknolojisine sahip cihazların tüketiciler için güvenlik sorunu yarattığının altı çizilmiştir³⁵³. Bu gibi gelişmiş teknoloji sistemleri üzerinden çocukların canlı görüntüleri uzaktan aile üyeleri tarafından izlenebilmektedir. Yani işlenecek veriler arasında bazı durumlarda çok hassas verilerin de yer alabileceği söylenebilecektir.

Diğer bir yönden yukarıdaki ifade ettiğimiz gibi bazı durumlarda hassas verilerin işleneceği bu sistemlerin bir takım veri koruma tedbirlerini beraberinde barındırmalarını beklemek çok fazla görülmeyecektir. Örneğin; nesnelerin interneti teknolojisini kullanan sistemler aracılığıyla işlenen verilerin yaklaşık 700 ayrı olayda yetkisiz üçüncü kişiler tarafından hacklendiği ortaya koyulmuştur. Daha spesifik bir emsalde hackerların bir aracı sürücüsü tarafından otoyolda kullanılırken hackledikleri kayıtlara geçmiştir³⁵⁴. Avrupa Birliği ekseninde bu sistemlere ilişkin hukuki düzenlemelere baktığımızda, yürürlükte olan Elektronik İletişim Direktifi kapsamında sadece önceden sadece telekomünikasyon hizmeti veren tedarikçilerin davranışları düzenlenirken, şu anda GVKT’nin de yürürlüğe girmesiyle artık tüm veri işleyenler bu açıdan gerekli önlemleri (yeterli güvenlik tedbirleri) almak zorunda kalmışlardır. Asıl sorun bu önlemleri belirleyen global bir düzenlemenin bulunmamasıdır. Budapeşte Siber Suçlar Konvansiyonu kural olarak bu hususa ilişkin bir minimum uluslararası sınır getirmiş ancak bu sadece kolluk kuvvetlerinin suça yönelik faaliyetleri açısından sınırlı kalmıştır³⁵⁵.

³⁵² Lilian EDWARDS, s. 16-27.

³⁵³ A.g.m., s. 36.

³⁵⁴ Andy GREENBERG, “Hackers Remotely Kill a Jeep on the Highway, with me in it”, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (s.y. 6 Mart 2022)

³⁵⁵ Konvansiyon imzaya 23.11.2001’de Budapeşte açılmış olup, yürürlüğe Avrupa Konseyi üyesi 5 ülkeden 3’ünün imzasıyla 01.07.2004 tarihinde girmiştir. 01.01.2015 tarihinde ise onaylanarak Türkiye Cumhuriyeti’nde yürürlük bulmuştur. Convention on Cybercrime, ETS No. 185, <https://rm.coe.int/1680081561> (s.y. 06 Şubat 2022); Ayrıca siber savaş ya da siber ihlallerde kritik altyapının korunması bakımından ayrıca 2008/114/EC no’lu Avrupa Kritik Altyapı Direktifi bulunmaktadır. Bkz. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF> (s.y. 06 Mart 2022)

Önceki dönemlerde insanların kamusal alanlarda izlenmesi faaliyetlerinin günümüz teknolojik gelişmeleri karşısında pratik anlamda değiştiği de söylenebilir. Yani teknoloji bugünkü haline gelmediği için kamusal alanda bu kadar çok sayıda kamera bulunmamaktaydı ya da yüz tanıma sistemleri bu kadar gelişmemiş olduğundan bireylerin kimlikleri direkt olarak ifşa olmuş sayılmazdı. Ancak günümüz teknolojisi bunu değiştirmiştir. Artık buharlaşan evler çağındayız ve Koops'un da dediği gibi her yerde izlenmenin ve verilerin toplanmasının söz konusu olduğu bir topluma doğru evrilmekteyiz³⁵⁶.

Nesnelerin internetini kullanan cihazların durmaksızın bireyler hakkında veri kaydı tuttukları, akıllı şehirler içerisinde dijital ayak izlerinin sürekli olarak kayıtlandığı, CCTV'lerin bireylerin hareketlerini kaydettiği görülmektedir. Bu sebeplerle artık bilginin gizli kalması istisna haline gelmekte ve çok zor bir uğraşmayı da beraberinde getirmektedir. Bir diğer akıllı şehir ve mahremiyet ilişkisi ise verilerin kullanılması hususundaki rızanın nasıl alındığı hususunda kendisini göstermektedir.

Veri koruma hukukunun savunduğu ilkeler ve temel kuralları bakımından verinin işlenmesine geçilmeden veri sahibi kişiden bilgilendirmeye dayalı ve özgür iradesi dahilinde bir rıza alınmasını gerekmektedir. Keza rızanın her zaman geri alınması şansı bulunur ve bu durumda veri işleme durdurulur. Bir görüşe göre, akıllı şehirlerde veri toplamaya dair bildirimler ve rızanın geri alınmasına dair uygulamalar anlamsız kalmaktadır³⁵⁷. Bu görüşte olanlara göre, “yüz tanıma sistemi kullanılmaktadır” ibaresinin yer aldığı bir kamusal alana girildiğinde bu durum ilgili kişinin gözetleyenlere veri işleme faaliyetine ilişkin onay verdiği anlamına gelmez. Keza trafiğin gözlenmesi ya da daha etkili elektrik dağıtımı için izlenmeye izin verilmiş olması, ilgili bireyin toplu taşımaya yönlendirilmesine ya da evinde kullandığı ampullerin değişiminin belirlenmesine izin verildiği anlamına gelmeyecektir³⁵⁸.

Teknoloji şirketleri de bu alandaki gelişimi görüp trene binmeye çalışanlardır. Hatta bazı durumlarda lokomotif oldukları dahi söylenebilir. IBM, Hitachi ve Cisco gibi dev uluslararası şirketler bu şehirlerde kullanılacak uygulamalar geliştirmeye yönelik çalışmalar yapmaktadırlar. Bu faaliyetlerinin amaçlarını da kentsel hizmetlerin kalitesini artırmak, şehirleri daha sürdürebilir kılmak ve kaynakların daha efektif kullanımını sağlamak olarak

³⁵⁶ Lilian EDWARDS, s. 13.

³⁵⁷ Iria GIUFFRIDA, s. 767.

³⁵⁸ A.g.m., s. 767.

göstermektedirler. Kentsel Yönetim Sistemleri adı verilen bu uygulamaları şehirlerin bir çok yönden yeniden tasarlanmasına yarayan tek bir üründen ziyade birden fazla unsuru bünyesinde barındıran bilgisayar destekli bir ekosistem olarak görmek daha yerinde olacaktır. Bu unsurlar dijital yönetim merkezlerinden daha büyük ölçekli yerel yönetim ağları içerisinde haritalama, altyapı tespit sistemleri, enerji yönetimi, su ve atık yönetimi, ulaşım, telekomünikasyon ve güvenlik gibi hizmetlerden oluşmaktadır³⁵⁹.

3. Diğer Kamuya Açık Alanlarda Kapalı Devre Kamera Sistemlerinin Kullanılması

Kolluk kuvveti, merkezi yönetim ya da yerinden yönetim teşkilatları tarafından kullanılan kapalı devre kamera sistemleri kamusal alanların büyük bir bölümünü kapsamaktadır. Önceki bölümde vurgulamaya çalıştığımız üzere, kamu ve özel sektör karar mekanizmaları güçlerini birleştirerek kamusal alanlarda neredeyse bireylerin gözetlenmediği alanları sıfıra indirmişlerdir. Bununla birlikte bu aktörlerin gözetleme alanı dışında kalan bir kamusal alanın da var olduğu söylenebilecektir.

Stadyumlar, bankalar, banka otomatları (ATM), dükkanlar, alışveriş merkezleri, ulaşım araçları, metrolar, metrobüsler, okullar, üniversiteler gibi tüm özel sektöre ait kamusal alanlar, bu faaliyetleri sunanlar tarafından kapalı devre kameralar ile gözetlenmektedir. İngiltere’de bulunan bir alışveriş merkezi New Strand Shopping Centre’da yer alan kapalı devre kameralar tarafından yakalanan görüntülerde henüz iki yaşında bir çocuk olan James Bulger’in katilleri tarafından alışveriş merkezinden çıkarıldığı kayıt altına alınmıştır. Küçük çocuk alışveriş merkezinden çıkarıldıktan sonra yakınlardaki bir tren istasyonuna götürülmüş ve burada dövülerek öldürüldükten sonra, tren raylarına atılmış ve tren tarafından ezilmiştir. Fazlasıyla trajik olan bu olay sadece Liverpool şehri sakinlerini değil neredeyse tüm İngiltere’yi kapalı devre kameralarla yapılan gözetimin gerekli olduğuna ikna etmeye yetmiştir³⁶⁰. Görüntülerin kalitesiz olması nedeniyle olayın failleri video görüntüleri üzerinden anında tespit edilememiş olsa da kamera gözetiminin faydası vurgulanarak, kameraların çoğalmasına karşı olanlar susturulmuştur³⁶¹.

³⁵⁹ Andres LUQUE–AYALA, Simon MARVIN, Urban Operating Systems: Producing the Computational City, The MIT Press, ABD 2020, s. 26.

³⁶⁰ Stephen GRAHAM, Jon BROOKS, Dan HEERY, s. 5.

³⁶¹ Nick TAYLOR, "You've Been Framed: The Regulation of CCTV Surveillance.", Journal of Civil Liberties, C. 7, S. 2, Y. 2002, s. 85.

Avrupa ve İngiltere'nin en büyük perakende satış alışveriş merkezlerinden biri olan ve 2.2 milyon metre karelik alan üzerine kurulu Metro Centre'da toplam 6.000 kişi çalışmakta ve yılda 10.5 milyon araç ziyarete gelmektedir. Kendi bölgesinde en geniş kapalı devre kamera sistemi gözetleme ağına sahip bu merkezde, £500.000 değerinde bir kontrol odası ve tüm ziyaretçilerin her anını izlemeye elverişli ekranlarda, 73 adet kameradan gelen görüntüler yer almaktadır³⁶². Değişen ihtiyaçlara da bağlı olarak sistem her an güncellenmektedir. Örneğin, araba hırsızlığına karşı alınan ek önlemler çerçevesinde merkez dışına hareket eden, plaka ve insanlara zoom yapabilen kameralar yerleştirilerek araçların güvenliği sağlanmıştır. Artık sadece bununla yetinilmeyerek, şahıs tanıma özelliği ile otoparka giren araçtaki şahıs ile çıkıştaki şahıs aynı olup olmadığının tespiti bile yapılmaktadır. Tüm bunların sonucu olarak bu mikro gözetim alanında işlenen suç sayısının diğer benzer alanlara göre daha az olduğu tespit edilmek birlikte, 1994 yılı içerisinde 12,400 araç ziyareti kayıt altına alınmış ve sadece 1 tane araç hırsızlığı meydana gelmiştir³⁶³.

CCTV kameralarıyla gözetleme alanlarından biri olan alışveriş merkezlerinden ülkemizde de çok sayıda bulunmaktadır. Yukarıda kapalı devre kamera gözetiminin kanuni dayanaklarından bahsederken belirttiğimiz üzere, Türkiye'de alışveriş merkezleri içerisinde gerçekleşen kapalı devre kamera gözetimi hususunda yasal bir dayanak bulunmaktadır. Bu yasal dayanak Alışveriş Merkezleri Hakkında Yönetmelik'in 19. maddesinin 2. fıkrası olmaktadır. Alışveriş merkezleri içerisindeki hangi alanlarda bu gözetime izin verilmesi gerektiği hususunda ise doğrudan ilgili düzenlemeyi incelememiz gerekecektir. Düzenlemeye göre, *"Alışveriş merkezinde bebek bakım odası ve tuvalet gibi niteliği itibarıyla kayıt altına alınması uygun olmayan alanlar dışındaki ortak kullanım alanları..."*, belirtildiği üzere burada bahsedilen alanlar hariç olmak üzere otoparklar dahil tüm ortak kullanım alanlarının izlenmesi ve kayıt altına alınması hukuka uygun görülebilecektir. Özellikle otoparkın araç güvenliği açısından çok sayıda hırsızlık ya da kaza gibi olayların yaşandığı görüldüğünden bu alanların gözetim dahiline alınmasının gerekli olduğu varsayılabilir.

Bir başka gözetim alanının ise fiziki olarak internete erişimin, internet kafelerin ya da kütüphanelerin gözetlenmesinden oluştuğunu görebiliriz. İnternete erişimin düzenlenmesine yönelik olarak alınacak tedbirlere yasak olan internet sitelerinin ya da içeriklerine erişimin durdurulması ya da filtrelenmesi dışında bu erişimin kameralar ile fiziksel olarak gözetlenmesi

³⁶² Stephen GRAHAM, Jon BROOKS, Dan HEERY, s. 12.

³⁶³ A.g.m., s. 13

de örnek gösterilebilir. Bu gözetim sırasında eğer yasak bir siteye erişim gerçekleştirilirse hukuki ve cezai sorumluluk söz konusu olabilecektir³⁶⁴. Bu yasaklama geniş çevrelere duyurulduysa, başkalarının bu yasaklı içeriklere girişleri de ihbarlar vasıtasıyla engellenebilecektir. Bu duyurunun bir benzeri Çin’de yapılmıştır. İki çizgi film karakterinin internet kullanıcılarını bu yönde uyardığı ve aykırı hareketleri ihbar etmeleri konusunda desteklediği görülmektedir. Benzer şekilde bir kamera gözetimi de kütüphaneler ve internet kafelerde gerçekleştirilmektedir. Kütüphanelerde bilgisayar ekranının neredeyse hepsi yöneticilerin görebileceği şekilde konumlandırılmıştır. Keza internet kafelerde monitörler CCTV kameralar ile izlenmektedir³⁶⁵.

Gözetim faaliyetlerinin yürütüldüğü bir diğer kamuya açık alan ise okullardır. Okul yöneticileri tarafından yapılan kamera gözetimleri iki temelde yürütülür. Birincisi okul içerisinde denetimin sağlanması ikincisi ise öğrencilerin gözlemlenmesi olarak karşımıza çıkmaktadır³⁶⁶. Birnhack ve Perry-Hazan tarafından yürütülen bir araştırmada, 10 ve 12. sınıf öğrencilerinin oluşturduğu farklı okullardan seçilen 83 adet öğrencinin okullara yerleştirilen kapalı devre kameralara karşı geliştirdikleri algıları incelenerek, kameralarla yapılan gözetimin örgütsel-eğitim deneyiminin bir parçası haline geldiği vurgulanmıştır. Gözetimin bu anlamda gerekliliğinden bahsetmek mümkün olsa da araştırma sonucunda ulaşılan bulgulara göre öğrencilerin belirli oranda mahremiyet beklentilerinin bulunduğunu da belirtmemiz gereklidir. Araştırmaya katılan öğrenci yorumlarından bir tanesi “(okulda) güven ilişkisi olmadığını, hedefe ulaşmak için korku ve caydırıcılığın kullanıldığını, güven ve insani ilişki söz konusu olmadığını” üzerinedir. Bir diğer yorum ise “kameraların sadece dış görünüşü izlemeye elverişli olduğu bunun ise öğretmenlerin öğrenciler hakkında sadece dış görünüş (kıyafetler ve pirsing yüzünden) üzerinde değerlendirme yapabilmesine ön verdiği ve bu nedenle ön yargılardan muzdarip olunduğu” yönündedir³⁶⁷.

Yukarıda belirtilen örneklerden de görüldüğü üzere okulda gözetleyenlerin güvenlik beklentilerinin karşılanması ile öğrencilerin mahremiyetleri arasında bir çatışma söz konusudur. Bu çatışmanın giderilmesi için ise iki beklenti arasında bir dengenin kurulması zorunluluğu bulunmaktadır. Mahremiyetin korunması amacına yönelik olarak, kamera

³⁶⁴ Steven J. MURDOCH, Ross ANDERSON, s. 64.

³⁶⁵ A.g.e., s. 65.

³⁶⁶ Michael BIRNHACK, Lotem PERRY-HAZAN, School Surveillance in Context: High School Students’ Perspectives on CCTV, Privacy, and Security, Youth & Society, C. 52, S. 7, Y. 2020, s. 1314.

³⁶⁷ A.g.m., s. 1319.

gözetiminin hukuki dayanağının bulunması, yapılan gözetimin ölçülü olması gereklidir. Ayrıca gözetimin yapıldığı yer, yani mekânsal faktör de bu bakımdan gözetimin hukuka uygunluğunu sağlayan diğer bir unsurdur. Örneğin; bir çok öğrenci sınıflarda kameraların bulunmaması gerektiğini belirtmekte, yine bir çoğu okulun farklı alanların diğerlerine nazaran daha kamusal ya da özel alanlar olabileceğini belirtmektedirler³⁶⁸. Mekansal faktör, bazı durumlarda ise dışarıda yapılan gözetimin olumlu karşılanması fakat içeride yapılan gözetimin daha rahatsız edici olması anlamına gelmektedir. Ayrıca veri koruma hukuku açısından çok önemli olan ve hukuk kurallarına aykırılık teşkil eden fonksiyon hatası (“function creep”, “surveillance creep”) tanımına dikkat çekmemiz gerekmektedir³⁶⁹. Okullara yerleştirilen kameraların yerleştirilmesindeki asıl sebep dışarıdan okula yönelen tehditlerin önlenmesi iken, aynı kameralar küçük disiplin olaylarının ya da öğretmenlerin davranışlarının tespitinde de kullanılıyor ise bu durum veri işlemenin asıl amacının dışında başka amaçlar için de gerçekleştirildiği anlamına geleceğinden hukuka aykırılık gündeme gelecektir.

Buna karşılık, aynı gözetim faaliyetinin öğretmenlerin bakış açısından değerlendirilmesi de yapılmıştır. Bu çalışmada ise bazı öğretmenlerin, okullara yerleştirilen kapalı devre kameralar nedeniyle asıl gözetim nesneleri olan öğrencilerden çok kendi mahremiyetlerinin tehlikeye düştüğüne yönelik çekinceleri olduğu ortaya konulmuştur³⁷⁰. Burada dikkat çekilmesi gereken kısım ise gözetleme vasıtalarının neler olduğu ya da nasıl meşrulaştığı değildir. Bu hususların zaten okul koşullarında nasıl karşılandığı yukarıda açıklanmıştır. Asıl belirtmemiz gereken yer gözetleyen konumda olan öğretmenlerin öğrencilerin mahremiyet hakkının bulunduğu bilincine sahip olup olmadıklarıdır. Bu hususta mahremiyet hakkı bilincine sahip olmayan öğretmen, öğrencisi kendisine bu yönde bir talep ile gelse bile bu hakkın ne olduğunu nitelendiremeyeceği için öğrencinin mahremiyet hakkı korunamayacaktır. Bu durumun bir açıdan sosyo-kültürel gelişim ile ilgisi de bulunmaktadır. Sosyo-kültürel gelişimi yüksek bir toplumda mahremiyet bilinci her daim daha yüksektir. Ayrıca ilgili hakkın sık olarak kullanılması, pratikliğin artırılması da bu yönde hak bilinci oluşmasına olumlu etki eder³⁷¹. Neticede gözetleyenlerin, gözetlenenleri hak sahibi birer birey olarak görmeleri gerektiğini, eğer sistem buna izin vermiyorsa ortaya çıkacak sonucun mahremiyet hakkının ihlali olarak görülebileceği söylenebilecektir.

³⁶⁸ A.g.m., s. 1323.

³⁶⁹ A.g.m., s. 1314.

³⁷⁰ Michael BIRNHACK, Lotem PERRY-HAZAN, Differential Rights Consciousness: Teachers’ Perceptions of Privacy in The Surveillance School, Teaching and Teacher Education, C. 101, Y. 2021, s.7.

³⁷¹ A.g.m., s.3.

Eğitimin sağlanması sırasında bir takım güvenlik tehditlerinin söz konusu olduğu durumlar ile de karşılaşmaktayız. Örneğin, 2018 yılında Florida ve Texas'daki okul baskınları ve bu baskınlarda zarar gören öğrenci ve öğretmenlerin bulunması sebebiyle okullarda güvenlik ve gözetim uygulamalarının sıklaştırılması gerekliliğinden bahsedilebilir. Bunun bir yönü de CCTV'ler ile öğrencilerin kayıt altında tutulması ve hareketlerinin gözetlenmesidir. Mevzu bahis ABD olduğunda değerlendirmenin de yerel düzlemde yapılması gereklidir. Burada gözetimin gerekliliği ve ölçülülüğünü, öğrencilerin bireysel mahremiyetleri bakımından Dördüncü Değişiklik'ten doğan hakları karşısında bir dengeye oturtmak gerekmektedir. Ancak sadece mahremiyetin korunması değil aynı zamanda bir başka temel hak olan federal eğitim hakkının, İkinci Değişiklik³⁷² kapsamındaki kişilerin silah taşıma özgürlüğü karşısında güçlendirilmesi gerektiği de söylenebilir³⁷³. Yani önce eğitim hakkının verilmesini tesis etmek buradaki öncelik iken, bunu yapabilmek için atılması gereken adımlar veri koruma ilkeleri göz önünde bulundurulmaksızın yapılmamalı ve bireysel mahremiyetin anayasal düzlemde korunduğu gözetilmelidir.

B. İşyerinde Kapalı Devre Kamera Sistemlerinin Kullanımı

Gözetim teknolojileri toplumun diğer alanlarında kullanıldığı gibi işyerinde çalışanların gözetimine yönelik olarak da kullanılmaktadır. Özellikle post-endüstriyel dönemde üretim ve hizmet sektörlerinde makinelerin kullanımının artması ile birlikte gelişme gösteren enformasyon teknolojileri, işyerlerinde çalışanların denetiminde büyük önem taşımaktadır. Buna çalışma yaşamında bireyler “enformatik gözetim”in kıskacı altında bulunmaktadır da diyebiliriz³⁷⁴. Çalışanların gözetlenmesi ve gözetim çıktılarının sistematik olarak kaydedilmesi sonucunda işe devam durumları, aile geçmişleri, performans bilgileri, karakter analizleri, ücret bordroları ya da izin bilgileri gibi çalışan hakkındaki bir çok bilgiye kolaylıkla ulaşılabilmektedir.

İşyerinde yapılan gözetim faaliyetlerinde kullanılan teknikler sadece yukarıda saydıklarımızla sınırlı değildir. Çalışma alanını gözetleyen kameralar, ilaç testleri, çalışanların

³⁷² Second Amendment of the Constitution of the United States (Amerika Birleşik Devletleri Anayasasının İkinci Değişikliği)

³⁷³ Romero MAYBELL, Educational Environments and the Federal Right to Education in the Wake of Parkland, University of Miami Law Review, C. 73, S. 3, Y. 2019, s. 778.

³⁷⁴ Uğur DOLGUN, Çalışma Yaşamında Gözetim, Sosyal Siyaset Konferansları Dergisi, S. 49, Y. 2005, s. 509.

internet geçmişleri, ziyaret ettikleri sayfalar ya da çalışanlara ait e-mail yazışmaları üzerinden de gözetim gerçekleştirilmesi mümkün olabilir. Tüm bu gözetim teknikleri yarı özel yarı kamusal alan niteliğindeki işyerini, yoğun gözetimin gerçekleştirildiği bir alan olarak karşımıza çıkarmaktadır³⁷⁵.

Çalışma yaşamındaki gözetimi yoğun ve katı olarak nitelendirmemiz söz konusu olabilir. Bu nitelendirme belirli bir zorunluluktan kaynaklanır. Eğer herhangi bir fabrikada üretim bandında çalışan bir işçi, kendisine verilen görevi aksatırsa bu durum diğer üretim aşamalarını da olumsuz etkileyecek ve sonuç olarak fabrikanın üretimi azalacak ya da tamamen duracaktır. Bu nedenle işçilerin mesai saatleri içerisinde kendilerinden beklenen şekilde hareket etmeleri gerekecek ve bu işçiler sadece verilen izin saatlerinde mola yapabileceklerdir. Bu örneği daha geniş ölçekli olarak düşündüğümüzde farklı ülkeler bulunan çalışanların dahi aynı çalışma sistemine entegre olarak hareket etme zorunluklarının bulunduğu gözlemlenebilir. Küresel dünyada endüstriyel ve ticari olarak ülkelerin birbirleriyle sürekli olarak bağlantı halinde olmaları sonucu farklı ülkelerde çalışan çalışanlar aynı zamanlarda uyanır, işe gider veya işten çıkarlar. Devasa bir makineden farksız çalışan toplumun, çalışma alanlarında her an gözetlenmesi sistemin kendisi tarafından dayatılmaktadır³⁷⁶. Nitekim bu çalışma düzeninde aksama olmaması için çalışanların gözetlenerek yönlendirilmeleri, hizaya sokulmaları bir zorunluluk olarak görülebilecektir.

Amerikan İşletme Vakfı (American Management Association) tarafından yayınlanan 2007 tarihli Elektronik İzleme ve Gözetim Raporu'na göre, araştırmaya katılan şirketlerin yaklaşık yarısı (%48) kameralar ile gözetimi hırsızlık, şiddet ve sabotaj faaliyetlerine karşı kullandıklarını belirtmişlerdir. Bu oran aynı anketin yapıldığı 2001 yılında sadece %33 olarak kayıtlara geçmiştir. Bu kıyaslama kamera gözetiminin işyerinde kullanımının arttığını ortaya koyar. Yine aynı araştırmada kameralar ile çalışanlarını gözetleyen bu şirketlerin, sadece %7'sinin kamera kayıtlarını çalışanların performanslarının izlenmesi amacıyla kullandıkları belirtilmiştir³⁷⁷.

³⁷⁵ David LYON, Gözetlenen Toplum, s. 129.

³⁷⁶ Alvin TOFFLER, s. 84.

³⁷⁷ American Management Association & ePolicy Institute Research, Electronic Monitoring & Surveillance Survey, 2007, <http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf> (s.y. 28 Kasım 2021)

Kişisel verilerin korunması açısından dikkat çeken diğer bir husus ise aynı araştırmada yer alan bilgiler ışığında çalışanlarını kapalı devre kamera ile gözetime maruz bırakan bu şirketlerin hiçbirinin, çalışanlarını kayıt altına aldıkları hususunda bilgilendirmemiş olmalarıdır³⁷⁸. Söz konusu durum işçinin veri işleme süreçlerine yönelik aydınlatılması yükümlülüğüne aykırıdır. Aydınlatma yükümlülüğü sadece duvara asılacak bir uyarı levhası ile kamera izleme faaliyetinin gerçekleştirildiğinin işçiye bildirilmesi olarak görülmemelidir. İşçinin sadece hareketlerinin kayıt altına alındığını değil ayrıca bu kayıtların hangi amaçlarla kullanıldığı, ne kadar süre ile saklanabileceği ve üçüncü kişilerle paylaşılıp paylaşılmadığını öğrenme hakkı bulunmaktadır. Dolayısıyla işverenin aydınlatma yükümlülüğünün kapsamının bu yönde genişlediğini söyleyebiliriz.

Bu amaçları belirlemek daha gözetime başlamadan önce yerine getirilmesi gereken bir işlem olarak görülebilir. Aksi durumda gözetimin amaca uygun olarak gerçekleştirilip gerçekleştirilmediğini tespit etmek zorlaşır. Fakat her ne kadar bu amaç önceden belirlenmiş olsa bile, fiili durumda amacın değişmesi ya da genişlemesi söz konusu olabilir. Bu bakımdan işyerinde kapalı devre kamera gözetiminin, gözetiminin amacından bağımsız olarak yürütülmekte olduğu ifade edilmiştir. Çünkü müşterilerin mağazadan bir şeyler çalmasına engel olmak için kurulan bir kamera aynı zamanda işçilerin yapacakları hırsızlığı ya da çalışanların performanslarını da kayıt altına almaktadır. Yani kameralar ile işyerinde yapılan gözetim Lyon'un dediği gibi, “genel bir yönetim aracı” olarak değerlendirilecektir³⁷⁹. Kişisel verilerin korunması açısından bakıldığında ise veri işleme süreçlerinin tamamında belirli, açık ve meşru amaçlar doğrultusunda hareket edilmesi gerektiği için amaca uygun olmayan bir gözetimin hukuki yönden riskli olacağını söylememiz mümkündür³⁸⁰.

İşyerinde gerçekleştirilen gözetimin amacı ile birlikte bu gözetimin kim tarafından yapıldığının ve hukuki dayanağının ne olduğunun irdelenmesi açısından ülkemizdeki uygulamaları değerlendirmek önemlidir. Öncelikle gözetim sürecinin taraflarının kimler olacağını netleştirmek gerekir. Bu bakımdan işyerinin kapalı devre kameralar ile gözetiminde gözetleyen tarafta işveren bulunur. Buna karşılık gözetimin hedefi ise işçidir. Taraflar arasında

³⁷⁸ İşyerinde hırsızlığa karşı kapalı devre kamera sistemleri ile çalışanlarını gözetime tabi tutan işverenlerden sadece % 78'i ; performans değerlendirmesi amacıyla kameralardan yararlanan işverenlerden sadece % 89'u, çalışanlarını işyerinde bulundukları süre boyunca kameralar ile izlendikleri konusunda bilgilendirmişlerdir. Bkz. Ag.i.

³⁷⁹ David LYON, Gözetlenen Toplum, s. 129.

³⁸⁰ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 231.

4857 sayılı İş Kanunu kapsamında geçerli bir iş sözleşmesinin bulunması gerekecektir³⁸¹. İşveren ile işçi arasındaki bu özel gözetim sürecinde gözetleyen konumunda işçi bulunacağı için örneğin; işverenin müşterilerin hareketlerini kamera gözetimine tabi tutması bu kapsama girmeyecektir.

Anayasa Mahkemesi tarafından verilen bir kararda, “...işlerin etkin bir şekilde yürütülmesi ile bilgi akışının kontrolünü sağlamak, işçinin eylemlerine bağlı cezai ve hukuki sorumluluğa karşı korunmak, verimliliği ölçmek veya güvenlik endişeleri gibi haklı ve meşru görülebilecek nedenlerle işverenin yönetim yetkisi kapsamında kural olarak...”, şeklinde belirtildiği üzere işverenlerin işçileri izleyebilecekleri ifade edilmektedir³⁸². Nitekim, Yargıtay 22. Hukuk Dairesi işçinin işyerinde gözetlenebilmesinin işverenin “yönetim hakkı çerçevesinde mümkün olduğunu ancak bu işçinin izleme faaliyetinden önce haberdar edilmesi gerektiğini” belirtmiştir³⁸³. İşverene verilen bu yönetim hakkı içerisinde tanımlanabilecek “denetim ve gözetim” kavramları³⁸⁴ ise hem işverene tanınan bir hak hem de bir ödev olarak görülür. Sonuç olarak işverenin işçi ile arasında bulunan iş sözleşmesi gereğince sahip olduğu yönetim hakkı kapsamında işçinin iş esnasındaki faaliyetlerinin izlenmesi ve denetlenmesi mümkün olmaktadır³⁸⁵.

³⁸¹ Gökhan C. ERBAŞ, 6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Elektronik Ortamda Gözetlenmesi, HHFD, C. 7, S. 1, Y. 2017, s. 100.

³⁸² Anayasa Mahkemesi Kararı (AYMK), E.Ü. başvurusu, b.n. 2016/13010, k.t. 17 Eylül 2020. Bu kararda her ne kadar işçinin iletişim araçlarının gözetlenmesi ve denetlenmesinden bahsedilmiş olsa da işçilerin kapalı devre kameralarla gözetlenmesi hususunda işverenin aynı yetkiye sahip bulunduğu ve gözetim gerçekleştirebileceği söylenebilir.

³⁸³ “İşverenin yönetim hakkının bir sonucu olarak işçiyi elektronik ortamda izlemesi ve takip etmesi her zaman mümkündür. Ancak bunun için işçinin bu izleme hakkında bilgilendirilmiş olması şarttır. İşçinin izlendiğine dair bilgilendirilmemesi veya gizlice izlenmesi, bu izleme neticesinde elde edilen veriler iş sözleşmesinin işçi tarafından ihlal edildiğini açıkça ortaya koysa dahi, hukuka aykırı olarak kabul edilmelidir.” Bkz. Yargıtay 22. HD., E. 2017/21857, K. 2019/9884, T. 07.05.2019. Burada bahsedilen yönetim hakkı iş ilişkisi süresince tarafların düzenleme boşluğu ile karşılaştıkları durumlarda, ilgili yasal düzenlemelere ve taraflar arasındaki iş sözleşmesine aykırı olmamak üzere, işveren tarafından işin yürütülmesine ilişkin olarak emir ve talimat vermek suretiyle işyerindeki faaliyetin devamlılığının sağlanmasına ilişkin hak olarak tanımlanabilir. Bkz. Gökhan C. ERBAŞ, s. 101

³⁸⁴ İşveren tarafından verilen işin işverenin denetimi ve gözetimi altında yapılması aynı zamanda iş sözleşmesinin belirleyici unsurlarından olan bağımlılık unsurunun varlığının tespitinde aranan ölçütlerdendir. Bu denetim ve gözetim hakkı ve ödevi hem işverenin yönetim hakkının doğal bir sonucu olarak ortaya konulmaktadır. Ancak bununla birlikte 6331 sayılı İş Sağlığı ve Güvenliği Kanunu’nun “işverenin genel yükümlülükleri” başlığı altındaki 4/1 maddesinde yer alan düzenleme kapsamında işverenin “işyerinde alınan iş sağlığı ve güvenliği tedbirlerine uyulup uyulmadığını izleme ve denetleme” yapabileceği belirtilmiştir. Bkz. Gökhan C. ERBAŞ, s. 102.

³⁸⁵ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hakkı Bağlamında İşçilere Ait İletişimin İşveren Tarafından Gözetlenmesi (Supervision of the Communication of the Workers in the Context of the Right to Protection of Personal Data), s. 5, <https://ssrn.com/abstract=3792265> (s.y. 8 Mart 2022)

İşverenin yönetim hakkı kapsamında kaydedeceği ya da sadece izleyeceği kapalı devre kamera görüntülerinin işçinin özel hayatının gizliliği hürriyeti ile çatışması ihtimali de bulunmaktadır. Bu kapsamda Anayasa'nın 20. maddesinin 3. fıkrası kapsamında bir değerlendirme yapılması gerekir. İlgili madde metninde belirtildiği üzere, *“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.”* Yukarıda belirtmiş olduğumuz Anayasa Mahkemesi kararında ise, *“Anayasa'nın 20. maddesinin 3. fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir...Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir.”* şeklinde bir yorumda bulunulduğu görülmektedir. Yani öncelikle işlenen görüntü kaydının kişisel veri içerip içermediğine bakılması gerekecek, akabinde ise Yüksek Mahkeme tarafından belirlenen denetim kriterleri üzerinden somut olay nezdinde bir değerlendirme yapılması gerekecektir. Bu değerlendirmeler sonucunda eğer özel hayata saygı bağlamında kişisel verilerin korunmasına müdahale eden üçüncü kişi aşağıdaki güvenceleri sağlamıyorsa, işçinin anayasal hakkının ihlal edilmiş olduğu söylenebilir.

Bu doğrultuda ilk olarak işverenin, kapalı devre kamera ile gözetimin haklı olduğunu gösteren meşru gerekçeleri olup olmadığı denetlenmelidir. İşverenin gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı irdelenmelidir.

İkinci güvence kişisel veri işlemeye başlanmadan önce yapılacak bilgilendirmeye ilişkindir. Yüksek mahkeme tarafından bu hususta, *“Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsamaması*

gerekir...Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.” denilerek, kişisel veri işleme faaliyetlerine ilişkin bilgilendirmenin önemi vurgulanmıştır.

Amaca elverişlilik bakımından ise işçinin kişisel verilerinin korunmasını isteme hakkına işveren tarafından yapılan müdahalenin, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli olması gerektiği belirtilmiştir. Buna ek olarak inceleme faaliyetiyle elde edilen kişisel verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir. Keza gerçekleştirilmesi istenen amaca daha hafif bir müdahale ile ulaşılabileceği mümkün ise bu yolun seçilmesi de zorunludur. Yüksek mahkemeye göre, “*..çalışanın CCTV gözetimine maruz kalması yerine onun kişisel verilerine daha az müdahale eden yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir.*³⁸⁶”

Ayrıca işveren tarafından işçinin kişisel verilerinin korunmasını isteme hakkında yönelik müdahalenin orantılı kabul edilebilmesi için ise kamera gözetimi kapsamında işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir. Buna ek olarak kamera gözetiminin işçi üzerindeki etkisi ve işçi bakımından sonuçları göz önünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması da gerekmektedir. Eğer taraflardan birine şahsi olarak aşırı külfet yükleniyorsa burada ihlalin varlığından söz edilebilecektir. Örneğin; bir çalışanın işyerinde bulunan giyinme odasında görüntü kayıtlarının alındığı durumda buradaki veri işlemenin şahsi olarak işçiyi dezavantajlı konuma getireceğini söylemek mümkün olabilecektir.

Yüksek mahkemenin kişisel verilerin korunması hakkına ilişkin değerlendirmesinin son aşamasının ise makul beklenti kriteri üzerine olduğunu görebiliyoruz. Bu doğrultuda, kapalı devre kameraların faaliyetlerine ilişkin tam ve açık bir bilgilendirme yapılmadığı durumlarda, temel hak ve özgürlüklerinin işyerinde de korunacağı yönünde işçide haklı bir beklenti oluşur. Yani işçiye açık bir bilgilendirmenin yapılmadığı hallerde hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir beklenti içinde olacaklarının

³⁸⁶ AYMK, E.Ü. Başvurusu.

kabul edilmesi gerekecek olup; işçinin temel hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerekecektir.

Buraya kadar ülkemizdeki işverenlerin işçilerine yönelen kapalı devre kamera gözetimi faaliyetlerini nasıl gerçekleştireceklerini ortaya koymaya çalıştık. Tüm bunlara ek olarak bu konuda bir takım uluslararası kuralların da uygulama alanı bulabileceği görülmektedir. Örneğin; UÇÖ tarafından oluşturulan ve örgütün 267. toplantısında onaylanan İşçilerin Kişisel Verilerinin Korunması Hakkındaki Uygulama Kuralları'nın 3. maddesine göre, "...kamera, video cihazları, ses cihazları, telefon,..." gibi farklı tekniklerin kullanılması yoluyla işçilerin izlenebileceği belirtilmekle; bu izlemenin bir takım sınırlar ve kurallara tabi olarak yapılacağını belirtmiştir³⁸⁷. Buna göre, işçiler gözetimin sebepleri, zaman çizelgesi, kullanılacak teknik ve izlenecek yöntemler ve toplanacak verilerin ne olduğu konusunda önceden bilgilendirilmelidir. (İşçilerin Kişisel Verilerinin Korunması Hakkındaki Uygulama Kuralları 6. madde 14. fıkra) Aynı maddenin 2. fıkrasında ise, işverenin kullanılacak izleme teknikleri açısından, işçilerin özel hayatları açısından en az müdahale teşkil edecek yöntemi seçme zorunluluğu bulunduğu belirtilmiştir³⁸⁸.

Ek olarak belirtmek gerekir, UÇÖ'nün çalışma hayatının geleceğine ilişkin hazırladığı raporda işyerindeki yapay zeka uygulamalarının üç farklı işlevi olduğundan bahsedilmiştir³⁸⁹. Yapay zekanın bu üç işlevi şunlardır: (i) eşleme işlevi, (ii) sınıflandırma işlevi, (iii) süreç yönetimi işlevi. Birincisinde yapay zeka sayesinde yapılan eşleşmeler sayesinde, müşteri veya tedarikçi bulma maliyetleri azaltılır ve büyüyen müşteri portföyüne daha ucuz çözümler sunulması için işletmeler perakende, konaklama, insan kaynakları ya da diğer hizmetlerin yönetiminde eşsiz bir destekten yararlanmış olur.

İşyerindeki yapay zeka uygulamalarının ikinci işlevi ise gözetimdeki artışa ilişkin sınıflandırmalar yapılmasını sağlamaktır. Son işlev olan süreç yönetiminde ise, ürünlerin kalitesi, sertifikasyon programları ve piyasa koşulları hakkında daha iyi bilgiye erişmek suretiyle, üreticilerin tedarik zincirlerini çeşitlendirmesi ve böylelikle güçlendirmesi söz

³⁸⁷ Mehmet TEKERGÜL, İşyerinde Elektronik Gözetim Uygulamaları (Yüksek Lisans Tezi) İstanbul 2010, s.25.

³⁸⁸ World of Work The Magazine of The International Labour Office, No. 59, Nisan 2007 , s. 18, https://www.ilo.org/wcmsp5/groups/public/---dgreports/-dcomm/documents/publication/wcms_082631.pdf (s.y. 22 Ekim 2021)

³⁸⁹ Antonio ALOISI, Elena GRAMANO, "Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", Comparative Labor Law & Policy Journal, C. 41, S. 1, Y. 2019, s. 98.

konusu olmaktadır. İşte bu sebeplerle yapay zekanın işyerine girişi söz konusu olur. Daha önce de ifade ettiğimiz gibi işyerinde gözetimin amacından bağımsız gerçekleştiği düşünüldüğünde, kamera gözetiminin yukarıdaki amaçlara istinaden gerçekleştiği her ihtimalde aynı zamanda işçilerin de gözetlenmesi söz konusu olacağından, bu kullanımlar sırasında bireysel mahremiyetin korunması açısından bir değerlendirme yapılması gerektiğini düşünebiliriz.

Çalışanların yapay zeka temelli, şeffaf olmayan kötü niyetli bir gözetime tabi tutulmalarını bir kafes modeline benzetebiliriz. Çalışanları kafes içerisine sokan diğer unsurlar ise çalışma saatlerinin belirlenmesi, işe alma işten çıkarma ya da terfi süreçlerinin değerlendirilmesi metrikleridir³⁹⁰. Örneğin, Fransa’da hiçbir gözetim sistemi ya da veri işleme faaliyeti çalışanların ya da temsilcilerinin önceden rızaları alınmaksızın başlatılamaz. Fransa Medeni Kanunu’nda çalışanların verilerinin toplanması ve bilgisayarının gözetimini düzenleyen üç temel ilke bulunur. Bunlar şeffaflık, orantılılık ve ilgili olma olarak karşımıza çıkmaktadır. Şeffaflık ilkesi kapsamında her çalışan gözetim sürecinin başlatılmasından önce bilgilendirilmelidir. Diğer ilkeler göre ise gerçekleştirilen gözetimin meşru, ölçülü ve gerçekleştirilmek istenen amaçla bağlantılı olması gerekmektedir³⁹¹. Bu unsurların KVKK’ya uygun veri işlemeye yönelik olarak da arandığını belirtmemiz gereklidir.

Ülkemizde KVKK’nın yürürlüğe girmesine kadar olan dönemde işçi ile işveren arasındaki gözetleme uygulamalarının sınırları yukarıdaki uluslararası düzenlemeler ve yerel mevzuatta bulunan bir takım hükümler kapsamında dikkate alınmakta iken, kanunun yürürlüğe girmesinden sonraki dönemde artık gözetlenen ve bu doğrultuda verileri işlenen işçiler ile işverenler arasındaki ilişkilerdeki sınırlandırmalar KVKK’nın uygulama alanına girecektir³⁹². Yukarıda aktardığımız İş Kanunu’ndan doğan işverenin yönetim hakkı işverene sadece gözetim yapma hususunda bir yetki sağlar, bunun dışında veri işlemenin kurallarının ve sınırlarının belirlenmiş olduğu bir hukuki düzenleme bulunmadığından sınırların çizilmesi bakımından KVKK’ya ihtiyaç duyulacağı söylenebilir.

Burada değerlendirilmesi gereken bir başka husus ise işverenin işçiye ait görüntüleri izleme ve/veya kaydetmesinin fesih nedeni olarak kabul edilip edilmeyeceğidir. Kapalı devre kamera gözetiminin işçi açısından özel hayatına müdahale olarak görüldüğü hallerde, işverenin

³⁹⁰ A.g.m., s.105.

³⁹¹ A.g.m., s.110.

³⁹² Gökhan C. ERBAŞ, s. 103.

iş sözleşmesini haklı ya da geçerli nedenle fesih hakkı bulunmayacaktır. Bu bakımdan eğer iş sözleşmesi feshedilirse iş güvencesi kapsamındaki işçinin işe iade davası açması mümkün olacaktır³⁹³. Yargıtay tarafından incelenen örnek olayda, işverenin işçileri katlarda bulunan kapalı devre kameralar aracılığıyla izlediği, bunu daha önce ifade ettiğimiz yönetim hakkı kapsamındaki denetim yetkisine dayandırdığı, çok sayıda işçinin katlarda bulunmadığının tespit edildiği ve bir kısım işçilerin görev başında olması gerektiği halde görev yerinde olmayıp yaşlı odalarında boş yataklarda üniforma ile uyuduklarını tespit edilmiştir. Bunun üzerine davacıya fesih yaptırımını uygulanmıştır. Mahkeme tarafından uygulanan fesih yaptırımının işçinin eylemi ile ölçülü ve orantılı olmadığı bu nedenlerle işveren feshinin geçersiz olduğu ve işe iade talebinin kabulüne karar verilmesi belirtilirken kararda ayrıca, olayın geçtiği yerin kamu kurumu olup iş başında bulunması gereken işçilerin üniforma ile görüntülenmesinin özel hayatın gizliliğinin ihlali sayılamayacağı ifade edilmiştir³⁹⁴.

Keza doğrudan kamera kayıtlarının iş akdinin feshine ilişkin davalarda delil olarak kullanıldığını başka Yargıtay kararları da bulunmaktadır³⁹⁵. Yargıtay 22. Hukuk Dairesi tarafından verilen bir kararda *“Davacı her ne kadar soruşturma raporunda alınan savunmasında, kendisine kapı pervazları sorulduğunda bilmiyorum demesinin sebebini yeni kapı kasalarının geldiğini ve onu sorduğunu sandığını beyan etse de, olayın kamera görüntüleriyle tespit edilmesinden sonra malzemeleri geri verdiği, tespit edilmeseydi geri vermeyeceği davacı tanık anlatımlarından ve davacının beyanlarından yola çıkılarak anlaşılmıştır. Hal böyle olunca, davaya konu olaydaki davacının eylemleri haklı fesih sebebi oluşturduğundan”* denilerek, işyerinde bulunan kamera görüntüsünün işverene iş sözleşmesini haklı nedene dayanarak feshetme olanağı verdiği görülmektedir³⁹⁶. Ancak Yargıtay’ın bazı durumlarda işyerinde kamera görüntülerine yansıyan olayların haklı neden ağırlığında olmadığı ve fakat olaydaki tutum ve davranışların iş sözleşmesinin feshi açısından geçerli neden olarak kabul edildiğini de görmekteyiz³⁹⁷.

³⁹³ Mehmet TEKERGÜL, s. 119.

³⁹⁴ Yargıtay 22. HD., E. 2017/818, K. 2017/656, T. 23.1.2017.

³⁹⁵ Yargıtay 9. Hukuk Dairesi, E. 2018/9908, K. 2019/8092, T. 08.04.2019; Yargıtay 9. HD., E. 2016/5785, K. 2019/14997, T. 04.07.2019.

³⁹⁶ Yargıtay 22. HD., E. 2015/18766, K. 2017/24395, T. 08.11.2017.

³⁹⁷ Yargıtay 7. HD., E. 2014/2443, K. 2014/5109, T. 04.03.2014. İlgili karara göre, “Gerek kamera kayıtları, gerekse davacının yukarıda belirtilen beyanları ve davalı savunması birlikte değerlendirildiğinde; kadın işçinin yazılı beyanı olmamasına, davacının dışında o gün ameliyathane biriminde başkaca nöbetçi personelin ve özellikle yardımcı personelin nöbetçi olduğunun ispatlanmamasına ve özellikle de erkek çalışanların, kadın çalışanların soyunma odalarına girmelerinin yasak olduğuna dair ispat yükümlülüğünün de yerine getirilmemesine karşın davacının, kadın işçilere ait soyunma odasında normalin çok üzerinde yaklaşık 30-35

Bir başka önemli kararında Yargıtay, aynı iş yerinde çalışan çalışanlar arasında tezahür eden olayların izlenmesinin çalışanların özel hayatlarına bir müdahale oluşturmayacağını belirtmiştir. İlgili kararda, iş yerinde satış temsilcisi olarak görev yapan davacı işçinin aynı işyerinde bulunan kadın çalışan ile duygusal ilişki içinde bulunduğu ve davacının kadın çalışanı iş yerinde öpmeye çalıştığı, bu durumun güvenlik kameraları tarafından kaydedildiği ifade edilmiştir. Bu olaylara güvenlik kameralarının kaydı nedeni ile vakıf olan davalı işverenin, davacı işçiyi bu fiili nedeniyle işten çıkarttığı anlaşılmaktadır. Mahkeme'nin “...*Özel hayat ve özel hayatın gizliliği kuralı iş yerinde ve başka bir çalışana karşı alenen yapılan fiili kapsamaz...*” şeklinde önemli bir yorum getirdiği görülmekte olup, davacı işçinin iş yeri ortamında başka bir çalışan ile yukarıda açıklanan şekilde bir olay yaşaması iş yeri kurallarına ve genel ahlak kurallara aykırı olduğundan davalı işverenin gerçekleştirdiği fesih haklı görülmüştür³⁹⁸.

Burada vurgulanması gereken eksiklik ise verilen kararların çoğunda yapılan gözetim faaliyetlerinin hukuka uygunluk değerlendirilmesinin yapılmamasıdır. Yüksek Mahkeme tarafından işçilerin kişisel faaliyetlerini yürüttüğü zamanların CCTV'ler tarafından tespit edilmesi söz konusu olduğunda, bunun işveren tarafı için bir fesih sebebi olacağı kabul edilse de öncelikle bu gözetim faaliyetlerinin hukuka uygunluk denetiminin yapılması gereklidir. Hukuka aykırı bir gözetim faaliyeti vasıtasıyla elde edilen veri ve belgeler her zaman hukuka aykırı olacak ve delil olarak kullanılması mümkün olmayacaktır³⁹⁹.

dakika süren ve birkaç kez odadan çıkmasına rağmen hemen tekrar aynı odaya girmesi, odadan çıkışlarında elinde herhangi bir ameliyathane malzemesi de bulunmadığı, sadece cep telefonu olduğu sonucuna varılan nesne bulunduğu ve bu hali ile de davacının bu tutum ve davranışları ile iş sözleşmesi gereği işin ifası sırasında göstermesi gereken özeni göstermediği, işverenin diğer işçilerinin ve özellikle kadın işçilerinin mahremiyetlerine saygı göstermediği, bu şekli ile işveren tarafından iş sözleşmesinin devamının beklenilmeyeceğinin açık olduğu, davacının tutum ve davranışlarının işverenin işçisine yönelik sataşma, cinsel taciz olarak değerlendirilmesinin mümkün bulunmadığı, ancak yukarıda belirtilen olayın gelişim şekli dikkate alındığında haklı neden ağırlığında olmamakla birlikte bu tutum ve davranışların geçerli neden olarak kabul edilmesi gerektiği sonucuna varılmıştır. O halde davanın reddine karar verilmesi gerekirken davacının işe iadesine karar verilmesi hatalı olup bozma nedenidir.”

³⁹⁸ Yargıtay 9. HD., E. 2016/33799, K. 2020/19760, T. 23.12.2020. Benzer yönde bir görüş için Bkz. Yargıtay 22. HD., E. 2016/2198, K. 2016/5732, T. 25.2.2016, “Bunun yanı sıra, ister işyerinde isterse işyeri dışında gerçekleşsin, işçinin işlediği suç ya da eylem, yüz kızartıcı nitelikte olmasa dahi, çalışma ortamını ve huzurunu doğrudan olumsuz yönde etkiliyorsa; işçi yaptığı fiil veya davranışın kendi özel hayatını ilgilendirdiği veya feshe konu işlemin kendi görev tanımı içinde bulunmadığı savunmasına sığınamaz. (Yargıtay 9. HD., E. 2004/73, K. 2004/12225, T. 24.05.2004). Örneğin, işçinin, rızası ile dahi olsa mesai arkadaşısı olan kadın işçiyi kaçırmaya ya da gayri meşru ilişki yaşaması durumunda, olayın sadece özel hayatı ilgilendirdiğinden bahsedilemez.”

³⁹⁹ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 645.

İşverenin iş sözleşmesini feshetmesi ya da kamera kayıtlarının delil olarak kullanılmasının dışında kamera gözetiminin işçilerin özel hayatına hukuka aykırı bir müdahale olarak nitelendirildiği bir durumda, işçinin bu iş ilişkisini sürdürmesi kendisinden beklenemez bir hal alabilecektir. Peki bu durumda işçi iş sözleşmesini haklı nedene dayalı olarak feshedilecek midir?

Bu sorunun cevabı için öncelikle gözetimin TCK md. 132-138’de düzenlenen “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”dan birini oluşturup oluşturmadığını bakılmalıdır⁴⁰⁰. Eğer kamera gözetimi bu suçlardan birini oluşturmaktaysa, bu durumda 4857 sayılı İş Kanunu (İş.K) md 24/II hükmünde yer alan haklı nedenle derhâl fesih hallerinden biri olan “işverenin, işçiye veya ailesi üyelerinden birine karşı hapsi gerektiren bir suç işlemesi” kapsamında işçinin iş sözleşmesini haklı nedenle derhal feshi söz konusu olabilir⁴⁰¹. Keza işçinin aynı maddenin (b) bendi kapsamında haklı fesih nedeni olan “işçinin...şeref ve namusuna dokunacak sözler söylemesi veya bu tür davranışlarda bulunması” düzenlemesi doğrultusunda da haklı nedenle fesih yoluna gidebilmesi mümkün olacaktır. Buna ilişkin örnek vermemiz gerekirse, işveren tarafından işyerinde duş ve soyunma odalarının kameralarla izlenmesinin işçi tarafından sözleşmenin feshi açısından haklı neden sayılması gerektiği söylenebilir⁴⁰².

Video teknolojilerinin gelişmesi ve özellikle depolama ve veri iletimi konusundaki ilerlemeler sonucunda, bugün kameraların daha fazla işyerinde bir gözetim aracı olarak kullanılması mümkün olmaktadır. Tüm dünyayı etkileyen Covid-19 salgını çalışma hayatının dinamiklerini temelinden değiştirmiş olup, çeşitli sebeplerden ötürü uzaktan çalışmak zorunda kalan çalışanların evlerindeki hareketleri bile kameralarla izlenebilmektedir. Çalışma alanlarının sadece ofisler ile sınırlandırılmadığı bu yeni sistemde bazı işverenlerin işçilerini bir takım bilgisayar teknolojileri aracılığıyla gözetim altında tutmaya çalıştıklarını görebilmekteyiz.

⁴⁰⁰ TCK md. 132’den itibaren başlayan “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” bölümü içerisinde özel hayatın gizliliğini tehdit eden fiillerin tanımlandığı farklı suç türlerinin yer aldığı görülmekle birlikte burada kapalı devre kamera görüntülerinin izlenmesi ve kaydedilmesi açısından en çok uygulama alanı bulabilecek suçların TCK md. 134 “Özel Hayatın Gizliliğini İhlal”, TCK md. 135 “Kişisel Verilerin Kaydedilmesi”, TCK md. 136 “Verileri hukuka aykırı olarak verme veya ele geçirme, TCK md. 138 “Verileri Yok etmeme” suçları olacağını söylemek mümkün olabilecektir.

⁴⁰¹ Mehmet TEKERGÜL, s. 116.

⁴⁰² A.g.m., s. 116.

10 Mart 2021 tarihli Resmi Gazete’de yayınlanan Uzaktan Çalışma Yönetmeliği’nin 10. maddesine göre, uzaktan çalışma sırasında iletişimin yöntemi ve zaman aralığı uzaktan çalışan ile işveren arasında belirleneceği söylenmiştir. Ancak uygulamada uzaktan çalışanın evinde gerçekten çalışıp çalışmadığı konusunda emin olmak isteyen işverenlerin bir takım yapay zeka destekli teknolojik uygulamalardan yararlandıklarını ya da toplantı sayılarını artırdıklarını görebilmekteyiz⁴⁰³. Kısaca ifade etmek isteriz ki bu görüntülerin çalışanların gözetimi açısından kullanılması söz konusu olursa, yukarıda belirttiğimiz hukuki değerlendirmelere tabi olacağı öngörülebilir.

C. Kamuya Açık Olmayan Yerlerde Kapalı Devre Kamera Sistemlerinin Kullanımı

Kamuya açık olmayan yerlerde kapalı devre kamera sistemlerinin kullanımı açısından ilk akla gelen alan, dört tarafı duvarlarla çevrili mahremiyet alanları olarak düşünülen evlerdir. Ev gözetiminde sıradan kameraların yanı sıra çok daha yüksek güvenlikli ev güvenlik sistemlerinin bulunduğu da görülebilmektedir. Ev güvenliğinde kapalı devre kameraların kullanılması hem evin içindeki kimseler (çocuk bakıcıları, diğer çalışanlar, ziyaretçiler, vb.) hem de komşular ya da dolaylı olarak kayıtlara giren üçüncü kişiler için özgürlük alanlarına bir müdahale sayılabilecektir.

Nitekim dünya üzerinde yüksek gelir düzeyine sahip olup, ayrıcalıklı yaşam alanlarında kendi dünyasını yaratma konusunda şansı bulunan belirli bir insan topluluğu bulunmaktadır. Bu fırsatı bulanlar kendilerini aynı şehrin diğer insanlarından izole etme ve kapalı topluluklar halinde yaşama eğilimindedir⁴⁰⁴. Bu eğilimin temelinde ise tehlikeye karşı korunma, evine zorla girilme, şiddete maruz kalma korkusu yatmaktadır. Hal böyle iken, bu kimselerin mülklerini izlemek için yüksek güvenlik teknolojilerinden yararlanması bir ölçüde doğal karşılanabilecektir. Örneğin; Londra’nın Belgravia ve Hampstead Garden gibi yüksek gelir düzeyinde insanların ikamet ettiği bölgelerinde insanlar güvenliği ön planda tutarak, evlerini adeta birer kaleye dönüştürmüşlerdir⁴⁰⁵. İçinde yaşayan bireyin dışarıdan gelecek tehlikeye karşı kendini koruması için önlemlere başvurması neredeyse insanlık tarihi kadar eski bir

⁴⁰³ Jessica DAVIS, “More Remote Work Leads to More Employee Surveillance”, IT Leadership//Team Building & Staffing, Information Week, <https://www.informationweek.com/strategic-cio/team-building-andstaffing/more-remote-work-leads-to-more-employee-surveillance/d/d-id/1341366> (s.y. 11 Mart 2022)

⁴⁰⁴ David, LYON, Gözetlenen Toplum, s. 116.

⁴⁰⁵ Stephen GRAHAM, Jon BROOKS, Dan HEERY, s. 3.

içgüdü ise de yüksek güvenlik sistemlerinin ya da kamera sistemlerinin bu amaçla kullanılması daha yeni sayılabilecek bir olgudur.

Bu açıdan ilk değerlendirilmesi gereken husus “ev” kavramı ile neyin ifade edildiği olabilir. AİHS madde 8 kapsamındaki alt-kategori haklardan biri olarak karşımıza çıkan “konuta saygı hakkı” ya da TCK’nın 116. maddesinde düzenlenen “konut dokunulmazlığını ihlal suçu” kapsamında bu tanıma ulaşmamız mümkün gözükmemektedir.

AİHM içtihatlarına göre, konut özel yaşamın ve aile yaşamının geliştiği, maddi olarak belirlenmiş bir yerdir. Bir yerin konut olarak kabul edilip edilmeyeceği noktasında orada yaşayan kimse ile yer arasında “yeterli ve devam eden bir bağ”ın kurulmuş olması gerekli olduğu ifade edilmiştir⁴⁰⁶. TCK içerisinde ise konutun tanımına doğrudan kanun içerisinde yer verilmemiş olmasına rağmen, konut dokunulmazlığını ihlal suçu kapsamında ceza öğretisinde konut, bir kimsenin geçici de olsa oturmak için sığındığı her nevi yer olarak tanımlanabilir⁴⁰⁷. O halde mekânsal sınırlama açısından bu alan içerisinde yapılan gözetimin evsel gözetim olduğundan bahsedebiliriz. Keza ceza uygulamasına baktığımızda konuta bağlı eklentilerin de bu sınırlandırmaya dahil olduğu görülmektedir⁴⁰⁸.

AB Hukuku’nda da ülkemizdekine benzer şekilde kameraların faaliyet gösterdiği kayıt alanlarını evler, eklentileri ve bahçeleri olarak nitelendirmek mümkündür. Ayrıca evin dışında olan kapı önlerini gözetleyen kameralar doğrudan kapıya odaklanmış olması kaydıyla bu kapsamda sayılacaktır⁴⁰⁹.

⁴⁰⁶ Gülay ARSLAN ÖNCÜ, Özel Yaşama ve Aile Yaşamına Saygı Hakkı, Epamat Basım, Ankara 2019, s. 125.

⁴⁰⁷ Bununla birlikte TMK md. 19/1’de yer alan ikametgah tanımının da konutun nitelendirilmesinde kullanılmaya çalışıldığı görülmektedir. Ancak TMK’da tanımlanan ikametgah ile TCK’nın 116. Maddesinde yer alan konut terimlerinin birbiriyle karıştırılmaması gerekir. TMK md. 19’a göre ikametgah (yerleşim yeri), “...bir kimsenin sürekli kalma niyetiyle oturduğu yerdir.” Bu bakımdan her ikametgahın TCK’nın belirlediği anlamda bir konut olacağı ancak her konutun TMK anlamında ikametgah olmayacağı ifade edilmiştir. Bkz. Mehmet Emin ARTUK, Esra ALKAN AKCAN, “Konut Dokunulmazlığının İhlali Suçu”, DEÜHFD, Prof. Dr. Durmuş TEZCAN’a Armağan, C. 21, Özel Sayı, Y. 2019, s. 2715.

⁴⁰⁸ Mehmet Emin ARTUK, Esra ALKAN AKCAN, s. 2717.

⁴⁰⁹ İngiltere Veri Koruma Otoritesi tarafından kişilerin CCTV’ler konusunda bilgilendirilmesine yönelik olarak ayrıntılı bir rehberde belirtilmiştir. Detaylı bilgi için bkz. “Domestic CCTV Systems Guidance for People: Using CCTV”, <https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/> (s.y. 02 Şubat 2021)

Diğer bir yönden gözetimin kim tarafından gerçekleştirileceğine bakmalıyız. Yukarıda ev sahibi ile yer arasında yeterli ve devamlı bir bağın bulunması gerektiğini söylemiştik. Bu açıdan bakıldığında gözetimin sadece malik tarafından yapılmasının şart olmayacağını söyleyebiliriz⁴¹⁰. Gözetim altında bulunan alanda gözetimi gerçekleştirilen hukuka aykırı bir şekilde ikamet ediyor olabilir. Örneğin; kira kontratının süresi dolmuş ya da iskan izni olmayan bir yerde kamera kaydı yapılıyor olabilir. Bu durum kapalı devre kamera sistemleri ile yapılan gözetimin niteliğini ya da hukuki gerekçelerini etkilemeyecek olup, kiracının ya da kira sözleşmesinin süresi bitmiş bir kiracının da aynı şekilde gözetleyen olabileceğinden bahsetmemiz mümkündür.

Bu alanda gerçekleştirilecek kapalı devre kamera gözetimini doğrudan düzenleyen, izin veren ya da bu gözetimin kurallarını belirleyen bir hukuki düzenleme bulunmamaktadır. Fakat evin aynı zamanda bir işyeri olarak nitelendirilmesi mümkün olabileceğinden, önceki bölümde yaptığımız bazı değerlendirmelerimizin burada da geçerlilik bulabileceğini söyleyebilmek mümkün olacaktır. Ancak ev hizmetlerinin İş.K'nın kapsamı dışında kalması nedeniyle ev hizmetlerinde çalışan işçiler ile işverenler arasında 6098 Türk Borçlar Kanunu (TBK) anlamında bir hizmet sözleşmesinin bulunması gerektiğini kabul etmemiz gerekecektir⁴¹¹. Keza bu hizmetlerin 6331 sayılı İş Sağlığı ve Güvenliği Kanunu (İSGK)'nın uygulama alanından da çıkarıldığı görülmektedir⁴¹². Daha önce bahsettiğimiz işyerinde işverenin yönetim hakkı ya da İSGK'dan doğan yükümlülüklerin yerine getirilmesi ile mümkün olan gözetim burada gerçekleştirilemeyecektir.

TBK'nın 417. maddesinin 2. fıkrasında, *“İşveren, işyerinde iş sağlığı ve güvenliğinin sağlanması için gerekli her türlü önlemi almak, araç ve gereçleri noksansız bulundurmak; işçiler de iş sağlığı ve güvenliği konusunda alınan her türlü önleme uymakla yükümlüdür.”* düzenlemesi kapsamında, işverenin teknik açıdan uygulanabilir ve işyerinin özelliklerine uygun bir takım önlemleri alabilmesi mümkün olacaktır⁴¹³. Yine TBK'da bulunan işçinin kişisel verilerinin korunmasına dair 419. madde kapsamında ise *“İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.”* olduğu düzenlenmiştir. Aynı maddenin ikinci fıkrasında ise bu hususta özel

⁴¹⁰ Gülşay ARSLAN ÖNCÜ, s. 126.

⁴¹¹ Ayşe Gül KÖKKİLİNÇ, “Ev Hizmetlerinde Çalışan İşçinin İş İlişkisi”, DEÜİFD, C. 20, S. 2, Y. 2019, s. 546.

⁴¹² 6331 sayılı İş Sağlığı ve Güvenliği Kanunu'nun “Kapsam ve İstisnalar” başlıklı 2. maddesinin 2. fıkrasının (c) bendinde “Ev Hizmetleri”nde, bu kanun hükümlerinin uygulanmayacağı belirtilmiştir.

⁴¹³ Ayşe Gül KÖKKİLİNÇ, 550.

kanun hükümlerinin saklı olduğu belirtilmekle KVKK'nın uygulanmasına yönlendirme yapma şansının bırakıldığı görülmektedir. Bu nedenle KVKK hükümlerinin bu alanı düzenlemeye yönelik kullanılmasının çok önemli olacağı söylenebilir.

Tüm bu hukuki düzenlemeler doğrultusunda ev hizmeti gören bir işçinin kapalı devre kamera vasıtasıyla işvereni tarafından izlenebileceği sonucunu çıkarmamız mümkündür. Bu veri işleme faaliyetinin hem TBK md. 419'a hem de KVKK'ya uygun olacak icra edilmesi ise kanuni bir zorunluluktur.

Ev içerisinde bulunan diğer üçüncü kişiler açısından inceleme yaptığımızda ise bu kimselerin kamera gözetimine konu olmaları bakımından KVKK'nın 28. maddesindeki istisna hükmünün uygulanıp uygulanmayacağını tespiti gerekir. Kanun'un 28. maddesinin 1. fıkrasının (a) bendine göre, kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülükler uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi istisna olarak görülmektedir. Bu açıdan KVKK'nın uygulama alanı dışında kalacağını söyleyebiliriz. Başta eve dışarıdan gelen ziyaretçiler olmak üzere diğer üçüncü kişiler açısından yapılan gözetim ise KVKK'ya tabi olacaktır denilebilir.

Komşular açısından ise iki farklı durum söz konusudur. İlk olarak eve ya da eklentisine giriş yapan bir komşu diğer üçüncü kişiler gibi değerlendirilmelidir. Buna karşılık kendi evi sınırları içerisinde bulunmasına rağmen, kameraların kurulum açısı gereği gözetim altında bulunabilen komşu açısından durum biraz daha farklıdır. Aslında her iki komşu aleyhinde uygulanan kamera gözetimi de KVKK'ya tabi olarak uygulanmalıdır. Ancak ikinci grupta bulunan komşunun görüntülediği alan kendi evinin sınırları içerisi olacağı için bu alanda özel hayatın gizliliğinin korunması sağlanmalı ve bu yönde bir gözetime izin verilmemelidir. Aksi durumda gözetleyen tarafından gerçekleştirilen gözetimin özel hayatın gizliliğini ihlal ettiği söylenebilir⁴¹⁴.

İngiliz Veri Koruma Otoritesi (Information Commissioner's Office – ICO)'ya göre kamera sistemlerinin kayıt altına aldığı alanlar sadece kişinin evi ve bahçesi ile sınırlandırılmış ise GVKT uygulama alanı bulmayacaktır. Fakat kameralar bu sınırlar dışındaki alanları

⁴¹⁴ Zeki HAFIZOĞULLARI, Muharrem ÖZEN, “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”, Ankara Barosu Dergisi, S. 4, Y. 2009, s. 17.

gözetliyorsa, yani bu kameraların görüntülerine sokakta yürüyen insanlar ya da kendi evlerinin bahçesindeki komşular da giriyor ise bu durumda hem GVKT hem de 2018 yılında yürürlüğe giren Veri Koruma Kanunu (Data Protection Act - VKK) hükümleri uygulanacaktır. Benzer şekilde Avrupa Adalet Divanı'nın “ev içerisinde yapılan gözetimde “eğer kameralar dışarıyı görüyorsa artık evsel faaliyet (household activity) değildir” şeklinde bir değerlendirmesi de bulunmaktadır⁴¹⁵. Bu görüş kapsamında CCTV kameraların evin dışına yönelik gözetim yapması söz konusu ise bu faaliyetin artık kişisel ya da evsel faaliyet olarak görülmesi mümkün değildir. Çünkü bu görüntüler ev içerisinde yaşamayan, söz konusu evdeki bireylerle ilgili bulunmayan ve bilgilerinin gizli kalmasını isteyen üçüncü kişilere ait veriler içerebilecektir⁴¹⁶.

Bu düzenlemeler ışığında KVKK uygulamasında tüm evsel gözetim faaliyetlere ilişkin bir istisna bulunmadığı, var olan istisnanın kapsamının “tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında” olduğu belirtildiği üzere, GVKT'de düzenlenene göre daha dar olduğu görülmektedir. GVKT'nın 2. maddesinin 2. fıkrasının (c) bendinde istisnanın “ tamamen kişisel ve evsel faaliyetler” şeklinde tanımlandığı ve kapsamının çok daha geniş olduğu söylenebilir.

Evlerin güvenliğinin sağlanmasına yönelik olarak kapalı devre kameraların kullanılması sırasında şunlara dikkat edilmelidir⁴¹⁷. İlk olarak güvenliğin sağlanması için bu tarz bir kamera sisteminin kurulmasına gerek olup olmadığı ortaya konulmalıdır. Yani kamera sistemi olmaksızın beklenen fayda alınabiliyorsa ya da sonuç gerçekleştirilebiliyorsa, bu durumda kameralara gerek bulunmayacak olup buna rağmen kameralar kurulup kayıt ve izleme yapılmışsa, veri koruma hukukunun esas ilkelerinden biri olan ölçülülük ilkesine aykırılık söz konusu olacaktır. Kullanılacak alternatifler olarak evin daha iyi aydınlatma sağlanması, evin etrafının çevrilmesi gösterilebilir. Ayrıca kameraların kayıt altına aldığı alanların tespit edilmesi açısından sadece evlerin ve bahçelerin kayıt altına alınması için kameraların uygun yerlere konumlandırılmasına, kameraların ses kaydı alıp almadığına dikkat edilmesi, ses kayıtlarının özel yaşamın gizliliği açısından çok önemli verileri kayıt yapanlara sunacağı da göz

⁴¹⁵ Bo ZHAO, Unraveling Home Protection in the IoT Age: Smart Living, Mixed Reality and Home 2.0., Columbia Science and Technology Law Review, C. 21, S. 1, Y. 2019, s. 28.

⁴¹⁶ Oliver BUTLER, The Expanding Scope of the Data Protection Directive: The Exception for a “Purely Personal or Household Activity”, Legal Studies Research Paper Series, University Of Cambridge, Faculty of Law, Paper No. 54/2015, Eylül 2015, s. 4.

⁴¹⁷ “Domestic CCTV Systems Guidance for People Using CCTV”, <https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/> (s.y. 30 Şubat 2022)

önüne alındığında görüntü ve ses kaydının birlikte alınmamasına dikkat edilmesi zorunludur.

ÜÇÜNCÜ BÖLÜM

KAPALI DEVRE KAMERALAR İLE GÖZETLENENLERİN KİŞİSEL VERİLERİNİN KORUNMASI

Bireysel özgürlükler ve demokratik kamusal alanın erozyona uğraması, yüz tanıma teknolojileri içeren gözetleme gelişmeleri, dijital gözetleme etkinlikleri sonucunda işlenen verilerin günümüz akışkan toplumları arasında aktarılması gibi olgular kapalı devre kameraları aracılığı ile toplanan bireylere ait kişisel verilerin korunması gibi bir sorunu karşımıza çıkarmıştır. Tez çalışmamızın bu bölümünde bireylerin bu gibi sorunlar karşısında kişisel verilerinin korunması için yararlanabilecekleri hukuki vasıtaları incelemiş bulunmaktayız. İlk olarak Türk hukuk sistemi içerisinde Anayasa'nın aşağıda değindiğimiz maddeleri ve KVKK kapsamında bir değerlendirme yapılması önemli görülmüştür. Bölümün devamında ise başta AB hukuku olmak üzere karşılaştırılmalı hukuk içerisinde kapalı devre kameralara özgü hukuki düzenlemeler incelenmeye çalışılmıştır.

I. Türk Hukuk Sisteminde Kapalı Devre Kameralar İle Gözetlenenlerin Kişisel Verilerinin Korunması

A. Kişisel Verilerin Anayasal Düzlemde Korunması

Kişisel Verilerin korunmasına hangi tür bir hak olduğu açısından yaklaştığımızda farklı görüşlerin bulunduğunu görmekteyiz. Bir taraftan bu hakka bir ekonomik hak olarak yaklaşan bakış açısı bulunmaktadır. Buna karşılık ikinci ve daha ağır basan görüşe göre, kişisel verilerin korunması temel hak ve özgürlüklerden bir tanesi olarak karşımıza çıkmaktadır⁴¹⁸. Kişisel verilerin korunmasında esas olan ve korunması gereken hukuki değer, kişinin mahremiyeti ve bireyin özel hayatına yönelik dışarıdan gelen müdahalelere karşı bireyi korumak olduğunu gördüğümüzde bu yoruma hak vermek mümkündür.

⁴¹⁸ Murat Volkan DÜLGER, İnsan Hakları ve Temel Özgürlükler Bağlamında Kişisel Verilerin Korunması, İMÜHFD, C. 5, S. 1, Y. 2018, s.77.

Kişisel verilerin korunması hakkının bir temel hak ve özgürlük olduğunu destekleyen diğer bir husus da kişisel verilerin korunması hakkı ile yakından ilişkili olan özel yaşamın gizliliği hakkının, BM Evrensel İnsan Hakları Bildirisi, Avrupa İnsan Hakları Sözleşmesi gibi bir takım evrensel insan hakları belgesinde güvence altına alınmış olmasıdır⁴¹⁹. Keza, Kıta Avrupası ve Anglosakson hukuk sistemlerinde kişisel verilerin korunmasına yönelik uygulamaların çoğu zaman özel yaşamın gizliliği hakkı kapsamında yorumlandığını görmekteyiz. Tüm bunlara paralel olarak, AİHM kararlarında bireylerin kişisel verilerinin korunması doğrudan AİHS'in 8. maddesi ile düzenlenen özel hayatın ve aile hayatının korunması hakkı içinde yorumlanmaktadır⁴²⁰.

Diğer bir görüşe göre ise, kişisel verilerin korunması her ne kadar özel yaşamın gizliliği hakkının içinde değerlendirilebilse de günümüzde bu hakkın kendine özgü bir düzenleme ile korunmaması bir eksikliktir ve bu eksikliğin ancak ayrı ve detaylı düzenlemeler yapılarak giderilmesi mümkündür⁴²¹.

12 Eylül 2010 tarihinde yapılan referandum sonucu değişen Anayasa'ya eklenen 20. maddenin 3. fıkrasına göre, *"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"*⁴²². Anayasa'nın lafzından açıkça anlaşılacağı üzere kişisel verilerin korunması açıkça anayasal güvenceye kavuşmuştur⁴²³.

Anayasa'ya yapılan bu ek ile kişisel verilerin korunmasının anayasal güvence altına alınmasından önceki dönemde ise kişisel verilerin korunmasının anayasal zemini Anayasa'nın

⁴¹⁹ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 127.

⁴²⁰ Kişisel verilerin kullanılması ve depolanması konularına ilişkin olarak, S. ve Marper Birleşik Krallığa karşı, Perry Birleşik Krallığa karşı, kişisel verilerin toplanması ve GPS verisine ilişkin olarak, Uzun Almanya'ya karşı kararları bulunmaktadır. S ve Marper, Birleşik Krallık'a karşı, b.n. 30562/04 ve 30566/04, k.t. 4 Aralık 2008; Perry, Birleşik Krallık'a karşı, b.n. 63737/00, k.t. 17 Ekim 2003; Uzun, Almanya'ya karşı, b.n. 35623/05, k.t. 2 Eylül 2010.

⁴²¹ Murat Volkan, DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 101.

⁴²² 7/5/2010 tarihli ve 5982 sayılı Kanun ile yapılan Anayasa değişiklikleri 12/9/2010 tarihinde halkoylamasına sunulurken kabul edilmiş, buna ilişkin 22/9/2010 tarihli ve 846 sayılı Yüksek Seçim Kurulu Kararı 23/9/2010 tarihli ve 27708 sayılı Resmî Gazete'de yayımlanmıştır.

⁴²³ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 323.

20. maddesi ile düzenlenen “*özel hayatın gizliliği hakkı*” olmuştur⁴²⁴. Bu maddeye göre, “*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*” Anayasa Mahkemesi (AYM)’nin çeşitli kararlarında, kişiliğin serbestçe geliştirilmesiyle uyumlu bir çok hukuki çıkarın da bu hakkın kapsamında korunmaya çalışıldığını görebilmekteyiz⁴²⁵. Bu minvalde, iki Anayasal hak arasında bağlantı bulunduğunu belirtmemiz yeterli olacaktır. Anayasa’nın 17. maddesinde düzenlenen “*kişinin dokunulmazlığı, maddi ve manevi varlığını koruma ve geliştirme hakkı*”na aşağıda değinilmiştir.

AYM’nin 2010 yılından önceki uygulamasını görmek amacıyla 2008 yılında verdiği bir kararı incelediğimizde, temel hak ve özgürlüklere müdahale teşkil edebilecek şekilde bireylerden veri ve bilgi talep edilmesinin zorunluluk kapsamında bulunup bulunmadığının değerlendirildiğini görebiliriz. Bu kararda, Anayasa’nın 20. maddesinin gerekçesinde özel hayatın korunmasının, her şeyden önce bu hayatın gizliliğinin korunması ve resmi makamların özel hayata müdahale edememesi anlamına geldiği belirtilmiştir. Neticede AYM, 5429 sayılı Türkiye İstatistik Kanunu’nda yer alan kişilerden istenen verileri, vermekle yükümlü olduklarına ve bu yükümlülüğe aykırı davrananlar aleyhinde idari para cezası uygulanmasını öngören kanun hükmünü Anayasa’nın 20. maddesinde yer alan özel yaşamın gizliliği hükmüne aykırı olması sebebiyle iptal etmiştir.⁴²⁶ Burada dikkatimizi çeken husus bireylerin verilerinin işlenmesinin özel hayatın gizliliği kapsamında değerlendirilmiş olmasıdır.

Keza AYM’nin, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu’nun 78. maddesi’ndeki, “*kişisel veri sayılan sağlık bilgilerinin işlenmesine, gizliliğinin korunmasına ve paylaşılmasına yönelik usul ve esasları belirleme ve bu konuda düzenleme*

⁴²⁴ Hollanda, İspanya ve Portekiz Anayasaları içerisinde kişisel verilerin korunmasına dair özel düzenlemelere yer verilmiştir. Bu durumun temel sebebinin bu anayasaların diğerlerine oranla daha yeni tarihli olmaları olduğunu söylememiz mümkündür. Buna ek olarak, örneğin Fransa’da kişisel verilerin korunması hakkı anayasada yer alan “özgürlük hakkı”na dayandırılırken, Almanya’da ise, bilgilerin geleceğini belirleme hakkı anayasal temelini “genel kişilik hakkı”ndan almaktadır. Ayrıntılı bilgi için bkz. Elif KÜZECİ, Kişisel Verilerin Korunması, s.318.

⁴²⁵ AYMK, Zafer Güvendi başvurusu, b.n. 2014/1214, k.t. 06 Aralık 2017; AYMK, Serap Tortuk başvurusu, b.n. 2013/9660, k.t. 21 Ocak 2015; AYMK, Taner Alır başvurusu, b.n. 2014/14400, k.t. 21 Kasım 2017; AYMK, Tevfik Türkmen başvurusu, b.n. 2013/9704, 03 Mart 2016.

⁴²⁶ AYMK, E. 2006/167, K. 2008/86, k.t. 20 Mart 2008. Bu kararda ayrıca Mahkeme tarafından, kişisel verilerin korunması bakımından özel yaşamın gizliliği hakkı ile düşünce ve kanaat hürriyeti arasındaki bağlantı ortaya koyulmuştur. Anayasa Mahkemesi kararında sadece Anayasa’nın 20. maddesinde düzenlenen özel yaşamın gizliliği hakkının değil aynı zamanda 25. maddesindeki düşünce özgürlüğünün de ihlal edildiğini belirtmiştir.

yapma yetkisinin bütünüyle yürütme organına bırakılmasına” ilişkin düzenlemenin Anayasa’nın 20. maddesi’ne aykırı bulunduğu dair kararı da mevcuttur⁴²⁷.

Yine bununla birlikte Mahkeme bir başka kararında, 20. madde kapsamında özel hayatın gizliliğinin korunması eksenine, kişiye ait görüntü ve ses kayıtlarını sokmuştur⁴²⁸. Ancak yine de 20/3 hükmü yürürlükte iken, kişisel verilerin korunmasına dair daha genel olan 20/1 hükmüne başvurulması kanaatimizce yerinde olmayabilir.

Kişisel verilerin korunması anayasal temelini özel hayatın gizliliği hakkı ya da kişilik hakkı gibi temel hak ve özgürlüklerden alabilse de, özellikle çağımızın getirdiği teknolojik yenilikler düşünüldüğünde bu hakkın tam ve etkin korunmasının sağlanabilmesi için bu konuya ilişkin özel bir düzenleme yapılması gereksinimi doğmuştur⁴²⁹. Bunun sebebi olarak ise henüz KVKK’nın yürürlüğe girmemiş olduğu dönemde, Anayasa’nın 20/3 hükmünde kişisel verilerin işlenmesini denetleyecek bağımsız bir organın öngörülmemiş olması ya da Anayasa’nın 20/3 ve 13. maddeleri gereğince temel hak ve özgürlüklerin sınırlandırılmasında “sınırlandırmanın yasayla yapılması” zorunlu olmakla birlikte bu yasal düzenlemelerin eksik olması olarak görülmüştür.

Netice itibarıyla 7 Nisan 2016 tarihinde yürürlüğe giren KVKK’nın bu beklentileri karşıladığı söylenebilir. Bazı yazarlara göre ise, Anayasa’nın 20/3 hükmü ile Anayasa’ya yapılan ekleme sadece bir başlangıç noktası olarak görülmüştür. Çünkü bu anayasal düzenleme, bireye “kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı” vermekte, bu hak kapsamında devlet bireyin özgürlük alanına girmesi sınırlandırılmaktadır. Bu durum devlet ile birey eksenindeki dikey ilişkiyi ifade eder. Buna karşılık bireylerin kişisel verilerinin korunmasını eşit konumda bulunan diğer bireylerden istemesinin dayanağını ise birey – birey arasındaki yatay ilişkiyi düzenleyen Kanun hükümleri oluşturur⁴³⁰. Bireyler arasındaki ilişkileri düzenleyen KVKK bu bakımdan çok önemli bir yeri doldurmuştur.

⁴²⁷ AYMK, E. 2013/122, K. 2014/74, k.t. 09 Nisan 2014. Bu kararda aynı zamanda Mahkeme tarafından kişisel verinin tanımı yapılmış olmaktadır. Buna göre, “*kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri... gibi kişi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.*”

⁴²⁸ Murat Volkan, DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 141; Karar için bkz. AYMK, Orhan Kayahan başvurusu, b.n. 2014/1970, k.t. 22 Kasım 2017

⁴²⁹ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 320.

⁴³⁰ Mesut Serdar ÇEKİN, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde, Kişisel Verilerin Korunması Hukuku, Onikilevha Yayıncılık, İstanbul 2020, s. 17-18.

Hemen belirtmemiz gerekir ki, kişisel verilerin korunmasının anayasal dayanağı sadece Anayasanın 20. maddesi olarak görülmemelidir. Anayasa’da yer alan aşağıda belirttiğimiz diğer maddelerin de kişisel verilerin korunması ile doğrudan ilişki içinde bulunduğu söylenebilir⁴³¹.

Anayasa’da yer alan “*Kişinin Hakları ve Ödevleri*” başlığı altındaki en önemli temel haklardan bir tanesi de “kişinin dokunulmazlığı, maddi ve manevi varlığını koruma ve geliştirme hakkı”dır. İlgili hükme göre, “*Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir.*” Bu hak kişisel verilerin korunmasının anayasal dayanaklarından bir tanesi olarak sayılabilir. Kapalı devre kameraların gözetimde kullanılmasına dair örnekten yola çıkarsak, bu teknik dahilinde yapılan yoğun gözetimin gerçekleştirilmesi sırasında birey kendisine ait kişisel verilerin ne kadarının, ne zaman ve nasıl işlenebileceğine karar verememektedir. Bu konuda karar verme gücünü kaybeden bireyin, maddi ve manevi varlığını geliştirme hakkını kaybedeceği de söylenebilir. Çalışmamızın önceki bölümlerinde de ifade ettiğimiz üzere, kamera gözetiminin disipline etme süreci ile yakın bağlantısı ile bireyleri bir takım hareketlerde bulunmaya ya da bulunmamaya yöneltmesi söz konusu olabilmektedir. Sürekli gözetlenen birey iktidarın ondan beklediğini yapmak hususunda üzerinde oluşan baskı sonucu bireyin kişiliğini serbestçe geliştirebilmesi hakkına bir müdahale olduğu söylenebilir.

Anayasa’nın 17. maddesi altında kişisel verilerin korunması değerlendirilmesi yapılmadan önce “insan onuru” kavramının tanınması önemlidir⁴³². Çünkü insanın maddi ve manevi varlığını geliştirme hakkı temelini insan onuru kavramından alır. Bu durum AYM’nin ilgili kararında yer alan “*kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verinin işlenmesi sırasında korumayı amaçlamaktadır.*” ifadesiyle açıkça görülmektedir⁴³³.

⁴³¹ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 325.

⁴³² Anayasa Mahkemesinin 28 Haziran 1966 tarihli kararında bu kavram “...insanın ne durumda, hangi şartlar altında bulunursa bulunsun surf insan oluşunun kazandırdığı değer tanınmasını ve sayılmasını anlatır. Bu öyle bir davranış çizgisidir ki ondan aşağı düşünce, muamele ona muhatao olan insanı insan olmaktan çıkarır.” Bkz. AYMK, E. 1963/132, K. 1966/29, k.t. 28 Haziran 1966; Ayrıca Federal Almanya Anayasa Mahkemesi’nin vermiş olduğu kararda “bilgilerin geleceğini belirleme” hakkını kişiliğin serbestçe geliştirilmesi ile insan onuruna dayandırdığını görmekteyiz. Bkz, Elif KÜZECİ, Kişisel Verilerin Korunması, s. 326.

⁴³³ AYMK, E. 2018/73, K. 2019/65, k.t. 24/06/2019, par. 166.

Federal Almanya Anayasa Mahkemesi ise insan onurunun ihlal edilip edilmediğine dair değerlendirmelerini “obje formülü”nden yararlanarak yapmaktadır. Federal Mahkeme tarafından belirtildiği üzere eğer birey, kamu gücü karşısında basit bir objeye ya da araç konumuna indirgenmiş ise insan onurunun ihlal edildiğinden bahsedilmesi söz konusu olacaktır⁴³⁴. Günümüz koşullarında teknolojik gelişmeler ve sürekli olarak dijital gözetim altında kalan bireyin, birey olmasından ziyade sadece bir takım veri bütününden oluştuğu ve böylelikle bir nesneye indirgendiğinden bahsetmemiz mümkündür. Bunun neticesi olarak birey bir obje sayılmakta ve bireyin insan onurunun ihlal edilmektedir. Burada toplumu oluşturan bireylere kişisel verilerinin geleceğini belirleme ve denetleme hakkı tanınmalıdır ki, ancak bu durumda bireylerin maddi ve manevi varlığını koruma ve geliştirme hakkına sahip olduğu söylenebilir.

Goold ise bireyin kendini geliştirmesi bakımından, içinde yaşadığımız dünyada gözetim faaliyetlerinden kaçınılamayacağını, bireyler hakkında sürekli olarak veriler toplanmakta olduğunu, bunu günümüz dijital dünyasında veri gözetimi olarak nitelendirebileceğimizi ifade ederek, gözetim faaliyetlerinin sürekli olarak çoğalması ve sürekli hale gelmesi sonucu⁴³⁵ bireyin toplumdaki rolünün katılaştığını belirtmektedir⁴³⁶. Bunun neticesinde birey kendi olmaktan çıkar ve toplumun ondan beklediği yönde hareket eder. Böylelikle kendini gerçekleştirmekten uzaklaşır ve sonuç olarak insan olmaktan çıkar. O halde tartışılması gereken hangi ölçüde bir gözetim bir hukuk devleti ya da demokratik toplum için fazladır, bunu tespit etmek gereklidir.

Yukarıdaki açıklamalar ışığında kişisel verilerin hukuka aykırı olarak işlenmesinin doğrudan Anayasa’nın 20/3 hükmüne, 20. maddede düzenlenen “*özel hayatın gizliliğine*” ve 17. maddede düzenlenen “*kişinin dokunulmazlığı, maddi ve manevi varlığını koruma ve geliştirme hakkı*”na aykırılık teşkil edeceğini söyleyebilmek mümkündür.

İlgili hakkın korunmasının anayasal dayanakları ile birlikte hangi koşullar altında sınırlandırılabilirliğini de incelemek yerinde olacaktır. Yaşam hakkı, işkence yasağı, düşünce

⁴³⁴ Oğuz ŞİMŞEK, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta, İstanbul 2008, s. 130.

⁴³⁵ Benjamin J. GOOLD, How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy, Allard Faculty Publications (Working Paper), 2010, s.47.

⁴³⁶ Benjamin J. GOOLD, s. 40.

ve ifade özgürlüğü gibi birinci kuşak haklar arasında yer alan özel yaşamın korunması, sınırlama ölçütlerine dayalı olarak ve sınırlama için öngörülen koşullar ve teknikler çerçevesinde sınırlandırılabilir⁴³⁷.

Özel yaşamın gizliliği hakkı ya da Anayasa'nın 20/3 hükmü kapsamında kişisel verilerin korunmasını isteme hakkı sınırlandırılabilen haklardır. Sınırlandırılabilen temel hak ve özgürlükler bakımından sınırlama ölçütlerinin ne olması gerektiğini, hakların keyfi şekilde sınırlandırılmaması olarak anlamak mümkündür. Burada sınırlandırma ölçütlerinin ne olduğunu, bu sınırlandırmanın hangi koşul ve tekniklere bağlı olarak yapılabileceğini ve sınırlandırmanın sınırının ne olacağını incelemek, bunu yaparken de hem Anayasa'nın 13. maddesi hem de hakkın özel sınırlama sebepleri için Anayasa'nın 20. maddesi düzenlenmelerinin incelenmesi gerekli olacaktır. Ancak 20/2 hükmünde belirtilen sınırlama yalnızca kişilerin üstünün, özel kağıtlarının ve eşyasının aranması ve bunlara el konulmasına ilişkin olduğundan incelemenin 20/3 ve 13. madde kapsamında yapılması gerektiği söylenebilir⁴³⁸.

Anayasa madde 20/3 'e göre, “ *Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*” Bu düzenleme kapsamında kişisel verilerin korunması hakkına getirilmiş bir sınırlamanın var olduğunu söylemek mümkündür. Şayet kanunda öngörülen hallerde veya açık rıza verilen durumlarda kişisel veriler işlenebiliyorsa, verisi işlenen kişinin özgürlük alanının daraldığını söylememiz mümkün olduğundan, temel hak ve özgürlüğünün sınırlandırıldığından söz edilebilir. Örneğin, kamera kaydı altında intihara kalkışan bir kimseye ait görüntülerin canlı olarak neredeyse tüm dünya ile anlık olarak paylaşılması durumunda, bu durumun görüntülerde yer alan kimse için Anayasa'nın 20. maddesinin 3. fıkrası kapsamında ihlale sebebiyet verebileceği açıktır. Çünkü buradaki özel sınırlama sebeplerinden bir tanesinin ya da genel anlamda Anayasa'nın 13. maddesinde bulunan sınırlama sebeplerinden bir tanesinin bu olayda bulunmadığı görülmektedir.

Temel hak ve özgürlüklerin sınırlandırılmasını düzenleyen Anayasa'nın 13. maddesine göre, “*Temel hak ve özgürlükler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu*

⁴³⁷ Mehmet Semih Gemalmaz, Ulusalüstü İnsan Hakları, s. 1631.

⁴³⁸ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 329.

sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.” O halde sadece bireysel yarar ile toplumsal yarar arasındaki dengeyi kuran yukarıda belirtilen amaçların yanı sıra aynı zamanda yapılacak sınırlamanın, Anayasanın ilgili maddelerinde belirtilen sebebe bağlı olarak yapılması, “kanuna dayanması” ve “gerekli olduğu ölçüde” yapılması gereklidir. Son olarak ise anayasada belirtildiği gibi, yapılacak sınırlama demokratik toplum düzeninin gereklerine uygun olmalı, ayrıca sınırlama yapılırken hakların ve özgürlüklerin özüne saygı gösterilmesi gerekmektedir⁴³⁹.

Sınırlandırmanın Anayasa’nın ilgili maddelerinde sayılan sebeplere dayalı olarak yapılması zorunluluğu açısından 20/3 hükmü kapsamında, kanunda öngörülen hallerde veya kişinin açık rızasının bulunduğu hallerde işlenebileceği düzenlendiği görüldüğünden sınırlama sebeplerini bunların oluşturduğu söylenebilir. Keza sınırlamanın Anayasa’nın sözüne ve ruhuna uygun olması da diğer bir sınırlama ölçütü olarak karşımıza çıkar. Kapalı devre kamera gözetiminin kanuni olması ve sınırlama sebeplerine bağlı olarak yapılmasının yanı sıra aynı zamanda Anayasa’nın sözüne ve ruhuna da uygun olması gerekecektir. Bu bağlamda hukukun genel ilkelerinden biri olan masumiyet karinesi bağlamında bir değerlendirilme yapılması söz konusu olacaktır. Kamuya açık alanda yapılan gözetimde şüpheli olup olmadığı dikkate alınmaksızın herkese yönelik olarak gerçekleştirilen izleme ve kayıt altına alma faaliyetleri masumiyet karinesine müdahale olarak görülebilir⁴⁴⁰. Ayrıca yukarıda belirttiğimiz demokratik toplum düzeni gereklerinden kastın sınırlamanın demokratik bir toplumda zorunlu ve kaçınılmaz olması anlamında geldiği anlaşılmalıdır. Bu bakımdan kamera gözetiminin suçun önlenmesi amacını gerçekleştirmek için gerekli, uygun ve elverişli bir tedbir olarak tespit edilmiş olması gerekir. Şayet daha hafif bir sınırlama ile aynı amaca ulaşılması mümkün ise daha ağır olan kamera gözetiminin tercih edilmesi demokratik toplum düzenine uygun olmayacaktır⁴⁴¹. Örneğin; belirli bir alana yerleştirilmiş kapalı devre kameraların bilhassa suç işlenmesini önlediği deneysel olarak kanıtlanmış olursa bu uygulamanın bu ölçüt açısından uygun olduğunu söylememiz mümkün olacaktır.

⁴³⁹ Mehmet Semih Gemalmaz, *Ulusalüstü İnsan Hakları*, s. 1635.

⁴⁴⁰ Buket, ABANOZ, *Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu*, On İki Levha Yayıncılık, İstanbul 2018, s. 101.

⁴⁴¹ A.g.e., s. 104.

Buradaki açıklamalara paralel kriterlerin bulunduğu bir diğer ölçüt ölçülülük olarak karşımıza çıkmaktadır. Bu ilkeye göre amaç ile araç arasında makul bir dengenin sağlanması gerekli olup, sınırlamada kullanılan aracın sınırlama amacını gerçekleştirmeye elverişli olması, bu aracın sınırlama amacı bakımından gerekli olması ve araçla amaç arasında ölçülü bir orantılılık olması gerekmektedir⁴⁴². Bu doğrultuda kamera sistemlerinin belirli bir alanda suçları önlemediği, sadece alanın değişmesine sebep olduğu anlaşılırsa burada müdahalenin suçun önlenmesi amacı için elverişli olduğunu söylemek mümkün olmaz. Yukarıda da ifade ettiğimiz daha hafif bir sınırlama ile aynı amaca ulaşılması mümkün iken daha ağır olan kamera gözetiminin tercih edilmesi bu sınırlandırmanın gerekli olmadığı anlamına da gelecektir. Bunlara ek olarak orantılılık değerlendirilmesinde ise kullanılan aracın bireylere ölçüsüz bir yükümlülük getirip getirmediğine ve müdahalenin katlanılabilir nitelikte olup olmadığına bakılmalıdır. Bu bakımdan kapalı devre kameraların sayılarının, kurulacak yerlerin ve kurulum açılarının değerlendirilmesi elzemdir. Bu hususa örnek olarak suç oranının fazla olduğu bölgelere kamera gözetimi yapılması ölçülü görülmekte iken, bireylerin evden bir başka yere giderken gözetlenmedikleri bir alanın bulunmaması her adımlarının kayıt altına alınması ölçüsüz olacaktır. Keza kimlik tespitinin gereksiz olduğu bir izleme faaliyeti gerçekleştiriliyorsa ve buna rağmen kimlik bilgileri tespit ediliyor ve yahut kayıtlanıyorsa faaliyetin ölçüsüz olduğu söylenmektedir⁴⁴³.

Özel yaşamın gizliliği hakkını sınırlandırılmasına ilişkin bir diğer kavram da makul beklenti kavramı olarak karşımıza çıkmaktadır. Bu kavram aslında bireyin mahremiyetine saygı duyulacağına ve korunacağına dair makul bir beklentiye sahip olup olmadığını ifade etmektedir⁴⁴⁴. Bu yönden değerlendirme bireyin bulunduğu mekana göre yapılmaktadır. Daha önce özel hayat-kamusal hayat ayrımı yapılırken, günümüzde kamusal alan ile özel alan ayrımı bulanıklaşarak imkansız hale geldiği için, bazı durumlarda bireylerin kamusal alanlarda da mahremiyetlerinin korunması için makul beklentilerinin olduğu iddia edilmektedir⁴⁴⁵. Kamera gözetiminin yapıldığı yerin caddeler, yollar, sokaklar vb. olduğu MOBESE faaliyetleri değerlendirmeye aldığımızda, bazı kaynaklarda bu faaliyetler dahilinde yapılan kamera

⁴⁴² A.g.e., s. 107.

⁴⁴³ A.g.e., s. 108.

⁴⁴⁴ Bu kavram AİHM mahkemesi tarafından özel yaşamın gizliliğinin ne zaman korunabileceği ya da özel yaşama müdahalenin ne zaman yapılabileceğinin tespiti hususunda kullanılmaktadır. Bkz. Murat HAS, AİHM Kararları Bağlamında Görüntü Hakkı, Anayasa Yargısı, C. 38, S. 1, Y. 2021, s. 230.

⁴⁴⁵ Murat HAS, s. 229.

gözetiminin temel hak ve özgürlüklere müdahale oluşturmayacağı ifade edilmiştir⁴⁴⁶. Bu görüşe göre yapılan gözetim bireylerin özel hayatlarına ilişkin olmamakta, konut veya işyeri gibi özel alanlar izlenmemekte ve bu nedenle sadece kamusal alanlar (caddeler, yollar, sokaklar vs.) gözetlenmektedir. Fakat biz bu görüşe katılmamaktayız. Dikkat edilmesi gerekir ki, bireylerin kamusal alanlarda da kayıt altına alınmasını istemedikleri bir takım davranışları olabilecektir. Bireylerin özel hayatları kamusal alanlarda da tezahür edebilecek olduğundan mahremiyet beklentisinin makul olduğu herhangi bir kamusal alanda, bireyin hareketleri izlenirken temel hak ve özgürlüklerine müdahalede bulunulmamalıdır.

AYM 13/10/2020 tarihli kararında, başvurunun infaz kurumu içerisinde kaldığı odayı görüntüleyen kamera sistemlerinin bulunduğunu ve bu suretle başvurunun yaşam alanının izlendiğini değerlendirerek, somut olayda özel hayata saygı hakkı ile bağlantılı olarak etkili başvuru hakkının ihlal edildiğini, özel yaşamı ihlal edilen başvurucuya etkin çare sunulmadığını belirtmiştir⁴⁴⁷. Mahkeme ilgili kararda, “kameraların odanın iç kısmını kaydedip kaydetmediğini, buna ilişkin şikayet süresince bir araştırma yapıp yapılmadığını, kamera sisteminin doğru şekilde kurulup kurulmadığını, açısının doğru olup olmadığını” hususlarında yeterli inceleme yapılmamış olduğunu vurgulamakla birlikte, başvurunun yaşam alanının kaydedilmesi ihtimaline dikkat çekmiştir. Konuya ilişkin olarak Cumhuriyet Başsavcılığı tarafından İnfaz Hakimliği’ne sunulan görüşte; 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun’un 8. maddesine dayanılarak kapalı ceza infaz kurumlarının tamamının ortak kullanım alanlarına kameraların yerleştirildiği, bu suretle genel ve kısmi aramalarda, sayım saatlerinde veya oda ve koğuş içinde meydana gelen asayiş bozan olaylara müdahale sırasında ortak yaşam alanlarına giren kurum personelinin kural dışı davranışlarının mevcut olup olmadığının izlendiği ifade edilmiş olmaktadır. Buna ek olarak havalandırma bahçelerindeki kameraların banyo, tuvalet ve ranzaların bulunduğu istirahat alanlarında bulunmadığı, bu kısımlarda kayıt yapılmadığı, kayıt uygulamasının belirtilen gerekçeler çerçevesinde havalandırma bahçesi ile sınırlı tutulduğu, havalandırmaya açılan odanın veya koğuş kapısının da kameranın görüş alanında olduğu, bu suretle havalandırmaya ve barınma odası ya da koğuşa giriş-çıkış yapanların görüntülendiği belirtilmiştir.

⁴⁴⁶ Hakan KARAKEHYA, “Gözetim ve Suçla Mücadele”: Gözetimin Tarihsel Gelişimi ile Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme, AÜHFD, C. 58, S.2, Y. 2009, s. 345.

⁴⁴⁷ AYMK, Meral Danış Beştaş başvurusu, b.n. 2017/34087, k.t. 13 Ekim 2020.

Cumhuriyet Başsavcılığı tarafından verilen görüş yazısında sadece ortak kullanım alanlarının, havalandırma alanlarının ve bunlara açılan yerlerin görüntü kaydı alındığını ve izleme yapıldığı ifade edilmekte olup, yine bu faaliyet güvenliğin sağlanması amacıyla ve kanuna dayanarak yapılmaktadır. Yukarıda açıkladığımız üzere temel hak ve özgürlüklerin sınırlandırılması kanun ile yapıldığında geçerli olmakla birlikte, bir takım diğer unsurların ve sınırlandırmanın sınırının da ayrıca değerlendirilmesi lazım gelmektedir. Anayasa'nın 20/3 hükmünde sınırlamanın “ancak kanunda öngörülen hallerde” yapılabileceği düzenlendiği için anayasada sayılan sınırlama sebeplerinden birinden dayandığını söyleyebiliriz. Yine sınırlamanın Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine uygun olduğu yorumu da yapılabilir. Bununla birlikte sınırlamanın hakkın özüne dokunup dokunmadığı açısından ise yapılan müdahalenin temel hak ve özgürlüklerin çekirdeğine müdahalede bulunmaması, o temel hakkın özüne dokunmaması gereklidir. Yani o hakkın kullanılmasını imkansızlaştıracak ya da son derece zorlaştıracak bir sınırlama yapılmaması gereklidir. Başvurucunun iddialarının özel hayatın gizliliğini ortadan kaldıracığı açıkça ortada olduğundan, hakkın özüne müdahalede bulunulduğu ve ayrıca gerçekleştirilmesi istenen amaç ile araç arasında makul bir denge bulunmaması nedeniyle müdahale ölçüsüz sayılacak olup kanaatimizce buradaki müdahalenin Anayasa'ya aykırı sayılması uygun olmuştur.

Ayrıca belirtmemiz gerekir ki, AYM önüne ister bireysel başvuru yoluyla ister iptal davası yoluyla gelmiş olsun, kişisel verilerin korunması alanına ilişkin farklı konularda kararları⁴⁴⁸ bulunmakla birlikte, Kanun'un uygulama alanının teknolojideki gelişmeler ve dijital dünyaya ayak uydurmada yaşanacak mahremiyet tartışmaları açısından gelişeceği göz önünde bulundurulduğunda, AYM önüne gidecek veri koruma uyuşmazlıklarının artış göstermesi şaşırtıcı olmayacaktır.

B. Kişisel Verilerin Korunması Kanunu Kapsamında Gözetlenenlerin Kişisel Verilerinin Korunmasını İsteme Hakkı

⁴⁴⁸ Sağlık verilerine ilişkin olarak AYMK, E. 2011/150, K. 2013/30, 14 Şubat 2013; AYMK, E. 2013/114, K. 2014/22, 04 Aralık 2014. Biyometrik verilere ilişkin olarak AYMK, E. 2014/180, K. 2015/30, 19 Mart 2015. Elektronik haberleşmeye ilişkin olarak AYMK, D.İd.D.K. başvurusu, b.n. 2013/122, 09 Nisan 2014. Unutulma hakkına ilişkin olarak AYMK, N.B.B. başvurusu, b.n. 2013/5653, k.t. 24 Ağustos 2016. Ayrıntılı bilgi için bkz. Elif KÜZECİ, Kişisel Verilerin Korunması, s. 338..

Türk hukuk sisteminde Anayasa ve Anayasa'nın 90/5. Maddesi gereği usulüne uygun olarak yürürlüğe girmiş uluslararası düzenlemelerden sonra kişisel verilerin korunması hususunda genel düzenleyici kanun metni 24 Mart 2016 tarihinde TBMM' de kabul edilerek, 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur. Kanunun yürürlüğe girmesinden önceki dönemde, birçok Avrupa ülkesinde yer alan yasal düzenlemeler yaklaşık kırk yıllık bir geçmişe sahipken, Türkiye' de kişisel verilerin korunması alanında özel bir kanun bulunmaması hem hukuki hem de ekonomik anlamda bir takım eksiklikler yaratmıştır.

Avrupa Konseyi (AK) üyesi olan devletlerden biri olarak, 108 sayılı Avrupa Konseyi Kişisel Verilerin Korunması Sözleşmesi (108 sayılı Sözleşme)'nin Türkiye tarafından onaylanarak kabul edilmesi sözleşmenin ilk imzalandığı tarihten itibaren yaklaşık otuz beş yıl sonraya denk gelmiştir. Kıta Avrupası hukuk sistemi içerisinde yer alan diğer düzenleme olan AB Veri Koruma Yönergesi (ABVKY) ve sonrasında getirilen GVKT ile sadece AB üyesi olan devletlerin ya da bu devletlerde bulunan kuruluşların değil, AB dışında bulunan ülkelerde bulunanların da veri işleme ve aktarma faaliyetlerinin düzenlenmesi öngörülmüştür. Nitekim GVKT'nin 45. maddesinde belirtildiği üzere AB üyesi olmayan üçüncü ülkeler ile yapılacak veri transferi, kural olarak sadece yeterli koruma seviyesi sağlanırsa mümkün olacaktır⁴⁴⁹. Bu durumda Türkiye'de bulunan yasal mevzuatların “yeterli koruma seviyesi”ni sağlama açısından kapsayıcı düzenlemeler yapması ve gereklilikleri karşılaması bir beklentinin karşılanması olarak görülebilir.

Ekonomik ve ticari yönden bakıldığında, Türkiye ile en çok ticari faaliyet yapan ülkelerin başında AB üyesi ülkelerin geldiği görülmektedir. 31 Aralık 2020 tarihinde yayınlanan TÜİK verilerine göre, aynı yılın Kasım ayında en fazla ihracat yapılan ülkenin AB üyesi ülkelere Almanya olduğu görülürken, ithalatta da yine Almanya'nın birinci sırada

⁴⁴⁹ GVKT'nin 45. maddesine göre, kural olarak sadece Komisyon' un hakkında yeterli koruma seviyesine sahip nitelendirilmesi yaptığı üçüncü ülkeler ya da uluslararası organizasyonlar ile veri aktarımının gerçekleştirilmesi mümkün olacaktır. Avrupa Komisyonu'nun Avrupa Birliği dışındaki herhangi bir ülke için alacağı bu yönde bir karar tüm üye ülkeler için geçerli sayılacaktır. Ayrıca yine aynı maddenin ikinci cümlesinde belirtildiği üzere, Komisyon karar aldıktan sonra veri kontrolörlerinin ve işleyicilerin herhangi bir özel yetkilendirmeye tabi olmaksızın veri transferi gerçekleştirmeleri mümkündür. Bu bakımdan çok önemli bir karar olan yeterlilik kararı bugün itibarıyla Andorra, Arjantin, Kanada (ekonomik kuruluşlar ile sınırlı olmak üzere), Faroe Adaları, Guernsey, İsrail, Man Adaları, Japonya, Jersey Adaları, Yeni Zelanda, İsviçre ve Uruguay hakkında alınmıştır. Yeterli koruma sağlayan ülkeler statüsü için aday durumda bulunan Güney Kore için ise süreç devam etmektedir. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/ad-equacy-decisions_en (s.y. 16 Kasım 2020)

olduğu görülmektedir. Almanya ile Türkiye arasında gerçekleşen toplam ithalat-ihracat hacmi sadece Kasım ayında 3 milyar 867 milyon dolar olarak kayıtlara geçmiştir⁴⁵⁰.

Yapılan ticaretin beraberinde veri paylaşımını da getirmesi bir zorunluluk olarak karşımıza çıkmakla, son dönemde gelişmekte olan ve belki de Covid-Sars 2019 Pandemisi ile altın çağını yaşayan e-ticaret ve internet tabanlı online uygulamalar, bireyleri kişisel verilerini sürekli olarak üçüncü kişilerle paylaşmak zorunda bırakmaktadır. Bu durum iki açıdan önem teşkil eder. İlk olarak ekonomik anlamda AB üyesi ülkeler ile ticaret yapmak zorunda olan Türkiye tarafından, Avrupa'da uygulanan mevzuat ve kurallara paralel düzenlemelerin yapılması gerekli olmaktadır. Bu durum kısaca mevzuatın AB düzenlemelerine uyumlu hale getirilmesi ve aynı zamanda Avrupa Birliği'ne üyelik sürecinde aşılması gereken bir duvar olarak karşımıza çıkmaktadır. İkinci olarak ise, kendi vatandaşlarının gelişen ve değişen teknoloji karşısında korunmasına yönelik kişisel verilerin işlenmesi ve aktarımını düzenleyen kanun çıkarmak ve etkin bir şekilde uygulanmasını denetlemektir.

Ülkemizde kişisel verilerin korunması hakkında yasal bir düzenlemenin bulunması aynı zamanda uluslararası işbirliği sağlanması amacıyla da önemlidir. Örneğin; Avrupa Konseyi üyesi devletler ile adli yardım süreçlerinin yürütülmesinde ya da Türk Mahkemelerinin adres tespiti, istinabe taleplerinde Türkiye tarafından kişisel verilerin korunmasına ilişkin yeterli koruma düzeyinin sağlanamadığından, bu konularda gerçekleştirilmesi istenen işbirlikleri gerçekleştirilememektedir⁴⁵¹. Avrupa polis teşkilatı EUROPOL veya ceza iş birliği teşkilatı EUROJUST gibi teşkilatlar ile işbirliği yapılamaması, elektronik veri aktarımı gerçekleştirilememesi gibi kanunun gerekçesinde⁴⁵² belirtilen diğer gerekçeler de uluslararası beklentileri karşılayabilecek bir kanun yapılmasını zorunlu kılmıştır. Özellikle belirtmemiz gerekir ki bu gibi amaçların gerçekleştirilebilmesi için sadece kanuni düzenlemenin yapılması ve yürürlükte olması yetmeyecektir. İlgili kanunun veri koruma açısından beklenen güvenliği sağlaması, kanuna aykırılık durumlarının aktif bir şekilde değerlendirilmesi ve buna göre yaptırımların uygulanıyor olması da gerekmektedir.

⁴⁵⁰ Türkiye İstatistik Kurumu, Dış Ticaret Verileri, Kasım 2020, Yayın Tarihi: 31/12/2020, Sayı: 33859, <https://data.tuik.gov.tr/Bulten/Index?p=Dis-Ticaret-Istatistikleri-Kasim-2020-33859> (s.y. 10 Ocak 2022)

⁴⁵¹ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 343.

⁴⁵² Kişisel Verilerin Korunması Kanunu Genel Gereke.

Tüm bu süreçlerden geçen ülkemizde kişisel verilerin korunmasına ilişkin olarak KVKK'nın önemli bir yeri bulunduğu doğrudur. Çalışmamızın bu bölümünde kapalı devre kameralar vasıtasıyla yapılan gözetime KVKK açısından bakacağız. Bu kapsamda bireye ait kapalı devre kamera kayıtlarının hukuki niteliğine, Kanun'un uygulama alanına, veri korumanın genel ilkelerinin nasıl uygulanacağı başta olmak üzere bu gözetim özelinde kişisel verilerin korunmasına ilişkin önem arz eden hususları, kişisel veri sayılan bu kayıtların hangi koşullar altında işleneceğini, ilgili kişilerin bu verilere erişmek için hangi prosedürlere tabi bulunduklarını inceleyeceğiz. Fakat öncesinde bazı önemli hususlarda bilgi vermemiz gerekecektir.

Öncelikle, KVKK'nın uygulama alanı bulabilmesi için ilk şart işlenen kişisel verilerin bir gerçek kişiye ait olmasıdır⁴⁵³. Kanun'un 3. maddesinin (d) bendinde yer alan kişisel veri tanımını da göz önünde bulundurduğumuzda, kişisel veri sayılan görüntü kayıtları ya da fotoğrafların “kimliği belirli” veya “belirlenebilir” bir gerçek kişiye ait olması zorunludur. Buradan çıkarılması muhtemel bir sonuç da kapalı devre kameralara yansıyan görüntülerdeki gerçek kişinin kimliğinin tespit edilme ihtimali bulunmuyorsa, bu Kanun'un uygulama alanı bulmayacağıdır.

KVKK'nın 2016 yılında yürürlüğe girmiş olması, geçici 1. maddesi'nin 3. fıkrasında belirtilen kanunun yayımı tarihinden önce işlenen kişisel verilerin yayım tarihinden itibaren iki yıl içerisinde kanuna uyumlu hale getirilmiş olması zorunluluğu ile birlikte düşünüldüğünde , hukukumuz açısından veri koruma hukuku kuralları ve uygulamalarının daha yeni olduğu söylenebilecektir. Bu durum aslında bir dezavantaj olarak görülebilir. Ancak aynı zamanda yapılması gereken düzenlemelerin teknolojik gelişmelerin sürekli ilerlediği bir döneme denk gelmesi, eğer hukuki düzenlemeler teknolojiadaki gelişmeler göz önünde bulundurularak yapılmakta ise mevcut durumu lehe çevirmek, avantajlı hale getirmek mümkün olacaktır.

Küzeci'ye göre; “temel hak ve özgürlüklerin korunması açısından bir boşluk oluşmaması için ilgili hükümlerin yeni gelişen teknolojiye de uyarlanabilmesi gerekir.”⁴⁵⁴ Nitekim, AB veri koruma hukuk sisteminde de yer alan bu görüş “teknoloji geçirmezlik” adlandırılmakta ve çok önemli görülmektedir. KVKK'da yer alan düzenlemelerin büyük ölçüde bu görüşü desteklediğini söyleyebiliriz. Keza Kanun'un 3. maddesinde yer alan kişisel verinin

⁴⁵³ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s 346.

⁴⁵⁴ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 355.

ne olduğunun ve kişisel verinin işlenmesi sayılan faaliyetlerin sınırlı sayı ilkesiyle sayılmadığı, aksine bu tanımlar kapsamında giren her türlü verinin kişisel veri olduğu, gerçekleştirilen her faaliyetin veri işleme kabul edildiği görülmektedir⁴⁵⁵. Böylelikle, yeni teknolojiler ile işlenen verilerin ya da yeni tekniklerle işlenen ya da toplanan kişisel verilerin de bu kanunun uygulama alanına gireceği açıktır. Kapalı devre kamera sistemleri, RFID teknolojileri ya da her türlü internet ağları veya mobil cihazlar aracılığıyla işlenen kişisel verilerin, KVKK'da yer alan veri işleme etkinliği açısından birbirinden farkı bulunmamaktadır⁴⁵⁶.

Bununla birlikte, tasarımda gizlilik (privacy by design) ilkesi dediğimiz ve veri korumanın teknik altyapının oluşturulması sırasında dikkate alınmasını gerektiren düzenleme GVKT'da yer bulmasına rağmen, KVKK'da bulunmamaktadır. İlerideki bölümlerde ayrıntısını vereceğimiz bu ilkenin sağladığı hukuki korumanın, teknolojideki gelişmelere paralel olarak gelişmesi çok önemlidir. Dolayısıyla bu durumu bir eksiklik olarak görmek mümkündür. Ancak diğer bir yönden, AB Hukuku uygulanmasının bir bütün olarak birlik üyesi olmayan Türkiye açısından imkanı bulunmayacağını göz önünde bulundurarak, teknolojik gelişim hususundaki görüşlerimizi Kişisel Verileri Koruma Kurulu'nun vereceği ilke kararlar ve çıkarılacak ikincil mevzuatı takip ederek geliştirmek de olası görülmektedir.

KVKK'nın Türk Hukuk sistemine girdiği dönemde GVKT'nın taslağı hakkında bilgi sahibi olma fırsatına sahip kanun koyucu, ABVKY'ye göre nispeten daha ayrıntılı düzenlemeler içerdiği görülebilen GVKT yerine ABVKY'yi emsal almıştır. Bu hususta kişisel verilerin korunması açısından daha kapsamlı ve etkin bir korumanın öngörüldüğü GVKT'yı göz ardı etmiş gibi görülen kanun koyucunun bu yönde eleştirilmesi mümkün olabilir. Ancak Kişisel Verileri Koruma Kurulu'nun faaliyete başladığından beri etkili bir çalışma performansına sahip olduğu, karar ve ilke kararları ile uygulamaya yön verdiği görüldüğünde bu eksikliğin bir bakıma da olsa giderildiğini söyleyebiliriz. Nitekim Kurul'un 2020 yılı içerisinde Kanun'un 25. maddesinin 4. fıkrasının (c) bendi kapsamında, Kurum içi ve Kurum dışından gelen 208 adet hukuki görüş talebine cevap verdiği tespit edilmiştir⁴⁵⁷. Keza aynı yıl içerisinde Kurul'un sonuçlandırdığı 1818 adet şikayet ve ihbarın 91 tanesi hakkında idari para

⁴⁵⁵ KVKK, md. 3.

⁴⁵⁶ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 355

⁴⁵⁷ Kişisel Verileri Koruma Kurumu, 2020 Yılı Faaliyet Raporu, s. 36, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/60c02fcc-0abf-4c8e-8b9b-514f34a1b0e6.pdf>, (s.y. 19 Mart 2022)

cezası uygulanmasına, 79 tanesinin talimatlandırılmasına ve 17 adedi hakkında ise kişisel veri işleme faaliyetinin durdurulmasına karar verilmiştir⁴⁵⁸.

1. KVKK Kapsamında Kapalı Devre Kamera Kayıtlarının Hukuki Niteliği

Kişisel Verilerin Korunması Kanunu’nun 3. maddesinin 1. fıkrasının (d) bendi uyarınca kişisel veri, *“kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi”* ifade etmektedir. Aynı maddenin 1. fıkrasının (e) bendi uyarınca *“kişisel verilerin işlenmesi”* ise; *“kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”* olarak tanımlanmıştır.

Yukarıda bahsedilen hükümler doğrultusunda Kanun’un kişisel veri işleme faaliyetini tanımlarken örnek olması adına bir takım işlemlerden bahsetmiş olduğu fakat işleme faaliyetini bunlarla sınırlı tutmadığı görülmüştür. Bu bakımdan, kişisel veriler üzerinde gerçekleştirilecek her türlü eylem, kişisel veri işleme faaliyeti olarak kabul edilecek ve KVKK kapsamında değerlendirilecektir.

Video kamera yoluyla gözetleme bireyin kişisel verilerine dayanılarak yapılır⁴⁵⁹. Kaydedilen görüntülerin çoğu zaman bir kişinin doğrudan ya da dolaylı olarak belirlenmesine olanak tanıdığı kabul edilmektedir⁴⁶⁰. Kayıt edilen ya da izlenen görüntüde kimliği belirli ya da belirlenebilen bir kimse bulunuyorsa kişisel verilerin işlendiğinden bahsedilmesi mümkündür. Bu nitelendirmeyi konumuza indirgeyerek gerçekleştirdiğimizde ise gerçek kişilere ait kapalı devre kamera kayıtlarının da kişisel veri olarak nitelendirilmesinin mümkün olduğunu söyleyebiliriz.

⁴⁵⁸ 2020 yılı içerisinde Kurul tarafından kesilen idari para cezasının toplam meblağı ise 21.390.000 TL olarak kayıtlara geçmiştir. Bu miktar 2019 yılı için 13.105.828 TL, 2018 yılı için ise sadece 870.000 TL’dir. Bkz. A.g.i., s. 44.

⁴⁵⁹ Murat Volkan DÜLGER, *Kişisel Verilerin Korunması Hukuku*, s. 625.

⁴⁶⁰ Elif KÜZECİ, *Kişisel Verilerin Korunması*, s. 507.

Çalışmamızın önceki bölümünde de vurguladığımız üzere, Türk hukuk sistemi içerisinde “kişisel verilerin korunmasını isteme hakkı” Anayasa md. 20/3 hükmüyle açıkça düzenlenmiştir. Bu maddede düzenlenen özel yaşamın gizliliği ve kişisel verilerin korunması hakları bir temel hak ve özgürlük olarak tanınmıştır. Ayrıca kişisel verinin hukuki niteliğine bakış açısından bu hakkın medeni hukuk alanı içinde kişilik hakkı kapsamında yer aldığına ilişkin görüşler de bulunmaktadır⁴⁶¹. Fakat kişisel verinin mülkiyet hakkı sahipliği dolayısıyla tam olarak bir mal olarak görülmesi ya da bir insan ürünü olarak tam olarak fikri mülkiyet hakkı kapsamında değerlendirilmesi⁴⁶², veri koruma hukukunun gerçek amacının yukarıda bahsettiğimiz evrensel metinlerde de vurgulandığı gibi insan onuru ve temel hak ve özgürlükler gibi daha geniş bir alanı olduğunu kabul ettiğimizde pek de yerinde görülmemektedir.

Tüm bu açıklamalar ışığında da kamera kayıtlarının kişisel veri olarak, temel insan haklarının özel hukuktaki tezahürü olarak kişilik hakkına yakın fakat sadece özel yaşamın gizliliği sınırlarına tabi olmadan, insani değerlerinde göz önünde bulundurularak multi-disipliner bir değer olarak görülmesi daha uygun olacaktır⁴⁶³.

2. Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı

KVKK’nın uygulama alanını bu konudaki farklı unsurları değerlendirmek suretiyle ortaya koymamız daha uygun olacaktır. Bu unsurları kanunun amacı, hakkın konusu, hakkın öznesi olan ilgili kişi, veri sorumlusu olarak adlandırılan hakkın yükümlüsü olarak sınıflandırmamız mümkün olup, bunların dışında yine kişisel veri işleme faaliyetlerini düzenleyen Kanun’un 5. maddesinde yer alan kişisel veri işleme şartları ya da Kanun’un 28. maddesinde düzenlenen istisnaların daha detaylı olarak ayrı bölümlerde incelenmesini gerçekleştireceğiz. Söz konusu unsurların KVKK içerisinde tanımlamaları yapılmış olsa bile bu tanımların kapsamının ne olduğunun, neleri kapsayıp neleri dışarda bıraktığının tespitinin kapalı devre kamera görüntüleri özelinde değerlendirilmesi tezimiz açısından önem teşkil eder.

KVKK’nın 1. maddesinde Kanun’un amacının “...*kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel*

⁴⁶¹ Sinan Sami AKKURT, Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış, Kişisel Verileri Koruma Dergisi, C.2 , S.1, Y. 2020, s. 26.

⁴⁶² Pamela SAMUELSON, Privacy As Intellectual Property?, Stanford Law Review, C. 52, S. 5, Y. 2000, s.1126.

⁴⁶³ Sinan Sami AKKURT, Kişisel Veri Kavramı, s. 30.

verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek...” olduğu belirtilmiştir. Daha önce yaptığımız kişisel verilerin korunması hakkının hukuki niteliğine ilişkin açıklamalara da paralel olarak kişisel verinin korunmasını bir temel hak ve özgürlüğün korunması olarak düşünmemiz gereklidir. Madde metninde ifade edilen birbiriyle bağlantılı iki amacı birlikte değerlendirdiğimizde, ilk olarak kişisel verilerin korunmasına ilişkin düzenleme yapılmasının temel amacının kişisel verilerin işlenmesinde özel hayatın gizliliği ile diğer kişilik haklarının korunmasına bağlandığı ifade edilebilir⁴⁶⁴. Kanun bununla birlikte kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile bu kişilerin uyacakları usul ve esasları düzenlemeyi amaçlamış olmaktadır. Neticede bu madde ve maddenin gerekçesi kapsamında Kanun’un kişisel verilerin işlenmesinde amaçladığı noktalar olarak şunları saymamız mümkündür: Kişilerin temel hak ve özgürlüklerini korumak, kişinin mahremiyet hakkını korumak, bilgi güvenliği hakkı kapsamında kişisel veri güvenliğini sağlamak, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile bu kişilerin uyacakları usul ve esasları düzenlemek⁴⁶⁵. Bu durumda kişisel verisi işlenen, teknik araçlarla toplanan ya da kaydedilen görüntülerde yer alan bireylerin bu görüntülerinden dolayı ihlale uğrayabilecek nitelikteki haklarının korunması amaçlanmış olmaktadır.

Kanun’un 3. maddesi’nde, “*kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır. KVKK’nın yürürlüğe girmesinden önceki dönemde ise diğer bazı mevzuat hükümlerinde kişisel veriye ilişkin düzenlemelerin olduğunu görebiliyoruz olsak da kişisel veri tanımının ne olduğuna ilişkin herhangi bir düzenleme bulunmadığından uygulamada zorluklarla karşılaşılılabiliyordu. Bu bakımdan TCK’nın 135 ile 140. maddeleri arasında düzenlenen kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme, verileri yok etmeme suçları örnek olarak gösterebilmek mümkündür⁴⁶⁶.

⁴⁶⁴ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 345.

⁴⁶⁵ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 346.

⁴⁶⁶ TCK ‘nın 135. maddesi metninde “*hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir*” şeklinde düzenleme yapılmış olmasına rağmen KVKK’ nın yürürlüğe girmesine kadar bu kişisel verinin tam olarak neyi ifade ettiği konusunda bir tartışma söz konusu olmuştur. Yargıtay Ceza Genel Kurulu (YCGK) 17 Haziran 2014 tarihli kararında, “*kişisel veriden ne anlaşılması gerektiğine ilişkin yürürlükte bulunan kanunlarda*” bir tanım yer almadığına işaret etmiştir. YCGK, E. 2012/12-1510, K. 2014/331, T. 17/06/2014; Suçta ve cezada kanunilik ilkesine aykırı olan bu durum ayrıca Anayasa Mahkemesi önüne taşınmış, ancak AYM tarafından Anayasaya aykırılık başvurusu, “*gerek ulusal ve uluslararası mevzuat gerekse Yargıtay içtihatları çerçevesinde kişisel veri kavramının, belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri ifade ettiği; kişisel veri kavramının bu çerçevede doktrin, uygulama ve yargı kararlarında belirlenerek anlam ve içeriğinin gelişip değişeceğinden*” bahsedilerek reddedilmiştir. Ayrıntılı bilgi için bkz. Elif KÜZECİ, s. 313.

Kanun maddesinde belirtilen her türlü bilgi ifadesinden ne anlaşılması gerektiği konusunda ilk vurgulanması gereken husus kanun koyucunun bu “veri”yi sınırlı olarak sayma yolunu tercih etmediği, böylelikle, kavramın sınırlarını gelişmeye açık bıraktığıdır. Bu bakımdan bilginin türüne ilişkin herhangi bir ayırım yapılmadığı, ses ya da görüntü, video kaydı gibi bir bilginin bu kapsamda yer alabileceğini söyleyebiliriz. Ancak bu bilginin, mutlaka belirli ya da belirlenebilir bir kişiye ait olması bir zorunluluktur. Burada dikkat edilmesi gereken husus ise bireylerden toplanan büyük ölçekli verilerin kullanılması yoluyla profil çıkarma işlemleri yapılmasıdır. Büyük verinin içerisinde, belirli bir anlam ifade eden kullanışlı bir verinin çıkarılmasına yönelik teknolojiler önem arz etmektedir. Veri madenciliği ve profil çıkarma denilen işlemler büyük ölçüde bu işlevi yerine getirmek için var olmuşlardır. Otomatik olarak oluşturulan bu analizler aynı zamanda gerçek kişiler arasındaki bağlantıları da ortaya koyabilmekte, bu nedenle hem gerçek kişi açısından hem de belirli gruplar açısından tehlike oluşturabilecektir⁴⁶⁷.

Yukarıdaki açıklamaya istinaden yapılan işlemler sonucu oluşturulan profiller üzerinden gerçek kişiye ulaşıyorsa zaten doğrudan Kanun’un uygulaması kapsamında girildiği söylenecektir. Profil çıkarma da dahil otomatik karar verme süreçlerinde kişisel verilerin işlenmesine dair GVKT’de açık bir düzenleme bulunmaktadır⁴⁶⁸. Aynı açıklıkta bir düzenleme KVKK’da olmasa bile, md.2’de yer alan kapsamın içerisinde “*kişisel verilerin tamamen veya kısmen otomatik yollarla*” işlenmesi faaliyetlerinin de belirtildiği görüldüğünde bu yönde profil çıkarma işlemlerinde de KVKK’nın uygulama alanı bulabileceğini söyleyebiliriz. Örnek vererek somutlaştırsak, herhangi bir video veri seti içerisinde belirli bir hareketi yapan ya da yapmayan bireylerin tespit edilmesi istenebilir. Örneğin; trafik kural ihlallerinin tespiti amacıyla yapılan ve çok büyük bir veri seti içerisinde anlamlı verilerin ayrıştırılması işleminde görüntüsü işlenen kişilerin KVKK’nın korumasından yararlanıyor olması gerekir.

KVKK’nın 3. maddesinin gerekçesine göre, “*Yalnızca ad, soyad, doğum tarihi ve doğum yeri gibi kişinin kesin teşhisini sağlayan bilgiler değil, kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o*

⁴⁶⁷ Bart CUSTER, Tapping and Data Retention in Ultrafast Communication Networks, Journal of International Commercial Law and Technology, C. 3, S. 2, Y. 2008, s. 96.

⁴⁶⁸ GVKT, md. 22.

kişinin tanımlanabilir hale getirilmesini ifade eder. Bu durum, kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar.” Kapalı devre kamera görüntülerinin, genellikle tek bir merkezde toplanmış, yetkililer dışında diğer üçüncü kişilerin bu sistemlere erişim sağlayamadığı bir video kamera sistemi bütünü (CCTV) bir parçası olarak üretildiğini görmekteyiz. Sistem tarafından oluşturulan görüntüler ise hakkın konusunu oluşturur. Kısacası kamera kayıtlarının ya da görüntülerinin kişisel veri olduğunu söyleyebiliriz.

Bizim veri koruma kanunumuzda video kamera ile izleme faaliyetlerinin direkt tanımı yapılmamış olsa da aynı konudaki tanıma, Avusturya Kişisel Verilerin Korunması Kanunu’nda yer verildiği görülmektedir. Bu düzenlemenin 50. maddesine göre, *“video kamera ile izleme belirli bir nesne ya da kişi ile ilgili görüntülerin sistematik ve sürekli olarak video aktarımına uygun cihazlarla tespit edilmesidir.”*⁴⁶⁹ Buradan çıkarılacak sonuca göre, veri işleme faaliyetinin konusunu teşkil eden kişisel verinin bir “kamera kaydı, görüntü” olduğu açıkça görülmektedir. O halde kişisel verisi hukuka aykırı olarak işlenen birey aslında üçüncü kişilerin kontrolündeki sistemler aracılığıyla oluşturulan görüntülerinin hukuka aykırı olarak kullanıldığını iddia etmektedir.

KVKK açısından incelememiz gereken diğer bir husus ise veri işleme faaliyetine konu edilen görüntünün kime ait olduğudur. KVKK’da *“kişisel verisi işlenen gerçek kişi”* nin yani veri öznesinin, “ilgili kişi” olarak tanımlandığını görmekteyiz⁴⁷⁰. Tüzel kişilerin bu hak kapsamına girip girmediği hususunda tartışmalar bulunsa da konumuz itibarıyla kameralar vasıtasıyla gözetlenen şeyin bir tüzel kişi olamayacağı açıkça ortada olduğundan bu tartışmalara değinmeyeceğiz⁴⁷¹. Fakat yine de doktrindeki baskın görüşe göre, KVKK’da belirtilen ilgili

⁴⁶⁹ Avusturya Veri Koruma Kanunu (Datenschutzgesetz) md. 50a’dan naklen Tevfik Sönmez KÜÇÜK, s .66.

⁴⁷⁰ Genel Veri Koruma Tüzüğü’nün 4. maddesi’nin 1. fıkrasına göre, kimliği belirli veya belirlenebilir verisi işlenen kişi, doğrudan veri öznesi olarak nitelendirilmiştir. GVKT, md. 4. f.1.

⁴⁷¹ Tüzel kişilerin ilgili kişi olup olamayacağının tespitinde KVKK’nın kapsam başlıklı 2. maddesini incelediğimizde, “kanun hükümlerinin kişisel verileri işlenen gerçek kişiler” hakkında uygulanacağını belirtildiğini görmekteyiz. Hem bu madde hem de tanımlar maddesinde ilgili kişinin gerçek bir kişi olarak tanımlandığını gördüğümüzde, tüzel kişinin ilgili kişi olmayacağı söylenebilir. Ancak bu durumun 2008 yılındaki KVKK Tasarısı’nda yer alan düzenlemeden farklı olduğu ortaya konulmalıdır. Zira bu tasarı içerisinde tüzel kişilere ilişkin bilgi ve belgeler de kişisel veri olarak tanımlanmıştır. KVKK (2008) md. 3. f.1. (ç). Bu görüş daha sonra gelen 2014 yılındaki tasarıda değiştirilerek, KVKK’da kanunlaştığı son haline evrilmiştir. Habip OĞUZ, Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, Elektronik Ticaret Hukuku Sempozyumu, 25 Nisan 2014, s. 18; Tüzel kişilerin de kişisel verilerin korunması düzenlemelerinin öznesi olup olamayacağına ilişkin Anayasa Mahkemesi tarafından

kişi kavramının kapsamına tüzel kişinin girmemesine yönelik kanuni tanımın yerinde bulunduğunu belirtmemiz yerinde olacaktır⁴⁷². Bu durum ayrıca Kişisel Verileri Koruma Kurulu’nun 3 Nisan 2019 tarihli, “*Tüzel kişiliğe ait verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkında 19/11/2018 tarihli ve 2018/131 sayılı Karar*” içerisinde değerlendirilmiştir. Kurul yukarıdaki açıklamalara paralel olarak, “*söz konusu başvuruda yer alan, tüzel kişiliğe ait verilere erişilmesi yönündeki talebin Kanunun 2. maddesi gereğince Kanun kapsamında değerlendirilemeyeceğine*” karar vermiştir⁴⁷³.

Kişisel verilerin korunması alanına ilişkin olarak KVKK’da yer alan ilgili kişi dışındaki diğer aktörler, “veri sorumlusu” ve “veri işleyen”lerdir. Kanun’ da yer alan tanıma göre, veri sorumlusu “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak ifade edilmiştir⁴⁷⁴. Yine aynı maddeye göre veri işleyen ise “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak belirtilmiştir.

Kişisel verileri işleyen taraf bakımından belirtilmesi gereken husus, verileri işlenen kişilerden farklı olarak bu tarafların gerçek ya da tüzel kişi olmasının mümkün olmasıdır⁴⁷⁵. Veri sorumlusunun bir tüzel kişiliğinin bulunması halinde, tüzel kişiliğin içinde bulunan departmanların ya da herhangi bir çalışanın doğrudan kanun kapsamında sorumlu konumunda bulunması söz konusu olamayacak olup, sorumluluk veri sorumlusu sıfatına sahip tüzel kişiye ait sayılacaktır⁴⁷⁶.

yapılan bir değerlendirmede AYM’nin, Anayasa’nın 20/3 hükmünde yer alan “herkes” ifadesinin tüzel kişileri de kapsadığı ve bu yönde tüzel kişilerinde de koruma kapsamında yer alması gerektiğine hükmettiği görülmüştür. Bkz. AYMK, E. 2013/84, K. 2014/183, K.T. 04/12/2014; Elif KÜZECİ, Kişisel Verilerin Korunması, s.342; Bu tartışmaya diğer bir yönden baktığımızda ise kişisel verilerin korunması hakkının bir insan hakkı olarak ele alınması gerekeceği, bireyin temel hak ve özgürlüklerinin sağlanması ile ilgili olduğu göz önünde bulundurularak, yasal korumanın gerçek kişilere yönelik olarak sınırlandırılması yerinde görülmüştür. Bkz. Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 346.

⁴⁷² Oğuz ŞİMŞEK, s. 207; Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 346.

⁴⁷³ Tüzel kişiliğe ait verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkında 19/11/2018 tarihli ve 2018/131 sayılı Karar Özeti, <https://www.kvkk.gov.tr/Icerik/5423/2018-131> (s.y. 20 Mart 2022) ; Bu kararın detaylı olarak incelenmesine dair bkz. Murat Volkan Dülger, Kişisel Verileri Koruma Kurulunun 3 Nisan 2019 Tarihli Karar Özeti’ne İlişkin Değerlendirme (Evaluation of the Personal Data Protection Board's Decision Summary dated 3 April 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792303, (s.y. 20 Mart 2022)

⁴⁷⁴ KVKK, md. 3.

⁴⁷⁵ Murat Volkan DÜLGER, Kişiler Verilerin Korunması Hukuku, s. 188.

⁴⁷⁶ A.g.e., s. 194.

Keza bu tüzel kişinin kamu veya özel hukuk kişisi olması durumu fark yaratmamakta olup, her iki tüzel kişiliğin de sorumluluğuna gidilebileceği kabul edilmektedir. KVKK md. 18 hükmünde, “*Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde*” şeklinde belirtildiği üzere ya da Kanun’un Geçici 1. maddesinin 5. fıkrasında belirtildiği üzere “*Bu Kanunun yayımı tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında bu Kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenerek Başkanlığa bildirilir*” hükmünden yola çıkarak, kamu kurum ve kuruluşlarının veri sorumlusu olarak nitelendirilmiş olduklarını açıkça görebilmekteyiz⁴⁷⁷. KVKK’da kamu kurumları ile özel kuruluşlar açısından ayırım yapılmamıştır. Dolayısıyla, Kanun’ un belirlediği usul ve esaslar tüm kurum ve kuruluşlar için geçerli olmaktadır.

Kanun koyucunun yapmış olduğu tanımlama doğrultusunda veri sorumlusu ile veri işleyen taraflar arasındaki farkın daha iyi anlaşılabilmesi yakın tarihli bir örnek vermemiz mümkündür. Bilhassa uzaktan eğitim sürecinde sıklıkla yararlanılan iletişim teknolojisi sistemlerinden biri olan Zoom uygulaması sunucuları yurtdışında bulunan ve video konferans gerçekleştirilmesini sağlayan bir bulut iletişim hizmeti olarak tanımlanabilir. Bu uygulamanın pandemi dolayısıyla örgün eğitim yerine alternatif olarak gelen uzaktan eğitimde ülkemizdeki neredeyse tüm özel eğitim kurumları tarafından kullanılıyor olması, bu sisteme erişim için tutulan ad, soyad, mail adresi, kullanıcı IP, işlem ve cihaz verileri gibi kişisel verilerin ya da özel nitelikli veriler sayılan ses, görüntü ve video kayıtları gibi biyometrik verilerin güvenliği bakımından, sunucuların yurtdışında bulunduğu bir sisteme öğrenci ve velilerin kişisel verilerinin işlenmesini öngörmesi, verilerin yurtdışına aktarımı anlamına geldiğinden fazlaca tartışılmıştır⁴⁷⁸.

⁴⁷⁷ GVKT’de kamu kurumlarının da veri sorumlusu ve veri işleyen olabileceğinin açıkça düzenlenmiş olduğu görülmektedir. Buna karşılık KVKK’nın tanımlar maddesinde bu şekilde açık bir düzenleme bulunmasa bile, diğer bölümlerinde kamu kurum ve kuruluşlarının veri sorumlusu olduğuna dair düzenlemelerin bulunduğu görülmektedir.

⁴⁷⁸ Kişisel verilerin yurt dışına aktarımının yapılabilmesi açısından ise henüz yeterli korumanın bulunduğu ülkeler kurul tarafından belirlenmediğinden, özel okullar tarafından ilgili kişilerden ya da yasal temsilcilerinden verilerin aktarımı hususunda açık rıza alındığı görülmektedir. Belirtmek gerekir ki, bu yönde alınacak açık rızanın alınmasından önce ilgilinin bilgilendirilmesi kapsamında hizmet sağlayıcı bulut iletişim hizmeti sunan şirketin, kişisel verilerin korunmasına ilişkin olarak aldığı güvenlik tedbirleri ve idari ve teknik tedbirlerin neler olduğu konusunda detaylı bilgi verilmesi ve ayrıca bu tedbirlerin Kurul tarafından hazırlanan Özel Nitelikli Kişisel Verilerin İşlenmesinde “Veri Sorumlularınca Alınması Gereken Yeterli Önlemler Kararı” kapsamında belirtilen şartlara uygun olması daha yerinde olacaktır. Bkz. “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı.

İletişim hizmeti sunan bu şirketin kendi personeli ile ilgili olarak tutmuş olduğu verilere ilişkin veri sorumlusu sayıldığı, fakat iletişim hizmeti vermiş olduğu müşterilerinden gelen işler dolayısıyla tutmuş olduğu veriler açısından veri işleyen olarak görüldüğü söylenebilecektir. Bu farktan bir başka gerçekliği çıkarmamız mümkündür. O da bazı durumlarda, kişisel verilerin işlenmesi açısından veri sorumlusu olan bir firma, aynı zamanda veri işleyen de olabilmektedir.

Veri işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği, veri sorumlusunun organizasyonu dışında yer alan bir gerçek ya da tüzel kişi olarak tanımlanabilir⁴⁷⁹. Nitekim veri işleyenin yapmış olduğu işlem genelde çok daha spesifik ve teknik bilgiye ihtiyaç duyulan bir işleve sahiptir. Kişisel verilerin toplanma yöntemleri, işlenecek kişisel verilerin türleri, bu verilerin hangi amaçlarla kullanılacağı, verilerin paylaşılıp paylaşılmadığı ya da üçüncü kişilerle olan aktarım sınırları ve saklama koşulları açısından alınacak tüm kararlarda, kararı veren veri sorumlusu olmaktadır. Veri sorumlusunun veri işleyenin faaliyetlerine yön verdiği, verilerin işlenme amacını ve yöntemini belirleyen veri sorumlusu olduğu görülse de, yine de bazı durumlarda veri sorumlusuna bu karar verme yetkisini veri işleyene bırakabilmesi mümkün olarak görülmektedir. Fakat, bu karar verme yetkisinin devredilmesi sadece taraflar arasında geçerli olarak yapılmış bir kişisel veri işleme sözleşmesi yapılmış olduğu durumda söz konusu olabilir.

Tüm bu açıklamalar ışığında çalışmamızın önceki bölümünde ifade ettiğimiz kapalı devre kamera sistemleri üreten teknoloji şirketlerinin yukarıdaki açıklamalarımız dahilinde veri işleyen olarak nitelendirileceğini söyleyebiliriz. Burada yapılacak değerlendirmede kamera görüntülerinin toplanma yöntemleri, hangi verilerin kayıtlara yansıtacağı, özel nitelikli veri toplanıp toplanmayacağı, bu görüntülerin paylaşılıp paylaşılmadığı, üçüncü kişilerle olan aktarım sınırları ve saklama koşullarının belirtildiği veri işleme sözleşmeleri ile veri işleme gerçekleştirilip gerçekleştirilmediğine bakılarak ya da herhangi bir servis ve bakım hizmeti alınıp alınmadığına bağlı olarak, veri işleyen bir taraf bulunup bulunmadığı tespit edilebilir. Bununla birlikte bahsedilen bu teknoloji şirketine veri işleme yetkisi verilmemiş olup, bu taraflardan sadece ürün satın alınmış ve ilk kurulumların gerçekleştirilmesi söz konusu olmuşsa bu tarafların veri işleyen olmadıkları söylenebilir.

⁴⁷⁹ Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Kişisel Verileri Koruma Kurumu, KVKK Yayınları, No:1, Ankara, Aralık 2019, s. 56-57.

3. KVKK Kapsamında Gözetlenenlerin Kişisel Verilerinin Korunmasına İlişkin Hükümler

Kişisel verilerin işlenmesi sırasında, başta veri sorumlusu olmak üzere diğer aktörlerin verilerin işlenmesi sırasında dikkat etmek ve uymakla yükümlü oldukları kuralların da açıkça KVKK’ da düzenlenmiş olduğunu görebilmekteyiz. Bu kapsamda, Kanun’un ikinci bölümünde yer alan kişisel verilerin işlenmesine ilişkin esaslar çeşitli hükümlerle düzenlenmiştir. Buna göre kanun tarafından, kişisel verilerin işlenmesinde uyulması gereken ilkeler, kişisel verilerin işlenme şartları, özel nitelikli kişisel verilerin işlenme şartları, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi, kişisel verilerin aktarılması, kişisel verilerin yurt dışına aktarılması gibi konulara ilişkin açık düzenlemeler yapılmıştır. Burada bahsettiğimiz kişisel verilerin işlenmesine yön veren kurallar, kanunun belkemiği olarak değerlendirilerek, kişisel verilerin işlendiği bütün iş alanlarında, ticaretten sağlık sektörüne nüfus hizmetlerinden pazarlama alanına kadar veri işlemenin temel ilkelerini oluşturur⁴⁸⁰.

a. Gözetlenenlerin Kişisel Verilerinin İşlenmesinin Kanuni Dayanağı

Kişisel verilerin korunması çerçevesinde kamera ile gözetlenen bireylerin izlenmeleri ve verilerinin işlenebilmesi için ilk olarak bu işleme faaliyetinin kanuni bir dayanağının bulunması şarttır⁴⁸¹. KVKK’nın 4. maddesinin 1. fıkrası hükmüne göre, “*Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.*” Buradan yola çıkarak örneklendirmemiz gerekirse, bir başka kanuni düzenlemeye dayanmayan bireylere yönelik kamera gözetimi ya da işçinin işyerindeki gözetimi sırasında işlenen video görüntülerinin KVKK kapsamında işlenmesi gerektiğini söyleyebiliriz. Bu nedenle bu kanunun veri sorumlusuna yüklemiş olduğu yükümlülüklerin, bilhassa aydınlatma yükümlülüğünün yerine getirilip getirilmediğinin tespiti de önemlidir.

Kişisel verilerin işlenmesine yönelik kanuni bir dayanak bulunması zorunluluğuna aynı zamanda Anayasal açıdan bakılması gerekir. Bir bireyin kameralarla video kaydının yapılması ilgili bireyin kişisel verilerinin korunmasını isteme hakkına bir müdahale sayılmakta ve Anayasa’nın 20/3 hükmü kapsamında koruma bulmaktadır. Bu hususu geçtiğimiz bölümlerde ifade etmiş bulunuyoruz. Kısaca vurgulamak gerekirse, Anayasal bir hakkın sınırlanması

⁴⁸⁰ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 327.

⁴⁸¹ A.g.e., s. 385.

sadece yasayla olabileceğinden, bahsedilen veri işleme faaliyetinin kanuni dayanağı bulunması aynı zamanda bir Anayasal zorunluluk olarak karşımıza çıkmaktadır⁴⁸².

AİHM'nin kamera kayıtları vasıtasıyla işlenen veriler açısından vermiş olduğu bir kararında, kanunilik kavramını irdelemiş olduğu görülmektedir. AİHM tarafından ilgili kararda, Sırbistan Kişisel Verilerin Korunması Kanunu'nun kamu kurumlarına kamusal binalara ulaşım yolunda kameralarla gözetim yapabileceğine ilişkin yetki vermiş olduğu fakat bu hükmün geniş yorumlanarak üniversite amfilerinde kameralarla izleme faaliyeti yapılamayacağı belirtilmiştir⁴⁸³. Buna paralel olarak Alman Federal Anayasa Mahkemesi ise Bavyera Veri Koruma Kanunu'nun 16/1 ve 17/1 maddelerinde açıkça ve kesin ifadelerle video gözetim yapılacağı anlamına gelen bir düzenleme yer almadığı üzerine, yapılan veri işlemenin kanunilik ilkesine aykırı olduğunu belirtmiştir⁴⁸⁴.

Tez çalışmamızın ikinci bölümünde detaylı olarak belirttiğimiz üzere MOBESE gibi kent güvenliğini sağlamaya yönelik olarak faaliyetler gösteren sistemlere ilişkin bu gözetimi hukuki anlamda meşrulaştıran yasal dayanak eksikliğinden bahsetmemiz mümkündür. MOBESE ya da KGYS adı verilerin bu sistemlerin bireylerin kişisel verilerinin korunmasını isteme hakkına sınırlama getirdiği açıkça ortada olmakla birlikte, ne KVKK'da ne de başka bir kanun ile açıkça düzenlenmemiş olduğu görülmektedir. Aynı ayrı çeşitli kanunlardaki yetkiye dayanılarak yapılan suçun önlenmesi ve güvenliğin sağlanmasına yönelik bu kayıt tutma işlemi açısından, veri işleme sınırlarının ne olduğunun açıkça belirlendiği, kamera kayıtlarının arşivlenme ya da imha şartlarının düzenlendiği yasal düzenlemelerin yapılması gerekmektedir⁴⁸⁵.

b. Gözetlenenlerin Kişisel Verilerinin İşlenmesinde Temel İlkeler

Kanunilik kavramı sadece veri işlemeye izin vermekle kalmayan aynı zamanda verinin hangi amaçlarla toplanabileceği, hangi koşullar altında işlenebileceği, hangi veri türlerinin işlenebileceği, toplanan verilerin ne kadar süre ile saklanabileceği gibi yükümlülükleri de düzenleyen bir ilkedir. KVKK bu gibi yükümlülükleri kapsamına giren tüm veri işleme faaliyetleri için zorunlu olarak getirmiş olup; KVKK dışında sadece verinin işlenmesine izin

⁴⁸² Tefik Sönmez KÜÇÜK, s. 71.

⁴⁸³ Antovic ve Mirkovic, Karadağ'a karşı, b.n. 70838/13, k.t. 28 Kasım 2017.

⁴⁸⁴ Ayrıntılı bilgi için ayrıca bkz. Tefik Sönmez KÜÇÜK, s. 72.

⁴⁸⁵ Tefik Sönmez KÜÇÜK, s. 74.

veren başka bir yasa olsa bile KVKK'nın bu maddelerinin uygulanması mümkün olabilecektir. Bu açıdan KVKK'nın diğer yasa ile aynı anda kendi bünyesinde bu düzenlemelere yön vererek, ilgili yasada var olabilecek açıkları doldurmaya çalıştığını söyleyebiliriz. KVKK md. 4/2' de yer alan kişisel verilerin işlenmesinde uyulması zorunlu ilkeler tespit edilmiştir. Buna göre,

“ Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- a) Hukuka ve dürüstlük kurallarına uygun olma.*
- b) Doğru ve gerektiğinde güncel olma.*
- c) Belirli, açık ve meşru amaçlar için işlenme.*
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.*
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.”*

Kanun tarafından getirilen bu ilkeler kapsamında ilk olarak veri işlemenin hukuka uygun olması yani, kişisel verilerin işlenmesinde yasalara ve diğer hukuki düzenlemeler uygun olarak davranma yükümlülüğü ifade edilmiştir. Dürüstlük kuralı ise her ne kadar Medeni Kanun'a göre daha geniş yorumlanabilirse de kişisel verilerin korunması açısından “veri sorumlusunun, veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate alması gerekliliği” olarak açıklanabilir⁴⁸⁶. Dürüstlük kuralının içeriğinin açık ve sınırlı bir biçimde sayılması mümkün olmadığından, kuralın içeriği her bir kişisel veri işleme faaliyetinde objektif olarak bir kimseden beklenecek davranış kriteri olarak görülen objektif özen yükümlülüğüne göre belirlenmelidir⁴⁸⁷. Bu bakımdan içeriğin somutlaştırılması için farklı durumlara ilişkin örnekler vermemiz yerinde olacaktır. Kişisel veri işleme faaliyetinin dürüstlük kuralına uygunluğundan bahsedilmek için veri işleme faaliyetinin açık, belirli ve şeffaf olması ya da dayanak yapılan hukuk kuralının amacı esas alınarak en az miktarda veri toplanması gerekecektir. Bunun tersine hukuka uygun olarak elde edilen ve işlenen kişisel verileri işleme amacı sona ermesine rağmen kişisel verilerin silme, yok etme veya anonimleştirme faaliyetlerinden herhangi birine konu edilmemesi de dürüstlük kuralına aykırılık teşkil etmektedir⁴⁸⁸.

⁴⁸⁶ Elif KÜZECİ, s. 201.

⁴⁸⁷ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 265.

⁴⁸⁸ A.g.e., s. 266-267.

Bu yönde dikkat edilmesi gereken bir diğer dürüstlük kuralının da yapılan kamera gözetiminin veri sahibi ilgililere bildirilmesi olduğu söylenebilir⁴⁸⁹. Nitekim Almanya Federal Verilerin Korunması Kanunu'na göre de “video kamera aracılığı ile izlemenin şartlarının ve sorumlu organın uygun bir tedbir aracılığı ile açık bir şekilde duyurulması gereklidir.⁴⁹⁰” Bu kanun hükmü ile KVKK'nın 10. maddesinde düzenlenen aydınlatma yükümlülüğünün benzer nitelikte olduğu söylenebilir. Kamera gözetimi vasıtasıyla kişisel veri elde edilmesi durumunda, ilgili madde kapsamında kameranın altında duran bir duvara ya da görülebilir şekilde yakınına asılacak bir bilgi panosu ile aydınlatma yükümlülüğünün yerine getirilmesi mümkündür⁴⁹¹. Nitekim örnek göstermek açısından, Fransa ve Belçika' da yer alan uygulamalara göre kamera aracılığıyla yapılacak kayıtlardan önce ilgilileri bilgilendirmek bir yükümlülük olarak karşımıza çıkmaktadır⁴⁹².

Kamera görüntüleri vasıtasıyla veri işleme faaliyeti gerçekleştiren sistemlerin varlığından veri sahiplerinin haberdar edilmesi, aynı zamanda verilere erişim hakkı kapsamında da önem teşkil etmektedir. İlgili kişi ilk olarak verilerinin işlendiğini öğrenmeli, ardından bu hakkını kullanmak için diğer veri koruma aktörlerine başvurmalıdır. Nitekim, burada kastedilen kamera gözetiminin gerçekleştirilmesine ilişkin ayrıntılı teknik bilginin, kameraların kaç tane olup nerelerde bulunduğu ya da kaç adet olduğunun doğrudan paylaşılması değil, gözetim alanındaki bireyin herhangi bir çaba göstermeksizin kolaylıkla, o alanda video kamera vasıtasıyla hal ve hareketlerinin kayıt altına alındığını bilmesi yeterli olacaktır⁴⁹³.

Yapılan gözetimin detaylı olarak aydınlatma metinleri dahilinde değil sadece kamera resmini içeren bir tabela ile yapılması da mümkün görülmektedir. Ancak burada mutlak suretle var olması gereken şey, veri işleme faaliyetini kimin yaptığı yani kameraların görüntü aktardıkları kontrol odalarında kimlerin bulunduğu⁴⁹⁴. Bu durum da kişisel verilere erişim hakkı kapsamında değerlendirilebilir. Ayrıca kamera gözetiminin yapılacağı alanın sınırlarının belirlenmesi ve bu sınırlara ilişkin bilginin, henüz kayıt altına girmeden önce ilgili kişiye bildirilmesi büyük öneme sahiptir. Çünkü bu durumda ilgili kişiye yapılacak veri işleme

⁴⁸⁹ A.g.e., s. 267.

⁴⁹⁰ Almanya Federal Verilerin Korunması Kanunu md. 6b/2'den naklen Tevfik Sönmez KÜÇÜK, s. 77.

⁴⁹¹ Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, KVKK Yönetim Dairesi Başkanlığı, Nisan 2019, Ankara, s. 14.

⁴⁹² Güçlü AKYÜREK, Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı, Seçkin, Ankara 2014, s. 275.

⁴⁹³ Oğuz ŞİMŞEK, s. 172.

⁴⁹⁴ Tevfik Sönmez KÜÇÜK, s. 78.

faaliyeti kapsamında aydınlatma yapılmakta ve o alana yine de girip girmeme yani kendisine ait kişisel verinin işlenmesine izin rıza verme konusunda takdir ilgili kişiye bırakılmaktadır.

Kişisel veriler belirli, açık ve meşru amaçlara yönelik olarak toplanır. Bu amaçlara uygun olmayan başka şekillerde işlenmesi mümkün değildir. Bu doğrultuda ilk olarak, veri işleme amacının belirli, açık ve meşru olması gerekir. Sonrasında ise sonraki işleme amacının, baştaki toplama amacına uygun olması gerekmektedir⁴⁹⁵. Kameralar vasıtasıyla yapılan gözetimin amacı, henüz veri işleme faaliyeti başlamadan önce belirli olmalı ve elde edilen veriler amaca uygun olarak kullanılmalıdır. Bu verilerin, yani kamera görüntülerinin toplanma amacı dışında kullanılması söz konusu olmamalıdır.⁴⁹⁶

KVKK md. 4 f. 2. uyarınca kişisel veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek zorundadır. Bu durum aynı zamanda amaca uygunluk ilkesinin de bir yansıması olarak karşımıza çıkar. Aslında bu zorunluluk tam olarak verilerin azaltılması (minimizasyonu) ilkesinin zamansal bir görünüm biçimi olarak ifade edilebilir⁴⁹⁷. Çünkü kamera kayıtlarının kullanılması açısından öngörülen amaç sona erdikten sonra bu verilerin imha edilmesi gerekmektedir. Buna benzer olarak sadece öngörülen amacın sona ermesiyle değil, aynı zamanda kanunda öngörülen işleme süresinin sona ermesiyle birlikte söz konusu verinin imhası gerekecektir. Örneğin Belçika Veri Koruma Kanunu'nda önleyici amaçlı video kayıtlarının en fazla bir ay süre ile muhafaza edilebileceği düzenlenmiştir⁴⁹⁸.

Türk hukukunda benzer nitelikte düzenleme açısından bakmamız gereken yer KVKK'nın 7. maddesinin 1. fıkrası ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 11. Maddesi olmaktadır. Her iki hukuki düzenleme de paralel olarak, kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalmasından itibaren silineceği, yok edileceği veya anonim hale getirileceğinden bahsedilmektedir. Yönetmelik bu yönde bir adım ileriye giderek, kişisel verilerin işlenmesinde öngörülen amaca

⁴⁹⁵ Nafiye YÜCEDAĞ, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, Kişisel Verileri Koruma Dergisi, C. 1, S.1, Y. 2019, s. 52.

⁴⁹⁶ Bu düzenlemeye getirilmiş nadir istisnalardan biri Almanya Federal Verilerin Korunması Kanunu'nda bulunmaktadır. Kanun'un § 6b/3 maddesine göre, “ kişisel veriler, kamu ya da devlet güvenliğine yönelik bir tehlikenin engellenmesi veya bir suçun soruşturulması için gerekli olması halinde kayıt altına alındıkları amaç dışında da kullanılabilir.” Bkz. Tevfik Sönmez KÜÇÜK, s. 79.

⁴⁹⁷ Nafiye YÜCEDAĞ, s. 60.

⁴⁹⁸ Güçlü AKYÜREK, s. 275.

ulaşıldıktan sonra en geç altı aylık periyodlar çerçevesinde imha politikasının işletilmesi gerektiğini düzenlemiştir. Nitekim Almanya Federal Verilerin Korunması Kanunu’nda yer alan düzenlemeye göre, “ amaca ulaşıldıktan sonra daha fazla gerekli değilse ya da verilerin kayıt altında tutulması ilgilinin menfaatine aykırıysa, görüntülerin derhal silinmesi gerektiği düzenlenmiştir.⁴⁹⁹”

Kişisel verilerin korunması özelinde kamera kaydı vasıtasıyla toplanan verilerin işlenmesi sırasında uyulması gereken bir diğer ilke “ölçülü olma” yani, ABVKY’de yer alan ifadeyle işlenen verilerin, “*toplanma ve/veya bunu izleyen işleme amaçları açısından yeterli ve onlarla ilgili olacak ve aşırı olmayacak*” olmasıdır⁵⁰⁰. Ölçülülük açısından, eğer kişisel veri işlenmeden amaçlanan hedefe ulaşmak mümkün oluyorsa, bu verinin hiç işlenmemesi gerektiği söylenebilecektir⁵⁰¹. O halde bu açıdan vurgulanmak istenenin veri işleme faaliyetinin, henüz veri işlenmeden önce belirli olan amacın gerçekleşmesine ne kadar hizmet ettiği önemlidir. Buna ilişkin olarak Kişisel Verilerin Korunması Kurumu’nun vermiş olduğu bir kararda, bir kamu kurumunun halk girişine ses kaydı yapan kamera yerleştirilmesi değerlendirilmiş olup, ses kaydı yapan kameralarla kişisel verilerin işlenmesi farklı açılardan değerlendirilerek hukuka aykırı bulunmuştur. Ölçülülük açısından ise Kişisel Verileri Koruma Kurulu’nun “*söz konusu kayıt ile beklenen faydanın ses kaydı olmaksızın görüntü kaydı ile elde edilebileceği hallerde ses kaydının da yapılması, gerçekleştirilecek kişisel veri işleme faaliyeti ile ulaşılmak istenen amaç arasındaki dengenin bozulmasına yol açacağından ölçülülük ilkesine aykırılık teşkil edecektir.*” şeklinde bir değerlendirmede bulunduğu görülmektedir⁵⁰².

⁴⁹⁹ “Federal Verilerin Korunması Kanunu md. 6b/5’te zikredilen “derhâl kelimesinin, 48 saat içerisinde olarak anlaşılması gerekir.” Bkz. Tefik Sönmez KÜÇÜK, s. 80; Gerçekten de AİHM tarafından Perry Birleşik Krallık’a karşı kararında belirtildiği üzere, güvenlik kameralarının kullanılması ancak meşru ve öngörülebilir amaca yönelik olarak mümkündür. Olayda ise gözaltı sırasında “kimlik tespiti amacıyla” polis merkezine getirilen başvurunun bilgisi olmaksızın kapalı devre güvenlik kameralarından alınan görüntülerini başkalarının da aralarında bulunduğu olay görüntülerine montajlayan polis tarafından, olayın faillerinin belirlenmesi amacıyla kullanılması ve aynı zamanda aynı görüntülerin mahkemede duruşma sırasında da izletilmesi söz konusudur. Mahkeme tarafından değerlendirilen husus ise bu kapsamda başvurunun kişisel verilerinin kullanılması ya da işlenmesi sebebiyle AİHS md. 8’e göre, özel yaşamının korunması hakkının ihlal edilip edilmediğinin tespit edilmesidir⁴⁹⁹. Polis tarafından gerçekleştirilen faaliyet kanun tarafından öngörülen prosedürlerin ötesinde, anormal ve beklenmeyecek bir uygulama olduğundan, video görüntülerinin normal kaydedilmesi amaçlarına uygun değildir. Keza, kimlik tespiti açısından kullanılacak bir kamera kaydının yapılmasından önce polis tarafından ilgilinin bilgilendirilmesi gereklidir. Kayıtların kalıcı olarak tutulması ve montajlanarak sonradan kullanılması kişisel verilerin hukuka aykırı olarak kullanılması anlamına gelmektedir. Tüm bu nedenler dolayısıyla mahkeme tarafından başvurunun özel yaşamının ihlal edildiğine karar verilmiştir. Perry, Birleşik Krallık’a karşı, b.n. 63737/00, k.t. 17 Ekim 2003.

⁵⁰⁰ ABVKY, md. 6/e.

⁵⁰¹ Elif KÜZECİ, s.208.

⁵⁰² İlgili kararda ayrıca, “sesli kamera kaydının hukuka uygun bir kişisel veri işleme faaliyeti olarak değerlendirilebilmesi için Anayasada belirtilen temel hak ve özgürlüklerin sınırlandırılmasında gözetilmesi

Bu kararda da ifade edildiği üzere amacı gerçekleştirmeye elverişli ve yeterli şekilde veri işleniyor olması önemlidir. Örneğin; suçun önlenmesi ve güvenliğin sağlanması amacıyla yönelik olarak kurulan kapalı devre kamera sistemlerinden daha az özel yaşamın gizliliği hakkına müdahale teşkil edebilecek nitelikte bir uygulama varsa, korunan yerdeki ışıkların ve güvenlik ekipmanlarının artırılması gibi, öncelikle bu uygulamaların yapılması, bunlar yeterli değilse kameraların gözetime eşlik etmesi gereklidir⁵⁰³. Bu yaklaşımı veri ekonomisine uygun bulmak mümkündür. Henüz verinin toplanması sırasında yapılan bu minimizasyonu, çok sayıda verinin toplanıp kullanılmayanların imha edilmesinden çok daha yerinde olacaktır.

Bu bakımdan değerlendirilmesi gereken bir husus da kameralar ile izlenen nesnelerin tanımlanmasının kolaylaştırılmasına yönelik olarak sinir ağlarının (neural networks) kullanılmasıdır⁵⁰⁴. İnsanların video gözetim amacıyla ekranların başında saatlerce trafik kameralarını ya da şehir gözetim kameralarını takip etmeleri hem zordur hem de kaynakları ehemmiyetsizce kullanmak anlamına gelebilecektir. Bununla birlikte, insan etki ve tepkilerinin yavaş olması nedeniyle günümüz teknolojilerinin kullanılması insan gücüne tercih ediliyor olabilmektedir. Teknolojinin gelişmesi ile birlikte video gözetim sistemlerinde nesnelerin tanımlanmasını kolaylaştıran sinir ağlarının kullanılmasıyla, gözetim sistemlerinde yaratılan algoritmalar dahilinde kameralar ile tespit edilen bireylerin hareketleri tamamen bilgisayarlar aracılığıyla otomatik olarak izlenebilmektedir.

Sonuç olarak video görüntüleri bireyler tarafından izlenmeksizin bir kimsenin işlediği yasak bir fiili tespit etmek mümkün olacaktır. Örneğin; yayaların trafikteki hareketleri bu bakımdan hareket tahmini senaryoları dahilinde bu sisteme yüklenen veri gruplarından bir

gereken ilkelere uygun olması gerekmektedir. Bu kapsamda söz konusu kayıt ile beklenen faydanın ses kaydı olmaksızın görüntü kaydı ile elde edilebileceği hallerde ses kaydının da yapılması, gerçekleştirilecek kişisel veri işleme faaliyeti ile ulaşılmak istenen amaç arasındaki dengenin bozulmasına yol açacağından ölçülülük ilkesine aykırılık teşkil edecektir. Bu anlamda, gözetim sistemlerinde görüntü kaydı ile birlikte ses kayıt sisteminin de kullanılmasının sadece görüntü kaydına göre çok daha müdahaleci olacağı açıktır. Diğer taraftan, kameralar vasıtasıyla görüntü ile birlikte ses kaydı yapılması, bireylerde her açıdan gözetim altında tutuldukları endişesi yaratabilecek olup, kişilerin kamusal alanda bile özel bir kısım diyaloglarının ya da yaşantı kesitlerinin bulunabileceği de dikkate alındığında bu yönde bir uygulamanın hakkın özüne zarar vereceği değerlendirilmektedir.” yönünde tespitlerde bulunulmuştur. Bkz. “Ses özelliği bulunan güvenlik kamerası kullanılması” ile ilgili Kişisel Verileri Koruma Kurulu’nun 12/03/2020 tarihli ve 2020/212 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6892/2020-212>, (s.y. 30 Mart 2022)

⁵⁰³ Tevfik Sönmez KÜÇÜK, s. 76.

⁵⁰⁴ Benny PLATTE, Rico THOMANEK, Tony ROLLETSCHE, Christian ROSCHKE, Marc RITTER, s. 21.

tanıdır. Bu sistemde nesnelerin tespiti hususunda bir takım üçüncü taraf eklentilerin kullanıldığı belirtilmiş olup, bu sistemlerin farklı eklentilerle zenginleşmesi de mümkündür⁵⁰⁵. Veri koruma bakımından ise bu tarz bir uygulamanın ölçülü olup olmadığının sorgulanması gerekecektir. Bu tarz bir sistemin uygulanması insan faktörü olmaksızın her CCTV kamerasının izlendiği anlamına gelebilecektir. Bir çok teknoloji-güvenlik firması yeni kamera sistemlerinde bu ve benzeri yapay zeka destekli insan tespit edebilen CCTV kameralarını piyasaya sürmekte olup, bu kameralar hayvanları ya da cansız nesneleri kesintisiz bir şekilde algılayabilmekte sürekli olarak veri işleme faaliyeti gerçekleştirmektedir. Veri analitiği ile birleşen bu tarz gözetim faaliyetleri insan hareket algılama dışında sınır geçişlerinin tespiti/algılanması, yüz tanıma sistemleri, nesne ve kişi sayma gibi diğer amaçlar için de kullanılmaktadır.

Güvenliğin sağlanması için kapalı devre kamera gözetimi yapılan bir mağazada kurulmuş olan kameraların sadece mağazanın içini değil, aynı zamanda dışını da gözetlemesi durumunda aşırı veri kullanımı olduğu söylenebilecektir. Bu durum ölçülülüğe aykırıdır⁵⁰⁶. Buna ilişkin bir davada Alman Mahkemeleri tarafından, market önündeki alanın en fazla bir metre çapına kadar izlenebileceği, aksine uygulamanın sokaktan geçenlere gözetlenmedikleri bir alan bırakılmayarak, insanın kendini güvensiz hissetmesine ve kişiliklerini geliştirmeleri açısından soruna yol açabilecektir. Kameralar ile sokakların tamamının gözetlenmesi ihtimali, kayıt altına alınan kişilere kişiliklerini geliştirebilecekleri bir yaşam alanı bırakmaz.⁵⁰⁷

Kişisel verilerin belirlenen amaçla ölçülü olması gerekliliğini açıklayan Kişisel Verileri Koruma Kurulu bu konu özelinde bir spor salonuna girişlerde güvenlik gerekçesiyle biyometrik parmak izi toplanmasının kişisel verilerin işlenmesinde ölçülülük ilkesi doğrultusunda ilgili kişilerden minimum düzeyde veri toplanması ilkesi ile uyumlu olmadığına karar vermiştir⁵⁰⁸. Dolayısıyla parmak izi ya da yüz görüntüsü gibi biyometrik verilerin işlendiği durumlarda her zaman bir ölçülülük değerlendirilmesi yapılması zorunlu görülmelidir.

⁵⁰⁵ A.g.m., s. 24.

⁵⁰⁶ Elif KÜZECİ, s. 209.

⁵⁰⁷ Marie TINNEFELD THERES, Benedikt BUCHNER, Thomas PETRI, Einführung in das Datenschutzrecht, Odenbourg Verlag, 5. Auflage, München, 2012, s. 245'ten naklen Tevfik Sönmez KÜÇÜK, s. 76.

⁵⁰⁸ "Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/167 Sayılı Karar Özeti", <https://www.kvkk.gov.tr/Icerik/6738/2020-167> (s.y. 21 Mart 2022)

Kapalı devre kamera sistemlerini düşündüğümüzde ise endüstri, finans ya da yönetim faaliyetlerinin bir çok alanında yüz tanıma sistemleri ve biyometrik yetkilendirme teknikleriyle donatılmış sürekli kayıt yapan CCTV sistemlerinin kullanıldığını görmekteyiz. Bu teknikler ise bireylere ait “biyometrik simge”lerden (yüz, avuç içi ya da iris) beslenmektedir. Bu biyometrik simgeleri içeren veri setlerinin yetkisiz üçüncü kişiler tarafından ele geçilmiş olması durumunda ilgili veri sahibi kişilerin yüzleri dijital ortamlarda yeniden canlandırılabilir⁵⁰⁹. Bu canlandırma sonucu oluşan yüz bilgisinin, günümüz bankacılık işlemlerinin gerçekleştirildiği cihazlarda kullanılmasının büyük ölçekli maddi ve manevi zararlara sebebiyet verebileceği ortadadır. Ayrıca biyometrik veriye yetkisiz erişim hukuki anlamda bir takım gizlilik ve güvenlik sorunları da doğuracaktır. Bunun temelinde biyometrik verinin niteliği gereği bir kere kaybedilmesi durumunda sonsuza kadar tehlikeye girmesi, ters çevrilemeyeceği ya da geri alınamayacağı gibi sebepler yatmaktadır⁵¹⁰. Eğer burada bahsedilen canlandırma işlemi belirli bir algoritma dahilinde yapay zekaya yaptırılıyorsa, verilerin güvenliğine dair endişelerin çok daha yüksek olması gerekecektir.

Söz konusu biyometrik veriler olduğunda ölçülülük ilkesinin karşılanması dışında ayrıca bir takım veri koruma tedbirlerinin alınması gerekecektir. Normalde yüz tanıma verisinin ilk işlenmesi sırasında bireylerin korunmasına yönelik olarak yüzün özelliklerini (*feature vector*) şifreleyerek muhafaza altına almak gibi geleneksel bir güvenlik yöntemi işletilmekte ancak yukarıdaki gerekçeye bağlı olarak bu koruma yetmediğinden, kötü amaçlı saldırılara karşı getirilmeye çalışan yeni güvenlik modelinde yüz özelliklerinin şifrelenerek alınması yerine yüzün harekete bağlı özelliklerinin (*movement vectors*) izlenmesi önerilmektedir. Bu hareket vektörleri yüzün canlandırılması açısından çok daha az bilgiyi barındırdığı için yetkisiz erişim durumlarında daha güvenli görülmektedir. Bu yöntem aynı zamanda bir iptal edilebilir biyometri tekniği olarak düşünülmektedir⁵¹¹. Yani bu protokole alınan biyometrik veri henüz bir veri tabanında depolanmadan kasıtlı ve sistematik olarak bozulmaktadır⁵¹². KVKK açısından ise Kurum tarafından “Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber” yayınlanmış olup, bu rehberin veri güvenliğine ilişkin kısmında

⁵⁰⁹ Marcin PLATA, Piotr SYGA, Marek KLONOWSKI, How to Save Your Face: a Facial Recognition Method Robust Against Image Reconstruction, IEEE 10th International Conference on Biometrics Theory, Applications and Systems, 2019, s.1.

⁵¹⁰ Pratima SHARMA, Gurjit Singh WALIA, Rajesh ROHILLA, "Recent Advancement in Cancelable Biometric for User Recognition: A Brief Survey," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, s.137.

⁵¹¹ Marcin PLATA, Piotr SYGA, Marek KLONOWSKI, s. 8.

⁵¹² Pratima SHARMA, Gurjit Singh WALIA, Rajesh ROHILLA, s. 138.

“biyometrik verilerin bulut sistemlerinde ancak kriptografik yöntemler kullanılarak muhafaza edilmesi gerektiği, türetilmiş biyometrik verilerin, orijinal biyometrik özelliğın yeniden elde edilmesine izin vermeyecek biçimde saklanması gerektiği ve yine biyometrik verilerin güncel teknolojiye uygun olarak, yeterliğı güvenliğı sağlayacak kriptografik yöntemlerle şifrelenmesi gerektiğı” belirtilmiştir⁵¹³.

Veri güvenliğı tedbirlerinin alınmasının yanı sıra veri korumanın temel ilkelerinden bir diğeri olan kişisel verilerin, ilgili mevzuatta öngörölen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek zorunda olunması nedeniyle kişisel verilerin işlendikleri amacın ortadan kalkması halinde artık elde tutulmaması gerekeceğinin söylenmesi mümkündür. Bir video kaydı ne kadar süre ile kayıt olarak kalmakta, hangi süreler dahilinde silinmekte, otomatik silme ya da manuel silme işlemlerinden hangisi yapılmakta ya da kayıtların aktarıldığı ortamlar bakımından bir çok soru gündeme gelmektedir.

Eğer daha önce belirttiğimiz Alışveriş Merkezleri Hakkında Yönetmelik’te belirtildiğı üzere mevzuatta öngörölen bir saklama süresi öngörölmüşse bu saklama süresine uyularak bir silme protokolü oluşturulmalı, böyle bir düzenleme bulunmuyor ise kişisel verilerin kullanım amaçları iyi değerlendirilerek amacın gerçekleşmesi üzerine verilerin ortadan kaldırılması gerekecektir⁵¹⁴. Belirtmemiz lazımdır ki meşru bir amaç dahilinde bile olsa kişisel verilerin elde tutuluyor olması her zaman bir risk faktörü olarak görölmelidir⁵¹⁵. Bu risk veri sorumlusu açısından kişisel verilerin güvenliğinin sağlanması zorunluğı olarak kendini gösterir. Verilerin elde tutulduğu süreçte herhangi bir veri güvenliğı zaafiyeti söz konusu olursa veri sorumlusu bundan sorumlu olmaktadır.

Nitekim KVKK’nın 12. maddesinde belirtildiğı üzere veri sorumluları uygun güvenlik düzenini temin etmeye yönelik her türlü teknik ve idari tedbiri almakla yükümlüdürler. Yani kapalı devre kameraların gözetim faaliyetlerinde kullanılması sırasında yukarıda bahsedilen tüm teknik tedbirin alınması ve işlem devam ettiğı sürece korunması gereklidir. Buna göre

⁵¹³ “Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”, <https://www.kvkk.gov.tr/Icerik/7047/Biyometrik-Verilerin-Islenmesinde-Dikkat-Edilmesi-Gereken-HususlaraIliskinRehber> (s.y. 05/11/2021)

⁵¹⁴ Alışveriş Merkezleri Hakkında Yönetmelik md. 19 f. 2 ‘ye göre,“Alışveriş merkezinde bebek bakım odası ve tuvalet gibi niteliğı itibarıyla kayıt altına alınması uygun olmayan alanlar dışındaki ortak kullanım alanları kamera ile kayıt altına alınır ve bu kayıtlar en az otuz gün süreyle saklanır. Bu kayıtların saklanmasıdan alışveriş merkezi yönetimi sorumludur.”

⁵¹⁵ Murat Volkan, DÜLGER, Kişisel Verilerin Korunması, s. 300.

kamera sistemlerinin kayıt cihazlarının dışarıdan gelen bilişsel ya da fiziksel müdahalelere karşı koruma altına alınmalı, IP kameralar üzerinden aktarılan veriler şifrelenmeli ya da gözetimin gerçekleştiği sırada monitörlere yetkisiz erişimlerin engellenmesi gibi tedbirleri sıralamak mümkündür.

Verilerin korunması açısından her türlü önlem alınsa bile insan faktörü gibi kesinlik vermeyen etkenler denklem içerisinde girdiğinde ihlal yaşanma riski her zaman söz konusudur. Daha önce bahsettiğimiz üzere yapay zekanın bu bakımdan faydalı olabileceğini düşündüğümüzü belirtmiştik. Ancak amaç maksimum güvenlik düzeyini tesis etmek ise bunu sadece kişisel verilerin elde tutulmaması ve işlenmemesi ile başarmak mümkün olacaktır⁵¹⁶.

Eğer güvenlik, adaletin sağlanması, denetim ya da gözetim amacıyla meşru bir kamera gözetimi gerçekleştirilecekse bu faaliyetin hiç veri işlenmeksizin yapılması mümkün olmayacak olduğundan, yapılması gereken verilerin işlenmek üzere toplandıktan sonra periyodik aralıklarla silinmesi, yok edilmesi veya anonim hale getirilmesidir. Kanuna göre⁵¹⁷, *“işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler re’sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir...”* Tam olarak burada akıllara şu soru gelecektir. Bir özel teşebbüs ya da kamu kurumu tarafından yapılan gözetimde kameraların 30 günlük kayıt tutma süreleri öngörülmüş olabilir. Ancak soruşturma makamları tarafından istenen bir video kaydı ya da bu video kaydından türetilen görüntünün kopyası çıkarıldıktan sonra arşivleniyorsa durum ne olacaktır? Belirtmemiz gerekir ki, kişisel verilerin korunması hukuku açısından verilerin yeni bir amaç doğrultusunda işlendiği aşıkardır. Artık gözetimi yapan otorite yani veri sorumlusunun dışında, veriyi yeni bir amaç ve kendi menfaatlerine yönelik olarak yine kendi hakimiyet alanında işlemeye başlayan bir aktör bulunmaktadır. Kolluk makamının bu faaliyeti eğer Kanun’un 28. maddesindeki istisnaya giriyorsa, veri işlemeyi gerçekleştirmesi söz konusu olabilir. Bunun aksine, bu tarz bir arşivleme faaliyeti tamamen gözetim yapan kurum tarafından yapılıyorsa kesinlikle Kanun’un uygulama alanı içinde yer alacak olup, arşivleme işlemi verilerin işlenmesinde hem ölçülülük ilkesine aykırı olacak hem de verilerin silinmesine ve imhasına dair yükümlülüklerin yerine getirilmediği söylenebilecektir.

⁵¹⁶ Murat Volkan, DÜLGER, Kişisel Verilerin Korunması, s. 538.

⁵¹⁷ KVKK, md. 7.

c. Gözetlenenlerin Kişisel Verilerinin İşlenmesi Koşulları

Kişisel verilerin ilgililerinden açık rıza alınarak işlenmesi kural olmak üzere, bu açık rızanın alınmasına gerek olmayan bir takım durumlar açıkça kanunda düzenlenmiştir. KVKK md. 5 f. 1’ de yer alan düzenlemeye göre, “*Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez*” denilmekle, kişisel verilerin işlenmesindeki genel kuralın “açık rıza”ya dayalı veri işleme olduğu vurgulanmıştır. Bu hükmü takip eden 2. fıkra hükmü ise belirli bazı durumları düzenleyerek, bu durumlar söz konusu olduğunda veri sahibinin açık rızasını almaya gerek bulunmadan kişisel veri işlenebileceğinden bahsetmektedir. Buna göre aşağıdaki kanun tarafından belirtilen hallerde gözetlenenlerin açık rızası alınmadan kamera görüntüleri işlenebilecek, izlenebilecek ve/veya kayıt altına alınabilecektir:

- a) “*Kanunlarda açıkça öngörülme.*” :
- b) “*Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.*”
- c) “*Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.*”
- d) “*Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.*”
- e) “*İlgili kişinin kendisi tarafından alenileştirilmiş olması.*”
- f) “*Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.*”
- g) “*İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.*”

Açık rızanın KVKK’da, “*belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak tanımlandığını görmekteyiz. Kavramı meydana getiren üç unsur bulunmaktadır: 1) belirli bir konuya ilişkin olma, 2) rızanın bilgilendirmeye dayanması, 3) özgür iradeyle açıklanma.

Açık rızanın belirli bir konuya ilişkin olmasından kasıt, açık rıza beyanının hangi konuya ilişkin verildiği ve o konu ile sınırlı olarak kalması gerektiğidir. Bu nedenle “*kişisel verilerimin işlenmesini kabul ediyorum*” şeklindeki ucu açık ve belirsiz bir rıza beyanının kanuna uygun bir açık rızayı karşılamayacağı açıktır. Rızanın bilgilendirmeye dayanması, bireylere,

verinin henüz işlenmesinden önce, veri işlemeye ilişkin bütün konuları kapsayan açık ve anlaşılır bir bilgilendirme yapılması, aynı zamanda bilgilendirmenin sadece konunun ne olduğu hususunda değil, bireyin rızasının sonuçları üzerinde de tam bir bilgilendirmeye sahip olması anlamını taşımaktadır⁵¹⁸.

Açık rızanın diğer unsurunu ise verilecek rızanın özgür iradeyle açıklanması teşkil eder. Özellikle taraflar arasında hiyerarşik bir ilişkinin bulunduğu alanlarda, rıza beyanını veren tarafın ne kadar özgür konumda bulunduğu dolayısıyla da verisi üzerindeki denetimini ne ölçüde sağlayabildiği önem arz eder. İşçi-işveren ilişkisinde ya da bir hizmeti almak isteyen ile hizmet sunan taraflar (özellikle tekel konumunda bulunan ya da bir haktan ya da hizmetten yararlandırılma için belirli bir şartı öngören hizmet sunanlar açısından) açık rızanın verilmesi sırasında, veri sahibinin ne kadar özgür davranabildiği tartışma konusu olabilecektir. Kişisel Verileri Koruma Kurulu tarafından verilen kararda⁵¹⁹, hizmetin açık rıza şartına bağlanması;

“ Veri sorumlusu tarafından Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında sözleşmenin taraflarına ait kişisel veri işlenmesi durumunda ayrıca açık rıza alması ve de açık rızayı üyeliğin ve hizmetin dolayısıyla sözleşmenin bir koşulu olarak dayatmasının;

- Diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği,

- Ayrıca hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı,

dikkate alındığında, bu durumun Kanunun 4 üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ve işleme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil etmesi nedeniyle”

yerinde görülmemiştir. Zira belirli bir hizmetin sunulup sunulmaması açık rıza şartına bağlanmışsa burada dürüstlük kuralına aykırı bir veri işleme faaliyetinin söz konusu olduğu da söylenebilir. Ayrıca kararda değinilen bir başka husus da sözleşmenin ifası için zorunlu olan

⁵¹⁸ Açık Rıza, Kişisel Verileri Koruma Kurumu, <https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf>, s. 4-5, (s.y. 30 Kasım 2021)

⁵¹⁹ Kişisel Verileri Koruma Kurulu, Karar Özetleri, Hizmetin Açık Rıza Şartına Bağlanması, (<https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi>, (s.y. 26 Ocak 2021)

bir konuda, bu durum zaten açık rıza alınmasını gerektiren bir istisna kapsamında yer almakta iken, açık rıza alınmış olması ve bunu sözleşmenin bir ön şartı olarak öngörmesi, KVKK kapsamında hukuka aykırı bulunmuştur. Açık rıza dışında bir hukuki dayanağı bulunan veri işleminin açık rızaya dayandırılmaya çalışmasının yapılan veri işleme faaliyetini dürüstlük kuralına aykırı hale getirmektedir.

İlgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer veri işleme şartlarından birine dayanarak, veri işleme faaliyetine devam etmesi de veri işleme faaliyetini dürüstlük kuralına aykırı hale getirmektedir. Bu durum, ilgili kişide yaratılan, “bilgilerinin geleceğini belirleme hakkı”nın yansımaları olan rıza kurumuna dayanarak işleminin sürdüğünü, rızanın geri alınması durumunda işleminin duracağı algısına karşılık, başka bir sebebe dayanarak veri işlemeye devam edilmesinin yine dürüstlük kuralına aykırı olacağı belirtilmiştir⁵²⁰.

Bu nedenle verilen açık rızanın neden ve sonuçlarının titizlikle değerlendirilmesi ve her koşulda veri işleminin genel ilkelerden amaca uygunluk ve ölçülülük hususları dikkate alınarak yapılması gerekmektedir. Örneğin; üniversite içerisinde geniş kitlelerin bir arada bulunduğu toplanma alanlarında, avlularda, konferans salonlarında, kütüphanelerde veya sadece geçiş alanları olarak nitelendireceğimiz koridorlarda öğrencilerin ya da öğretim görevlerinin CCTV kameralar ile kayıtları alınması durumunda bunun açık rıza dahilinde yapılıp yapılmayacağının tartışılması gerekebilir. Bu bakımdan veri sorumlusu olan üniversitenin “ öğrencilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla meşru menfaat” kapsamında bu görüntüleri işleminin mümkün olup olmadığına bakmamız gerekir. Şayet bu hukuki sebep söz konusu değilse bu takdirde öğrencilerden alınacak açık rıza ile kişisel verilerin işlenmesi mümkün olabilecektir.

Üniversitenin meşru menfaati açısından, üniversite yönetiminin güvenlik beklentisinin karşılanması ile öğrencilerin mahremiyetleri arasındaki çatışmanın incelenmesi gerekir. Bu çatışmanın giderilmesi için ise iki beklenti arasında denge kurulması, kamera gözetiminin hukuki dayanağının bulunması ve yapılan gözetimin ölçülü olması gerekecektir. Ölçülülüğün sağlanması açısından, gözetimin gerçekleştirildiği yerin kamusal bir alan olması önemli bir detay olarak karşımıza çıkar. Örnek olarak tuvalet gibi özel hayatın gizliliğine dair beklentinin yüksek olduğu bir alanda görüntüleme faaliyetinin yapılması ölçüsüz olarak nitelendirilebilir.

⁵²⁰ Elif KÜZECİ, s. 395.

Ayrıca bu veri işleme faaliyeti “kanunlarda açıkça öngörüldüyse”, açık rıza alınmasına gerek bulunmayacaktır. Üniversitelerin yerleşkelerinde güvenliği sağlama amacıyla kapalı devre kamera verilerini işleme faaliyetlerini 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun’a ve bu kanuna dayanılarak çıkarılan uygulamaya ilişkin Yönetmelik’e dayandırdıklarını görebilmekteyiz⁵²¹. Ancak hem sözü geçen Kanun’da hem de Yönetmelik’te doğrudan kamera faaliyetlerinin gerçekleştirilmesine izin veren ve bu faaliyetlerin yerine getirilmesine ilişkin esasları belirleyen bir düzenlemeye yer verilmediğinden kanunda açıkça öngörülen bir düzenlemenin bulunduğundan bahsetmek mümkün değildir. Öğretim görevlerinin bu alanlardaki hareketlerinin kayıt altına alınması bakımından ise üniversite ile aralarında bulunan sözleşmesel ilişki gereği gözetimin işyerinde yapılan bir gözetim olarak görülmesi gerektiğini ifade edebiliriz⁵²². Buna ilişkin değerlendirme çalışmamızın devamında yapılacaktır.

KVKK’nın gerekçesinde belirtildiği üzere açık rızanın tanımı yapılırken ABVKY örnek alınmıştır. Bu kapsamda ABVKY’ye göre açık rızanın, “*ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı*” olduğu belirtilmiştir⁵²³.

Açık rıza kavramı Türk hukuk sistemi içerisinde sadece KVKK’ da değil aynı zamanda Anayasa’ nın 20. maddesinin 3. fıkrasında kişisel verilerin işlenebilmesi için bir ön şart olarak düzenlenmiştir. İlgili maddeye göre KVKK’daki düzenlemeye paralel olarak, kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği hüküm altına alınmıştır. Burada belirtilen kanunun KVKK’yı veya KVKK md. 5 f. 2 (a) bendindeki düzenleme ile paralel olarak diğer kanunları ifade ettiği söylenebilir.

İşyerinde gerçekleştirilen gözetim faaliyetleri açısından dikkat edilmesi gereken birkaç hususa değinmemizde fayda bulunmaktadır. Evimizden dışarıya adımını atan insan gün içinde bulunduğu bir çok ortamda gerek farkında olarak gerekse de farkında olmaksızın kameralar

⁵²¹ Hacettepe Üniversitesi, “Güvenlik Kamera Sistemleri Kurma ve İşletme Yönergesi”, https://hacettepe.edu.tr/duyuru/yonergeler/HUGuvenlikKameraSistemleriKurmaIsletmeYonergesiEk_240521.pdf (s.y. 24 Mart 2022), 03.04.2019 Karar Tarihli, Eskişehir Osmangazi Üniversitesi Senato Kararı, https://guvenlik.ogu.edu.tr/Storage/KorumaVeGuvencilikAmirliigi/Uploads/SKMBT_22319041111170.pdf (s.y. 24 Mart 2022)

⁵²² AİHM de bir kararında üniversite amfilerinde gerçekleştirilecek kamera kayıtlarına ilişkin olarak benzer yönde bir ayrıma gitmiştir. Bkz. Antovic ve Mirkovic, Karadağ’a karşı, b.n. 70838/13, k.t. 28 Kasım 2017.

⁵²³ KVKK Gerekçe, md. 3.

vasıtasıyla gözlemlenmektedir. Bu durumun modernitenin ve teknolojik gelişmelerin etkisiyle farklı alanlara da yayıldığından bahsetmiştik. İnsanın evi dışında, belki de en çok vakit geçirdiği yer sayılan işyerinde gözetim altında tutulması da gözetimin büyük sayılabilecek bir alanını oluşturmaktadır. Temel olarak işçi ve işveren arasında kurulan bir iş sözleşmesi kapsamında karşılıklı edimlerin sunulduğu bu ilişki, güvene dayanmalıdır. Bu ilişki içerisinde işveren tarafından “kaynakların korunması, işletmesel nedenler, bilgi akışının kontrolü, hukuki ve cezai sorumluluğa karşı koruma veya yasalara uygunluk, yasal sorumluluk gerekliliği, performans değerlendirmesi, verimlilik ölçüsü, güvenlik endişeleri”⁵²⁴ gibi nedenlerden dolayı işçinin kişisel verilerinin işlenmesinde ve kamera kayıtlarının tutulmasında, işverenin haklı sebebinin bulunduğu söylenebilir.

Türk Hukuku’nda işçinin işyerinde kameralar ile gözetlenmesine dair işverene bir gözetme yetkisi veren ayrıntılı bir yasal düzenleme mevcut değildir. Her ne kadar İş K. md. 75’te ya da TBK md. 419’da kişisel verilerin kullanılması açısından işverene bir yetki tanınmış da olsa, bu kameralarla gözetimin sınırlarını ve kurallarını belirleyen ayrıntılı bir düzenleme olmaktan çok uzakta yer almaktadır⁵²⁵. Burada gözetimin dayanağı olabilecek en önemli kaynak önceki bölümde açıkladığımız üzere, işverenin yönetim hakkı olabilecektir.

Yönetim hakkı ve beraberinde gelen denetim ve gözetim yetkileri dahilinde işverenlerin kamera görüntülerini işleyebildiği, bunları izleyebildiği ve kaydedebildiğini vurgulamıştık. Ancak bu yönetim hakkının açık rıza olmaksızın veri işlemeyi mümkün kılacak bir “kanunda açıkça öngörülme” şartını sağladığını söyleyebilmek zordur. Kamera kayıtlarının tutulmasında açık rızanın alınmasının istisnasını oluşturan olgunun, işverenin meşru menfaatinin işlemeyi zorunlu tutması olduğu ifade edilebilir⁵²⁶. O halde işveren tarafından yapılan kamera

⁵²⁴ Burcu F. SAVAŞ, İş Hukukunda “Siber Gözetim”, Çalışma ve Toplum, 2009/3, s. 98.

⁵²⁵ A.g.m., s. 114; TBK md. 419 hükmüne göre, “İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.”; İş Kanunu md 75 hükmüne göre, “İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin hakkı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.” Kamera kayıtlarına ilişkin kısım bu maddenin “her türlü belge ve kayıtları saklamak” konusunda işverene verdiği yetki olarak görülmektedir. Keza maddenin devamında bu kayıtların dürüstlük kurallarına ve hukuka uygun olarak kullanılması zorunlu olduğu üzere temel veri koruma ilkeleri ile paralel olduğu görülmektedir. Son cümlede yer alan “gizli kalmasında işçinin hakkı çıkarı bulunan bilgiler” açısından ise bu verilerin sır saklama yükümlülüğü kapsamında üçüncü kişilere açıklanmaması gerektiği ifade edilmiştir. Bkz. Miray Özer DENİZ, “İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması ve Bundan Doğan Sorumluluk”, Türkiye Adalet Akademisi Dergisi, S. 45, Y. 12, Ocak 2021, s.366.

⁵²⁶ Gökhan C. ERBAŞ, s. 105 .

gözetiminin ilgili kişinin rızasına bağlı olmaksızın yapılabileceğini kabul etmemiz mümkün olabilir. Ancak yine de buna dair aydınlatmanın yapılması gerekli ve önemlidir.

İşyerinde gerçekleştirilen gizli kamera kaydı alınmasına ilişkin faaliyetlere ilişkin, Alman Federal İş Mahkemesi tarafından verilmiş olan bir kararda⁵²⁷,

“İşyerinde gizli kamera kayıtlarının asıl itibarıyla problem teşkil ettiğini, işçinin işverene güvenerek işyerinde hareketlerinin kayda alınmadığı zannı ile hareket ettiğini, normal şartlar altında böyle bir durumda yapılan gizli kamera kaydının, işçinin kişilik haklarına haksız müdahale olarak nitelenebileceğini belirtmiş, ardında da işyerinde gizli kamera kaydının çok katı şartlar altında kabul edilebilir olduğunu, işçinin suç teşkil eden eylemi işlediğine dair somut ciddi şüphelerin bulunması halinde gizli kamera kaydının kabul edilebilir niteliğe bürüneceği” belirtilerek, işverenin meşru menfaatlerinin sağlanması açısından gizli kamera kaydının tutulmasına izin verildiği görülmüştür.

İşçi işveren arasındaki özel ilişkinin dışında daha geniş bir ilişki içerisinde bulunan yurttaş ile devlet arasında gerçekleşen ya da birey ile özel hukuk tüzel kişisi arasında gerçekleşecek kamera gözetiminde ise hem devletin kurumlarının hem de özel hukuk kişilerinin gözetleyen konumlarında bulunduklarını daha önceden de ifade etmiştik. Bu aktörlerin ilgili kişilerin açık rızalarını almaksızın veri işleme faaliyeti gerçekleştirmeleri mümkün müdür?

Bu şekilde işlemeyi sağlayabilecek hukuki nedenlerden bir tanesi de açık rıza olmaksızın kişisel verilerin işlenmesini sağlayan bir diğer durum olan, kişisel verilerin “ilgili kişinin kendisi tarafından alenileştirilmiş olması” halidir. Alenileştirmek kanun gerekçesinde “herhangi bir şekilde kamuoyuna açıklanmış olma” durumu olarak ifade edilmekle birlikte, daha anlaşılır bir ifadeyle kişisel veriyi “herkes tarafından bilinir kılma” olarak tanımlanabilir⁵²⁸. Örneğin kişilerin sosyal medya hesapları üzerinden yapmış oldukları herkese açık paylaşımları nezdindeki görüntüleri buna örnek teşkil etmektedir⁵²⁹. Keza buna benzer bir örnekte de kişinin çalıştığı üniversitenin internet sayfasında yayınlanan fotoğrafının alenileştirilmiş sayılıp sayılmayacağına ilişkin olarak, buradaki kişisel veri olan fotoğrafın ilgili kişi tarafından değil çalıştığı üniversite tarafından alenileştirilmiş olduğu düşünüldüğünde

⁵²⁷ A.g.m., s. 105.

⁵²⁸ 6689 Sayılı Kanun’ da Yer Alan Terimler, Kişisel Verileri Koruma Kurumu, <https://www.kvkk.gov.tr/Icerik/4186/6698-Sayili-Kanunda-Yer-Alan-Terimler> (s.y. 02 Şubat 2022)

⁵²⁹ Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, s. 405.

kişisel verinin işlenmesi açısından hukuki sebep teşkil etmeyeceği açıktır⁵³⁰. Buna ilaveten yapılacak değerlendirmenin aynı zamanda amaca yönelik bir işleme bulunup bulunmadığı yönünde de yapılması gereklidir. Yani Üniversite örneğinde, akademik personelin iletişim bilgilerinin sadece kurumsal ve akademik amaçlı iletişim için kullanılması mümkün olacaktır⁵³¹. Aynı amaca uygun kullanım kapalı devre kameralar aracılığı ile toplanan görüntüler açısından da söz konusu olmalı ve çalışmamızın daha önceki bölümlerinde ifade ettiğimiz güvenliğin sağlanması ya da suçun önlenmesinin dışında amaca uygun olmayan işleme amaçlarıyla bu veriler işlenmemelidir.

Aleniyetten anlaşılması gereken ilgili kişinin kişisel verilerini belirsiz sayıda kişilerle paylaşmış olması olarak da ifade edilebilir. Burada ifade edilen belirsiz kişiyle paylaşım aleniyetin objektif unsuru olarak görülmektedir. Bu objektif unsur yanında aleniyetin bir de sübjektif tarafı bulunmakta olup, bu da ilgili kişinin kişisel verisini paylaşmaktaki amacı ve makul beklentisidir⁵³². Bu amaç ve beklenti ile örtüşmeyen veri işleme faaliyetlerinin, hukuka uygunluk sebebi olarak görülmesi mümkün gözükmemektedir.

Kişisel verilerin bu şekilde bir alenileştirilmesine bağlı olarak ifade etmemiz gereken bir diğer durum da kişisel verilerin alenileştirilmesinin üzerinden ne kadar çok zaman geçerse, kamunun bu bilgiye ulaşma menfaatinin de o kadar azalmış olacağıdır. Bu durum Google Spain kararında ifade edilmiştir⁵³³. Buradan çıkaracağımız sonuç doğrultusunda, ilgili görüntünün aleni hale geldiği tarih göz önüne alındığında bu fotoğrafın yıllar sonra alınarak kullanılmasının sorun yaratabileceğini söyleyebiliriz.

Başka bir örnekte ise kamuya mal olmuş bir sanatçının ünlü olarak tanındığı imajından tamamen farklı bir şekilde, mensubu olduğu dine ait kıyafetler ile kaydedilen kamera görüntülerinin, maddi menfaat sağlanmak ve tehdit amacıyla basına sızdırıldığını düşündüğümüzde nasıl bir yorum yapılabilir? Bu hususta hukuki değerlendirme yapmak için bazı unsurları incelememiz gerekmektedir.

⁵³⁰ Elif KÜZECİ, *Kişisel Verilerin Korunması*, s. 398.

⁵³¹ İpek Şehriban AŞIKOĞLU, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, On İki Levha Yayıncılık, İstanbul 2018, s. 192.

⁵³² Eşref Barış BÖREKÇİ, *Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu* (TCK md. 136.), On İki Levha Yayıncılık, İstanbul 2020, s. 118; Ayrıca Alenileştirme hukuka uygunluk sebebinin sübjektif tarafına ilişkin çeşitli değerlendirmelere dair kararları için bkz. Yargıtay 12. CD, E. 2017/2960, K. 2018/1541, T. 14.2.2018, Yargıtay 12. CD, E. 2015/3247, K. 2015/16760, T. 4.11.2015.

⁵³³ Mesut Serdar ÇEKİN, s. 115; İlgili karar için bkz. ABAD, C-131/12, Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, 13 Mayıs 2014.

Öncelikle belirtmemiz gerekir ki kamuya açık alanlardaki görüntülemeler açısından ortada KVKK'da belirtilen veri işleme şartlarından bir tanesi bulunmuyorsa bu görüntülerin işlenmesi, fotoğraf ya da video kaydı alınması mümkün olmayacaktır⁵³⁴. Kanun'da sayılan diğer veri işleme şartlarından herhangi biri bulunmuyorsa görüntü kayıtları sadece ilgili kişinin açık rızası kapsamında işlenebilecektir. Kamuya açık alanlarda, davet ve etkinliklerde yer alan kimselerin görüntülerinin işlenmesi durumunda alenileştirilmiş olma hukuki sebebinin uygulanması mümkün olacaktır⁵³⁵.

Ancak doktrinde kamuya açık alanlarda yer alan ya da etkinliklere katılan herkesin, görüntüsünü alenileştirme iradesine sahip bulunmayacağı ya da en azından alenileştirmenin görüntünün kullanım amacını kapsamıyor olabileceği kabul edilir⁵³⁶. Bu bakımdan alenileştirme hukuki sebebinin gerçekleşmesi için görüntü alındığı hususunun veri sahiplerince bilinebilir olması temin edilmeli, çekimler aleni olarak yapılmalı, bu faaliyete dair aydınlatma yapılmalıdır. Bu şekilde hem KVKK açısından aydınlatma yükümlülüğü yerine getirilmiş olacak hem de görüntülerinin fotoğraf ya da video şeklinde kayda alınmasını istemeyenlerin bu veri işleme faaliyetlerine itiraz etme hakları doğmuş olacaktır.

Kamuya açık olmayan ya da az sayıda kişinin bir araya geldiği toplantı ya da etkinliklerde görüntülerin alenileştirilmesinden bahsedemeyiz. Dolayısıyla yukarıda da ifade ettiğimiz şekilde alenileştirme dışında herhangi bir hukuki sebep bulunmuyorsa (açık rıza da yoksa) bireylerin kameralar vasıtasıyla görüntülerinin izlenmesi ya da kaydedilmesi hukuka aykırı olacaktır⁵³⁷.

Alenileştirmeye ilişkin olarak Kişisel Verileri Koruma Kurulu'nun yapmış olduğu tespite göre ise kişisel verinin, aleni kabul edilebilmesi için öncelikle ait olduğu kişinin aleni olmasını istemesi gerekecektir. Diğer bir ifade ile kişinin bu yönde bir iradesinin var olması gerekir. Bu anlamda tek başına kişisel verinin kamuoyuna açık hale gelmesi, örneğin herkesin görebileceği bir yerde olması ya da herkesin erişimine açık durumda bulunması alenileştirilmiş olması bakımından yeterli olmamakta; eylemin, ilgili kişinin iradesi ile de desteklenmesi

⁵³⁴ Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, s .409.

⁵³⁵ A.g.e., s .409.

⁵³⁶ A.g.e., s .409.

⁵³⁷ A.g.e., s .410.

gerekmektedir. Kişinin iradesi dışında bir sebeple kişisel verinin kamuoyuna açıklandığı durumlarda Kanun kapsamında bir alenileştirmeden söz etmek mümkün olmayacaktır⁵³⁸.

Bu durumun tespiti yani kişinin alenileştirme iradesi olup olmadığı sosyal medya platformlarında kolaylıkla tespit edilmektedir. Kişi eğer profilini ya da ilgili görüntüyü umuma açık hale getirmişse buradaki kişisel verilerin de umuma açık, alenileştirilmiş olduğunu kabul etmek gerekecektir⁵³⁹. Kapalı devre kameralar açısından ise gözetimin kamuya açık alanlarda icra edildiğini düşündüğümüzde alenileştirme iradesinin gözetim altındaki alana giriş ile birlikte direkt olarak söz konusu olduğu ifade edilebilir. Daha önce de belirttiğimiz üzere CCTV gözetimi yapılan alanların bireysel mahremiyet beklentisinin daha az olduğu alanlar olduğu ve kamera gözetiminin yapıldığı caddeler, yollar, sokaklardaki kamera gözetiminin temel hak ve özgürlüklere müdahale oluşturmayacağı ifade edilmiştir⁵⁴⁰.

Her ne kadar kamuya mal olmuş sanatçının özel yaşamının gizliliği hakkı, kamuoyunun haber alma özgürlüğü derecesine bağlı olarak ifade ve haber alma özgürlüğü kapsamında sınırlandırılabilir da sanatçıya ait görüntülerin izinsiz olarak işlenmesi ve aynı zamanda sanatçının insanların kendisini tanıdığı ya da kendisini kamuoyuna açıklamış olduğu görünüş halinin dışında bulunması dolayısıyla “alenileştirme” de söz konusu olmayacağından buradaki veri işleme hukuka aykırı olacaktır⁵⁴¹. Burada aynı zamanda mensubu olduğu dine ait kıyafetler ile görüntü alındığını düşündüğümüzde özel nitelikli kişisel verilerin işlenmesinin söz konusu olduğunu da ifade etmemiz gerekir. Dolayısıyla kişinin özel nitelikli verilerinin ortaya çıktığı bu olay özelinde bu verilerin niteliğine uygun şekilde yeterli hassasiyet gösterilmeli ve gerekli veri koruma tedbirlerinin alınması gereklidir.

İşlenen görüntü kayıtlarına dair açık rıza alınmasının mümkün olmadığı durumlardan bir tanesi de günlük yaşamımızda, kamuya açık alanlarda fotoğraf ya da video kayıtları alınırken bu görüntülere giren üçüncü kişilerin kişisel verilerinin işlenmesi hali olmaktadır.

⁵³⁸ “Alenileştirme” Hakkında Kamuoyu Duyurusu, <https://www.kvkk.gov.tr/icerik/6843/-alenilestirme-hakkinda-kamuoyu-duyurusu> (s.y. 23 Mart 2022)

⁵³⁹ Mesut Serdar ÇEKİN, s. 116.

⁵⁴⁰ Bkz. yuk. s. 145.

⁵⁴¹ Özel hayatın gizliliği ile ifade ve haber alma özgürlüğü arasında bir dengenin kurulmaya çalışıldığı AİHM tarafından verilen bir kararda Mahkeme, halkın halka mal olmuş kişilere ilişkin bilgileri öğrenme hakkına ilişkin bir değerlendirmede bulunmuştur. Bu kararda, halka mal olmuş kişilerin de diğer herkes ile birlikte özel hayatlarının korunmasını isteme hakları bulunması nedeniyle, başvuranın özel hayatının korunmasına ilişkin “meşru bir beklentiye” sahip olması gerektiği belirtilmiştir. Bkz. Von Hannover, Almanya’ya karşı, b.n. 59320/00, k.t. 24 Haziran 2004.

Örnek vermemiz gerekirse, İstanbul'un tarihi yarım ada bölgesinde turistik fotoğraf çekilen bir kimsenin fotoğrafında arka planda yer alan bir üçüncü kişinin kişisel verilerini hangi koşullarda işliyor olabiliriz. Gerçekten de işlenen verinin bu üçüncü kişiye ait bir kişisel veri olduğu ve veri işleme süreçlerinden haberdar edilmeden kayıt yapıldığı bir gerçektir. Bu kişilerden aynı şekilde açık rıza alınması da somut olay bakımından imkansız görülebilir. Bu nedenle bu kimselerin kişisel verilerinin işlenmemesi daha uygun olacaktır. Eğer görüntülerde yer buluyorlarsa, en azından yayın aşamasında kayıtlarda yer alan üçüncü kişilerin yüzleri veya diğer belirlenebilir özellikleri silinmeli ya da puslulaştırma gibi teknik tedbirler kullanıldıktan sonra yayınlanmalıdır⁵⁴².

Yargıtay'ın bu konuda vermiş olduğu bir kararda, *“Özel hayat kavramının; kişinin sadece gözlerden uzakta, başkalarıyla paylaşmadığı, kapalı kapılar ardında, dört duvar arasındaki yaşantısı ve mahremiyetten ibaret değil, herkesin bilmediğini veya bilmemesi gereken, istenildiğinde başka kişilere açıklanabilen, tamamen kişiye özel hayat olayları ve bilgilerin tamamını içermesi karşısında, kamuya açık alanda bulunduğu dahi, ”kalabalığın içinde dikkat çekmezlik, tanınmazlık, bilinmezlik” prensibinin geçerli olduğu ve kamuya açık alana çıkan her kişinin, bu alandaki her görüntü veya sesinin kaydedilip, sürekli ve izinsiz olarak elde bulundurulmasına rıza gösterdiğinin kabulünün mümkün bulunmadığı nazara alınarak...”* şeklinde tespitte bulunduğu görüldüğünde, kişinin sadece bireysel mahremiyet alanı sayılan özel alanlarında değil kamusal alanlarda bile izinsiz bir şekilde görüntüsünün alınmasının kabul edilemeyeceği ve bu bakımdan kişinin özel hayatına saygı gösterilmesini isteme hakkının baki olduğu vurgulanmıştır⁵⁴³.

Buraya kadar incelediğimiz kısımda kapalı devre kamera görüntülerinin işlenmesinde açık rızanın önemini ve verilerin ilgili kişi tarafından alenileştirilmiş olması hallerini incelemiş bulunmaktayız. Ancak uygulamada bazı hallerde açık rızanın alınmasının zor olduğu ya da anlamlı bir açık rızanın elde edilemediği durumlarla karşılaşılacaktır. Örneğin, nesnelerin interneti teknolojisinin, bireyler için getirdiği en geniş ölçekli tehditler gizlilik ve güvenliğe yönelik tehditlerdir. Çok kuşatıcı bir hale geldiği görülen bu teknolojileri neredeyse her alanda kullanmaktayız. Ancak bu kullanımlar öncesinde yürütülen aydınlatma ve açık rıza alınması süreçlerinin ne ölçüde hukuka uygun olduğu bir soru işareti olarak karşımıza çıkmaktadır. Nesnelerin interneti teknolojisi bu yönüyle CCTV gözetiminin ötesine geçmekte ve bireyi

⁵⁴² Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, s .411.

⁵⁴³ A.g.e., s .411.

evinin içerisinde bile rahat bırakmayarak, bireyi kendi evinde bile izleniyor hissettirmektedir. Bu ekosistemde kullanılan bir takım uygulamalar ise bireylerin daha iyi kredi notundan yararlanması, sigorta primlerinin belirlenmesi, istihdam tercihlerinde öne geçme gibi amaçlara hizmet etmektedir. Bu nedenle bu uygulamalara yönelik olarak tüketici konumunda bulunan bireyleri bilgilendirme ve onaylarını alma süreçlerinin kişisel verilerin korunmasına dair kanunlara ya da diğer rehberlere göre yürütülmesi gerekmektedir⁵⁴⁴.

Sürücüsüz araçlarla seyahat etmekte olan ve konum bilgileri sürekli olarak toplanan insanlar bu hizmetin alınması için gerekli olan her türlü bilgi, sürekli olarak belki önceden bildirime dayalı bir açık rıza kapsamında belki değil, işlenmesi için üçüncü taraflara aktarılmaktadır. İlginçtir ki, gizlilik beklentileri hususunda kapalı devre kameralara iltimas göstermeyen bireyler cep telefonlarından sürekli bir biçimde görsel içerik paylaşma konusunda çok isteklidirler. Bu sebeple, ilgili uygulamalarda kendilerine gösterilen aydınlatmaya dair metinleri ya da rıza beyanlarını ayrıntılı olarak incelemeyen rızalarını sunmaktadırlar.

Bir başka örnek ise internet üzerinden yapılan satışlarda yer alan ilan fotoğraflarına ilişkindir. Gerçek bir kimseye ait her türlü bilginin içine, doğal olarak kişiye ait plaka bilgisi, araç bilgisi, aracının özellikleri, kullanım durumları gibi bilgiler de girmektedir. İnternet sitesinde yayınlanan görüntülerin, ilgilisi tarafından alenileştirilmiş olduğundan bahisle, aynı bilginin pazarlama amacıyla kullanılması hukuka aykırı olacaktır. Bu bakımdan Kişisel Veilleri Koruma Kurulu bir kararında, *“şikayetçinin kişisel verilerine kendisi tarafından daha önce alenileştirilen internet sitesinden ulaşılması halinde dahi şikayetçinin bu bilgilerinin internet sitesinde bulunma ve alenileştirme amacıyla kullanılmadığını”* belirtilerek, sadece kişisel verinin alenileştirilmiş olmasının yetmediğini, buna ilaveten kullanılacak verinin alenileştirme amacına uygun olarak işlenmesi gerekmesini bir zorunluluk olarak tasvir etmiştir⁵⁴⁵.

Bu başlık altında değerlendirilmesi gereken diğer hukuka uygunluk sebepleri ise kanunlarda açıkça öngörülme, bir veri sorumlusunun hukuki yükümlülüğünü yerine getirmek amacıyla ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması olarak karşımıza

⁵⁴⁴ Swaroop POUEDEL, Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security, Berkeley Tech. Law Journal., Annual Review, C. 31, Y. 2016, s. 1013.

⁵⁴⁵ “İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/331 Sayılı Karar Özeti, <https://kvkk.gov.tr/Icerik/6623/2019-331>, E.T: (s.y. 22 Aralık 2020)

çıkılmaktadır. İlk olarak değineceğimiz “kanunlarda açıkça öngörölme” hukuki sebebinin devlet mekanizmaları tarafından yapılan CCTV gözetimi açısından bulunmadığını, çünkü bu alandaki en geniş kapsamlı CCTV sistemleri olan MOBESE’lere dair herhangi bir yasal düzenlemenin yasal mevzuatımız içerisinde yer almadığını ifade etmemiz mümkündür. Bununla birlikte ilgili veri işlemenin devletin hukuki yükümlülüğünü yerine getirmek kapsamında yapılmasını değerlendirdiğimizde karşımıza ilk olarak, TCK m. 24, f. 1’de düzenlenen, “*Kanunun hükmünü yerine getiren kimseye ceza verilmez.*” şeklindeki görevin ifası hükmü gelmektedir. Hükme göre, kanun hükmü kişiye herhangi bir konuda bir hak veya yetki vermiş olursa, bunun öngördüğü şekilde uygulanması durumunda hukuka aykırılık söz konusu olmayacaktır. Kamera ile gözetleme faaliyetinin, kanunun yüklediği birtakım mükellefiyetlerin yerine getirilmesi kapsamında bu şekilde kullanılmasının mümkün olacağı söylenebilir. Ancak daha önce de belirttiğimiz İl idaresi Kanunu’nda, PVSK’da ya da diğer kanuni düzenlemelerde yer alan hükümlerin hiç birinin, bireylerin yirmi dört saat aralıksız videoya kaydedilmesine imkân veren kameralı gözetleme faaliyetine doğrudan yetki vermediği belirtilmiştir⁵⁴⁶.

Keza devletin kurum ya da kuruluşlarının bu genel gözetimi meşru menfaatleri kapsamında yapmalarının temel hak ve özgürlükler problemlerini beraberinde getirdiği görülebilmektedir. Bu kapsamda daha önce de yaptığımız açıklamalar çerçevesinde, veri işlemenin ölçülü ve amaca uygun olması, özel hayatın gizliliğini isteme hakkının sınırlandırılmasının sınırlarına uyulması gibi beklentilerin karşılanıyor olması gerekecektir.

İşyerinde işveren tarafından işçilerin gözetlenmesi bakımından kanunda açıkça öngörölmeekten ziyade gözetimin meşru menfaate dayandırıldığı görülmektedir. Bu bakımdan Dülger, “*işverenlerin bu denetimi yapmakta meşru menfaatlerinin olduğunu söylemek mümkünse de; ekonomik nedenlerden dolayı bireylerin özellikle güçsüz konumda bulunan işçilerin temel hak ve özgürlüklerinden vazgeçmesini beklemek mümkün olmadığı gibi hukuka uygun da değildir.*” diyerek, meşru menfaat değerlendirilmesinin yapılması sırasında her iki tarafın da menfaatlerinin dengelenmesi gerektiğini belirtmiştir⁵⁴⁷.

⁵⁴⁶ Buket ABANOZ, s. 142.

⁵⁴⁷ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 629.

4. Kişisel Verilerin Korunması Kanunu Kapsamında Gözetlenenlerin Hakları

Gözetleme ve denetim amacıyla olsun ya da olmasın, kapalı devre kamera sistemleri tarafından izlenen ve kaydedilen görüntülerin ilgisi konumunda bulunan bireyler, bu görüntülerin kişisel verilerin korunması kapsamında hukuki koruma altında olduğunu bilmelidirler. KVKK açısından kişisel veri olarak tanımlanmış olan görüntünün sahibi olan kimse, yine bu kanun tarafından getirilen haklardan yararlanmayı isteme şansına sahiptir. Nitekim bu amaçla kanun koyucu tarafından özel bir başlık altında düzenlenen “ilgili kişinin hakları” başlıklı KVKK md. 11’ e göre,

“ 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 halinde 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 silinmesini veya yok edilmesini 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 zarar uğraması halinde zararın giderilmesini talep etme,*
- haklarına sahiptir. ”*

Yukarıda düzenlenen haklar esasında kişisel verilerin işlenmesi sürecinde kurumlar ya da büyük şirketler karşısında daha güçsüz durumda bulunan kişilerin, haklarının korunmasına yönelik olarak bireyi veri koruma hukukunun nesnesi konumundan öznesi konumuna yükseltmektedir. KVKK’nın bu maddesi uyarınca ilgili kişinin bilgilere erişim, yanlış bilgileri

düzeltilme, hukuka aykırı olanları sildirme, aktarılmasını engelleme gibi hakları düzenlenmiştir⁵⁴⁸.

KVKK kapsamında ilgili kişiye tanınmış olan bu haklar, kişisel verilere erişim hakkı kapsamında ilgili kişinin yararlanabileceği haklardır. Bahsi geçen ilgili kişi yani kanundaki tanımıyla, kişisel verisi işlenen gerçek kişi, bu hakkını kullanarak veri sorumlusuna başvurup kişisel verisinin işlenip işlenmediği öğrenebilecektir. Kişisel verilere erişim olmadan, bu kanundaki bir kısım hakların kullanılmasını talep etme hakkı da tam olarak kullanılamayacağından, hukuki nitelik olarak bu kanun kapsamında tanınan diğer haklara da bir nevi temel teşkil etmektedir. Örnek vermemiz gerekirse, ilgili kişi kişisel verilerine erişmeden, bu konuda bir bilgi sahibi olmadan, hangi kişisel verilerinin silinmesini istemesi içi boş bir talep olarak nitelendirilebilecektir. Yine kanımızca, kişisel verilerin kanuna aykırı olarak işlenmesi durumu söz konusu ise zararın giderilmesini talep etmek için ilk olarak hangi verilerin işlendiğini öğrenme hakkın uygulanması açısından zorunlu görülmektedir.

Kişilerin kendileri hakkındaki yanlış veya eksik işlenen verilerin düzeltilmesini isteme hakları KVKK'nın genel ilkelerinden bir tanesi olan *“kişisel verilerin doğru ve gerektiğinde güncel olması”* ilkesiyle doğrudan bağlantılı olmaktadır⁵⁴⁹. Bu yönde iki taraflı bir değerlendirme yapılması mümkündür. Bir taraftan görüntüleri işleyen veri sorumluları açısından zaten uymakla yükümlü oldukları bir kural olarak ortaya çıkarken, diğer taraftan da ilgili kişi her zaman buna ilişkin bir talepte bulunarak kurala uygun davranılmasını isteme hakkına sahip olabilecektir.

KVKK'nın 11. maddesinin (e) fıkrasında düzenlenen *“öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme”* hakkı ise silme (unutulma) hakkı olarak tanımlanmaktadır⁵⁵⁰. Unutulma hakkı olarak tanımlanan ve ilgili kişilere dijital geçmişte internet üzerinde haklarında yer alan rahatsız edici içerikleri veya üzerinde hak sahibi oldukları kişisel verileri silme ve daha fazla yayılmasını önleme yetkisi veren bu hak, bireylerin internet ve sosyal medya alanlarında kendileri hakkındaki bir kişisel veriyi tamamıyla kontrol etmesiyle ilgili olmaktadır⁵⁵¹.

⁵⁴⁸ Elif KÜZECİ, *Kişisel Verilerin Korunması*, s. 421.

⁵⁴⁹ Murat Volkan DÜLGER, *Kişisel Verilerin Korunması Hukuku*, s. 486.

⁵⁵⁰ A.g.e., s. 490.

⁵⁵¹ Aydın AKGÜL, “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, *Türkiye Barolar Birliği Dergisi*, S. 116, Y. 2014, s. 17.

Her türlü kişisel verinin sınırsız biçimde kayıt altına alındığı ve bir kere kayıt altına alınmasından sonra hızlı ve geniş paylaşım nedeniyle ortadan kaldırılmasının oldukça zor olduğu günümüz teknolojik platformları içerisinde, bireyin üçüncü kişilerin gözetiminden kurtulma ve dolayısıyla yaşamını özgür biçimde sürdürebilme isteği unutulma hakkına olan ihtiyacı doğurmaktadır. Bu durum ise bireyin internet ortamındaki izlerinin kendi talebine istinaden bütünüyle silinip silinemeyeceğine dair tartışmaları beraberinde getirmektedir.

Aslında unutulma hakkı; bir kişinin kendisi hakkındaki bilgileri kapsamlı ve geniş biçimde yeni bir silme hakkı olarak da görülmektedir. Silme hakkı ilgili görüntünün silinmesi için üçüncü şahısları zorlama yetkisini bireye tanırken, ayrıca hakkında olumsuz yorumlara neden olabilecek geçmiş bilgi ve fotoğraflarının da kaldırılmasını isteme hakkı vermektedir⁵⁵².

Geçmişte başından geçen bir olaya ait CCTV görüntüleri internet ortamında yayınlan bir kimsenin unutulma hakkı kapsamından yararlanarak bu görüntülerin bulundukları ortamdan kaldırılmasını talep etme hakları bulunmalıdır. Buna dair yapılacak değerlendirmede, veri sorumlularının çoğunlukla basın ve ifade özgürlüğü gereği kamuoyunu bilgilendirme hakları bulunduğunu ileri sürdükleri görülecektir. Ancak veri sorumlusunun bu iddialarına karşılık ilgili kişinin de manevi varlığını geliştirme hakkı, insan onuru, şeref ve haysiyetinin korunması, özel hayatın gizliliği ve kişisel verilerin korunması haklarından yararlandırılması gerekmekte birlikte her iki tarafın talepleri arasında adil ve makul bir dengenin oluşturulması gerekecektir⁵⁵³.

Yukarıdaki dengenin sağlanması bakımından Avrupa Birliği Adalet Divanı (ABAD) tarafından verilen Google kararının incelenmesi uygun olacaktır. Unutulma hakkına ilişkin olarak ABAD'ın Google kararında belirttiği üzere, kişinin ismine dayalı olarak üçüncü kişiler tarafından internette yasal olarak işlenmiş ve yayınlanmış kişisel veriler, geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelmiş ise işlenmesi amacını aşan ve arama motorları tarafından internet ortamına yüklenen ve buna ilişkin sonuç listesinde yer alan bilgilerin silinmesi gerektiği belirtilmiştir⁵⁵⁴. Bunun dışında ilgili kararda, kişinin adı yazılarak, on altı yıl önce gerçekleşmiş bir olaya ilişkin bilginin çıkacağı bir link verilmesinin kabul

⁵⁵² A.g.m., s. 18.

⁵⁵³ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 499.

⁵⁵⁴ Aydın AKGÜL, s. 31.

edilemeyeceği, kişinin bu şekilde bir link verilmemesi şeklinde bir talep hakkının doğduğu da belirtmiştir⁵⁵⁵. Bu yönde değerlendirmemizi iki yönde yapabiliriz. İlk olarak kamera görüntülerinin bulunduğu sitelere link veren Google gibi arama motorlarının bu yönde veri işlemeye son vermesi gerekliliğidir. Diğer yönden link verilen internet sitelerinde yer alan görüntülerin de “geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelmiş” olmalarını dayanak alarak amacını aşan bir veri işleme söz konusu olduğunu söyleyebiliriz.

Ayrıca, eğer ilgili kişi örneğin yukarıdaki CCTV görüntülerine yansıyan fiil nedeniyle yargılanmış ve sonuçta beraat etmiş ise ilgili görüntülerin silinmesini derhal isteyebilmelidir. Bu sonuca veri sorumlusunun kişisel verileri işleme faaliyeti sırasında verileri belirli, açık ve meşru amaçlar için işleme, verilerin işlenmesi bakımından amaç için gereken süre kadar muhafaza edilme ile doğru ve gerektiğinde güncel olma ilkelerine uyma gerekliliği doğrultusunda ulaştığımızı söyleyebiliriz⁵⁵⁶.

Uygulamada gerçek kişilerin kişisel verilerini işleyen taraf olarak görülen kamu kuruluşları ya da ticaret şirketlerinin internet sitelerinde de kanundaki düzenlemelere paralel olarak aydınlatmalar yapıldığı, kişisel verilerin işlenmesi ya da veri koruma ve imha politikaları başlıkları altında gerçek kişilere kişisel verilerinin işlenmesine ilişkin bir takım bilgilerin aktarıldığı görülmektedir.

Aşağıda değerlendireceğimiz KVKK md. 28’de düzenlenen ve bütünüyle Kanun’un uygulama alanına girmeyen durumların yanı sıra, ilgili kişinin haklarını kullanamayacağı bir takım istisna durumlarının da kanunda açıkça düzenlendiği görülmüştür. Buna göre, “*“Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:*

- a) *Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.*
- b) *İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.*

⁵⁵⁵ A.g.m., s. 32.

⁵⁵⁶ Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 500.

- c) *Kişisel veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.*
- ç) *Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.”*

Bu istisna düzenlemesi kapsamında veri sahibi ilgili kişinin, KVKK md. 11’de yer alan haklardan zararın giderilmesini isteme hakkı dışındaki haklarını kullanamayacağını söyleyebiliriz. Buna ek olarak verileri işlenen gerçek kişilerin Bilgi Edinme Hakkı Kanunu kapsamında kişisel verileri işleyen kurum ve kuruluşlara başvurularda bulunmaları da mümkün olmaktadır.

24 Nisan 2004 tarihinde yürürlüğü giren 4982 sayılı Bilgi Edinme Hakkı Kanunu bireylere idarenin elinde bulundurduğu kişisel verilerini öğrenme hakkı vermekte olup, bireyi kamu gücü karşısında edilgen konumdan etkin konuma getirmiştir⁵⁵⁷. Bu işlevi bakımından hakkın, yukarıda değerlendirdiğimiz ilgili kişinin KVKK’dan doğan haklarına çok benzediği görülmektedir. Ancak henüz KVKK’nın var olmadığı bir dünyada yasa koyucunun temel amacının bu işlevi yerine getirmek için bilgi edinme hakkının kullanılmasını düzenlemek olmadığı söylenebilir. Bu kanunun amacının “*demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemek*” olduğu ifade edilmiştir⁵⁵⁸.

Kanun’un 2. maddesinde yer bulan kapsam sınırlandırması itibarıyla bu hakkın kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarına karşı ileri sürülebileceği ve yalnızca bu taraflardan bilgi edinilebileceği öngörülmüştür. Çalışma konumuzun kapsamında yer alan MOBESE sistemini kullanan EGM ve JGK’ya da bu sistemlere ilişkin veri işleme faaliyetleri hakkında bilgi edinme hakkı başvuruları yapılmıştır⁵⁵⁹.

Bahsedilen kuruluşlara verilen başvuru dilekçelerinde ifade edildiği üzere;

⁵⁵⁷ Elif KÜZECİ, *Kişisel Verilerin Korunması*, s. 580.

⁵⁵⁸ BEHK, md. 1.

⁵⁵⁹ Civan BAŞAR, s. 114.

“...Kent Güvenliği Yönetimi Sistemleri (KGYS) kapsamında kamera sistemleri, Plaka Tanıma Sistemi (PTS), Hız veya Ortalama Hız ölçüm vb. amaçla yapılan görüntü tespitleri ile ilgili olarak elde edilen kayıtların, gerek il ve ilçe merkezlerinde gerekse de kurumunuz merkez biriminde;

- a. Ne kadar süre ile muhafaza edildikleri ve muhafaza edilirken herhangi bir nedenle aranan şahıs veya araç olup olmadığına bakılıp bakılmadığı ve muhafaza işleminde bunların farklı uygulamaya tabi tutulup tutulmadıkları,
- b. Hangi kayıtların ne kadar süre sonra ve hangi prosedür ve kurallara göre silindikleri,
- c. Bu kayıtları talep eden adlî merciler dışında diğer kamu kurumları ile özel tüzel kişiler ile gerçek kişilere verilir verilmeyeceği,
- d. 5442 ve 2559/2803 sayılı kanunlarda münhasır düzenleme bulunmaması karşısında, kurumunuz ve bağlı birimlerince elde edilen bu görüntü kayıtlarının, muhafazası, silinmesi, kullanılması ve başka kurum ve kuruluşlara verilmesi iş ve işlemlerinin nasıl yapılacağına ilişkin idari düzenlemeler (genelge, tamim vb.) bulunup bulunmadığı, hususlarında tarafıma 4982 sayılı Bilgi Edinme Hakkı Kanunu hükümleri uyarınca bilgi verilmesi, saygılarımla talep olunur.” şeklinde bilgi istenmiştir.

Bu dilekçelere karşılık olarak verilen cevapların ise konuyu aydınlatma bakımından yeterli olmadıkları görülmüştür. Emniyet Genel Müdürlüğü’nün cevabını “... talep ettiğiniz bilgilerin niteliği itibarıyla ayrı bir araştırma ve çalışma neticesinde oluşturulabilecek türden olduğu, bir kısmının kurum içi uygulamalara yönelik olduğu değerlendirildiğinden cevap verilemeyeceği hususunu bilgilerinize rica ederim. “ şeklinde oluşturduğu; keza Jandarma Genel Komutanlığı tarafından da “... Başvurunuzda belirtmiş olduğunuz hususlarla ilgili olarak yapılan inceleme neticesinde; Jandarmanın, görüntü ve plaka tespiti ile ilgili işlemleri 2803 sayılı Jandarma Teşkilatı Görev ve Yetkileri Kanunu ve Yönetmeliği, 2559 sayılı Polis Vazife ve Salahiyet Kanununun verdiği yetkiler çerçevesinde yürüttüğü tespit edilmiştir. ...” şeklinde cevap verilmiştir⁵⁶⁰.

Kişisel verilere erişim hakkı ile benzer işlevi haiz olan bilgi edinme hakkının kullanımına karşı verilen cevapların yetersiz olması, bu cevapların kişilerin özel hayatlarının

⁵⁶⁰ Civan BAŞAR, s. 116.

gizliliğine ilişkin önemli bir faaliyeti hiçbir hukuki incelemeye konu etmeden oluşturulmuş olması, bize göre hem bu Kanun'un uygulamasının dar yorumlandığını hem de ilgili kuruluşların cevap sağlamakta isteksiz olduklarını göstermektedir. Oysa ki, kamu kurum ve kuruluşları ilgililerin başvuruları üzerine uyguladıkları kamera gözetiminin dayanaklarını, nasıl gerçekleştirildiğini, saklanma koşulları ve sürelerini veya üçüncü kurum ve kuruluşlarla hangi şart ve koşullar altında paylaşılmasına izin verildiğini açıkça belirtmeli; ilgili kişinin başvurusuna karşı olarak olsa bile belirli ölçüde bir bilgilendirme sağlamalıdır. Nitekim yukarıda da ifade ettiğimiz üzere yapılacak bu bilgilendirme, kanunun amacı olan “demokratik ve şeffaf yönetimin gereği olan açıklık ilkesine” uygun düşecektir.

e. İstisnalar

KVKK'nın 28. maddesinin 1. fıkrasında yer alan düzenlemeye göre, kanunda belirtilen amaçlarla belirli konularda kişisel verinin işlenmesi bu kanunun uygulanmasından istisna edilmiştir. İlgili kanun metnine göre, gerçek kişinin kendisiyle veya aynı konutta yaşayan aile bireyleriyle ilgili verileri işleme; istatistik, araştırma ve planlama amacıyla verilerin işlenmesi; sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında verilerin işlenmesi; önleyici, koruyucu ve istihbari faaliyetler kapsamında kişisel verilerin işlenmesi; soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin verilerin işlenmesi söz konusu ise bu faaliyetlere KVKK hükümleri kesinlikle uygulanmayacaktır⁵⁶¹.

Bir gerçek kişinin kendisiyle veya aynı konutta yaşayan aile bireyleri ile ilgili veri işleme, bir çok evde güvenlik amacıyla kullanılan kamera sistemleri tarafından işlenen görüntülerin bu kapsamda yer alıp almayacağını önemli kılmaktadır. KVKK'nın md. 28 (a) fıkrası ise maddeyi sınırlamak açısından yerinde olan bir açıklama getirmiştir. Kişisel veri ancak üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülöklere uyulması kaydıyla işleniyorsa bu istisna uygulanabilecektir⁵⁶². Neticede, bu görüntülerin istisna kapsamında yer alarak Kanun'un uygulanması dışında kalması için, üçüncü kişilerle paylaşımının yapılamaması ve veri güvenliğine ilişkin yükümlölöklere uyulması gerekmektedir. Yani tam anlamıyla bir istisnadan bahsedilmesi mümkün olmayacaktır.

⁵⁶¹ KVKK, md. 28.

GVKT'ya göre, kişisel amaçla (purely personal) ya da ev içi faaliyetlerde (household activity) veri işleme sadece gerçek kişi tarafından profesyonel ya da ekonomik bir amaç olmaksızın işlenen veriler için geçerli olacaktır. Burada yer alan istisna, iletişim, adres bilgisi, sosyal ağlar üzerindeki bilgileri, çevrimiçi faaliyetleri de bu bağlamda kapsamına almaktadır⁵⁶³. GVKT ile KVKK arasındaki bir diğer fark ise, Avrupa veri koruma sisteminde daha genel bir tabir kullanılarak “ev içi faaliyetler” tanımı yapılmış olmasına karşılık, KVKK’ da getirilen düzenlemeye göre sadece “aynı konutta yaşayan aile bireyleri ile ilgili faaliyetler” istisna kapsamına alınmaktadır. Buna göre, KVKK uygulaması kapsamında Türkiye’de istisnanın uygulama alanının daraltıldığını açıkça görebilmekteyiz.

Bir diğer istisna ise sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında verilerin işlenmesidir. Bilhassa ifade özgürlüğü ile kamera kayıtları aracılığıyla gözetlenme arasındaki bağlantı, topluma mâl olmuş ünlü kişilerin gözetlenmesini ya da “paparazzi” faaliyetlerini akla getirmektedir. Bilindiği üzere, özel yaşamın gizliliği ile yakından ilgili olan kişisel verilerin korunması aynı zamanda görüntülere konu olan kişilerin de temel hak ve özgürlüklerinin teminatı olarak karşımıza çıkmaktadır. 1997 yılında geçirdiği bir trafik kazası sonucu Paris’te bir alt geçitte hayatını kaybeden Galler Prensesi Lady Diana’nın ölümünün ardından dokuz fotoğrafçı Fransa’da yargılanmıştır. Fransa Yüksek Mahkemesi tarafından gazetecilerin kazadan sonra çekmiş oldukları fotoğraflar ifade özgürlüğü bağlamında değerlendirilmiştir⁵⁶⁴. Bu kararın önemli özelliklerinden birisi de fotoğrafların çekilmesi ve yayılmasında kamunun bilgilendirilmesi ve kamu yararının, kamuya mâl olmuş kişiler için ifade özgürlüğünden daha baskın olduğunu göstermesidir. Ayrıca, fotoğrafların çekildiği yerin “kişisel alan” dışında olmasının da kararda etkili olduğu söylenebilir.

Kişisel Verileri Koruma Kurulu vermiş olduğu bir kararında, bir gerçek kişinin adının gazetede yayınlanan köşe yazısında geçtiği ve bu nedenle köşe yazısının silinmesini talep ettiği görülmekle birlikte, Kurul tarafından ilgili kişinin hala “kamuyu ilgilendiren bir konumda olduğu” hususu vurgulanarak, veri işlemenin ifade özgürlüğünün bir yansıması olan basın özgürlüğü kapsamında olduğu değerlendirilmiştir. Böylelikle Kişisel Verileri Koruma Kurulu

⁵⁶³ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 377.

⁵⁶⁴ Diana Paparazzi Trio Face Retrial, http://news.bbc.co.uk/2/hi/uk_news/4442659.stm (s.y. 02 Nisan 2022)

tarafından, KVKK md. 28/1 hükmü kapsamına giren veri işleme faaliyetinden dolayı herhangi bir ihlal olmadığına karar verilmiştir⁵⁶⁵.

Kamera sistemlerinin büyük çoğunluğunun kullanılmasında suçun önlenmesi, adaletin sağlanması, güvenliğin ve denetimin sağlanması gibi amaçların hedeflendiği görülmektedir. Tam olarak bu amaçlarla bağlantılı olarak getirilen birden fazla sayıda istisna hüküm kanun koyucu tarafından KVKK’ da düzenlenmiştir. Kişisel verilerin milli savunmayı, milli 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 kanun tarafından açıkça istisna kapsamına alınmıştır. Bu durumda suçun önlenmesi amacıyla sadece kanunla belirlenmiş kamu kurum ve kuruluşları tarafından yapılan kamera gözetimi faaliyetlerinde KVKK’nın uygulanmayacağı söylenebilecektir. Nitekim buna ilişkin olarak doktrinde bu faaliyetlerin istisna kapsamında yer aldığını ifade eden görüşler de bulunmaktadır⁵⁶⁶. Ancak bu durumda bile istisna kapsamına giren veri işleme faaliyetlerinde, KVKK’nın getirdiği toplanan kişisel verilerin sadece toplandıkları amaca uygun olarak işlenmesi, veri işlemenin hukuka ve dürüstlük kuralına uygun olması, verilerin doğru ve güncel olması, işleme faaliyetinin ölçülü olması gibi temel veri koruma ilkelerinin uygulama alanı bulabileceği vurgulanmaktadır⁵⁶⁷.

Kanun’un 28. maddesinin 2. fıkrasında ise birtakım durumlarda KVKK’da sayılan belirli hükümlerin uygulanmayacağı açıkça düzenlenmiştir⁵⁶⁸. Bu durumlardan bir tanesi de “suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması” halidir⁵⁶⁹. Bu düzenleme kapsamında ise suç işlemenin önlenmesi veya ceza soruşturması sırasında gerçek kişilere ait kişisel verilerin işlenmesi durumunda KVKK’nın amaç ve ilkelerine uyulacak;

⁵⁶⁵ Detaylı karar bilgisi için bkz., <https://kykk.gov.tr/Icerik/5407/-Bir-Gercek-Kisinin-Adinin-Gectigi-Kose-Yazisinin-Silinmesi-Talebi> (s.y. 02 Nisan 2022)

⁵⁶⁶ Tefik Sönmez KÜÇÜK, s. 73.

⁵⁶⁷ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 382.

⁵⁶⁸ KVKK md. 28. f. 2’ye göre, “*Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz: a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması. b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması. ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.*”

⁵⁶⁹ Neslihan CAN, Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul 2021, s.3.

ancak veri sorumlusunun aydınlatma yükümlülüğü (md. 10), zararın giderilmesini talep hariç veri sahibinin hakları (md. 11) ve veri sorumluları siciline kayıt hükümleri (md. 16) uygulanmayacaktır. Sonuç olarak, 28/1 hükmü ile önleyici faaliyetler kapsamında işlenen kişisel verilerin KVKK'nın uygulama alanı dışında tutulduğu, ancak 28/2 hükmü ile de suçların önlenmesi sırasında işlenen kişisel verilerin KVKK'nın uygulama alanında yer alacağı söylenmektedir⁵⁷⁰. Yani bu bakımdan KVKK kısmen de olsa uygulama alanı bulacak olup, önleyici faaliyetler kapsamında görüntü kayıtları işleniyorsa bu işleme KVKK'nın tamamen dışında bir hukuk rejimine tabi olmayacaktır⁵⁷¹.

Ayrıca KVKK'daki bu düzenlemeye göre, kişisel verilerin önleyici faaliyetler kapsamında işlenmesinin tek başına bir hukuka uygunluk sebebi yaratmayacağı ve doğrudan istisna oluşturmayacağı da belirtilmiştir. Bu istisnanın söz konusu olabilmesi için önleyici faaliyeti gerçekleştiren kolluğa yetki veren bir yasal düzenleme bulunması gerekmektedir⁵⁷². Daha önce ifade ettiğimiz gibi mevzuatımızda doğrudan MOBESE'lere ilişkin bir yasal düzenleme bulunmadığından, kanaatimizce MOBESE faaliyetlerinin bu istisna kapsamına sokulmasının hatalı olacağı söylenebilir.

MOBESE ya da KGYS gibi kent güvenliğinin sağlanmasına yönelik sistemler ile suç işlenmesinin önlenmesi amacıyla ya da suç soruşturması için gerekli olması nedeniyle kamu tüzel kişileri tarafından kişisel verilerin işlenmesi durumunda bu istisnanın kapsamını değerlendirdiğimizde, söz konusu istisna hükümlerinin uygulanacağı alanın çok geniş yorumlanmaya elverişli bırakıldığını söylememiz mümkündür. Kanımızca bireylerin kişisel verilerin korunmasının Anayasal temele dayandığı, bu hakka getirilecek kısıtlamanın hakkın özüne dokunmaması ve istisnanın yasayla yapılması gerekliliğini zorunlu tutması nedeniyle önleyici polislik faaliyetlerinin bir bütün olarak bu istisna kapsamında değerlendirilmesi yerinde olmayacaktır.

C. Özel Nitelikli Kişisel Veri Sayılan Kapalı Devre Kamera Görüntüleri

1. Özel Nitelikli ve Özel Nitelikli Olmayan Kapalı Devre Kamera Görüntülerinin Ayrımı

⁵⁷⁰ A.g.e., s. 4.

⁵⁷¹ Eşref Barış BÖREKÇİ, s. 128.

⁵⁷² A.g.e., s. 128.

Özel nitelikli kişisel verilerin veri korumaya ilişkin hukuki metinlerin neredeyse tümünde aynı yaklaşım altında, diğer verilere göre özel ve daha kapsamlı bir korumadan yararlandırılmaya çalışıldığı görülmektedir. Bu kapsamla, “özel bir rejime” tabi olarak düzenlenen özel nitelikli kişisel verilerin kapsamına hangi tür verilerin girdiği gibi, bu tür verilerin hangi koşullar altında işlenebileceği gibi düzenlemeler veri koruma yasalarında yer almaktadır. Doktrinde özel nitelikli veri tanımı açısından bir yeknesaklık bulunmadığı görülmekle, bu verilerin genellikle “*hassas veri*” (sensitive data) , “*özel nitelikli veri*” ya da özel “*kategorili kişisel veri*” (special categories of personal data) şeklinde ifadelerin yer aldığı belirtilmiştir⁵⁷³.

KVKK’ da özel nitelikli kişisel verilerin açıkça tanımı yapılmamakla birlikte, kanun koyucu tarafından sınırlı sayı ilkesi ile belirtilen bir takım kişisel verilerin hassas verileri oluşturduğu kabul edilmiştir⁵⁷⁴. İlgili düzenlemeye 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 veridir.*” Kanun gerekçesinde ise, bu veri türünün diğer verilere göre daha hassas olmasının ve bu nedenle daha fazla korunmasının temel nedeni, bu verilerin öğrenilmesi durumunda ilgili kişinin ayrımcılığa maruz kalabilmesi veya ilgilinin mağduriyetine neden olabilmesi ihtimali bulunması olarak görülmüştür⁵⁷⁵. Bir kapalı devre kamera görüntüsünün özel nitelikli veri kategorisinde yer bulabilmesi için bu verinin ya ilgili kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ya da genetik verileri ile ilgili verilerini açığa çıkarmaya yönelik olarak işlenmesi ya da doğrudan biyometrik veri sayılması gerekecektir.

Kamera kayıtları, görüntüler ya da fotoğraflar gibi kişisel veriler her zaman biyometrik veri sayılmazlar. Bu sebeple her durumda özel nitelikli kişisel veri sayılmadıkları da söylenebilecektir. Dolayısıyla bu veri türünün hangi durumda özel nitelikli sayılıp sayılmadığının tespiti önem teşkil etmektedir. Mevcut durumun özelliklerine göre hangi

⁵⁷³ Cemil KAYA, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, İÜHFİM, C. 69, S. 1-2, Y. 2011, s. 317-334.

⁵⁷⁴ Murat Volkan, DÜLGER, Kişisel Veriler, s. 177; KVKK md. 6/1.

⁵⁷⁵ KVKK, Gerekçe, md. 6.

durumlarda bir verinin özel nitelikli olup, hangi verilerin özel nitelikli olmadığı açısından yapılacak değerlendirmelerde çoğunlukla büyük güçlükler yaşanmaktadır.

Bu tereddütlerin daha az yaşanması için, kişisel verilerin işleme amacı temel alınarak değerlendirme yapılması öngörülmektedir. Küzeci'nin de belirttiği gibi, “ *İlgili kişinin video görüntüsü özel nitelikli veri kategorisindeki bilgileri açığa çıkarmaya yönelik işleniyorsa bu kapsamda kabul edilirken, kamera görüntüleri yalnızca güvenlik amacıyla alındıysa hassas veri kategorisinde görülmeyebiliyor.*⁵⁷⁶” Örneğin; siyasi amaçla gerçekleştirilen toplantıya katılan bir kimsenin bu sırada görüntülerinin güvenlik kameraları aracılığıyla kaydedildiği bir durumda, bu kimse siyasi görüşünü açığa çıkaracak bu görüntü kayıtlarının ifşa edilmesini ya da herhangi bir şekilde işlenmeye veya aktarılmaya konu edilmesini istemiyor olabilecektir. Elde edilen görüntüler ilgili kişinin siyasi düşüncesini üçüncü kişilere açığa çıkarma amacıyla kullanılıyorsa bu durumda özel nitelikli verinin işlendiğinden bahsetmemiz mümkündür. Eğer böyle bir amaç bulunmuyor, veriler sadece güvenlik prosedürleri kapsamında izleniyor veya kaydediliyorsa özel nitelikli veri işlemenin söz konusu olmadığını söyleyebiliriz.

GVKT'nın 4. maddesinin 14. fıkrasında yapılan tanıma göre, biyometrik veri, özel teknik yöntemler kullanılmasıyla kişilere ait fiziksel, psikolojik ya da karakteristik veriler üzerinden o kişiyi teşhis edebilmeye yarayan verilerdir⁵⁷⁷. Bir verinin biyometrik veri olarak tanımlanabilmesi için verinin, özel teknik yöntem kullanıldıktan sonra o kişiyi işaret etmesi gereklidir. Böylece kişinin yüzünün, vücudunun ya da yürüyüşünün görüldüğü sıradan bir kamera kaydının biyometrik veri sayılmayacağı söylenebilecektir. Bu kamera kaydına biyometrik veri denilebilmesi için, “ *böyle bir tanıma sistemine özgü olarak hazırlanmış veri bulunması (parmak izi, retina kaydı, biyometrik ses ya da görüntü kaydı) veya bunları tanıyan bir sistemde işlenmesi (özel bir biyometrik kayıt yapılmaksızın çalışan biyometrik yüz yanına sistemleri) gerekir.*”⁵⁷⁸ Bugün herhangi bir fotoğrafçıda çektilen normal vesikalık fotoğraf ile pasaport ya da vize başvurusunda kullanılan biyometrik fotoğraf arasındaki fark tam olarak bu ayrımı ortaya koymaktadır. Yukarıdaki örnekte siyasi partinin toplantısına katılan bireyin biyometrik görüntü kaydına alındığını düşünürsek, toplantı sırasında kayda alınan görüntüleri veri kategorizasyonu açısından hem biyometrik veri hem de siyasi düşünce bilgisi olarak

⁵⁷⁶ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 407.

⁵⁷⁷ GVKT md. 4/14. madde metninde biyometrik verilere örnek olarak yüz görüntüsü ve parmak izi dayanarak kimlik belirleme yöntemi olan daktiloskopi gösterilmiştir.

⁵⁷⁸ Murat Volkan, DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 181

nitelendirilebilecektir. Ancak uygulamada bu verilerin işlenmesi için alınacak tedbirler ve güvenlik önlemleri aynı olacaktır.

Nitekim, yasal düzenlemelerde ilgili verinin kategorizasyonunu yapmak ya da sınırlı olarak saymak, veri türleri arasındaki geçişkenliği azaltmamaktadır. Normalde biyometrik işleve sahip bir kamera olmaksızın kayıt altına bir fotoğraf ya da video kaydı özel nitelikli olmayan veri sayılmaktadır. Ancak, siyah tenli bir insanın fotoğrafları ten rengi ve ırkı, etnik kökeni hakkında insanlara bilgi verebileceğinden, söz konusu fotoğraflar özel nitelikli veri olarak değerlendirilip değerlendirilmeyeceğinin titizlikle tespit edilmesi gereklidir. Bu örneğin kaynağını İngiltere’de görülen Naomi Campbell MGN Limited’e karşı davası oluşturur. Mahkeme tarafından, Naomi Campbell’in bağımlılığa karşı destek almak için katıldığı bir etkinlikten ayrılırken çekilen fotoğraflarının niteliğine ilişkin olarak, Naomi Campbell’in ulusal ve uluslararası düzeyde ünlü bir manken olarak gittiği her yerde hakkında haberlerin çıktığını, ayrıldığı toplantının toplum gözünde saygı duyulan bir dernek olduğu, davacının aslında gizlice fotoğraflarının çekilmesine karşı çıkmadığını, fotoğrafların yine de ırksal kökene dair bilgi barındırdığını fakat fotoğrafların yayınlanma amacı göz önüne alındığında bu durumun önem teşkil etmediğini ve çekilen fotoğrafların hassas veri olarak kabul edilmeyeceğini belirtmiştir. Fakat buna karşılık aynı kararda, Narcotics Anonymus adlı dernekte alınan tedaviye ilişkin bilgileri ise fiziksel ve zihinsel sağlık durumuna ilişkin bilgi olarak değerlendirip, bu verileri özel nitelikli olarak kabul etmiştir⁵⁷⁹. Yani Mahkeme tarafından ırksal köken bilgisinin ayrımcılık gerçekleştirilmesi amacıyla kullanılmadığı ancak sağlık durumuna ilişkin bilgilerin bu amaçla kullanıldığı değerlendirilmiştir.

Biyometrik tarayıcıların kullanımlarının artması bireysel mahremiyet alanında bir takım düzenlemelerin yapılmasını gerektirmektedir. 2018 yılında Microsoft tarafından yapılan çağrıda, yüz tanıma teknolojilerinin yasal bir düzenleme ile yapılması teklif edilmiştir. Bu bilinç sonucunda son dönemde, fotoğraflar üzerinden yüz tanıma kullanan ya da çalışanlarının parmak izleri üzerinden biyometrik tarayıcı kullanan bir çok şirket aleyhine davalar açılmıştır⁵⁸⁰. Kişisel Verileri Koruma Kurulu tarafından iki spor merkezi hakkında verilen biyometrik verilerin işlenmesine dair ihlal kararı bulunmaktadır. Bu karara göre, Kurum biyometrik verinin özel nitelikli kişisel veri olduğunu ve GVKT kapsamında “yüz görüntüleri veya daktiloskopik

⁵⁷⁹ Cemil KAYA, Hassas (Kişisel) Veriler, s. 322.

⁵⁸⁰ Matthew B. KUGLER, “From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms”, UC Irvine Law Review, C. 10, S. 1, Y. 2019, s. 108.

veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler” olarak tanımlandığını, GVKT’nın gerekçesinde ise biyometrik verilerle ilgili açıklamalara yer verildiği ve fotoğrafların işlenmesinin doğrudan biyometrik veri olarak nitelendirilemeyeceği, yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde, bu verilerin biyometrik verilerin tanımı kapsamında kabul edileceği açıklamalarına yer verildiği görülmektedir. Kurum burada yapılan faaliyetin özel nitelikli kişisel veri işlendiği olduğunu kabul ettikten sonra, spor salonuna giriş yapmak gibi bir amaç için bu kadar hassas bir verinin toplanmasının Kanun’un 4. maddesinde yer aşan ölçülülük ilkesine aykırı olup olmadığını değerlendirmiştir⁵⁸¹.

Ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği vurgulanarak, dikkate alındığında spor salonuna giriş için bu iki spor tesisi tarafından uygulanan “el ve parmak izi taraması” sisteminin, hizmetten faydalanmak için zorunlu ve tek yol olarak üyelere sunulmasının, kişisel verilerin işlenmesinde ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olarak değerlendirilmemiştir.

Kurum bu kararı verirken Danıştay’ın 2014/2242 Esas sayılı, 2014/4562 Esas sayılı kararlarında belirttiği şekilde, “parmak izi ya da yüz tarama sistemi gibi biyometrik yöntemlerin, kamusal alan da olsa “özel hayatın gizliliği” ilkesi kapsamında bulunduğu ve toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmadığı göz önünde tutularak hukuka aykırı bir işlem olarak değerlendirildiği”ne ilişkin yorumlarını da incelemiştir.

⁵⁸¹ Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti. <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165>, (s.y. 01 Kasım 2021); Danıştay kararları için bkz. D.15.D, E.2014/4562, k.t. 11 Eylül 2014; D.İd.D., E.2014/2242, k.t. 9 Aralık 2015.

2. Özel Nitelikli Kapalı Devre Kamera Görüntülerinin Korunmasına İlişkin Tedbirler

Özel nitelikli kişisel verilerin diğer verilere göre korunmaya daha fazla ihtiyaç bulundukları ve bu veri türünün kendine özgü bir işleme ve korunma rejimine sahip olduğu açıktır. Buradaki temel amaç, kişisel verileri korunan kişinin temel hak ve özgürlüklerinin etkin bir şekilde korunmasının tesisinin sağlanarak, ayrımcılığa uğrama ihtimalini bertaraf etmektir. Önceleri veri koruma hukuku açısından “genetik veriler” ve “biyometrik veriler”in, sağlık verileri içerisinde yer alan alt veri grupları olarak değerlendirildiğini, fakat sonrasında teknolojinin de gelişmesiyle günlük yaşam içerisinde daha fazla kullanılır hale gelen bu veri türlerinin kendilerine has veri grupları oluşturdukları kabul edilmiştir⁵⁸². Gerçekten de her iki grup verinin de özellikle teknik bilgiyle ulaşılır olmalarından ötürü bu şekilde bağımsız kabul edilmeleri yerinde gözükmemektedir. Örneğin, Bankalar, Finansal Kiralama, Faktoring ve Finansman şirketlerinin dijital kanallar üzerinden müşterileri ile yüz yüze gelmeden mesafeli olarak kimlik tespiti yapılması suretiyle düzenledikleri sözleşmeleri dijital sözleşmeler şu an finansal sektörün olmazsa olmaz bir parçasıdır⁵⁸³.

Dijital sözleşme kavramına ilişkin kanunda açık bir tanım olmasa da, 5411 Sayılı Bankacılık Kanunun 76. maddesinin 2. fıkrasını değiştiren 18/06/2020 tarihli 7247 sayılı Kanunun 6. maddesi lafzı doğrultusunda aşağıdaki tanıma ulaşmak mümkündür⁵⁸⁴. Buna göre, uzaktan iletişim araçlarının kullanılması suretiyle mesafeli olarak ya da mesafeli olsun olmasın BDDK’nın yazılı şeklin yerine geçebileceğini belirlediği ve bir bilişim veya elektronik haberleşme cihazı üzerinden gerçekleştirilecek ve müşteri kimliğinin doğrulanmasına imkân verecek yöntemler yoluyla kurulacak sözleşmeye dijital sözleşme denilmektedir. Dünyadaki uygulamalarına bakıldığında uzaktan kimlik tespitiyle müşteri ediniminde (digital onboarding) ağırlıklı olarak video konferans yöntemi, dijital kimlik ya da e-kimlik kartı kullanımı ve her

⁵⁸² Cemil KAYA, Hassas (Kişisel) Veriler, s. 320.

⁵⁸³ Son dönemde küresel ölçüde etkisini gösteren salgın, internet erişiminin kolaylaşması ve teknolojik gelişmeler, her geçen gün sisteme dahil olan yeni dijital uygulamalar, finansal kuruluşların piyasaya ulaşım kanallarını güçlendirmesini ve mevcut iş modellerinde değişikliğe gitmeyi zorunlu hale getirmektedir. 18 Haziran 2020 tarihli Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun ile Bankalar, Faktoring ve Finansman şirketleri, uzaktan erişim vasıtasıyla müşterinin merkez ya da şubeye gelmesine gerek kalmaksızın, faktoring ve finansman sözleşmelerinin kurulması gibi süreçleri dijital ortamda yürütebileceklerdir.

⁵⁸⁴ 26/06/2020 tarihinde Resmi Gazete’ de yayınlanarak yürürlüğe giren, 18/06/2020 tarihli 7247 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun, <https://www.resmigazete.gov.tr/eskiler/2020/06/20200626-1.htm> (s.y. 15 Ekim 2020).

birinin tamamlayıcısı olarak üçüncü tarafa güven ilkesiyle ilerlendiği görülmektedir. Bu uygulamalar ile birlikte finansal kuruluşlar, şubelerine yönlendirmeksizin müşterilerinin kimliğini uzaktan kimlik tespiti yöntemleri (video konferans, görüntülü kimlik tanıma sistemleri, elektronik imza, biyometrik özellikli kimlik kartları vb.) ile tespit edebilecek ya da bunu yapmak için, söz konusu müşterilere daha önce kimlik tespiti yapmış başka bir bankadan (açık bankacılık servisleri aracılığıyla) hizmet alabileceklerdir.

Öyleyse, kişilerin biyometrik verilerin işlenmesi suretiyle banka hesaplarına ulaşmaları, para transferlerini yönetmeleri gibi işlemleri gerçekleştirebilmeleri finansal açıdan da önemli olduğu için yüksek düzeyde bir korumanın sağlanması gereklidir. Yüz tanıma, retina tarama ya da kimlik tespitini sağlayan diğer biyometrik verilerin, diğer veri türlerine göre üst düzey tedbirlerle korunması yerinde görülmektedir. Nitekim 2006 yılında İngiltere’de gerçekleştirilen bir araştırmaya göre, ABVKY ya da 1998 yılında çıkarılan İngiliz Veri Koruma Kanunu’na göre, özel nitelikli veri olarak sayılmayan “finansal veriler” in ankete katılanlar tarafından özel nitelikli olarak görüldüğü ortaya konulmuştur⁵⁸⁵. Bu durum hem finansal verilerin hem de finansal verilere erişmekte kullandığımız biyometrik verilerin önemini bizlere göstermektedir.

KVKK’nın “*özel nitelikli kişisel verilerin işlenme şartları*” başlıklı 6. maddesinin 2. fıkrasına göre, “*Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.*” Kanunun düzenlemesine göre, özel nitelikli kişisel verilerin kural olarak, işlenmeden önce ilgiliden açık rıza alınması zorunluluk olduğu söylenebilir. Bu zorunluluk aynı zamanda doktrinde “*kesin işlem yasağı*” olarak da ifade edilmiştir⁵⁸⁶. Aynı maddesinin 3. fıkrasında ise, “*Birinci fıkrafta sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.*” denilerek, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, sadece belirtilen amaçlar dahilinde, ilgilinin açık rızası olmaksızın işlenebileceği öngörülmüştür.

⁵⁸⁵ Nitekim anket sonuçları incelendiğinde görülecektir ki, finansal veriler ankete katılanların yüzde 88’i tarafından özel nitelikli kişisel veri sayılırken, sağlık verileri katılanların yüzde 72’ si tarafından özel nitelikli veri olarak görülmektedir. Bkz. Cemil KAYA, (Avrupa Birliği) , s. 320.

⁵⁸⁶ Sevgi TÜRKMEN, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, (Yüksek Lisans Tezi), İstanbul 2019, s, 93.

KVKK kapsamında özel nitelikli kişisel verilerin korunması ile özel nitelikli olmayan kişisel verilerin korunmasında belirtilen açık rıza kavramı tam olarak aynı kavramı karşılamaktadır. Bu açıdan herhangi bir videoya kaydına konu olacak kişiden alınan açık rıza ile biyometrik görüntüleri içeren bir video kaydına konu kişiden alınacak açık rıza büyük ölçüde benzer olacaktır⁵⁸⁷. Buradaki fark, sadece verinin niteliğine ve işleme prosedürlerine ilişkin olmaktadır. Yani alınacak rıza öncesinde ilgili kişiye yönelik bilgilendirme yapılırken, işlenecek verinin ve özel nitelikli olduğundan dolayı alınacak önlemlerin ve tedbirlerin niteliği değişeceğinden bunlar konusunda ilgili kişinin bilgilendirilmesi gerekecektir.

Bu kategori altında yer alan verilerin işlenmesi açısından Kanun tarafından ikili bir ayrıma gidilmiştir. İlgili düzenlemeye göre, sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde, ilgili kişinin açık rızası aranmaksızın işlenebilecek iken; sağlık ve cinsel hayata ilişkin veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilecektir.

Özel nitelikli kişisel verilerin genel nitelikli kişisel verilere göre daha güçlü korunması ilkesi açısından baktığımızda KVKK'nın 6/3. maddesinde yer alan açık rızaya ilişkin “kanunlarda öngörülen haller” istisnasının yerinde olmadığını görmekteyiz. Özel nitelikli olmayan veriler açısından Kanun 5. maddesi “*kanunlarda açıkça öngörülme*” durumunu açık rızanın istisnası olarak düzenlemiş olduğu görüldüğünde, özel nitelikli verilere de en azından aynı statüde bir korumanın getirilmesi beklenebilirdi⁵⁸⁸.

Her ne kadar hukuk sistemimiz içerisinde doğrudan uygulanması mümkün görülme de Kolluk ve Ceza Adaleti Direktifi'nin içerisinde özel nitelikli verilere ilişkin bir takım düzenlemeler bulunmaktadır⁵⁸⁹. Bu Direktif'in 10. maddesinin 1. fıkrasına göre, özel nitelikli kişisel veriler; AB hukuku yahut üye devlet hukukunun izin verdiği hallerde, veri sahibi yahut

⁵⁸⁷ DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 420

⁵⁸⁸ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 407.

⁵⁸⁹ Avrupa Birliği üyesi devletler arasında cezai konularda işbirliğine direkt katkı sağlayacak şekilde kişisel veri işlenmesi ve aktarılmasının, doğrudan bağlayıcı olmayan bir form ile korunması verilerin kullanım amacından kaynaklanmaktadır. “Polis ve ceza adaleti faaliyetlerinde veri işlemenin genel düzenleme olan GDPR yerine Kolluk ve Ceza Adaleti Direktifi ile düzenlenmesi bu alanın mahiyetinin sonucudur.” Bkz. Neslihan CAN, s. 37.

üçüncü kişinin hayati önemi haiz menfaatinin bulunduğu hallerde işlenebilecektir⁵⁹⁰. Bununla birlikte özel nitelikli kişisel verilerin temel hak ve özgürlüklerin korunması için güvencelerin sağlanması şartına bağlı olarak işlenebileceği de ifade edilmiştir. Burada sayılan güvenceler ise ek güvenlik önlemleri, organizasyonel yapının sağlanması, verilerin elektronik ortamda tutulması durumunda özel kriptografik yöntemlerin kullanılması, log kayıtlarının tutulması, veri işleme süreçlerinde yer alan kişilerin eğitilmesi ve ayrıca gizlilik artırıcı teknolojiler (Privacy-Enhancing Technologies-PETs) şeklinde tezahür etmektedir⁵⁹¹.

Son olarak belirtmemiz gerekir ki, Kanun tarafından özel nitelikli verilerin işlenmesi açısından yukarıda belirtilen düzenlemelerin haricinde, aynı zamanda Kurul tarafından belirlenen yeterli önlemlerin alınması da şart gözükmektedir⁵⁹². Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı bu konuda Kurul tarafından alınan ve uyulması gereken düzenlemelerden bir tanesini oluşturmaktadır.

3. Termal Kamera Görüntülerinin Kamu Sağlığı Amacıyla Kullanılmasının Değerlendirilmesi

Dünya Sağlık Örgütü tarafından küresel ölçekli bir pandemi olarak ilan edilen Covid-19 Pandemisi sürecinde bazı devletlerin, yerinden yönetimlerin veya şirketlerin termal kameralar vasıtasıyla kişisel veri işleme faaliyetlerinde bulundukları görülmüştür. Termal kameralar vasıtasıyla kişilerin vücut sıcaklıklarının ölçümünün yapılmasının, örnek olarak işyerinde çalışanlara veya bir toplu taşıma aracına binenlere zorunlu olarak şart koşulması, bu verinin temelde sağlık verisi olması nedeniyle hassas nitelikte olması, ayrıca kayıt altına alınıp alınmaması, kamu sağlığı gibi hukuki sebeplerle işlemenin hukuka uygun olup olmaması, sağlık yönünden insanlar arasında ayrımcılık yapılmasına sebebiyet verebileceği ve belki de bireylerin toplum hayatından dışlanmaları gibi farklı konular hakkında inceleme yapılması gerekecektir.

⁵⁹⁰ Kolluk ve Ceza Adaleti Direktifi, md. 10. f. 1.

⁵⁹¹ Neslihan CAN, s. 145.

⁵⁹² KVKK, md. 6/4.

Pandemi koşulları altında bireylerin termal kameralarla izlenmesi aynı zamanda, bu kişilerin sağlık verilerinin de işlendiği anlamına gelecektir. Sağlık verileri ise kişisel verilerin korunması hukuku açısından hassas veriler olup, diğer verilere göre korunmalarına ve mahremiyetine daha fazla dikkat edilmelidir⁵⁹³. Sağlık verilerinin işlenmesi tanı amaçlı, tedavi amaçlı araştırma ya da sağlık politikalarını belirlemek amaçlarıyla mümkün olabilecektir. Hastalara kişisel sağlık verilerine neden ulaşıldığını bakımından bilgilendirmede bulunulması gereklidir⁵⁹⁴.

Termal kameralar vasıtasıyla elde edilen sonuçlar eğer hastanelerde, havalimanlarında ya da işyerleri gibi yerlerde veri tabanlarında saklanıyorsa, arşivleniyorsa, diğer kurum ya da kuruluşlarla paylaşıyorsa bu gibi veri işleme faaliyetlerinin tamamının KVKK'nın 6. maddesine uygun olarak yapılması gereklidir. Sağlık verisi sayılan bu verinin kural olarak KVKK'nın 6/2 maddesi gereği, veri sahibinden alınan açık rıza ile işlenmesi gerekecektir. Ancak eğer anılan maddenin 3. fıkrasının 2. cümlesindeki hallerden bir tanesi bulunuyorsa açık rıza olmaksızın işlenmesi de mümkün olabilecektir. İlgili fıkra göre, *“Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.”*

Yukarıda yer alan şartlara bakıldığında, pandeminin kamu sağlığının korunması amacına yönelik olarak açık rıza olmaksızın veri işlemeyi sağlayan sebebi oluşturduğu söylenebilir. Ancak bu istisnai düzenleme içerisinde verileri kimlerin işleyebileceği de sayılmıştır. Bu kapsama giren kişilerin ilk olarak doktorlar olduğu doktorların yanı sıra eczacılar, ebeler ve bunların sağlık memuru ve hemşireler gibi yardımcılarının bu kapsama girdiğini söyleyebiliriz. Ayrıca Sağlık Bakanlığı, devlet hastaneleri, özel hastaneler, klinikler ve sair sağlık kuruluşları gibi kurum ve kuruluşları çalışanları için de aynı yorumu yapabilmek mümkündür⁵⁹⁵.

⁵⁹³ Sinan Sami AKKURT, Kişisel Sağlık Verilerinin İşlenmesi ve Covid-19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukuki Bir Bakış, İTÜSBD, Covid-19 Hukuk Özel Sayısı, 2019, s. 143.

⁵⁹⁴ Banu Fulya YILDIRIM, “Sağlığın Kişiselleşmesi ve Kişisel Sağlık Bilgi Sistemleri, Bilim Yönetimi Dergisi”, C.2, S.2, 2019, s.129

⁵⁹⁵ Buradaki maddeden farklı olarak GVKT içerisinde ise aynı durumda verilerin kimler tarafından işleneceğine yönelik olarak herhangi bir kısıtlama bulunmamaktadır. Bkz. Sinan Sami AKKURT, Kişisel Sağlık Verilerinin İşlenmesi, s. 150.

Burada değerlendirilmesi gereken bir husus da KVKK md. 6 f. 3 hükmü kapsamında, sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi için belirtilen amaç ve kişi şartlarıyla birlikte, diğer özel nitelikli veriler için aranan “kanunlarda öngörülme” şartının da aranıp aranmayacağıdır. Kanun’un düzenlemesine baktığımızda bu hususta bir kesinlik söz konusu olmadığı görülmektedir.

Dolayısıyla, KVKK md. 6 f. 3 düzenlemesine göre sağlık ve cinsel hayat dışındaki veriler için “kanunlarda öngörülme” şartının aranmış olmasından sonra, maddenin devamındaki cümlede sağlık ve cinsel hayata ilişkin veriler için farklı şartların öngörüldüğü yönünde bir yorum yapılması mümkündür. Buna göre, sağlık ve cinsel hayata ilişkin kişisel verilerin kanunlarda öngörülme dahi, KVKK m. 6/3’te sayılan amaçlarla ve kişiler tarafından işlenebileceği sonucu çıkmaktadır. Ancak bu durumun eleştirilere konu olduğu görülmektedir⁵⁹⁶. Çünkü sağlık ve cinsel hayata ilişkin verilerin işlenmesi için “kanunlarda öngörülme” şartının aranmaması, bu veriler bakımından amaçlanan korumanın zayıflamasına yol açacaktır⁵⁹⁷. Bu yönde bir işleme sağlık ve cinsel hayata ilişkin getirilen korumanın diğer özel nitelikteki verilere göre daha az olacağının öngörülmesi anlamına gelir ki, bu kesinlikle yanlış bir önerme olacaktır.

Öte yandan KVKK md. 6. f. 3.’ün lafzına bağlı kalarak ve ilgili maddeyi bir bütün olarak değerlendirerek özel nitelikli kişisel verilerin ancak kanunlarda öngörülen hâllerde işlenebileceği; sağlık ve cinsel hayata ilişkin verilerin ise ayrıca maddede belirtilen amaçlarla ve kişiler tarafından işlenebileceği yorumunu yapmak da mümkündür⁵⁹⁸. Kanaatimizce, yukarıda belirttiğimiz ilk görüşün savunulması yerinde olacaktır. Kanun kapsamında sağlık ve cinsel hayata ilişkin verilerin, diğer özel nitelikli verilerden ayrı işleme şartlarına tâbi tutulmuş olmasının sebebi korumanın zayıflatılması değil, aksine güçlendirilmesidir. Sonuç olarak bu madde kapsamındaki düzenlemede özel nitelikli kişisel veriler için getirilen koruma seviyesinin sağlık ve cinsel hayata ilişkin veriler bakımından daha da artırıldığının söylenmesi mümkündür.

Avrupa Veri Koruma Otoritesi (European Data Protection Supervisor - EDPS)’ne göre, tüm yüksek teknoloji ürünü ya da yapay zekaya sahip gözetim sistemleri uygulamaya

⁵⁹⁶ Canan İMANÇLI, Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu, İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi, On İki Levha Yayıncılık, İstanbul 2020, s. 128.

⁵⁹⁷ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 406.

⁵⁹⁸ Canan İMANÇLI, s. 128.

konulmadan önce veri etki değerlendirmesi yapılması gereklidir. Bu kapsama termal kameraların da gireceği söylenebilir. EDPS'nin getirmiş olduğu rehber mahiyetindeki Avrupa Veri Koruma Otoritesi Video Gözetim Kuralları⁵⁹⁹ doğrultusunda yapılacak bu ön değerlendirme açısından, termal kamera sistemleri ile kişisel verilerin işlenmesine henüz başlamadan şu hususlara dikkat edilmesi önemlidir. Bu değerlendirmenin kullanılacak farklı tekniklere, farklı amaçlara ya da lokasyonun özelliklerine göre ayrı ayrı yapılması gerekmektedir. Örneğin; yapay zeka algoritması kullanan bir termal kamera için algoritmanın, ölçümlerin daha sağlıklı yapılması için en doğru ölçüm değerlerinin ölçülebildiği alın ve göz kenarlarına odaklanacağı bilineceğinden, bu teknolojinin yüz tanıma teknolojilerine ilişkin ek veri koruma tedbirlerine bağlı olarak çalıştırılması gerekecektir.

Gözetim sistemleri faaliyetlerine başlamadan önce biyometrik verileri işleyip işlemeyeceğine ya da bu sistemlerin başka bir veri tabanına bağlı olup olmayacağına karar verilmelidir. Örneğin; kameralarda görüntülenen yüzlerin sisteme alınarak kimlik tanımlama sistemleri ile karşılaştırılması ya da araç kayıtlarının alınarak plaka veri tabanlarından kontrol edilmesi gibi⁶⁰⁰. Ayrıca her türlü dinamik önleyici gözetim (örneğin, önceden tanımlanmış şüpheli davranış, hareket, kıyafet, vücut diline dayalı otomatik uyarılar oluşturmak için otomatik davranış analizi yazılım uygulamalarının kullanılması), hareketli nesneleri veya insanları izleyebilen bir izleme yazılımı uygulamasıyla tamamlanmış bir kamera ağı, ses tabanlı uyarı sistemleri (ani bağırma gibi gürültü düzenlerindeki değişikliklerle tetiklenenler), kızılötesi veya yakın kızılötesi kameralar, termal görüntüleme cihazları ve karanlıkta veya düşük ışık koşullarında görüntüleri yakalayabilen, duvarların arkasını görebilen ve kıyafetlerin altında arama yapabilen diğer özel kullanımlı kameralar (örn. vücut tarayıcı) ve gelişmiş optik ve dijital yakınlaştırma özelliklerine sahip özel amaçlı kameraların barındırdıkları tüm bu yüksek teknoloji unsurları açısından kişisel verilerin işlenmesi amaçlarıyla kullanılmaları durumunda veri mahremiyetini ne ölçüde etkileyeceği hususunda kapsamlı araştırmalar yapılmalıdır.

⁵⁹⁹ Giovanni BUTARELLI, The European Data Protection Su Video-Surveillance Guidelines, 17 Mart 2010, https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf (s.y. 02 Nisan 2022)

⁶⁰⁰ Samuel J. HODGE, s. 58.

II. Karşılaştırmalı Hukukta Kapalı Devre Kameralar İle Gözetlenenlerin Kişisel Verilerinin Korunması

A. Karşılaştırmalı Hukukta Kapalı Devre Kameralarla Gözetimde Kişisel Verilerin İşlenmesi

Kamera kayıtları vasıtasıyla yapılan gözetim ile bireylerin mahremiyet alanlarına yapılacak herhangi bir saldırının önüne geçilebilmesi için bu alanın hukuk kuralları vasıtasıyla düzenlenmesine ihtiyaç bulunmakta olup bu bağlamda yapılan gözetimin hukuka uygun olarak yapılmasının sağlanması gerekmektedir. Bu düzenlemeler yapılan gözetimin türüne göre çeşitli ülkelerde farklı şekillerde tezahür etmiştir. Örneğin Kıta Avrupası hukuk sistemi içerisindeki bazı ülkelerde; gözetim sonucunda ortaya konulan kayıtların muhafaza sürelerine ya da gözetimin yapıldığına dair bireyleri bilgilendirmek için asılan işaretlerin nerede ve nasıl bulundurulması gerektiğine ilişkin detaylar ülkelerin iç hukuklarında açıkça düzenlenmiştir.

Kanada ve İtalya gibi ülkelerde, özel ya da kamu hukuku otoriteleri tarafından yapılan kamera gözetimini düzenleyen regülasyonların var olduğu, Fransa ve Çin gibi bazı ülkelerde ise bu konuda yasal düzenleme bulunmasına rağmen, bu düzenlemelerin daha fazla özel hukuk aktörlerinin gerçekleştirdiği kamera kayıt faaliyetlerine ilişkin olarak getirildiği görülmektedir⁶⁰¹. Ülkemizde ise bu konuya ilişkin olarak herhangi bir özel yasal düzenleme bulunmamaktadır.

Kıta Avrupası hukuk sistemine daha genel düzlemde bakıldığında ise karşımıza ilk olarak GVKT çıkmaktadır. Ancak GVKT içinde doğrudan bireylere ait kamera kayıtları ya da görüntüler açısından kişisel verilerin korunmasına ilişkin bir hukuki düzenlemeye yer verilmediğini, işlenen verinin özel nitelikli olup olmadığına göre ya da diğer tüm veri kategorileri için geçerli olan kuralların aynı zamanda kameralarla yapılan gözetim için de geçerli olduğunu söyleyebiliriz. Bununla birlikte, Avrupa hukuk sistemi içerisinde video kameralarla gözetime ilişkin bağlayıcı metinlerin başında 45/2001 sayılı “Bireylere Ait Kişisel Verilerin Topluluk Kurum ve Organları Tarafından İşlenmesi ve Bu Verilerin Serbest

⁶⁰¹ Mahmood Q. RAJPOOT, Christian D. JENSEN, Video Surveillance: Privacy Issues and Legal Compliance, V. Kumar, J. Svensson (Ed.), Promoting Social Change and Democracy through Information Technology, IGI Global, Y. 2015, s. 10.

Dolaşımına İlişkin Tüzük” gelmektedir. Bu tüzük doğrultusunda hazırlanan rehber kurallar uygulamaya ilişkin olarak önemli noktalara açıklık getirmektedir⁶⁰².

Kişisel verilerin korunması alanındaki ilk bağlayıcı düzenleme sayılan Avrupa Konseyi tarafından oluşturulan, AK 108 No’ lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi kurallarının ve GVKT’ dan önceki dönemde ABVKY’ nin belirli ya da belirlenebilir bireylere ait ses ve/veya görüntülerden oluşan video gözetimleri bakımından uygulanabilir olduğu konusunda herhangi bir tereddüt bulunmamaktadır⁶⁰³. Devam eden süreçte, Avrupa Konseyi tarafından gözetim tekniklerinden olan video gözetime dikkat çekilerek, tamamen bu amaçla oluşturulmuş bir heyete yetki verilerek, video gözetim hakkında rehber ilkeler oluşturulmasına karar verilmiştir. Sonuç olarak, toplamda 12 maddeden oluşan rehber ilkeler 2003 yılında Avrupa Komitesi Hukuki İşbirliği Komitesi’ nin 78. toplantısında yayınlanmıştır⁶⁰⁴.

Bununla birlikte, önceki bölümlerde açıkladığımız üzere kameralar yoluyla gözetimin bireylerin özel yaşamlarının gizliliği ve mahremiyetleriyle olan bağlantısı sebebiyle, Türkiye ya da diğer ülkelerde gerek Anayasal mevzuat ile gerekse de diğer kanun hükümleriyle bu alana ilişkin düzenlemelerin yapıldığı görülmektedir. Nitekim yine ülkemiz açısından KVKK’ nın bireylerin kişisel verilerinin korunması açısından bu alanda uygulama alanı bulduğu açıkça görülmektedir. Amerika’ da ise konuya ilişkin hukuki korumayı sağlayan düzenlemeler açıkça Anayasa’ da yer almasa da, bazı mahkeme kararlarında korumanın Anayasa’ da yer alan diğer haklara gönderme yapılarak sağlandığını görmekteyiz⁶⁰⁵.

Konuya Kanada ve Danimarka açısından baktığımızda ise; video gözetimin haberleşmenin gizliliğine ilişkin getirilmiş mevzuat içerisinde düzenlendiğini ve bu gözetimin bir takım kanuni şartlar dahilinde yapılabileceğini söylemek mümkündür⁶⁰⁶. Örneğin, haberleşmenin gizliliğine müdahale sayılacak bu video gözetim faaliyetine başlanmadan önce,

⁶⁰² Bkz. d.n. 600.

⁶⁰³ ABVKY’ nin video gözetim aracılığıyla kişisel verilerin işlenmesi durumlarında uygulanmayacağı istisnalar (Örneğin; kamu güvenliği, savunma, ulusal güvenlik gibi amaçlar dahilinde yapılan veri işleme etkinlikleri) için ayrıca bkz. “4/2004 of the Article 29 Data Protection Working Party on the Processing of Personal Data by means of Video-Surveillance, part 7 (E)”, s. 13, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf, (s.y. 30 Mart 2022)

⁶⁰⁴ “Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003)”, European Committee on Legal Co-operation (CDCJ), 20-23 Mayıs 2003, <https://rm.coe.int/168068416b>, (s.y. 30 Mart 2022)

⁶⁰⁵ Mahmood Q. RAJPOOT, Christian D. JENSEN, s. 11.

⁶⁰⁶ A.g.m., s. 11.

ilk olarak mahkemeden video kaydının süresinin belirtildiği, buna ilişkin bir kararın alınması zorunludur. Bu süre sınırı ceza soruşturmalarında daha uzun olabilir, örneğin üst sınırı 2 yıl veya daha fazla hapis cezası öngörülen bir suçun soruşturulması açısından mahkemenin verebileceği gözetim süresi, basit suçlardan ya da kabahatlerden daha fazla olabilecektir. Nitekim bu bakımdan 2002/58/AT sayılı Elektronik İletişim Yönergesi'nde belirtilen iletişimin gizliliğine ilişkin kuralların uygulanması gerekliliğinden ötürü ilgili bireyin rızası olmaksızın yapılacak herhangi bir gözetimde verilerin izlenmesi ya da kaydedilmesi için gerekli önlemlerin alınması bir zorunluluk olarak karşımıza çıkmaktadır⁶⁰⁷.

İngiltere'de de Amerika'dakine benzer şekilde Anayasa'da doğrudan özel yaşamın gizliliğini koruyan bir hüküm bulunmamaktadır. Haberleşmenin gizliliği açısından mahkeme kararına gerek bulunmamakta, yürütme erkinin yapılan gözetime onayı bu bakımdan yeterli görülmektedir. 2012 yılında yürürlüğe giren Özgürlüklerin Korunması Yasası'nın (Protection of Freedoms Act) verdiği yetkiye dayanılarak, 2013 yılında çıkarılan "Gözetim Kameralarına İlişkin Uygulama Kuralları"⁶⁰⁸ konuya ilişkin düzenleme yapsa da gözetim otoritelerinin kurallara aykırı davranmasını engelleyici bir bağlayıcılık ihtiva etmediğinden, sadece uygulamaya yol gösterici bir kurallar bütünü olarak kalmıştır⁶⁰⁹. Nitekim, uygulama kuralı madde 5. altında, İngiliz Veri Koruma Otoritesi ile işbirliği halinde faaliyet gösterecek bir Kamera Gözetim Otoritesi kurulması öngörülmüş olmakla birlikte, Kamera Gözetim Otoritesi'nin fonksiyonları olarak; bu kurallara uyulmasını teşvik etmek, bu kurallara uyulmasını denetlemek, kuralların uygulanması, değiştirilmesi ya da ihlali durumunda tavsiye sunmak sayılmıştır. İlgili kurumun fonksiyonları arasında herhangi bir cezai yaptırım müeyyidesinin yer almaması da bir eksiklik olarak değerlendirilebilir, ancak ICO'nun işbirliği dahilinde bu kurallara uyulmaması durumunda, ICO tabir-i caizse büyük kardeş olarak duruma müdahale ederek, gerektiğinde bu kurallara uyulmasını sağlayacaktır.

Gözetim Kameralarına İlişkin Uygulama Kuralları madde 2/6'da video gözetim kameralarının faaliyetlerine ilişkin aşağıdaki kurallar kabul edilmiştir:

⁶⁰⁷ 2002/58/AT sayılı AB Yönergesi, m.5.

⁶⁰⁸ Surveillance Camera Code of Practice, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf, (s.y. 06 Şubat 2021)

⁶⁰⁹ Mahmood Q. RAJPOOT, Christian D. JENSEN s. 13.

- 1) Kameralar her zaman, meşru ve spesifik bir ihtiyacın karşılanması için belirli bir amaç için kullanılmalı,
- 2) Kameralar kullanılırken bireylerin ve özel yaşamlarının üzerindeki etkileri dikkate alınmalı ve kullanımın meşruluğu düzenli olarak gözden geçirilmeli,
- 3) Kameralarla gözetim faaliyetlerinde şeffaflık sağlanmalı, erişim hakkı kapsamında bireylere şikayet ve bilgi taleplerini iletebileceği muhatap gösterilmeli,
- 4) Kamera gözetiminde yer alan tüm faaliyetler, toplanan, tutulan ve kullanılan görüntüler açısından sorumluluk ve hesap verilebilirlik söz konusu olmalı,
- 5) Gözetim faaliyetinin başlamasından önce, buna ilişkin politikalar, kurallar ve prosedürlerin belirlenmiş ve bunlara uymakla yükümlü olan ilgililere duyurulmuş olması gerekli,
- 6) Gerektiğinden fazla görüntü saklanmamalı, kullanım amacı yerine geldikten sonra görüntüler silinmeli,
- 7) Video görüntülerine erişimin kısıtlı olması, verilere kim ya da kimler tarafından ve hangi amaçlarla erişilebileceği açıkça belirtilmeli, ayrıca bu görüntülerin 3. kişilere açıklanması aynı amaçlar doğrultusunda ya da kanunun gerektirmesi halinde mümkün olabilmeli,
- 8) Kamera gözetim sistemlerinin teknik ve yeterlilik standartlarını sağlaması ve kullandıkları süre boyunca bu gereksinimleri karşılaması gerekli olmalı,
- 9) Kamera gözetim sistemleri yetkisiz erişim ve kullanıma izin vermeyecek güvenlik standartlarını sağlamalı,
- 10) Kanuni yükümlülüklerin, uygulama politikalarının ya da diğer standartların karşılanması için etkili inceleme ve denetim mekanizmaları bulunmalı, bu denetim sonucunda tutulan raporlar yayınlanmalı,

11) Kamera gözetim sistemleri meşru ve acil bir amaç doğrultusunda kullanılıyorsa, kanıt değeri taşıyan görüntüler açısından kamu güvenliği ve kolluk kuvvetlerinin desteklenmesi sağlanmalı,

12) Kamera gözetim sistemleri dahilinde kullanılan bilgi destek sistemlerinin, merkezi veri tabanı ile eşleştirilmesi açısından, doğru ve güncel olmaları gerekmektedir.

ICO tarafından yayınlanan ve video gözetiminde bir yol gösterici olan “Kamera Gözetimi Rehberi” (Guidance on Video Surveillance) 24 Şubat 2022 tarihinde güncellenmiştir⁶¹⁰. Kurum, rehberin önsözünde video kamera gözetiminin gerek kurulu gerekse de taşınabilir kameralar aracılığıyla özel teşebbüsler ve kamu kurum ve kuruluşları tarafından giderek artan ölçüde kullanıldığını, klasik kamera gözetiminin yerini yapay zeka teknolojilerine bıraktığını vurgulamıştır. Bu görüşüne paralel olarak rehberde yüz tanıma teknolojilerinin hangi sınırlar çerçevesinde kullanılabileceğine dair açıklamalar yer almış, ayrıca bu başlık altında yapay zekanın bu sistemin bir elementi olduğuna dikkat çekilmiştir⁶¹¹.

Rehberin bu bakımdan sunduğu bilgiler uygulama açısından çok önemli olabilecek niteliktedir. Öncelikle yüz tanıma sisteminin gerekli ve ölçülü olup olmadığı değerlendirilmesinin her olayın maddi özelliklerine yapılacağı vurgulanmış, yüz tanıma teknolojilerinin kullanılabileceği yerlerin ve senaryoların sınırlı olarak sayılmadığı belirtilmiştir⁶¹². Örneğin; alışveriş merkezlerinde bu teknolojinin kullanılmasının hukuka uygun ve amaca ulaşmak için gerekli olduğunun, ayrıca aynı amaca ulaşmak için kullanılabilecek daha az müdahaleci başka bir yol olmadığının açıkça ortaya konulması gerektiği vurgulanmıştır⁶¹³. Gerçekten de gerekmediği halde çok sayıda kişinin yüz bilgilerinin işlenmesi ve fakat bunlardan çok azının sadece gerektiğinde kimliklerinin tespit edilmesi bizce ölçülü bir uygulama olmayacaktır. Son olarak yüz tanıma sistemlerine bilgilerini sunmak istemeyen bireylerin zarara uğramamalarının sağlanması da gereklidir⁶¹⁴. Örneğin; belirli bir alana girmek için yüz tanıma bilgisinin zorunlu tutulması, bu bilgilerin işlenmesini istemeyen

⁶¹⁰ ICO, “Guidance on Video Surveillance”, <https://ico.org.uk/media/for-organisations/guide-to-dataprotection/key-dp-themes/guidance-on-video-surveillance-0-0.pdf>, (s.y. 30 Mart 2022)

⁶¹¹ A.g.i., s. 38.

⁶¹² A.g.i., s. 41.

⁶¹³ A.g.i., s. 42.

⁶¹⁴ A.g.i., s. 42.

bireyler açısından zarara sebebiyet verebileceğinden, alternatif giriş seçeneklerinin oluşturulması sağlanmalıdır.

Alman Federal Veri Koruma Yasası ise kamuya açık alanlardaki bireylerin video gözetimlerini düzenleyen açık hükümler içermektedir. BDSG' ye göre, *“görüntülerin işlenmesi ve kullanılması ancak belirli amaçlar doğrultusunda söz konusu olabilir. Kamusal alanlarda video gözetimine izin verilebilmesi, (i) kamusal görevlerin yerine getirilmesi, (ii) giriş-çıkış iznine sahip olanları saptama hakkı, (iii) açıkça tanımlanmış amaçlar doğrultusunda haklı çıkarların izlenmesi halinde olanaklıdır. Ancak bu durumda da bazı sınırlamalar söz konusudur. Öncelikle bu amaçlarla izleme ancak ilgili kişinin meşru haklarının üstünlüğüne ilişkin bir işaret yoksa söz konusu olabilir. İlgili kişi bilgilendirilmelidir. Ayrıca izlenen alan ve veri sorumlusunun kimliği uygun araçlarla görülebilir kılınmalıdır. Belirlenen amaç için gerekli olmaması ya da sonraki işlemler karşısında ilgilinin meşru çıkarlarının üstün gelmesi hâlinde veriler gecikmeksizin silinecektir.”*⁶¹⁵ İlgilinin meşru çıkarlarının ne olduğuna ilişkin yapılan örnek ise bir banka ya da petrol istasyonunda tutulan günlük kamera kayıtlarının eğer özel bir olayı göstermediği düşünülüyorsa anında silinmesinin gerekmesi iken; şayet bir suç soruşturmasının takibi açısından kaydedilen görüntülerin daha uzun tutulabilmesinin mümkün olmasıdır⁶¹⁶.

Bu konuya ilişkin bir diğer kaynağımız da 18 Aralık 2000 tarihli 45/2001 sayılı “Bireylere Ait Kişisel Verilerin Topluluk Kurum ve Organları Tarafından İşlenmesi ve Bu Verilerin Serbest Dolaşımına İlişkin Tüzük”tür. Söz konusu Tüzük kapsamında Avrupa Birliği kurum ve organları tarafından işlenen verilere ilişkin uyulması gereken kurallar ve yükümlülükler düzenlenmiştir⁶¹⁷. Tüzüğün 41. maddesinde öngörülen EDPS'ye ilgili Tüzük kapsamında getirilen kuralların uygulanıp uygulanmadığını izleme ve aykırı davranılması halinde 47. maddede belirtilen bir takım müeyyidelerin uygulanmasına karar verme yetkisi tanınmıştır. Tüzük kapsamında çıkarılan ek düzenlemelerden bir tanesi de 17 Mart 2010 tarihli Avrupa Veri Koruma Otoritesi Video Gözetim Kuralları'dır⁶¹⁸. Burada bahsettiğimiz kurallar dahilinde, video gözetime ilişkin “tasarımda gizlilik” ilkesinden, video gözetimin yerindeliğine,

⁶¹⁵ Elif KÜZECİ, Kişisel Verilerin Korunması, s. 512.

⁶¹⁶ A.g.e., s. 512.

⁶¹⁷ The EDPS: Supervising EU institutions and bodies & enforcing data protection principles, EDPS factsheet 3, European Data Protection Supervisor, https://edps.europa.eu/sites/edp/files/publication/factsheet_3_en.pdf, (s.y. 30 Kasım 2021)

⁶¹⁸ Giovanni BUTARELLI, The EDPS Video-Surveillance Guidelines.

kameraların kurulacakları alanları tespit etme esaslarından, kayıtların ne kadar süre için tutulacağına kadar kapsamlı ve çeşitli bilgilere yer verilmiştir. Bu kuralların aynı zamanda özel sektör aktörlerine örnek oluşturduğu ve GVKT kapsamında verilerin hukuka aykırı olarak işlenip işlenmediği değerlendirilirken, EDPS tarafından dikkate alınacağı göz ardı edilmemelidir.

Avrupa Veri Koruma Otoritesi Video Gözetim Kuralları'nın video telefon görüşmelerine, video konferanslara ya da kapı otomatiğindeki video kameralar gibi herhangi bir video kaydı yapılmayan sistemlere, bilimsel amaçlar için kurulan kontrollü alanlarda yapılan video kayıtlarına, artistik ya da habercilik amaçlı yapılan kayıtlara, konferans, seminer ya da toplantılarda alınan kayıtlara bu kuralların uygulanmayacağını açıkça belirtmiştir. Bununla birlikte, burada bulunan alanlarda yapılan kayıtlar için, eğer GVKT'da tanımlanan istisnalardan bir tanesi yoksa, GVKT'nın uygulama alanı bulacağı tartışmasızdır.

Kamera kayıtlarında açıkça tanınan ve bilinen bir kişiye ait yüz görüntüsünün olması şart olmamakta olup, başka bilgilerin de kullanılması suretiyle kamera görüntülerini ilgili kişiyle ilişkilendirmek mümkünse kişisel veri işlendiği kabul edilerek kuralların uygulaması mümkün hale gelecektir. Örneğin, nispeten yüksek bir konumda bulunan kameraya ilişkin kayıtların ceza soruşturmasında kullanılması sırasında, şüphelinin olay sırasında üzerinde yer alan kıyafetlerin, vücut ölçülerinin ya da kayıt sırasında elinde taşımakta olduğu beraberinde bulundurduğu cisimler üzerinden ilgili kişiyi belirleyebiliyorsa, o halde buradaki verinin o kişiye ait bir kişisel veri olduğu konusu tartışmasızdır⁶¹⁹.

Kamera gözetim sistemleri aracılığı ile veri işlenecek ise veri işleme amacının açık, belirli ve kesin olması ayrıca, bu amacın kamuya açıklanması gerektiği kurallar metninde belirtilmiştir. Genel ve kapsayıcı amaçlar, başlangıçta belirtilmeyen ve fakat sonradan ortaya çıkan kullanım amaçları ile veri işlemeyi hukuka uygun hale getiremez. Avrupa Veri Koruma Otoritesi Video Gözetim Kuralları md. 5.1.3'de açıkça belirtildiği üzere, belirli amaçlar için kaydedilen video kayıtlarının daha sonradan kullanılma ihtimaline dayanılarak tutulması yasaktır. Bu duruma ilişkin "işlev kayması" tabiri kullanılmış ve işlev kaymasının bu bakımdan yasak olduğu ayrıca ifade edilmiştir⁶²⁰. Dolayısıyla, işyerine güvenlik sebebiyle bir kapalı devre kamera gözetim sistemi kurduran işveren tarafından, çalışanlarına kameranın güvenlik

⁶¹⁹ The EDPS Video-Surveillance Guidelines, s. 9.

⁶²⁰ A.g.r., s. 17.

sebebiyle kurulduğunu bildirildikten sonra kamera kayıtlarının işçilerin performanslarının değerlendirilmesi amacıyla kullanılamayacağı açıktır.

Eğer kullanılacak video gözetim tekniği, güvenliğin sağlanması amacına yönelik olarak kurulmuşsa, bu durumda veri sorumlusunun güvenliğin sağlanması gerekçesine ilişkin riskleri değerlendirerek, açık bir şekilde bu gerekçenin içine hangi olası olgu ve olayların girdiğini de ortaya koyması gereklidir. Bu nedenle, veri sorumlusu ya da veri kontrolörü tarafından “güvenliğin sağlanması açısından tüm anomalilerin gözlenmesi” ya da “güvenlik gerekçesi ile her türlü olay ile ilgili” gibi açıklamalar dahilinde 3. kişilere yapılan bilgilendirmeler yahut bu tarz yüzeysel gerekçeler yetersiz sayılmaktadır. Doğal olarak herhangi bir işletme, kurum ya da kuruluşun kamera sistemlerinden faydalanmasının temel sebebi güvenliğin sağlanmasıdır, ancak bunu genel bir gerekçe ile yansıtmak yerine, bu gerekçe altında aslında hangi durumların ortaya çıkmasının beklendiği ve buna ilişkin güvenliğin sağlanmaya çalışıldığının ifade edilmesi beklenmektedir⁶²¹. Bu bakımdan örnek bir gerekçenin “kısıtlı ve güvenli özel mülk alanlarına yetkisiz fiziksel girişler”, “protesto ya da gösteriler sırasında binalara verilecek fiziksel zararın tespiti” ya da “çalışanların kişisel eşyalarına karşı hırsızlık tehlikesi” gibi güvenlik olaylarının engellenmesi şeklinde ayrı ayrı belirtilmesi yerinde olacaktır.

Video gözetim tekniklerinin kullanılması, güvenliğin sağlanmasını hem potansiyel faillerin tespit edilmesini kolaylaştırması hem de acil durum vakıalarına karşı hızlı müdahaleyi sağlaması açısından kolaylaştırmaktadır. Bir alanda kamera gözetimi yapılması, potansiyel failler açısından caydırıcılığı beraberinde getirmektedir. Bazı durumlarda ise video kameralar güvenliğin sağlanmasından çok suç işlendikten sonra suçun ve faillerin tespiti, delillerin tespiti işlevine hizmet etmektedir. Burada önemli olan bu şekildeki kullanımın sadece suç ya da haksız fiil teşkil eden bir olayın gerçekleşmesinden sonra söz konusu olabilecek olmasıdır⁶²².

Bunun tersine, örneğin şüphe dahilinde bir kasa görevlisinin zimmetine para geçirip geçirmediğini anlamak için işyerinde günlük hareketlerinin veri sorumlusu tarafından izlenmesi söz konusu olmamalıdır. Keza markette çalışan bir kasa görevlisinin mesai süresince sürekli olarak gözetlenmesi, kendisine bu bakımdan yeterli bilgilendirme yapılsa bile yerinde olmayacaktır. Böylesine bir gözetimin verinin işleme amacı bakımından “işlev kayması” yaratacağı söylenebilir.

⁶²¹ A.g.r., s. 21.

⁶²² A.g.r., s. 22.

Kameralar vasıtasıyla bireylere ait özel nitelikli kişisel verilerin işlenmesi bakımından en çok dikkat edilmesi gereken noktanın, görüntünün ya da video kaydının bireyi ayrımcılığa maruz bırakma potansiyelinin olup olmadığı hususu olduğundan bahsetmiştik. EDPS'ye göre, video gözetim sistemlerinin hedefleri özel nitelikli verileri işlemek olmasa da eğer gözetim yapılacak alanda yüksek ihtimalle özel nitelikli kişisel verilerin işlenmesi durumu söz konusu olma durumu varsa burada gözetim yapılmamalıdır. Ayrıca bireylerin yüzlerine ya da farklılıklarını yansıtacak yönlerine odaklanılmaması gerektiği de açıkça belirtilmiştir. Bu durumun istisnası ise, güvenliğin sağlanması amacıyla gösteriler sırasında kamu güvenliğine karşı tehdit, saldırı ya da vandalizm tehlikesi yaratılması durumu olarak karşımıza çıkmaktadır. Eğer bu durumlardan biri söz konusu ise kameralar bireylerin yüzlerine kimliğin tespiti açısından odaklanabilir ya da onu diğerlerinden ayıran özelliklerine odaklanabilir⁶²³.

Kayıtların muhafaza edilme süresi açısından genel kural, kayıtların belirlenen işleme amacı için gerekli olduğu süre kadar muhafaza edilmesidir, ancak kamera kaydına başlanmadan önce henüz ilk aşamada kayıt tutulmasına gerek bulunuyor mu yoksa kayıtsız sadece izleme yoluyla gözetim belirlenen amacı gerçekleştirmeye yeterli mi bu sorunun cevaplanması gerekir. Eğer sadece anlık gözetim belirlenen amacı gerçekleştirmeye yetiyorsa, ölçülülük ve veri minimizasyonu ilkesi de göz önünde bulundurularak kamera kaydı tutulmaması yerinde olacaktır.

Özel işletme ya da kamu kurumu ayrımı yapılmaksızın, bu işletmelerin kamera gözetimlerinde kayıt altına aldıkları kayıtların imha süreleri bakımından Veri Koruma Çalışma Grubu özellikle belirtmektedir ki, eğer kayıt tutmadan izlemek yeterliyse bu şekilde gözetleme yapılması gerekir, ancak bu mümkün değilse kayıtların birkaç saat için tutulması ve sürenin dolmasıyla birlikte silinmesi, bilhassa ertesi güne bırakılmaması ya da en azından haftanın sonunda silinmesi gerekmektedir. Bu durumun istisnası polis ya da yargı erkinin bu konudaki kararları oluşturur, ancak bu durumda daha uzun süre kayıtların muhafazası mümkün olabilir. Danimarka ve İsveç Veri Koruma Kurumları video kayıtlarının yalnızca kısa bir süre için muhafaza edilebileceğini ve bu sürenin 30 günü aşmayacağını açıkça belirtmişlerdir ancak, Çalışma Grubu yine de “ölçülülük” bakımından bu sürenin en fazla 1 hafta olabileceğini

⁶²³ A.g.r., s. 29.

söylemektedir⁶²⁴. Nitekim, Avrupa Veri Koruma Otoritesi de aynı görüşte olduğunu, zaten belirli bir soruşturmaya ya da şikayete bağlı talebin çoğu zaman kolluk tarafından saatler içerisinde geleceğini, bu bakımdan 7 günlük muhafaza süresinin hatta daha kısa bir sürenin dahi yeterli olacağını ifade etmiştir⁶²⁵.

Kapalı devre kameralar aracılığıyla yüz modelleri ve davranış modelleri gibi kişisel veriler işlenmekte ve yeri geldiğinde kaydedilmektedir. Kaydedilen bu verilerin saklanma süreleri dışında hangi güvenlik tedbirleri dahilinde korunduğu da önemlidir. Gözetim gerçekleştirilirken gizliliğin korunması konusunda geleneksel metotlar bulunmakla birlikte, RFID sistemlerinin bu geleneksel gözetim sistemine entegre edilmesi yoluyla kişisel verilerin güvenliği anlamında çok daha etkili bir teknik daha ortaya konulmuştur⁶²⁶. Keza bu güvenlik tedbirinin kötücül amaçlarla sisteme dışarıdan girişi engelleyecek yetkilendirme protokolleriyle güçlendirilmesi de mümkündür⁶²⁷. Bunlar güncel ve en gelişmiş yöntemler olarak görülebilir ancak diğer geleneksel koruma tedbirlerine de göz atmamız gereklidir.

CCTV'ler aracılığıyla gerçekleştirilen veri işleme faaliyetleri sırasında alınabilecek geleneksel veri koruma tedbirlerinden bir tanesi mozaikleştirme tekniği olarak karşımıza çıkmaktadır. Mozaikleştirilen bir görüntünün ifşası durumunda veri sahibi kişinin kimliği saklı kalmaktadır. Böylelikle görüntülerde yer alan bireylerin mahremiyetlerinin güvence altında olduğu kabul edilecektir. Verilerin korunmasına hizmet etmesi bakımından yerinde olan bu tekniğin olumsuz yönü ise bazı durumlarda görüntülerde birden fazla kişi bulunuyorsa ya da görüntü karmaşık ise hangi nesnenin mozaikleştirileceğini belirlemenin zor olmasıdır. Keza herkesin otomatik olarak mozaikleştirildiği bir gözetim sisteminin amacını tam olarak yerine getireceğini söylemek mümkün olmaz. Bu geleneksel metot içerisinde RFID teknolojisinin dahil olması da mümkündür. Böylelikle, hangi nesnelerin (insanların) gözetleneceği, kameralarla kayıt altına alınırken arka planda işletilen bir video görüntü işleme sistemi ve RFID teknolojisi dahilinde tespit edilecek ve aslında gözetlenmemesi gereken nesnelerin yüzleri doğrudan mozaikleştirilmiş halde ekranlara yansıyacaktır. Bu tekniğin görüntü sistemlerine

⁶²⁴ 4/2004 of the Article 29 Data Protection Working Party on the Processing of Personal Data by means of Video Surveillance, part 7(E), s. 20.

⁶²⁵ The EDPS Video-Surveillance Guidelines, s.33.

⁶²⁶ Hae-Min MOON, Sung Bum PAN, SSIRI 2009 Fast Abstract Implementation of the Privacy Protection in Video Surveillance System, Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009, s. 291.

⁶²⁷ Tae-Sung PARK, Moon-Seog JUN, User Authentication Protocol for Blocking Malicious User in Network CCTV Environment, 2011 6th International on Computer Sciences and Converges Information Technology (ICCIT), 2011, s. 18.

yansıyan yüzleri tanınamayacak şekilde işleme tabi tutması veri koruma hukuku açısından beklenen korumayı sağlamaktadır⁶²⁸.

GVKT'ya göre, video görüntülerine ilişkin olarak psödonimleştirme (takma ad kullanımı), şifreleme ve tasarımdaki gizlilik tedbirleri kapsamında bir takım veri koruma önlemlerinin alınabileceği ortadadır. Keza bu tedbirler KVKK kapsamında da alınması mümkün ve hatta gerekli olan tedbirlerdir. Psödonimleştirme, anonimleştirmeden farklı olarak belirli bir kişiye ait olan verinin geri döndürülemez şekilde anonim hale getirilmesini değil, sadece kişisel verinin işleme tabi tutulurken bu veriye bir unvan (takma ad) verilmesi anlamına gelir. Aradaki farkı İrlanda Veri Koruma Komisyonu'nun ifadesi ile belirtecek olursak, psödonimleştirilmiş veri üzerinden ilgili kişiyi tespit etme, veri ile veri sahibi arasında bağlantı kurma ihtimali bulunmaktadır⁶²⁹. Anonimleştirmede ise böyle bir ihtimalden söz edilmesi mümkün değildir.

Bu tekniklerin de ilerisinde olan bir takım başka güvenlik tedbirleri de söz konusudur. Video redaksiyonu denilen, video görüntülerinde yer alan kişilerin yüzlerinin ve kişiyi tanımlamaya yarayan diğer vücut işaretlerinin örneğin dövme, yara izi vb. bulanıklaştırılması faaliyetleri bu ileri tekniklerin bir tanesidir.

Bunların dışında birçok farklı teknik ile videolara yansıyan verilerin korunmasının sağlanması mümkündür. Bunlara örnek olarak pikselleştirme, maskeleye, morphing, scrambling ve tokenlaştırmayı gösterebiliriz. Pikselleştirme orijinal görüntüde yer alan piksellerin genişletilmesi yoluyla görüntünün bir nevi puslu hale getirilmesidir. Scrambling terimi ise görüntüdeki verinin permütasyonunun alınarak düzenli ya da düzensiz olarak yeniden şekillendirilmesidir. Tokenlaştırma ile görüntü pikselleri yerlerine gelecek sıradan sayılarla değiştirilmekte iken, morphing tekniği ile bu değişiklik doğrudan bir başka görüntü ile yapılır⁶³⁰. Morphing tekniğini, uygulamada görünmesi istenmeyen yüzün yerine, herhangi bir hayvanın yüzünün getirilmesi olarak örneklendirmek mümkündür. Tüm bu veri koruma

⁶²⁸ Bununla birlikt benzer amaçla piyasada bulunan JPEG 2000 adlı program ise ilgi alanı (ROI - Region of Interest) tekniğine göre görüntülerde yer alan bireylerin yüzlerini gizlemeyi başarmaktadır. Bu teknik görüntüye giren tüm alanları katmanlara ayırarak sadece ilgi alanlarının görüntülenmesine izin vermektedir. Bkz. Hae-Min MOON, Sung Bum PAN, s. 291.

⁶²⁹ Mamoon N. ASGHAR, Nadia KANWAL, Brian LEE, Martin FLEURY, Marco HERBST, Yuansong QIAO, Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective, IEEE Access, C. 7, Y. 2019, s. 15.

⁶³⁰ A.g.m., s. 18.

tedbirleri içerisinde puslulaştırma, pikselleştirme, mozaikleştirme, maskeleyme, morphing tekniklerinde bir kez uygulama yapıldıktan sonra verinin orijinal haline geri dönüş imkanı bulunmamakta, veriler anonim hale getirilmiş sayılmaktadır. Ancak scrambling ve tokenlaştırma tekniklerinde geriye dönüş ve ilgili verinin belirli bir kişiyle bağlantısının kurulması olanağı her zaman vardır⁶³¹.

Bulut sistemlerinin dijital gelecek içerisinde üstünlüğünü nasıl ilan edeceğini daha önceki bölümde açıklamıştık. Bu dijital hizmet sağlayıcı sistem, uzaktan erişilebilir olması nedeniyle mesafeye bağlı kalmaksızın verilerin aktarılmasını kolaylaştırmakta olduğundan bu sisteme entegre hizmetlerden gün geçtikçe daha çok sayıda insan yararlanmaktadır. Ancak bu durum bulut sistemleri hacker ya da siber korsanların hedefine haline getirmektedir. Netice itibarıyla, özellikle bulut tabanlı veri depolama alanlarının korunması büyük önem taşımaktadır. Bu nedenle, bulut tabanlı video depolama sistemleri üzerinde, veri koruma açısından daha etkin bir koruma sağlayan, video datalarının kendileri üzerinde bir şifreleme işlemi dahilinde bir abone anahtarı üretilerek saklanması tekniği geliştirmiştir. Bu uygulama dahilinde video verileri bir kere ilgili işleme tabi tutulursa hacklenmesi durumunda bile şifreleri çözülemeyecek ve veri koruma ihlallerine ve siber saldırılara karşı daha dayanıklı sayılacaktır⁶³².

Tartışılması gereken bir diğer husus ise kamera kayıt sistemlerine kimlerin ulaşabileceğidir. Öncelikle kamera sistemlerine ya da kayıt edilen görüntülere kimlerin erişim yetkisine sahip bulunduğu, erişim amaçlarının ve yetkilerinin nelerden oluştuğu tespit edilebilmeli ve bunların ilgili politika ve bilgilendirme metinlerde açıkça belirtilmiş olması gerekmektedir. Bu yetkiler kamera kayıtlarını gerçek zamanlı olarak izleme, kameraları yatay ve dikey hareket ettirme, yakınlaştırma, kayıtlı görüntüleri izleme, kopyalama, indirme, silme ve kayıt üzerinde değişiklik yapma yetkilerinden oluşmaktadır⁶³³. Yine veri koruma tedbirlerinin alınması açısından, yetkili kimsenin sadece kendisine tanımlı olan yetki çerçevesinde hareket etmesinin sağlanması için güvenlik standartlarının ve yazılımlarının işler halde bulundurulması gerekmektedir. Örneğin, görüntülerden kopya alma yetkisine sahip birinin sadece kendisine verilen şifre ile bu işlemi gerçekleştirebiliyor olması gerekmektedir.

⁶³¹ A.g.m., s. 18.

⁶³² Choi Il KANG, Lee Hee JUNG, BHUM Cheol LEE, " A Distributed Cloud based Video Storage System with Privacy Protection " *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, s. 834.

⁶³³ The EDPS Video-Surveillance Guidelines, s.36.

Yukarıda açıkladığımız üzere verilerin işleme amacı bakımından herhangi bir işlev kaymasının yaşanmaması, işleme sebeplerinin açık ve net olması son derece önemlidir. Bunun gibi kamera kayıtlarının veri transfer süreçlerinin de işleme sebebi ile bağlantılı şekilde açık şekilde ortaya koyulması elzemdir⁶³⁴. Şöyle ki, güvenliğin sağlanması amacıyla kaydedilen görüntülerin sadece bu amaçla kullanılacağı ve yine bu amaçlarla kolluk kuvvetlerine aktarılabilceğı, güvenlik kameralarına ilişkin politikalar dahilinde çalışanlara açıklanmışsa artık bu kayıtların işyerinde birlikte çalışan ve altında çalışanların işe giriş-çıkış saatlerini öğrenmek isteyen amire ya da üst düzey yöneticiye aktarılması yasak hale gelecektir. Bu gereklilik, veri güvenliğinin sağlanması ilkesi ile ilgilidir.

Avrupa Veri Koruma Otoritesi tarafından benimsenen görüş çok katmanlı bir yaklaşımı ifade etmektedir. Buna göre, kamuoyuna ya da 3. kişilere video gözetimi hakkında bilgi verilirken yapılan bilgilendirmenin etkili ve kapsamlı bir şekilde yapılması, yerinde bildirim ile o anda gözetim gerçekleştirildiğine ve gözetimin içeriğine ilişkin esaslı unsurlardan bireyin haberdar edilmesi (bu çoğu zaman resimler aracılığı ile yaratılan anlamlı işaret ve simgeler kullanılarak yapılan ikazlar tabelalarından oluşur) ve buna ek olarak kurum ya da işletmenin internet sitesinde daha ayrıntılı politikaların ve kuralların yayınlanması gerekecektir.

Yerinde bildirim yapılırken kullanılan resim ve işaretler dışında bir takım bilgilerinde bu ikazların içerisinde yer alması gerekmektedir. Bireylere Ait Kişisel Verilerin Topluluk Kurum ve Organları Tarafından İşlenmesi ve Bu Verilerin Serbest Dolaşımına İlişkin Tüzük'ün 12. maddesi altında düzenlenen bireylere sağlanması gereken bilgiler ve GVKT'nın 15. maddesi kapsamında sayılan ve erişim hakkı dahilinde veri sahibinin bilgilendirilmesi gereken hususların, burada da görüntüsü işlenen kişiye sağlanması önemlidir. Bu açıdan ilgililer tarafından kolaylıkla görülebilecek bir alanda yer alan ikaz tabelasında, kamera kaydına ilişkin bir işaretin yanı sıra en azından veri işlemenin amacı (örneğin güvenliğin sağlanması), kameraların izleme alanının neresi olduğu, kameralarla sadece anlık izleme mi yapıldığı, eğer kayıt tutuluyorsa ayrıca imha süresi belirtilmesi gerekli olup, diğer hususlar ve detaylı bilgilendirmeye internet adresi, telefon ya da e-mail adresi üzerinden erişim sağlanması yeterli olacaktır. Ayrıca gözetim yapılan yer eğer çok sayıda farklı ülkeden bireyin bir arada bulunma

⁶³⁴ A.g.i., s.39.

ihtimali olan bir yer ise, birden fazla dilde ya da en azından yerel dil dışında İngilizce olarak bilgilendirme yer alması uygun görülebilir⁶³⁵.

Mahkeme tarafından verilen karar hem 7 Aralık 2018 tarihinde İspanya Veri Koruma Yasası'nın yürürlüğe girmesinden sonra video kayıtlarının geçerliliğine ilişkin olarak verilen ilk karar olması sebebiyle hem de kararda yeni Veri Koruma Yasası'ndan ve GVKT'nin uygulanmasından bahsedilmiş olması önemlidir. Keza GVKT'nin yürürlüğe girmesinden sonra çıkarılan Veri Koruma Yasası çoğu yönden GVKT ile uyumluluk göstermektedir. AİHM tarafından verilen benzer bir kararda ise, gizli kameralarla kayıt altında bulunan işçiler bakımından, bu video gözetiminden haberdar edilmesi İspanya Veri Koruma Yasası tarafından öngörülmüş olduğu açıkça belirtilerek, buna uyulmamış olmasının doğrudan AİHS md. 8 kapsamında ihlal sayılacağını belirtmiş olduğunu görmekteyiz⁶³⁶.

Belirli bazı durumlarda, kapalı devre kamera sistemleri aracılığıyla gözetime başlanmadan önce kamu kurum ve kuruluşlarının ya da özel sektör temsilcisi veri sorumlusunun, düzenleyici ve denetleyici kurumdan izin alınması ya da belirli bir sicile kayıt olması zorunlu olmaktadır. Örneğin; İspanya'da gerek özel sektör işletmeleri gerek kamu kuruluşları kameralar ile gözetime başlamadan önce İspanya Veri Koruma Kurumu'na başvurarak yapılacak kamera gözetiminin diğer yöntemlere göre daha etkili olacağını ortaya koyarak, gözetimin meşru olacağını ispatlamak zorundadır⁶³⁷. Bu durumun ülkemizde de uygulamaya konulması, kapalı devre kamera sistemlerinin faaliyetlerine başlamadan önce veri koruma hukuku ilkeleri bakımından değerlendirilmesine olanak tanıyacağından yerinde olacaktır. Uygulama da böyle bir değişikliğe gitmek ilk bakışta zor gibi görünse de teşebbüslerin kameralar ile veri işlemeye başlamadan mahremiyet etki değerlendirmesi şeklinde bir rapor hazırlayarak bunu denetleyici kuruma sunması, denetleyici kurum tarafından ise veri koruma kriterlerine sahip teşebbüslere izin verilmesi hem bu alanda bir yeknesaklığın oluşmasına hem de bireylerin mahremiyet alanlarının belirli ölçüde koruma altına alınmış olmasına fayda sağlayacaktır.

⁶³⁵ A.gi., s.64.

⁶³⁶ Lopez Ribalda ve diğerleri, İspanya'ya karşı, b.n. 1874/13 ve 8567/13, k.t. 17 Ekim 2019.

⁶³⁷ Mahmood Q. RAJPOOT, Christian D. JENSEN, s. 11.

B. Yapay Zeka ve Kapalı Devre Kameralar

Makinelerin yapay zeka dahilinde derin öğrenme faaliyetlerini belirli bir yere kadar takip edip anlamlandırabiliyoruz. Ancak bu teknolojinin sınırlarına gelmek bir yana dursun, neredeyse daha çok başındayız. Bu bakımdan kişilerin mahremiyeti, verilerin korunması ve fiziksel bütünlük de yapay zeka ve robotik süreçlerin kuşatıcı entegrasyonundan etkilenmektedir. GVKT'nın getirdiği hukuk kaideleri kişisel verilerin korunması bakımından yeterli olacak mıdır? Yoksa yapay zekanın hukuk kuralları ile düzenlenmesi aslında imkansız mıdır? Öncelikle ifade etmemiz gerekir ki, yapay zekanın da dahil olduğu robotik süreçlere emanet edilen kişisel verilerin işlenmesi bir takım zorlukları beraberinde getirecek; orantılılık, ölçülülük ya da şeffaflık ilkesinin otonom (özerk) bir robotik süreç içerisinde dikkate alınması bir hayli zor olacaktır.

GVKT'nın içerisinde yapay zeka ya da robotik süreçlerin veri işleme faaliyetlerinde kullanılmasına ilişkin doğrudan bir düzenleme bulunmamaktadır⁶³⁸. Yapay zeka gibi önemli bir alanın Tüzük içerisinde açıkça düzenlenmemiş olması sorgulanabilir. Ancak diğer yünden Tüzük hükümleri uygulanırken sadece belirli bir teknolojiye bağlı kalmaması yani teknoloji geçirmez nitelikte olması faydalı olarak görülebilir. GVKT'nın genel ilkeleri arasında yer alan “teknoloji geçirmezlik” kapsamında gerçek kişilerin korunması ilgili dönemde kullanılan teknolojik tekniklere bağlı olmamalı, teknoloji geçirmez olmalıdır⁶³⁹.

Buna karşılık GVKT'nın 2. maddesinin 1. fıkrasında öngörülen “*Bu Tüzük, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır.*” hükmü gereğince, yapay zeka ve yapay zekaya entegre sistemler dahilinde işlenen kişisel veriler açısından GVKT'nın uygulama alanı bulacağı çıkarımında bulunabiliriz.

Bu açıdan; GVKT'nın yapay zekaya bakışına ilişkin Tüzüğün gerekçesinin 4. ve 78. maddelerinin değerlendirilmesi gerekebilir. Gerekçenin 4. maddesi kapsamında, kişisel verilerin işlenmesi, insanlığa hizmet etmek amacına ilişkin olarak tasarlanmalıdır. Kişisel

⁶³⁸ Robert van den HOVEN van GENDEREN, “Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics”, European Data Protection Law Review (EDPL), C. 3, S. 3, Y. 2017, s. 346.

⁶³⁹ Helena URSİC, “Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control.” SCRIPTed: A Journal of Law, Technology and Society, C. 15, S. 1, Y. 2018, s. 50.

verilerin korunması hakkı mutlak bir hak olarak görülmemeli; toplumdaki işlevi ile bağlantılı olarak, orantılılık ilkesi kapsamında değerlendirilmeli ve diğer temel haklarla dengelenmelidir. Bu bakımdan topluma hizmet etmek amacıyla robot geliştiren yapay zeka kullanımının ne kadar orantılı olacağını düşünmek gerekir.

Gerekçenin 78. maddesinde ise, kişisel verilerin işlenmesiyle ilgili olarak kişilerin hak ve özgürlüklerinin korunmasının gerekliliği, GVKT’da öngörülen gerekliliklerin yerine getirildiğini garanti altına almak için gerekli teknik ve organizasyonel önlemlerin alınması gerektiği düzenlenmiştir.

Nitekim GVKT’ya göre, yapay zeka teknolojileri açısından bireysel mahremiyet korunmasının sağlanması için veri minimizasyonunun sağlanması, verilerin muhafaza edildiği alanların gerekli korumaya sahip olması ve tasarımda gizlilik ilkesine uygun olarak veri koruma ilkeleri doğrultusunda hareket edilmiş olması gerekmektedir. Ancak her ne kadar burada belirttiğimiz önlemler alınsa bile yine de bu gizlilik probleminin tam anlamıyla çözüldüğünü söylememiz de mümkün olmayacaktır. Çünkü yapay zekayla desteklenen yüz tanıma sistemleri bireyleri yüz bilgilerine, dış görünüşlerine, cinsiyetlerine ya da fiziksel semptom gösterip göstermediklerine göre sınıflandırarak, insanlar arasında belirli seviyede bir ayrımcılığa sebep olabilecektir. Örnek olarak, bir oyuncak mağazasında bulunan beyaz ten renkli bir çocuk ile aynı yaştaki siyah ten renkli bir çocuğa farklı reklamların sunulabileceğini düşünmek mümkündür. Sadece dış görünüş kapsamında bu şekilde bir ayrıma izin verilmesinin doğru olmayacağını söyleyebiliriz.

Reklam panolarının, kişilere özel içerikler üreterek bunları ilgililerin karşısına çıkardığını ve bu kapsamda verilerin anlık olarak kullanıldığını, gerçek zamanlı olarak veri işleme yapıldığını önceki bölümlerde belirtmiştik. Veri mahremiyeti açısından veri işlemenin anlık gerçekleştirilmesi ve sonradan kullanılmak üzere veri toplanmıyor olması önemli bir gelişme olarak görülebilir. Ancak diğer bir çekince de bu veriler üzerinden kimlik belirlemenin mümkün olup olmadığıdır. Eğer reklam panolarının bu değerlendirme kapsamında belirli ya da belirlenebilir bir kimseye ait görüntüleri işlediği söylenebilecek ise mahremiyet sorunu devam edecektir. Tanımlanabilir olma kriteri bakımından 29 No’lu Çalışma Grubu’nun yapmış olduğu nitelendirmeye göre; belirli bir kişi ancak belirli grup içerisinde, grubun diğer üyelerinden ayrıldığı zaman tanımlanmış sayılmaktadır. Örneğin; yaya yolundaki trafik ışığında bekleyen “siyah takım elbiseli adam” olarak nitelendirdiğimiz bireyin tanımlanmış olduğu

söylenbilir⁶⁴⁰. Yapay zekayla çalışan yüz tanıma teknolojisi barındıran reklam panoları her ne kadar yukarıda belirtildiği üzere gelecekte kullanılmak üzere kayıtlansa da anlık veri işleme aşamasında bireyleri tanımlamaktadır. İlgili veri işleme faaliyetinin çok işlek bir alanda sürekli olarak yapılması; ayrıca verisi işlenen kişiler arasında çocukların da olması gibi durumların veri koruma bakımından mahremiyet sorunları doğuracağı açıktır.

Tüm bu açıklamalar ışığında çeşitli uygulama ve hizmetlerin sağlanması, ürün geliştirilmesi alanlarında yapay zeka uygulamaları tarafından kişisel verilerin işlenmesi durumlarında GVKT’de yer alan veri koruma hukuku düzenlemelerin uygulanmasının mümkün olacağını söylememiz mümkündür. Fakat yukarıdaki örnekte bulunan çocuklara ait kişisel veri işleyen sistemlerin ya da derin öğrenme temelli yapay zeka uygulamaları açısından ise en gelişmiş veri koruma tedbirlerinin bile yetersiz kalma ihtimali bulunabileceğinden⁶⁴¹ daha yüksek seviyede bir takım tedbirlerin alınması gerekmektedir.

Yüz tanımlama sistemlerinin bireysel mahremiyet alanında yaratacağı riskleri somutlaştıran bir örnek olarak hem Avrupa hem de Amerika’da kullanılan bir program olan Clearview AI’ı ele alabiliriz. Amerikan kolluk kuvvetleri tarafından da kullanılan bir yüz tanımlama programı olan Clearview AI içerisinde kullanılan yazılım dahilinde tüm internet ağları içerisinde kamuya açık olan fotoğrafları (örneğin; Facebook, Twitter, Youtube vb. de dahil olmak üzere) tarayarak, bu fotoğrafları tek bir veri tabanına aktarmaktadır. Programın ilgi alanına giren görüntülerin kamuya açıklığı üzerinde bir tartışma söz konusudur. Bu bakımdan bir kimsenin kendi fotoğrafını ilgili sosyal medya hesabına ya da internet ortamına yüklemesi sırasında bu fotoğrafın kamuya açık hale gelmesine rıza göstermiş olduğu ve kendi rızasıyla ifşa etmiş olduğu varsayılabilir ancak bireyin kendisinin de içinde bulunduğu toplu bir fotoğrafın internete yüklenmesinde aynı rızanın gösterilmiş olduğunu varsaymamız mümkün olmamaktadır. Burada kesinlikle bireye ait verinin paylaşılmasında açık rızası bulunmamaktadır⁶⁴². Bu bakımdan Patel ile Facebook arasındaki yargılamanın değerlendirilmesi uygun olabilir⁶⁴³. Davacı, Facebook aleyhine açtığı davada, etiket önerileri özelliği kapsamında yüz tanıma teknolojisinin hukuka aykırı olarak kullanıldığını iddia etmiştir. Facebook tarafından yapılan savunmaları yetersiz bulan Mahkeme ilgili kararında, şirketin

⁶⁴⁰ Peter Alexander EARLS DAVIS, s. 376.

⁶⁴¹ Robert van den HOVEN van GENDEREN, s. 346.

⁶⁴² Emmanuel, A. P. JIMENEZ, s. 1873.

⁶⁴³ Patel Facebook’a karşı, No. 18-15982, d.t. 08.08.2019.

müşterilerinin yüz şablonlarının yaratması, kullanması ve muhafaza etmesinin, bu verilerin kullanımlarının bir kez oluşturulduktan sonra sınırsız olabileceği, her gün sisteme dahil olan milyonlarca insanın bu şekilde veri işlemeye maruz bıraktığı şeklinde değerlendirmelerde bulunmuştur. Sonuç olarak taraflar 30 Ocak 2020 tarihinde taraflar bu uyuşmazlığın çözümü için uzlaşma yoluna gitmişlerdir⁶⁴⁴.

Yukarıdaki paragrafta belirtilen kolluğun kullanmakta olduğu yüz tanımlama yazılımı olan Clearview, 2019 yılı sonrasında Avrupa'daki kullanımı yaygınlaşmaya başlamıştır. Bu program dahilinde toplanan veriler, kolluk kuvvetlerinin kullanımı için toplanma amacından farklı bir şekilde, başka bir amaçla daha kullanılmaktadır. Clearview standart yüz tanıma araçlarından çok daha ötesinde bir faaliyet sunmaktadır. Sıradan yüz tanıma teknolojileri bu sistemi kendi sınırlı veri tabanları ile yapabilirken, Clearview ise global internet ağını veri tabanı olarak almakta ve eşleştirmelerini 3 milyarın üzerinde bir kaynak arasında yapmaktadır.

Aslında Clearview tarafından yapılan veri toplama tekniğini aynı zamanda “veri kazıma” olarak da nitelendirmemiz mümkündür. Veri kazıma tekniği, verinin bulunduğu internet alanlarının sahiplerinden izin almaksızın, geniş ve çok sayıdaki internet ortamından veri toplama anlamına gelmektedir⁶⁴⁵. Bu şekilde yapılan bir veri işleme faaliyeti GVKT'ne aykırı sayılacaktır. Çünkü bir bireyin sadece sosyal medya hesabında yüz görüntüsünü paylaşması her koşulda açık rıza dahilinde verilmiş sayılamaz.

Clearview aynı zamanda GVKT içinde belirtilen periyodik veri imha gerekliliklerine de uymamaktadır. Hem ABAD'ın hem de AİHM'in paralel şekilde verilerin silinmesi için uygun bir zaman belirlenmesi ya da verilerin muhafazasının değerlendirilmesi için periyodik bir değerlendirmeyi öngördüğü görülmektedir⁶⁴⁶. Bir an için Clearview tarafından yapılan tüm bu yüksek miktartlı veri toplama faaliyetlerinin hukuka uygun olarak yapıldığını varsaysak bile, kolluk kuvvetlerinin bu özel olarak oluşturulmuş ver tabanını sürekli olarak kullanması büyük veri koruma tehlikelerini barındırmaktadır. Bunun önüne geçilmesi açısından kullanımın sadece sınırlı olarak kullanılmasına izin verilmesi söz konusu olabilir. Yine de kolluğun

⁶⁴⁴ Rachel PESTER, “Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act (“BIPA”) Violation Suit”, Ed. Jordan KENNEDY, <https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit>, (s.y. 27 Mart 2022); Bkz. Samuel J. HODGE, s. 79.

⁶⁴⁵ Isadora Neroni REZENDE, “Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective”, New Journal of European Criminal Law, C. 11, S. 3, Y. 2020, s. 377.

⁶⁴⁶ A.g.m., s. 386.

kullanımına verilecek bu devasa platform, Avrupa eksenin uygulama bulan veri güvenliği gereklilikleri karşılamayabilir⁶⁴⁷.

Bir başka özel hukuk aktörü olan Amazon da yüz görüntülerinden oluşan veri tabanını bir ürün gibi üçüncü kişilere sunmaktadır. Bu hizmet üzerinden, on milyonlarca yüz verisi arasında gerçek zamanlı yüz taramaları yapılmakta olup, tek bir fotoğrafta yer alan 100'e kadar yüzün tespit edilmesi, analiz edilmesi ve dosyalanması, ayrıca kalabalık alanlarda, havalimanı gibi kamuya açık alanlarda ya da grup fotoğrafları üzerinde yer alan kişilerin duygularının analiz edilmesi mümkün olmaktadır⁶⁴⁸. Örnek vermek adına, Illinois eyaletindeki bu şekilde kullanımlar özel hukuk aktörlerinin kullanımına yasaklanmıştır. Texas ve Washington'da da bunu yasaklayan hukuk kuralları bulunmaktadır. Texas ve Washington'daki uygulamada, koruma hakkından doğan davayı sadece eyalet başsavcıları açabilmekte iken Illinois eyaletinde ise özel hukuk kişilerine bu davayı açma hakkı tanınmıştır. Bu nedenle ABD'de bu konuda açılan davaların çoğunun Illinois' da yerleşik şahıslar tarafından açıldığı görülebilmektedir.⁶⁴⁹.

C. Tasarımda Gizlilik ve Kapalı Devre Kameralar

GVKT'nın 25. maddesinde “tasarımda gizlilik” ve “varsayılan gizlilik” ilkeleri düzenlenmiştir. Veri korumaya ilişkin faaliyetlerin, verileri işleyecek sistemin ilk kurulduğu andan itibaren başlaması gerektiğini ifade eden bu düzenleme veri sorumlusu açısından bir takım yükümlülükleri beraberinde getirmektedir. Bu ilkeler doğrultusunda veri sorumlusu ya da GVKT'deki benzer tanımla kontrolör tarafından oluşturulacak politikalar doğrultusunda tasarımdan itibaren verilerin korunması ve mahremiyetlerinin sağlanması açısından gerekli tedbirlerin alınması gerekmektedir⁶⁵⁰. Söz konusu düzenleme ilk olarak GVKT ile yasal zemine kavuşmuş olsa da aslında veri koruma hukuku açısından temellerini geçmişte bulmaktadır. Bazı yazarlara göre bu amaç ya da uygulama neredeyse 25 yıllık bir geçmişe sahiptir⁶⁵¹.

⁶⁴⁷ A.g.m., s. 389.

⁶⁴⁸ Amazon “Rekognition” adlı hizmetini, “görüntülerinizden ve videolarınızdan bilgi ve öngörüler elde etmek için önceden eğitilmiş ve özelleştirilebilir görüntülü işleme (CV) özellikleri sunar.”, şeklinde tanıtmıştır. Detaylı bilgi için bkz. <https://aws.amazon.com/tr/rekognition/> s.y. 29 Mart 2022)

⁶⁴⁹ Matthew B. KUGLER, s. 118.

⁶⁵⁰ Murat Volkan DÜLGER, İnsan Hakları ve Temel Özgürlükler, s. 101.

⁶⁵¹ Dag Wiese SCHARTUM, “Making Privacy by Design Operative”, International Journal of Law and Information Technology, Oxford University Press, C. 24, S. 2, Y. 2016. s. 151.

Tasarımdaki gizlilik ya da varsayılan olarak gizlilik ilkelerine göre, toplanacak kişisel verinin türü, miktarı, işlenen verinin hangi amaçla ve sınırlar çerçevesinde işleneceğine dair sınırlar, verilere ilişkin muhafaza süreleri ve verilere erişim gibi konulardaki tüm önlemler daha süreç tasarlanırken alınmalı ve uygulanmalıdır⁶⁵². Büyük ölçekli bir kapalı devre kamera gözetiminde, çoğunlukla bu süreçlerin yönetildiği görece büyük bir kontrol ve izleme odası ve ayrıca bu gözetimin nasıl yapılacağına karar veren bir veri sorumlusu bulunur. İşte buna benzer durumlar dahilinde veri sorumlusunun tasarımdaki gizlilik ilkesine uyması ilk olarak yapılan gözetimin sınırlarını belirlemesi, işlenecek verilerin hangi amaçlarla işleneceğinin, bu amaçlara uygun miktarda verinin işleneceğinin ve bu verilere kimlerin erişebileceğinin kararını vermesi, bu hususlarda etkin bir denetim mekanizması sağlaması, saklama sürelerinin ne olduğuna ilişkin politikalarını oluşturması ve veri işlemenin ilk anından itibaren bu kural ve politikalara uygun hareket edilmesini sağlaması, gereken her türlü teknik tedbiri alması, veri minimizasyonuna uygun davranmasını ifade etmektedir. Bu şekilde oluşturulan kapalı kamera kayıt ve izleme sistemlerinin, GVKT'ye uygun olduğu kabul edilecektir. Keza bu şekilde kurulmuş ve faaliyetine devam eden bir kamera sisteminin ayrıca Türk Hukuku açısından da yasal düzlemde kabul göreceğini söylememiz mümkündür. Yukarıdaki özellikler KVKK tarafından aranan kriterleri karşılamaktadır.

Yukarıdaki bahsettiğimiz “yasaya uygun” sistem üzerinde değişiklik yapılması durumunda nasıl hareket edilmesi gerektiği ise bir başka problem olarak karşımıza çıkmaktadır. Veri işleme faaliyetlerinde meydana gelen değişiklik, daha önce kullanılan verilere ek olarak yeni bir veri türünün işlenmeye başlamasını içinde barındırmaktadır. Bu durumda ise tasarımda gizlilik ilkesinin devamlılığının sağlanması için “mahremiyet etki değerlendirilmesi” (privacy impact assessment) yapılması gerekecektir. Mahremiyet etki değerlendirmesi, veri işleme faaliyetlerinin tanımlanması ve veri işlemenin gerekliliğinin ve ölçülülüğünün değerlendirilmesi suretiyle veri işlemenin bireylerin hak ve özgürlükleri açısından yaratabileceği riskleri yönetmeye yardımcı olmayı amaçlayan bir süreç olarak tanımlanmakta olup hem yeni başlayan veri işleme faaliyetlerinde hem de yukarıda belirttiğimiz gibi sonradan değiştirilen veri işleme faaliyetleri açısından uygulanabilir⁶⁵³. Değişikliğe bağlı olan bu

⁶⁵² Murat Volkan DÜLGER, İnsan Hakları ve Temel Özgürlükler, s. 308.

⁶⁵³ Susan DOE, “Practical Privacy: Report from the GDPR World”, Legal Information Management, C. 18, S. 2, Y.2018, s. 76. Bu cümle içerisinde yer alan tanım doğrudan GVKT içerisinde yer almamakla birlikte Çalışma Grubu 29 tarafından hazırlanan 4 Nisan 2017 tarihli uygulama rehberinden edinilmiştir. Ayrıntılı bilgi için bkz. “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/document.cfm?doc_id=44137, (s.y. 24 Mart 2022)

yükümlülük GVKT'nın 35. maddesinin son fıkrasında gözden geçirme yükümlülüğü olarak ifade edilmiştir.

Önemli bir araç olarak görebileceğimiz mahremiyet etki değerlendirmeleri veri işlemeye dair proje tasarım aşamalarında karşılaşılabilecek risklere karşı, veri koruma düzenlemelerinin uygun bir şekilde yerine getirilmesini sağlamaktadır⁶⁵⁴. GVKT'nın 35. maddesi kapsamında, veri kontrolörüne, ilgili kişilerin hakları ve özgürlükleri açısından yüksek risk teşkil etme ihtimali bulunan yeni veri işleme süreçlerine başlamadan önce mahremiyet etki değerlendirmesi yapma yükümlülüğü getirmektedir. Bu değerlendirme sırasında yürütülen belirli aşamalar bulunmaktadır. Ön değerlendirme yapılarak veri kontrolörünün sektörel ve organizasyonel gerekliliklerinin belirlenir, mahremiyet etki değerlendirmesinin kapsamının oluşturulur, toplanan, işlenen ve imha edilen verilerin neler olduğu belirlenir ve tüm bu bilgiler doğrultusunda organizasyonların karşılaşması muhtemel risklerin tanımlanarak ve yasal mevzuata göre uygun çözümlerin üretilmektedir⁶⁵⁵.

Daha önce ICO tarafından getirilen güncel rehberde, yüz tanıma sistemlerinin video gözetimde kullanılmasının ancak belirli şartlar altında olabileceğinin vurgulandığını belirtmiştik. Bu şartlardan bir tanesi de yüz tanıma teknolojisi kullanacak özel teşebbüslerin ya da kamu kurumlarının uygun bir mahremiyet etki değerlendirilmesi hazırlamaları gerekliliği olarak karşımıza çıkmaktadır⁶⁵⁶.

Keza Avrupa Veri Koruma Otoritesi Video Gözetim Kuralları madde 3/2. kapsamında belirtilmiş olduğu üzere, tasarımda gizlilik ilkesi de dikkate alınarak, henüz video gözetim sistemi kurulmadan ya da yeni güncelleme yapılmadan önce, Veri Koruma Otoritesi ile işbirliği içinde veri mahremiyeti etki değerlendirmesi yapılması hem tasarımda gizlilik ilkesinin sağlanması açısından hem de bu doğrultuda yapılacak gereksiz harcamaların önlenmesi açısından yerinde olacaktır. Bununla birlikte, video ile gözetime başlamadan önce; etki değerlendirme analizi yapılması, kullanılan teknolojinin amaçla uyumlu olması ve özellikle süreklilik göstermeyen, büyük çaplı organizasyonlar, toplantılar gibi faaliyetler açısından sadece o faaliyet süresince tek seferlik kamera gözetim faaliyetlerinin uygulanmaya konulması yararlı olacaktır. Örneğin; uluslararası bir konferansın gerçekleştirileceği bir otelde, devlet

⁶⁵⁴ Christopher KUNER, Massimo MARELLI, Handbook on Data Protection in Humanitarian Action, 2017, s.82

⁶⁵⁵ Metin BİLGİN, Sema ERKAN, İdil ATASU, Enes YILMAZ, Privacy Impact Assessment as a Tool for GDPR Compliance Preparation, Kişisel Verileri Koruma Dergisi, C: 1 , S: 2, Y.2019, s. 75-86.

⁶⁵⁶ ICO, "Guidance on Video Surveillance", s. 41.

görevlerinin, ulusal ya da uluslararası hükümet temsilcilerinin bu konferansa katılımları söz konusu olacaksa, normal şartlarda tutulan kamera kayıtlarına ilişkin özel düzenlemeler yapılabilir⁶⁵⁷.

Sonuç olarak bu uygulama veri kontrolörünün, kişisel verileri işlemenin bireylerin temel hakları ve özgürlükleri üzerinde nasıl bir etki doğuracağı ve bu etkinin mevcut yasal düzenlemeler ile ters düşüp düşmediği konusunda önceden bilgi vermektedir. Bu bakımdan kameralar aracılığı ile herhangi bir gözetim faaliyetine başlamadan önce, bu faaliyete ilişkin mahremiyet etki değerlendirilmesinin yapılması ve bu kapsamda veri işlemenin tasarımda ve varsayılan olarak gizlilik ilkelerine de uygun olarak yapılmasına dikkat edilmelidir. Ayrıca bu açıdan dikkat edilmesi gereken ve değerlendirmede belirtilmesi gereken birkaç husus bulunmaktadır. Veri işleme amaçlarının açık ve haklı olması bir gerekliliktir. Örneğin; salgınların önlenmesi amacıyla ısı algılayıcı kameraların kullanılması, gösteriler sırasında kalabalıkların gözlenmesi için kameraların kullanılması haklı işleme amaçları arasında gösterilebilir fakat aynı zamanda toplanan verilerin, toplanması amacıyla bağlantılı olarak yeterli, ilgili ve aşırı olmaması da gerekecektir. Kamera kayıtlarının sonradan başka amaçlarla kullanılmadığının, anonimleştirme ya da imha politikalarının nasıl işlediğinin, görüntülerde yer alan 3. kişilerin yüzlerinin otomatik olarak bulanıklaştırıldığının belirtilmesi ve sistemin bu şekilde çalıştırılmasının zorunlu olması bu açıdan önemli değerlendirme kriterleri olarak görülebilir.⁶⁵⁸

D. Kapalı Devre Kamera Verilerine Erişim Hakkı

Kapalı devre kameralar tarafından verileri işlenen kimselerin yararlanabilecekleri çeşitli haklar bulunmaktadır. Veri sahibi kişinin hakları genellikle ilgilinin hakları ya da erişim hakkı olarak ifade edilmekle birlikte bu haklar farklı ülke uygulamalarına göre değişiklik göstermektedir.

Kıta Avrupası Hukuk Sisteminde kişisel verilere erişim hakkının dayanağı GVKT'dır. GVKT'nın 3. maddesi kapsamında Tüzük, merkezi AB sınırları içerisinde olan bir veri kontrolörünün (ya da veri işleyen) gerçekleştirdiği veri işleme faaliyetlerine doğrudan

⁶⁵⁷ The EDPS Video-Surveillance Guidelines, s. 10.

⁶⁵⁸ Christopher KUNER, Massimo MARELLI, s.95.

uygulanacaktır. Burada veri işleme faaliyetinin nerede gerçekleştirildiği önem taşımaz. Ancak bu hükmün devamında düzenlenen 2. fıkraya göre ise merkezi AB sınırları içerisinde olmayan veri sorumlularının da belirli koşullarda Tüzük'ün uygulama alanında yer alacağı düzenlenmiştir⁶⁵⁹. Bu durumlardan biri söz konusu veri sorumlusunun AB içerisinde bulunan veri sahiplerine mal ya da hizmet sunuyor olması iken; diğeri veri sahibinin davranışlarının AB içerisinde gerçekleşmesi halinde davranışlarının izlenmesi olarak düzenlenmiştir⁶⁶⁰. Bu durum GVKT'nın uygulanma alanını oldukça genişleten bir uygulama olarak karşımıza çıkmaktadır. Nitekim yukarıdaki şartlar altında Türkiye'de yerleşik bir tüzel kişinin AB sınırları içerisinde yaşayan bir bireyin kişisel verisini işlemesi durumunda GVKT'nın uygulanacağını söylenebiliriz. Bu bakımdan, erişim hakkını kullanmak isteyen bir bireyin bu hakkın korumasından yararlanması ile doğrudan ilgili olan Tüzük'ün kapsamını bilmesi çok önemli olacaktır aksi halde erişim talebini yanlış üçüncü kişilere yönlendirmesi söz konusu olabilecektir.

Tüzük kapsamında sık sık karşımıza çıkan “*controller*” yani veri kontrolörü, kişisel veri işlemenin amaçlarını ve yöntemini belirleyen, veri işleyicisi ise veri kontrolörü adına kişisel verileri işleyen kişiyi ifade etmektedir. Sorumluluk açısından baktığımızda ise kişisel veri ihlallerine ilişkin durumlarda hem veri kontrolörünün hem de veri işleyicisinin sorumluluklarının bulunduğunu söyleyebiliriz⁶⁶¹.

GVKT'nın 3. bölümünün 2. kısmında “Veri sahibinin verilere erişim hakkı” başlığı altındaki 15. maddede, veri sahibinin kişisel verilerine erişim talep etme hakkı düzenlenmiştir. Bu maddeye göre, veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini kontrolörden teyit etme ve veri işleme söz konusu ise faaliyet hakkında aşağıda belirtilen bilgileri talep etme hakkı bulunmaktadır⁶⁶². Bu durumlar ise şunlardır:

- a) Kişisel verinin işlenme amacı hakkında bilgi alma,
- b) Kişisel verinin ilgili olduğu kategoriler hakkında bilgi alma,

⁶⁵⁹ GVKT, md. 3.

⁶⁶⁰ Ufuk DAL, “Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti”, Kişisel Verileri Koruma Dergisi, C.1, S.1, Y. 2019, s. 25.

⁶⁶¹ GVKT md. 24, 82.

⁶⁶² GVKT md. 15. Tüzük'ün gerekçesinde erişim hakkına ilişkin talep şu şekilde değerlendirilmiştir. Kişisel verisi işlenen kişi, özellikle işlenen verilerin doğrulanması ve veri işleme işleminin yasal düzenlemelere uygun olarak yapıldığının incelenmesi amacıyla, kendisiyle ilgili toplanan kişisel verilere kolayca ve makul aralıklarla erişme hakkına sahip bulunmalıdır. Bkz. GVKT, Recital, md. 63.

- c) Kişisel verilerin açıklandığı veya açıklanacağı üçüncü taraflar (üçüncü ülkelerdeki veya uluslararası kuruluşlardaki alıcılar) veya alıcı kategorileri hakkında bilgi alma,
- d) Mümkün olduğu takdirde kişisel verilerin depolanacağı öngörülen süre, eğer bu mümkün değilse depo süresini belirlemek için kullanılan kriterler hakkında bilgi alma,
- e) Kişisel verilerin düzeltilmesine ya da silinmesine ilişkin talep hakkının varlığı hakkında bilgi alma ya da veri sahibini ilgilendiren verinin işlenmesi konusundaki sınırlandırmalar hakkında ya da bu sürece ilişkin itirazda bulunma hakkı konusunda bilgi alma,
- f) Şikayetin yapılacağı yetkili merciin ve buna ilişkin talimatlar hakkında bilgi alma,
- g) Kişisel veri, veri sahibinden elde edilmemişse, bu kişisel verinin kaynağının ne olduğu hususunda her türlü bilgi alma,
- h) Sonucunda analiz edilen ya da en azından profil oluşturulan otomatik olarak işlenen kişisel verinin işlendiğini bilme ve bunlar hakkında bilgi edinme.

Kameralar vasıtasıyla kişisel verisi işlenen her kimse, kişisel verisini, işlenme amaçlarını, mümkün olduğunda bu kişisel verinin işlenme süresini, kişisel verilerin gönderildiği üçüncü kişileri bilme hakkına sahiptir. Ancak bu yetkilerin kullanılması kişiye sınırsız bir talep hakkı da vermeyecektir. Nitekim bu hakkın kullanılması üçüncü kişilere ait ticari sırlara, fikri mülkiyet haklarına ve özellikle yazılımı koruyan telif haklarına yönelik bir müdahaleyi beraberinde getiriyorsa, kişisel verilere erişim hakkının kullanımının sınırlandırılması gerekecektir⁶⁶³. Fakat, erişim hakkının kullanılmasının sınırlandırılması sebep gösterilerek, veri sahibinin veriye erişme talebi peşin olarak reddedilmemelidir. Kanımızca burada sınırlandırmanın sınırı çizilerek, veri kontrolörünün veri sahibinin taleplerine yönelik bilgi vermekten kaçınmasının önüne geçilmesi istemiştir. Bu çerçevede, Tüzük'ün veri kontrolörünün hakkını kötüye kullanmasını engellenmiş olmasının yerinde bir uygulama olduğunu söyleyebiliriz.

Tüm bu düzenlemelerin ışığında kişisel verilere erişim hakkının çok önemli olduğunu söylememiz mümkündür. Çünkü, veri sahibinin bu Tüzük kapsamında koruma altına alınan birçok hakkını kullanabilmesinin ilk koşulu verilerine erişmekte özgür olabilmesidir. Örneğin; hukuka aykırı olarak toplanan kamera kayıtlarının ya da görüntülerin düzeltilmesini ya da silinmesini isteme hakkını kullanabilmek için verisi işlenen kişinin önce kişisel verisinin hangi

⁶⁶³ GVKT, Recital, md. 63.

koşullarla işlendiğini bilmesi gerekmektedir. Keza GVKT kapsamında erişim hakkına ilişkin taleplerin ihmal edilmesi ya da eksik açıklamada bulunulması durumunda, bu duruma sebebiyet veren cezai olarak sorumluluğun olduğu da düzenlenmiştir⁶⁶⁴. Uygulamada ise kişisel verilere erişim konusunda herhangi bir talep geldiğinde, ilk olarak kontrolör bilgi isteyen kişinin kişisel verilerinin işlenip işlenmediğini kontrol etmelidir. Burada önemli olan husus kontrolörün kişisel veri işlenmese dahi olumsuz olarak bir cevap verme yükümlülüğünün bulunmasıdır. Aksi halde erişim talebinin ihmale uğradığı yönünde bir suçlama ile karşılaşılabilir.

İngiltere’de 2018 yılında yürürlüğe giren VKK ve GVKT birlikte uygulanmaktadır⁶⁶⁵. GVKT’nın bir özelliği de İngiliz iç hukuk sisteminde öngörülen ceza meblağlarını artırmış olmasıdır. GVKT’dan önce kişisel verilerin korunmasının ihlal edilmesi durumunda verilecek ceza için üst limit 500.000 sterlin iken, GDPR’ dan sonra verilecek cezalar için iki seviye bulunmaktadır. Düşük nitelikli ihlallerde 10 milyon € ya da şirketin küresel cirosunun yüzde 2’si kadar ceza kesilebilirken; ciddi ihlallerde bu rakamlar 20 milyon € ya da şirketin küresel cirosunun yüzde 4’üne kadar (hangisi daha yüksek ise) çıkabilmektedir. Buna örnek olarak, 1998 tarihli Veri Koruma Kanunu kapsamında TalkTalk adlı bir iletişim şirketine 2016 yılında kesilen ceza 400.000 Sterlin iken⁶⁶⁶; GDPR’ın uygulanması ile bu cezanın 59.000.000 Sterlin’e kadar çıkması söz konusu olabilecektir. Bununla birlikte, Pharmacy2U adlı şirkete yine aynı yıl içinde kesilen ceza 130.000 Sterlin iken, bu cezanın da GDPR ile birlikte 4.400.000 Sterline çıkması mümkündür. GVKT çerçevesinde kesilecek azami cezalar artacak olsa bile Tüzük’te, cezaların yapılan ihlale “orantılı” olarak verilmesi gerektiği de belirtilmiştir. Ayrıca, veri sorumlularının Tüzük’e uyumlu olduğundan emin olmak için gerekli özen yükümlülüğüne uygun hareket etmesine rağmen bu ihlalin meydana geldiği ispat edildiği takdirde, veri koruma otoritesi tarafından verilecek cezada tenkise gidilmesi söz konusu olabilecektir.

⁶⁶⁴ Sebastian J. GOLLA, "Is Data Protection Law Growing Teeth: The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR." *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, C. 8, S. 1, Y. 2017, s. 75.

⁶⁶⁵ 23 Mayıs 2018 tarihinde, GVKT’ nin yürürlüğe girmesinden hemen önce İngiliz Veri Koruma Kanunu yürürlüğe girmiştir. Bu kanunun hazırlanmasında GVKT taslağı örnek olarak alınmıştır. Kanun’ un birinci bölümünde genel bakış altındaki 1. maddede, bu kanunun kişisel verilerin işlenmesi yönelik hükümleri içerdiği, 2. maddede ise kişisel verilerin işlenmesi konusunda GVKT’ye atıf yapıldığı görülmektedir. Bununla birlikte, kanunun diğer maddelerinde de görüldüğü üzere, GVKT ile Veri Koruma Kanunu bir çok hükümde birlikte kullanılmış, aralarında paralellik bulunduğu ve amaçlarının aynı olduğu böylelikle kanıtlanmıştır. İlgili madde bkz. Data Protection Act 2018, (c.12) Part 1 – Preliminary, www.legislation.gov.uk/ukpga/2018/12/part/1 (s.y. 31 Mar 2022)

⁶⁶⁶ TalkTalk Gets Record £400,000 Fine for Failing to Prevent October 2015 Attack, ayrıntılı bilgi için bkz. <https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded> (s.y. 02 Nisan 2022)

Bu Kanuna göre, kişisel verilere erişim hakkı, kanunun “Verisi İşlenen Kişinin Hakları Başlığı” altındaki 45. maddesi ile 94. ve 95. maddelerinde düzenlenmiştir⁶⁶⁷. Genel olarak bu düzenlemelere göre, hak sahibi verisinin işlendiğini öğrenebilecek, kendine ait kişisel verisine ve bunlara ek olarak tutulan diğer bilgilere ulaşabilecektir. Bu düzenlemeler ışığında kişisel verilere erişim hakkını, kişisel verisi işlenen kişiye, kişisel verilerinin bir kopyasını ve buna ilave olarak tutulan ek bilgileri talep etme hakkı veren hak olarak tanımlayabiliriz. Bu hak sayesinde bireyler kişisel verilerinin nasıl ve neden kullanıldığını konusunda bilgi sahibi olmakta ve temel işlem olan kişisel verinin işlenmesi işleminin hukuka uygun olarak yapılıp yapılmadığını kontrol etme imkanı bulmaktadırlar. Bu nedenle bize göre bu hak sayesinde korunan hukuki değer bu kanun kapsamındaki kullanılan diğer birçok hakkın kullanımı için olmazsa olmazdır.

Yukarıda da bahsedildiği üzere, veri sahibinin kişisel verisine ilişkin bir kopyanın kendisine verilmesi hakkı dışında, veri sahibi aşağıda listelenen bilgilerin de kendisine verilmesini talep hakkına sahiptir:

- Kişisel verinin işlenme amacı,
- Kişisel verinin paylaşıldığı üçüncü taraflar veya üçüncü taraf kategorileri,
- Kişisel verinin saklanma süresi, bunun mümkün olmadığı durumda saklama süresine karar verme kriterinin ne olduğu,
- Kişisel verinin düzeltilmesi, silinmesini ve kısıtlanmasını talep etme veya bu tür işlemlere itiraz etme haklarının varlığı,
- ICO (Bilgi Komisyonu Ofisi) veya başka bir denetleme otoritesine şikayette bulunma hakkı,
- Kişisel veri doğrudan kişisel verisi işlenen kişiden elde edilmemişse, verinin kaynağı hakkında bilgi alma,
- Otomatik karar verme sistemlerinin (profil oluşturma da dahil) varlığı hakkında bilgi alma,
- Kişisel veriler üçüncü bir ülkeye veya uluslararası bir kuruluşa transfer ediliyorsa, sağlanan güvenlik önlemleri hakkında bilgi alma hakkı.

⁶⁶⁷ VKK, md. 45., 94. ve 95., <https://www.legislation.gov.uk/ukpga/2018/12/part/1> (s.y. 31 Mart 2022)

Uygulamada bu bilgilerin çoğunun, şirketlerin internet siteleri veya yazılı evraklarında gizlilik bildirimi başlığı altında verildiğini görebilmekteyiz.

Hem VKK hem GVKT, veri kontrolörüne yöneltilmesi gereken geçerli bir talebin nasıl yapılması gerektiği konusunda ayrıntılı bir düzenleme getirmemiştir. Bu sebeple, veri sahibinin sözlü ya da yazılı olarak başvuruda bulunması mümkün olmaktadır. Ayrıca bu başvurunun, başvuru yöneltilen kuruluşun belirli bir departmanına yapılması zorunluluğu yoktur. Hak sahibi, kişisel verisini işleyen kuruluşun sosyal medya hesabı üzerinden dahi söz konusu talebini iletebilir⁶⁶⁸.

E. Avrupa İnsan Hakları Mahkemesi ve Yerel Mahkeme İçtihatları

İşığında Kapalı Devre Kameralar ile Gözetim

4 Kasım 1950 tarihinde Avrupa Konseyi üyesi devletlerin imzasına açılan ve Kıta Avrupası Hukuk Sisteminin en önemli temel insan hakları metinlerinden biri sayılan Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesi aşağıdaki gibidir:

"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."

⁶⁶⁸ Kişisel verilere erişim hakkının kullanılmasının herhangi bir ücrete bağlı olmaksızın kullanılması kuralıdır. Ancak VKK'da belirtildiği üzere, talebin açıkça dayanaktan yoksun veya aşırı olduğu durumlarda, idari maliyetler açısından makul bir ücret başvuruca alınabilecektir. Eğer kişisel verisi işlenen kimse, talebine ek olarak işlenmekte olan kişisel verilerinin kendisine verilecek olanın dışında kopyasını da istiyorsa, kuruluş kendisinden makul bir ücret isteyebilecektir. Burada istenen ücretin sebebi, ek kopyalar hazırlamanın idari maliyet yarattığı düşüncesi olmaktadır. Ayrıca VKK'ya göre, talep alındıktan sonra herhangi bir gecikme olmaksızın ve en geç alındığı tarihten itibaren 1 aylık süre içinde cevabın, hak sahibine sunulması gereklidir. Veri sahibinin erişim hakkına dair detaylı bilgilendirme için bkz. Right of Access, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/individualrights/right-of-access/> (s.y. 19 Nisan 2021)

AİHS metninde kişisel verilerin korunması hakkı, bağımsız bir hak olarak düzenlenmemiş olup, sözleşmenin 8. maddesinin koruma alanında yer almaktadır. Avrupa İnsan Hakları Mahkemesi'nin içtihatları ve genel bakış açısına göre 8. maddenin kişisel verilerin korunması açısından önemli bir yere sahip olduğunu söyleyebiliriz⁶⁶⁹.

Sözleşmenin 8. maddesinde düzenlenen özel hayatın korunmasına dair temel hak kapsamında kişisel verilerin korunması hususunda devletin hem negatif hem de pozitif yükümlülüğünün bulunduğu söylenebilecektir. Yani devlet ilk olarak bireylerin kişisel verilerinin korunmasına yönelik olarak, kişisel verilere hukuka aykırı olarak müdahalede bulunmayacak ve veri koruma ilkelerine aykırı veri işleyemeyecektir. Diğer yandan pozitif yükümlülüğü gereği ise kişisel verilerin korunması hakkının ihlal edilmemesi için gereken yasal düzenlemeleri yapmak ve bunlara uyulmaması durumunda uygulanacak yaptırımları düzenlenmek, veri koruma hukuku ilkeleri kapsamında her türlü idari ve teknik önlemi almak zorundadır⁶⁷⁰.

Yukarıda da belirttiğimiz üzere AİHM'in önüne gelen uyumsuzlukları çözümlerken yaratmış olduğu içtihatların da önemi büyüktür. Sözleşme içerisinde kişisel verilerin korunmasını isteme hakkı gibi doğrudan bir düzenleme olmadığı için, kişisel verilerin korunması hakkının AİHS md. 8 kapsamında değerlendirilmesi büyük ölçüde AİHM içtihatlarına dayanmaktadır. Mahkeme kararlarını oluştururken kişisel verilerin korunması alanında somut olay bazında hareket etmekte, bu olaylar kapsamında bireylerin verilerinin korunması hususunda ihlalin söz konusu olup olmadığını değerlendirmektedir. Nitekim doktrinde AİHS düzleminde kişisel verilerin korunmasının açık bir hükümle düzenlenmemiş olması ve içtihatlar vasıtasıyla AİHS md. 8 kapsamında bir korunma sağlanmaya çalışılmasını karmaşık olarak nitelendirenler yazarlar da bulunmaktadır⁶⁷¹. Kanımızca bu durum her ne kadar bir dezavantaj gibi görülse de sözleşmenin genel anlamda yorumlanması bağlamında düşünüldüğünde karmaşıklık ya da tehlike yaratmamaktadır. Çünkü hem AİHM hem de doktrin sözleşmeyi “yaşayan bir enstrüman olarak” nitelendirmektedir⁶⁷². Tyrer Birleşik Krallık'a karşı kararında Mahkeme, AİHS'in yorumlanmasına ilişkin olarak “sözleşme yaşayan bir

⁶⁶⁹ Murat Volkan, DÜLGER, Kişisel Verilerin Korunması Hukuku, s. 124.

⁶⁷⁰ Eren SOLMAZ, Avrupa İnsan Hakları Mahkemesi Kararları'nın “Kişisel Verilerin Korunması”na Katkısı, İdare Hukuku ve İlimleri Dergisi, C. 18, S. 1, Y. 2018, s.64.

⁶⁷¹ Lee A. BYGRAVE, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, International Journal of Law and Information Technology, S. 6, S. 3, Y. 1998, s. 252.

⁶⁷² Michael O'BOYLE, David HARRIS, Colin WARBRICK, Law of the European Convention on Human Rights, 3. Baskı, Oxford University Press, Oxford 2014, s. 9.

enstrümandır, bu nedenle günümüzün koşulları ışığında yorumlanmalıdır” diyerek, sözleşmedeki maddelerin koruma kapsamlarını genişletmiştir⁶⁷³. Bu yorumun kabulü sözleşmenin lafzına sıkı sıkıya bağlı kalınmasını engelleyerek kişisel verilerin korunmasını istemeye dair taleplerin de özel hayatın gizliliği maddesi içerisinde değerlendirilmesine olanak sağlamaktadır. Bize göre bu yönde bir bakış açısının geliştirilmesi doğru olmakla birlikte, aynı zamanda sürekli gelişen teknolojiler karşısında bir zorunluluktur. Aksi durum, AİHM gibi önemli bir hukuk mekanizmasının bu teknolojiler karşısında uygulanabilirliğini azaltacaktır.

AİHS md. 8 altında koruma altına alınan özel hayat, aile hayatı, konut ya da haberleşme gibi alt kavramların da sözleşme içerisinde tanımlanmamış olduğunu görmekteyiz. Bu kavramların içerisine nelerin girdiği de ancak sözleşmenin yorumu ve AİHM kararları doğrultusunda ortaya çıkmaktadır. AİHM önüne gelen bir dosyada yerel mahkemelerin bu kavramlardan ne anladıklarıyla pek ilgilenmemekte olup bu kavramların tanımlarını ön yargılardan etkilenmeyecek bir şekilde yapmaktadır. AİHM’in bu gayreti sonucu, kavramların tanımları değişip genişleyebilecek olduğundan bireylere sağlanan korumanın uygulama alanı da genişleyebilecektir⁶⁷⁴.

AİHM içtihatları bizlere göstermektedir ki temelde dört tane gibi görünmekte olan korunan değerlere (özel hayat, aile hayatı, konut ya da haberleşme) ek olarak cinsiyet eşitliği, çocuk bakım işlemleri, arama ve gözetim almaya ilişkin işlemler, kişisel verilerin korunması ya da çevresel meseleler de AİHS madde 8. altında korunmaya değer bulunabilmektedir⁶⁷⁵.

Mahkeme tarafından verilen bir kararda⁶⁷⁶, “Bir kişinin, özel yaşamına ilişkin verilerin kaydedilmesi, 8. madde anlamında müdahale oluşturmaktadır. Kaydedilen bilgilerin, daha sonra kullanılmış olup olmamasının bir önemi yoktur. Bununla birlikte, resmi makamlar tarafından muhafaza edilen kişisel nitelikli bilgilerin, özel yaşamın belirtilen unsurlarından birini devreye sokup sokmadığını tespit etmek için, Mahkeme, bu bilgilerin hangi çerçevede alındıklarını ve muhafaza edildiklerini, verilerin türünü, kullanıldıkları ve işlendikleri şekli ve bunlardan çıkarılabilecek sonuçları dikkate alacaktır.” denildiği görülmekle, ilgili kararda kişisel verilerin korunması açısından madde 8’in uygulama alanı bulunduğu görülmektedir.

⁶⁷³ Tyrer, Birleşik Krallık’a karşı, b.n. 5856/72, k.t. 25 Nisan 1978.

⁶⁷⁴ Barbulescu, Romanya’ya karşı, b.n. 61496/08, k.t. 5 Eylül 2017.

⁶⁷⁵ Michael O’BOYLE, David HARRIS, Colin WARBRICK, s. 522.

⁶⁷⁶ S ve Marper, Birleşik Krallık’a karşı, b.n. 30562/04 ve 30566/04, k.t. 4 Aralık 2008.

Tez çalışmamız doğrultusunda bireylere ait kişisel veri niteliği olan kamera kayıtlarının korunması ilişkin kararlara baktığımızda, ilk olarak karşımıza Peck Birleşik Krallık'a karşı kararının çıktığını görmekteyiz. İhlal iddialarının konusu olan 20 Ağustos 1995 tarihli CCTV kamera kayıtlarında, başvuranın elinde bir bıçakla Brentwood'un merkezindeki bir kavşakta bileklerini keserek intihara teşebbüs ettiği görülmektedir. Kapalı devre kamera sisteminin operatörü olan Brentwood Belediye Meclisi tarafından polise haber verildikten sonra başvurana müdahale edilerek gerekli sağlık işlemleri yapılmış, göz altına alınan başvuran polis tarafından daha sonra serbest bırakılmıştır. Bu olaydan sonra başvurana ait kamera kayıtları Belediye Meclisi tarafından sloganlaştırılarak basına yansıtılmış ancak bu faaliyet gerçekleştirilirken bile başvuranın yüzü sansürlenmemiştir. Basının bu duruma ilgisi giderek artmış ve en sonunda ortalama 350.000 kişilik izleyici kitlesine sahip yerel bir kanalın bu görüntüleri haber amacıyla yayınladığı, bu yayın sırasında ise başvuranın yüzü kısmi olarak sansürlenmeye çalışılsa da saç şekli ve bıyığı nedeniyle onu tanıyan herkes tarafından kolaylıkla tanınabileceği tespit edilmiştir. İngiltere'de CCTV sistemlerinin faydalarının tanıtılmasına yönelik kampanyaların (kapalı devre kameraların suçun azaltılmasının yanı sıra şiddet olaylarının önlenmesine yönelik etkisinin bulunduğu özellikle vurgulanmıştır.) bir anda dayanak noktası olan başvuranın kamera kaydı verisinin daha sonra ulusal kanalda yaklaşık 9,2 milyon izleyiciye yayınlanmasına yönelik itirazda bulunduğu da belirtilmiştir⁶⁷⁷.

Başvuranın ailesine, arkadaşlarına ve diğer yakın çevresine ifşa etmek istemediği bir olayı açığa çıkarmak ve ülkede herkesin bu görüntüleri izlemesine olanak sağlamak kişinin mahremiyet alanına bir saldırı niteliğindedir. AİHM tarafından verilen kararda, özel hayat kavramının sınırlı olarak sayılabilecek nitelikte olmayan geniş bir kavram olduğu vurgulanarak, AİHS md. 8'in koruma kapsamına kimlik bilgilerinin, kişiliğini geliştirme hakkı kapsamındaki bilginin, cinsiyet bilgisinin, cinsel yönelimlerin ve bunun dışında diğer insanlarla kurulan ilişkiler kapsamında açıklanan her türlü bilginin girdiği belirtilmiştir⁶⁷⁸.

Mahkeme'nin gözetim faaliyetlerinin gerçekleştirileceği yer açısından ise ilgili kişinin evinin ya da özel mülkünün dışında yer alan kamusal alanlarda özel hayatının korunmasına ilişkin değerlendirmelerde bulunduğu görülebilir. Mahkeme bu kapsamda, sokakta yürüyen bir

⁶⁷⁷ Crime Beat: Soft Target, BBC One London, 11 March 1996 20.30, A series which reveals the truth about crime in the UK, Combatting crime in public places, (s.y. 1 Nisan 2022)

⁶⁷⁸ Peck, Birleşik Krallık'a karşı, b.n. 44647/98, k.t. 28 Ocak 2003.

kişinin kaçınılmaz olarak orada bulunan diğer insanlar tarafından görülebilir olduğunu ancak bu kamusal alanda teknolojik araçlarla görüntülenme ve kayıtlamanın sistematik olarak yapıldığı ve kalıcı olarak devletin elinde bulundurulmasının özel hayatın gizliliği açısından değerlendirmeye muhtaç olduğu ifade edilmiştir⁶⁷⁹.

Bir başka kararda ise polis memurlarının sorgu sırasında şüphelilerin seslerinin daha fazla analiz edilmek üzere kaydedilmesi, özel hayatlarına saygı haklarına müdahale anlamına gelen kişisel verilerin işlenmesi olarak kabul edilmiştir⁶⁸⁰. Burada Mahkeme özellikle gizli dinleme cihazlarının faaliyete konulmasında herhangi bir yasal dayanak bulunmadığına dikkat çekmiştir.

Kamuya açık alanlarda bireylerin günlük hareketlerinin kameralarla izlenmesi kendiliğinden özel hayata müdahale sayılmayacaktır. Ancak bu izleme faaliyetlerinin kayıt altına alınması ya da oluşturulan verilerin işlenmesi özel hayata müdahale teşkil edebilecektir⁶⁸¹. Peck kararının devamında belirtildiği üzere, kişisel verilerin ifşa edilmesine ilişkin davalarda Mahkeme, ilgili çatışan kamu ve özel menfaatler arasında adil bir denge kurulabilmesi için yetkili ulusal makamlara bir takdir payı bırakılması gerektiğini kabul etmiştir. Aynı kıyaslamayı sözleşmenin 8. maddesi ile 10. maddesi arasında gerçekleştirilen, özel yaşamın gizliliğinin ifade ya da basın özgürlüğü arasındaki kıyaslama ile benzer görmek mümkündür⁶⁸².

Peck kararında, bir taraftan başvuranın özel hayatına yapılan müdahalenin niteliği ve ciddiyetine dikkat çeken mahkeme diğer yandan CCTV sistemlerinin tanıtılmasında suç önlemede başarılı olmasını da göz ardı etmemiştir. Bu kapsamda her ne kadar CCTV sistemlerinde suçun ve şiddetin önlenmesi için bu görüntülerin yayınlanmasına izin verilecek olsa da bu işlemin önce başvurandan izin alınarak yapılması gerekmektedir. Ayrıca yayınlanan görüntülerin daha fazla sansür uygulanarak yayınlanması da başka bir detay olarak karşımıza çıkmaktadır. Kısacası Mahkeme, medyanın bu görüntüleri yayınlaması açısından üzerine düşen azami özeni gösterme konusunda yetersiz kaldığını vurgulamıştır. Sonuç olarak bu davada mahkeme tarafından, yukarıdaki hususları ve ayrıca suç önleme amacı ve

⁶⁷⁹ Michael O'BOYLE, David HARRIS, Colin WARBRICK, s. 560.

⁶⁸⁰ P.G. ve J.H., Birleşik Krallık'a karşı, b.n. 44787/98, k.t. 25 Eylül 2001.

⁶⁸¹ Michael O'BOYLE, David HARRIS, Colin WARBRICK, s. 555.

⁶⁸² Von Hannover, Almanya'ya karşı, b.n. 59320/00, k.t. 24 Haziran 2004.

görüntülerin paylaşıldığı ortam üzerinde özel bir denetleme yapılmasını gerektirir nitelikte olduğundan bahisle ve söz konusu tarihte, başvuranın özel hayata saygı hakkının ihlaliyle ilgili olarak başvurabileceği bir iç hukuk yolu bulunmadığı gerekçesiyle Sözleşme'nin 8. maddesiyle bağlantılı olarak 13. maddesinde belirtilen etkili başvuru hakkının da ihlal edildiğine karar verilmiştir.

AİHM tarafından verilen nispeten daha yeni bir kararda ise çalışma saatlerinde video kaydına alınan işçilerin özel hayatlarına saygı gösterilmesine ilişkin çeşitli değerlendirilmelerde bulunulmuştur. Bilindiği üzere mahkeme önüne gelen bir davada yargılamaya başlamadan önce birtakım kabul edilebilirlik koşullarına bakmaktadır. Bu kabul edilebilirlik şartlarından biri de başvurunun açıkça dayanaktan yoksun olmaması olup, eğer mahkeme esas incelenmesine geçilmesine gerek duymuyorsa bu aşamada davadan el çekebilmektedir. Burada verilen kararda başvurunun kabul edilmez olduğu kabul edilse bile yargılama sırasında hem kişisel verilerin işlenmesi hem de çalışanın özel hayatına saygı gösterilmesi hakkı ile işverenin mülkiyet haklarının korunması konusundaki menfaatleri ve adaletin gerektiği şekilde tesis edilmesindeki kamu menfaati arasında adil bir denge kurulduğuna dikkat çekilmiştir⁶⁸³. Yani Başvurucunun hırsızlık yaptığı görüntülerin gizli olarak kayıt altına alınması ve bunun kullanılması ile başvuranın kendisine önceden haber verilmeden işten çıkarılması olguları birbirini dengelemektedir. Mahkeme kararında ayrıca işyerinde kurulu olan gözetleme kameralarının belirli bir süre ve alanda faaliyet göstermeleri ve sadece amacı için kullanılıyor olması nedeniyle veri işleme faaliyetini ölçülü görmüştür⁶⁸⁴. Buradaki amaç güvenliğin sağlanması olmaktadır.

Bu olayda işveren tarafından yaptırılan gözetimin gizli olarak yapılması da önemlidir. Burada gerçekleştirilen gizli gözetleme faaliyetlerinin istisnai olarak yapılıyor da olsa demokratik toplum gerekliliklerine uygun olması gerektiğine, bu faaliyetler gerçekleştirilirken özel yaşamın gizliliğini korumak açısından getirilen tedbirlerin elverişli ve etkili olması gerektiğine dikkat çekilmiştir⁶⁸⁵. AİHM ayrıca bu kararına destek olarak iç hukukta var olan ve işverenin keyfi uygulamalarına karşı işçiyi koruyan hükümlerin zaten mevcutta etkin korumayı sağladığını ve Alman Federal İş Mahkemesi tarafından yapılan yargılama sırasında bunların değerlendirildiğini belirtmiştir. Yani AİHM başvuranın iç hukukta yeterli olarak korunduğunu düşünmektedir. Ayrıca kamera kayıtlarına başlama zamanının, malların kaybolduğunun

⁶⁸³ Köpke, Almanya'ya karşı, b.n. 420/07, k.t. 5 Ekim 2010.

⁶⁸⁴ HARRIS/O'BOYLE/WARBRICK, s. 557.

⁶⁸⁵ A.g.e., s. 555.

anlaşılmasının ardından gerçekleştirilen stok sayımı sonrasında ve çalışanın görev yaptığı departmanda başka birtakım düzensizliklerin baş göstermesinden sonra başlatılması, video kaydının sadece iki haftalık bir dönem için sınırlı olarak ve belirli bir alan için yapılması gibi nedenlerin de mahkemenin kararında dayanak gösterdiği diğer hususlardır⁶⁸⁶. Verilerin elde edilmesi açısından ise sınırlı sayıda insanın bu gözetim sisteminin başında bulunduğunu ve bunların özel dedektiflik ajansı çalışanları ve diğer işyeri çalışanları olduğunu özellikle vurgulanmıştır. Elde edilen veriler keyfi olarak üçüncü kişilerle paylaşılmamış olup, sadece çalışanın iş sözleşmesinin sona erdirilmesine yönelik olarak yerel mahkeme ile paylaşılmıştır.

Mahkeme burada başvurucunun AİHS md 8'deki özel yaşamın korunması hakkı ile işverenin AİHS'ne ekli 1.No'lu Protokol'ün 1. maddesinde yer alan mülkiyet hakkı kapsamında korunan değeri arasında bir denge kurmaya çalışmıştır. Aynı değerlendirme Alman yerel mahkemesinde de yapılmıştır. İşverenin temel haklarından bir tanesi olan mülkiyet hakkının tehlikede olması ve bunun ise ancak çalışanın hukuka aykırı olarak gerçekleştirdiği suç eyleminin ispatlanması amacıyla kanıt toplanması yoluyla korunabileceğini göz önünde bulundurulmuştur. Bu durum aynı zamanda adaletin sağlanmasına yönelik olması açısından kamu yararının sağlanmasına da hizmet etmektedir.

Ayrıca AİHM tarafından gelecek dönemde yeni ve daha gelişmiş teknolojilerin ortaya çıkmasıyla birlikte özel hayata yönelik müdahalelerin boyutunun değişeceği göz önünde tutulduğunda, söz konusu çatışan çıkarların ağırlıklarının sürekli olarak değişebileceğine dair açıklamalarda bulunulmuştur. Kişisel verilerin korunması hakkını AİHS md. 8 altında değerlendirirken sözleşmenin yaşayan ve sürekli yeni gelişen teknolojileri de kapsayacak şekilde geniş olarak yorumlanması zorunlu olarak karşımıza çıkmaktadır. Sözleşmenin yorumlanmasına ilişkin kısımda ifade etmiş olduğumuz üzere, AİHS sistemi içerisinde yer alan maddelerin yorumlanmasına ilişkin bu ilkenin bulunması ilerde icat edilecek birçok yeni gözetim aracı üzerinden toplanan kişisel verilerin de hakkın koruma alanına gireceğini garantileyerek, bireysel özgürlükleri teminat altına almaktadır.

Kişisel verilerin işlenmesi faaliyetlerine ilişkin olarak ilgili kişinin rızasının ne zaman alınması gerektiği, veri sorumlularının hangi durumlarda ilgili kişinin rızası olmaksızın veri işleyebileceği çoğu iç hukuk sisteminde yasalarla düzenlenmiştir. AİHM içtihatlarında da ilgili kişinin rızası bakımından çeşitli değerlendirilmeler yapılmıştır. Perry Birleşik Krallık'a karşı

⁶⁸⁶ Köpke, Almanya'ya karşı, b.n. 420/07, k.t. 5 Ekim 2010.

kararında mahkeme tarafından, başvuranın polis merkezinde suçlunun teşhisi amacıyla gizli kamera kaydı kullanılarak alınan görüntülerinin, kendisine bildirilmeksizin alınmasının özel hayatına müdahale sayılacağı ifade edilmiştir⁶⁸⁷. Kolluk tarafından, polis karakolunun kamuya açık bir alan olduğu ve özel bir alan beklentisinin olmamasının gerektiği ve bu alanlarda yer alan kameraların başvuran tarafından görülmesi sebebiyle kayıt altına alındığına dair bilgisi olduğu savunulmuştur. Kural olarak kamusal alanlarda, caddelerde, alışveriş merkezinde, parklarda ya da polis merkezlerinde kameralar ile gözetleme yapılması meşru ve öngörülebilir bir amaca hizmet etmesi AİHM tarafından ihlal olarak değerlendirilmemektedir. Ancak olayda, standart bir kapalı devre kamera kaydı alınmamış, ihlal iddiasında bulunan kişinin yakından net bir şekilde görülebildiği kendisinin teşhis edilmesine elverişli özel bir video kayıt mekanizması vasıtasıyla oluşturulmuş görüntüler söz konusudur.

Görüntülerin işlenmesi hususunda kişisel verisi işlenen kişinin rızasının olduğunu savunan kolluk kuvveti, diğer suçlu teşhis yöntemlerinden biri olan kimlik albümlerindeki fotoğrafların burada kullanılabileceğini savunmuştur. Nitekim bu albümler oluşturulurken alınan fotoğraflardan veri sahibinin haberi vardır. Kolluk her iki faaliyetinde de benzer amaçlara sahip olduğunu ve kimlik fotoğraflarının kullanılmasının kanuna aykırı olmadığını belirtmiştir ancak benzer olduğu söylenen kimlik albümlerindeki fotoğrafların genelde pasaport başvuruları sırasında elde edildiği ya da ilgililerin bilgisi dahilinde polis tarafından diğer usullerle hukuka aykırı yollarla elde edilmiş olduğu göz önüne alındığında, bu davadaki elde etme yönteminin belirtilen diğer hukuki yöntemlerden ayrıldığı dikkat çekmektedir. Netice olarak bu davada, görüntülerin kalıcı olarak kaydedilmesi ve daha sonra kullanılmak üzere montajlanması, kimlik tespiti açısından yerine getirilmesi gereken iç hukuk düzenlemelerine aykırı davranılmış olması ve yukarıda belirtilen diğer gerekçeler dahilinde başvuruçunun özel yaşamının korunması hakkının AİHS md. 8 kapsamında ihlal edildiğine karar verilmiştir.

Mahkeme, kanunilik ilkesinin de bir yansıması olarak, iç hukukta ne tür bilgilerin kaydedilebileceğinin, hakkında bilgi toplama ve saklama gibi izleme tedbirleri uygulanabilecek kategorideki kişilerin kimler olduğunun, bu tür tedbirlere başvurulabilecek koşulların ya da izlenecek usullerin neler olduğunun yasa ile düzenlenmesi gerektiğini özellikle vurgulamaktadır. İç hukuk kuralları ile birlikte bilgilerin ne kadar süreliğine tutulabileceğine dair düzenlemeler yapılması gerekmektedir. Ayrıca veri güvenliğine ilişkin olarak verilere

⁶⁸⁷ Perry, Birleşik Krallık'a karşı, b.n. 63737/00, k.t. 17 Ekim 2003.

erişim yetkisi olan kişilere, izlenecek usule ya da bu yolla elde edilen bilgilerin ne şekilde kullanılabileceğine ilişkin açık ya da ayrıntılı düzenlemelerin var olması gereklidir⁶⁸⁸.

Kameralar vasıtasıyla gerçekleştirilen faaliyetlerden ilgili kişinin bilgilendirmesi de bir zorunluluk olarak görülmektedir. Aksi durum gözetlenenler açısından hak ihlali anlamına gelecektir. İspanya ile Lopez Ribalda arasındaki uyuşmazlık AİHM önüne geldiğinde mahkeme tarafından, ilgilinin kişisel verilerinin işlendiğine dair bilgilendirilmesine yönelik olarak bazı önemli noktalar belirtilmiştir⁶⁸⁹.

İspanya hukuk sistemi içerisinde, video gözetim hakkında İspanya Kişisel Verilerin Korunması Kanunu ve bu kanun doğrultusunda çıkarılan talimat gereğince özel düzenlemelerin yapıldığı ve birtakım tedbirler getirilmiş olduğu görülmektedir. Mahkeme de bu düzenlemeleri göz önünde bulundurmak suretiyle, kişisel verileri toplamaya veya işlemeye tabi tutulan kişilerin haklarına herhangi bir uygunsuz müdahaleyi önlemek amacıyla iç hukukun belirli sayıda güvence öngördüğünü belirtmiştir. 14 Ocak 2000 tarihinde yürürlüğe giren İspanya Veri Koruma Kanunu’nun 5. maddesi kapsamında verileri işlenecek veri sahiplerinin daha önceden, açık ve belirli bir şekilde bilgilendirilmesi zorunludur. Bu bilgilendirmenin kapsamına işlenecek verinin ne olduğu, verileri sağlamanın ya da sağlamayı reddetmenin sonuçları, verilere erişim hakkı, düzeltilme ya da silinme hakkı ile itiraz etme hakkı, ayrıca veri kontrolörlerinin ya da yasal temsilcilerinin kimlik ve adres bilgilerinin veri sahibine sunulması girmektedir. Keza 6. maddede veri sahibinin açık rızası ve aynı maddenin ikinci fıkrasında ise açık rızanın gerekmediği haller yer almaktadır.

Video kamera gözetimlerine ilişkin olarak İspanya Veri Koruma Otoritesi tarafından çıkarılan talimatın 3. maddesinde “gözetlenen alanlara en azından herkesin görebileceği yeterlilikte bilgilendirme metinlerinin asılması gerektiği ve ayrıca bu bilgilendirmeyi içeren dokümanlara herkesin ulaşabilmesinin gerektiği” belirtilmiştir⁶⁹⁰. 4. maddede ise yine veri koruma hukuku açısından çok önemli bir ilke olan ölçülülük ilkesi düzenlenerek, kameralarla gözetimin sadece hukuka uygun, meşru ve belirli amaca yönelik olarak uygun, gerekli ve ölçülü olarak yapılabileceği belirtilmiştir. Kararda belirtilen diğer önemli düzenleme olan İş

⁶⁸⁸ Rotaru, Romanya’ya karşı, b.n. 28341/95, k.t. 26 Kasım 2014.

⁶⁸⁹ Lopez Ribalda ve diğerleri, İspanya’ya karşı, b.n. 1874/13 ve 8567/13, k.t. 17 Ekim 2019.

⁶⁹⁰ Instruction no. 1/2006 of 8 November 2006 on the processing of personal data for monitoring purposes using video-surveillance devices, issued by the Spanish Data Protection Agency.

Yönetmeliği' nin 20/3 maddesi'ne göre ise; işverenin, çalışanlarını çalışma koşulları altında gözetimi bu gözetim faaliyetlerinin insan şerefi ile bağdaşır nitelikte olması şartına bağlamıştır.

İspanya İş Mahkemesi ilk olarak anayasal içtihatlarına uygun olarak video gözetimin kurulmasının meşru dayanaklarını incelemiş bu doğrultuda son aylarda süpermarkette hırsızlık nedeniyle gerçekleşen önemli ölçüdeki kayıplara ve işveren açısından bakıldığında işlerinin düzgün olarak devam etmesinin sağlanması, kayıplardan sorumlu olanların tespit edilmesi ve cezalandırılması hususlarında meşru menfaatinin bulunduğu kanaatine varmıştır. Ayrıca kameraların sadece kayıpların meydana geldiği kasa etrafındaki alanlarda faaliyette olduğu göz önüne alındığında, tedbirin ölçülülük açısından da uygun olduğu görülmüştür. İzleme faaliyeti mağazanın tamamına yayılmamıştır.

Mahkeme, bu bağlamda, bir çalışanın mahremiyetinin korunması ışığında video gözetim tedbirinin orantılılığının analizinde, izlemenin yapıldığı çeşitli yerleri ayırt etmenin gerekli olduğu görüşündedir. İzleme faaliyetlerinin yapıldığı yerler açısından makul beklenti şartının karşılanması gereklidir. Bu beklenti, tuvaletler veya vestiyerler gibi doğası gereği özel olan, yüksek korumanın ve hatta video gözetiminin tamamen yasaklanmasının haklı olduğu yerlerde çok yüksektir. Bu bakımdan ofis gibi daha dar çalışma alanlarında alışveriş merkezi kasalarındaki çalışma alanlarına göre daha yüksek bir mahremiyet algısı söz konusudur. Ofisler daha az kamuya açık olduklarından, daha az görülebildiklerinden o alana yerleştirilecek bir CCTV, daha kamusal bir alana yerleştirilene kıyasla kişisel verilerin korunması açısından daha büyük bir müdahale sayılabilecektir.

Kayıt sürelerine ilişkin olarak ise mahkeme tarafından başvuranların iddia ettiği gibi, işveren tarafından video gözetim süresi önceden belirtilmemiş olsa da aslında toplamda 10 gün sürdüğü ve amaçla bağlantılı olarak en kısa sürede sona erdirildiği kaydedilmiştir. Bu nedenle video kaydının uzunluğu ölçülü olarak değerlendirilmiştir. Ayrıca gözetim vasıtasıyla elde edilen verileri sadece süpermarket müdürü, şirketin yasal temsilcisi ve sendika temsilcisi görmüş olup, mahkeme tarafından bu unsurlar değerlendirilerek başvuruçuların mahremiyetlerine hakkın özüne etkili olacak şekilde müdahale edilmemiş olduğuna kanaat getirilmiştir.

AIHM tarafından 6 Eylül 1978 tarihinde verilen Klass ve Diğerleri Almanya'ya karşı davasında, başvuranların tümü tarafından Alman Posta, Posta ve Telekomünikasyonun Gizliliğine İlişkin Kısıtlamalara Dair 13 Numaralı Kanun'un getirmiş olduğu gözetleme

yetkilerinin, özel yaşamın gizliliğini koruyan AİHS'in 8. maddesini ihlal ettiği ileri sürülmüştür. Başvurucular ihlal iddiasında özellikle devletin yasal mevzuatında öngörülen tedbirlere başvurmasına değil, bu tedbirlerin ilgili kişilere bildirilmemesine ve bu tür tedbirlerin uygulanmasına karşı itiraz etme ya da dava açma hakkı bulunmamasına itiraz etmektedirler. İlgili hükme göre, belirli yetkililerin, posta ve postaları açıp incelemesine, telgraf mesajlarını okumasına ve telefon konuşmalarını izlemesine ve kaydetmesine izin verilmiştir⁶⁹¹.

Bu davada AİHS 8. maddeye göre ortaya çıkan temel mesele, müdahalenin 8.maddenin 2.fıkrası hükmüne göre haklı olup olmadığıdır. Bu fıkra, sözleşme ile güvence altına alınan bir hak için istisna öngördüğü için, dar bir şekilde yorumlanacaktır. Gizli gözetim yetkilerine izin verilmesi ya da bu yetkilerin kullanılmasının AİHS açısından ihlal teşkil etmemesi açısından bu istisnai uygulamaların ancak demokratik kurumların korunması için gerekli olduğu ölçüde yapılıyor olması ve her şeyden önce "yasaya uygun" olması gerekmektedir.

Müdahalenin yasal dayanağının bulunmasının dışında diğer unsur ilgili gözetim tedbirinin uygulanmasının demokratik toplumda gereklilik arz etmesi olduğuna değinmiştik. Bireylerin anayasal temel hak ve özgürlüklerinin olası suistimallere karşı gerekli korumanın sağlanamadığı görülse de mahkeme özellikle ilgili kısıtlayıcı kanun hükümleri dolayısıyla gözetim faaliyetleri uygulanmadan önce bu kısıtlayıcı koşulların öngörüldüğüne ve somut olayda bunların yerine getirildiğine dikkat çekerek⁶⁹² müdahalenin demokratik bir toplumda gerekli olduğunu, ulusal güvenliğin çıkarlarını, düzenin korunması ve suç işlenmesinin önlenmesi amaçlarını gözettiğini değerlendirmek için haklı gerekçelerinin söz konusu olduğunu kaydetmiş olmaktadır. Bunun sonucu olarak da Sözleşme'nin 8.maddesinin ihlal edilmediğine karar vermiştir. Mahkeme bu kararı verirken günümüzde demokratik toplumların son derece gelişmiş casusluk biçimleri ve terör gibi nedenlerle tehdit edildiğini ve bunun sonucunda da devletlerin bu gibi tehditlerle mücadele edebilmek için kendi yetki sınırları içerisinde faaliyet gösteren bölücü unsurları gizli bir şekilde izleme görevini üstlenebilmesi gerektiğini kaydederek e-mailler, postalar ve çeşitli iletişim araçları üzerinde gizli teknik takibin yapılmasına imkân veren mevzuatın var olmasının ulusal güvenlik gerekçesiyle ve/veya kargaşa ya da suçun önlenmesi amacıyla demokratik bir toplumda gereklilik arz ettiğini özellikle vurgulamıştır.

⁶⁹¹ Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief- Post- und Fernmeldegeheimnisses).

⁶⁹² Klass ve diğerleri, Almanya'ya karşı, b.n. 5029/71, k.t. 6 Eylül 1978.

Bireylerin özel yaşamlarına müdahalenin sadece yasalar tarafından düzenlenmesi durumunda mümkün olabileceği, yasalarda düzenlenmesinin yanı sıra getirilecek sınırlamanın da demokratik toplumun gerekliliklerine uygun olması gerektiğini neredeyse her AİHM karar metninde görmekteyiz. Buna ilişkin Malone kararında da mahkeme kendisine çalıntı malların hileli bir şekilde satılmasına ilişkin suçlar isnat edilmiş olan başvuranın haberleşmelerinin dinlenmesi ve telefonunun izlenmesine ilişkin kayıtların polisin elinde bulunmasının iç hukukta kanuni dayanağı olmadığından bahisle AİHS md. 8'in ihlal edilmiş olduğuna hükmetmiştir⁶⁹³. Buna benzer, 24 Nisan 1990 yılında karar verilen Kruslin davasında⁶⁹⁴ yine sözleşmenin aynı madde doğrultusunda ihlal edildiğini ancak bunun sebebinin yargı makamları tarafından gözetleme yetkilerinin kapsamı ve kullanılma şekline yönelik olarak yeterli açıklığın sağlanmamış olduğunu belirtmiştir. Mahkeme tarafından başvuranın demokratik bir toplumda hukukun üstünlüğü gereği vatandaşlara tanınan asgari düzeydeki korunma hakkından faydalanamamış olduğu vurgulanmıştır.

⁶⁹³ Malone, Birleşik Krallık'a karşı, b.n. 8691/79, k.t. 2 Ağustos 1984.

⁶⁹⁴ Kruslin, Fransa'ya karşı, b.n. 11801/85, k.t. 24 Nisan 1990; Aynı yönde diğer kararlar için bkz. Kopp, İsviçre'ye karşı, b.n. 13/1997/797/1000, k.t. 25 Mart 1998; Amann, İsviçre'ye karşı, b.n. 27798/95, k.t. 16 Şubat 2000.

SONUÇ

Tez çalışmamızın içerisinde de belirttiğimiz üzere, önceki dönemlerde gözetim doğrudan insan gözüyle yapılmaktaydı. Bu bakımdan gözetleyenler kimi zaman mimari yapılardan, kimi zaman ise şehir düzenlemelerinden, ışıklardan ya da nesneyi görülebilir kılan diğer tekniklerden yararlanmaya çalışmışlardır. Günümüzde ise kapalı devre kamera sistemleri neredeyse tüm diğer gözetim tekniklerine karşı baskın gelmiştir. Teknolojinin de gelişimi ile kapalı devre kameralar aracılığıyla gerçekleştirilen gözetim faaliyetleri yoğunlaşmıştır. Günümüzde caddeler ya da kavşaklar gibi kalabalıkların bulunduğu alanların her yanında CCTV'lerin bulunması bir yana dursun, yeri geldiğinde insansız hava araçları ile birlikte o anda aklımıza gelen belirli bir alanı havadan gözetlememiz mümkün olmaktadır. Böylelikle gözetimin kuşatıcılığı ile birlikte sınırlarının da genişlediğini söylememiz mümkün olacaktır.

Kapalı devre kamera sistemlerinin sayıca çok olması, bir takım teknolojik yazılım ya da donanımların bu sistemlere entegre edilmesi veya yapay zekanın kullanılması gibi sebeplerden ötürü kapalı devre kamera sistemlerinin bir insan gözünün yapabileceği şeylerden çok daha fazlasını başarması olanağı bulunmaktadır. Kameraların görüntü alanına giren bir kimsenin kimlik bilgisi ve geçmiş yaşantısına dair farklı bilgilere çeşitli veri tabanları üzerinden anında erişim sağlanabilmektedir. Neredeyse tüm kamusal alana yayılan bu gözetim tekniği karşısında bireylerde mahremiyet kaygılarının oluşması muhtemeldir.

Bu bireysel mahremiyet kaygılarının belirli ölçüde giderilmesi açısından kapalı devre kameralar ile gözetlenen bireylerin KVKK kapsamından yararlanıyor olmaları önemlidir. Zira KVKK, 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 düzenlemek amacıyla getirilmiş bir düzenlemedir. Çalışmamız kapsamında KVKK'nın hangi yönlerden kapalı devre kamera sistemlerinin faaliyetlerine uygulanacağı, hangi durumlarda bu faaliyetlerin Kanun'daki istisna kapsamına girdiği belirtilmiştir. Bu bakımdan tartışmalı olan bir diğer konunun, suçun önlenmesi amacıyla MOBESE/KGYS gibi kent güvenliği sistemleri tarafından yürütülen veri işleme faaliyetlerinin bu Kanun'un uygulama alanına girip girmediği olduğu da vurgulanmıştır.

Bu sistemlerin istisna kapsamına girebilmesi için kişisel verilerin sadece önleyici faaliyetler amacıyla işleniyor olması yetmeyecek, bununla birlikte önleyici faaliyeti gerçekleştiren kolluğa yetki veren bir yasal düzenleme bulunması gerekecektir. Fakat mevzuatımızda doğrudan bu görüntüleme sistemlerine ilişkin bir yasal düzenleme bulunmadığından, kanaatimizce MOBESE/KGYS faaliyetlerinin doğrudan bu istisna kapsamına sokulması hatalı olarak görülebilecektir.

Bununla birlikte, mevcut yasal düzlemde söz konusu istisna hükümlerinin uygulanacağı alanın geniş yorumlanmaya elverişli bırakıldığını da belirtmeliyiz. Bu sistemler aracılığıyla işlenen kişisel verilerin nasıl ve hangi koşullarda işlenebileceği, elde edilen verilerin kimlere aktarılabilirliği ya da bu sistemlere dair alınması gerekli veri koruma tedbirlerinin neler olduğu yasayla düzenlenmelidir. Aksi halde bireylerin kişisel verilerinin korunması Anayasal temele dayandığından ve bu hakka getirilecek kısıtlamanın da yasayla yapılması gerekli olması gibi nedenler dahilinde, veri işlemenin bireyin Anayasal temel hak ve özgürlüklerine bir saldırı sayılabileceği söylenebilir.

MOBESE/KGYS dışında diğer kapalı devre kamera sistemleri açısından da gözetim faaliyetlerini düzenleyen yasal düzenlemeye ihtiyaç bulunduğu görülmektedir. Bu bakımdan yukarıdaki açıklamalarımız kapsamında MOBESE'nin veri işleme faaliyetlerini de kapsayan, bununla birlikte hem devlet hem özel hukuk aktörleri tarafından yapılan tüm CCTV gözetim faaliyetlerinde uygulanacak ve gerçekleştirilecek gözetimin sınırlarını detaylı olarak çizecek yasal bir düzenlemenin yapılmasını gerekli görmekteyiz. Şayet bu yapılmıyorsa, KVKK'ya ek olarak çıkarılacak bir ikincil düzenlemeyle bu alandaki hukuki belirsizliğin giderilmesi uygun olabilir. Çıkarılacak yasal düzenlemelerin GVKT'da yer alan tasarımda gizlilik ilkesine benzer ilkeleri barındırması ve en azından CCTV sistemlerinin kurulmasından önce mahremiyet etki değerlendirmelerinin yapılmasını zorunlu tutması veri koruma hukumuz açısından önemli olacaktır.

Kanunlaştırma sürecinde atılması gereken bir diğer adım ise mevcutta yaşanan ya da yaşanma ihtimali bulunan potansiyel mağduriyetlerin giderilmesidir. Buna ilişkin olarak ise kapalı devre kameralar aracılığıyla işlenen kişisel verilere dair geçici önlem mahiyetinde bir rehber çalışma hazırlanması ve Kişisel Verileri Koruma Kurumu tarafından yayınlanması beklenebilir. Burada Kıta Avrupası hukuk sistemi içerisinde bulunan ve tez içerisinde inceleme

fırsatına sahip olduğumuz rehberlerin emsal alınması önemlidir. Bu rehberler detaycı ve açıklayıcı ruhu özellikle örnek alınmalıdır.

Tüm bunlara ek olarak yapay zekanın kapalı devre kamera sistemlerinde kullanılması birtakım avantajları ve dezavantajları beraberinde getirmektedir. Bilhassa yapay zekayı besleyen veri setlerinin kalitesiz olması ya da daha doğru ifadeyle ideal seviyeye gelmemiş olmasından dolayı ayrımcılığa maruz kalma gibi istenmeyen olayların da meydana gelebileceği öngörülebilir. Bu gibi durumlara karşı, yapay zekanın hiç kullanılmaması gibi bir argüman üretilmesi kanımızca mantıklı olmayacaktır. Çünkü yapay zeka birtakım önemli avantajları da beraberinde getiren bir teknolojidir ve insanlık için yapabilecekleri bakımından büyük bir potansiyele sahiptir. Ancak yine de yaratılan olumsuz sonuçlara karşı mağdur olan ilgililere etkin itiraz hakkı tanınması yerinde olacaktır. Bu bakımdan ayrımcı sonuçlara karşı önleme ve etkin itiraz prosedürlerinin belirlenmesi ve ilan edilmesi gerekli görülebilir.

KAYNAKÇA

ABANOZ, Buket, Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu, On İki Levha Yayıncılık, İstanbul 2018.

ACAR, Hasan, “Kamu Güvenliğinin Sağlanmasında Weberyen Bürokrasi ve Hiyerarşi Kavramı”, Uluslararası Yönetim İktisat ve İşletme Dergisi, C. 14, S. 3, 2018.

ACEMOĞLU, Daron; RESTREPO, Pascual, “ Robots and Jobs : Evidence From US Labor Markets”, Journal of Political Economy, C. 128, S. 6, 2020, <https://economics.mit.edu/files/19696> (s.y: 20 Şubat 2022).

Açık Rıza, Kişisel Verileri Koruma Kurumu, <https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf>, s. 4-5, (s.y. 30 Kasım 2021).

AGHAEI, Sareh, International Journal of Web & Semantic Technology (IJWest), C. 3, S. 1, Y. 2012, <http://www.airccse.org/journal/ijwest/ijwest.html> (s.y. 10 Şubat 2022).

AKGÜL, Aydın, “Kişisel Verilerin Korunmasında Yeni Bir Hak: “ Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, Türkiye Barolar Birliği Dergisi, S. 116, Y. 2014.

AKINLAR, Cüneyt, Yusuf OYSAL, Hüseyin POLAT, Efnan GÜNAL, Güvenlik Sistemleri, 1., Eskişehir 2012.

AKKURT, Sinan Sami, Kişisel Sağlık Verilerinin İşlenmesi ve Covid-19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukuki Bir Bakış, İTÜSBD, Covid-19 Hukuk Özel Sayısı, 2019.

AKKURT, Sinan Sami, Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış, Kişisel Verileri Koruma Dergisi, C.2 , S.1, Y. 2020.

AKSOY, Hüseyin Can; HALICIOĞLU, Mesut, AB ve Türk Hukukunda Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme, Kişisel Verileri Koruma Dergisi, C.3, S.1, Y. 2021.

AKYILMAZ, Bahtiyar; SEZGİNER, Murat; KAYA, Cemil, Türk İdare Hukuku, 1. Baskı, Seçkin, Ankara 2009.

AKYÜREK, Güçlü, Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı, Seçkin, Ankara 2014.

ALOISI, Antonio; GRAMANO, Elena, “Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context”, Comparative Labor Law & Policy Journal, C. 41, S. 1, Y. 2019.

Amazon “Rekognition”, <https://aws.amazon.com/tr/rekognition/> (s.y. 29 Mart 2022).

American Management Association & ePolicy Institute Research, Electronic Monitoring & Surveillance Survey, 2007, <http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf> (s.y. 28 Kasım 2021).

AN, Yun Joo; CHOI, Paul Moon Sub; HUANG, Seth H., “Blockchain, Cryptocurrency, and Artificial Intelligence in Finance”, P. M. S. CHOI, S. H. HUANG (Ed.), Fintech with Artificial Intelligence, Big Data, and Blockchain, Springer, 2021.

ANDERSEN, Ulrik Christian; POLD, Bro Soren, The Metainterface: The Art of Platforms, Cities, and Clouds, The MIT Press, ABD 2018.

ANDERSON, Steve F., Technologies of Vision: The War Between Data and Images, The MIT Press, ABD 2017.

AREDDY, James T., China Creates Its Own Digital Currency, a First for Major Economy, <https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-formajoreconomy11617634118> (s.y. 19 Şubat 2022).

Arsenal escape FA action for coin throwlingard- the second time they have avoided punishment for missile being launched from the crowd, <https://www.thesun.co.uk/sport/football/8357559/arsenal-escape-fa-action-cointhrowlingard/> (s.y. 21 Ekim 2021).

ARTUK, Mehmet Emin; ALKAN AKCAN, Esra, “Konut Dokunulmazlığının İhlali Suçu”, DEÜHFD, Prof. Dr. Durmuş TEZCAN’a Armağan, C. 21, Özel Sayı, Y. 2019.

ASGHAR, Mamoon N.; KANWAL, Nadia; LEE, Brian; FLEURY, Martin; HERBST, Marco; QIAO, Yuansong, Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective, IEEE Access, C. 7, Y. 2019.

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

Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, KVKK Yönetim Dairesi Başkanlığı, Ankara, Nisan 2019.

BARRETT, Lindsey, “Ban Facial Recognition Technologies for Children - And for Everyone Else”, Boston University Journal of Science and Technology Law, C. 26, S. 2, Y. 2020.

BARTSCH, Byron; COYNE, James; GRAY, Katherine, Drones In Society, Exploring The Strange New World Of Unmanned Aircraft, Routledge, Londra 2018.

BAŞAR, Civan, Devletin Kitleli Gözetleme Araçlarının Özgürlükler ve Hukuk Güvenliği Üzerindeki Etkileri ile Bunların Yasal Dayanakları Üzerine Bir İnceleme, Türkiye Barolar Birliği Dergisi, S. 133, Y. 2017.

BAŞTÜRK, Efe, Panoptikon’ dan Post Panoptikon’ a Gözetimin Soykütüğü (Doktora Tezi), Ankara 2016.

BAUMAN Zygmunt, Küreselleşme, Toplumsal Sonuçları, çev. Akın Emre Pilgir, Ayrıntı Yayınevi, İstanbul 2020.

BAUMAN, Zygmunt, David LYON, Akışkan Gözetim, çev. Elçin Yılmaz, Ayrıntı Yayınevi, İstanbul 2018.

BAYRAKLI, Enes, Kazım KESKİN, Avrupa’nın Mülteci Krizi, Akademik İncelemeler Dergisi, C. 12, S. 2, Y. 2017.

BENNETT, Colin J., Regulating Privacy, Data Protection and Public Policy in Europe and the United States, Cornell University Press, ABD 1992, s. 21’den naklen Elif KÜZECİ, Kişisel Verilerin Korunması.

BENTHAM, Jeremy; PEASE-WATKIN, Catherine; WERRET, Simon; ÇOBAN, Barış; ÖZARSLAN, Zeynep, Panoptikon: Gözün İktidarı, çev. Barış Çoban & Zeynep Özarslan, 3. Baskı, Su Yayınevi, İstanbul 2019.

BIRNHACK, Michael; PERRY-HAZAN, Lotem, Differential Rights Consciousness: Teachers’ Perceptions of Privacy in The Surveillance School, Teaching and Teacher Education, C. 101, Y. 2021.

BIRNHACK, Michael; PERRY-HAZAN, Lotem, School Surveillance in Context: High School Students’ Perspectives on CCTV, Privacy, and Security, Youth & Society, C. 52, S. 7, Y. 2020.

BİLGİN, Metin; ERKAN, Sema; ATASU, İdil; YILMAZ, Enes, Privacy Impact Assessment as a Tool for GDPR Compliance Preparation, Kişisel Verileri Koruma Dergisi, C: 1 , S: 2, Y.2019.

Blokzincirlerde Güvenlik ve Mahremiyet Raporu, Tübitak Bilgem Blokzinciri Araştırma Laboratuvarı, Nisan 2020.

BLOOM, Cara; TAN, Joshua; BAUER, Lujo, "Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles, Proceedings of the Thirteenth Symposium on Usable Privacy and Security, 2017, s. 357, https://www.ftc.gov/system/files/documents/public_comments/2017/11/00046141905.pdf (s.y. 21 Şubat 2022).

BOUCHAGIAR, George, "Privacy and Web 3.0: Implementing Trust and Learning from Social Network, "Review of European Studies, C. 10, S. 4, Y. 2018.

BOUSSIOS, Emanuel Gregory, , "Termination or Accountability? The Controversy over the United States Use of Cyberintelligence." Polish Quarterly of International Affairs, C. 25, S. 2, Y. 2016.

BÖREKÇİ, Eşref Barış, Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu (TCK md. 136.), On İki Levha Yayıncılık, İstanbul 2020.

BRADFORD, Ben; YESBERG, Julia A.; JACKSON, Jonathan; DAWSON, Paul, Live Facial Recognition: Trust And Legitimacy as Predictors of Public Support for Police Use of New Technology, The British Journal of Criminology, C. 60, S 6, Y. 2020.

Brainwash projesi, <https://exposing.ai/brainwash/> (s.y. 02 Kasım 2021), <https://purl.stanford.edu/sx925dc9385> (s.y. 02 Kasım 2021).

BROBST, Jennifer A., The Metal Eye: Ethical Regulation of the State's Use of Surveillance Technology and Artificial Intelligence to Observe Humans in Confinement, California Western Law Review, C. 55, S. 1, Y. 2018.

BROOME, Lissa L., "Banking on Blockchain." North Carolina Journal of Law & Technology, C. 21, S. 1, Y. 2019.

BROUSSELLE, Astrid; BRUNET-JAILLY, Emmanuel; KENNEDY, Christopher; PHILLIPS, Susan D.; QUIGLEY, Kevin; ROBERTS, Alasdair, Beyond COVID-19: "Five Commentaries On Reimagining Governance For Future Crises And Resilience", Canadian Public Administration, C. 63, S. 3 , 2020.

BRUNNON-ERNST, Anne, Beyond Foucault: New Perspectives on Bentham's Panopticon, TY Book, ABD 2012.

BUTARELLI, Giovanni, The European Data Protection Su Video-Surveillance Guidelines, 17 Mart 2010, https://edps.europa.eu/sites/edp/files/publication/100317_videosurveillance_guidelines_en.pdf (s.y. 02 Nisan 2022).

BYGRAVE, Lee A., Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, International Journal of Law and Information Technology, S. 6 , S. 3, Y. 1998.

CAN, Neslihan, Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul 2021.

CASTELLS, Manuel, Ağ Toplumunun Yükselişi, ABD 1996, s. 386'dan naklen: David LYON, Gözetlenen Toplum.

Central bank digital currencies: executive summary, September 2021, <https://www.bis.org/publ/othp42.pdf> (s.y: 19 Şubat 2022).

CERRAH, İbrahim, Bilişim Teknolojileri ve Etik, Bilişim Teknolojilerinin Güvenlik Hizmetlerinde Kullanımının “Etik Boyutu” ve “Sosyal Sonuçları”, Turkish Journal of Police Studies, C. 4 S.1-2, Y. 2002.

CHALMERS, David, What Should Be Considered a Crime in the Metaverse, <https://www.wired.com/story/crime-metaverse-virtual-reality/> (s.y. 14 Şubat 2022).

CHEN, Mu K.; WU, Yonfeng; FENG, Lei; FAN, Qingbin; LU, Minghui; XU Ting; TSAI Din P., Principles, Functions, and Applications of Optical Meta-Lens, Advanced Optical Materials, C.9, S.4, Y. 2021, <https://onlinelibrary.wiley.com/doi/10.1002/adom.202001414> (s.y: 23 Şubat 2022).

CHOI-FITZPATRICK, Austin, The Good Drone-How Social Movements Democratize Surveillance, The MIT Press, ABD 2020.

CLARKE, Roger, “Dataveillance: Delivering ‘1984’”, 9 Şubat 1993, <http://www.rogerclarke.com/DV/PaperPopular.html> (s.y. 8 Şubat 2022).

COMANDE, Giovanni, "The Rotting Meat Error: from Galileo to Aristotle in Data Mining", European Data Protection Law Review (EDPL), C. 4, S. 3, Y.2018.

Crime Beat: Soft Target, BBC One London, 11 March 1996 20.30, A series which reveals the truth about crime in the UK, Combatting crime in public places, (s.y. 1 Nisan 2022).

CUSTER, Bart, Tapping and Data Retention in Ultrafast Communication Networks, Journal of International Commercial Law and Technology, C. 3, S. 2, Y. 2008.

ÇEKİN, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde, Kişisel Verilerin Korunması Hukuku, Onikilevha Yayıncılık, İstanbul 2020.

DAL, Ufuk, “Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti”, Kişisel Verileri Koruma Dergisi, C.1, S.1, Y. 2019.

DAVIS, Jessica, “More Remote Work Leads to More Employee Surveillance”, IT Leadership//Team Building & Staffing, Information Week, <https://www.informationweek.com/strategic-cio/team-building-andstaffing/more-remote-work-leads-to-moreemployee-surveillance/d/d-id/1341366> (s.y. 11 Mart 2022).

DENİZ, Miray Özer, “İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması ve Bundan Doğan Sorumluluk”, Türkiye Adalet Akademisi Dergisi, S. 45, Y. 12, Ocak 2021.

DERDİMAN, Cengiz; TATAROĞLU, Nihal, “Devlet Gözetimi İle İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri”, İnÜHFD, C.7, S.1, Y. 2016.

Diana Paparazzi Trio Face Retrial, http://news.bbc.co.uk/2/hi/uk_news/4442659.stm (s.y. 02 Nisan 2022).

DOE, Susan, “Practical Privacy: Report from the GDPR World”, Legal Information Management, C. 18, S. 2, Y.2018.

DOLGUN, Uğur, Biri Bizi Gözetliyor, Kutu Yayınları, İstanbul 2019.

DOLGUN, Uğur, Çalışma Yaşamında Gözetim, Sosyal Siyaset Konferansları Dergisi, S. 49, Y. 2005.

DOLGUN, Uğur, Enformasyon Toplumundan Gözetim Toplumuna, Ekin Kitabevi, Ankara 2005.

DRAPER, Robert, They Are Watching You and Everything Else on the Planet, National Geographic, (Şubat 2018), <https://www.nationalgeographic.com/magazine/2018/02/surveillance-watching-you/> (s.y. 17 Ekim 2021).

DÜLGER, Murat Volkan, İnsan Hakları ve Temel Özgürlükler Bağlamında Kişisel Verilerin Korunması, İMÜHFD, C. 5, S. 1, Y. 2018.

DÜLGER, Murat Volkan, Kişisel Verileri Koruma Kurulunun 3 Nisan 2019 Tarihli Karar Özetlerine İlişkin Değerlendirme (Evaluation of the Personal Data Protection Board's Decision Summary dated 3 April 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792303, (s.y. 20 Mart 2022).

DÜLGER, Murat Volkan, Kişisel Verilerin Korunması Hakkı Bağlamında İşçilere Ait İletişimin İşveren Tarafından Gözetlenmesi (Supervision of the Communication of the

Workers in the Context of the Right to Protection of Personal Data), s. 5, <https://ssrn.com/abstract=3792265> (s.y. 8 Mart 2022).

DÜLGER, Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul 2020.

EARLS DAVIS, Peter Alexander, “Facial Detection and Smart Billboards: Analysing the 'Identified' Criterion of Personal Data in the GDPR”, European Data Protection Law Review (EDPL), C. 6, S. 3. Y.2020.

EDWARDS, Lilian, “Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective”, European Data Protection Law Review (EDPL), C. 2, S. 1, Y.2016.

ELLIN, Nan, Korkunun Mimarisi, Princeton Architectural Press, New York 1997, s. 44’ten naklen David LYON, Gözetlenen Toplum.

ERBAŞ, Gökhan C., 6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Elektronik Ortamda Gözetlenmesi, HHFD, C. 7, S. 1, Y. 2017.

ERYILMAZ, Mustafa Bedri, Ceza Muhakemesi Hukuku Dersleri, 1. Baskı, Ankara 2012.

Eskişehir Osmangazi Üniversitesi Senato Kararı, https://guvenlik.ogu.edu.tr/Storage/KorumaVeGuvencilikAmirliigi/Uploads/SKMBT_22319041111170.pdf (s.y. 24 Mart 2022).

Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System, <https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html> (s.y: 20 Ekim 2021).

Facial Recognition Tech Is Growing Stronger, Thanks to Your Face, <https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognitiontechnology.html> (s.y. 05 Kasım 2021)

Facial Reconition Technology: Fundamental Rights Considerations in the context of Law Enforcement, European Union Agency For Fundamental Rights, <https://op.europa.eu/en/publicationdetail/publication/0de97f9910db11ea8c1f01aa75ed71a1/language-en#> (s.y. 30 Şubat 2022).

FOUCAULT, Michael, Büyük Kapatılma, çev. I. Ergüden & F. Keskin, Ayrıntı Yayınları, İstanbul 2000.

FOUCAULT, Michel, Hapishanenin Doğuşu, Gözetim Altında Tutmak ve Cezalandırmak, çev. Mehmet Ali Kılıçbay, İmge Kitabevi, Ankara 2019.

FRITH, Jordan, A Billion Little Pieces: RFID and Infrastructures of Identification, The MIT Press, ABD 2019.

FYFE, Nicholas R.; BANNISTER, Jon, City Watching: Closed Circuit Television Surveillance in Public Spaces, The Royal Geographical Society (with the Institute of British Geographers), C. 28, S. 1, Y. 1996.

GANDY, Oscar H., The Panoptic Sort. A Political Economy of Personal Information, Oxford University Press, Oxford Scholarship Online, 2021, s. 29. <https://oxford.universitypressscholarship.com/> (s.y. 30 Mart 2022)

GAUL, Thomas, 2007, Untersuchung der verfassungsrechtlichen Anforderungen an Videoüberwachungsmaßnahmen des Staates im öffentlichen Raum mit und ohne biometrische Erkennungsverfahren unter besonderer Berücksichtigung der hermeneutischen Erkenntnismethoden im Verfassungsrecht, zur Erlangung der Würde eines doctor iuris der Juristischen Fakultät der Julius Maximilians Universität, Würzburg s. 183'ten naklen Cengiz DERDİMAN, Nihal TATAROĞLU.

GEMALMAZ, Mehmet Semih, Temel Belgelerde İnsan Hakları: Maddi Hukuk, İnsan Hakları Derneği Yayını, İstanbul 1996, s. 309-323.

GEMALMAZ, Mehmet Semih, Ulusüstü İnsan Hakları Hukukunun Genel Teorisine Giriş, 7. Baskı, Legal, İstanbul 2010, s. 148.

GEORGE, Joseph; RAMCHANDRAN, Sreelakshmi; A. Nezmi K.; NAIR, Shreya, "Video Surveillance Using Deep Learning", Journal of Critical Reviews, C.7, S. 9, 2020.

GIDDENS, Anthony, Siyaset, Sosyoloji, ve Toplumsal Teori, Toplumsal Düşüncenin Klasik ve Çağdaş Temsilcileriyle Hesaplaşmalar, İstanbul 2017.

GIUFFRIDA, Iria, Smart Cities and Sustainability: A New Challenge to Accountability? Symposium Issue: Sustainability in the City, William & Mary Environmental Law and Policy Review, C. 45, S. 3, Y. 2021.

GIVENS, John Wagner; LAM, Debra, "Smarter Cities or Bigger Brother? How the Race for Smart Cities Could Determine the Future of China, Democracy, and Privacy", Fordham Urban Law Journal, C. 47, S. 4, Y. 2020.

Glasgow City Council, Mobile CCTV, <https://www.glasgow.gov.uk/article/23765/Mobile-CCTV> (s.y. 20 Ekim 2020)

GOLLA, Sebastian J., "Is Data Protection Law Growing Teeth: The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR." Journal of

Intellectual Property, Information Technology and Electronic Commerce Law, C. 8, S. 1, Y. 2017.

GOOLD, Benjamin J., How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy, Allard Faculty Publications (Working Paper), 2010.

GOOLD, Benjamin J., Open to all? Regulating open street CCTV and the case for “symmetrical surveillance”, Criminal Justice Ethics, C. 25, S. 1, 2006.

GÖZÜBÜYÜK, Şeref A.; TAN, Turgut, İdare Hukuku, Genel Esaslar, 6. Baskı, Turhan Kitabevi, Ankara 2008.

GRAHAM, Stephen; BROOKS, Jon; HEERY, Dan, “Towns on the Television: Closed Circuit TV Surveillance In British Towns and Cities”, Electronic Working Paper No. 17, <https://www.ncl.ac.uk/mediav8/apl/files/guru-ewp/ewp17.pdf> s. 6, (s.y. 28 Kasım 2021).

GRAHAM, Stephen, The Fifth Utility, Sage Journals, C. 29, S. 3, 2000.

GREENBERG, Andy, “Hackers Remotely Kill a Jeep on the Highway, with me in it”, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (s.y. 6 Mart 2022).

HABERMAS, Jürgen, , İletişimsel Eylem Kuramı, çev. Mustafa Tüzel, Alfa Yayınları, İstanbul 2019.

Hacettepe Üniversitesi, “Güvenlik Kamera Sistemleri Kurma ve İşletme Yönergesi”, https://hacettepe.edu.tr/duyuru/yonergeler/HUGuvenlikKameraSistemleriKurmaIsletmeYonergesiEk_240521.pdf (s.y. 24 Mart 2022).

HAFIZOĞULLARI, Zeki; ÖZEN, Muharrem, “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”, Ankara Barosu Dergisi, S. 4, Y. 2009.

HAGGERTY, Kevin D.; ERICSON, Richard V., “The Surveillant Assemblage”, British Journal of Sociology C. 51, S. 4, Y. 2000.

HAS, Murat, AİHM Kararları Bağlamında Görüntü Hakkı, Anayasa Yargısı, C. 38, S. 1, Y. 2021.

HELD, Cornelius; KRUMM, Julia; MARKEL, Petra; SCHENKE, Ralf P., “Intelligent Video Surveillance”, in Computer, C. 45, S. 3, Y. 2012.

HELMS, Shawn C., “Translating Privacy Values with Technology”, Boston University Journal of Science and Technology Law, C.7, Y. 2001.

HENDERSON, Harry, Privacy in the Information Age, Facts of File, ABD, 2006.

HODGE, Samuel J., Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century, University of Cincinnati Law Review, , C. 89, S. 1, Y. 2020.

HOLLIS, Meghan E., Security or Surveillance, Examination of CCTV camera usage in the 21st century, CCTV Surveillance or Crime Prevention, Criminology & Public Policy, S. 18, Y. 2019.

HU, Junyan; LANZON, Alexander, “An innovative tri-rotor drone and associated distributed aerial drone swarm control”, Robotics and Autonomous Systems, S. 103, Mayıs 2018.

HUNTER, Dan; BAGARIC, Mirko; STOBBS, Nigel, “A Framework for the Efficient and Ethical Use of Artificial Intelligence in the Criminal Justice System”, Florida State University Law Review, C. 47, S. 4, Y.2020.

ICO, “Guidance on Video Surveillance”, <https://ico.org.uk/media/for-organisations/guide-to-data-protection-key-dp-themes/guidance-on-video-surveillance-0-0.pdf>, (s.y. 30 Mart 2022).

IGNAC-NOWICKA, Jolanta, Visual Monitoring as a Tool in Industrial Security Engineering, Mape, C. 4, S.1, Y. 2021.

Information Commissioner’s Opinion: The Use of Live Facial Recognition Technology in Public Places, 18 Haziran 2021, s. 4, <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places20210618.pdf> (s.y. 11 Kasım 2021).

Instruction no. 1/2006 of 8 November 2006 on the processing of personal data for monitoring purposes using video-surveillance devices, issued by the Spanish Data Protection Agency.

International Labour Office, Conditions of Work Digest, Workers’ privacy Part II: Monitoring and surveillance in the Workplace, C. 12, S. 1, Y. 1993.

International Labour Office, Technical and Ethical Guidelines for Workers’ Health Surveillance, Cenevre 1998.

Into The Metaverse, Powering the development of the future internet 3.0: themetaverse, <https://www.wired.com/sponsored/story/into-the-metaverse/> (s.y. 14 Şubat 2022).

İçişleri Bakanlığı İller İdari Genel Müdürlüğü'nün 30 Kasım 2018 tarih ve Alınacak Tedbirler Konulu Yazısı, <https://www.istesob.org.tr/wp-content/uploads/2018/12/214-Nolu-Genelge-Alinacak-TedbirlerHakkinda.pdf> (s.y: 28 Kasım 2021).

İHA Duyurusu İstanbul Valiliği, <http://istanbul.gov.tr/kurumlar/istanbul.gov.tr/guncel/duyurular/insasiz-hava-araci-duyurulari/iha-gelen-emir.pdf> (s.y. 30 Şubat 2022).

İMANÇLI, Canan, Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu, İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi, On İki Levha Yayıncılık, İstanbul 2020.

JABOTİNSKY, Hadar Y.; SAREL, Roe, “How the Covid-19 Pandemic Affected the Cryptocurrency”, Columbia Law School’s Blog on Corporations and The Capital Markets, Marc 2021, <https://clsbluesky.law.columbia.edu/2021/03/26/how-the-covid-19-pandemic-affected-the-cryptocurrency-market/> (s.y. 19 Şubat 2022).

JIMENEZ, Emmanuel, A. P., The Fourth Amendment Limits of Facial Recognition at The Border, Duke Law Journal, C.70, S. 1837, Y. 2021.

JOH, Elizabeth E., The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing, Harvard Law & Policy Review, C. 10, S. 1, Y. 2016.

KANG, Choi Il; JUNG, Lee Hee; LEE, BHUM Cheol, "A Distributed Cloud based Video Storage System with Privacy Protection " *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017.

KANG, Choi Il; JUNG, Lee Hee; LEE, Bhum Cheol, Cloud Based Video Storage System With Privacy Protection, *17th International Conference on Advanced Communication Technology (ICACT)*, 2015.

KARAKEHYA, Hakan, “Gözetim ve Suçla Mücadele”: Gözetimin Tarihsel Gelişimi ile Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme, AÜHFD, C. 58, S.2, Y.2009.

KAYA, Cemil, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, İÜHFM, C. 69, S. 1-2, Y. 2011.

KGYS ve PTS Projesi, Bilgi Teknolojileri ve Haberleşme Daire Başkanlığı, <https://www.egm.gov.tr/bilgiteknolojilerivehaberlesme/kgysvepts> (s.y. 2 Mart 2022)

KHERIA, Smita; SITHIGH, D. Mac; RAUHOFER, Judith; BURKHARD, Schafer, “CCTV Sniffing”: Copyright and Data Protection Implications, S. 2013/2, CREATE Working Papers, Y. 2013.

KHOUDOUR, Louahdi, DEPARIS, Jean Pierre; BRUYELLE, Jean-Luc, CABESTAING F.; AUBERT, Didier; BOUCHAFA, Samia; VELASTIN, Sergio A.; VICENCIO-SILVA, Maria Alicia; WHERETT M., Project Cromatica, International Conference on Image Analysis and Processing (ICIAP), C.2, Y. 1997.

KIETZMANN, Jan; ANGELL, Ian, “Panopticon Revisited”, Communications of the ACM, C.53, S. 6, Y. 2010.

KIM, Pauline T., "Data Mining and the Challenges of Protecting Employee Privacy under U.S. Law", Comparative Labor Law & Policy Journal, C. 40, S. 3, Y. 2019.

Kişisel Verileri Koruma Kurulu, Karar Özetleri, Hizmetin Açık Rıza Şartına Bağlanması, (<https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi>, (s.y. 26 Ocak 2021).

Kişisel Verileri Koruma Kurumu, 2020 Yılı Faaliyet Raporu, s. 36, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/60c02fcc-0abf-4c8e-8b9b514f34a1b0e6.pdf> (s.y. 19 Mart 2022).

Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Kişisel Verileri Koruma Kurumu, KVKK Yayınları, No:1, Ankara, Aralık 2019.

KOCACIK, Faruk, “Bilgi toplumu ve Türkiye”, C.Ü. Sosyal Bilimler Dergisi, C. 27, S. 1, Y.2003.

KÖKKİLİNÇ, Ayşe Gül, “Ev Hizmetlerinde Çalışan İşçinin İş İlişkisi”, DEÜİFD, C. 20, S. 2, Y. 2019.

KRUEGLE, Herman; ABRHAM, Frank, CCTV Surveillance: Analog and Digital Video Practices and Technology, Butterworth-Heinemann, ABD 2006.

KUGLER, Matthew B., “From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms”, UC Irvine Law Review, C. 10, S. 1, Y. 2019.

KUNER, Christopherİ MARELLİ, Massimo, Handbook on Data Protection in Humanitarian Action, 2017.

KURT, Leyla Müjde, Kamuya Mal Olmuş Kişi Kavramı, AÜHFD, C. 66, S. 3, Y. 2017.

KÜÇÜK, Tevfik Sönmez, Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı ile Önleyici Amaçla İzlenmesi, YUHFD, C. 15 , S. 1, Y. 2018.

KÜZECİ Elif, Kişisel Verilerin Korunması, Onikilevha Yayıncılık, İstanbul 2021.

KÜZECİ, Elif, Sayısal Fil, Bilişim Teknolojileri, Devlet ve Hukuk Kesişiminde Bir İnceleme, İnkılap Kitabevi, İstanbul 2021.

KWET, Michael, , The Rise of Smart Camera Networks, and Why We Should Ban Them, The Intercept, Police are using cameras at private businesses and homes, along with AI, to expand their video surveillance — raising privacy concerns. January 27 2020, 8:53 p.m., <https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/> (s.y. 15 Kasım 2021).

LESSIG, Lawrence, Code Version: 2.0, Basic Books, New York 2006.

LODDER, Arno R., “Dutch Supreme Court 2012: Virtual Theft Ruling a One-Off or First in a Series? ”, Journal of Virtual Worlds Research, C. 6, S. 3, Y. 2013.

LOYAL, Steven, The Sociology of Anthony Giddens, Pluto Press, Virginia 2003.

LUCK, Morgan, “The Gamer’s dilemma: An analysis of the arguments fort he moral distinction between virtual murder and virtual paedophilia” , Ethics and Information Technology, S.11, Y. 2009.

LUQUE–AYALA, Andres; MARVIN, Simon, Urban Operating Systems: Producing the Computational City, The MIT Press, ABD 2020.

LYON, David, Elektronik Göz, çev. Dilek Hattatoğlu, Sarmal Yayınevi, İstanbul, 1997.

LYON, David, Gözetim Çalışmaları, Genel Bir Bakış, çev. Ali Toprak, Kalkedon, İstanbul 2013.

LYON, David, Gözetlenen Toplum, Günlük Hayatı Kontrol Etmek, çev. Gözde Soykan, Kalkedon, İstanbul 2006.

LYON, David, Vesikalı Yurttaş , Gözetim Aracı Olarak Kimlik Kartları, çev. Barış Baysal, Kalkedon, İstanbul 2012.

MARSHALL, Gordon, A Dictionary of Sociology, <https://www.encyclopedia.com/social-sciences-and-law/sociology-and-social-reform/sociology-general-terms-and-concepts-80> (s.y. 8 Şubat 2022).

MATHIESEN, Thomas, The Viewer Society, Theroerical Criminology, C.1, S.1, 1997.

MATTELART, Armand, Gözetimin Küreselleşmesi, Güvenlileştirme Düzeninin Kökeni, çev. O. Gayretli & S. E. Karacan, Kalkedon, İstanbul 2012.

MAYBELL, Romero, Educational Environments and the Federal Right to Education in the Wake of Parkland, University of Miami Law Review, C. 73, S. 3, Y. 2019.

MAYER, Marco; SCALZI, Niccolo de; MARTINO, Luigi; CHIARUGI, Iacopo, International Politics in the Digital Age: Power Diffusion or Power Concentration?, XXVIIth SISP CONFERENCE, University of Florence, 12-14 Eylül 2013.

MERLER, Michele; RATHA, Nalini; FERIS, Rogerio; SMITH, John R., Diversity in Faces, IBM Research AI, Nisan 2019.

MESSERI, Lisa, The Man, the Myth, and the Metaverse, <https://www.wired.com/story/theman-the-myth-and-the-metaverse/> (s.y. 14 Şubat 2022).

MILLER, Arthur R., The Assault on Privacy, Computers, Data Banks, and Dossiers, The University of Michigan Press, ABD 1971.

MOON, Hae-Min; PAN, Sung Bum, SSIRI 2009 Fast Abstract Implementation of the Privacy Protection in Video Surveillance System, Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009.

MÖLLERS, Norma; HÄLTERLEIN, Jens, "Privacy issues in public discourse: the case of "smart" CCTV in Germany", Innovation: The European Journal of Social Science Research, C. 26, S. 1-2, 2013.

MUKHOPADHYAY, Subhas Chandra, Internet of Things: Challenges and Opportunities, Springer, 2014.

MURDOCH, Steven J.; ANDERSON, Tools and Technology of Internet Filtering, Ronald DEIBERT, John PALFREY, Rafal ROBOZINSKI, Jonathan ZITTRAIN (Ed.), Access Denied: The Practice and Policy of Global Internet Filtering, The MIT Press, ABD 2008.

MURPHY, Julian R., Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests. Washington and Lee Law Review Online, S. 75, Y. 2018.

MUTLU, Didem; ARI, Mehmet, Foucault ve Agamben Düzleminde Biyo-Politika, Fiscoeconomia, C. 4, S. 1, Y. 2020.

National Nanotechnology Coordination Office, Nanotechnology: Big Things from a Tiny World (Brochure), 16 Mart 2018.

NELSON, Anthony, "Smart Transportation Systems: Sustainable Mobilities, Autonomous Vehicle Decision-Making Algorithms, and Networked Driverless Technologies." Contemporary Readings in Law and Social Justice, C. 12, S. 2, Y. 2020.

NEWEL, Bryce Clayton, Police On Camera: Surveillance, Privacy and Accountability, Routledge, New York 2020.

NICHOLLS, Andy, Nick LOWLES, Hooligans 2: The M-Z of Britain's Football Hooligan Gangs, Milo Books, Birleşik Krallık 2007.

NORRIS, Clive; MORAN, Jade; ARMSTRONG, Gary, Surveillance, Closed Circuit Television and Social Control, Routledge, New York 2016.

NORRIS, Clive; MCCAHERILL, Mike; WOOD, David, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", Surveillance&Society, C.2, S.2/3, Y. 2004.

NOUH, Rayan M.; SINGH, Dhananjay, "Introducing Blockchain for Smart City Technologies and Applications", Dhananjay SINGH, Navin Singh RAJPUT (Ed.), Blockchain Technolog for Smart Cities, Springer, 2020.

O'BOYLE, Michael; HARRIS, David; WARBRICK, Colin, Law of the European Convention on Human Rights, 3. Baskı, Oxford University Press, Oxford 2014.

O'DONOGHUE, Amy, "Sovereign Exception: Notes on the Thought of Giorgio Agamben, <https://criticallegalthinking.com/2015/07/02/sovereign-exception-notes-on-the-thought-of-georgioagamben/> (s.y: 22 Şubat 2022).

O'FLAHERTY, Michael, "Facial Recognition Technology and Fundamental Rights". European Data Protection Law Review (EDPL), C. 6, S. 2, 2020.

OĞUZ, Habip, Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, Elektronik Ticaret Hukuku Sempozyumu, 25 Nisan 2014.

ORWELL, George, 1984, 3. Basım , çev. Celal Üster, Can Yayınları, İstanbul 2019.

ÖNCÜ, Gülay ARSLAN, Özel Yaşama ve Aile Yaşamına Saygı Hakkı, Epamat Basım, Ankara 2019.

PARK, Tae-Sung; JUN, Moon-Seog, User Authentication Protocol for Blocking Malicious User in Network CCTV Environment, 2011 6th International on Computer Sciences and Converges Information Technology (ICCIT), 2011.

PAŞAOĞLU, Cengiz; CEVHEROĞLU, Emel, Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması, Bilişim Teknolojileri Dergisi, C. 13, S. 2, Nisan 2020.

PESTER, Rachel, “Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act (“BIPA”) Violation Suit”, Ed. Jordan KENNEDY, <https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit>, (s.y. 27 Mart 2022).

PLATA, Marcin; SYGA, Piotr; KLONOWSKI, Marek, How to Save Your Face: a Facial Recognition Method Robust Against Image Reconstruction, IEEE 10th International Conference on Biometrics Theory, Applications and Systems, 2019.

PLATTE, Benny; THOMANEK, Rico; ROLLETSCHEKE, Tony, ROSCHKE, Christian; RITTER, Marc, “Person Tracking and Statistical Representation of Person Movements in Surveillance Areas”, International Journal of Design, Analysis and Tools For Integrated Circuits And Systems, C. 7, S. 1, 2018.

POLNet Nedir ?, Bilgi Teknolojileri ve Haberleşme Daire Başkanlığı, <https://www.egm.gov.tr/bilgiteknolojilerivehaberlesme/projeler/> (s.y. 20 Şubat 2022).

POPOV, Serguei, “IOTA; Feeless and Free”, IEEE Blockchain Technical Briefs, January 2019, <https://blockchain.ieee.org/technicalbriefs/january-2019/iota-feeless-and-free> (s.y. 20 Şubat 2022).

POSTER, Mark, The Second Media Age, Polity Press, Büyük Britanya 1995.

POUDEL, Swaroop, Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security, Berkeley Tech. Law Journal., Annual Review, C. 31, Y. 2016.

PRATES, Marcelo M., "Money in the Twenty-First Century: From Rusty Coins to Digital Currencies.", Ohio State Business Law Journal, C. 15, S. 1, Y. 2021.

Preparing for Large-scale Community Transmission of Covid-19, Guidance for Countries and Areas in the WHO Western Pacific Region, World Health Organization, 28 Şubat 2020.

PRIDMORE, Jason, Loyalty Cards in the United States and Canada, Elia Zureik (Haz.), Surveillance, Privacy and the Globalization of Personal Information, Montreal; McGill Quen’s University Press, ABD 2010.

QUIROZ-GUTIERREZ, Marco, “Crypto is fully banned in China and 8 other countries”, <https://fortune.com/2022/01/04/crypto-banned-china-other-countries/> (s.y. 19 Şubat 2022).

RAHIM, Eva Rose, “Informartion Security In The Internet Age”, İsmail NORISWADI, Edwin Lee YONG CIEH (Ed.), Beyond Data Protection, Strategic Case Studies and Practical Guidance, Springer Books, Y. 2013.

RAJPOOT, Mahmood Q., Christian D. JENSEN, Video Surveillance: Privacy Issues and Legal Compliance, V. Kumar, J. Svensson (Ed.), Promoting Social Change and Democracy through Information Technology, IGI Global, Y. 2015, s. 10.

RAVENSCLAF, Eric, What Is the Metaverse, Exactly?, <https://www.wired.com/story/what-is-themetaverse/> (s.y. 04 Şubat 2022).

RETTINGER, Lizie, “The Human Rights Implications of China's Social Credit System”, Journal of High Technology Law, C. 21, S. 1, 2021.

REZENDE, Isadora Neroni, “Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective”, New Journal of European Criminal Law, C. 11, S. 3, Y. 2020.

RICHARDS, Neil M., The Dangers of Surveillance, Harvard Law Review, C. 26, S. 7, Y. 2013.

Right of Access, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-generaldata-protection-regulation-gdpr/individualrights/right-of-access/> (s.y. 19 Nisan 2021).

ROBIN, Lily; PETERSON, Bryce E.; LAWRENCE, Daniel S., How Do Close-Circuit Television Cameras Impact Crimes And Clearances? An Evaluation of The Milwaukee Police Department’s Public Surveillance System, Police Practice and Research, C. 22, S. 2, Y. 2021.

RUBINSTEIN, Ira S., Privacy Localism, Washington Law Review, C. 93, S. 4, Y. 2018.

SAMOILI, Sofia; LOPEZ-COBO, Montserrat; GOMEZ, Emilia; De PRATO, Giuditta, MARTINEZ-PLUMED, Fernando; DELIPETREV, Blagoj, “AI Watch Defining Artificial Intelligence, Towards an operational definition and taxonomy of artificial intelligence”, Publications Office of the European Union, Luxembourg Y. 2020.

SAMUELSON, Pamela, Privacy As Intellectual Property?, Stanford Law Review, C. 52, S. 5, Y. 2000.

SAVAŞ, Burcu F., İş Hukukunda “Siber Gözetim”, Çalışma ve Toplum, 2009/3.

SAYGILI, Abdurrahman, Mikro-İktidarın Bir Fiziği: Hapishane, AÜHFD, C. 53, S.2, Y. 2004.

SAYIN, Ali Kemal, ILO Normlarının ve Örgütün Denetim Mekanizmasının Türk İş Hukukuna Etkisi, Çalışma ve Sosyal Güvenlik Bakanlığı, Çalışma Dünyası Dergisi, C.1, S. 1, Temmuz – Eylül 2013.

SCHAFER, Burkhard, Crowdsourcing and Cloudsourcing CCTV Surveillance, Datenschutz und Datensicherheit, C. 37, S. 7, Y. 2013.

SCHARTUM, Dag Wiese, "Making Privacy by Design Operative", International Journal of Law and Information Technology, Oxford University Press, C. 24, S. 2, Y.2016.

SCHUEFFEL, Patrick, The Concise Fintech Compendium, Friborg: School of Management Fribourg 2017, https://www.researchgate.net/publication/322819310_The_Concise_Fintech_Compendium (s.y. 13 Şubat 2022).

SCHWITZGEBEL, Eric, "Should Your Driverless Car Kill You Others May Live?" , A Theory of Jerks and Other Philosophical Misadventures, MIT Press, ABD 2019.

SHARAD, Mrigank; SIDHU, Robin Singh, Smart Surveillance System for Detecting Interpersonal Crime, International Conference on Communication and Signal Processing (ICCSP), 2016.

SHARLACH, Molly, Researchers Shrink Camera to the Size of a Salt Grain, Princeton University, <https://www.nanowerk.com/nanotechnology-news2/newsid=59252.php> (s.y: 23 Şubat 2022).

SHARMA, Pratima; WALIA, Gurjit Singh; ROHILLA, Rajesh, "Recent Advancement in Cancelable Biometric for User Recognition: A Brief Survey," *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 2020, s.137. SHORT, Emma, Jason DITTON, "Does CCTV Affect Crime?", CCTV Today, C. 2, S. 2, Y. 1995.

SINGH, Gurinder; GARG, Vikas; TIWARI, Pooja, "Introduction to Blockchain Technology", R. AGRAWAL, N. GUPTA (Ed.), Transforming Cybersecurity Solutions Using Blockchain, Springer, 2021.

SIMONJAN, Jennifer; AKYILDIZ, Ian F.; JORNET, Josep Miquel; RINNER, Bernhard, Nano-Cameras: A Key Enabling Technology for the Internet of Multimedia Nano-Things, NANOCOM, Reykjavik, İzlanda, 5-7 Eylül 2018.

SLOBOGIN, Christopher, "Government Data Mining and the Fourth Amendment", The University of Chicago Law Review, C. 75, S. 1, Y. 2007.

SOLMAZ, Eren, Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunması"na Katkısı, İdare Hukuku ve İlimleri Dergisi, C. 18, S. 1, Y. 2018.

SOLOVE, Daniel J., The Digital Person: Technology and Privacy in the Information Age, New York University Press, 2004.

Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti. <https://www.kvkk.gov.tr/Icerik/5496/2019-81-165>, (s.y. 01 Kasım 2021).

STANLEY, Jay, Police Body-Mounted Cameras: WithRight Policies in Place, a Win For All, Version 2.0, American Civil Liberties Union (ACLU) Policy, 2015.

Statista, “Global digital population as of January 2021”, <https://www.statista.com/statistics/617136/digitalpopulationworldwide/#:~:text=As%20of%20January%202021%20there,the%20internet%20via%20m> (30 Mart 2022).

STERNLIGHT, Jean R., Justice in a Brave New World? Connecticut Law Review, C. 52, S.1, Y. 2020.

STEWART, Russell; ANDRILUKA, Mykhaylo; NG Andrew Y., End-to-End People Detection in Crowded Scenes, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.

Suicide Statistics (Freedom of Information request to Transport for London) , What Do They Know, Ekim - Kasım 2011, https://www.whatdotheyknow.com/request/suicide_statistics (s.y. 28 Kasım 2021).

SURETTE, Ray; IDREES, Haroon; SHAH, Mubarak, “Enhancing Camera Surveillance Using Computer Vision:A Research Note”, Policing: An International Journal, C. 41, S. 2, 2018.

Surveillance Camera Code of Practice, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/282774/SurveillanceCameraCodePractice.pdf>, (s.y. 06 Şubat 2021).

Surveillance Chess, <http://chess.bitnik.org/> (s.y. 10 Şubat 2022).

ŞİMŞEK, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta, İstanbul 2008.

T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı, DPT Yayın No: 2826, Bilgi Toplumu İstatistikleri, Haziran 2011.

TalkTalk Gets Record £400,000 Fine for Failing to Prevent October 2015 Attack, ayrıntılı bilgi için bkz. <https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded> (s.y. 02 Nisan 2022).

TANSUĞ, Avniye, “AB’ nin Yeni Ekonomik Silahı: “ Veri Saklama Hukuku”, Bilişim Hukuku, (Der.) Mete Tevetoğlu, Kadir Has Üniversitesi Yayınları, İstanbul 2006.

TAYLOR, Nick, "You've Been Framed: The Regulation of CCTV Surveillance.", Journal of Civil Liberties, C. 7, S. 2, Y. 20002.

TEKERGÜL, Mehmet, İşyerinde Elektronik Gözetim Uygulamaları (Yüksek Lisans Tezi) İstanbul 2010.

TERZİOĞLU, Faruk, Bitcoin’de Mahremiyet, 26.09.2019, <https://blokzincir.bilgem.tubitak.gov.tr/bzcalistay/bzcalistay2/documents/sunum/Faruk%20Terzio%C4%9Flu.pdf> (s.y: 20 Şubat 2022).

The EDPS: Supervising EU institutions and bodies & enforcing data protection principles, EDPS factsheet 3, European Data Protection Supervisor, https://edps.europa.eu/site/s/edp/files/publication/factsheet_3_en.pdf (s.y. 30 Kasım 2021).

TIAN, Zifeng, , “A Robust Framework for Mining You Tube Data” , Theses, Dissertations and Capstones, Marshall Digital Scholar, Marshall University, S. 1129, Y. 2017.

TINNEFELD THERES, Marie; BUCHNER, Benedikt; PETRI, Thomas, Einführung in das Datenschutzrecht, Odenbourg Verlag, 5. Auflage, München, 2012, s. 245’ten naklen Tevfik Sönmez KÜÇÜK.

TOFFLER, Alvin, Üçüncü Dalga, çev. Selim Yeniçeri, Koridor Yayıncılık, İstanbul 2018.

Trafik Yönetim Sistemleri, Ulaşım Yönetim Merkezi, <https://uym.ibb.gov.tr/hizmetler/trafik-yonetim-sistemleri>, (s.y. 5 Mart 2022).

Türkiye Cumhuriyeti Merkez Bankası, “Merkez Bankası Dijital Türk Lirası Ar-Ge Projesi Hakkında Basın Duyurusu”, S. 2021-40, 15/09/2021, <https://www.tcmb.gov.tr/wps/wcm/connect/7afe5eab0a8f4a859e2790f2d41f225f/DUY202140.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-7afe5eab-0a8f-4a85-9e27-90f2d41f225f-nLF8y.z> (s.y: 19 Şubat 2022).

Türkiye İstatistik Kurumu, Dış Ticaret Verileri, Kasım 2020, Yayın Tarihi: 31/12/2020, Sayı: 33859, <https://data.tuik.gov.tr/Bulten/Index?p=Dis-Ticaret-Istatistikleri-Kasim-2020-33859> (s.y. 10 Ocak 2022).

TÜRKMEN, Sevgi, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, (Yüksek Lisans Tezi), İstanbul 2019.

Tüzel kişiliğe ait verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkında 19/11/2018 tarihli ve 2018/131 sayılı Karar Özeti, <https://www.kvkk.gov.tr/Icerik/5423/2018-131> (s.y. 20 Mart 2022).

URSİC, Helena, "Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control." *SCRIPTed: A Journal of Law, Technology and Society*, C. 15, S. 1, Y. 2018.

van den HOVEN van GENDEREN, Robert, "Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics", *European Data Protection Law Review (EDPL)*, C. 3, S. 3, Y. 2017.

van den HOVEN, Jeroen; VERMAAS, Pieter E., Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon, *Journal of Medicine and Philosophy*, S. 32, Y. 2007.

VERECKEY, Betsy, "Bitcoin: Who owns it, who mines it, who's breaking the law", MIT Management Sloan School, <https://mitsloan.mit.edu/ideas-made-to-matter/bitcoin-who-owns-it-who-mines-it-whos-breaking-law> (s.y. 19 Şubat 2022).

VERMEULEN, Mathias; BELLANOVA Rocco, European "Smart" Surveillance: What's at Stake for Data Protection, Security and Human Rights, C. 23, S. 4, Y. 2013.

WHO Director-General's opening remarks at the media briefing on COVID-19, 11 Mart 2020, <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> (s.y. 28 Kasım 2021).

WOLFRAM, Stephen, A Kind of Science, Wolfram Media Inc., Kanada 2002, s. 1193.
World of Work The Magazine of The International Labour Office, No. 59, Nisan 2007.

WURSTER, Simone; KAMARA, Irene; SVEINSDOTTIR, Thordis, Certified Security Systems For Sustainable Cities of The 21st Century, *ITU Kaleidoscope: ICTs for a Sustainable World*, 2016.

XIAO, Bin; WU, Haiping; WEI, Yinchun, "Simple Baselines for Human Pose Estimation and Tracking", *European Conference on Computer Vision*, 2018.

YAKUPOĞLU, Aylin; ÇALICI, Can; ZİYALAR, Neylan, "Suçların Aydınlatılmasında CSI Etkisi", *Adli Tıp Bülteni*, C. 21, S. 2, Y. 2016.

YILDIRIM, Banu Fulya, "Sağlığın Kişiselleşmesi ve Kişisel Sağlık Bilgi Sistemleri, *Bilim Yönetimi Dergisi*", C.2, S.2, 2019.

YILDIRIM, Turan; YASİN, Melikşah; KAMAN, Nur; ÖZDEMİR, Eyüp; ÜSTÜN, Gül; TEKİNSOY, Özge Okay, İdare Hukuku, 6. Baskı, On İki Levha, İstanbul 2016.

YÜCEDAĞ, Nafiye, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, Kişisel Verileri Koruma Dergisi, C. 1, S.1, Y. 2019.

YÜKSEL, Erkan M.; ZAİM Halim A., Otomatik Nesne Tanımlama Teknolojisi Olarak RFID ve RFID' in Faydaları, s.1, https://www.emo.org.tr/ekler/c005118de912f94_ek.pdf (s.y. 12 Eylül 2021).

“4/2004 of the Article 29 Data Protection Working Party on the Processing of Personal Data by means of Video-Surveillance, part 7 (E)”, s. 13, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf, (s.y. 30 Mart 2022).

“Alenileştirme” Hakkında Kamuoyu Duyurusu, <https://www.kvkk.gov.tr/icerik/6843/-alenilestirme-hakkinda-kamuoyu-duyurusu> (s.y. 23 Mart 2022).

“Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”, <https://www.kvkk.gov.tr/Icerik/7047/BiyometrikVerilerinIslenmesindeDikkatEdilmesiGereken-HususlaraIliskinRehber> (s.y. 05/11/2021).

“Domestic CCTV Systems Guidance for People: Using CCTV”, <https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/> (s.y. 02 Şubat 2021)

“Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/document.cfm?doc_id=44137, (s.y. 24 Mart 2022).

“Güvenli Parklar” projesi hakkında bkz. <https://www.fatih.bel.tr/tr-TR/parklarimizin-guvenligini-artirmaya-devam-ediyoruz-8345> (s.y. 5 Şubat 2022).

“İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/331 Sayılı Karar Özeti, <https://kvkk.gov.tr/Icerik/6623/2019-331>, E.T: (s.y. 22 Aralık 2020).

“Karar verildi! İstanbul’da 15 bin taksiye kamera” , <https://www.hurriyet.com.tr/gundem/15-bin-taksiye-kamera-41896672> (s.y. 5 Mart 2022) “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı.

“Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003)” , European Committee on Legal Co-operation (CDCJ), 20-23 Mayıs 2003, <https://rm.coe.int/168068416b>, (s.y. 30 Mart 2022).

“Ses özelliği bulunan güvenlik kamerası kullanılması” ile ilgili Kişisel Verileri Koruma Kurulu’nun 12/03/2020 tarihli ve 2020/212 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6892/2020-212>, (s.y. 30 Mart 2022).

“Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/167 Sayılı Karar Özeti”, <https://www.kvkk.gov.tr/Icerik/6738/2020-167> (s.y. 21 Mart 2022).

“Taksilerde Ses ve Görüntü Kaydı Yargıya Taşındı”, <https://www.istanbulbarosu.org.tr/HaberDetay.aspx?ID=12625> (s.y. 05 Şubat 2022).

“Toplu Ulaşım Hizmetleri Müdürlüğü Kamera Görüntü Talep İşlemleri İçin İzlenecek Adımlar”,<https://tuhim.ibt.gov.tr/haberler/topluula%C5%9F%C4%B1mhizmetlerimuedue%rlue%C4%9Fuekameragoeruentuetalep%C4%B0%C5%9Flemleri%C4%B0%C3%A7in%C4%B0zlenecek-ad%C4%B1mlar/> (s.y. 6 Şubat 2022).

6689 Sayılı Kanun’ da Yer Alan Terimler, Kişisel Verileri Koruma Kurumu, <https://www.kvkk.gov.tr/Icerik/4186/6698-Sayili-Kanunda-Yer-Alan-Terimler> (s.y. 02 Şubat 2022).