Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Kamu Hukuku Anabilim Dalı

KAMUSAL ALANDA İDARENİN VİDEO GÖZETİMİNİN KİŞİSEL VERİLERİN KORUNMASI HUKUKU BAĞLAMINDA DEĞERLENDİRİLMESİ

Ezgi TURGUT BİLGİÇ

Yüksek Lisans Tezi

Ankara, 2023

KAMUSAL ALANDA İDARENİN VİDEO GÖZETİMİNİN KİŞİSEL VERİLERİN KORUNMASI HUKUKU BAĞLAMINDA DEĞERLENDİRİLMESİ

Ezgi TURGUT BİLGİÇ

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Kamu Hukuku Ana Bilim Dalı

Yüksek Lisans Tezi

Ankara, 2023

ÖNSÖZ

Video gözetim sistemleri bugün pek çok ülkede kamu otoritelerince başvurulan, teknolojiye paralel olarak günden güne gelişen görüntü takip cihazlarıdır. Artık bu sistemlerin kurulumları geçmiş yıllara nazaran çok daha ucuz ve kolaydır. Ancak yaygın şekilde kullanılan gözetim cihazlarının kişisel veri elde etmesi durumunda özel hayatın gizliliğine yönelik olası ihlallerin önüne geçilmesi ve kayda alınan bireyler ile görüntüleri kaydeden kamu otoritelerinin menfaat dengesinin sağlanması gerekir. Video gözetimin tercih sebepleri genel olarak; kamu güvenliğinin tesisi, suç işlenmesinin önlenmesi, suçluların yakalanması, tehlikeli olaylara kolayca müdahale edilmesinin sağlanması, caydırıcılık sağlama şeklinde örneklendirilebilecek "güvenlik" sebepleridir.

Çalışmamda güvenlik-özgürlük ikilemini ele alarak video gözetime dair hukuk kurallarının mahremiyet, özel hayatın gizliliği ve kişisel verilerin korunması alanlarında tek başına işlevli olmayabileceğini ve bunun sebepleri ile çözümlerini sorgulamak, sosyal yaklaşımı temel alan bir kavrayış geliştirmek istedim. Bu maksat ise hem gözetim literatürünün kendisini hem mahremiyete dair temel tartışmaları hem de veri koruma hukukunun konu ile bağlamını ortaya koymayı gerektirdi. Umarım tezimi yazarken fikirleri, soruları, doğrudan veya dolaylı şekilde katkıları olan kişiler de çalışmanın genel arayışından hoşnutlardır.

Dersine girdiğim ilk andan itibaren sorgulamanın ve bir fikri akademik açıdan öne sürmenin nasıl yapılması gerektiği konusunda örnek aldığım, tez danışmanım, değerli hocam Sayın Doç. Dr. Duygu HATİPOĞLU AYDIN'a çalışmama olan katkıları, tüm çabası, bana olan güveni ve yoluma tuttuğu ışık için,

Tez jürimde yer alan değerli hocalarım Sayın Dr. Öğr. Üyesi Muammer KETİZMEN ve Sayın Dr. Öğr. Üyesi Ulaş KARADAĞ'a çalışmaları arasında ayırdıkları anlamlı vakit, tezimi incelemek için verdikleri emek ve faydalı katkıları için,

Çalışma arkadaşım Yurdagül KOCA'ya objektif bakış açısı ile sorgulamalar yaptığımız değerli kıldığı onca an, verdiği güç, duyduğu inanç ve gerek mesleki gerek akademik çalışmalarıma olan samimi katkıları için,

Kıymetli annem Nevin TURGUT'a öğretmenlik mesleğini gönülden ve ilkeli icra ediş biçimiyle verdiği ilham, beni saatlerce bıkmaksızın dinleyerek gösterdiği sabır, koşulsuz destek ve geriye kalan ifadesi zor "her şey" için,

Son olarak; yürüdüğüm yollar zorlaştığı anlarda bana güven ve umut vermekten vazgeçmeyen, yorulmak bilmez kişiliği ve çalışma azmi ile örnek aldığım, varlığını hep ve "iyi ki" yanımda hissettiren saygıdeğer eşim Mehmet BİLGİÇ'e gönülden teşekkürü borç bilirim.

ÖZ

TURGUT BİLGİÇ, Ezgi, *Kamusal Alanda İdarenin Video Gözetiminin Kişisel Verilerin Korunması Hukuku Bağlamında Değerlendirilmesi,* Yüksek Lisans Tezi, Ankara, 2023

Günümüzde yaşanan teknolojik ve teknik gelişmeler kamusal alanlara yerleştirilen video kayıt cihazlarının kapasite ve sayılarında artışa sebep olmuştur. Bugün yapay zekâ kullanabilen akıllı kameralara da kamu otoritelerince çeşitli maksatlarla başvurulması durumu söz konusudur. Kamusal alanlardaki kameraların, bazı durumlarda kişisel veri elde etmesi ve bu verileri kaydetmesi veri işleme faaliyeti sayılacağından, bu faaliyetler bakımından kişisel verilerin korunması hukukuna uygun hareket edilmelidir. Bunun dışında kameraların kamu otoriteleri tarafından yaygın şekilde tercih edilmesi etik, sosyal, teknik kaygılar doğurmakta; işlevsellik, totaliterliğe veya kötüye kullanıma elverişlilik, insan hakları ve hukuk güvenliği açılarından eleştirilere konu edilmektedir.

Çalışmada, gözetim ve mahremiyet tartışmalarından başlayarak kameralı izleme ele alınmış, kamusal alanda kullanılan video kayıt cihazlarının tercih edilme gerekçeleri incelenmiştir. Ayrıca video gözetim ile kişisel verilerin korunması hukuku arasındaki ilişki ortaya konarak, hukuk kurallarının kameralar karşısında bireysel özgürlüklerin koruması için tek başına yeterli olmayacağı fikri ifade edilmiştir. Çalışmanın amacı ve kapsamı genel olarak gözetim literatüründen ve yaygın gözetime yönelik sorgulamalardan dayanak almış, kişisel verilerin korunması alanında gelişimini sürdüren hukukun, sosyal yaklaşım ile zenginleştirilmesi gerektiği fikrine bağlı şekillenmiştir.

Anahtar Kelimeler: Gözetim, Video Gözetim, CCTV, Kamusal Alan, Kişisel Veri, GDPR, Kamu Otoritesi.

ABSTRACT

TURGUT BİLGİÇ, Ezgi, *Evaluation of Video Surveillance of Administrative Bodies in Public Space in the Context of Personal Data Protection Law,* Master's Thesis, Ankara, 2023

With the effect of digitalization technological and technical developments have led to an increase in the capacity and number of video recorders placed in public spaces. Today, smart cameras that can use artificial intelligence are also used for various purposes by administrative bodies. Since cameras in public areas, in some cases, obtaining personal data and recording this data, are considered data processing activities, the law on the protection of personal data should be followed in terms of these activities. Apart from this the widespread preference of cameras by public authorities raises ethical, social and technical concerns and it is subject to criticism in terms of functionality, totalitarianism or abuse, human rights and legal security.

In the study, video surveillance was discussed starting from the discussion of surveillance and privacy and the reasons for the preference of video recording devices used in the public space were examined. In addition, by revealing the relationship between video surveillance and the law on the protection of personal data, the idea that the rules of law alone will not be sufficient for the protection of individual freedoms against the cameras has been expressed. In general, the aim and scope of the study; based on the surveillance literature and inquiries regarding widespread surveillance has been shaped by the idea that the law which continues its development in the field of personal data protection should be enriched with a social approach.

Keywords: Surveillance, Video Surveillance, CCTV, Public Areas, Personal Data, GDPR, Public Authority.

İÇİNDEKİLER

KISALTMALAR DİZİNİ

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

AİHM: Avrupa İnsan Hakları Mahkemesi

AİHS: İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme (Avrupa İnsan Hakları Sözleşmesi)

ALPR: Automatic License Plate Recognition (Otomatik Plaka Tanıma Sistemi)

APEC: Asia-Pasific Economic Cooperation (Asya Pasifik Ekonomik İş birliği Örgütü)

AYM: Anayasa Mahkemesi

bkz.: Bakınız

BM: Birleşmiş Milletler

BM Rehber İlkeleri: Birleşmiş Milletler tarafından 14 Aralık 1990 tarihinde kabul edilmiş 45/95 sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler

BWC: Body Worn Camera (Yaka Kamerası)

CIA: Central Intelligence Agency (Merkezî İstihbarat Teşkilâtı)

CCTV: Closed Circuit Telelevision (Kapalı Devre Televizyon Sistemi)

CMK: 5271 sayılı Ceza Muhakemesi Kanunu

CNIL: Commission Nationale de l'Informatique et des Libertés (Fransa Veri Koruma Otoritesi)

Çev.: Çeviren

Veri Koruma Direktifi : 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

ECOWAS: Economic Community of Western African States (Batı Afrika Ülkeleri Ekonomik Topluluğu)

Ed.: Editör

EDPB: European Data Protection Board (Avrupa Veri Koruma Kurulu)

EDPS: European Data Protection Supervisor (Avrupa Veri Koruma Denetçisi)

EDS: Elektronik Denetleme Sistemi

GDPR: 2016/679 sayılı ve 27 Nisan 2016 Tarihli Gerçek Kişilerin Kişisel Verilerin İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 95/46/EC sayılı AB Yönergesini Yürürlükten Kaldıran Avrupa Parlamentosu ve Avrupa Konseyi Tüzüğü (General Data Protection Regulation-Avrupa Birliği Genel Veri Koruma Tüzüğü-GVKT)

Ibid.: Aynı yerde

JTGYK : 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu

KGYS: Kent Güvenlik Yönetim Sistemi

KVKK: 6698 Sayılı Kişisel Verilerin Korunması Kanunu

m.: Madde

NSA: The National Security Agency (Ulusal Güvenlik Teşkilatı)

OECD: Organisation for Economic Co-operation and Development (Ekonomik İş Birliği ve Kalkınma Örgütü)

OECD Rehber İlkeleri: Ekonomik İş birliği ve Kalkınma Teşkilatı tarafından 23.09.1980 tarihinde kabul edilen ve 2013 yılında güncellenen Özel Yaşamın Korunmasına ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler

Polis-Adalet Direktifi: 2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İş Birliği Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Direktif

PVSK: 2559 sayılı Polis Vazife ve Salahiyet Kanunu

s.: sayfa

TDK: Türk Dil Kurumu

vb.: ve benzeri

vd.: ve devamı

108 +: Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Modernize Edilmiş Sözleşme

108 sayılı Sözleşme: Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Madde 29 Çalışma Grubu: The Working Party on the Protection of Individuals with regard to the Processing of Personal Data

78-17 sayılı Yasa: 6 Ocak 1978 tarihli 78-17 sayılı Veri Koruma Yasası (Loi no 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la loi Informatique et Libertés)

25 Mayıs 2021 Yasası: 2021-646 sayılı Kapsamlı Güvenlik Koruma Özgürlükleri İçin 25 Mayıs 2021 Yasası (Loi no 2021-646 du 25 Mai 2021 Pour Une Sécurité Globale Préservant les Libertés)

"Kanunlar daima kanun koyucunun tutkularına ve ön yargılarına ayak uydurur. Kimi zaman kanunlar bunların içinden geçer ve rengini alır, kimi zamansa içinde kalıp bunlara karışır." [1]*Montesquieu*

GİRİŞ

Video kayıt cihazları veya CCTV'ler[2], günlük hayatımızı yaşadığımız ve sosyal yaşama dahil olduğumuz kamusal alanlarda bizleri izleyen birer gözdür. Tarihsel olarak devletlerce temelde güvenlik yönetimini sağlama amacıyla kullanılan kameralar, zaman içinde teknik ve teknolojik gelişmelerin itici gücü ile kamusal alanlarda daha çok tercih edilmeye başlanmıştır. Bu tercihin sebebi, kameraların artık çok daha gelişmiş olması ve daha geniş alanları izlemeye imkân sağladığı için güvenlik sağlamada daha etkili bir araç haline gelmesi olabilir. Ancak özellikle şehirlerdeki kameraların artmasında güvenliğin sağlanması amacının yanında sosyal kontrolü sağlama, güvenli yaşam psikolojisi yaratarak devlet gücünü ortaya koyma, bilginin özel şirketlerdense tek elde, egemen devlette toplanması gibi pek çok farklı sebep tartışma konusu edilmektedir.

Son yıllarda kapsamı gitgide genişleyen kişisel verileri koruma hukuku ise; kameraların bazı durumlarda kişisel veri elde etmesi, depolaması kısacası veri işlemesi gerekçesiyle kullanımlarında devreye girmektedir. Bu durumda kamu otoritelerince kamusal alanlarda video gözetim cihazları kullanılırken, kişisel verilerin korunması mevzuatına uygun hareket edilmesi beklenir. Öyleyse kamusal alanlardaki kameralı gözetimde hangi hallerde kişisel veriler işlenmiş sayılır? Hangi kurallara uyulması beklenir? Güvenlik amacıyla yapılan izleme faaliyetleri, veri koruma kurallarından tamamen istisna mıdır? Bu sorulara verilen cevaplar, çalışma ile ortaya konmaya çalışılan fikrin altyapısını oluşturmaktadır.

---

[1] MONTESQUIEU, Baron de La Brède. (2019). Kanunların Ruhu Üzerine. (Berna Günen Çev.) İstanbul: Türkiye İş Bankası Kültür Yayınları. (Orijinal Eserin Yayın Tarihi:1758). s.758.
[2] Closed Circuit Telelevision (Kapalı Devre Televizyon Sistemi)

Çalışma konusunun takdimi ve sınırlandırılması açısından; video gözetim cihazlarının kamusal alanda kullanılmasında ayrıca değerlendirilmesi gereken bazı hususlar bulunmaktadır. Zira bu alanlar, toplumsal hayata katılımın sağlandığı, mahremiyetin daha yoğun olduğu evlerin dışa açılan yüzüdür. Bu sebeple kamusal alanlarda yoğun şekilde kullanılan cihazların yaptığı gözetim faaliyetinin hem bireysel hem de kamusal alanlar açısından etkileri olduğu söylenebilir. Çalışmanın kapsamı, kullanılan kavramların doğasından kaynaklı olarak oldukça geniştir. Ayrıca ifade edilmelidir ki; okullar, iş yerleri, apartmanların önü ve apartman daireleri gibi kamusal alanlar dışındaki alanlar ve özel mülkiyete tabi alanlarda kullanılan cihazlar çalışma kapsamında ele alınmamıştır.

Böylece çalışmada; kamusal alanlarda kamu otoritelerince kurulan video gözetim cihazlarının kullanım amacı, kişisel verilerin korunması hukuku çerçevesinde ele alınmış ancak konunun oldukça geniş bir konsepte sahip olması nedeniyle salt hukuk kurallarının kişisel verileri veya mahremiyet ile özel hayatı koruma altına almaya yetmeyeceği fikri savunulmuştur. Çalışmada ele alınan problem ise; mahremiyet kavramının ve mahremiyet ile özel hayatın gizliliğini koruma temelinde gelişen kişisel verilerin korunması hukukunun kapalı bir kurallar sistemi şeklinde ele alınmasının yeterli olup olmadığı olmuştur.

Kişisel verilerin ve mahremiyetin korunması mevzuatının oluşumunda teknolojik (gözetim cihazlarının gelişimi), ekonomik (cihazlara ayrılan bütçeler) ve politik (ülkeden ülkeye değişen güvenlik stratejileri, siyasi eylemler gibi olaylara karşı iktidarların tutumu) etkiler gözlemlenmektedir. Bu sebeple temel düşünce ortaya konmaya çalışılırken, amaç-araç bakımından çeşitli sorgulamaların yapılması da hedeflenmiştir.

Çalışmanın birinci bölümü genel çerçevede gözetimin bir kavram olarak ele alınması, hangi konular ile ilişki içinde olduğu, tarihsel süreç içinde nasıl şekillendiği ile ilgilidir. Bunu yaparken devletlerin gözetime neden ihtiyaç duyduğu sorgulanmış, özellikle sosyal kontrol görüşleri bu sorgulamaya dayanak olarak ele alınmıştır. Sosyal kontrol görüşleri, gözetime salt güvenliğin tesis edilmesi aracı olarak yaklaşılmasının ötesine geçip, gözetimin araçsallaştırılmasına geniş bir perspektiften, devletin bir bilgi

kontrol mekanizması olarak çıkarına hizmet eden denetim biçimi olarak yaklaşır. Bu türden sorgulayıcı bir yaklaşım, çalışmanın tümüne sirayet etmiş, kamusal alanların sistemli şekilde izlenmesinin güvenlik dışında hangi maksatlarla yürütülüyor olabileceğine ilişkin fikirlere yer verilmesine sebep olmuştur.

Gözetim ve mahremiyet birbirini kapsayan, bazen dışlayan bazen de bütünleyen kavramlar olarak kökensel bir birliktelik içindedir. Kişisel verilerin korunması düşüncelerinin doğmasında da bireysel mahremiyetin ve özel hayatın korunması ihtiyacı yatar. Bu sebeple bir olgu olarak mahremiyetin tanımı, kavramın tarihsel dönüşümü, hangi başka kavramlarla etkileşimde olduğu, bir hak olarak ortaya çıkışı ve buna sebep olan olaylar, günümüzde nasıl bir mahremiyet kavrayışının hakim olduğu gibi konulara yer verilerek; mahremiyet, kişisel verilerin korunması ve gözetimin birbiriyle bağlantısı kurulmaya çalışılmıştır.

Öte yandan gözetimin nasıl başladığı tarihsel bir yaklaşımla ele alınmış, günümüzde kullanılan "artırılmış" (*augmented*) veya yapay zekâ kullanabilen kamera sistemlerine hangi süreçlerden geçerek gelindiği incelenmiştir. Bunun yanında gözetim çalışmalarının temelinde olan panoptikon kurgularına, kurguyu oluşturan Jeremy Bentham'ın düşüncelerine ve panoptikon-devletin disipline etme arzusu-modern hapishane kavramlarına dair çalışmalarıyla öne çıkan Michel Foucault'nun iddialarına yer verilmiştir. Zira Bentham ve Foucault'nun panoptikon mizanseni üzerinden devlet gözetimi, bilginin ve izlemenin kontrolü üzerinden sağlanan egemenlik ve güç, şeffaflığın yarattığı absürdite, mahremiyetin yitimi gibi kavramları sorgulayış biçimi bugüne dair tartışmalara da şekil vermektedir.

İkinci bölümde devletin kameralı gözetimi çerçevesinde video gözetim sistemlerinin kullanımının hangi süreçlerden geçtiği, CCTV olarak adlandırılan video gözetim cihazlarının temelde nasıl bir mekanizmaya sahip olduğu ve bu cihazlar ile ne tür veriler toplandığı kısaca incelenmiştir. Akabinde çalışmada ele alınan kamusal alanlara, çalışma konusu ile ilgisi doğrultusunda çeşitli açılardan yer verilmiştir. Kamusal alanlar; demokratik bir toplumdaki sosyalleşme, toplumsal hayata katılma alanları olarak video gözetimden oldukça etkilenmiştir. Bu etkilenme nasıl olmuştur, kamusal alanların

kapsamı nedir, bu alanlar neden önemlidir? İlgili başlıkta bu soruların olası cevapları tartışılmıştır.

Bunlarla birlikte devletin hangi amaçlarla video gözetim cihazlarını kullandığı sorgulanmış, kamusal alanda yürütülen izleme faaliyetlerine yönelik eleştirilere yer verilmiştir. Eleştiriler, çalışmada ortaya konmaya çalışılan kamusal alandaki video gözetim açısından kişisel verileri koruma mevzuatının tek başına yeterli olmayabileceği görüşünün desteklenmesi için dayanak olmuştur. Bu kaygıyla video gözetime yönelik argümanların; "işlevsellik, totaliterliğe veya kötüye kullanıma elverişlilik, temel hak ve hürriyetlere aykırılık ve hukuki güvenliğin sorgulanması" şeklinde tasnifine gidilmiştir.

Çalışmanın son bölümünde ise; kişisel verilerin korunması hukukunun ortaya çıkışı ve genel kapsamı ele alınarak, temel düzenlemelere yer verilmiştir. Burada özellikle Avrupa Birliği (AB) düzenlemeleri hem tarihsel olarak hem de kapsam bakımından diğer ülkelerin veya toplulukların mevzuatlarına kıyasla oldukça kapsamlı olduğundan, çalışmada ele alınan problem bakımından da temel alınmıştır. Video gözetime ilişkin hukuki düzenlemelere yine bu bölümde yer verilmiştir. Bununla birlikte, AB'deki veri koruma hukukunun ikili bir sistem üzerinden uygulanışı, konunun bir örnek ile somutlaşmasını gerektirmiş, aynı zamanda bir "iyi uygulama örneği" olarak Fransa, kamusal alanlardaki video gözetim bağlamında ele alınmıştır. Bunun yanında ülkemizde uygulanan video gözetime de kapsam dahilinde yer verilmiş, iki ülkedeki genel durum kısaca karşılaştırılmıştır.

Netice itibarıyla çalışmada kamusal alanda idarenin video gözetimi bakımından kişisel verilerin korunması hukukuna sosyal yaklaşım büyütecinden bakılması gerektiği fikri savunulmuş, alanın çeşitli teknik ve toplumsal boyutlarının da baskın olması sebebiyle yapılan hukuki düzenlemelerin bu yaklaşım ile yorumlanması gerektiği fikrine yer verilmiştir. Video gözetim oldukça geniş kapsamlı ve çok sayıda konu ile ilintili bir faaliyettir. Bu sebeple bu faaliyete yönelik hukukun yalnızca veri güvenliğine dayalı kurallar dizisi, uygulanmaları bakımından içselleştirilmesi zor temel ilkeler bütünü olarak değil, aynı zamanda topluma ve ayrı ayrı bireylere ait sosyal çıktısı olan bir kalkan olarak görülmesinin önemi vurgulanmıştır.

Çalışma konusu gözetim ve mahremiyet gibi oldukça geniş kavramlar üzerine kurulu olduğundan, kapsam ve kaynaklar açısından da geniş bir literatürden faydalanılmıştır. Hukuki düzenlemeler incelenirken; salt kanunlar ve sair hukuk normlarından değil aynı zamanda ulusal ve uluslararası mahkeme kararlarından da faydalanılmıştır. Mahremiyet ve gözetim tarihsel perspektiften ele alınırken, kavramlarına temas edilen sosyal disiplinlere ilişkin ulusal ve yabancı kaynaklar incelenmiş, literatürde öne çıkan fikirlere özellikle yer verilmeye çalışılmıştır.

Çalışmada ortaya konulması amaçlanan düşüncenin kapsamı konusunda ise; birinci bölümde genel çerçeve ve bağlamın temelindeki fikirler ya da kavrayışlar ele alınmış, ikinci bölümde video gözetime yönelik eleştirilerden yola çıkılarak mevzuatın tek başına yeterli işleve sahip olmayacağına dayanak olan hususlara dikkat çekilerek bölüme bir -köprü- işlevi kazandırılması hedeflenmiş, son bölümde ise sorgulama konusu edilen mevzuata yer verilerek video gözetim ile kişisel verilerin korunması hukuku arasındaki ilişki kurulmaya çalışılmıştır.

1. BÖLÜM

KAVRAMSAL AÇIDAN GÖZETİM VE GÖZETİMİN GENEL ÇERÇEVESİ

Günümüzde evimizden dışarı adımımızı attığımız andan itibaren elektronik gözlerden kaçmak neredeyse imkânsız bir hale gelmiştir. Havaalanından, caddeye, okullardan, iş yerlerine ve parklara kadar her yerde kameralar tarafından izlenmekteyiz. Üstelik gözetim yalnızca bununla sınırlı da kalmayıp, dijital ayak izi bıraktığımız her siber mecradan yeni bir "biz" yaratacak boyuttadır. Fakat gözetim tartışmaları, güncel teknolojik gelişmelere paralel olarak şekillenen yapay zekâya sahip kamera sistemlerinin yaptığı izlemelerin ötesinde bir boyutu da kapsamaktadır ki bu boyut bizi gözetimin hukuki açıdan sorgulanmasına, tarihsel evrimine ve sosyal etkilerine kadar götürür. Zira gözetimin tarihi oldukça eskidir ve dolayısıyla gözetimden etkilenen bireyler, toplum, toplumsal hayat ve kamusal alanlar, bizatihi kavramın kendisiyle birlikte şekillenmiştir.

Gözetim nedir ve hangi faaliyetler gözetimin kapsamına dahildir? Gözetime dair hangi tartışmalar yürütülmüş ve bu tartışmalar gözetim eylemlerine nasıl bir yön vermiştir? Özellikle devletin bireylere yönelik yaptığı gözetim, geçmişten günümüze nasıl şekillenmiştir? Bu konudaki hukuki düzenlemeler, gözetim karşısında bireylerin mahremiyetlerinin sağlanması gerektiği anlayışı ile ne kadar uyumludur? Bu sorular doğrultusunda çalışmanın birinci bölümünde bir kavram olarak gözetim ele alınmış ve konunun genel çerçevesi çizilmeye çalışılmıştır. Bu açıdan çalışmada ortaya konulan savın daha belirgin hale gelmesi bakımından, video gözetime dair çeşitli temel konu ve tartışmalara değinilmesi, öncesinde ise gözetimin kendisinin nasıl temellendiğinin izahı gerekmiştir.

Bölüm kapsamında öncelikle; gözetim bir kavram olarak incelenmiş ve çalışmada gözetimin hangi kavram setleri ile birlikte kullanıldığı ifade edilmiştir. Zira video gözetime tarihsel izlekten bakılması, konunun diğer boyutları ile bağlam oluşturmayı

sağlayabilecektir. Akabinde gözetleme gücüne muktedir esas aktör olan devletin, gözetim ve sosyal kontrol ile ilişkisine yer verilmiştir. Öte yandan zaman zaman mahremiyet ile çatışma halinde olan gözetimin, bu kavram ile dönüşümlü etkileşimine değinilmiştir.

Bu başlık altında gözetim tartışmalarını alevlendiren ve akademik dünyada da yankı uyandıran panoptikon fikirleri ele alınmış, özellikle Bentham ve Foucault gibi düşünürlerin yaklaşımları öncelenerek gözetimin boyutları ve kapsamına dair iddia veya fikirlere yer verilmiş, algoritmik veya "akıllı araçlar aracılığıyla" yapılan gözetime kadar olan süreç, tarihsel bir perspektiften ele alınmıştır. Burada çalışma konusu olan kamusal alanlardaki video gözetime yönelik, gözetleyen ve gözetlenenlerin menfaatlerinin temellendirilmesi amaçlanmıştır.

Bu sebeple çalışma konusunun sınırlanmasında önem arz eden "kamusal alanlar" ifadesine dahil olan yerlerin kapsamı belirtilmiş, çalışmada niçin kamusal alanların ele alındığı izah edilmeye çalışılmış özellikle akıllı video kayıt sistemleri ile yapılan gözetimin kamusal alanları da dönüştürdüğü fikri üzerinde durulmuştur. Son olarak; gözetimin küreselleşmesi ile elde edilen maddi menfaatlerin gözetimin kendisini körüklediği görüşlerine de bu bölümde kısaca yer verilmiştir.

1.1. BİR KAVRAM OLARAK GÖZETİM

1.1.1. Gözetim Kelimesi

Gözetim kavramı TDK sözlüğüne göre; gözetme işi, nezaret, himaye anlamlarında kullanılmaktadır[3]. Sözcüğün etimolojik Türkçe kökenine bakıldığında ise; közet "beklemek, korumak" fiilinden evrildiği, gözetmek fiilinin eski köz "göz" sözcüğünden "-at" ekiyle türetilmiş olabileceği belirtilmektedir[4]. Kavramın İngilizce karşılığı olan "*surveillance*" kelimesinin ise; Fransızca "üzerinde" anlamındaki "*sur*" kelimesi ile

[3] Türk Dil Kurumu Sözlükleri, "Güncel Türkçe Sözlük", (Erişim Tarihi:23.06.2022) https://sozluk.gov.tr/. "gözetim".
[4] Nişanyan Sözlük, (Erişim Tarihi:23.06.2022) https://www.nisanyansozluk.com/kelime/g%C3%B6zetim. "gözetim".

izlemek anlamına gelen ve Latince "*vigilare*" kelimesinden alınan "*veiller*" fiilinin birleşmesi ile meydana gelmiş olduğu düşünülmektedir[5]. Kelime anlamı ve etimolojik kökeni dışında gözetimin, anlamının ötesinde manalar barındırdığını ifade etmek mümkündür.

1.1.2. Gözetimin Kapsamı ve Boyutları

Jeremy Bentham için gözetleme daha çok; halkın içinde şeffaflık, soyutun teşhiri, görünüş yoluyla caydırma-caydırılma, görüldüğü hissini duyma fakat bundan hiçbir zaman emin olamama anlamlarına gelir[6]. Bu anlamda Bentham'ın yaklaşımında gözetim zaten özel alanları dışlamakta, halka açık alanlarda yapılan ve genellikle bireylerin farkına var(a)madığı bir faaliyettir. Michel Foucault'nun bakışıyla ise; tıpkı bir hapishanenin yaptığı mekânsal çevreleme gibi, gözetim bir "teftiş", bir "milis birliği" veya "devriye"dir[7]. Muhakkak bir kayıt sisteminden faydalanılan gözetim, her cadde veya sokakta bulunan bu cihazlar ile adeta bir mahalle emini gibi halkın rollerine dair kayıt tutmaktadır, bu şekilde en küçük toplumsal hareket dahi denetlenebilmektedir[8].

Ontolojik olarak toplumun denetlenmesi, devlet, egemenlik, kapitalizm, teknoloji ile birlikte ele alınması gereken gözetimin, toplumsal düzenin ve güvenliğin sağlanması arayışı ile de doğal bir alakası vardır. Öyle ki bir görüşe göre gözetim, bireylerin toplumun kurallara uygun davranmasının sağlanması için ortaya çıkmış, bu durumda egemenliğin sağlanmasına hizmet etmiş ve modern gözetime bu şekilde ulaşılmıştır[9]. Modern gözetim ise daha kurumsal ve kapsayıcı hale gelen teknikleri içeren, sermayedarlarına da hizmet eden bir elektronik göz yani kameralar tarafından sürekli izlenme biçimine evrilmiştir[10]. Dolayısıyla günümüz gözetiminin, modern sosyolojik

---

[5] Oxford Learner's Dictionaries, (Erişim Tarihi 18.08.2022) https://www.oxfordlearnersdictionaries.com/definition/english/security?q=security "security".
[6] BOZOVIC, M. (1995). "Jeremy Bentham the panopticon writings". Verso: London and New York. s.6-13.
[7] "FOUCAULT, M. (2015) Hapishanenin Doğuşu. (Mehmet Kılıçbay Çev.) Ankara: İmge Kitabevi, 6. Baskı. (Orijinal Eserin Yayın Tarihi: 1992)". s.289-291.
[8] Ibid, s.292-293.
[9] "DOLGUN, U. (2015). Şeffaf Hapishane yahut Gözetim Toplumu: Küreselleşen Dünyada Gözetim, Toplumsal Denetim ve İktidar İlişkileri (3. Baskı). İstanbul: Ötüken Neşriyat." s.22.
[10] Ibid, s.22-23.

unsurlar ile de iç içe girerek hem bir güvenlik sağlama hem de bu arayıştan ekonomik çıkar elde etmeyi sağlayan çok yönlü bir iktidar faaliyeti olduğu ifade edilebilir.

David Lyon ise dijital gözetimi modern topluma katılım biçimi olarak tasavvur eder ve onun esasen pek çok günlük faaliyetin ta kendisi olduğunu düşünür. Ona göre; bir banka makinesinden para alma, telefon görüşmesi yapma, araba veya kredi kartı kullanma, istenmeyen e-posta alma, kütüphaneden kitaplar alma, yurtdışı gezileri yapma gibi günlük ve sıradan eylemlerin hepsinde bilgisayarlar işlemlerimizi kaydeder, bilinen diğer ayrıntılara karşı kontrol eder, başkalarının değil bizim tarafımızdan faturalandırıldığından veya ödeme yapıldığından emin olur, biyografilerimizin parçalarını saklar, mali, yasal veya ulusal konumumuzu değerlendirir[11]. Esasında belirtilen eylemler ile bilgisayarlara bırakılan her iz veya bilgisayarların aracılık ettiği her işlem, elektronik gözetim altında olmayı da beraberinde getirecektir.

Gözetim olgusunun ne olduğuna bakmak dışında, kavramın doğrudan tesir ettiği toplumun kendisi üzerinde olan etkileri de incelemek gerekir. Gözetim toplumu, izleme yapmak maksadıyla bu maksada dayalı özel teknikler kullanılarak örgütlenmiş ve yapılandırılmış bir toplumdur[12]. O halde gözetim altında olmak, toplumları yapılandıran kuruluşlar ve hükümetler adına, teknolojiler tarafından kaydedilen hareketler ve faaliyetler hakkında bilgi sahibi olmak anlamına gelir[13]. Kayıt cihazlarınca elde edilen bilgiler daha sonra gerekli şekilde sıralanır, elenir, kategorilere ayrılır ve bireylerin özel hayatlarını etkileyen kararların temeli olarak kullanılır[14]. Bu sebepledir ki devletlerce gözetime yönelik olarak verilen kararlar, sağlığımızı, genel refahımızı, kamusal ve özel alanlardaki hareketimizi, haklara, işe, ürünlere, hizmetlere, ceza adaletine hak kazanma ve erişim potansiyelimizi ilgilendirir.

---

[11] KLING, R., & LYON, D. (1994). "The Electronic Eye: The Rise of the Surveillance Society". In Contemporary Sociology (Issue 4). University of Minnesota Press.
[12] BALL, K., GRAHAM, S., GREEN, N., & LYON, D. (2006). A Report on the Surveillance Society. In Polity (Vol. 70, Issue September), s.5.
[13] Ibid, s.5.
[14] Ibid.

Gözetimi bir kavram olarak incelemek, onu doğal olarak etkileşim içinde olduğu diğer kavramlarla birlikte ele almayı gerektirir. Gözetim; iktidar, kültür, eşitlik, mahremiyet, güvenlik, sosyal kontrol, teknoloji, kapitalizm ve sair unsurlar ile şekillenerek, bunlardan hem etkilenir hem de bunlar üzerinde etkili olur. Örneğin toplumsal düzenin sağlaması ve bu düzende yer alan normlara ve kurallara uyulup uyulmadığının denetimi gözetim mekanizması ile sağlanabilir[15]. Öte yandan modernite öncesi dönemlerde monarşilerin, imparatorlukların egemenlik aracı olan gözetim[16], modern çağda akıllı teknolojilerin veya cihazların da eklenmesi ile ciddi bir güç haline gelmiştir. Dolayısıyla gözetim tarihsel açıdan oldukça eski sorgulamalar ve kavrayışlara dayanırken, diğer taraftan da teknolojik gelişmeler ve getirdiği özel hayatın gizliliğine dair tehditler gibi çeşitli "modern" unsurlardan kopartılmamalıdır. Çalışmada gözetimin bu "çok kültürlü" ve "çok disiplinli" yapısından ötürü tek bir yaklaşım biçimine bağlı kalınmamıştır.

Gözetim genel olarak birbirine bağlı, dağıtılmış ve birbirinden uzak bir dizi kurum, sistem, bürokrasi ve sosyal bağlantı aracılığıyla gerçekleşir[17]. Bu sebeple gözetime dahil olan unsurlar günlük yaşamın birçok normal biçimine gömülü oldukları için, gözetimin etkilerini izlemek de zordur[18]. Gözetim aynı zamanda tarihsel bir sosyal süreçten gelen uygulamaları kapsadığından, hem kurumsal rutinlerin diğer deyişle iktidarın sürdürdüğü eylemlerin hem de insanın bir günlük sosyal hayatının bir parçası olmuştur. Bu anlamda bireylerin sosyalleşmesinin ve dolayısıyla örgütlenmesinin, gözetimde oldukça önemli bir rol oynadığına dair görüşlerin doğmasına yol açmıştır.

Öte yandan gözetim; gözetlenenler yani toplum ve gözetleyen egemen güç açısından da farklı yorumlanmalıdır[19]. Gözetlenenler çoğu zaman gözetim faaliyetinin farkına dahi varamazken, gözetleyen çeşitli gözetleyici kontrol araçlarını elinde tutarak, izlemenin boyutunu veya kapsamını belirlemeye muktedirdir. Gary Marx, gözetleyen

---

[15] DOLGUN, 2015, s. 21.
[16] Ibid, s.21-22.
[17] HAGGERTY, K. D. (2012). "Surveillance, crime and the police". In K. Ball, K. Haggerty, & D. Lyon (Eds.), Routledge Handbook of Surveillance Studies. Routledge. s.1
[18] Ibid.
[19] ÇETİN, M., & ASIL, S. (2017). "Günümüz Toplumunda Gözetim Olgusu". Third Sector Social Economic Review, 52(1). s.182.

egemenin yani Devletin, bir taraftan gözetim yaparken diğer taraftan kendi paradoksunu yaşadığını iddia eder ve bu paradoksu Kraliçe Elizabeth'in yaşadığı çıkmaza benzetir[20]. Buna paradoksa göre Devlet/Kral/egemen bir taraftan kendisine karşı olanları, "zararlıları" bilmek ve onlardan gelebilecek riskleri bertaraf etmek isterken, diğer taraftan kişinin onurunu ve haysiyetini de koruyarak arzulanan özgürlüğü bahşetmeyi amaçlar. Kraliçe Elizabeth paradoksu hem güvenliği hem de -kendi çizdiği sınırlar içinde kalmak suretiyle- mahremiyeti tesis etmeye çalışan devletleri ifade eder. Çalışmada bahis konusu olan da esasen, modern hukukun bu güvenlik-mahremiyet açmazını çözmeye ehil olup olmadığını değerlendirmektir.

Bu bağlamda gözetlemenin hem tehditlere yanıt hem de tehdit olarak görüldüğü bir dünyada, "gözetleme iyi midir kötü mü?" diye sormadan önce gözetimin temel yapılarını ve süreçlerini anlamak için hangi kavramlara ihtiyaç olduğunu sorgulamamız gerekir. Zira gözetimin iyi veya kötü, mahremiyetin katili veya güvenliğin anahtarı olup olmadığı, onun çeşitli kavram ve davranışlar ile bağlamı ortaya konulmadan anlaşılamayacaktır. Marx'a göre; gözetim, hükümetler, casusluk veya gizlilikle sınırlı olmayan, bilgi sınırları olan genel bir süreçtir[21]. Bununla birlikte gözetim ve mahremiyet mutlaka birbirinin karşıtı olarak yorumlanmak zorunda değildir, bilakis mahremiyet, bilgiye erişimin kontrol edilmesinde olduğu gibi gözetime ilişkin kuralları ve sınırları sigortalamanın da bir yolu olabilir[22]. Bu ise, gözetime multi disipliner bir perspektif ile yaklaşarak sağlanabilir.

Gözetim, kanıt toplamak için başkalarını izleme eylemi olarak, kolluk kuvvetlerinin şüphelileri soruşturmak veya delil toplamak için kullandığı en yaygın yöntemlerden biridir ve gözetlenen kişinin bilgisi ile (açık gözetleme) veya olmaksızın (açık olmayan gözetleme) gerçekleştirilebilir[23]. Diğer taraftan gözetim yapılışı bakımından genel olarak, elektronik (dijital gözetim) veya sabit şekillerde yapılabilir. Dijital gözetim, telefon dinleme, ortam dinleme, videoya kaydetme (video gözetim), coğrafi konum izleme, veri

---

[20] MARX, G. T. (2015). "International Encyclopedia of the Social & Behavioral Sciences". 23, s.733.
[21] Ibid, s.734.
[22] Ibid.
[23] Cornell Law School, Legal Information Institute, (Erişim Tarihi: 22.09.2022) Surveillance. https://www.law.cornell.edu/wex/surveillance

madenciliği, sosyal medya haritalama ve internet üzerindeki veri ve trafiğin izlenmesini içebilirken; sabit gözetleme (*stake-out surveillance*) bireylerin gizli şekilde gözetimini içerir[24]. Ancak çalışmada bir dijital gözetim biçimi olan video kamera sistemleri ile yapılan gözetim ele alınacağından, sabit gözetleme konusuna bu genel ifade dışında yer verilmemiş, ilerleyen başlıklarda video gözetim konusu daha ayrıntılı şekilde izah edilmiştir.

1.2. DEVLET, GÖZETİM VE SOSYAL KONTROL

1.2.1. Devletin Gözetimi

Lyon gözetimin iki yüzü olduğunu söyler[25]. Bu iki yüzden ilki aşırı mahremiyet yanlısı olmanın olası kayıpları açısından diğeri ise güvenliğin her konuda öncelenmesinden ötürü devletler için yanıltıcı olabilir[26]. Gözetim aynı zamanda bürokratik bir uğraş olduğundan, devletlerin günümüzün modern tekniklerine, elektronik kayıt ve dijital depolama ve erişim sistemlerine adapte olmasında, geçmişteki gözetim tekniklerinin etkili olduğu düşünülmektedir[27]. Hatta gözetim vizyonları veya stratejileri olmaksızın modern devletin bildiğimiz şekli ve bürokrasisi ile var olamayacağı savunulur. Zira vergilerin toplanması, sosyal yardımlara hak kazanılması, bulaşıcı hastalıkların yayılmasının kontrol altına alınması, kanunların uygulanması ve hatta ceza adaletinin sağlanmasının altında yatan esas faaliyet gözetimin ta kendisidir[28]. Böyle bir bakış açısıyla gözetim, sosyal yapıya da dokunan ve onu şekillendiren bir iktidar kurma biçimi olarak belirmektedir.

Devletlerin gözetim faaliyetlerinin esas odağı güvenlik olmakla birlikte, devletler hem dijital uygulamalar, şehirlere konuşlandırılan CCTV'ler, sınır kontrollerinin sağlanması ve sair hususlarda kendi güvenlik gerekçelerini uygulamak hem de küresel güvenlik anlayışını yerine getirmek için bir takım karmaşık ilişkiler ağının bir parçası

---

[24] Ibid.
[25] KLING & LYON, 1994, s.201.
[26] Ibid.
[27] NORRIS, O. ve ARMSTRONG, G. (1999) "The Maximum Survaillance Society". Oxford-New York: Berg. s.3.
[28] Ibid.

olurlar[29]. Diğer taraftan bazı devlet kurumları aynı anda hem mahremiyetin korunması hem de gözetim faaliyetlerini yürütmek konularında görevler üstlenmektedir[30]. Elbette gözetimin veya gözetim yapan video kamera sistemlerinin tek boyutu güvenliğin sağlanması değildir.

Bu noktada devletlerin elzem bazı güvenlik ihtiyaçlarının ötesinde bir toplumsal veya sosyal kontrol arayışından da bahsedilmektedir. Sosyal kontrol teorisi, görünen güvenlik gerekçelerinin ardındaki sebepleri araştırarak özellikle kitlesel kamera gözetimi etrafında örgütlenen bu kontrol biçimlerinin hem teknik hem de normatif özelliklere sahip siyasi stratejiler olduklarını iddia eder[31]. Dolayısıyla gözetimin ardında yatan ve caydırıcı olmanın ötesine geçen bir kontrolde tutma hali ortaya çıkmaktadır.

1.2.2. Sosyal Kontrol Yaklaşımları

Sosyal kontrol teorisi genel olarak; insanların neden kurallara uyduklarının gerekçesini sunar, bu uyum davranışı için sosyalleşmenin altını deşer, davranışın toplumda genel olarak beklenen davranışa nasıl uyduğuna dair bir açıklama sağlamaya çalışır ve öncelikle dış faktörlere ve bunların etkili olduğu süreçlere odaklanır[32]. Ayrıca teori, başkalarıyla yakın ilişkilerin yokluğunun, bireyleri sosyal kısıtlamalardan nasıl özgürleştirebileceğine ve böylece onların suçluluğa girmelerine izin verebileceğine de odaklanır[33]. Dolayısıyla gözetimin sosyal kontrol teorisi ile bağlamında; hem devlet, iktidar, politika üretimi hem de kamusal alanların ve dolayısıyla sosyal hayat ile sosyalleşmenin dönüşümü bulunmaktadır.

Foucault'ya göre, gözetimin disipline edici toplumsal kontrolünün gücü, totaliter bir devlet rejimindeki merkezileşmesinde değil, hapishanedeki idealleştirilmiş biçiminden toplumsal dokuyu oluşturan sayısız kamu ve özel kurum boyunca

---

[29] HATİPOĞLU AYDIN, D. (2022) Siber Alan ve Hukuk. İstanbul: Onikilevha Yayınları. s.184.
[30] Ibid, s.185.
[31] INNES, M. (2003). "Understanding Social Control: Deviance, Crime and Social Order". Open University Press. s.5, 28.
[32] KEMPF-LEONARD, K. and MORRIS, N.A. (2012). Social Control Theory.
[33] Ibid.

dağılmasında yatar[34]. Diğer deyişle, problemli görülen konu, kamusal alanların dolayısıyla toplumun gözetim ile kontrolündeki riskin denetimsizce ya da kuralsızca yayılmasıdır. Bu nedenle, CCTV'ler gibi gözetim aygıtlarının konuşlandırılmasının, bazı münferit disiplin normlarının uygulanmasını sağlamayı değil, genel bir sosyal kontrolü amaçlaması söz konusu olabilir. Clive Norris ve Gary Armstrong; futbol stadyumlarında, CCTV gözetiminin sadece düzensizliğin daha belirgin tezahürlerine değil, yerinde olmadığı düşünülen -tehlikeli olmayan- davranışların da tespitine yönelik olduğunu, CCTV'nin şehir merkezlerinde konuşlandırılmasının ise; doğru türde tüketiciyi çekmeye elverişli bir ortam yaratmak isteyen iş dünyasının ticari kaygıları tarafından yönlendirildiğini belirtir[35].

Sosyal kontrol; güç, devlet ve sosyal düzen arasındaki ilişkiyi yansıtır ve kent mimarisinden günlük yaşama kadar hayatın her alanını etkiler. Bu sebeple gözetim ile yapılan sosyal kontrolün altında yine devletin egemenlik anlayışı ve güç gösterme ihtiyacı aynı zamanda bunları yaparken toplum içindeki düzeni koruma arzusu bulunabilir. Sosyal kontrol perspektifinden CCTV'nin anlamı, çoğu zaman belirli sosyal çıkarlara eğilimli ve güçlü olan müttefikler ile iş birliği ve yine belirli siyasi vizyonları teşvik edebilmek için arzulanan üstün konum ve hayal edilen bir sosyal düzen sağlama aracı olmaktır[36]. Öyleyse bu düşünceler ile video gözetim ile ilgili şu sorular yanıtlanmayı beklemektedir. CCTV'lerin yayılması kamu yararının tesisi veya sosyal dayanışma ve toplumu güçlendirme olarak görülebilir mi? Böyle bir toplumsal denetim biçimi, suçu ve sapkınlığı aşırı derecede kınayan dolayısıyla yöneten kurumları, bir tür ahlaki katılık ve otoriterlikle destekleyen sağlıksız bir topluma mı işaret eder? Sosyal kontrol perspektifinden bakıldığında, ilk sorunun cevabının hayır, ikincisinin ise evet olması beklenir.

Emile Durkheim, toplumsal dayanışmanın gerekliliğine odaklanarak, toplumsal kontrole ilişkin önemli fikirler ortaya koymuş, büyük sanayi merkezlerini veya şehirleri,

---

[34] FOUCAULT,2015, s. 256 vd.
[35] NORRIS ve ARMSTRONG,1999, s.7-9.
[36] COLEMAN, R. (2004). "Reclaiming the Streets surveillance, social control and the city". Willan Publishing. s.12.

sosyal değişimin hızını ve sosyal düzeni istikrarsızlaştırma olasılıkları olarak görmüştür[37]. Bu anlamda sürekli bir gözetim ile dönüşen sosyal alanların ve bireylerin, Durkheim açısından da incelenmeye değer bir yönü bulunur. Ona göre hem devletçe yapılan yukarıdan gözetim hem de bireylerin birbirine olan sürekli gözetimi ile, herkes aynı düşünüp yaşamaktadır ve bireysel farklılıklar neredeyse imkânsız hale gelmiştir[38]. Zira suçluları ve onların ruhunu eğitmeyi amaçlayan disiplin iktidarı, insanı uzay zaman içinde sınıflandırma, gözetim ve rutinleştirme süreçlerine tabi kılan yeni hapishaneler geliştirmiş, hapishanenin gelişmesiyle birlikte panoptisizm ilkesi altında yeni bir disipliner iktidar biçimi yaratılmıştır[39].

Bu noktada sosyal kontrol perspektifini tabiri caizse "dışlayan" risk yaklaşımına da değinmekte fayda bulunur. Dışlama ifadesinin sebebi kanımca risk yaklaşımını savunanların liberal müdahaleci sosyal kontrol stratejilerine karşı bir şüphecilik içinde olmaları, direkt olarak suça, suçluya, suçtan korunmaya odaklanmalarıdır. Özellikle Malcolm M. Feeley and Jonathan Simon'un çalışmalarında; tehlikelere göre sınıflandırılmış grupları tanımlama ve yönetme teknikleri üzerine kurulu yeni bir penolojiden bahsedilmektedir[40]. Buna göre; hukukun diğer alanlarında da benzerleri bulunan bu yeni dil, odağı ceza hukuku ve kriminolojinin birey odaklı geleneksel kaygılarından uzaklaştırmakta ve onu aktüeryal değerlendirmeye yönlendirmektedir[41].

Bu değişimin ise; hapsedilmeye artan güveni kucaklayan ve gözetim ile gözaltı endişelerini birleştiren, bireyleri cezalandırmaktan onları yönetmeye geçen yeni bir tür cezai süreç vizyonunun veya modelinin geliştirilmesi gibi birtakım sonuçları vardır[42]. Risk görüşleri, sosyal kontrol görüşlerinin aksine neredeyse tamamen suç azaltma potansiyeline odaklanmıştır. Ancak gözetim ile risk yaklaşımının birlikte

---

[37] Ibid, s.16.
[38] DURKHEIM, É., SPAULDING, J. and SIMPSON, G. (2005). "Suicide: A Study in Sociology. Routledge". , s.114.
[39] COLEMAN, 2004,s.20.
[40] SIMON, J., ve FEELEY, M. M. (1992). "The new penology: Notes of the emerging strategy of corrections and its implications. Criminology", 30(4), s. 449.
[41] Ibid, s.449.
[42] Ibid.

değerlendirildiği gözlense de kanımca CCTV'nin suçu azaltıp azaltmadığı ve suçluların hangi oranda tespit edildiğine ilişkin soruların cevaplarına da odaklanmak gerekir.

Sosyal kontrol çerçevesinden, suçun önlenmesinden daha fazlası olan, bulunduğu toplumsal yapı ile birlikte yorumlanması gereken CCTV ve türevleri, bu "güvenlik amaçlı kullanımı aşma" durumunu çeşitli sorular ile iç içe geçerek yapar. Örneğin; CCTV'lerin kullanımı çoğunlukla suçlara yönelik kaygılarla mı ilgilidir yoksa kamusal alanda belirli tavırlardan kaçınmayı tetikleme amacı da var mıdır? Kamusal alanlarda kullanılan gözetim sistemlerinden ciddi kârlar elde eden şirketler var mıdır, bu çıkarlar ile vatandaşların gözetim ile elde ettiği fayda ve kaybedilen mahremiyet gibi unsurlar dengelenmekte midir? CCTV'lere toplumsal karşı çıkışın az olduğu gözlemine dayanarak, bu denli yüksek oranlı rızalar ne ölçüde üretilmektedir? Gözetim sistemlerinin işleyişine ne gibi sınırlar konmaktadır ve bu sınırlar mahremiyeti koruyan sınırlar veya kurallar ile ne şekilde örtüşür? Bu sorulara hukukun tatmin edici bir yanıt verebilmesinin yolu ise; konuya sosyo-hukuki bir perspektiften bakabilmeye, normların ifade ettiği değer ve anlamların altını deşebilmeye bağlıdır[43].

Nihayetinde video gözetim sistemlerinin sosyal bir ortama girmesi sayesinde, yeni bir sosyal kontrol yöntemi olarak cihazlar, üzerinde kontrol mekanizması kurulmaya çalışılan toplumun bazı yönlerini değiştirir[44]. Bu, belirli bir kontrol tarzına tabi olan bazı insanlar için disipline edilmeyi içerebilir ancak aynı zamanda insanların sosyal olarak belirlenmiş davranış normlarından nasıl, ne zaman, neden ve hangi amaçlarla saptığını da şekillendirecektir[45]. Gözetim sosyal kontrol penceresinden, izlenen davranışı şekillendirmek için yapılan bir veri toplama yönetimidir ve bu haliyle dahi çok çeşitli kamusal alanlara entegre olmuştur. Bu ise bireylerin hayatlarında ve dolayısıyla sosyal düzende doğal olmayan yani kendiliğinden gelişmeyen birtakım değişikliklerin veya uyarlamaların olması anlamına gelecektir.

---

[43] HATİPOĞLU AYDIN,2022, s.298.
[44] INNES, M. (2003). "Understanding Social Control: Deviance, Crime and Social Order". Open University Press.s.128.
[45] Ibid.

Günümüzde dünya nüfusunun %60'dan fazlası internet kullanıcısıdır[46]. Diğer taraftan bu kullanıcıların %55'inin dijital ayak izlerini kaldırmak veya maskelemek için çerezleri temizlemekten e-postalarını şifrelemeye kadar uzanan adımlar atmakta oldukları gerçeği ise bireylerin yalnızca kameralarla değil internet üzerinden de sürekli izlendiğini düşündüğünün veya bildiğinin göstergesidir[47]. Kişilerin kuruluşlar veya hükümet tarafından gözlemlenmekten kaçınmak için dijital dünyada adımlar atması, kamusal alanda kameralı gözetleme durumundan farklıdır. Zira kişisel mahremiyetin ihlal edildiğinin düşünüldüğü noktada, kamusal alanlara çıkmaktan veya sosyal hayata karışmaktan imtina edilmesi oldukça güçtür.

Bu sebeple CCTV'lerin konuşlandırılmasına dayanak olan hukuki düzenlemelerin çok boyutlu bir değerlendirme sonucunda yapılması daha önemli hale gelmektedir. Nitekim bireylerin bundan kaçınma fırsatı veya ihtimali - yerleşimin olmadığı yerlerde tecritte yaşamak dışında- yoktur. Öyle ki bugün Fransa'nın kırsal bölgelerinde dahi CCTV proje çalışmaları yürütülmektedir[48]. Kanımca gözetimi tek başına anlamaya çalışmanın tehlikesi, sosyal kontrolün diğer yönleriyle olan bağlantıların kaçırılmasıdır.

1.3. GÖZETİM VE PANOPTİKON KURGUSU

Başlık altında gözetim çalışmalarında oldukça önem arz eden panoptikon fikirlerine yer verilmiş, bu kurgunun gerçeklikle arasındaki bağlam oluşturulmaya çalışılmıştır. Bunu yaparken panoptikon tartışmalarının fitilini ateşleyen Bentham ile tartışmalara devlet-otorite-disiplin ve güç açılarından yaklaşan Foucault'nun görüşleri üzerinde özellikle durulmuş, sonrasında Foucault'dan miras kalan fikirlerin gelişimi kısaca incelenmiştir.

---

[46] The World Bank, "Individuals using the Internet (% of population)", (Erişim Tarihi: 02.07.2022). https://data.worldbank.org/indicator/it.net.user.zs

[47] York, J. the harms of surveillance to privacy, expression and association, Global Information Society Watch.

[48] "Les Caméras De Vidéosurveillance Peuvent Désormais Vidéo-Verbaliser".(Erişim Tarihi:28.09.2022) https://toulouse.sous-surveillance.net/spip.php?page=article&id_article=132&connect=sosu

1.3.1. Bentham'dan Foucault'ya Panoptikon

Bentham'ın panoptikonu, günümüz gözetim tartışmalarını anlamlandırmak, iktidar-gözetim arasında ilişki kurmak ve kapitalizmin gözetimin boyutları üzerindeki etkisini sorgulamak için temel bir kurgudur. Öyle ki Foucault da konu hakkındaki çalışmasını, Bentham'ın panoptikonuna dayandırır ve aynı kurguyu geliştirir. "Göz"ün iktidar, "hapishane"nin de toplum veya kamusal alan olduğu bir düzenekte, iktidar kapitalizmin etkisiyle küreselleşirken, mahremiyet daha çok yok olmakta, yerel "iktidarlar" ise bu döngünün içinde ekonomik faydalar elde etmektedir[49].

Panoptikon yazıları, toplam yirmi bir mektupta tasavvur edilen ve çeşitli kurgusal imgelerden meydana gelen bir *jeu d'esprit*[50]'dir. Panoptikon, çok sayıda küçük hücreden oluşan, ortasında bir gardiyan gözetleme evi olan, gözetmenin mahkumları gözetlediği ve fakat mahkumların izlendiklerini bilip, göremedikleri bir hapishane modelinin adıdır. Bu mimari modeli Bentham şöyle tanımlar:

> *"…Bina daireseldir. Mahkumların hücreleri daireyi kaplar. İsterseniz onlara hücreler diyebilirsiniz. Bu hücreler birbirinden ayrılır ve bu sayede mahkûmlar, çevreden merkeze doğru yayılan yarıçaplar biçimindeki bölmelerle birbirleriyle her türlü iletişimden uzak tutulur…Gözetmenin dairesi merkezi işgal eder, eğer rica ederseniz onu arayabilirsiniz. (…) Hücrenin iç çevresi, hücrenin herhangi bir bölümünü denetçinin görüşünden gizlemeyecek kadar hafif bir demir ızgara ile oluşturulmuştur. Bu parmaklığın yeterince büyük bir kısmı, mahkûmu ilk girişinde kabul etmek ve gardiyan veya yardımcılarından herhangi birine herhangi bir zamanda izin vermek için bir kapı şeklinde açılır. (…) Bu amaçla, locanın zemin katının zemini, hücrelerin ilk katının zemininin yaklaşık %4 fit içine yükseltilir. Bu sayede gözetmenin gözü, ayağa kalktığında, hücrelerin yukarıda belirtilen üst katının zemin seviyesinin üzerinde veya biraz üzerinde olacaktır ve her halükârda hem buna hem de hücrelerin temel bölümüne zorluk çekmeden ve duruş değiştirmeden komuta edecektir. (…) planın özü, gözetleyenin durumunun merkeziliğiyle, görülmeden görmeye yönelik iyi bilinen ve en etkili düzeneklerle birleştirilmiş olmasıdır. (…) Belki de en önemli nokta bu olsa da denetlenecek kişilerin kendilerini her zaman denetleniyormuş gibi hissetmeleri gerektiğini, en azından böyle olma ihtimallerinin büyük*

---

[49] BENTHAM, J., PEASE-WATKIN, C., WERRET, S., ÇOBAN, B. VE ÖZARSLAN, Z., 2019, s.7.
[50] Nükte, akıl oyunu. (fr.)

olduğunu, ancak hiçbir şekilde öyle olmadığını gözlemlemenizi rica ederiz"[51].

Görüleceği üzere böyle bir mimarinin yapılmasındaki esas amaç, mahkumların izlendiklerinden "şüphelendikleri" ancak bundan hiçbir zaman tam olarak emin olamayacakları bir sistem oluşturmaktır. Böyle bir sistemin kurulmasının avantajları ise; mahkumların karşı konulamaz bir yönetim ve baskı altında olması sonucunda, suçu önlemek için yapılan onca çaba yerine doğrudan ve etkili bir denetim yapılması ve böylece yargının yükünün hafiflemesidir[52]. Bentham, iktidarı gardiyanın gözü olarak yansıtmış, bu şekilde güç kazanan iktidarın sürekli olarak yeniden doğmasını sağlamıştır. Bireyler sürekli olarak izleniyormuş hissi ile devamlı baskılanacak ancak bundan emin olamadıkları için de buna karşı bir eylemde bulunamayacaklardır. Bu şekilde hem göz yani gözetleyen bir "mitos" olarak dilden dile dolanacak hem de bu şekilde duyulan korkunun derine inmesi sebebiyle bireyler suçtan kaçınacaklardır.

Bentham'ın panoptikonunun üzerine başta Foucault olmak üzere pek çok kişi tuğla koymuştur. Özellikle Foucault, Bentham'ın fikrini hapishane sınırlarından çıkararak topluma, kamusal alanın kendisine yaymıştır. Bu kamusal alanda ise; iktidarın "göz"ünü hisseden bireyler otoriteyi tüm benliklerinde hissetmekte, sosyal kontrol çemberinin dışına hiç çıkamamaktadırlar. Sosyal kontrol çemberinden çıkılamayacak olmasının sebebi, bu çemberin hayatın bizzat kendisi olmasıdır. Okullardaki yemekhaneden, yolların geometrisine, alışveriş yerlerinden, iş yerlerine kadar her yerde hiyerarşik, devamlı ve amaçsal bir gözetim bulunmaktadır.

Foucault gözetim iktidarının bu denli yaygınlaşmasını, yeni iktidar mekanizmalarına bağlar[53]. Bu yeni mekanizmalar sayesinde hem ekonomik ilişkiler hem de düzeneğin diğer araçları, bu disiplin sisteminin içine iyice girip birbiriyle

---

[51] BOZOVIC, M. (1995). "Jeremy Bentham the panopticon writings". Verso: London and New York. s.35-43.

[52] BENTHAM, J., PEASE-WATKIN, C., WERRET, S., ÇOBAN, B. VE ÖZARSLAN, Z. (2019) "Panoptikon: Gözün İktidarı" (3. Baskı). (Barış Çoban, Zeynep Özarslan Çev.). İstanbul: Su Yayınları.s.45-48.

[53] Ibid, s.264.

bütünleşmiştir[54]. İktidarı gözetimi adeta bir makine gibi çalışmakta ve çok yönlü bir denetimsel hiyerarşi ile daima uyanık olarak, kendini yine kendi yaratımı olan mekanizmalarla desteklemektedir[55]. Foucault'nun yeni iktidar mekanizması olarak tanımladığı araçlar günümüzde teknik gelişmelerle daha belirgin hale gelmiştir. Bunun anlamı ise kanımca iktidarın kendini destekleme aracı olan hukuk normlarının öneminin artmasıdır.

Foucault'nun disiplinci toplumunda iktidar, arzunun bastırılması, arzunun sınıflandırılması, tablolaştırılması ve düzenlenmesi yoluyla toplumu baskı altına alır[56]. Bu, modern bireyciliğin kendine has öz denetim, özgürlük veya mahremiyet gibi özellikleri için de bir çelişki gibi görünmektedir. Bununla birlikte böyle bir gözetim, ekonomi politik ve onun tamamlayıcısı olan bazı araçların desteği üzerine kuruludur[57]. Yani sistem tüm modern araçları ve unsurları ile topyekûn bir işleme halindedir. Kanımca burada ele alınan asıl problem tek tek iktidar araçları da değil, yapının kendisidir.

Diğer taraftan, Foucault'nun gözetim konusunda kullandığı kavram setleri, kriminoloji ve hukuk sosyolojisi ile de derinden ilgilidir. Böylece, yalnızca hapishaneler, akıl hastaneleri, mahkemeler gibi "zorlayıcı" kurumların toplumu nasıl disipline ettiği değil aynı zamanda gündelik hayatı basit bir şekilde kolaylaştıran eğitim kurumları, hastaneler, sosyal güvenlik kurumları gibi yerlerin de aslında bir disiplin işlevine sahip olduğu anlaşılmıştır[58]. Görüldüğü üzere Foucault'un yarattığı senaryo, tahakküm ve kapsamlı kontrol üzerine kuruludur. Böyle bir kurguda Bentham'ın hapishanesindeki gibi bir iktidar, tüm yönleriyle baskıcıdır ve özne olan birey, iktidarın gözetimi altında deyim yerindeyse "nesneleşmiş" durumdadır.

Çalışmada ortaya konulacak sav açısından önemli olan husus ise; Foucault'nun "hukuk reformu" anlayışıdır. Gözetleyene karşı hukuka dayanak bir modern devlet

---

[54] FOUCAULT, 2015, s.264.
[55] Ibid.
[56] KLING & LYON, 1994,s.211.
[57] BAŞTÜRK, E. (2018). "Post Yapısalcı Teori Bağlamında Post-Panoptik Gözetimin Küresel Politikası". Siyasal: Journal Political Sciences, 27(1), 47–68.s.50.
[58] LACOMBE, D. (1996). "Reforming Foucault: A Critique of the Social Control Thesis". The British Journal of Sociology, 47(2), s.333.

savunusu oluşturmak için, sosyal aktörlerin eylemlerine de bakmak gerekir. Foucault toplumsal yapı ve toplumsal aktörler gibi karşıt gibi görünen kavramların ikilikler yaratılarak yorumlanmasına ve hukuk üretim sürecine bu şekilde katılmasına karşı uyarıda bulunur[59]. Hukuk reformunda yapı/fail ikiliğine karşı Foucault, toplumsal dünyanın ilişkisel ve üretken bir kavrayışını önerir[60]. Dolayısıyla karşımıza yine gözetim araçları karşısında örülmesi gereken bir sosyal-hukuk ağı çıkar.

1.3.2. "Multi-Panoptik" Dönemde Gözetim

Gözetimin yeni teknikler ile daha yaygın hale gelmesi ile panoptikon fikirleri de başkalaşmış, sosyal kontrolün boyutlarının değişiminin de etkisiyle Foucault sonrası bu yeni dönemde gözetim konusunda post panoptik fikirler ortaya konmaya başlanmıştır. Gözetimin bir hapishane metaforu içinde disipline edilmeye çalışılan bir toplum aracılığıyla ifade edilmesinden çok, devlet teorisindeki dönüşümlerin, politik ekonominin, mekânların, olasılıkların teknoloji ile birlikte yorumlayıcı bir hale gelmesinden bahsedilmektedir[61]. Zira günümüzde Rousseau'nun yarattığı şeffaflık toplumunun bir ifşa toplumuna dönüşerek totaliter bir yapıya bürünmesi, Bentham'ın merkez-çevre ayrımı olan panoptikonunun dönüşerek perspektifsiz bir hale gelmesi, insanın artık her yerden ve herkes tarafından gözetlenmesi söz konusudur[62]. Gerçekten de bu panoptik perspektifsizlik veya kendine özgü panoptiklik içinde artık yukarıdaki bir "göz" tarafından gözetlenmeden çok, daha etkili ve her açıdan gözetim süreci doğmuştur.

Byung-Chul Han, Bentham'ın kurgusu ile bugün arasında bir fark daha ortaya koyar. Ona göre Bentham'ın hapishanesinde ki mahkumlar bir gözetleyen olduğunun -bir şekilde farkında iken; günümüzde bu farkındalık da yok olmuş, bireyler özgür oldukları zannı içinde hiper iletişim çağında kendilerini panoptik pazarda sergileyen birer ürün haline gelmiş ve yalnızca mahkûm değil aynı zamanda hem kurban hem de fail

---

[59] LACOMBE, 1996,s.349.
[60] Ibid.
[61] BAŞTÜRK, 2018,s.51.
[62] HAN, B.C (2020) "Şeffaflık Toplumu. (Haluk Barışcan Çev.)" İstanbul: Metis Yayınları. 6. Baskı., s. 67.

olmuşlardır[63]. Bunun ötesinde her gün yeni gözetleme tekniklerinin çıktığı ve herkesin herkesi kontrol ettiği şeffaf toplum içinde, azalan güven sebebiyle toplumlarda bir güvensizlik hakimdir ve üretim ilişkilerinin de şeffaflaşmasıyla toplumsal unsurlar da değersiz ve işlevsiz hale getirilmiştir[64].

Han'ın ifade ettiği perspektif yitimi, bugün tüm dünyada geniş kitlelere hitap eden sosyal medya uygulamaları ele alındığında daha açık bir şekilde göze çarpmaktadır. Bu uygulamaların her biri ayrı birer gözetleme merkezi rolünü üstlenmekte, bireyler bu "hapishanelere" ıslah olmak için değil hem gözetlemek hem de gözetlenmek için birer gönüllü olarak girmektedir. Kanımca buna "multi-panoptik" dönem de denilebilir. Bu dönem kendi içinde hem geçmişten gelen ve git gide azalan mahremiyet kaygıları, hem sosyal hayata başka türlü entegre olamama korkusu ile ifşa ihtiyacı, hem de güvenlik kaygıları duyulan bir dönemdir.

Zygmunt Bauman, ne kadar yeni dönemin özellikleri ile süslenmiş olursa olsun, panoptik çağın henüz sona ermediğini savunur[65]. Bunun yanında, insanların sermaye kaynağı olarak görüldüğü bu çağda, herkesin kendi panoptikonunu sırtında taşıdığını, mahremiyet konusunda da bireylerin kendi bekçileri olmak durumunda olduğunu, artık gözetimin bireylerin erişebileceği hükümetlerce değil, uluslar üstü ve küresel bir hale geldiğini belirtir[66]. Dolayısıyla burada bir küresel güvensizliğin varlığı söz konusu olacaktır.

Lyon ise gözetime ilişkin en büyük gerekçelerden birinin güvenlik olduğunu, güvenliği sağlamanın gözetimin en büyük motivasyonu olduğunu belirtse de ona göre günümüzde özellikle de 11 Eylül saldırılarından sonra artık devletin özellikle akıllı sistemlerle gözetimde tamamen güvenliği sağlama sebebine sırtını dayaması çelişkilidir[67]. Lyon, yapay zekâ kullanan CCTV'ler, otomatik plaka tanıma sistemleri,

---

[63] Ibid. s.68-69.
[64] HAN,2020, 69-71.
[65] BAUMAN, Z., & LYON, D. (2016). "Akışkan Gözetim (Elçin Yılmaz Çev.)". Ayrıntı Yayınları.2. Baskı, s.72.
[66] Ibid, s.70-75.
[67] Ibid, s.115.

yüz okuyan ve biyometrik veri elde eden gelişmiş kamera sistemlerinin yaratacağı mahremiyet kaygıları ile güvenlik sağlanması istencinin yarattığı ikiliklerden bahseder. Bu aşırı güvenlik istenci ve mahremiyet kıskacında kalan birey, hem eski liberal söylemlerin etkisinde kalmakta hem de dijital sistemlere yeni dönemin askeri gibi güvenmenin tereddütlerini yaşamaktadır.

Yeni dönemdeki gelişmelerin bir sonucu olarak gözetim ve güvenlik ikilemi Torin Monahan açısından bir değiş tokuş ilişkisidir. Öyle ki; özgürlüğe karşı güvenlik, mahremiyete karşı güvenlik ve maliyete karşı güvenlik sorgulamaları sürekli devam ederken; esas konu cevaplanamayan sorular ile perdelenmektedir[68]. Bu noktada halkın karar vermesine izin verilen tek şey, daha fazla ulusal güvenlik sağlamak için gerekli fedakarlıkları yapmaya istekli olup olmadığıdır[69]. Diğer ifadeyle; ulusal güvenlik sağlanması için mahremiyet yitimine veya sınır aşımlarına göz yumulmaması adeta güvenliğin sağlanmamasına razı olmak anlamını taşımaktadır. Peki multi-panoptik dönemde bu sorun nasıl aşılmalıdır?

Gözetim-mahremiyet-güvenlik ve hukuk hakkındaki çalışmaların pek çoğunda, hukuk yapımındaki şeffaflık, hakların dengelenmesi, ölçülülük gibi hususlara değinilse de bu sorunun nasıl aşılacağı hakkında net bir çerçeve çizilememektedir. James B. Rule'a göre bu dengeleme dili oldukça belirsizdir ve böyle bir "kolaya kaçış" önemli sorular sorulmaksızın etkisiz kalacaktır[70]. Örneğin; okula giden çocukların her hareketini izlemekle ilgili riskler ne kadar kötüdür? Muhtemel teröristleri tespit etme umuduyla sıradan bireylerin hareketlerini takip etme ihtiyacı ne kadar zorlayıcıdır[71]? Bu sorular gibi genel vargı üretecek sorulara cevap bulabilmek, mahremiyet ve gözetim tartışmasının temelinde yer alması gereken esaslardandır.

---

[68] MONAHAN, T. (Ed.). (2006). "Surveillance and Security Technological Politics and Power in Everyday Life". Routledge., s.2.
[69] Ibid, s.2.
[70] RULE, J. B. (2012). "Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience.", s.183.
[71] Ibid.

Rule güvenlik sağlamak için neredeyse kamusal olan her yerde yapılan izlemeyi, aile içi şiddet, sevgisizlik ve dolayısıyla toplumsal "bozuklukları" ve "güvensizlikleri" önlemek için evlerin içinin de izlenmesi örneği ile değerlendirir[72]. Toplum düzeni ve güvenliğini temin etmek için evlerin içine de kamera konulmasına engel olan unsur mahremiyet ve özel hayat ise; bunları bütün sosyalleşme alanlarının izlenmesinden ayıran hususların ortaya konulması, konu hakkındaki çelişkileri gidermek için etkili olabilir.

Gözetim ve güvenlik sistemlerinin ardındaki politikada, "güvenlik" ile ne kastedildiği, neyin veya kimin bu gözetimden, daha fazla ulusal güvenlik sağlamada gözetleme sistemlerinin ne kadar etkili olduğu, devletler açısından onların niçin "yatırıma değer" olduğu sorularını sorabilmek, bu sistemlerin gerçekten çalışıp çalışmadığına ilişkin sorulardan daha önemlidir[73]. Zira devletin, kamusal alanlarda kameralı gözetim sistemlerine niçin bu kadar yatırım yaptığı, bu şekilde hangi güvenlik zafiyetlerinin giderildiği, hangi tür sistemlerin niçin tercih edildiğini ve bu sistemlerin ne üzerinde etkili olduğunu vatandaşlarına anlatabilmesi, CCTV'lerin bazı durumlardaki gerekliliğine ve etkinliğine de vurgu yapabilecektir.

Bu konuda Daniel Solove, tartışmadaki birçok argümanın, yasanın mahremiyeti nasıl koruduğuna dair yanlış varsayımlara dayandığını, hukukun tartışmadaki pek çok hatalı argüman tarafından şekillendirildiği ve bunların yasama ve yargı görüşlerini etkilediğini, gizliliğin veya mahremiyetin güvenlik için bir tehdit oluşturmaksızın da korunabileceğini savunarak, yeni teknolojilerle gelişen gözetim olanakları karşısında bunların benimsenip benimsenmeyeceğine ve sonuçlarından korunmaya dair hukuken hazırlıklar yapılması gerektiğini ifade eder[74].

Solove, hakların dengelenmesi anlayışına karşı değildir ve gözetim sistemleri kurulurken belirli soruların özellikle cevaplanmasından yanadır: Sistem iyi çalışıyor mu? Sistemin kullanılması mahremiyet ve sivil özgürlükler açısından herhangi bir sorun yaratır mı? Ne tür bir gözetim ve düzenleme hangi sorunları çözecek veya iyileştirecektir?

---

[72] Ibid, s.189.
[73] MONAHAN, 2006,s.2
[74] SOLOVE,2011, s.205.

Mahremiyeti korumak adına güvenlik önlemi ne ölçüde sınırlandırılmalıdır? Mahremiyetin tesisine ilişkin sınırlar, güvenlik önleminin etkinliğini ne kadar engeller? Mahremiyet sınırları tesis edilen azaltılmış etkinlikte cihazlar, maliyete değer mi?

Günümüzde artık hem güvenlik hem de otorite tesisi için bireylerin devletler ve toplumlarca sınırlandığı dönemlerden, teknolojik imkanların etkisiyle "izleyerek kontrol" dönemine geçilmiştir. Armand Mattelart'a göre; güven ve istikrarın göç, ekonomi, saldırganlıklar gibi çeşitli sebepler ile azalmasına ve küresel ekonomik çıkarların artmasına dayanarak, bilgi teknolojisinin kullanımı karşısında uluslararası hukuk veya bazı liberal değerler etkisiz kalmıştır[75]. Bu etkisizlik içinde de güvenlik-özel hayatın gizliliği ve mahremiyetin yarattığı çelişkilerin içinde, "rızaya dayalı ve meşru" bir özgürlüklerden alıkonulma durumu söz konusu olur[76]. Yani toplumlar, güvenliğin sağlanması uğruna, yeterince bilinçli olmayarak mahremiyetlerinden kayıtsız bir şekilde vazgeçmektedir.

Mattelart'ın önerisi ise; güvenliğin bir hak olarak "eğitim, sağlık, çalışma…" gibi hakların arasına entegre edilerek, bunun özgürlükler bu denli sınırlanmadan sağlanmasının devletin asli görevi haline getirilmesidir[77]. Fakat kanımca bu şekilde, güvenlik hakkının yaygın bir gözetim ile elde edilmesi özel hayatın gizliliğini ihlal etse de, güvenlik hakkının tesisi amacıyla da sınırlanabilecek, dolayısıyla önceki durum ile yeni durum arasında bir fark olmayacaktır.

Evgeny Morozov, çağımızdaki dijital gözetimi bir tür dijital bozgunculuk olarak görür ve onu, otoriter hükümetlerin işine yarayan, kimi zaman halkı eğlendirmek için havuç kimi zamansa resmi çizgiye meydan okumaya cesaret edenleri cezalandırmak için sopa olarak kullanılabilen bir iktidar veya güç aracı olarak görür[78]. Bu sebeple, Facebook gibi bir sosyal platformun İran veya Çin'deki aktivistlerin özel bilgilerini ifşa ettiğini ve

---

[75] MATTELART, A. (2012) (Onur Gayretli ve Su Elif Karacan Çev.) "Gözetimin Küreselleşmesi: Güvenlileştirme Düzeninin Kökeni". İstanbul: Kalkedon Yayınları. (Orijinal eserin yayın tarihi:2007. s.300-301.
[76] Ibid, s.300-301.
[77] Ibid, s.305.
[78] MOROZOV, E. (2011). "The Net Delusion: The Dark Side of Internet Freedom". In New York (Vol. 9, Issue 04). Public Affairs. s.16.

hükümetleri aktivistler ile Batılı fon sağlayıcıları arasındaki gizli bağlantılara yönlendirdiğini hayal etmek hiç de zor olmayacaktır[79]. Böylece multi-panoptik dönemde gözetim, politik ve ekonomik çıkarlardan ayrılmadan, otoriter devletlerin, politika yapıcıların veya büyük şirketlerin hüküm sürdüğü ve tüm gücü elinde tuttuğu bir devasa yapı halindedir.

Multi-panoptik dönemde iletişim teknolojilerinin ve teknik diğer imkânların artmasıyla birlikte, ekonomi de gelişen teknoloji ile eşgüdümlü olarak dijitalleşerek ilerlemiş, yeni-ekonomi, gözetim teknolojilerini kapsamına almıştır. Bu şekilde, gözetim cihazları ile elde edilen veriler ticari birer ürün haline gelmiş ve küresel ekonomik döngünün içine girmiştir. Böylece veri üreticisi olan bireyler ile veri tüketicisi olan işletmelerin veya hükümetlerin, çok çeşitli kaynaklardan birikmiş verileri topladığı, düzenlediği ve paylaştığı küresel bir dijital ekosistem oluşmuştur[80]. Veri ekonomisi, sektörün uygulamalarını halktan gizlemek için tasarlanmış bir "dijital perde" etrafında yapılandırılıp, kişisel veriler şirket malı ve özel bir sır olarak kabul edildiğinde ise; bu dijital perdenin biraz aralanması için tüketici, hükümet ve piyasa güçlerinin bir araya gelip artık kullanıcılara ürettikleri veriler üzerinde daha fazla kontrol sağlaması durumu söz konusu olmuştur[81].

Data oligarkları olarak da nitelendirilen büyük şirketlerin sahipleri olan teknoloji milyarderlerinin, kitlelere bir benzeri görülmemiş bilgi geçitleri açtığı, muazzam bilgi yığınlarını yönettikleri ve en önemlisi nasıl elde edildiği anlaşılamayan bu bilgi yığınlarının, politik amaçlar güderek devletlerle paylaştıkları tartışılmaktadır[82]. Örneğin; Google'ın hareket ettiği zeminin her zaman kaygan olduğu ve şirketin adeta vekaleten devlet adına izleme yapabilecek güçte olduğu belirtilmektedir[83].

---

[79] Ibid.
[80] MIT Technology Review(2016), "Capitalizing on the data economy", (Erişim Tarihi: 19.11.2022) https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/
[81] Harvard Business Review(2022), "The New Rules of Data Privacy", (Erişim Tarihi: 19.11.2022) https://hbr.org/2022/02/the-new-rules-of-data-privacy
[82] JASANOFF, S. (2021) "Teknoloji ve İnsanın Geleceği. İstanbul: Bgst Yayınları", 1.Baskı. s.121-122.
[83] Ibid. s.123.

Diğer taraftan NSA'in (*The National Security Agency*), ABD'de bulunan bazı bilişim şirketleri ile Facebook, Google, Yahoo, Apple gibi büyük şirketlerin merkezi sunucularına erişebilmesi de iddia konusudur[84]. Muammer Ketizmen ve Aslıhan Kart'ın çalışmasında da yer verildiği üzere; günümüzde şirketlerin piyasada tutunma yolu olarak verileri para ile doğrudan ilişkilendirmesi, birbirlerine veri satmaları ve kiralamaları şeklindeki argümanlar ile dijital kartellerin ortaya çıkması gibi durumlar, veri ekonomisinin büyüklüğünü gösterir[85].

Shoshana Zuboff ise içinde bulunduğumuz çağda artık dijital bağlantılarımızın başkalarının ekonomik veya ticari çıkarları için araçsallaştırıldığını, bu şekilde insan deneyiminin pek çok yönünden fayda elde edildiğini, gözetim kapitalizminin her dakika yayılarak dijital reklamcılıktan, akıllı-internet bağlantısı olan ev aletlerine, bireylerin gelecekte nasıl bir tercih yapabileceğine varan davranış kodlamalarından, bireysel özerkliğimize kadar toplumların içine sirayet ettiğini belirtir[86]. Diğer taraftan Zuboff'a göre, gözetimden ekonomik çıkar elde eden "gözetim kapitalistleri"nin, günümüzdeki yaygın gözetimin bir zorunluluk olduğunun bireylerce düşünülmesinin arzulandığı bir çelişki söz konusudur[87].

Öte yandan, bilişim teknolojilerini üretebilen gelişmiş ülkelerin ürettikleri yeni gözetim sistemleri tüm dünyaya yayılmakta ve büyük ekonomik kazançlar getirmektedir[88]. Özellikle reklam endüstrisinin yaygın kullanım aracı olan internet veya siber alan, büyük şirketlere hitap ettikleri hedef kitleyi anlama şansı tanımış, kişisel verilere sahip olan şirketler neredeyse birer istihbaratçı olmuş, bilgi sahibi olmak güç

---

[84] Greenwald, G., MacAskill, E.(07.06.2013), "NSA Prism program taps in to user data of Apple, Google and others", The Guardian (Erişim Tarihi: 19.11.2022) https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[85] KETİZMEN, M., KART, A. (2019). "Kişisel Veri ve Rekabet Hukuku Kapsamında Big Data", Kişisel Verileri Koruma Dergisi. 1(1), s.67.

[86] ZUBOFF, S. (2019). "The Age of Surveillance Capitalism. Public Affairs". www.publicaffairsbooks.com ,s.5-18.

[87] Ibid, s.21.
Ayrıca konu hakkında LOKKE, E. (2020) "Mahremiyet: Dijital Toplumda Özel Hayat (Dilek Başak Çev.)". İstanbul: Koç Üniversitesi Yayınları. (Orijinal Eserin Yayın Tarihi:2017).

[88] DOLGUN, 2004, s.2

sahibi olmak halini almıştır[89]. Böyle bir döngüyü yaratan ekonomik ilişkiler bütünü, gözetim kapitalizminin sonucudur ve kapsamında devamlı aktif olan büyük oyuncular yer almaktadır[90].

Yıllar içinde video kameraların sayısı, kameralı izlemeye yönelik yazılımlar, kamera üreten şirketler ve devletin video kayıt sistemlerine ayırdığı bütçe gibi video izleme ekonomisine dahil olan unsurların dikkat çekici seviyede arttığı bilinmektedir. Örneğin; İngiltere'nin 2009-2019 arasında CCTV'ye üç milyar sterlin harcadığı, bunun yüzde 17'lik bir artışa tekabül ettiği, belediyelerde bazı departmanların bütçeleri kesilirken, CCTV'ye yönelik harcamaların saldırgan olduğu belirtilmiştir[91]. Bunun anlamı video gözetime ayrılan bütçelerin diğer kalemlerden daha önemli kabul edildiğidir. Bunun sebepleri ise çalışmanın ikinci bölümünün konusudur.

Hukuka, insan haklarına veya mutlak olduğu kabul edilen kişilik hakkında aykırılıkların oluştuğu durumlarda başvurulan, ölçüsüz veya kuralsız kişisel veri kullanımına karşı mahremiyeti tesis eden hukuk normlarının, bu türden aykırılıklara karşı bir çözüm olması amaçlanmaktadır. Bu sebeple çalışmanın üçüncü bölümünde yer verildiği üzere kişisel verilerin korunması adına pek çok hukuki düzenleme yapılmıştır. Bu noktada eleştirilen ise, yüksek para cezalarının yer aldığı GDPR (Avrupa Birliği Genel Veri Koruma Tüzüğü) ve sair temel nitelikteki düzenlemelerin, gözetim ekonomisinde birer meşru rıza alma aracı haline dönüşmüş olmasıdır. Zira bu bakışla problem, GDPR'da yer alan aydınlatılmış onamın (*informed consent*), olup bitenin ne olduğu anlaşılamayan bir gözetim sarmalında gerçekten işe yarayıp yaramayacağı veya "aydınlatılma" durumunun oluşup oluşmayacağıdır[92]. Ayrıca mahremiyeti koruyan hukuk normlarının anlaşılabilir olmadığı, izleme ekonomisi karşısında bireylerin tam olarak anlayabileceği açıklıkta metinler bulunmadığı, bazı mefhumların oldukça

---

[89] ARIK, E. (2018) "Dijital Mahremiyet Yeni Medya ve Gözetim Toplumu". Konya: Literatürk Akademia , s.155.
[90] Ibid. s.155.
[91] The Times (2019), "Town halls cut services but spend millions on CCTV".
[92] BALL, J. (2021) Sistem. (Yasin Konyalı Çev.) İstanbul: Timaş Yayınları. (Orijinal eserin yayın tarihi 2020). s.172.

karmaşık olduğu, büyük şirketlerin nasılsa kendilerine has çeşitli mekanizmalarla mevzuatlara karşı uygun davranışlar geliştirebildikleri de iddia edilmektedir[93].

GDPR ve diğer düzenlemelerin, büyük şirketlere dair en büyük sorunları hala ortadan kaldırmadığı, veri simsarlarının hala bilgilerimizi stokladığı ve sattığı, özellikle çevrimiçi reklamcılık sektörünün potansiyel suiistimallerle dolu olmaya devam ettiğine dair söylemler ele alındığında[94], kamuoyunun bu konuda tatmin olduğunu söylemek oldukça güç görünmektedir. Bunları önleyebilmek için oluşabilecek risklerin ve eşitsizliklerin incinmeye en açık olan gruplar bakımından ayrıca değerlendirilmesi, kuralların uygulanması bakımından, riskli durumlarda önceden davranma mekanizmaları oluşturulması önerilmektedir[95].

1.4. GÖZETİM VE MAHREMİYET

1.4.1. Mahremiyet Kavramının Kısa Tarihi

Tarih boyunca çeşitli rejimler, gözetim yoluyla insanların hayatlarını kontrol etme amacında olmuşlardır. İmparatorlukların bugün gözetim için kullanılan teknik araçlara sahip olmadıklarından gizliliği denetlemekte başarısız oldukları ifade edilir[96]. Yani antik çağda mahremiyetin daha fazla sağlanmasının, dönemsel otoritenin gözetim istenci yokluğundan çok, teknolojinin gelişmemiş olmasından kaynaklandığı söylenebilir. Mahremiyet kavramı, bireyciliğin ortaya çıkışıyla doğrudan bağlantılıdır ve kökenleri Rönesans ve Reform hareketlerine kadar uzanır[97]. Matbaanın icat edilmesi ve yazılı malzemenin hızla yaygınlaşmasıyla, sosyal hayatta özel ve kamusal alanların ayrımı görünür olmuştur[98]. Örneğin dini alanlarda ve bireylerin yaşadıkları özel alanlarda bir

[93] Ibid. s.174-175.
[94] Wired (2022), How GDPR is Failing?
[95] JASANOFF,2021, s. 65.
[96] "VAN DER SLOOT, B.; GROOT, A. D. (2018) The Handbook of Privacy Studies". Amsterdam: Amsterdam University Press.s.23.
[97] Ibid, s.25.
[98] VAN DER SLOOT ve GROOT, 2018, s.25.

geri çekilme olmuş, bu alanlar kamusal alanların ve kentlerin baskılarından uzakta, bireyselleşme alanları olarak var olmaya başlamıştır.

Rönesans ile birlikte gelişen birey olma algısı hemen kabul görmemiştir. Mahremiyetin insanlar için değişen anlamı, özel bir alan olarak aileyi ve aile konutunu da dönüştürmüştür. Önceleri kalabalık aile içinde yer alan hizmetçi sınıfın yeri değişmiş, aile ve toplum arasında bir mesafe konulması amacıyla, örneğin evlerde odaların açıldığı koridor biçimi yaygınlaşmış, böylece konutların tasarımı dahi mahremiyeti sağlamak üzere farklılaşmıştır[99]. Mutlakıyetçi rejimlerin zayıflamasıyla "birey olarak vatandaş" fikri güçlenmiş, 19. yüzyıl mahremiyet kavramının hukuk açısından yorumunun da değişmesine yol açmıştır. Hukuk tarihi açısından mahremiyet bu dönemde her vatandaş açısından bir özlem ve "olması gereken" olarak görülmüş, 1789 Fransız Devrimi sonrası İnsan Hakları Evrensel Bildirgesi de mahremiyete dair bu özlem ve ideali sahiplenmiştir[100].

Mahremiyet olgusu tarihsel süreçte, nüfus artışı ve yeni teknolojiler olarak ifade edilebilecek iki temel unsur üzerine biçimlenmiştir. 19. yüzyılın başından itibaren nüfusun artması, bireylerin mahremiyeti ihtiyacında da bir artışa yol açmıştır. O dönem açısından yeni olan telefon, telgraf gibi teknolojiler, bir yandan kişilere dair özel bilgilerin toplanmasının araçları olurken, aynı zamanda bireysellik ve öznellik bilgisi ve duygusunu da güçlendirmiştir. Mahremiyet talebinin artması, mahremiyetin ihlali potansiyelinde de bir artış anlamına gelmiştir.

Solove, mahremiyetin her zaman insanlar için önemli olduğunu belirtir ve zaman içinde ortaya çıkan güvenlik-mahremiyet ikileminin bir denge içinde yorumlanması gerektiğini vurgular[101]. Hannah Arendt ise Nazi Almanyası'nda mahremiyet iddia edebilecek tek kişinin uyuyan kişi olabileceğini ifade ederek[102], mahremiyeti yok etmeyi

---

[99] Ibid, s.25-26.
[100] Ibid, s. 28.
[101] SOLOVE, D. J. (2011). "Nothing to Hide : the False Tradeoff Between Privacy and Security". Yale University Press. s.5-15.
[102] ARENDT, H. (1979) "The Origins of Totalitarianism". Harvest Book: New York.s. 338-339.
"(…) the Nazis could rightly announce: The only person who is still a private individual in Germany is somebody who is asleep."

totaliterlik ile bağdaştırır[103]. David Vincent, liberal değerlerin ortaya çıkışı ve yaygınlaşması öncesinde, mahremiyetin, devletin insanlara sunması sebebiyle kullanılabilen bir olgu olduğunu ve Devletin otoritesini özel alandan isteyerek çekmesi sonucunda kimi değerlerin ön plana çıkabildiğini not eder[104].

Devletin modern ve liberal bu biçiminin güçlenmesinin, bireylerin mahremiyetlerini ve gizliliklerini korumakta karşılarına çıkabilecek tehditlerin farkına varmaları sonucunu doğurduğu söylenebilir. Özellikle iki dünya savaşı arasında mahremiyet ve güvenliğin sağlanması amacıyla gözetim ikilemi daha görünür hale gelmiş ve pek çok sınırlandırıcı uygulama karşısında kamu yararı fikri güç kazanmıştır[105]. 1948 tarihli Birleşmiş Milletler İnsan Hakları Bildirgesi'nde de 12. madde ile mahremiyete keyfi şekilde müdahale edilemeyeceği vurgulanmıştır. Ayrıca mahremiyet talebi AİHS'de yer alan, "*herkesin özel ve aile hayatına, evine ve yazışmalarına saygı gösterme hakkına sahip olduğu"* hükmüyle görünür olmuştur.

Dijitalleşme konusunda yaşadığımız çağa damgasını vuran kadınlara ve çocuklara özgülenmiş düzenlemeler, kitle iletişim araçları olarak radyonun ve televizyonun yaygınlaşması, refah toplumlarının güçlenmesi, vatandaşların sosyal hizmetler, sosyal güvence gibi olanaklardan sahip olmak için devletlerle daha çok muhatap olmaları, kişilerin gözetiminin aile ve dahil oldukları sosyal grubu aşarak, bireylerin devletin sistematik gözetimine maruz kalmaları ve bunun için güvenlik hizmetlerinin daha geniş çaplı hale gelmesi gibi durumlar, mahremiyetin ve bunun korunmasının bir "hak" olarak öne sürülebilme koşullarını sağlamıştır.

---

[103] Ibid, s.139.
[104] "VINCENT, D. (2017) Mahremiyet Kısa Bir Tarih. (Deniz Cumhur Başaraner çev.) Ankara: Epos Yayınları". s.131-178.
[105] Ibid, s. 164.

1.4.2. Bilgisayarların Doğuşu Sonrası Dönem ya da Algoritmik Gözetimde Mahremiyet

Pek çok toplumsal ilişkinin dönüşümünde etkili olan ve dijital çağın araçları olarak bilgisayarların yükselişi, internetin doğuşu, World Wide Web'in yaygınlaşması hem kamusal alan hem de farklı dönemlerde farklı sebeplerle değişen mahremiyet algısını kökten dönüştürmüştür. Artık yalnızca devletlerin gözetim faaliyetinin bir parçası olarak bilgi toplama ve arşivleme faaliyeti, yeni teknolojilerle harmanlanınca mahremiyet ve gözetim olguları yeni tartışmalara yol açmıştır. Yeni tartışmaların erken dönem örneklerine örnek vermek gerekirse, 1969 yılında "The Death of Privacy" kitabında Jerry Rosenberg, bilgisayarlar tarafından kişilere ait verilere doğrudan doğruya ulaşılabildiğini iddia etmiştir.

ABD'de oluşturulan "Mahremiyet Komitesi Raporu'nun tarihi 1972'dir. Henüz o yıllarda resmi tartışmalarda, mahremiyetin olanaksızlığı ileri sürülmüş, artan gözetimin "akıllı" araçlarla gerçekleştirilmesine ve mahremiyetin korunması gerekliliğine dikkat çekilmiştir[106]. Ayrıca ekonomik gelişmeler bireylerin sahip olduğu itibarın daha önemli hale gelmesine sebep olduğundan, mahremiyet ve bireysel özgürlükler iç içe geçmiş, geleneksel toplum normları da dönüşerek yaşanan değişim gözle görülür hale gelmiştir[107]. Bu dönüşüme örnek olarak bilhassa Batılı ülkelerdeki evlilik algılamalarındaki değişim, yaşayış biçimlerindeki artan bireysellik verilebilir. Artık bireyler mahremiyetlerinin kullanımının kendi ellerinde şekil almasını arzulamaya başlamıştır.

Diğer yandan mahremiyetin mutlak bir hak olarak ileri sürülmesine karşı çeşitli seslerin de yükseldiğini vurgulamak gerekir. Özellikle 1900'lerin sonunda, AIDS salgını, eşcinsellerin hakları, kürtaj, ekonomik krizler ve benzeri gelişmeler, Hristiyan sağ fikirlerin mahremiyete karşı çıkışlarına temel olmuştur[108]. Yine de özellikle gelişmiş

---

[106] DWORKIN, G. (1973). The Younger Committee Report on Privacy. *The Modern Law Review*, *36*(4), s. 399.
[107] VINCENT,2017, s. 178-200.
[108] Ibid, s. 201.

ülkelerde, bireylere verilmiş mahremiyetin korunmasını talep etme hakkından geri adım atılmamış; hükümetler, insanların özel alanlarına müdahil olmaktan kaçınmışlardır[109].

Mahremiyet, genel gizlilik tartışmaları ve gözetim ile beraber 11 Eylül saldırılarından sonra teröre karşı yapılan hukuki düzenlemelerin de etkisiyle artan şekilde tartışma konusu olmuştur. Burada özellikle terörü önleme veya güvenlik sağlama gibi gerekçeler ile gözetim yapılabilmesi anlayışında yayılma, aynı zamanda da liberal değerlerin korunması çabaları devam ederek mahremiyet, özel hayat veya kişisel verilerin korunmasına yönelik hukuk normları üretilmeye devam edilmiştir. Yaygın gözetime ilişkin, devletlerin (özellikle ABD) hukuka aykırı faaliyetlerini ifşa eden(sızdıran) Wikileaks gibi oluşumlar ortaya çıkmış, bu oluşumların kamuoyu ile paylaştığı gizli bilgiler büyük yankı uyandırmıştır.

Wikileaks'ın kurucusu Julian Assange toplumlarca bir kurtarıcı veya özgürleştirici olarak görünen internetin totaliter amaçlar için işe yarar bir araca dönüştürüldüğünü ifade eder[110]. Ayrıca Assange'a göre; mahremiyet toplumlarda hâkim durumda olan kesimin manipülasyon aracı olan şeffaflığa zarar verdiği için fazla arzulanmaz-ki bu onu zayıf kesimler açısından daha gerekli kılar[111]. Bu anlayışa göre günümüzde toplumlar reklamcılık, devlet gözetimi gibi pek çok yöntem ile yoğun şekilde izlenir. Bu izlemeden elde edilen kazançlar karşısında kazanç elde etmeyen toplum kesimlerinin verileri, mahremiyeti birer araç haline geldiğinden daha çok korunmalıdır. Gözetim kapitalizmi literatüründe bu tartışmalar yoğun şekilde yer alır ve dayanaklandırılmaya çalışılır.

NSA skandalını ortaya çıkaran Edward Snowden, ABD'nin öncülük ettiği geniş çaplı gözetime vurgu yaparken, teknik bilgi sahibi olmayan sıradan insanların bütün hayatlarının her ayrıntısıyla izlendiğini ve "tekno-kapitalist" şirketlerin bu durumu bilerek sorumluluklarını azaltmak adına yeni kriptografik veri güvenliği yöntemleri arayışında olduğunu iddia etmiştir[112]. Dünya çapındaki yaygın gözetim ağını ortaya

---

[109] Ibid, s. 201.
[110] "ASSANGE, J. (2012). Cypherpunks New York and London: OR Books."
[111] Ibid, s. 97.
[112] "SNOWDEN, E. (2019) Permanent Record. London: Metropolitan Books".s. 314.

döken ifşalar, bir yandan devletlerin gözetim faaliyetlerini hangi biçimlerde gerçekleştirdiğini ortaya koyarken diğer yandan mahremiyetin korunmasında insanların bilinçlenmesinin ve hukuki düzenlemelerin güçlendirilmesinin önemini ortaya koymuştur. Burada oluşan pek çok soru işaretinden belki de en baskın olanı, devletlerin hukuka aykırı veya ölçüsüz olarak yaptığı gözetimden kaynaklı sorumluluklarının doğup doğmayacağıdır. Nitekim özellikle kamu yararı-kamu güvenliği gibi genel sebeplere dayanarak yapılan gözetimde, ölçülülük kuralının işlerliğinin sağlanması daha önemli hale gelecektir. Bu durum, hukuk normlarının doğru şekilde inşasının önemini bir kez daha vurgulamaktadır.

Çağımızda yapılan gizli gözetleme ve dinlemeler, dijital çağın bir sonucu da olarak bazı hukuki tartışmalar veya sorunlar doğurur[113]. Kimi zaman fiziksel kimi zamansa kimi manipülatif yöntemler ile bilgi teknolojileri kullanılarak yapılabilen gözetim faaliyetlerinin biçimleri Alan Westin tarafından merakı ve ifşa etmeyi de bünyesinde barındırır[114]. Günümüzdeki bireyin mahremiyet ve gözetim karşısındaki durumu; dijital dönemdeki toplumdan uzaklaşmayı ve liberal değerlerin de etkisiyle bireysellik iddialarını, diğer taraftan da sosyal medya gibi dönemin sahip olduğu belirli birtakım araçlar ile bir ölçüde gönüllü mahremiyet yitimini yansıtır. Konu hakkındaki bazı çalışmalarda, ekonomik durum, sosyal çevre, eğitim durumu gibi değişkenlere bağlı olarak bireylerin kendilerini ifşa etme durumundan bazı sosyal ve ekonomik çıkarlar elde ettiği fikirleri yer almaktadır[115]. Tüm bunlar, dijital çağdaki mahremiyet algılamasının toplumsal ve bireysel açıdan dönüşüm içinde olduğunu göstermektedir.

Mahremiyet ve gözetim arasındaki ilişkinin birbiri ile sınırlarını ortaya koymak, bu iki kavramı özellikle hukuk normları ile tesis ederken, doğru anlamlandırmak ve

---

Ayrıca Snowden'in ifşaatlarının ABD'nin kitlesel izleme politikaları ile ilişkilendirildiği bir çalışma olarak bkz. GELLMAN, B. (2020) "Dark Mirror: Edward Snowden and the American Survaillance State". Penguin Press: New York.

[113] YÜKSEL, 2014, s.185.

[114] WESTIN, A. (1967). "Privacy and Freedom". New York: Ig Publishing. s.28-10.

[115] AKGÜL, M. ve HEKİMOĞLU TOPRAK, H. "Sosyal Ağlarda Mahremiyetin Dönüşümü: Instagram Örneği". Online Academic Journal of Information Technology 2019 Yaz/Summer - Cilt/Vol: 10 - Sayı/Num: 38. s.105 vd.

Facebook özelindeki kullanıcı motivasyonlarına ilişkin bkz. KÖSEOĞLU, Özgür (2012). "Sosyal Ağ Sitesi Kullanıcılarının Motivasyonları: Facebook Üzerine Bir Araştırma", Selçuk İletişim Dergisi.

mahiyetlerini birbirlerine etkimeleri üzerinden yorumlamayı gerektirir. Myron Brenton mahremiyetin ölümünün ilan edildiği asırda henüz 1964 yılında yazdığı "Mahremiyet İstilacıları" (*The Privacy Invaders*) kitabında reklamcılıktan hayat sigortası denetimlerine, derinlemesine bilgi alan-kazuistik istihdam başvuru formlarından kurumsal casusluğa kadar piyasada, çalışma hayatında ve toplumda kısacası kamusal alanda artan müdahalelerin altını çizmiş ve bazı "meraklı" gözetleme mekanizmalarından bahsetmiştir[116].

Brenton gözetim ve mahremiyet arasındaki etkinin altını çizdiği ve çeşitli gözetim araçları ile mahremiyetin ihlal edildiğini savunduğu kitabında, bir kişinin hayatının, onun banka hesap özetlerinden, telefon faturalarından, kredi kartı makbuzlarından ve sair evrak kayıtlarından derlenebileceğini öne sürmüş, böylece mahremiyetin kişiler farkında varmaksızın nasıl "usulca" yok olduğunu anlatmıştır. Brenton'un 60'lı yıllarda gözetim çalışmalarının henüz başlangıcında küçük kameraların, gizli mikrofonların, dahiyane aynaların ve dijital dosyalama sistemlerinin mahremiyetin ihlali için nasıl birer silah haline gelebileceğini belirtmesi oldukça önemlidir.

Brenton ile birlikte Vance Packard'ın aynı yıl yayımlanan "Çıplak Toplum" (*The Naked Society*) adlı kitabından da söz etmek gerekir. Bu iki çalışma adeta birbirini tamamlayan mahiyettedir. Packard da artan gözetim tekniklerinden bahseder ve tıpkı Brenton gibi gözetimin günden güne yaygınlaşması ile mahremiyeti savunmanın veya sağlamanın zorlaştığını belirtir. Packard, Batı Dünyasında henüz o yıllarda başlayan ve yaygınlaşan gözetim tekniklerini, insan hakları savunuları karşısında oldukça yayılmacı, belirgin ve müdahaleci bulur[117]. O'na göre gözetime ilişkin uygulanan tekniklerin veya güçlerin bir etkisi, mahremiyete olan saygının altının oyulmasıdır[118]. Burada Packard tarafından iddia edilen devletler tarafından daha az müdahaleci yöntemler keşfetmek yerine, bireyleri sıralamak, saymak, denetlemek, kontrol etmek ve onlara "göz kulak olmak" için adeta "gönüllü – zorlayıcı" bir gözetim yapıldığıdır. Packard ayrıca mahremiyetin altını deşen beş unsuru şu şekilde belirtir; şehir yaşamında veya organize

---

[116] BRENTON, M. (1964) "The Privacy Invaders", New York: Coward-McCann, s. 163.
[117] PACKARD, V. 1964. "The Naked Society". New York. Ig Publishing.s.38.
[118] Ibid.

yaşamda artış, savaşan devlet zihniyetinin benimsenmesi, bolluğun yarattığı baskılar, özel sektör soruşturmalarının artması, elektronik gözler, kulaklar ve (kayıt altına alınan) anılar[119].

1.4.3. Mahremiyetin Hukuki Yansımaları ve Kişilik Hakkı Yaklaşımı

Mahremiyet olgusunun tanımlanmasındaki güçlük, onun ancak farklı ilişkiler bağlamında sorgulanmasıyla anlaşılabilmesine sebep olmaktadır. Bu bakımdan mahremiyeti yalnızca hukuk metinlerinde açıklamaya çalışmak, izah ve anlam yönlerinden eksiklikler yaratacaktır. Mahremiyet ve onunla bağlantılı şekilde veri gizliliğinin korunmasında iki farklı yaklaşımın ön planda olduğu söylenebilir. Avrupa ve ABD arasında, mahremiyete ilişkin farklılıkları ve benzerlikler, mahremiyetin ne olduğuna dair yapılacak bir açıklamayı besler. Bu başlıkta, gözetim ve mahremiyet ilişkisi ve bu iki kavramın birbirinin "aksi" olup olmadığı ve belirtilen sorulara cevap verebilecek sorgulamalar hususları ele alınmak istenmiştir.

Konuyla ilgili iki dava, mahremiyetin bir hak olup olmadığına ilişkin sorgulamalara cevap niteliği taşımasının önemini ifade eder. İlk örnek davada rıza ile yapılan ve bir kraliçe ile prense ait olan gravürlerin rıza olmadan sergilenmesi durumu söz konusudur[120]. Konu hakkında mahkeme tarafından, bireylerin mahremiyetlerinin kapsamı ifade edilmiş, mahremiyetin bireylere ait olan ifade biçimlerinin, inzivaya ilişkin duygularının yansıtılmasını da içerdiğine dair karar verilmiştir[121]. Samuel Warren ve Louis Brandeis ABD'de mahremiyet konusundaki tartışmaları ivmelendiren "Right to Privacy"[122] çalışmalarında, bu mahkeme kararının mahremiyetin ayrı bir hak olarak tanınmasındaki önemini vurgulamıştır[123]. Warren ve Brandais, medeniyet ilerledikçe yoğunlaşan yaşamın insanlar açısından bir inzivayı gerekli kıldığını, mahremiyetin bu

---

[119] Ibid.
[120] "Prince Albert v. Strange, High Court of Chancery. (1849) 1 Mac & G 25, [1849] EWHC Ch J20, 41 ER 1171, (1849) 18 LJ Ch 120."
[121]Prince Albert v. Strange, (Erişim Tarihi: 13.07.2022.) "https://www.casemine.com/judgement/uk/5a8ff8d260d03e7f57ecdced"
[122] WARREN, S. D. ve BRANDEIS L.D., (1890) "The Right to Privacy, Harward Law Review," 4.5, s.193–220.
[123] Ibid, s. 208.

karmaşık yaşamda bir ihtiyaç haline geldiğini, bu sebeple de mahremiyete yönelik saldırıların en az bedene yapılan saldırılar kadar can acıtıcı olduğunu belirtir.

Warren ve Brandeis'in mahremiyetin ihlaline dair istila ve saldırı tanımlamaları yaparken, mahremiyetin korunmasıyla ilgili günümüz düzenlemelerinin o yıllarda oluşturulmadığını vurgulamak gerekir. Yine de bu hukuki tartışma, mahremiyetin ihlali ve korunmasının kapsamını belirleyen bir başlangıç noktası ve rehber olarak nitelendirilebilir.

Mahremiyetin korunmasının kişilerin hangi alanlarını kapsadığını tespit edebilmek için kişilik hakkını tartışmak gerekir. Ancak bir kişilik hakkının varlığında bireylerin toplum hayatındaki konumları ve buna bağlı olarak sahip oldukları değerler, mahremiyet kapsamında korunabilir. Bireylerin sahip olduğu varsayılan kişilik hakkı sayesinde kişiler konum ve değerlerinin korunmasıyla kendilerini geliştirebilirler, bu nedenle de kişi olmalarından ötürü kişilik hakkının sağladığı korumadan istifade ederler. Bu koruma hem kendi manevi bütünlüklerini ve hem de dışarıya karşı mahremiyeti de kapsayan şekilde bir koruma sağlar. Kişilik hakkının içeriği, bireyi toplum içinde özne kılan ve onun korunması gereken değerlerinden oluşur, bu sebeple kişilik hakkının kapsamı her durumda yeniden değerlendirilmelidir ve geniş yorumlanmalıdır.

Kişilik hakkı kapsamında yer alan hayat alanları; kamuya açık, özel hayatın geçtiği alanlar ve gizli alanlar şeklinde üç kısımda ele alınır[124]. Kamuya açık alanda mahremiyetin kural olarak korunmadığı belirtilebilse de sürekli ve sistemli bir izlemenin bunun istisnası olacağı ifade edilmelidir. Zira bireylerin görüntüleri veya onları diğer insanlardan ayırmaya yarayan dış görünümleri kişilik hakkı çerçevesinde korunmaktadır. Yani kameralarca elde edilen hareketli veya hareketsiz görüntüler aynı zamanda kişisel değer ile ilişkilendirilen kişilik hakkı yaklaşımı kapsamında olacaktır. Alanlara ilişkin Edward Hall'un "proksemikler" sınıflandırmasına göre çemberin en dışındaki alan sosyal alan olup en az seviyede mahremiyet iddiası içerirken, çember daraldıkça ihtiyaç duyulan

[124] Ibid, s.55.

mahremiyet artacaktır[125]. Bu husus mahremiyeti anlamak bakımından önemlidir. Çünkü bu en dar gizlilik alanı, aynı zamanda bireyin toplumsallaşması sürecindeki en öznel alandır. Bireyin öznelliğine en yakın bu alan salt ortada kişi olduğu için korunmalıdır.

Anayasa Mahkemesi bir bireysel başvuruya ilişkin vermiş olduğu kararında;

> *"(...) Bireyin mahremiyet hakkının mekânı, kural olarak özel alandır. Ancak özel yaşamın korunması hakkı bazı durumlarda kamusal alana da genişleyebilir. Zira meşru beklenti kavramı, bireylerin mahremiyetlerinin kamusal alanda da bazı koşullar altında korunmasını mümkün kılmaktadır. (...) Kamusal makamların bir hakkın sınırlandırılması sürecinde iki ayrı aşamada takdir yetkisi bulunmaktadır. Bunlardan ilki, sınırlama ölçütünün seçimidir. İkincisi ise, ilgili sınırlama ölçütü çerçevesinde izlenen meşru amacı gerçekleştirmek üzere yapılan sınırlamanın gerekliliğidir… Kullanılan argümanların elverişli, zorunlu ve orantılı olması gerekir. (...) Mahremiyet hakkı öncelikle mekânsal bir alana tekabül etmekte olup, bu alan da bireyin konutu ve müştemilatıdır. Bu mekân dışında bireyi etkileyen önlemlerin, özel hayatın gizliliği hakkı kapsamında ele alınıp alınmayacağının, birtakım ölçütler ışığında değerlendirilmesi gerekir. (...) özel yaşamın gizliliği hakkı kapsamındaki mahremiyet hakkının uygulanabilirlik alanı kural olarak özel yaşam alanı olmakla birlikte, bireylerin diğer insanlarla etkileşim içinde oldukları bazı kamusal alanlar ya da bağlamlar da özel yaşamın korunması hakkının kapsamında yer alabilirler. Bunun yanı sıra, özel yaşamın gizliliği hakkı bireye, içinde özgürce hareket edebileceği ve kişiliğini geliştirip gerçekleştirebileceği bir kişisel alan sağlamaktadır. (...)"*

hususlarını belirtmiştir[126]. Böylece Anayasa Mahkemesi tarafından mahremiyet ve özel hayata ilişkin yapılan yorumda alanlar teorisinin de kullanıldığı görülebilir. Anayasa'nın 20. maddesindeki özel hayatın korunmasına dair hüküm, mahremiyetin korunmasına ilişkin hukuki çıkarı da kapsamaktadır. Ancak mahremiyet yalnızca "yalnız bırakılma" hakkı anlamına gelmez, bireylerin "kendileri hakkındaki bilgileri kontrol edebilme" haklarını da ilgilendirir. Diğer taraftan mahremiyet iddiası, bazı durumlarla sınırlı ölçekte de olsa özel alanların yanında kamusal alanda da söz konusu olabilmektedir.

---

[125] HALL, E. T. vd. (1968) "Proxemics (and Comments and Replies) Current Anthropology" . 9:2/3, s. 83-108.

[126] 2013/1614 sayılı ve 03.04.2014 tarihli karar.

Anayasa Mahkemesi mahremiyeti, özel alanda tanımlarken, bu alan, devletin müdahalesinden uzakta, meşru amaçlarla ise yalnızca asgari biçimde müdahale edebileceği bir alandır. Bu özel alanda mahremiyetin korunması hakkı kamusal alana da dahil olabilir, kişilerin açık alanlardayken fotoğraflanmamaları konusunda meşru bir beklenti içinde olmaları buna örnek olarak verilebilir[127]. Dolayısıyla burada kamusal alanda korunmaya değer bir özel alan, mahremiyet hakkı olmayacağına dair görüşler dışlanmış olmaktadır.

1.4.4. Mahremiyetin Geniş Kapsamı ve Mahremiyet 2.0

Mahremiyet kavramının kapsamına ilişkin doktrinde farklı yaklaşımlar vardır. Bu yaklaşımlarda kullanılan terminolojideki farklılaşmayı da ortaya koymak gerekir. Elif Küzeci bu farklılaşmayı açıklarken, mahremiyetin Anglo-Amerikan hukuk sistemlerinde "özel hayatın gizliliği" teriminin, "kişisel verilerin korunması"na tercih edilmesini örnek gösterir[128]. Kanımca, kişisel verilerin korunması ifadesi mahremiyetin kapsamını karşılamaz, kişilik hakkının bir uzantısı olarak ele alınsa da mahremiyet bundan çok daha fazlasıdır.

Türk Dil Kurumu'na göre mahremiyet "gizlilik" anlamına gelir. Sözcük arapça kökenli olmakla birlikte, sözcüğün etimolojik kökeninde özel alana aitlik belirten ifadeler karşımıza çıkar[129]. Belirtilmelidir ki çalışmada mahremiyet kelimesine ingilizce privacy kelimesine karşılık olarak yer verilmiştir. Mahremiyet yalnızca kişisel verilerin korunduğu alan değil bu alanın ötesinde hem özel hayatın gizliliğini ifade eden hem de çeşitli açılardan gizliliğin elde edilmesini içeren pek çok uzantıya sahiptir. Bu sebeple de mahremiyete dair açık bir konsept benimsemek zordur.

---

[127] Kişilik hakkının yansıması olarak kişinin görüntüsü üzerindeki hakları için bkz. PARLAK BÖRÜ, Ş. (2013) Fotoğraf Üzerindeki Haklar (doktora tezi). Yök Tez Merkezi. (330323)
[128] KÜZECİ, E. (2021), "Kişisel Verilerin Korunması, On İki Levha Yayıncılık, 4. Baskı, İstanbul", s.15.
[129] Türk Dil Kurumu Sözlükleri.

Solove'ye göre mahremiyet kişilere ait fikirler, eylemler ve duyguları içeren, onları toplum veya devlet gibi dış etkenlerden koruyan bir garantiyi içerir[130]. Burada hem bireysel hem de toplumsal bazı çıkarlar devreye girdiği için de bu çıkarların dengelenmesi, hukuk düzeni tarafından korunan mahremiyet için gereklidir[131]. Zira toplumun ve bireyin çıkarları her zaman örtüşmez. Bu noktada kişiliğin uzantısı kabul edilen mahremiyet kimi zaman toplumsal faydaların sağlanması için feda edilebilir. Bunu gözetim açısından ele aldığımızda ise özellikle kamu yararı veya güvenlik gerekçeleriyle yapılan CCTV izlemelerinin, bireylerin mahremiyetlerinin korunmasını isteme hakkı ile çatıştığı değerlendirmesi yapılabilir. Fakat bu teorik saptamaya rağmen video gözetime ilişkin olay bazında yapılabilecek değerlendirmeler ve hukuk kuralları ile bu çatışma temel hakları koruma temelli bir yaklaşımla dengeye oturtulabilir.

Solove bir hak olarak mahremiyete bireyci değil toplumcu bir yaklaşım ile bakar ve toplumun mahremiyetin korunmasından fayda elde edemeyeceği ya da zarar göreceği noktada bu hakkın da artık savunulamayacağını düşünür[132]. Bu fikre göre; bireyin mahremiyet savunusu esasen topluma karşı gizlilik olmasına rağmen, bu gizlilikten toplumun da çıkarları tatmin edilmeksizin bireysel fayda elde edilebilmesi çok gerçekçi olmayacaktır. Solove mahremiyeti yalnız kalabilme, dış dünyanın erişiminden korunma, gizlilik elde etme, kişisel verilerini kontrol edebilme, bireyselliğini muhafaza edebilme ve yakın münasebetlerini kontrol edebilme istekleri ile ilişkilendirir[133]. Görüldüğü üzere kavramın ilişki içinde olduğu çok fazla boyut bulunur.

Mahkeme kararlarında mahremiyet özel yaşamın gizliliğinin bir unsuru olarak ele alınsa da bunun kamusal alanı ilgilendiren yönleri de olduğu kabul edilmektedir. Bu bakımdan mahremiyetin ele alınması konusunda, aslında özel yaşama dair gizliliğin korunmasının kamusal alana genişletilerek yorumlanması ama bu yorumun "bireyin verilerinin geleceği hakkında söz sahibi olma hakkı"na kadar genişlemediği söylenebilir.

---

[130] "SOLOVE, D. J. (2011). Nothing to Hide : the False Tradeoff Between Privacy and Security. Yale University Press".s.49.
[131] Ibid.
[132] Ibid.
[133] SOLOVE, D. J. (2002) "Conceptualizing Privacy.California Law Review", 90(4), s.1099-1121.

Ferdinand David Schoeman buna karşı durarak, mahremiyetin daha dar yorumlanması, kişisel verilerin geleceği üzerinde tasarruf hakkından ayrı olarak değerlendirilmesi gerektiğini iddia eder[134]. Mahremiyet bütün veriler üzerinde söz sahibi olmayla eş anlamlı kullanılırsa, bu aynı zamanda kişinin de gizli tutulması gerektiği varsayımını kabul etmek anlamına gelir[135]. Yalnızca kişinin kendisine ait bilgileri yönetebilmesi gibi bir anlama gelen ifade ise; bireyi yanlış bir şekilde (toplumsallıktan ayırarak) bütünüyle mahremiyet içinde yaşayan bir varlığa indirgemesi, kendisine ait bilgiler üzerinde başka bir etken olmaksızın yönetim gücünü haiz olması sebepleri ile yeterli olmayacaktır[136]. Adam D. Moore ise bir hak olarak mahremiyeti kişisel veriler üzerinde söz sahibi olma şeklinde yorumlayarak bu haliyle hakkın sağlanmasının bireysel ve toplumsal gelişmeye de hizmet edeceğini vurgular[137].

Mahremiyetin korunması konusunda hukukun dönüşümünün en önemli sebepleri, yapay zekâ kullanan yazılımlar gibi yeni teknolojik gelişmeler ile daha önce karşılaşılmayan veri ihlalleri gibi teknik bazı durumların yarattığı bilinmezliktir. Bu sebeple özellikle veri koruma otoriteleri bakımından her gün yeni teknik tedbirler oluşturulmakta, bulut bilişim, online eğitim, elektronik ticaret gibi pek çok sahada yeni düzenlemeler ortaya çıkmaktadır. Bunlar dışında unutulma hakkı gibi yeni şekillenen ve dijitalizasyon ile hayatımıza giren kavramlar hukuk düzenleri tarafından tanınmaya başlanmış, teknolojik ve teknik gelişmelerin kişilerin özel hayatlarını olumsuz etkilemesinin önüne geçilmeye çalışılmıştır. Bu sebeple siber alandaki tehlikeler hem farklı türden mahremiyet yorumlamalarını hem de hukukun dönüşümünü gerekli kılmıştır.

Teknolojik ilerlemeler ile kişilerin çok daha kolay ve yaygın şekilde gözetime tabi tutulduğu iddiası[138] mahremiyetin aşınması sürecinin en önemli unsuru olmuştur. Bu

---

[134] SCHOEMAN, F. D. (1992). "Privacy and Social Freedom. Cambridge University Press".s.3.
[135] Ibid.
[136] Ibid.
[137] DE CEW, Spring 2018, s.6.vd. ve MOORE, A.D. (2016) "Privacy, Security and Accountability: Ethics, Law and Policy". Rowman & Littlefield International: London&New York. s.5.
[138] "KILINÇ ÖZÜÖLMEZ, P. (2019) Michel Foucault'nun İktidar ve Özne Kavramsallaştırmasına Gözetim Sorunu Üzerinden Bakmak: Black Mirror – Arkangel, Selçuk Üniversitesi İletişim Fakültesi Akademi Dergisi, 12(2)", s.647.

şekilde kişilerin yapay zekâ ile donatılan akıllı cihazlar karşısında bir özel hayatlarının var olması oldukça güç hale gelmiş, diğer yandan gelişen teknikler karşısında veri ihlalleri riskleri artarken Sandbox[139] gibi bu risklerden korunmayı sağlayan yeni yöntemler geliştirilmeye başlanmıştır.

Teknolojik gelişmeler karşısında dijital ortamlarda yaşanan değişmelerin ve yeniliklerin yanında, birer özne olarak doğrudan bireylerin de dönüşümü yaşanmıştır. Foucault açısından bireyler toplum tarafından örülen veya biçim verilen konumda yer alırlar[140]. Bu biçim verme sürecinde, inşa edilmiş hale gelen toplumu ve ayrı ayrı bireyleri kontrol altında tutma ihtiyacı duyan bir gözetimci devlet de bulunur[141]. Foucault açısından tıpkı birer hapishane gibi sınırları belirlenmiş ülkelerdeki iktidarlar tek taraflı şekilde kişileri çeşitli açılardan sürekli gözetime tabi tutar[142].

Günümüzde bunun ötesine geçilerek, aşınan mahremiyet içinde istekleri başkalaşan bireyin, omniptikon gözetimde herkesin herkesi izlediği bir alanda sıkıştığı gözlemlenmektedir. Dolayısıyla modernleşmenin etkilediği gelişmeler ile gözetim daha yaygın hale gelmiş, bazı yapısal değişikliklere uğramıştır[143]. Böylece bireylere dair temel bir tartışma ortaya çıkmış olur. Bu dönüşüm sürecinde hem dijitalleşmenin içinde kalmayı arzulama ve belirli bir mahremiyet fedakarlığı hem de bireyselliği ve mahremiyeti elde tutma istenci bireyleri kaotik bir kimlik dönüşümüne sürükler[144]. Öznenin dijital ortamda bedenden kurtulduğu bu başkalaşımı, mahremiyetin dışında kamusal alan, demokrasi gibi çok farklı kavramlara iç içe geçip bunlar ile birlikte yeniden yorumlanır[145].

---

[139] Dijital ortamda kullanılan programlar ile kullanıcı arasında güvenlik sağlayan bir mekanizma.
[140] KILINÇ ÖZÜÖLMEZ, 2019, s.645.
[141] Ibid.
[142] Ibid.
[143] "BİTİRİM OKMEYDAN, S. (2017) Postmodern Kültürde Gözetim Toplumunun Dönüşümü: Panoptikon Dan Sinoptikon ve Omniptikon'a, AJIT-e: Online Academic Journal of Information Technology." s.45.
[144] Ibid.
KARAGÜLLE, A. E. (2015) "Günümüzde Değişen Mahremiyet Algısının Sosyal Ağlar Bağlamında İncelenmesi İlişkisi" (yayınlanmamış yüksek lisans tezi). İstanbul Ticaret Üniversitesi, İstanbul. s.iii.
[145] "DOLGUN, U. (2004), "Gözetim Toplumunun Yükselişi: Enformasyon Toplumundan Gözetim Toplumuna", Yönetim Bilimleri Dergisi, 1(3)," s.62.

Eğer mahremiyetin varlığı teknolojiye bağlı bir halde yorumlanırsa, teknoloji tarafından kuşatılan bireysel alandan bahsedilebilir[146]. Nitekim Foucault'nun da bahsettiği gibi, bu düşünceye göre bireyi dört bir yandan kuşatan kameralar, onu şehre hapsetmeyi amaçlar[147]. Ancak burada çeşitli sorular konuyu bu düşüncenin ötesine taşır. Öznenin dönüşen mahremiyet algılamaları karşısındaki bedensizleşmesi, mahremiyetin aşınmanın ötesinde bütünüyle ortadan kalktığını gösterir mi? Kameralar ile izlenen şehirlerde özel alanlar dışındaki toplumsal hayatta özel hayat bütünüyle yok mu olmuştur?

Kanımca mahremiyet kavramına dair yapılan tartışmalar karşısında, kavramın herhangi bir yönde ele alınması veya sınır belirlenmesi gerekliliği yoktur. Zira kavramın kendisinin hukuk kurallarıyla tanınması da özel hayatın gizliliği veya kişisel verilerin korunmasını isteme hakkı şeklindedir. Halbuki hem bu kavramları hem de bunlar dışındaki pek çok unsuru bünyesinde barındıran mahremiyet, her gün dönüşen bir kavrayış olarak çeşitli kalıplar içinde inşa olur. Günümüzde kişiler mahrem alanlarına ulaşan CCTV'ler sebebiyle damgalanabilmekte, dijital gözetim ile özellikle hükümetlerce mahremiyet neredeyse tamamen yok olma riski ile karşı karşıya kalabilmektedir[148]. Bu durumda klasik bir tanıma sığdırılmaya çalışılan mahremiyetten bahsetmek zor olacağından, sınırları daha muğlak, gözetime göre boyut veya anlam değiştiren "mahremiyet 2.0" yeni bir mefhum olarak tartışılabilir.

Mahremiyet mekânsal değil de bilginin aldığı biçime veya bilgiyi elde tutma erkine göre de kavranabilir[149]. Ancak böyle bir yorum ile mahremiyetin sadece kişinin kendisine ait bilgilere yani kişisel verilere etki edebilme yönü kabul edilmiş, diğer hususlar dışlanmış olur. Halbuki kavram bilhassa tüm boyutları ile geniş şekilde ele alınması sebebiyle bir hak olarak doğmamış mıdır? Mahremiyetin kavram olarak idraki, onu koruyan kuralların da işlevine ilişkin bir kavrayışa sebep olabilir. Hem kişisel verilerin

---

[146] GÜVEN, O. Ö. (2014) "Gözetim Tekniklerinin Güç İlişkileri Bağlamında Dönüşümü ve Toplumsal Denetimi", Atatürk İletişim Dergisi, 7, s.107.
[147] Ibid.
[148] The Wall Street Journal, NSA Officers Spy on Love Interests, (Erişim Tarihi: 03.07.2022). https://www.wsj.com/articles/BL-WB-40005 ve Toronto Sun,
[149] "SCHÜNEMANN, W. J.; BAUMAN, M. O. (2017) Privacy, Data Protection and Cybersecurity in Europe. Switzerland: Springer International Publishing". s.2.

korunması hem de özel hayat şemsiyesinde yer alan mahremiyetin korunması kişinin bizzat kendisinin korunmasıdır. Zira sosyal hayata katılım, kendini ifade etme biçimi, diğer kişilerle olan-veya olmayan gizli alanlar mahremiyete dahildir. Bu şekilde toplumsal faydalar, çıktılar veya gereklilikler de gözetilerek ancak hukuk kuralları ile ölçülü şekilde sınırlandırılan mahremiyet (dolayısıyla özel hayat ve kişisel veriler) hukuk dışı gözetim karşısında korunmuş olacaktır.

2. BÖLÜM

DEVLETİN KAMUSAL ALANDAKİ KAMERALI GÖZETİMİ

Çalışmanın ilk bölümünde genel olarak gözetim olgusu ve olgunun ilişki içinde olduğu kavramlar, disiplinler ve gözetimin meydana getirdiği bazı tartışmalar ifade edildikten sonra, ikinci bölümde bu genel gözetim literatürü basamağının üstüne basarak video gözetimin doğuşu, video gözetim sistemlerinin neler olduğu incelenmiştir. Akabinde devletlerin video gözetimi -kural olarak- kamusal alanlarda gündeme geleceğinden, mekânsal olarak kamusal veya halka açık alanlarda yapılan video gözetim ele alınmış, çalışma konusunun çerçevesi itibarıyla iş yerleri, özel mülkler gibi "özel alanlar" kapsam dışı bırakılmıştır. Bu sebeple kamusal alanların çerçevesi çizilerek, video gözetimin bu alanları ne şekilde dönüştürdüğü ve nasıl etkilediği belirtilmiştir. Ayrıca video gözetimin kamu otoritelerince ağırlıklı olarak hangi gerekçelerle yapıldığı ele alınarak, kamusal alandaki kameralı gözetimin ağırlıklı olarak hangi hususlara yönelik eleştirildiğinin altı çizilmiştir. Devletlerce yapılan gözetiminin maksadını ve muhtemel sonuçlarını kavramak, bir araç olarak kamera kullanıldığında ortaya çıkabilecek potansiyel riskleri anlamlandırmak bakımından oldukça önemlidir.

Çalışmanın bu bölümü ile amaçlanan, gözetimin genel mahiyetinin ele alındığı ilk bölüm ile video gözetime dair hukuk kuralları arasındaki bağlantıyı oluşturabilmektir. Nihayet çalışmada iddia edilen kişisel verilerin korunması hukukunun kamusal alanlardaki gözetim karşısında kişisel verilerin veya mahremiyetin korunması yönünden tek başına yeterli olmayabileceğidir. Savın ortaya konulması bakımından bu bölümde, kamu gücü kullanılarak kurulan sistemlerin hangi maksatlarla kurulduğunun, hangi hukuk kurallarına nasıl dayanıldığının ve uygulamaların doğurduğu endişelerin ele alınması önemlidir. Zira doktrindeki video gözetim tartışmalarının ağırlıklı olarak eleştiriler üzerinden yürütüldüğü gözlemlenmektedir.

2.1. VİDEO GÖZETİM VE CCTV'NİN YÜKSELİŞİ

2.1.1. Video Gözetimin Genel Kapsamı

Yapılan bir çalışmaya göre; 2021 yılında dünya çapında bir milyardan fazla CCTV bulunmaktadır[150]. Video gözetim sistemlerinin, her geçen gün kamusal güvenlik ve halka açık alanlarda kontrolün sağlanması amaçlarıyla devletler ve bireyler tarafından daha çok tercih edildiği göze çarpmaktadır. Parklar, caddeler, meydanlar, havaalanları, alışveriş merkezleri gibi pek çok halka açık yer, aralarında kimi teknik farklılıklar olabilmekle birlikte çeşitli video kayıt sistemleri aracılığıyla takip edilmektedir.

Bu sistemler esasen, elde edilen görüntülerin yönetilmesi ve kullanılması işine hizmet etmek için kullanılan bir dizi teknik araçtan oluşur veya gözetime aracı kılınır. Gelişen teknoloji elbette CCTV cihazlarına da yön vermekte, yapay zekâ kullanan kamera sistemleri, biyometrik veri elde edebilen kameralar gibi cihazlar kullanılabilmektedir. Ancak daha önemli olan husus yalnızca bu cihazların kullanımı değil, cihazlar ile elde edilen kişisel verilerin, özel hayatın gizliliğinin veya mahremiyetin korunmasıdır. Bununla birlikte video gözetimin, sosyal normların farklı şekilde nitelendirilmesine ve değişmesine yol açan toplu bir "yeniden tanımlama" veya biçim verme anlamında, çeşitli sapma biçimlerinin inşasına da katkıda bulunduğu ifade edilmektedir[151].

Video gözetim hem kullanıldığı halka açık alanların bizatihi kendisini dönüştürmüş, hem gözetim ile elde edilen kişisel verilerin ve özel hayatın korunması ihtiyacını ortaya çıkarmış hem de bu genel sebeplerle devletlerin video gözetim uygulamaları için kendilerini sınırlayıcı bazı hukuk normları üretmelerine sebep olmuştur. Böylelikle video gözetim yöntemi, gerekli koruma ve denetim mekanizmalarının bulunmaması halinde ayrımcı grupların ve davranışların

---

[150] TURTIAINEN, 2020,s.1.
[151] BÉTIN vd., 2003,s.22.

tanımlanmasına yol açabileceği için ölçülü uygulanması konusunda hassasiyetle üzerinde durulması gereken bir tercih haline gelmiştir[152].

Gözetim teknolojilerinin günümüzde geldiği aşama ve nihayetinde ulaşım, toplumsal alanlar, haberleşme gibi faaliyetlerin nasıl bir kameralı izlemeye tabii olduğu konusu, mahremiyetin korunmasına dair bazı soru, kaygı ve aynı zamanda çeşitli ihtiyaçları ortaya çıkartmıştır. Bugün pek çok ülkede bireylere hukuk dışı izlemeler karşısında özel hayatın ve bireyselliğin korunması hakkı tanıyan hukuki düzenlemeler olmakla birlikte, mahremiyet savunuları karşısında toplumsallaşmanın bir gereği olan güvenlik ihtiyacı ile yapılan izlemenin mahremiyeti koruyan haklarla bir örtüşme içinde uygulanması gerekir. Bu sebeple çalışmanın bu bölümünde, video gözetimin veya CCTV'nin kullanımının nasıl başladığına dair tarihsel bir perspektif oluşturulmaya çalışılarak "fotografik" gözetim sistemlerinin bugün geldiği yeri anlamlandırmak amaçlanmıştır.

2.1.2. Tarihsel Perspektiften Video Gözetim

Video kaydı elde eden kameraların kullanımı, esasen fotoğrafın suç kontrolü amacıyla kullanılması ile ilişkilendirilebilir[153]. Burada henüz 1850'lerde Amerika'da gözaltına alınan mahkumların fotoğraflarının çekilmesi ve bu uygulamanın önce ulusal ölçekte sonrasında daha geniş çapta yayılması, fotoğrafın suç işlenmesinin önüne geçmek için kullanılması karşımıza çıkar[154]. Fotoğrafı olan suçluların, hapishaneden kaçmaya çalışmasında, mükerrer suç işlenmesinde veya genel olarak suç işlenmesinin önlenmesinde devletin fotoğraf teknolojisi ile suç arasında bir tür kontrol ilişkisi kurmaya başlaması durumları göze çarpmaktadır. Teknoloji ile olan bu ilişki bazı tarihsel gelişmeler ile birlikte daha geniş bir çerçeveye kavuşmuş, ekonomi politik, tarihsel, sosyolojik ve nihayetinde hukuki dönüşümler ile günümüzdeki halini almıştır.

---

[152] Ibid.
[153] NORRIS ve ARMSTRONG,1999, s.13.
[154] Ibid.

Birbirini etkileyen gelişmeleri başlatan olay, 1960'larda video kaset kaydedicinin (*VCR-videocassette recorder*) ortaya çıkması olmuştur. Böylece bir kameradan alınan görüntüler kimyasal bir işlemeye gerek kalmadan filme alınabilmiştir. Bu sayede daha ucuz ve basit bir kayıt yöntemi oluşmuş ayrıca görüntüler tek bir kişi tarafından uzaktan izlenebilir hale gelmiştir. Üstelik görünen/kaydedilen her şeyin kalıcı bir şekilde saklanabildiği merkezi kontrol odalarına bağlı kameraların yolu açılmıştır[155]. VCR gelişmesi panoptik tartışmaların güçlenmesine de katkıda bulunmuştur.

İnsanın görme yeteneğinin ötesine geçen video kayıtları, daha o yıllarda bile rekabet edilemez bir aşamadadır. 1960'larda suç işlenmesi konusunda bir caydırıcılık yaratmak, hırsızları korkutmak ve yakalamak için geliştirilen CCTV'nin kullanımı, 1970'li yıllarda hız kazanmıştır. ABD polis kuvvetlerince caddelerde 24 saat gözetim yapan kameraların henüz o yıllarda bile pek çok yerde kurulduğu ifade edilmektedir[156]. Video gözetim sistemleri, 1980'lerde teknolojideki gelişmeler ile yakaladığı ivmelenme neticesinde, özellikle 1990'lar ve sonrasında deyim yerindeyse bir patlama yaşamış ve idarenin bu sistemleri kullanımı da oldukça artmıştır.

Christopher Dandeker'e göre, CCTV'nin yükselişi modernitenin yükselişiyle içsel ve direkt olarak bağlantı içindedir[157]. Öyle ki geç modernitede bir dizi yeni teknolojiden yararlanarak, yaşamın neredeyse tüm alanlarında gözetimin yoğunlaşması görülmüş, kameralar ile elde edilen görüntülerden oluşan dosyaları kapsayan veri tabanları oluşturmak "suçu önlemek" amacıyla devletler için bir rutin haline gelmiştir[158]. Diğer taraftan; sanayileşme, toprak reformu, nüfus artışı ve buna bağlı olarak şehirlerin büyümesi, şehirlerin güvenliğinin sağlanması konusunda artan bir güvenlik ihtiyacı doğurmuştur.

---

[155] NORRIS ve ARMSTRONG,1999, s.13.
[156] ÇAPAR, S. (2011) "Birleşik Krallıkta CCTV, Türkiye'de Mobese Caddelerde Güvenlik Nöbetindeki Kameralar". Ankara: Turhan Kitabevi Yayınları.s.13.
[157] DANDEKER, C. (1990) "Surveillance, Power and Modernity: Bureaucracy and Discipline From 1700 to the Present Day". Polity Press: Cambridge.s.15.vd.
[158] Ibid.

Özellikle Nicholas R. Fyfe ve Jon Bannister tarafından ele alınan bu bağlam; mülkiyet ilişkileri, sermaye dolaşımı, bürokratikleşme, çağdaş kapitalizmde mekânın üretimi ve sair unsurlar ile birlikte değerlendirilir[159]. CCTV'nin yükselişinde; göç gibi tarihsel olaylar ve sanayileşme ile değişen toplumsal katmanların sebep olduğu farklılaşma veya farklılık korkusu, kapitalizm ile başkalaşan kentlerin kontrolü ihtiyacı, "tehlikeler barındıran" kamusal alanın denetlenmesi gibi olguların ilerleyen yıllarda daha da etkili olduğu göze çarpmaktadır. Bu tartışmalara, çalışmanın ilerleyen bölümlerinde kamusal alan ve kamusal alanın dönüşümü konuları içinde yer verilmiştir.

Bir görüşe göre; dikkate değer gözetleme cihazlarının çoğunun geliştirilmesindeki itici güç, savunma ve uzay araştırmalarından ve bu alanda Ruslara ayak uydurma çabalarından kaynaklanmıştır[160]. Soğuk savaşın etkisi ile kızılötesi fotoğrafçılıktaki ilerlemelerin büyük ölçüde, kameralar için otomatik tetikleme cihazlarının yaptığı gibi havadan keşif araştırmalarından kaynaklandığı ve CCTV'deki birçok erken gelişmenin füze fırlatma komplekslerindeki insanların yanı sıra makinelerin ve kadranların gözetiminde kullanılmak için meydana geldiği ifade edilmektedir[161]. Öte yandan soğuk savaşın akıllı izleme, otomatik navigasyon ve tanıma sistemleri, termal görüntüleme sistemleri ve entegre veri tabanı yönetimi gibi orijinal olarak ordu için geliştirilen uygulamaların, CCTV ile birlikte kullanılmak üzere sivil piyasada hedeflenmesini sağladığı belirtilmektedir[162].

Soğuk savaş sonrasındaki siyasi iklim, CCTV'nin devletlerce suça karşı siyasi tepki ve kontrol bağlamında yaklaşılması, kent çevrelerindeki alışveriş merkezlerinin artması ile CCTV'ler aracılığıyla "güvenli tüketim alanları" oluşturma ihtiyacı, ana caddelerden uzaklaşan kalabalıkların merkezler dışında da gözetlenmesi yani gözetimin yayılması CCTV'nin "iyi ve güvende hissetme" faktörünü teşvik edeceği ve iş finansmanını çekmek için satış sahasını sağlayan ana caddeyi ve şehir merkezini canlandıracağı argümanlarının ortaya çıkması gibi gelişmelerin video gözetim sistemlerinin kullanımının artması

---

[159] FYFE, N.R.(Ed.) (2006) "Images of the street: Planning, identity and control in public space". London and New York: Routledge. s.248-261. https://doi.org/10.4324/9780203026496
[160] PACKARD,1964.s.48.
[161] Ibid.
[162] NORRIS ve ARMSTRONG,1999, s.28-29.

üzerindeki etkisi dikkatlerden kaçırılmamalıdır[163]. Bunlarla birlikte, soğuk savaş sonrasında iki kutuplu sistemden çıkılmasının devletlerin kendi güvenliklerini içte ve dışta sağlama ihtiyacının artması sebebiyle, politik gelişmelerin CCTV'ler üzerindeki etkisi de azımsanmamalıdır.

CCTV'lerin devletler tarafından kullanımı ile "suç işlenmesini önleme", "sosyal kontrol veya düzen sağlama", "güvenlik birimlerinin hareket kabiliyetini artırma ve kolaylaştırma" maksatları arasında doğrudan bir bağlantı bulunduğu görülmektedir. İfade edildiği üzere bu bağlantı aynı zamanda diğer sosyal, ekonomik, politik ve sair teknolojik unsurlardan beslenmektedir. Bu sebeple CCTV'lerin yükselişinin, genel olarak gözetim çalışmalarının tamamına hâkim olan bir interdisipliner hukuki perspektiften yorumlanması gerekir. Dünya savaşları sonrasındaki göç, ekonomik bunalımlar, toplumsal dönüşümler gibi tarihsel gelişmelerin etkisi ile İngiltere gibi sanayileşmiş ülkelerin çoğunda suç oranlarında patlama yaşanmasının devletleri kamusal alanda suç işlenmesinin önüne geçilmesine ittiği belirtilmektedir[164].

Bazı görüşlere göre her ne kadar CCTV'lerin yoğun kullanımı 1980'ler ve sonrasına dayandırılsa da video kayıt sistemlerinin yalnızca ve tamamen suçu ve suçluyu takip için bu kadar yoğun kullanıldığı savına dayanmak doğru olmayacaktır. Zira İngiliz polisi tarafından kamuya açık CCTV sistemlerinin kullanımının çok daha öncesine uzanan bir geçmişi vardır[165]. Henüz 1930'larda Birinci Dünya Savaşı'nda yapılan uygulamalarla başlayan bir merkezileşme ve makineleşme, 1960'larda yüksek kablolama maliyetleri nedeniyle başarılı olamasa da CCTV'lerin ilk kalıcı kullanımı, Londra'nın merkezindeki siyasi gösterilerin gözetimi için yapılmıştır[166]. Bu yaklaşıma göre CCTV, bir gözetim gücüne sahip olma arzusuna uyarlanan, suçu kontrol etmede araçsal etkisi

---

[163] Ibid, s.38-39.
[164] ÇAPAR, S. (2011) "Birleşik Krallıkta CCTV, Türkiye'de Mobese Caddelerde Güvenlik Nöbetindeki Kameralar". Ankara: Turhan Kitabevi Yayınları.s.13-14.
[165] WILLIAMS, C. A. (2003). "Police surveillance and the emergence of CCTV in the 1960s. Crime Prevention and Community Safety", 5(3), 27–37. s.27.
[166] Ibid.

sanıldığı kadar büyük olmasa da sembolik olarak genel bir caydırıcı etki nedeniyle benimsenen bir teknik araç olarak karşımıza çıkar[167].

CCTV'lerin kamusal alandaki kullanımı birinci bölümde tartışma konusu edilen pek çok konu ile bütünlük içindedir. Yukarıda da ifade edildiği şekilde özellikle Asya, Avrupa, Kuzey ve Güney Amerika'da yer alan bazı devletlerin çok yönlü etkenler ile şekillenen tercihleri, video kayıt cihazlarını artan oranda kullanmak yönünde olmuştur[168]. Kamusal alandaki video gözetimin yoğunluğu; otoriterleşme, özel hayatın gizliliğinin veya insan haklarının bazı başka açılardan ihlali gibi pek çok tartışmayı beraberinde getirmiştir[169]. Video gözetim sistemlerinin kamusal alanlardaki kullanım gerekçelerinin detaylandırılması ve güncel eleştirilere ise çalışmanın ilerleyen bölümlerinde yer verilmiştir.

2.2. VİDEO GÖZETİM SİSTEMLERİ

2.2.1. Video Gözetim Sistemlerinin İşlevi

CCTV'ler veya video gözetim sistemleri gerek kamusal gerek özel alanlarda temelde güvenliğin sağlanması amacıyla oldukça fazla kullanılmaktadır. Video gözetim sistemleri, veri akışının esas olarak önde yer alan kameradan kontrol merkezine doğru ulaştığı bir yapılanma olarak, izinsiz giriş dedektörü tarafından verilen alarmı kontrol etmek için devriye muhafızları veya polislerin yerini almak üzere güvenlik alanında ilk olarak fiziksel koruma sistemine dahil edilmiştir[170]. Gözetim yapan video kayıt sistemleri 2005 yılındaki Londra bombalamalarının soruşturma sürecinde şüphelileri tespit etmekte olduğu gibi pek çok benzer olayda, suç sonrasındaki süreçte önemli ipuçları sağlamıştır ve böylelikle hükümetlerin video gözetim sisteminin şehir yaşamının güvenliği veya

---

[167]Ibid, s.33.
[168] THOMAS, A. L., PIZA, E. L., WELSH, B. C., & FARRINGTON, D. P. (n.d.). "The internationalisation of cctv surveillance: Effects on crime and implications for emerging Technologies". International Journal of Comparative and Applied Criminal Justice, 46(1), s.1.
[169] INNES, M. (2003). "Understanding Social Control: Deviance, Crime and Social Order". Open University Press. s.15-16.
[170] ZHANG, H., LI, P., DU, Z., & DOU, W. (2020). "Risk entropy modeling of surveillance camera for public security application". IEEE Access, 8, s.45343.

kamusal güvenlik için önemli olduğunu düşünmesine sebep olmuştur[171]. 13 Kasım 2022 yılında İstanbul İstiklal Caddesi'nde bombalı saldırıyı gerçekleştiren kişinin de tespiti, güvenlik kameraları ile elde edilen görüntüler ile yapılmıştır[172].

Bir video gözetim sistemi analog ve dijital cihazlar ile bir yazılımdan oluşur, burada amaç bir sahnenin görüntülerini yakalama, görüntü işleme ve bunları bir operatöre göstermektir[173]. Kısa ismi ve yaygın kullanımı ile CCTV olarak bilinen, kapalı devre görüntü ve kayıt sistemleri; bir veya birden fazla kamera kullanılarak belirli bir alanın izlenmesini, izleme neticesinde edinilen görüntülerin kaydedilmesini, video şeklinde oynatılmasını sağlamaktadır[174].

Teknolojik gelişmeler CCTV'lerin kurulum ve kullanım maliyetlerini de azalttığından, bu sistemler banka, kalabalık cadde ve sokaklar ile eğitim kurumları gibi kamusal alanlarda dikkat çeken ölçüde kullanılmaya başlanmıştır. Öyle ki 2021 yılının sonu için dünya üzerinde toplam 1 milyar kamera kurulduğu, bunun her 8 insan için bir kamera anlamına geleceği ifade edilmektedir[175]. Elbette dünya üzerindeki her ülkede aynı oranda video kayıt sistemi bulunmaz. 2021 yılı için Çin ve ABD'de sırasıyla 4,1 ve 4,6 kişiye bir kamera düştüğü, en yüksek CCTV yoğunluğuna sahip 10 şehirden altısının Çin'de, üçünün ise Hindistan'da olduğu, Asya dışında Londra, New York, İstanbul, Paris gibi metropollerde CCTV'ye daha çok başvurulduğu belirtilmektedir[176].

Suç oranları, kilometre veya kişi başına düşen analizlere göre yapılabilen çeşitli karşılaştırmalar, güvenlik-gözetim-mahremiyet ikilemine daha çok giren ülkeleri açığa çıkarmaktadır. Örneğin; suç endeksi 46.29 olarak ifade edilen New York'ta 1 km2 başına 25.97 CCTV düşmekte, kamera sayısı ise 31.490 olarak ifade edilmekteyken; suç endeksi 47.85 olan İstanbul'da 1 km2 başına 42.3 CCTV düşmekte ve cihaz sayısının 109.000

---

[171] Ibid, s.45343.
[172] Voa, İstiklal Caddesi Saldırısı Failinin Kimliği Açıklandı. (Erişim Tarihi: 18.11.2022) https://www.voaturkce.com/a/istiklal-caddesi-saldirisi-failinin-kimligi-aciklandi/6833192.html
[173] European Data Protection Board, Guidelines 3/2019.s.29.
[174] AKINLAR, C. (2012). Kapalı Devre Görüntü ve Kayıt Sistemleri. Güvenlik Sistemleri. (Yusuf OYSAL, Ed.; 1). Anadolu Üniversitesi Yayınları. s.83.
[175] Surfshark, Surveillance Cities, (Erişim Tarihi: 28.07.2022) https://surfshark.com/surveillance-cities
[176] Ibid.

olduğu belirtilmektedir (bu rakam Paris için 26.834, Bağdat için 120.000, Moskova için 193.000, Pekin için 1.150.000'dir)[177]. Doğrudan CCTV kurulan alanın büyüklüğüne veya direkt olarak suç oranına bakarak CCTV'lerin kurulumunun "yerindeliğini" sorgulamak ise ayrı bir tartışmanın konusudur.

CCTV esasen bir tür durumsal suç önleme stratejisi oluşturarak, suç fırsatlarının sayısını azaltarak ve fiziksel çevrenin değiştirilmesi yoluyla algılanan suç işleme riskini artırarak suçu önlemeye odaklanmaktadır[178]. Bu durumda CCTV'nin birincil amacı, suçluyu suçtan kaçınmaya ikna edecek şekilde seçim yapılandırma özelliklerini etkileyen bir algısal mekanizmayı tetiklemek olarak ifade edilir[179]. Bununla birlikte CCTV sistemlerinin kurulma ve kullanılma amaçları; güvenlik, gözetleme ve denetleme şeklinde üç ana grupta incelenmektedir[180]. Video kayıt sistemlerinin kullanım amaçlarına ilerleyen başlıklar altında ayrıca yer verilmiştir.

2.2.2. Analog ve Dijital Kamera Sistemleri

CCTV kamera mimarisinde öncelikli olarak ortaya çıkan ve hali hazırdaki kurulumların çoğunluğunu teşkil eden analog CCTV yapısı; minimum olarak bir kayıt cihazı ve kameraların elde ettiği görüntülerin gösterildiği bir monitörden oluşan, analog kameraların hepsi ayrı ayrı olmak suretiyle kablo aracılığıyla bir kayıt sistemine bağlanan, yakalanan görüntülerin mekanizmaya/kayıt sistemine analog sinyaller biçiminde iletildiği ve eğer kurulan sistem eski teyp sistemi değilse kaydedici cihaza gelen görüntülerin elektronik bir kart ile sayısal bir hale getirildiği bir biçimde işler[181].

Bugün sadece çok küçük CCTV sistemlerinin basit kamera-monitör konseptini kullandığı, daha büyük olanların çoğunun bir şekilde, sinyal monitörde görüntülenmeden

---

[177] Ibid.
[178] PIZA, E. L., WELSH, B. C., FARRINGTON, D. P., & THOMAS, A. L. (2019). "CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. Criminology and Public Policy", 18(1), s.137.
[179] Ibid, s.137.
[180] AKINLAR,2012, s.83.
[181] Ibid.

önce video değiştirme veya işleme ekipmanı kullandığı ifade edilmektedir[182]. Daha büyük analog sistemlerin çoğunda, sinyal bir monitörde görüntülenmeden önce video değiştirme veya işleme ekipmanı kullanır, analog video sinyallerinin sayısallaştırıldıktan sonra tüm anahtarlama ve işleme işlemleri, ağ ve ağ anahtarlayıcıları üzerinden yapılır[183]. Analog kameraların avantajları dijital muadillerine göre daha az maliyetli olma ve daha düşük fiyata ihtiyaç duyulan tüm özelliklere sahip modelleri edinebilme imkânı yaratması, kurulum kolaylığı, bant genişliğinin ağı zorlamaması şeklinde sayılırken; kablolama, görüntü kalitesi, kapsama alanı, konumlandırma sınırları, bağlantı noktası sınırları, şifreleme problemleri gibi dezavantajları olduğu belirtilir[184]. Dijital video kayıt cihazlarının kullanıma sunulmasıyla birlikte, analog CCTV'lere duyulan ihtiyacın azaldığı söylenebilir.

Yeni nesil olarak ifade edilen ve IP (*internet protocol*) destekli sayısal kameralar ise; doğrudan ağlara bağlanır, elde ettikleri görüntüleri sayısal hale getirir ve bu sayısal ifadeleri NVR (*network video recorder*) adı verilen ağ kayıt cihazına göndererek gelen görüntüleri kaydetmiş ve ağdaki bilgisayara talep halinde göndermiş olurlar[185]. IP kameralı CCTV sistemlerinin kurulumu için ayrı bir iletişim hattı çekilmesine gerek yoktur, tüm kameralar ve kaydedici diğer ekipmanlar hali hazırda yerel IP ağına bağlanabilirler dolayısıyla kameralar için ayrı bir kablo hattı çekilmez ve sistem yeni eklenecek kameralar ile genişletilebilir[186]. Dijital kameraların avantajları ise kısaca görüntü kalitesi, kapsama alanı genişliği (üç-dört adet analog kamera genişliğinde), daha az kablo gerektirmesi, konumlandırma sınırlarının ortadan kalkması, ethernet üzerinden güç alabilme, şifreleme avantajları iken; dezavantajları kurulum veya başlangıç maliyeti, yüksek bant genişliği ihtiyacı, sabit sürücüde daha fazla alan gereksinimi olarak belirtilir[187].

---

[182] DAMJANOVSKI, V. (2014). "CCTV From Light to Pixels (3rd ed.)". Elsevier, s.255.
[183] Ibid.
[184] Security Magazine (12.04.2018), "Pro's and Cons for IP vs. Analog Video Surveillance", (Erişim Tarihi:29.08.2022).https://www.securitymagazine.com/articles/88854-pros-and-cons-for-ip-vs-analog-video-surveillance
[185] AKINLAR,2012, s.88.
[186] Ibid.
[187] Security Magazine (12.04.2018), "Pro's and Cons for IP vs. Analog Video Surveillance",

Suçlardaki geleneksel değişim ölçütleri CCTV'yi tek bir ölçü olarak ele alma eğiliminde olsa da kamera sistemlerinin uygulama tarzlarında, teknolojik yeteneklerde, yönetim tarzlarında ve izleme metotlarında, her biri her sistemi benzersiz kılan geniş bir çeşitlilik bulunur ve bu durum kamera sistemlerinin çalışmasını etkiler[188]. Bu nedenle CCTV sistemleri pratikte birbirinden önemli ölçüde farklılık göstermektedir ve halka açık alanda kullanılan sistemler çoğu zaman analog ve dijital türlerin melezidir[189]. Zira bu iki türün de izleme için farklı açılardan tercih edilebilir yanları vardır.

2.3.VİDEO KAYIT SİSTEMLERİ TARAFINDAN ELDE EDİLEN VERİLER

Veri (*data*), bilgi (*information*) ve kanaat (*knowledge*) kelimelerinden özellikle veri ve bilginin kimi zaman birbirleri yerine veya gelişigüzel şekilde kullanılabildiği dikkat çekmektedir. Oysa bu kavramlar iç içe olsalar da farklı anlamlar taşır ve esasen veri-bilgi- kanaat şeklinde bir anlamsal hiyerarşi ile yorumlanır. Genel manada kullanıldığı şekliyle "veri" *-ki genellikle ham veri denir-* anlamı olmayan bir metin, sayı ve sembol koleksiyonu olduğundan, veriler anlam kazanmadan önce işlenmeli veya bir bağlamla sağlanmalıdır[190].

Aslında veriler tek başına bir anlam ifade etmeyen, bağlamsız ifadeler kümesidir. Diğer taraftan bilgi; genellikle bilgisayar tarafından verilerin işlenmesi sonucunda, işlenen verilerin bağlam içinde kullanılmasını ve anlam kazanmasını sağlayan gerçekler veya anlamı olan verilerdir[191]. Bilginin kullanımı sonucunda üretilen ve oluşan problemlerin nasıl çözüleceğine dair kullanılabilecek düzeydeki çıkarımlar ise kanaat şeklinde tanımlanabilir. O halde, kameralar ile edinilen veriler tek başına bir anlam ifade

---

[188] SPRIGGS, A., & GILL, M. (2006). "CCTV and Fight Against Retail Crime: Lessons from a National Evaluation in the U.K". Security Journal, 19(4), s.241.
[189] Ibid.
[190] Cambridge International AS & A Level Information Technology 9626 For examination from 2017, Data, information and knowledge, (Erişim Tarihi:29.07.2022). s.4.chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cambridgeinternational.org/images/285017-data-information-and-knowledge.pdf
[191] Ibid, s.5.

etmeyip, işlenerek birer "bilgi" olduklarında, "kullanılabilir ve kanaat oluşturabilir" seviyeye gelirler.

Bu verilerden bazıları doğrudan kişilere mündemiç olduklarından, kişilere ait bilgiler haline getirilebilirler ve tam da bu noktada konu hukuki incelemenin hedefi hale gelir. Detayları çalışmanın üçüncü bölümünde belirtilecek olmakla birlikte kişisel veri; uluslararası düzenlemelerde genel kabul gören tanımına göre;

> *"…tanımlanmış veya tanımlanabilir bir gerçek kişiye (data subject, veri sahibi veya KVKK'ya göre ilgili kişi) ilişkin her türlü bilgidir; tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir…"*[192].

Dolayısıyla video gözetim sistemleri ile elde edilen görüntülerde yer alan, kişilere ait genel görüntüler, kullanılan cihaza göre değişmekle birlikte biyometrik veriler de elde edebileceğinden korunmaya muhtaç birtakım kişisel veri ihlalleri meydana gelebilecektir. İfade edilmelidir ki; video gözetim cihazları ile kişisel veri elde edilmesinin mümkün olması, her durumda kişisel verilerin işlenmesi veya kişisel verilerin korunması hukuku kapsamına girmeyecektir. Bu noktada hangi durumlarda veri işleme faaliyeti yürütülmüş sayılacağı, uygulamadaki düzenlemeler ve mahkeme kararlarından anlaşılmaktadır. Video gözetime yapılan eleştirilerin çerçevesi ilerleyen başlıklar altında ve video gözetim ile kişisel verilerin korunması hukukunun bağlamı ise üçüncü bölüm kapsamında ele alınmıştır.

Devletlerce halka açık alanlarda kullanılan kamera sistemleri ise genel olarak; otomatik plaka tanıma sistemleri (*ALPR-Automatic License Plate Recognition*), vücut kameraları, yüz ve iris tanıma özellikli kameralar, CCTV'lerin dahil olduğu gözetim

---

[192] "2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü" (GDPR), Avrupa Birliği Bakanlığı Çevirisi Türkçe Versiyon, m.4/1.

kameraları, gün ışığında veya kızılötesinde video veya hareketsiz görüntü kaydedebilen insansız hava araçları (*drone*) şeklinde sayılabilir[193].

Bugün pek çok ülkede güvenlik birimleri tarafından yaygın şekilde kullanılan ALPR'ler; tipik olarak sokak direklerine, sokak lambalarına, otoyol üst geçitlerine, mobil römorklara veya polis ekiplerine bağlı, yüksek hızlı, bilgisayar kontrollü kamera sistemleri olup görüntülenen tüm plaka numaralarını konum, tarih ve saatle birlikte otomatik olarak yakalar, aracın ve bazen de sürücüsü ile yolcularının fotoğraflarını içeren verilerin daha sonra merkezi bir sunucuya yüklenmesini sağlar[194].

Bu sistem ile, sabit bir yere monte edilen veya gezici araç/görevlilerce kullanılan ALPR kameraları, plaka numaraları, otomobilin rengi (ve belki markası), ilgili tarih ve konum verileriyle birlikte daha sonraki araştırmalarda kullanılmak üzere diğer verilerin saklanmasına ve özellikle geçmiş veya gelecekteki suç mahalline yakın araçların varlığını doğrulamak veya ilgi-şüphe çekici araçların şehirdeki hareketini izlemek için ilgili birimlere iletilmesine yarar[195]. Yine plaka verilerinin araç tescili ve ehliyet veri tabanları aracılığıyla plaka sahiplerine ilişkin ayrıntılı diğer -sabıka kaydı gibi hassas nitelikli de olabilen- kişisel verilere de ulaşılmasını sağlaması mümkündür.

Yaka kameraları (BWC- Body Worn Camera) ise; polisler ve diğer kullanım yetkisi olan kişilere, kesiştikleri kişiler hakkında gerçek zamanlı veriler sağlama kapasitesi ve sokak ile kontrol odası arasındaki sürekli veri akışını sağlamak yönünden saha operasyonları üzerinde artan merkezi koordinasyonu kabiliyeti sunmaktadır[196]. BWC'lerin açılıp kapanması veya gerektiğinde durdurulması kullanan yetkilinin takdirinde olan, özellikle dar alanlarda kolluk kuvvetleri tarafından oldukça fazla kullanılan, genellikle video ve aynı zamanda ses verilerinin merkez sunuculara aktarıldığı

---

[193] Electronic Frontier Foundation, Street Level Surveillance. (Erişim Tarihi:29.07.2022) https://www.eff.org/tr/issues/street-level-surveillance
[194] "Electronic Frontier Foundation, Automated License Plate Readers" (ALPRs).
[195] SKOGAN, W. G. (2019). "The future of CCTV". Criminology and Public Policy, 18(1), s.163. https://doi.org/10.1111/1745-9133.12422
[196] Ibid, s.164.

takip kameralarıdır[197]. Yine yüz ve iris taraması yapan kameralar -her ne kadar kamusal alanda yaygın bir kullanıma sahip olmasalar da- değişmez nitelikteki biyometrik verileri elde ettiklerinden, ölçüsüz kullanımları konusunda çeşitli eleştiriler doğururlar.

2.4. VİDEO GÖZETİM VE KAMUSAL ALAN

2.4.1. Kamusal Alanların Kapsamı

Kamusal veya halka açık alanlar, kişilere gayri resmi bir sosyalleşme olanağı ve bu sebeple de sivil yaşam için bir temel oluşturma hakkını sağlar. Zira bir görüşe göre; kamuya açık yerler aracılığıyla insanların gündelik faaliyetleri, toplumsal sözleşmeyi ve toplulukların kimliklerini doğrular[198]. Bir diğer görüşe göre bu alanlar, kimlik konumlarının kurulduğu ve müzakere edildiği kritik aşamaları kapsar, halkın eylemler ve diğer bir araya gelme faaliyetleri ile inşa edilen bir demokratikleşme aracıdır[199]. Bu sebeple kamusal alan genellikle ticari veya kurumsal bir ön bahçe olarak algılansa da bu yerler aynı zamanda sosyal ritüeller ve kültürel davranışlar, sosyal roller üstlenme ve sosyal dönüşüm sağlama anlamlarını taşıdıkları için önemlidir[200].

Bunlar gibi önemli işlevleri sebebiyle kamusal alanlardaki sosyal durumun muhafazası ve belirli bir güvenlik seviyesinde tutulması gerekir. Bu şekilde genel olarak güvenlik gerekçesi ile video gözetim altında tutulan kamusal alanların hem toplumsal hem bireysel öneminden ötürü gözetiminin sınırları açıkça belirlenebilen şekilde yapılması da önem teşkil etmektedir. Bu noktada kamusal alan olarak tanımlanan yerlerin, genel olarak kapsamına değinmek gerekir.

---

[197] BUNN, N. And CUNNINGHAM B. (23.10.2015), "Which Data Should Police Body Cams Collect?", The Atlantic.
[198] PATTON, J. W. (2000). "Protecting privacy in public? Surveillance technologies and the value of public places". Ethics and Information Technology, 2, s.181.
[199] DIAMOND, B. (2010). "Safe Speech: Public Space as a Medium of Democracy". Journal of Architectural Education, 64(1). s.105. https://about.jstor.org/terms
[200] Ibid.

Bir görüşe göre, kamusal alanda işlenen suçların çoğunluğu dijital olmayan ortamlarda meydana gelmektedir ve bu ortamlar bireyler tarafından her zaman erişilebilen parklar, yaya yolları, tüneller, sokaklar, binalar arasındaki boş alanlar, otobüs durakları gibi ulaşım aracılığı yapılan yerler, mahalle ve sokaklardaki diğer halka açık alanlardır[201]. Diğer taraftan kamusal alanlar; kentsel yaşamın zenginliğiyle yakından ilişkili olan çeşitli kullanımları destekleyen, ulaşım, performans, alışveriş, politik aktivizm, gayri resmi değişim fırsatları ve tesadüfi buluşmalar için maddi bir temel oluşturan sokaklar, kaldırımlar, parklar ve meydanları içermekle birlikte bu yerler hakkında münhasır mülkiyet iddiasında bulunulamaz[202].

Bireylerin özel alanlarında veya dışlamacı bir yaklaşımla kamusal alanların dışında kalan bölgelerde, bir suç işlenmesi, işlenmesi tehdidi doğması gibi durumlarda polisin ya da kamu gücünün müdahalesi, halka açık alanlarda yapılabilecek müdahalelerle kıyaslandığında çok daha sınırlı olacaktır. Başka bir bakışla; kamusal alan, bireylerin bir suçun kurbanı olduğu herhangi bir yeri veya çevresinin fiziksel ve sosyal özellikleri nedeniyle suç korkusu, endişe ve diğer güvenlik endişelerini tetikleyen herhangi bir yeri tanımlamak için kullanılan genel bir terimdir[203].

Terimin kapsamına ise bireylerin alışveriş merkezi, spor stadyumu, park veya tren platformu gibi ücretsiz ve halka açık bir yere kısmen veya tam erişime sahip olduğu yerler ile parklar, sokaklar, mahalleler ve otobüs duraklarının yanı sıra yol üzerindeki yerler gibi halk için değişen derecelerde erişime sahip çok çeşitli halka açık yerler girmektedir[204]. Öyleyse bu türden alanların belirlenmesi konusunda bir tanım birliği olmasa da kamusal alanların genel olarak, toplumu teşkil eden bireylerin kamusal bağ kurup geliştirdiği, özel mülkiyet iddiasında bulunulamayan ve herkesin girebildiği yerleri kapsadığı yorumu yapılabilecektir. Çalışmada kamusal alan, özel alanların dışında kalan, kamu otoriteleri

---

[201] CECCATO, V., & NALLA, M. K. (Eds.). (2020). "Crime and fear in public places : towards safe, inclusive and sustainable cities". Routledge. s.8.
[202] PATTON, 2000, s.181.
[203] CECCATO & NALLA, 2020,s.8.
[204] Ibid.

tarafından gözetim yapılan, halka açık alan veya mekânları ifade etme çerçevesinde kullanılmıştır.

2.4.2. Video Gözetimin Kamusal Alanlar Üzerindeki Etkisi

Özellikle 90'lı yıllar ve sonrasında, şehir hayatının kamusallığı içinde oldukça artan oranlarda kullanılmaya başlanan video gözetim, yukarıda ifade edildiği sosyo-ekonomik, tarihsel unsurdan etkilenmiş ve kent yaşamını, mimarisini, kent ekonomisini, sosyalleşme biçimlerini ve sair pek çok unsuru etkilemiştir. Liberal değerlerin yükselişe geçmesi ile geleneklerinden, aile bağlarından ve sair kültürel arka planlardan etkilenerek bir bireysellik anlayışı ortaya çıkmıştır. Esasen bu durum hem şehirlerde sosyalleşmeyi, ışıklı sokaklarda sosyal hayata entegre olmayı beraberinde getirirken aynı zamanda kamusal alanlarda da asgari bir mahremiyet beklentisi doğurmuştur. Öyle ki alanın kamusallığı bireylerin özel hayatın gizliliğinin veya mahremiyetin korunması iddialarından tamamen vazgeçeceği anlamına gelmemiş, bu yorum pek çok yargı kararı ile desteklenmiştir. Bu konuya mahremiyete yönelik eleştiriler başlığı altında "hukuk güvenliği" çerçevesinde yer verilmiştir.

Fyfe ve Bannister; artan video gözetim ile kentlerdeki estetik algısı tamamıyla değiştiğini, alışveriş merkezlerinde devriye gezen özel güvenlik görevlilerinden, avlulu konutlara erişimi kontrol eden uzaktan kumandalı kapılara kadar, pek çok merkezin vatandaşların davranışlarını izlemek ve düzenlemek için bir dizi insani, fiziksel ve teknolojik yöntem içerdiğini ifade eder[205]. Şehir merkezlerini tam anlamıyla dört koldan denetleyen, büyük direklere ve binaların yan taraflarına yerleştirilmiş, kamusal alanlarda yer alan CCTV'ler; şehirleri "endüstriyel çorak arazilerden, sanayi sonrası kültür merkezlerine" dönüştürdüğü iddialarına karşılık, "kale şehirlerdeki yönetimli, kontrol edilen alanların sert gerçekliği" nin açığa çıkmasını sağlamıştır[206]. Bu yaklaşıma göre

---

[205] FYFE, N.R. ve BANNISTER J. (2006) "The Eyes Upon The Street Closed-Circuit Television Surveillance and the City". N. Fyfe (ed.), "Images of the Street: Planning, Identity and Control in Public Space", Routledge: London and New York. s.248.
[206] Ibid.

artık CCTV'ler kent yapısının bir parçası haline gelen, kamusal yaşamın bizatihi kendisini temsil eden araçlardır.

Diğer taraftan hırsızlık gibi suçların kamera ile izlenen alanlardan, kameraların olmadığı ancak halk tarafından rutin olarak kullanılan şehir merkezi alanlarına/caddelerine kaydığını gösteren çeşitli çalışmalar yapılmıştır[207]. Bu durumun önünde geçmek için, genel bir güvenlik stratejisi olarak CCTV olmayan yerlere de cihazlar yerleştirmenin yerindeliği tartışma konusudur.

Roy Coleman ise CCTV ile şehirlerdeki kamusal alanların ilişkisinin, konunun kendisini çevreleyen süreçlerden ayrı olarak görmez. O'na göre; bir sosyal düzen stratejisinin yürürlüğe konmasına yönelik birleşik çabanın bir parçası olarak kamusal alanda video gözetim; şehir merkezinde "yenilenme" süreci yaratan güçlü koalisyonların ve ortaklıkların stratejilerini yansıtan siyasi, ideolojik ve ekonomik zorunluluklar içinde bir kameralı gözetleme ağının gelişiminden ibarettir[208].

Bu görüş; yerel, bölgesel, ulusal ve uluslararası ölçeklerde süreklilikler ve süreksizlikler sergileyen hegemonik bir küresel söylem olan neo-liberalizm ile, CCTV'yi yalnızca suç önleme teknolojisinin bir parçası olarak değil, daha geniş bir sosyal düzen stratejisinde kilit bir mekanizma olarak yorumlar[209]. Böylece kamusal alan gözetimi, bilhassa gelişmiş şehirlerde neo-liberalizmin doğasını, yönetim stratejilerini yansıtarak, şehirleri politik bir biçimde yeniden yapılandırmıştır. Coleman şehirlerdeki gözetimi, neo-liberal politikaların dayatılması, politize bir "girişimci şehircilik" biçimi, yalnızca devletin sınırlarını değil, aynı zamanda bu devletin gücünün bir ifadesi olarak bir sosyal kontrol vizyonu şeklinde ele alır[210].

---

[207] BROWN, B. (1995). "CCTV in Town Centres: Three Case Studies. In Crime Detection and Prevention Series". s.63-64.
[208] COLEMAN, R. (2004). "Reclaiming the Streets surveillance, social control and the city". Oregon: Willan Publishing.s.63.
[209] Ibid.
[210] Ibid,s.62-63.

Modernleşme ve sonrası dönemde sosyal hayatın, toplumsallığın inşası için büyük önem taşıyan şehirlerin, her geçen gün sayısının arttığı gözlemlenen video gözetim cihazlarından etkilenerek başkalaştığı belirtilmelidir. Bu başkalaşımda; kamusal alanlardaki ekonomik akış, devletlerce benimsenen güvenlik politikaları, Foucault'nun mekânsal bağlamında ifade edilen şehir mimarilerinin değişimi ve sair unsurların etken olduğu söylenebilir.

Şehirlerin güvenlik mimarisinde genellikle "durumsal suç önleme" ve "savunulabilir alan" fikirleri hâkim olsa da CCTV'lere "hükmeden" akıllı teknolojinin ve akıllı şehirlerin ortaya çıkışı ile kentsel peyzajların yönetimini dönüştürme potansiyeline sahip olan güvenlik stratejilerinin daha geniş bir çerçeveden yorumlanması gerektiği belirtilmektedir[211]. Dolayısıyla bugün kitlesel gözetime bağlı şekillenen akıllı şehir tartışmaları yapılırken diğer taraftan gizliliği koruyan hukuki düzenlemelerin de bu dönüşümden etkilendiği ve her geçen gün hukuka düşen payın arttığı ortadadır.

2.5. İDARENİN VİDEO KAYIT SİSTEMLERİNİ KULLANIM AMAÇLARI

Devletlerin kamusal alanda video gözetimi tüm dünyada yoğun şekilde kullanmasına sebep olan, çeşitli sosyal risk, olgu veya olaylardan kaynaklanan ve küresel politik gelişmeler ile şekillenen ortak amaçlar bulunur. Gerek kişi başına birden fazla kamera düşen Çin Halk Cumhuriyeti gerek her 10 kişiye ortalama iki kamera düşen ABD ve gerekse her 16 vatandaş için bir CCTV kamerasına sahip olduğu için üçüncü sırada yer alan Birleşik Krallık[212] video kayıt sistemlerinin kullanımı bakımından benzer sebeplere dayanır.

Bu sebepler genel olarak "güvenlik" veya "düzen" sağlama şeklinde ifade edilebilecek, kamu güvenliğinin sağlanması, trafik kontrolü yapılması, suç işlenmesinin önlenmesi (engelleyici maksat), suç işlendikten sonra suçlu yakalama veya delil toplama

---

[211] SCHUİLENBURG, M., PEETERS, R. (2018) "Smart cities and the architecture of security: pastoral power and the scripted design of public space". City Territ Archit 5**,** 13.s.1-9.
[212] BRANDL, R. (03.02.2022) The world's most surveilled citizens. Tooltester.

(izleyici maksat) gibi sebeplerdir. Başlık altında; idarenin kamusal alanda video gözetim sebepleri genel çerçeveden ele alınmış, böylece gözetime karşı dünyada yükselen seslere, kaygılara ve üretilen hukuk normlarına ilişkin, devletlerin dayanakları ele alınmaya çalışılmıştır.

2.5.1. Genel Olarak Güvenlik Gerekçeleri ile Video Gözetim

Güvenlik bir ülkeyi, binayı veya kişiyi bir saldırıya, tehlikeye ve bunlar gibi zarar verici durumlara karşı korumaya yönelik faaliyetleri kapsayan geniş bir kavramdır[213]. Ancak güvenliği tanımlamaya çalışırken bazı anlam karmaşaları oluşabilir. Geleneksel ulus devletler için askeri güvenlik olarak tanımlanabilecek olan kavram, zaman içinde bireysel güvenlik ve emniyeti de içerecek şekilde genişletilmiştir[214]. Modern devletlerce kullanılmaya başlanan güvenlik sağlama amacı, hukuk devletlerinde yaşanan bazı dönüşümlerin etkisiyle önce liberalleşmiş daha sonra küreselleşme, soğuk savaş gibi sebeplerle devletler için tekrar ön plana çıkmış, bir strateji geliştirme konusu olmuştur[215]. Video gözetim sistemlerinin kullanımı ile güvenlik(sağlama) arasında hem hukuki hem de diğer sosyal disiplinlerin konu edindiği pek çok tartışma bulunur.

Devletlerin kendi gözetim ve denetimleri altında güvenliği, toplumun ve ayrı ayrı kişilerin huzurunu ve refah içinde yaşamasını, millî güvenliği, kamu düzenini, kamu güvenliğini, suçların önlenmesini, suçluların cezalandırılmasını sağlamak ve güvenliğe ilişkin olası riskleri bertaraf etmek gibi görevleri vardır. Hatta genel çerçeveden "güvenlik" potasında eriyen bu sebepler topyekûn devletlerin varlık sebebi addedilir. Bu noktada çalışmanın temelinde sorgulandığı üzere, John Locke ve Thomas Hobbes'un toplumsal sözleşme kuramları ve devletlerin varlık sebeplerine bakış açıları karşımıza çıkar. Hobbes'un savunuları, bir güç aktörü olarak devletin bireylere güvenlik tesis etmesi, bireylerin ise devlete bu sebeple bazı ödev ve sorumluluklarının olması

---

[213] Oxford Learner's Dictionaries. https://www.oxfordlearnersdictionaries.com/definition/english/security?q=security

[214] KROENER, I. And NEYLAND, D. (2012). "New technologies, security and surveillance" . (Kirstie Ball. Kevin Haggerty. David Lyon. Ed.) Routledge Handbook of Surveillance Studies. Routledge: London and New York. s.141.

[215] BAYRA, E. (2019). "Güvenlik Devleti: Leviathan'dan Hukuk Devletine, Hukuk Devletinden Leviathan'a". İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 6(1), s.125.

noktasında toplanırken; Locke esas güvenliğin bireysel temel hak ve özgürlükler savunularak ve sağlanarak tesis edilebileceğini savunur[216].

Çalışmada savlanan, kişisel verilerin korunmasına yönelik mevzuatın kamusal alanlarda video gözetim sistemlerince yapılan izlemelere yönelik sorgulamalara açık olduğu düşüncesi; güvenlik-gizlilik ikilemi yönüyle Locke ve Hobbes'un güvenlik konusundaki çatışmalarını bünyesinde barındırır. Esasen Hobbes devletin kendi güvenliğinin, bütünlüğünün sağlanması amacıyla güvenliği savunurken, Locke bu tartışmayı bireylerin şahsi güvenliği ve hakları temelinde yapar[217]. Hobbes için devlet, bireylerin barış ve güvenlik ihtiyaçlarını sağlamak için var olan bir devasa yapılanma iken[218]; Locke bireylerin özgürlüklerinin elinden alındığı bir güvenlik anlayışının, onları devlete düşmanlaştıracağını savunur[219].

Bu anlamda devletlerin, "hükümran gücün kuşatıcı karakteri"ni[220] yansıttığı güvenlik sağlama maksadı ile yıllar içinde şehirlerin hemen her yerinde kameralı gözetim sistemi kurması, temel hak ve hürriyetler, kısacası özgürlükler ile ne kadar uyuşur? Diğer yandan devletlerin kendilerini sınırlayan hukuk kurallarını uygulayarak yaptığı kameralı gözetim, bu hukuk kurallarının varlık amacını sağlayacak "ölçüye" uygun mudur? Bu soruların cevapları, konunun kapsamı itibarıyla net savunular ortaya koyabilmeyi engellese de devletlerin video gözetim yaparken dayandığı sebepleri incelemek, sis perdesinin bir nebze aydınlanmasını sağlayabilir.

Düzenlenen pek çok hukuki metin veya resmî açıklamada kamusal alanda uygulanan gözetimin öncelikli ve meşru amaçlarının; suç işlenmesinin önlenmesi veya

---

[216] EMEKLİER, B. (2011). "Thomas Hobbes ve John Locke'un Güvenlik Anlayışının Karşılaştırmalı Bir Analizi". Güvenlik Stratejileri Dergisi, 7(13), s.99. https://dergipark.org.tr/en/pub/guvenlikstrtj/issue/7530/99185

[217] Ibid, s.120.

[218] HOBBES, T. (1651). "Leviathan Or The Matter, Forme, & Power Of A Common-Wealth Leviathan Or The Matter", Ecclesiastical And Civill: Vol. 2009. The Project Gutenberg E-Book of Leviathan, s.367.

[219] LOCKE, J. (1680). "Second Treatise Of Government. The Project Gutenberg EBook of Second Treatise of Government".,s.6.

[220] KARADAĞ, U., (2020). "Süreklilik mi Kopuş mu? Thomas Hobbes ve John Locke'un Toplum Sözleşmesi Teorilerinin Sınırlı Bir Mukayesesi", Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi, 15(185), s. 108.

suçlu takibi, tehlikeli faaliyetlerin gözlenmesi, suç sonrası izleme şeklinde ifade edildiği gözlemlenmektedir. İngiltere'nin henüz 2013'te ilk kez yayınlanan ve 2021 yılında değiştirilen gözetim kameralarına ilişkin uygulama kurallarını içeren rehberine (*surveillance camera code of practice*) göre;

> *"Güvenlik kameralarıyla ilişkili veya başka şekilde bağlantılı olan teknoloji sistemlerinin kullanımı görüntülerin ve ilgili bilgilerin toplanması ve kullanılması için artan bir potansiyel sağlamakta, teknolojik ilerlemeler, görüntüleri, bilgileri ve verileri yakalama, depolama, paylaşma ve analiz etme yeteneğini ve kapasitesini büyük ölçüde artırmakta, sensör teknolojisindeki ve yapay zekâdaki gelişmeler ve bu teknolojileri gözetim kameralarıyla entegre etme yeteneği giderek artan bir hızla gelişmektedir"*[221].

Bu açıklamalara dayalı olarak, kameralı gözetim sistemlerinin yaygın biçimde kurulma amacı; güvenlik kamerası sistemleri operatörlerinin, mevcut teknolojiyi halkın haklı olarak bekleyeceği bir şekilde kamu güvenini ve düzenini koruyan bir standartta yasal olarak kullanmalarını sağlamak, -uygun şekilde kullanıldıklarında- kamu güvenliğine ve güvenliğine katkıda bulunmaları ile hem insanların hem de mülkün korunmasına katkıda bulunmaları şeklinde ifade edilmiştir[222]. Aynı belgede, bu sistemlerin karmaşık bir sahiplik, operasyon ve hesap verebilirlik ortamının bir parçasını oluşturduğu ve güvenlik sağlama amaçlarına ancak doğru kullanıldıklarında hizmet edebilecekleri de dolaylı biçimde belirtilmiştir[223].

Fransız veri koruma otoritesi CNIL (*Commission Nationale de l'Informatique et des Libertés*) tarafından da kamuya açık alanlarda özellikle saldırganlık, hırsızlık veya uyuşturucu kaçakçılığı, terör eylemleri riskine maruz kalan yerlerde, kişi ve mal güvenliğine yönelik saldırıları önlemek için video gözetim sistemleri kurulabileceği

---

[221] Govenment U.K., "Guidance Amended Surveillance Camera Code of Practice (accessible version) Updated 3 March 2022".
[222] "Govenment U.K., Guidance Amended Surveillance Camera Code of Practice (accessible version)"
[223] Ibid.

belirtilir[224]. Yine Rusya'da da CCTV'lerin benzer amaçlarla suçu önlemek ve suçluların takibi için kullanıldığı, halka açık yerlerde CCTV'lerin sayısının giderek arttığı ve fakat vatandaşların görüşlerinin, polis birimlerinin kullandığı teknolojilerin suç önleme, güvenliği ve polisin hesap verebilirliğini artırmadaki etkinliği konusunda tereddütlü olduğu belirtilmektedir[225]. Emniyet güçlerinin veya diğer yetkili birimlerin video gözetim cihazları kullanma, kullanılması karar verme konusunda belirtilen mahremiyet/özel hayatın gizliliği veya temel hak ve hürriyet ihlali konularındaki kaygılar, cihazların suçla mücadelede "yeteri kadar" etkili olup olmadığı bu başlık kapsamında incelenmemektedir.

İçişleri Bakanımız tarafından, devlet hizmetlerinde MOBESE (mobil elektronik sistem entegrasyonu) ve EDS (elektronik denetleme sistemi) gibi teknolojik araçların kullanımının hem zamandan hem paradan tasarruf edilmesini sağladığı, Bakanlıkça kurulan Güvenlik ve Acil Durumlar Koordinasyon Merkezi (GAMER) isimli sistem aracılığı ile tüm toplumsal olaylarda MOBESE kameralarına ve polislerin kullanmakta oldukları vücut veya yaka kameralarına ulaşılabildiği, bu şekilde gerekli koordinasyonun kurulduğu, acil olaylara bu yöntemler ile daha çabuk müdahale edilebildiği belirtilmiştir[226].

Ülkemizde kamusal alanlarda gözetim yapmak için kurulan KGYS'nin (Kent Güvenlik Yönetim Sistemi) varlık amaçlarının ise; vatandaşların can ve mallarının güvenliğinin sağlanması, kamu düzeni ve kamu güvenliğinin tesisi, suç işlenmesinin önlenmesi, trafik güvenliğinin sağlanması şeklinde olduğu görülmektedir[227]. Uygulanan ve esasında adli değil daha çok idari (genel güvenlik sağlama ve caydırıcılık açısından)

---

[224] "CNIL, La vidéosurveillance – vidéoprotection sur la voie publique"(03.12.2019), (Erişim Tarihi: 19.11.2022)https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique

[225] GURINSKAYA, A. (2020). "Young Citizens Attitudes Towards CCTV and Online Surveillance in Russia. In book: Digital Transformation and Global Society", s.61-62.

[226] Türkiye Cumhuriyeti İçişleri Bakanlığı (11.10.2017) "Valiler Buluşması", (Erişim Tarihi:01.08.2022) https://www.icisleri.gov.tr/valiler-bulusmasi11102017

[227] T.C. İçişleri Bakanlığı Emniyet Genel Müdürlüğü, Bilgi Teknolojileri ve Haberleşme Daire Başkanlığı, KGYS ve PTS Projesi, (Erişim Tarihi:02.08.2022) https://www.egm.gov.tr/bilgiteknolojilerivehaberlesme/kgysvepts#:~:text=Kent%20G%C3%BCvenlik%20Y%C3%B6netim%20Sistemi%20(KGYS,g%C3%B6r%C3%BCnt%C3%BCleme%20ve%20plaka%20tan%C4%B1ma%20sistemleridir.

bir uygulaması olan MOBESE veya KGYS sistemine ayrı bir başlık altında yer verilmiştir.

Güvenlik sebebiyle CCTV kullanımının 11 Eylül saldırılarından sonra küreselleşen bir algıyı şekillendirdiği hemen her kaynakta ifade edilir. Terörle mücadele için bilgi ve gözetim teknolojilerini kullanılması, şiddet eylemlerini önleyici bir şekilde durdurmak için kolluk kuvvetleri tarafından kamuya açık ortamlarda video gözetiminin yoğunlaştırılması, şehirlerde kamu/özel ortaklıkları ile yeni gözetim sistemlerinin kurulması ve var olan kamera sayılarının artırarak ve yeni yüz tanıma özellikli sistemlere entegre hale getirilerek genişletilmesi sonucunu doğurmuştur[228].

Video gözetim sistemlerinin kamusal alanlarda güvenliğe yönelik sağlayacağı faydalar genel olarak; polisin kameralarla kaydedilen suçluları kolayca tespit edebileceği, kameralar sayesinde hem suçun oluşması engellenip hem de ceza davalarının maddi delillerle hızlıca çözülebileceği, hırsızlık ve vandalizm sorunlarının gerileyeceği, suç işlenmesi konusunda caydırıcılık sağlanacağı, bireylere güvende "hissettirmesi", bireylerin kameraların varlığını bildikleri takdirde tuhaf veya anormal davranmaktan kaçınacağı, yüz tanıma gibi yazılımların gelişmesi ile oluşturulan öngörüler sayesinde çok daha doğru raporlamalar yapılabileceği şeklinde sayılmaktadır[229].

Görüleceği üzere devletlerin güvenlik amacıyla video gözetim sistemlerini kullanmasına ortak motivasyon kaynakları vardır. Bunlar genel olarak; geniş alanların anlık görüntülenebilmesi, vücut kameraları ile daha sınırlı alanlarda suçlu takibinin daha kolay hale gelmesi, maliyet yönünden elde edilen faydalar, müdahale imkanının artması olarak sayılabilir. Fakat bu noktada önemli olan bir güvenlik sebebinin olmasından çok, bu sebebin ne kadar "meşru" olduğu, meşruluğun sınırının nasıl belirleneceği ve

---

[228] YEŞİL, B. (2006). "Watching ourselves: Video surveillance, urban space and self-responsibilization". Cultural Studies, 20(4–5), s.400. https://doi.org/10.1080/09502380600708770

[229] IFSEC GLOBAL, "Role of CCTV Cameras: Public, Privacy and Protection".

sağlanacağı ayrıca yine meşruluğun temel hakları koruma noktasında yeterli olup olmayacağıdır.

Kişisel verilerin korunmasına ilişkin şu üç soruya cevap verilebilmesi önemlidir: Video gözetim sistemlerinin kamusal alanlarda uygulanmasında kişisel verilerin veya özel hayatın korunması için hangi önlemler alınmaktadır? Kamusal alana yerleştirilen kameralar hangi hukuki/kanuni dayanağa sahiptir? Hukuki düzenlemeler, olası ihlalleri önlemek için yeterli midir? Bu sorulara çalışmanın üçüncü bölümünde yanıt verilmeye çalışılmıştır.

2.5.2. Diğer Gerekçeler ile Video Gözetim

Bugün pek çok devletin video gözetim sistemlerine ciddi yatırımlar yaptıkları, hali hazırdaki sistemleri teknolojik gelişmelere entegre etmeye çalıştıkları açıktır. Peki genel manada güvenlik sağlama, ulaşım akışının kontrolü, kamusal alanları ya da binaları koruma gibi yine güvenlik çatısına dahil edilebilecek sebepler dışında, kameralı gözetimi arzu edilir kılan farklı gerekçeler mevcut mudur?

Elbette devletlerin kamusal alanları kameralar aracılığıyla güvenli kılması kimi durumlarda anayasalar ile güvence altına alınan yaşam hakkı, seyahat özgürlüğü gibi temel hak ve hürriyetlerin kullanılması için dahi söz konusu olabilir. Bunun dışında idarenin de dijital hale gelmesi yani yönetişimin dijitalleştirilmesi ile devletlerin yürütmekte olduğu kamu hizmetleri ile halkın güvenini ya da memnuniyetini kazanması, güvenlik eksenli politikalara halkın da katılımının sağlanması durumları hali hazırdaki tablodan görünenlerdir. Ancak bu tablonun başka yansımaları da var mıdır? Güvenlik sağlama dışında, devletlerin video gözetimine dair hangi tartışmalar yürütülmektedir?

Bir görüşe göre; CCTV'lerle amaçlanan, güvenlik "sağlamaktan" çok güvenlik duygusu "yaratmaktır"[230]. Zira nihayetinde bu cihazların polise ve ceza adalet sistemine

[230] GOOLD, B., LOADER, I., & THUMALA, A. (2013). "The banality of security: The curious case of surveillance cameras. British Journal of Criminology", 53(6), s.984.

asıl faydası, başka görgü tanığı yoksa dahi kameraların orada olmasıdır ki bu durum, CCTV'lerin apaçık fayda sağladığıyla ilgili varsayımda bulunmaya yarar[231]. Bu inanç temelli yaklaşımda; video gözetim sistemlerinin suç işlendikten sonra delil toplamak açısından faydalı olduğu, bu maksatla her yere kamera koymanın hukuka uygun olmayabileceği, bu şekilde toplumda bir inanç perdesi yaratılıp cihazların devletin kendi görevini kolaylaştırmak ve toplumsal kontrol sağlamak amacıyla temel hakları tehlikeye attığı savunuları yapılır.

Diğer taraftan Andy Croll çalışmasında, kamusal alanların özgürlük fikriyle tanımlanan alanlar olarak kentsel yerleşim biçimi ile her türlü istenmeyen şeyin istilasına maruz kalan savunmasız alanlar haline geldiğini, kentlerin her yanını kontrol etmenin her geçen gün zorlaştığını, en güvenli olması gereken alanların bile her an güvensiz hale gelebileceğini ancak polislerin de şehir gözetiminde birer uzman olmadıklarını belirtir[232]. Öyle ki gözetim pratikleri şehirleri orta sınıf sakinler için "güvenli" hale getirmeyi amaçlar ve kamusal alanların güvenli hale getirilmesi bir sınıf projesinin ürünü dahi olabilir[233]. Bunun anlamı, saygın toplumun değerleri dışında kalan bireylerin kontrol altında tutulup, onların her hareketi gözlemlenirken, toplumun geri kalan tabakalarının güvenlik mutluluğu ile kentsel yaşamlarına devam etmesidir. Yine Clive Norris ve Gary Armstrong, kamusal alanların gözetlenmesinin "sapkın" olma ihtimali en fazla olan gruplara karşı yapıldığını, bu grupların hiçbir açık sebep olmaksızın sürekli izlendiğini ve hedeflerin sürekli değiştiğini ifade eder[234].

Video gözetim sistemlerinin yayılmasının, aynı zamanda iktidarın kapitalist özelliklerinin yayılması, kameralar gibi dijital araçların aracı yapılarak daha önce var olanlardan farklı, yeni egemen yapıların doğması şeklinde yorumlayan görüş[235], yukarıda ifade edilen "sınıf gözetimi" görüşünden çok farklı değildir. Bu okumalarla, gözetim

---

[231] Ibid.
[232] CROLL, A. (1999). "Street Disorder, Surveillance and Shame: Regulating Behaviour in the Public Spaces of the Late Victorian British Town". In Social History (Vol. 24, Issue 3). https://www.jstor.org/stable/4286578. s.267.
[233] Ibid.
[234] NORRIS ve ARMSTRONG, 1999, s.4-5.
[235] LYON, D. (1997). "Elektronik Göz- Gözetim Toplumunun Yükselişi (Dilek Hattatoğlu Çev.)". Sarmal Yayınevi., s.70-71.

sistemleri devletlerin güvenlik sağlamanın yanında otoriter eğilimlerinin demokratik yüzüdür ve bu haliyle mahremiyet yalnızca belirli kesimlerin elde edebildiği bir imtiyaz durumundadır[236]. Dolayısıyla amaçsal yaklaştığımızda, bu perspektiften yapılan kameralı gözetimdeki maksat, her kesimi tatmin eden bir güvenlik sağlama durumu değil, belirli sosyal tabakaların kontrolü, belli az sayıda grubun ise bir parça mahremiyet ile tatmin edilmesi, bunlar olurken de devletin totaliter hedeflerini meşru araçlarla elde etmesidir.

Kameralar başlangıçta çocuk kaçırma ve terörizm gibi üst düzey suçlara karşı bir araç olarak meşrulaştırılmıştır. Bu cihazların kamunun davranışlarının ayrıntılı izleme yeteneğinin keşfedilmesinin, bu durumun yetkilileri bir dizi daha düşük seviyeli (yerlere çöp atılması, el ilanı asılması vs.) sosyal konuyu ele almak için kameraları kullanmaya teşvik ettiği belirtilir[237]. Düşük seviyeli sosyal problemlerin boyutu veya devletler tarafından nasıl algılandığı ülkeden ülkeye ve ülkelerin yaşamakta olduğu sosyal olaylar, terör sorunları gibi sebeplere göre değişebilmektedir. Fakat burada bahis konusu edilen, toplumun ayrıntılı izlenmesinin hedeflenmesidir.

2.6. KAMUSAL ALANDA VİDEO GÖZETİME YÖNELİK ELEŞTİRİLERİN GENEL ÇERÇEVESİ

Gerek gözetim çalışmalarının tümünde gerekse ceza hukuku, idare hukuku gibi diğer çalışma alanları ve sair disiplinlerde, kamusal alandaki kameralı gözetime yönelik ciddi bir eleştirel yaklaşım literatürü göze çarpmaktadır. CCTV'lerin güvenliğe oldukça fayda sağladığına ilişkin iddiaların içinde dahi bu cihazların artan kullanımına dair kaygılar ifade edilmektedir. Başlık altında öncelikle bu geniş çaplı ve yönelimli eleştiriler, çalışmayla ilgisi açısından ele alınıp odak noktalarına göre; işlevsellik, totaliterliğe ve kötüye kullanıma elverişlilik, temel hak ve hürriyetlere aykırılık, hukuki güvenliğin sorgulanması şeklinde tasnif edilmeye çalışılmıştır.

---

[236] Ibid.
[237] HAGGERTY, K. D. (2012). "Surveillance, crime and the police. In K. Ball, K. Haggerty, & D. Lyon (Eds.), Routledge Handbook of Surveillance Studies". Routledge. s.235.

Bu başlıkta yer alan eleştiriler, özellikle üçüncü bölüm altında yer verilen hukuki düzenlemeler ile birlikte ele alındığında, kamusal alandaki video gözetime ilişkin kişisel verilerin korunmasına dair hukuki düzenlemelerin, eleştirilere bir çözüm olup olmadığı anlaşılabilecektir. Zira oldukça yeni ve dinamik bir alan olan kişisel verilerin korunması hukukunun amacı, kısaca bireylerin özel hayatlarının gizliliğinden kaynaklanan temel hak ve hürriyetlerini korumaktır. Dolayısıyla video gözetim cihazlarının yaygın kullanımına ilişkin bu alanda yapılan düzenlemelerin, konu hakkındaki kaygılara veya hali hazırdaki hak ihlallerine bir yanıt verip vermediğini incelemek çalışmanın amacı için elzemdir.

2.6.1. İşlevsellik Argümanları

Kameralara karşı işlevsellik argümanlarının odak noktasında bazı ortak soru ve sorunlar bulunur. Kamusal alanlara yerleştirilen kameralar suçların işlenme oranlarında bir azalmaya sebep olur mu? Oluyorsa özellikle etkin oldukları belirli suçlar var mıdır? Kameralar suçun işlenmesinin önüne geçer mi? Geçerse bunu nasıl yapar? Bunlar ve benzer sorulara verilen cevaplar esasen ülkeye, suç tipine, kameraların yerleştirildiği lokasyona ve diğer değişik etkenlere göre farklılaşmaktadır. Ancak açıkça ifade edilebilecek olan husus, kamusal alandaki kameraların suç işlenmesini önlediğini ve suç oranlarını ciddi düzeyde azalttığını söylemenin doğru olmayacağıdır.

CCTV'lerin etkinliğine yönelik çalışmalardan biri[238]; kameraların farklı suç tipleri üzerinde farklı etkiler doğurabileceğini, suçların CCTV'lerin olduğu yerlerden olmayan yerlere doğru kayabileceğini, çalışmada CCTV'nin yayılmacı bir pozitif etkisine rastlanılmadığını, çalışma konusu edilen bölgede halkın güvende hissetmesinden kaynaklı bir desteğin bulunduğunu fakat bu desteğin her zaman devam etmeyebileceği hususlarına yer verir[239].

---

[238] ÇAPAR,2011.s.63-63.

[239] Aynı doğrultudaki bir çalışma için bkz. an, E. (2012) "Gözetleme Toplumu Bağlamında Çağdaş Sosyal Kontrol Araçları: Kapalı Devre Kamera Sistemleri Ve Toplumsal Fayda Ve Maliyetleri:Ankara İli Örneği(yüksek lisans tezi)". Yök Tez Merkezi. (347549)

Brandon C. Welsh ve David P. Farrington'un, CCTV'nin halka açık yerlerde suç üzerindeki etkilerinin ifade edildiği meta-analizine göre ise; CCTV'nin Birleşik Krallıkta en çok otoparklarda işlenen araç suçlarını azaltmak üzerinde etkili olduğu, diğer suçların azaltılması üzerinde ciddi bir etkisinin olmadığı, bu cihazların suçu işleyenlerin tespiti açısından sağladığı faydanın suçluları caydırarak suçu azaltmadaki faydalarından çok daha fazla olduğu, CCTV'lerin yaya ve trafik güvenliğinin artmasını sağlayabileceği, şüphelilerin eylem içinde olduğu paketlerin belirlenmesi yoluyla veya eylem sonrasında şüphelilerin tanımlanmasına, yakalanmasına ve mahkum edilmesine yardımcı olarak terör eylemlerinin önlenmesini sağlayabileceği saptanmıştır[240]. Zira hem ABD'de hem diğer Batılı ülkelerde 11 Eylül saldırılarından sonra CCTV'lerin yaygınlaşması konusunda en büyük dayanak terör faaliyetlerinin önlenmesi olmuştur.

Bir başka çalışmada, CCTV'lerin suçu azaltma konusunda belirgin bir etkileri olmasa da araç hırsızlığı gibi daha kolay görünebilen genellikle şehir merkezinde işlenen suçlar üzerinde daha çok etkili olduğu belirtilmiştir[241]. Son yıllarda konu hakkında yapılan çalışmalar arttıkça daha yeknesak sonuçlara varıldığı gözlemlenmektedir. Öyle ki hırsızlık gibi suçların dışında daha ağır veya şiddet içeren suçlar açısından, hiçbir çalışmada video gözetim cihazlarının etkisi olduğuna dair kanıt bulunamamış, CCTV'lerin suçu önlemedeki etkileri incelenmiş, bu etkinin büyük olmadığı gözlemlenmiştir[242].

Bazı kaynaklarda ise; yeni teknolojiye harcanan milyarlarca pounda rağmen, bir örnek olarak Birleşik Krallık'ta suçu önlemek için CCTV kameralarına yapılan büyük yatırımın önemli bir etki yaratmadığı, İngiltere'nin Avrupa'daki herhangi bir ülkeden daha fazla güvenlik kamerasına sahip olmasına rağmen, Londra'daki sokak soygunlarının sadece %3'ünün CCTV görüntüleri kullanılarak çözüldüğü, biyometrik özellikli

---

[240] WELSH, B. C., & FARRINGTON, D. P. (2009). "Public area CCTV and crime prevention: An updated systematic review and meta-analysis". Justice Quarterly, 26(4), s. 735-742. https://doi.org/10.1080/07418820802506206

[241] MATCZAK, P., WÓJTOWİCZ, A. vd. (2021): "Effectiveness of CCTV systems as a crime preventive tool: evidence from eight Polish cities". International Journal of Comparative and Applied Criminal Justice. s.16-17.

[242] NORRIS, C. (2012) "The success of failure: Accounting for the global growth of CCTV". Routledge Handbook of Surveillance Studies. (K. Ball,K. Haggerty, D. Lyon ed.) Routledge: London and New York.

kameraların sayısallaştırılmış veri tabanlarının aranması ve şüphelilerin görüntülerini bilinen suçlularla eşleştirmek için kullanılabileceği belirtilmiştir[243].

Kameraların işlevselliğini sorgulayan eleştirilerin yanında özellikle yüz tanıma özelliği olan cihazlar, kimi olayları açıklığa kavuşturmak bakımından önemli olabilir. Tartışma ve gündem konusu olan bir olayda, sahip olduğu yüz tanıma algoritmasını sosyal medya kullanıcılarının sosyal platformlara yüklemiş olduğu fotoğrafları üzerinden rızaları olmadan geliştiren Clearview AI adlı bir yazılım yeniden gündeme gelmiştir[244]. Araç ile insan öldürmekle suçlanan Floridalı bir kişinin avukatı tarafından özel erişim izni ile kullanılan Clearview AI, kaza yerinde çekilen görüntüleri ile algoritmada bulunan 20 milyar kişinin yüzü içinden eşleştirerek suçlanan kişinin aracı kullanan kişi olmadığını saptamıştır[245]. Suçlanan bir kişinin bu algoritma aracılığıyla 15 yıl hapis cezası almaktan kurtulması, yüz tanıma özelliğine sahip cihazların potansiyel faydalarının da olabileceği, kayıp kişilerin bu cihazlar ve algoritmalar ile bulunabileceği, işlenen suçların izini süren avukat, polis gibi aktörler açısından faydalı bir araç olabileceği hakkında fikirler de öne sürülmektedir[246].

İki yönlü değerlendirmenin de bulunduğu konu hakkında ifade edilen faydaların yanında, değişmez nitelikteki yüz verileri rızaları dışında kullanılan bireylerin bu kullanımın farkında bile olmamaları, bireylerin çıkarına hizmet ettiği savunulan olaylar karşısında aksi nitelikte olayların da yaşanması, veri güvenliğinin tam olarak sağlanamaması hallerinde kişilerin yüzlerinin ve görüntülerinin deep fake[247] gibi yeni yöntemler ile kötüye kullanılması mümkün olabilecektir. Bunun dışında yüz tanıma

---

[243] BOWCOTT, O. (06.05.2008). "CCTV boom has failed to slash crime, say police". The Guardian, (Erişim Tarihi:05.08.2022). https://www.theguardian.com/uk/2008/may/06/ukcrime1

[244] DASCALESCU, A. (20.09.2022). "The Controversial Clearview AI Was Used By Florida Man's Lawyer to Clear Him Of Vehicular Homicide Charges". Techthelead. (Erişim Tarihi: 22.09.2022) https://techthelead.com/the-controversial-clearview-ai-was-used-by-florida-mans-lawyer-to-clear-him-of-vehicular-homicide-charges/

[245] HILL, K. (24.06.2020). "Wrongfully accused by an algorithm", The Seatlle Times. (Erişim Tarihi: 05.08.2022) https://www.seattletimes.com/business/technology/wrongfully-accused-by-an-algorithm/

[246] Ibid.

[247] Konu hakkında bir çalışma için bkz. BERK, M. E. (2020). "Dijital Çağın Yeni Tehlikesi Deepfake". OPUS International Journal of Society Researches, 16 (28), 1508-1523. DOI: 10.26466/opus.683819

özelliğine sahip cihazların sağlayabileceği belirtilen işlevlerin karşısında yer alan diğer eleştirilere, aşağıda yer alan başlıklarda yer verilmiştir.

2.6.2. Otoriterliğe veya Kötüye Kullanıma Elverişlilik Argümanları

Biyometrik veri elde eden cihazlara paralel olarak, bu türden hassas verileri toplayabilen kameraların da arttığı gözlemlenmektedir. Devletlerin kısaca suç işlenmesinin önlenmesi ve suçlu takibi için yüz tanıma teknolojilerini kullanan "akıllı", yapay zekâ ile donatılan kameralar kullanmaya başlaması ile eleştiriler de farklı bir boyut almıştır. Zira bu teknolojiler, kişilerin yüzlerini hali hazırda elinde olan diğer veriler ile kıyaslayarak yapay zekâ algoritmaları ile tespit etmekte, bu veriler üzerinde derin öğrenme (*deep learning*) yöntemi ile çeşitli işlemler yapabilmekte, biyometrik veri toplayabilmektedir[248].

Üçüncü bölümde daha detaylı açıklanacağı üzere, biyometrik veriler kişiye doğrudan ve bütüncül olarak bağlı oldukları için değişmez niteliktedir. Bu sebeple biyometrik veri eden yüz tanıma sistemlerinin kendisine yönelik kaygılar, bu sistemlerin devletlerce kullanılması durumunda daha da artmaktadır. Yüz tanıma sistemlerinin hatalı tespitler yapabilme ihtimali, biyometrik verilerin toplandığı sistemlerden uzunca süreler çıkarılmaması sonucu güvenlik açığı ihtimalinde hassas nitelikteki bu verilerin ele geçirilme olasılığı, yapay zekâ kullanan sistemlerin ön yargılı veya yanlış analizler yapabilmesi, sistemlere yetkisiz erişim gibi hem teknik hem de kötüye kullanıma dayalı açılardan eleştirildiğini belirtmek gerekir[249].

Yüz tanıma sistemleri okullarda, bankalarda, havaalanlarında, hastanelerde ve süpermarketlerdeki gibi çeşitli izleme sistemlerine paralel olarak bağlanarak, güvenlik olaylarını izlemek ve tespit etmek için havaalanları, yollar, toplu taşıma ve şehir

---

[248] İÇER, Z., & DÖNMEZ, E. (n.d.). "Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku Ve Ceza Muhakemesi Süreçlerindeki Kullanımı Ve Sınırları". CHD, 15(43), s.423.
[249] İÇER & DÖNMEZ, s.430-431.

merkezleri gibi halka açık yerlerde de yaygın olarak kullanılmaktadır[250]. 2010'larda kullanımı artan yüz tanıma teknolojileri, 2011'de Usame Bin Ladin'in kimliğinin doğrulanmasında, 2014'te önemli bir hırsızlık davasındaki failin mahkûm edilmesinde, 2015'te Baltimore'da meydana gelen olaylarda ve bazı önemli protestolara katılanların tespitinde kullanılmıştır[251].

Akıllı sistemlerin sağladığı faydaların karşısında ortaya konulan kaygılar veya tehlikeler ise hafife alınacak boyutta değildir. Amerika'da ilk "yanlış pozitif vakası" olarak bilinen, sistemlerce yanlış şekilde tespit edilen kişinin tutuklanması vakasından sonra Amazon, IBM, Microsoft gibi şirketler, kolluk kuvvetlerine bu yüz tanıma sistemlerinin satılmasının durdurulacağını açıklamışlarsa da[252], bu durdurmanın doğruluğunu yalnızca bu açıklamalara dayandırmak çok olanaklı değildir. Yapay zekânın farklı bir yüz ile eşleştirme yapması neticesinde yalnızca kamera tespitine dayanılarak yapılan tutuklamalar, temel hak ve hürriyetlerin korunduğu zemini sarsmaktadır.

Yüz tanıma sistemlerinin, kolluk kuvvetlerince kamu denetimi veya güvenliği için kullanımında, yazılıma dahil olan algoritmaların kara kutu olarak kaldığı, bu algoritmaların nasıl çalıştığının çözülemediği dolayısıyla halkın bu sistemlerin denetiminin nasıl yapıldığını bilmesinin mümkün olamayacağı belirtilmektedir[253]. Amazon, kolluk kuvvetlerinin meşhur Rekognition yüz tanıma yazılımını kullanmasını süresiz yasaklarken, yüz tanıma sistemlerini kullanımında polislerin potansiyel şüphelileri ararken bazı düzenlenmiş fotoğrafları, eskizleri, çarpık görüntüleri kullanabildiğinin tespit edildiği ve bu gibi eylemlerin zaten var olan, potansiyel yanlış

---

[250] TRAICHUK, A. (12.11.2021). "CCTV and Facial Recognition: Where Do the Two Technologies Overlap, Data Science Central". (Erişim Tarihi: 05.08.2022) https://www.datasciencecentral.com/cctv-and-facial-recognition-where-do-the-two-technologies-overlap/

[251] KLOSOWSKI, T., (15.07.2021). "Facial Recognition Is Everywhere. Here's What We Can Do About It". Wirecutter, (Erişim Tarihi: 05.08.2022) https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/

[252] HILL, K. (24.06.2020). Wrongfully accused by an algorithm,

[253] KLOSOWSKI, T., (15.07.2021). Facial Recognition Is Everywhere.

tespit ihtimallerini artırdığı konuları tartışılmaya uzun süre devam edecek gibi görünmektedir[254].

Hastaneler, trafik akışı olan yerler, kimi toplumsal olaylarda özellikle tercih edildiği gözlemlenen yaka kameraları yani BWC'ler ise; daha önce de açıklandığı üzere polis, jandarma gibi yetkililerce kullanılan, vücutta yaka, gözlük gibi bölgelere takılabilen, görüntü ve ses kaydedebilen, belirlenen politikalara veya prosedürlere göre otomatik veya manuel olarak çalıştırılabilen cihazlardır. Erken denemeleri Birleşik Krallık ve Avustralya'da yapılan ve 2000'lerden günümüze kadar artan oranlarda kullanılan BWC'lerin bugün toplam sayısını belirlemenin çok mümkün olmadığı, ABD ve Birleşik Krallık'ta yaşayan bireylerin üniformalı bir polis memuru ile her karşılaşmalarında esasen ses ve görüntülerini bir video kayıt cihazı ile kayıt altına alan biriyle karşılaşmış olacakları ifade edilmektedir[255]. Oldukça yaygın kullanımları olan BWC'lerin bu denli tercih edilmesine ilişkin bilhassa "hesap verilebilirlik" noktasında pek çok kaygı olduğu göze çarpmaktadır.

Öncelikli eleştiri bu cihazların kullanımının etkileri konusundadır. Zira suçun önlenmesi ve suçluların yakalanması konusunda hızlı hareket ve müdahale edebilme kabiliyeti sağlaması, polisin aşırı güç kullanımının azaltılması, suç soruşturmasına ilişkin deliller elde edebilme gibi nedenlerle tercih edilen BWC'lerin memurlar ve vatandaşların davranışları üzerindeki etkinliğinin belirsiz olduğu, yüksek beklentileri karşılayıp karşılamadığının yeterli şekilde sorgulanmadığı belirtilir[256]. BWC'lerin davranışlar üzerindeki etkilerinin, kişilerin kameraya kaydedilirken ve izlenirken oluşturulan öz farkındalık olduğu ve bunun onları yanlış veya sosyal olarak istenmeyen davranışlardan caydırabileceği, kullanan yetkililerin davranışlarına yönelik de etkili olabileceği hakkında

---

[254] HARWELL, D. (18.05.2021). "Amazon extends ban on police use of its facial recognition technology indefinitely". The Washington Post. (Erişim Tarihi: 05.08.2022) https://www.washingtonpost.com/technology/2021/05/18/amazon-facial-recognition-ban/

[255] LUM C, KOPER CS, WILSON D.B. vd. (2020). "Body-worn cameras' effects on police officers and citizen behavior: A systematic review". Campbell Systematic Reviews. Volume 16. Issue 3. s. 3-4.

[256] Ibid, s.5.

çalışmalar bulunsa da[257], her olayda vatandaşların kolluk kuvvetlerinin yaka kamerası kullandığını biliyor veya açıkça anlayabiliyor olduğu söylenemeyecektir.

Yetkililerin BWC'leri kullanımındaki takdir yetkisi ve bu yetkinin denetiminin zorluğu ise bir başka eleştiri noktasıdır. Takdir yetkisinin kötüye kullanılması durumunda, keyfi şekilde bireylerin özel hayatlarına müdahale edilmiş olacağı söylenebilir. Dolayısıyla yetkililerin BWC'leri açıp kapatma konusundaki takdir yetkilerinin sınırlı durumlarda kullanılması ve azaltılması polisin güç kullanımını azaltabileceği gibi[258] cihazların kullanım amacının önüne geçilmesi durumunu engelleyecektir. Diğer taraftan özellikle kamusal alanlarda kullanılan BWC'lerin kayıt altına alınmak istenmeyen, gerekli olmayan görüntülerin ses ve kayıt altına alınması sonucunu da doğurabileceği, bir memurun dahil olunan olayın videosunu izlemesi durumunda, gerçekte tanık olunan veya deneyimlenen ancak videoya alınmamış olan ayrıntıları unutma riskiyle karşı karşıya olduğu (*retrieval-induced forgetting*), kolluk kuvvetlerinin yaka kameralarının varlıklarına duyduğu güven ile bazı ara güç seçenekleri kullanma noktasında azalma olabileceği belirtilir[259].

ALPR'lerin (otomatik plaka okuyucular) ise; sadece önemli bulunan noktalarda değil yerleştirildikleri hemen her yerdeki tüm araçların fotoğrafı, plaka numarası, araçların hangi tarih-saatte hangi konumda olduğu bilgisini topladıklarından ve tüm bu bilgilerin sıkı şartlara tabi olmadan yetkilendirilen birimler arasında paylaşılmasından ötürü mahremiyet ve temel hakların korunmasıyla ilgili riskler barındırdığı ifade edilmektedir[260]. Giderek daha fazla uzayan saklama süreleri, yaygın paylaşım, veri tabanlarının protesto gibi toplumsal eylemlerde tespit-fişleme yapmak için kullanılması, olması gereken şekilde güvence altına alınmayan veri tabanlarının kötüye kullanım

---

[257] ARIEL, B., FARRAR, W. A., & SUTHERLAND, A. (2015). "The effect of police body-worn cameras on use of force and citizens' complaints against the police: A randomized controlled trial. Journal of Quantitative Criminology," 31(3), s. 509–535.

[258] LUM, KOPER, WILSON vd., 2020, s.2.

[259] KLIEM, V. (17.09.2020). "Body-Worn Cameras and Memory". Force Science. (Erişim Tarihi:09.08.2022)
https://www.forcescience.com/2020/09/body-worn-cameras-and-memory/

[260] American Civil Liberties Union. (July 2013). "You Are Being Tracked". (Erişim Tarihi:12.08.2022) s.2.
www.aclu.org

amaçlı izlemeye kapı açarak, erişimi olan herkesin çeşitli amaçlarla bireylerin hayatlarına göz atmasını sağlaması gibi endişeler karşısında[261], hukuki güvencelerin doğru şekilde sağlanması önemlidir. Bu paralelde, Birleşik Krallıktaki ALPR sisteminin toplam 8,6 milyon karayolu seyahatinin kaydını ortaya çıkardığına dair haber[262] öne sürülen eleştirileri adeta doğrular niteliktedir.

Küresel siber tehdit ortamının, devletler için büyük bir endişe nedeni olduğunu söylemek yanlış olmayacaktır. Nitekim dijital video gözetime, vatandaşların ve devletin kendisinin güvenliğinin sağlanması için her gün daha fazla güvenildiği ve ümit bağlandığı görülmektedir. Ancak, elde edilen ses ve biyometrik olan veya olmayan görüntülere bilhassa kolluk personelinin yaygın erişimi hakkındaki gizlilik endişelerinin ötesinde, kamera ağları ağırlıklı olarak doğrudan internete bağlı olduğundan, bu ağlar üzerinden kötü niyetli erişim risklerinin (siber saldırı, yetkisiz erişim vs.) de bertaraf edilmesi beklenir, -ki bunun her zaman mümkün olmayabileceği pek çok olayda görülmektedir[263].

Otoriterliğe ve kötüye kullanıma elverişlilik argümanlarında güvenlik-özgürlük ikilemi fazlaca göze çarpar. Bir taraftan suç ve suç karşısında duyulan mağduriyet korkusu ile güvenliğin daha çok sağlanması arzusu, diğer taraftan ise devletlerin güvenlik sağlamak için uyguladığı yöntemlerin kimi zaman bizzat kendilerince birer güvenliksizleştirme aracı haline gelebilmesi, devletlerin elindeki bilgilerin onları otoriterliğe sürükleyebilecek gücü vermesi ve bireylerin sistemli şekilde kontrol altında tutulması ihtimali belirmektedir.

Çoğulculuğun sınırlılığı, iktidar kullanımının keyfiliği riski, toplumsal hayat üzerindeki baskılar[264] gibi hususlar kameraların yaygın kullanımı noktasında "otoriterleşen devlet" düşüncelerini öne çıkartmaktadır. Lyon'a göre; teknolojik açıdan

---

[261] Ibid, s.3 vd.
[262] Security Magazine (01.05.2020). "Automatic Number-Plate Recognition System Exposes 9 Million Record" s. (Erişim Tarihi: 09.08.2022) https://www.securitymagazine.com/articles/92287-automatic-number-plate-recognition-system-exposes-9-million-records
[263] Iran International (06.02.2022). Tehran's 5,000 Surveillance Cameras, 150 Sites Hacked. (Erişim Tarihi: 09.08.2022) https://www.iranintl.com/en/202206025165
[264] KARADAĞ, U. (2020). "Kamu Hukuku Açısından Otokratik Yönetim-Gayrişahsi Devlet İktidarı İlişkisi ve 'Staatsgewalt' Kavramı". SÜHFD. C. 28, S. 3. s. 1442.

gelişmiş toplumların bilişim teknolojilere bu denli bel bağlamaları tek başına onları otoriter yapmaya yetmez[265]. Yoğun gözetim otoriterliğin önemli bir bileşeni olarak bireylere üzerlerinde kullanılan bu yeni teknolojilerin rolüne dair sorular yöneltebilme hakkı tanımak zorunda ise de cihazların "başarıları" karşısında bireylerin kaygıları ve soruları önemsiz veya ikincil durumda kalmaktadır[266]. Modern demokrasilerde yaygın şekilde var olduğu gözlemlenen otoriter devlet kontrolü, siyasal, hukuki ve iktisadi unsurlar ile birlikte[267], bu kontrolün sağlanması için araçsallaştırılan kameralar eliyle belirgin hale gelmektedir.

Bugün özellikle GDPR'ın etkin koruma sağlayan hükümler içerdiği, devletlere ve kişisel verileri (bilgileri) elinde tutanlara onları olabilecek en az müdahalecilik ile işlemeyi zorunlu kıldığı ifade edilebilse de konunun diğer yüzü esasen bilgiye sahip olmanın verdiği güçtür. Zira köklü demokrasilerin de bozulma, bugün meşru addedilen amaçların da yarın kötüye kullanılma riski söz konusu olabilir. Böyle durumlarda sahip olunan bilgilerin hangi amaçlar doğrultusunda kullanılacağının bir garantisi yoktur. Var olan hukuk kuralları güçlü maddi yaptırımlar öngörmüş olsa da (GDPR'da yer alan yıllık cironun %4'ü kadarlık bir para cezası gibi) kimi zaman veri ihlallerinin kaynağının tespiti dahi oldukça zor olabilmektedir. Bu sebeple olabilecek en az kişisel verinin elde edilmesi yani veri minimizasyonu (*data minimisation*) genel bir kaide olarak temel hakların korunması adına mutlak suretle uygulanmalıdır.

2.6.3. Temel Hak ve Hürriyetlere Aykırılık Argümanları

Video gözetim sistemlerinin yaygınlaşması ile bireylerin kamusal alanlarda gizli ya da bir ölçüde anonim olma, özel hayatın gizliliği iddiasında bulunma ihtimalleri oldukça zayıflamış olsa da bu tür iddiaların hiç öne sürülemeyeceği de iddia edilemez. Kişisel verilerin korunmasını isteme hakkı bir temel hak ve özel hayatın gizliliğinin parçası olarak yasalarca düzenlenmekte veya korunmaktadır. Kamusal alandaki kameralı gözetim karşısında da belli durumlarda bu temel hakkın ileri sürülebileceği kabul

---

[265] KLING & LYON, 1994,s.12.
[266] Ibid.
[267] KARADAĞ, 2020, s.1442, 1457,1458.

edilmektedir. Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde düzenlenen "özel hayata ve aile hayatına saygı hakkı" çerçevesinde, hakkın kullanılmasına kamu otoritesinin müdahale etmesi ancak maddede belirtilen ulusal güvenlik, kamu güvenliği, suç işlenmesinin önlemesi (…) gibi sebeplerle, zorunluluk hasıl olduğu takdirde ölçülü şekilde kanun ile söz konusu olabilecektir.

Avrupa İnsan Hakları Mahkemesi'nin kararlarında, kamusal alandaki her faaliyet olmasa da CCTV'ler gibi süreklilik arz eden eylemlerin özel yaşamın gizliliğinin ihlali olarak kabul edildiği görülmektedir. AİHM'in yerleşik içtihadı gereği CCTV'lerin kaydettiği kişisel veriler 8. madde kapsamında korunan kişilik hakkının unsurlarıdır ve madde bunların yanında kişilerin dış dünya ile bağlantı kurma, sosyal çevre ile ilişkilerini geliştirme gibi kamusal alanda da var olabilecek etkileşimlerini korur[268]. İfade edilmelidir ki; bir kamusal alanın kamu otoriteleri tarafından sistemli ve sürekli biçimde izlenmesi ve elde edilen verilerin kaydedilmesi ile fotoğraf makinesi aracılığıyla kaydedilmesi aynı sonucu doğurmayacaktır[269].

Diğer taraftan; kişisel veriden bahsedebilmek için CCTV'lerin kişilerin görüntülerini kimlik belirlenebilir şekilde elde etmesi, görüntülerin anlık şekilde depolanarak mı yoksa kayıt edilerek mi izlediği de önem taşır[270]. Elde edilen görüntüler kaydedilerek, kalıcı veya sistematik şekilde yapılan faaliyet açısından kişisel verilerin korunması hukuku devreye girecektir.

Bununla birlikte kamusal alandaki video gözetim, özel hayata bir müdahale anlamına gelebileceğinden, hakkın sınırlaması muhakkak kanun ile yapılmalıdır.

---

[268] AİHM. Peck ve Birleşik Krallık Kararı. Başvuru No: 44647/98. Karar Tarihi: 28 Ocak 2003. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]} (Erişim Tarihi: 13.08.2022) ayrıca kişisel verilerin korunması ve kişilik hakkı arasındaki ilişki hakkında bkz. BASKIN, O. (2021) "Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması". Ankara: Seçkin Yayıncılık.s.67-108.

[269] AİHM. Herbecq ve Diğer v. Belçika Kararı. Başvuru No: 32200/96 ve 32201/96. Karar Tarihi: 14 Ocak 1998.
Sistemli ve sürekli izlemenin özel hayata müdahale olduğuna dair karar için bkz. AİHM. Vukota-Bojić v. Switzerland Kararı. Başvuru No: 61838/10. Karar Tarihi: 18.10.2016. (Erişim Tarihi: 13.08.2022) https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-11261%22]}

[270] KÜZECİ,2021, s.508.

Nitekim; özel yaşamın gizliliğinin tek başına olabilme, kişisel bilgiler üzerinde kontrol sağlayabilme, mahremiyet elde etme, kişiye sınırlı ulaşım veya özerklik gibi pek çok boyutu olduğundan[271] bu temel hakkın korunması çeşitli bireysel ve sosyal alanlarda yankı bulmaktadır.

Özel hayatın gizliliğine yönelik sınırlamanın kanun ile yapılmaması durumunda hukuka uygun bir temel hak sınırlaması yapıldığından elbette bahsedilemeyecektir. AİHM bir başka kararında; dekan tarafından bazı üniversite amfilerine video gözetim cihazları konulması ile ilgili, faaliyetin başvuruculların ülkesinin kanununda yer almadığı ve bu haliyle uygulanamayacağı, can ve mal güvenliğine yönelik herhangi bir tehlike riskinin video gözetim için meşru gerekçeler arasında olmadığı, üniversitenin kamu yararına faaliyet yürüten bir kamu kurumu olmasının da bir dayanak olmayacağı, bireylerin özel ve sosyal yaşamlarına ilişkin düzenlemelerinin kısıtlayıcı olduğu durumlarda bile bu kısıtlamaların hakkı sıfıra indiremeyeceğine, özel hayata saygının "gerektiğinde sınırlandırılsa dahi" asgari ölçüdeki varlığını sürdüreceğine karar vermiştir[272].

CCTV'lerin kamusal alanda kullanımının hukuk ile koruma altında olan bir temel hak sorunu olduğu ortadadır. Bu sebeple cihazları kullanan kamu otoritelerinin de temel hakların sınırlandırılması için aranan koşullara riayet etmesi gerekir. Aksi halde en başta AİHS ve sair uluslararası düzenlemelerde konu ile ilgili yer alan hükümlere aykırı davranılmış olunacaktır. Özellikle yüz tanıma özelliği olan kameralar bireylerin değişmez yapıdaki kişisel verilerini elde ettiğinden fazla müdahaleci olarak tanımlanır ve orantısız kullanımları bireyler arasında eşitsizlik yaratan sonuçlar da doğurabileceğinden bu türden kameralara çok daha sınırlı-ölçülü-belirli şekilde başvurulması gerektiği savunulur[273]. Yüz tanıma cihazları kullanılarak belki eşkali aranan belli bir kişiye ulaşılabilir fakat bu

---

[271] YÜKSEL, S. (2012) "Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale". İstanbul: Beta Yayıncılık.s. 9-28.

[272] AİHM. Antovic ve Mirkovic v. Karadağ, Başvuru No: 70838/13, Karar Tarihi: 28.11.2017, (Erişim Tarihi: 13.08.2022) https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-11757%22]}

[273] URQUHART, L., & MIRANDA, D. (2021). "Policing faces: the present and future of intelligent facial surveillance". Information and Communications Technology Law ,s.8. https://doi.org/10.1080/13600834.2021.1994220

yöntemle herkesin biyometrik verisi elde edilmiş olacağından yepyeni güvenlik sorunları ve ihlaller ortaya çıkmış olacaktır[274].

Olası başka insan hakları ihlallerine sebep olmamak için bu teknolojiler kullanılmadan önce aynı amaca daha az risk barındıran bir yöntemle ulaşmanın mümkün olup olmadığı, cinsiyet, ırk, engellilik gibi yeni şüphe ve risk kategorileri yaratılmaması, özel sektörün bu cihazları kullanmasının kontrolünün sağlanması, yüz tanıma verilerine yetkisiz erişimin engellenmesi, kolluk kuvvetlerinin ve halkın olası risklere karşı bilgilendirilmesi gibi bir dizi kurala riayet edilmesi gerekir[275].

Gary Gumpert ve Susan J. Drucker yaygın gözetimi bir "zihniyet", gözetimden korunmayı da bir "hak" olarak görür[276]. Gözetim zihniyetinin uygulanmasındaki bariz çelişki ise; bir taraftan güvenlik ihtiyacı teşvik edilirken diğer taraftan mahremiyet hakkının/gizliliğin korunması çağrısıyla dolu olan yasalar yapılmasıdır[277]. Özellikle demokrasi ve insan hakları bağlamında yoğun kaygılara sebep olan ülkeler için bu çelişkinin olduğunu söylemek fazla iyimser bir ifade olacaktır. Çin'de kullanılan kameraların etnik olarak farklı olan Uygur ve Tibet mahallelerinde veya siyasi muhaliflere karşı hedefli şekilde kullanımı[278] insan hakları açısından çok ciddi sonuçlara gebedir.

Alanur Çavlin Bozbeyoğlu ise; insan hakları ve video gözetim eleştirisini neo-liberalizm üzerinden yapar. Güvenlikle ilgili artan endişelerin kameraların da artmasına sebep olması ile ortaya çıkan mahremiyet sorunları diğer sosyal haklarda olduğu gibi

---

[274] Ibid.
[275] Ibid, s.23-25.
[276] GUMPERT, G., & DRUCKER, S. J. (2001). "Public boundaries: Privacy and surveillance in a technological world. Communication Quarterly", 49(2), s.125. https://doi.org/10.1080/01463370109385620
[277] Ibid.
[278] DOYLE, A., LIPPERT, R., & LYON, D. (Ed.). (2012). "Eyes Everywhere The global growth of camera surveillance". Routledge.s.4.

erozyona uğramış, neo-liberal dönemde mahremiyet, güvenlik adına feda edilmiş ve temel bir insan hakkı olarak önemini yitirmiştir[279].

2.6.4. Hukuki Güvenliği Sorgulayan Argümanlar

Bir çalışmada günümüzde güvenliğin CCTV'lerin yaygınlaşması açısından banal hale gelmesinden bahsedilerek, esas güvenliğin beşerî olan altyapıya duyulan güven ile elde edilebileceğinden, güvende hissetmenin bireyleri güvence altına alan hukuki düzenlemelere duyulan güven ile sağlanacağı ve ancak böyle bir güvenin hem bireyselliği hem de toplumsallığı koruyacağı ifade edilir[280]. Çalışmada kullanılan "*banalité*" sözcüğü gelişigüzel bir seçim gibi görünmemektedir. Nitekim bireyleri güvence altına alan cihazların bu denli yaygın hale getirilerek sıradanlaştırılması, aynı zamanda hedeflenen güvenliğin altını oymak için gerekli koşulları da yaratmak anlamına gelebilecektir[281]. CCTV'lerin de sıradan hale getirilmesiyle, toplumların güvenlik düzenlemeleri bu cihazlar üzerinde kurulu olup, cihazların yaygınlığı artık güvenlik denetiminin ötesine geçmektedir ki bu durum sadece güvenliğin değil, aynı zamanda demokratik yönetişimin, onun kalitesinin ve ona erişimin de zarar görmesine sebep olur[282].

Bu savın, kameraların işlevselliğine yöneltilen sorulara ve çekincelere karşı onların etkinliğinin gerektiği ölçüde tartışılmayıp, genellikle suçu önleme veya suçlu takibi gibi argümanların ortaya konulduğu temel alınarak yerinde olduğu ifade edilebilir. Üçüncü bölümde ele alındığı üzere, yapılan video gözetim faaliyetleri açısından hukuki düzenlemelerde yer alan "ölçülülük, meşru sebep, suç işlenmesinin önlenmesi, kamu güvenliği" gibi sebepler ile kişisel verilerin korunması bakımından hukuka uygunluk sağlanmış olacak mıdır? Bunların yanında video gözetim sistemlerinin ne ölçüde etkin olduğu, suç rakamlarını ne kadar azalttığı, suçtan caydırıcılıkta işe yarar olup olmadığı gibi soruların da sorulması ve meşru sebeplerin bunlara verilecek cevaplara göre yerine

---

[279] BOZBEYOĞLU, A.Ç. (2012) "The Electronic Eye Of The Police:The provincial information and security system in Istanbul".
[280] GOOLD, B., LOADER, I., & THUMALA, A. (2013). "The banality of security: The curious case of surveillance cameras". British Journal of Criminology, 53(6), s.992-994. https://doi.org/10.1093/bjc/azt044
[281] Ibid.
[282] Ibid.

getirilmiş sayılması gerekir. İşte "güvenliğin banalleşmesi" ile ifade edilen, bu tartışma konularının adeta bir dev kaya haline gelen kamera sistemleri karşısında küçük birer taş olarak kalmasıdır.

Norris ve Armstrong'a göre; CCTV'nin suçu azaltıp azaltmadığını sorgulamanın yanında, onun suçun önlenmesinden daha fazlası da olan, operatör kararlarının neye göre verildiği, cihazların hangi noktalarda hangi davranış biçimleri karşısında "şüphe" üzerine konuşlandırıldığı, bu konuşlandırmanın açıkça suçla ilgili kaygılarla mı sınırlı yoksa kamusal alanda görgü ve tavır konularını düzenlemeye ve belirli insan tiplerini dışlamayı amaçlamaya mı yaradığını tespit etmek gerekir[283]. Ayrıca CCTV sistemlerinin kullanımında gerçekten kimin çıkarlarının desteklendiğini sorgulamak, kamusal alandaki kullanımlarda iş dünyasının çıkarların ne derecede olduğunu saptamak, CCTV sistemlerinin kullanımına karşı "rızanın" toplum tarafından ne ölçüde ve nasıl "üretildiğine" odaklanmak gereklidir[284].

Bu açıdan gözetimin bir iktidar biçimi olarak ele alınarak, bu gücün nasıl hesaba katıldığını ve işleyişine hangi sınırların niçin getirildiğinin analizine ihtiyaç vardır ki burada gerekli başlangıç noktası olarak ele alınacak hukuk kurallarının "kitaplardaki kural olma"nın ötesine geçerek, yasaların eylem halinde ele alınması ve bu kurallara ne ölçüde uyulduğunun incelenmesi gerekir[285]. Üçüncü bölümde çerçevesi çizilen, video gözetim cihazlarına karşı oluşturulan hukuk kurallarının, bireylerin kişisel verilerinin, mahremiyetlerinin ve özel hayatlarının korunmasını sağlayıp sağlamadığına ilişkin "şüpheci" argümanlar, esasen gözetimin veya dijitalizasyonun küreselleşmesine, "kamu düzeni", "kamu güvenliği", "meşru sebepler" gibi ifadeleri içeren hukuk kurallarının geniş yorumlanabilmesine dayanır.

Bireylerin devletin yaygın gözetime karşı korunmasını sağlayan, devletleri "sınırlandıran" hukuk kurallarının kapsamına dahil olan meşru menfaat sebeplerinin tanımlanmasındaki özgürlüğün sınırının, video gözetim bakımından nasıl çizildiği açık

---

[283] NORRIS ve ARMSTRONG, 1999, s.10.
[284] Ibid.
[285] Ibid, s.10-11.

değildir. Bir temel hakkın uzantısı veya "yüzü" olan kişisel verilerin korunmasını isteme hakkının, hukuk kurallarında yer alan meşru gerekçeler ile sınırlanmasında kuralların oluşturulma amacındaki perspektife veya temel gayeye dönülmesi gerekecektir. Özellikle devletlerin kitlesel kameralı gözetim faaliyetleri bakımından yerine getirilen "kanunilik şartı"nın, hali hazırda yalnızca ihdas edilmiş bir kanun hükmünün bulunması şeklide yorumlanmasının, kişisel verilerin veya özel hayatın korunmasına yetmeyeceğini ifade etmek gerekir.

GDPR'ın sağladığı hukuki güvence, günümüzde özellikle yapay zekâyı da kapsamına alan kameraların kullanımı yönünden sorgulamalar doğurmaktadır. Düzenlemenin gözetim toplumunun inşasını durdurmayıp onu yasallaştırdığı, yüz tanıma teknolojisi ile biyometrik verilerin toplanmasının vatandaşların açık rızası olmadıkça yasaklandığı fakat suçla mücadelede olduğu gibi kamu yararının sağlanması açısından getirilen istisnaların adeta genel kural haline gelmesi tartışma konusu edilmektedir[286]. İfade edilen husus, GDPR kapsamındaki istisnaların uygulamasının genişliği, istihbarat servisleri ile kolluk kuvvetlerinin kullanabildiği cihazların birçok şirket ve mülk sahibi tarafından da kullanıma açık hale gelmesi riski olduğudur[287].

Diğer taraftan kısaca kişisel verilerin korunmasının sağlanması (hukukun işlerliği) ve düzenleyici işlemler tesis etmek için kurulan, sayıları da her geçen gün artan veri koruma otoritelerinin eylem ve işlemlerinin de bazı "ikircikli" durumlara sebep olduğu öne sürülmektedir. Örneğin, İsveç veri koruma otoritesinin, öğrenci katılımını kaydetmek için yüz tanımayı kullanması sebebiyle bir liseye para cezası uygulaması ancak bu kullanımın yasa dışı olmadığına karar vermesi; Fransız veri koruma otoritesi CNIL'in ortaokullarda yüz tanıma sistemlerinin kullanımının yasalara aykırı olduğuna karar vermesi ancak hükümetin zorunlu ulusal dijital kimlik programı için yüz tanımayı

---

[286] HARE, S. (10.11.2019). "These new rules were meant to protect our privacy:they don't work". The Observer. (Erişim Tarihi: 10.08.2022) https://www.theguardian.com/commentisfree/2019/nov/10/these-new-rules-were-meant-to-protect-our-privacy-they-dont-work

[287] Ibid.

kullanma planına itiraz etmemesi gibi olayların tutarlı bir koruma sunmaktan uzak olduğu belirtilmektedir[288].

Bugün kamuya açık alanlarda da özel hayatın ve mahremiyetin-sınırlı da olsa-bulunduğu kabul edilmektedir. Bunun yanında, devletler hangi politikaları benimsemiş olursa olsun, kişisel veriler insan yaşamı üzerine doğrudan yansımaları olan ve bazı özel ilkelere göre elde edilmesi gereken bilgiler olarak, herhangi bir veri türüymüş gibi ele alınmamalıdır[289]. Peki birer kanun hükmü şeklinde tezahür edecek bu ilkeler nasıl olmalıdır ki aynı anda hem veri güvenliğinin sağlanmasını hem kişisel verilerin yetki, şekil ve sebep yönlerinden uygun biçimde elde edilmesini hem de hükümlerin doğuşundaki amacı koruyarak devletin amaçladığı güvenliğin sağlanmasına da hizmet etsin? Bu soruya hali hazırda verilen cevapların Avrupa ve Amerika'da farklı olduğunu Çin gibi totaliter eylemlerin açıkça gerçekleştirildiği ülkelerde ise daha çok uygulanış ve denetim yönünden "bambaşka" olduğunu belirtmek gerekir.

Bu durumda hemen her yerde aynı tanıma sahip kişisel verilerin hukuk aracılığı ile korunmasının da neredeyse benzer kurallar ile yapılması beklenmez mi? Bu farklılıklar mahremiyet koruma çabalarıyla savunulması gereken, temelde korunan "menfaatler" ile kaçınılması gereken en "kötü" senaryoların da ülkeden ülkeye değiştiği anlamına mı gelir? Rule bu soruya olumlu yanıt verir. İşte bu çalışma ile amaçlanan da mer'i hukukun politik stratejilerden de etkilenen sosyal bir disiplin olarak, bireylerin kamusal alanda kameralara karşı mahremiyetleri tesis etmeye tek başına yeterli olmayabileceğini ortaya koymaktır. Nitekim "güvenlik sağlama amacı" kimi ülkelerde vatandaşlık skoru ile sağlanmaya çalışılırken, kimi ülkelerde ise devletlerin kendisini çok daha fazla sınırlamayı kabul ettiği bir eksenden ilerler. Belirtmek gerekir ki Rule yukarıdaki soruya verilebilecek olumlu cevap sonrasında çıtayı daha da yükselterek, polisin ve kolluk

---

[288] Ibid.
[289] RULE, J. B., & GREENLEAF, G. (2008). "Global privacy protection: The first generation". In J. B. Rule & G. Greenleaf (Eds.), Global Privacy Protection: The First Generation. Edward Elgar Publishing. s.1-5.

kuvvetlerinin özellikle "isimsiz" veya "güçsüz" nüfusları, kimin tam olarak kim olduğunu bilmek için gözetlediğini de iddia eder[290].

Bir başka çalışmada, veri koruma ve insan hakları mevzuatlarının, bir dereceye kadar kamera gözetiminden kaynaklanan mahremiyet ve güvenlik konularını ele aldığı ancak yalnızca yasal hükümlerin varlığının, gözetim sistemlerinin güvenilirliği ile aynı anlama gelmeyeceği savunulur[291]. Zira düzenlemelerin kişisel verilerin toplandıktan sonra korunmasını değil, bilhassa toplanmasını ele alarak daha yeknesak bir şekilde temel hak ve özgürlükleri koruması beklenir. Ülkeden ülkeye farklılaşan, yerleşik olmayan demokrasilerdeki gayri meşru sayılabilecek yasalar ihdas edilmesi ise; bu yeknesaklığın sağlanmasını zorlaştırmaktadır. Ayrıca veri koruma alanında oldukça ileride olan AB'de var olan yasalara rağmen hükümetlerin kitlesel izlemelere devam ettiği iddiaları, ABAD kararları ile ulusal mevzuatın çatıştığı durumlarda kişisel verilerin korunması hukuku alanındaki güvenliğin ve rejimlerin sorgulanmasına sebep olmaktadır[292].

---

[290] Ibid, s.5.
[291] DOYLE, A., LIPPERT, R., & LYON, D. (Eds.). (2012).,s.14.
[292] MANANCOURT, V. (06.07.2022) Europe's state of mass surveillance. Politico. (Erişim Tarihi: 02.10.2022) https://www.politico.eu/article/data-retention-europe-mass-surveillance/

3. BÖLÜM

KAMUSAL ALANDA VİDEO GÖZETİM ve KİŞİSEL VERİLERİN KORUNMASI HUKUKU

Ana caddeler, sokaklar, meydanlar, parklar, istasyonlar ve diğer "halka açık" alanlarda, kameralar aracılığıyla yapılan izlemelerin hukuki dayanağı nedir? Bu izlemelerin yapılmasını talep eden, izlemeler sonucu elde edilen görüntüleri elinde bulundurmaya hangi kişi veya kurumlar yetkilidir? Kullanılan cihazlar ile yüz tanıma gibi yenilikçi ve görece daha riskli teknolojiler kullanıldığında hangi ek güvenceler sağlanır?

Bu başlık, yukarıda yer alan eleştiriler ve yapılan sorgulamalara karşı video kayıt sistemlerinin yaygın kullanımına yönelik hukuki dayanakları ortaya koyma amacı taşımaktadır. Bu şekilde ilk bölümde izah edilen temellendirme üzerine ikinci bölümde ele alınan riskler ve eleştirilerin karşısında hangi hukuk normlarının yer aldığı ile temel hak ve hürriyetlerin hangi güvencelerle korunduğu, kişisel verilerin korunması hukuku boyutuyla ele alınacaktır. Son olarak hukuk kurallarının ne tür bir yaklaşım ile yorumlanması gerektiği ve video gözetim konusunda tek başına işlevli olup olmadığı sorgulanacaktır.

3.1. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GENEL KAPSAMI VE TARİHSEL GELİŞİMİ

Hukukun nasıl değiştiğini ve hukuktaki değişimleri gözlemleyebilmek için, hem ortaya çıkmayı bekleyen değişikliklerin izini sürmek hem de hukuk normlarını neyin oluşturduğuna bakmak gerekir[293]. Bu izlerin tam olarak açığa çıkarılması mümkün olmasa da var olan belirli eylemlerin açıklanmasına yardımcı olması durumunda amacın

[293] FUSTER, G.G. (2014). "The Emergence of Personal Data Protection as a Fundamental Right of the EU". Brussel: Springer.s.13.

gerçekleşmiş sayılabilmesi söz konusu olabilir[294]. Böyle bir yaklaşımla kişisel verileri koruma hukukunun bir bütün halinde ele alınmadan önce, "bir temel hak olarak kişisel verilerin korunmasını isteme hakkı" ortaya konulmalı, alandaki hukukun gelişimi incelenmelidir.

3.1.1. Kısa Tarihsel Gelişim ve Hukuki Korumanın Artan Kabulü

Kişisel verilerin korunmasına yönelik düzenlemeler amaç bakımından oldukça eskidir. Öyle ki hekimlerin hastalarının kişisel bilgilerini "sır saklama yükümlülüğü" ilkesi yani "Hipokrat Yemini" altında saklaması M.Ö. 5. yüzyıldan beri geçerliliğini korumaktadır[295]. Dolayısıyla yüzyıllardır çeşitli meslek gruplarında yine meslek sebebiyle edinilen bilgilerin saklanması gerektiği kabulü, kişilerin itibarlarının, finansal durumlarının, sosyal faaliyetlerinin kısacası kendilerinin korunması için sağlanmıştır denilebilir. Hal böyle olmakla birlikte kişisel verilerin korunması hukuku yeni sayılabilecek bir alandır ve kendine has dinamik yapısı ile medeni hukuk, ceza hukuku, idare hukuku gibi pek çok temel hukuk dalı ile ilişkili olarak gelişimine devam etmektedir.

Mahremiyetin dönüşümü, devletlerin gözetimi gibi yapısal olarak kişisel verilerin korunması hukukunun oluşumunda etkileri olan hususlara çalışmanın birinci bölümünde değinildiğinden bu bölümde salt hukuk kuralları ele alınmıştır. Bu "yeni" hukukun doğması, mahremiyet kavramının dönüşümünden koparılarak ifade edilmemelidir. Zira çok yönlü mahiyeti ile mahremiyet, aslında korunan menfaatin ta kendisidir.

Mahremiyete dair endişeler, bilişim sistemleri günümüzdeki boyutunu almadan önce henüz 1948 yılında BM İnsan Hakları Evrensel Beyannamesi'nin 12. Maddesinde[296] yerini bulmuştur. Maddeye göre bireylerin özel hayatlarına keyfi olarak karışılamayacağı ve özel hayatın olası müdahalelere karşı yasalar ile korunacağı düzenlenmiştir. AİHS'in

---

[294] Ibid.
[295] KÜZECİ,2021, s.115.
[296] "Universal Declaration of Human Rights",(Erişim Tarihi:19.11.2022)

8. maddesinde ise özel hayata karşı müdahalede bulunulmaması aynı paralelde yer almış ve bu hakkın kamu makamınca sınırlandırılmasında, kanun ile belirtilme, suç işlenmesinin önlenmesi, milli güvenlik, kamu güvenliği, ekonomik refahın sağlanması ve düzenin korunması gibi şartları zorunlu kılmıştır. Yeri gelmişken tıpkı Anayasamızın 13. maddesinde olduğu gibi AİHS'in 8. maddesine göre de video gözetim ile kamusal alanlardaki özel hayata getirilen sınırlamaların kanun ile yapılması gerektiğini belirtmek gerekir. 1969 yılında imzalanan Amerikan İnsan Hakları Konvansiyonu'nun 11. maddesi de aynı doğrultudadır[297].

Bu alandaki hukukun oluşmasına zemin olan gelişmelere bakıldığında karşımıza ilk olarak Almanya çıkar. Sonradan "veri koruması" olarak İngilizce'ye çevrilecek olan ve Almanca "Datenschutz" adını taşıyan ilk yasal belge, 1970'te Almanya'nın federal eyaletlerinden biri olan Hessen tarafından onaylanmış, Hessen Veri Koruma Yasası, eyaletin hükümet dosyalarında saklanan bilgileri nasıl kullanacağını düzenlemiştir[298]. Bu yasa Datensicherung veya Datensicherheit (veri güvenliği) gibi daha önce mevcut Alman yasal terimleri tarafından açıkta kaldığı düşünülen bir dizi güvenlik önlemini de sağlayarak, tüm Avrupa'yı etkilemiş, kavram diğer yasalara da veri koruma ve buna benzer ifadelerle girmiştir[299].

Akabinde Almanya'da federal çaptaki düzenleme olan 28 Ocak 1977 tarihli Federal Veri Koruma Kanunu (*Bundesdatenschutzgestez*), Fransa'da 6 Ocak 1978 tarihli 78-17 sayılı Veri Koruma Yasası (*la loi Informatique et Libertés*), Avusturya'da 1980 ve İsviçre'de 1992 yıllarında yürürlüğe giren federal düzeydeki kanunlar, Birleşik Krallık'ta ise 1998 yılında yürürlüğe giren Veri Koruma Kanunu (*Data Protection Act*) ile git gide yayılan bir hukuki koruma kültürü oluşmaya başlamıştır.

---

[297] "American Convention on Human Rights", (Erişim Tarihi:20.09.2022). https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm .
[298] FUSTER, 2014, s.56
[299] Ibid.

3.1.2. Kişisel Veri Kavramında Yeknesaklık

Uygulamada ve öğretide kabul edilen, kişisel verinin kapsamını net olarak belirlemenin zor olduğu ve böyle bir çizgi çizmenin kişisel verilerin korunmasını talep hakkının sınırlarını daraltabileceği, belirli veya belirlenebilir nitelikte ve "kişilere mündemiç" olan her türlü bilginin kişisel veri olduğu yönündedir. Dolayısıyla kişinin görüntüsü ve görüntüsünde onu belirlenebilir kılan özel unsurlar, yürüyüşü gibi kişi ile ilişkilendirilebilecek her türlü bilgi kişisel veri sayılmalıdır. Yine başka örneklendirmeler yapmak gerekirse; kameraların tanınabilir kıldığı yani açıkça görüntülenebilen bireylere ilişkin elde edilen görüntüler, müşterilerce bankalara onay verirken kaydedilen ses, kişileri belirlenebilir hale getiren çizimler kişisel veri kapsamındadır[300].

Tüm bu bilgileri değerli kılan hususlar, bunların hem kişilerin toplumsal bir özne olarak hangi kişisel tercihlerinin olduğuna veya daha genel bir ifade ile "özel hayatlarına" dair olmaları hem de tamamen kendi tekellerinde olan giz alanlarının kontrolünü kapsamalarıdır. Yani bahis konusu olan, kişisel verilerin kişilerin kamusal veya kamusal olmayan alandaki yansımalarının dış dünyaya karşı korunmasıdır. Kamusal alanda bulunulduğunda da mahremiyetin tamamen sona ermeyeceğine yönelik genel kabulün hatırlatılmasında isabet vardır.

Kişisel verilerin tanımını yapan uluslararası belgelere bakacak olduğumuzda ilk olarak 1980 tarihli "OECD'nin Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri" karşımıza çıkmaktadır ki bu rehberde kişisel veriler, belirli olan ya da belirlenebilen kişiye dair bilgi olarak tanımlanmıştır[301]. Akabinde Avrupa Konseyi çatısında akdedilen 1981 tarihli 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nde ise (108 nolu

---

[300] Kişisel Verileri Koruma Kurumu Yayınları (Haziran 2019). "Örneklerle Kişisel Verilerin Korunması, No 29". (Erişim tarihi:25.04.2021) , https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a23bfe08-9b3a-4c2f-8a97-a259dcc0e667.PDF,s.2.

[301] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (Erişim Tarihi: 25.04.2021)

Sözleşme)[302] kişisel veri kavramının 1980 tarihli OECD rehber ilkelerinde belirtilen tanım ile birebir aynı olduğu görülmektedir.

Günümüzde kişisel verilerin korunması alanında temel kabul edilen ve 2016 yılında AB tarafından kabul edilip 2018'de yürürlüğe giren GDPR tarafından yürürlükten kaldırılan 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi" de konunun kapsamını tespit etmek bakımından önemlidir. 1995 yılında kabul edilip 1998'de yürürlüğe girmiş olan bu metinde de kişisel verilere ilişkin OECD Rehber İlkeleri'ndeki tanım aynen kabul edilmiş*;* veri sahibi *(data subject- 6698 sayılı Kişisel Verilerin Korunması Kanununa göre ilgili kişi)* ise; *"özellikle bir kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen kişi"* olarak ifade edilmiştir[303].

96/46/EC sayılı Direktif temel alınarak hazırlanan KVKK ise ondan önceki düzenlemelerde belirtilen tanımları benimsemiş ve kişisel verileri 3. maddesinin birinci fıkrasının (d) bendinde; *"kimliği hali hazırda tanımlanmış ya da tanımlanması mümkün olan gerçek kişiye dair her türlü bilgi"* şeklinde belirtmiştir. Böylece elimizde, "kişisel veriye ilişkin belirli veya belirlenebilir gerçek kişi" ve bu "kişiye ilişkin tanımlama veya ilişkilendirme yapmaya yarayan bir faktör" şeklinde iki grup tanımlama aracı kalmış olur.

---

[302] Council Of Europe (1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[303] Official Journal of The European Communities Directive 95/46/EC Of The European Parliament And Of The Council (1995), On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data.

3.1.3. Temel Uluslararası Düzenlemeler

3.1.3.1. OECD Rehber İlkeleri

1970'lerin sonundan itibaren ülkeler ve uluslararası kuruluşlar arasında oluşan iş birliği, ABD de dahil olmak üzere Avrupalı ve Avrupa dışındaki ülke ve toplulukları bir araya getirmiş, bu şekilde iki temel iç içe geçmiş düzenleme olan 1980 tarihli OECD Rehber İlkelerinin ve 108 sayılı Sözleşme'nin oluşmasını sağlamıştır[304]. Vatandaşlar ile kamu otoritelerini bir araya getirerek, birlikte çeşitli sosyo-ekonomik durumlar hakkında uluslararası standartlar oluşturmayı amaçlayan OECD[305] hem ABD hem de Avrupa ülkeleri tarafından üzerinde mutabık kalınan ilk uluslararası ilkeler beyanı olan 23.09.1980 tarihinde kabul edilen ve 2013 yılında güncellenen Özel Yaşamın Korunmasına ve "Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler"i *(Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)* oluşturmuştur. Düzenlemenin amacı ise; kişisel verilerin artan kullanımından kaynaklanan endişeleri ve sınır ötesi bilgi akışındaki kısıtlamalardan kaynaklanan küresel ekonomilere yönelik riskleri ele almak olarak belirtilmektedir[306].

Rehber İlkeler'e baktığımızda karşımıza birbirini tamamlayan, veri elde etmede sınırlama, veri kalitesinin sağlanması, amaçta belirlilik, sınırlama ilkesinin kullanılması, güvenlik önlemlerinin alınması, açıklık, bireysel katılımın sağlanması, hesap verilebilirlik gibi temel ve bugün hemen her kişisel verileri koruma mevzuatında yer alan ilkeler çıkar[307]. Bu ilkelerden veri elde etmeye ilişkin sınırlama, kişisel verilerin ancak verinin sahibinin rızası ile toplanması eğer rıza yoksa ancak belirli yasal sınırlar dahilinde hareket edilmesi gerektiğini ifade eder. Yine veri kalitesi ilkesine göre; verilerin kullanım amacıyla ilgili, gerekli olduğu şekilde doğru, noksansız ve güncel tutulması gerekecek,

---

[304] Ibid., s.75.
[305] OECD, Who we are, https://www.oecd.org/about/ (Erişim Tarihi 18.08.2022)
[306] OECD Legal Instruments, Background information.
[307] OECD Legal Instruments, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

kişiler ile ilgili olduğu zannını uyandıran yanlış veriler onlarla eşleştirilemeyecektir. Bu noktada, yüz tanıma cihazlarının yanlış eşleştirme yaptığı bazı örneklerde, kişilerin mağduriyetlerine yol açıldığı hallerde (yanlış yere suçlanma gibi) bu ilkenin sağlanmamasının doğurduğu sonuçlarla yüzleşmek zorunda kalınmaktadır. Bu sebeple kişisel verilerin elde edilmesinde bir genel ilke olarak veri kalitesinin sağlanması, hak kayıplarının önüne geçmek açısından oldukça önemlidir.

Rehber İlkeler kontrolörlere de (*data controllers- KVKK'ya göre veri sorumlusu*), faaliyetlerini verilerin elde edilmesinde gizlilik risk değerlendirmesi ve çeşitli tasniflere göre uyarlama yapma, iç denetim ve yönetim mekanizmaları ile veri güvenliğini sağlama, veri sahiplerine yönelik ayrımcılıkları önleme maksadıyla çeşitli ölçütler getirme gibi çeşitli görevler yükler. Üye ülkeler açısından bağlayıcı olmayan OECD Rehber İlkeleri konu kapsamında yeni düzenlemelerin önünü açması ve bu düzenlemelerin kapsamını belirlemesi bakımından oldukça önemlidir[308]. Bu ilkeler, sadece Avrupa'da değil, Japonya, Yeni Zelanda, Hong Kong, Avustralya gibi pek çok ülkede yapılan düzenlemeler üzerinde de etkin olmuştur[309].

3.1.3.2. Birleşmiş Milletler'in Düzenlemeleri

1948 yanında kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi ile aynı doğrultuda, 1976 yılında yürürlüğe giren *"Siyasi ve Medeni Haklar Uluslararası Sözleşmesi-International Covenant on Civil and Political Rights"* mahremiyet hakkını 17. maddesinde ele alır[310]. Bunun yanında BM İnsan Hakları Komitesi'nin bu maddeye 16. genel yorumu ile bir izah getirdiği, bu izahta gerek kamu otoritelerinin gerek özel kişilerin elde edip saklaması gereken kişisel verilerin bir düzenlemeye tabi olması gerektiği, bireylerin verilerinin saklanması karşısında birtakım hakları olduğu, kişisel verilerin gizliliğinin ve korunmasının sağlanması gerektiği belirtilmiştir[311]. Ayrıca

---

[308] KÜZECİ,2021, s.131.
[309] Ibid, s.132.
[310] "United Nations Human Rights. International Covenant on Civil and Political Rights". (Erişim Tarihi:19.08.2022) https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[311] University of Minnesota, Human Rights Library, (Erişim Tarihi:19.08.2022) http://hrlibrary.umn.edu/gencomm/hrcom16.htm

Komite kişisel verilerin korumasını kişilerin şeref ve itibarının korunması ile bağlantılı olarak görmüş, devletlerin veri koruma yolları sağlama yükümlülüğünün denetlenmesinin öneminden bahsetmiştir[312]. Komite'nin 1988 yılındaki 23. oturumu ile varılan bu görüş, güncel kişisel verilerin korunması hukukunun da temelindedir ve hatta varlık sebebidir.

1990 yılına gelindiğinde ise BM'nin "*45/95 sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler-Guidelines for the Regulation of Computerized Personal Data Files*" düzenlemesi büyük bir yankı uyandırmıştır. Düzenlemenin "genel yorum ve öneriler" bölümünde; insan haklarının kişisel verilerin/bilgilerin dijitalleşmesinden etkilendiği ön kabulü ile mahremiyet kavramının her hukuk sistemine özgü özelliklere sahip olduğu ve mahremiyet ihlalinin bireyleri günlük sosyal yaşamlarında da (çalışma koşulları, toplu faaliyetler…) tehdit edilebileceği vurgulanmıştır[313].

BM Rehber İlkelerinin düzenlenme sebebinin ise; ülkeler arasındaki ve ulusal düzenlemelere yeknesaklık getirmek olduğunu söyleyebiliriz. Ülkelerin ulusal hukuklarında uymaları tavsiye edilen kurallar ise; doğruluk, güncellik, amaçsal belirlilik, veri sahibinin erişimi, ayrımcılık yapmama, ulusal hukukta belirli yasal sebepler ile istisnalar getirebilme, veri güvenliğini sağlama olarak sayılabilir. Ek olarak denetleme ve yaptırım, sınır ötesi veri akışı gibi konulara da değinilmiştir. Yıllar içinde git gide büyüyen alandan deyim yerindeyse elini çekmeyen BM, bünyesinde 2016'da özel yaşamın gizliliği hakkında özel raportör raporu yayınlanmıştır[314].

3.1.3.3. Avrupa Konseyi ve Avrupa Birliği: Alanı Domine Eden Düzenlemeler

Kişisel verilerin korunması hukuku alanında en geniş çerçeve Avrupa Birliği tarafından çizilmiştir. Zira topluluk içinde geçerli olan hem temel insan haklarını koruyan daha genel

---

[312] Ibid.
[313] United Naitons Digital Library, (1988) "Guidelines for the Regulation of Computerized Personal Data Files: final report / submitted by Louis Joinet, Special Rapporteur." (Erişim Tarihi:19.08.2022) https://digitallibrary.un.org/record/43365?ln=en
[314] KÜZECİ,2021.s.138.

mahiyetli anlaşmalar hem de münhasıran özel konular (yapay zekâ, çerezler, kameralar, online eğitim, dijital reklamcılık/pazar vs.) doğrultusunda yapılmış düzenlemeler mevcuttur. Bu noktada AİHS'in 8. maddesi uyarınca, "bir kişinin kişisel verilerinin işlenmesi karşısındaki korunma hakkı, özel ve aile hayatına, konutuna ve yazışmasına saygı hakkının bir parçasını" oluşturur[315]. Ayrıca *"AB'nin İşleyişine İlişkin Antlaşma-The Treaty of the Functioning of the EU"* 16. maddesinde de kişisel verilerin korunması açıkça koruma altına alınmış, Avrupa Parlamentosu ve Konseyine, olağan yasama usulüne göre belirlenen şekilde, kişisel verilerin birlik kurumları, organları ve sair birimleri ile üye devletler tarafından işlenmesine ilişkin olarak bireylerin korunmasına ilişkin kuralları belirleme görevi verilmiştir[316].

1970'lerin ortalarından itibaren, Avrupa Konseyi Bakanlar Komitesi, AİHS'nin 8. maddesine atıfta bulunarak kişisel verilerin korunmasına ilişkin çeşitli kararlar almış ve düzenlemeleri kabul etmiş, 1981 yılına gelindiğinde ise 108 sayılı Sözleşme veri koruma alanında yasal olarak bağlayıcı olan ilk uluslararası belge olarak kabul edilmiştir[317]. 108 sayılı Sözleşme yargı ve kolluk kuvvetleri tarafından yapılan veri işlemeler dahil olmak üzere özel sektör ve kamu tarafından gerçekleştirilen tüm faaliyetler için geçerli olup bireyleri kişisel verilerin işlenmesine eşlik edebilecek suiistimallere karşı koruyarak kişisel verilerin uluslararası aktarımına sınırlar/kurallar getirmeyi amaçlar[318].

Kişisel verilerin işlenmesiyle ilgili olarak, sözleşmede belirtilen belirli meşru amaçlar için verilerin adil ve yasal olarak toplanması, gerekenden daha uzun süre saklanmaması, veri kalitesinin sağlanması gibi kişisel verilerin korunmasına yönelik temel ilkeler bulunmaktadır. Onaylayan devletler için bağlayıcı olan 108 sayılı Sözleşme ayrıca, imzacı ülkeler arasındaki veri akışını düzenleyerek, eşdeğer korumayı sağlamayan ülkelere yapılan kişisel veri akışlarına kısıtlamalar getirir.

108 sayılı Sözleşme'nin yenilenme ve modernize edilme çabaları devam etmektedir. Ayrıca belgede 2001 yılında yapılan değişiklikle, 1999 yılındaki temel

---

[315] "Handbook On European Data Protection Law" (2018) Poland: Drukarnia Interak Printing House. s.17.
[316] Consolidated version of the Treaty on the Functioning of the European Union, Part I, Title II, art.16.
[317] "Handbook On European Data Protection Law" (2018) Poland: Drukarnia Interak Printing House.s.24 vd.
[318] Ibid.

katılım değişikliğinden sonra 108 sayılı Sözleşme'ye ek protokol kabul edilmiş, protokol ile üçüncü ülkeler olarak belirtilen taraflara sınır ötesi veri akışları ve ulusal veri koruma denetleme makamlarının zorunlu olarak kurulmasına ilişkin kurallar belirtilmiştir. Ayrıca teknolojideki ilerlemeler ve dolayısıyla yeni olası problemler karşısında devam eden çalışmalar sonucunda 2018 yılında 108 + olarak bilinen "Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Modernize Edilmiş Sözleşme" henüz yürürlüğe girmese de Bakanlar Komitesi tarafından kabul edilmiştir. Modernizasyon çabalarının sebepleri belgede; yeni teknolojilerin yaygınlaşan kullanımından kaynaklanan gizlilik sorunlarını bertaraf etmek, 108 sayılı Sözleşme'nin uygulanmasını ve takibini güçlendirmek, temel hak ve özgürlüklere daha "güvenceli" bir koruma sağlamak olarak ifade edilmektedir[319].

1995 yılından 2018 yılının Mayıs ayına kadar AB'de kişisel verilerin korunmasına yönelik temel yasal belge *"95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi-Veri Koruma Direktifi-Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*" olmuştur. Veri Koruma Direktifi 1995 yılında kabul edildiğinde hali hazırda yürürlükte olan 108 sayılı Sözleşme'de bulunan veri koruma ilkeleri kabul edilmiş ve genişletilmiştir. GDPR'ın yürürlüğe girmesiyle uygulamadan kalkan Veri Koruma Direktifi'nde belirtilen veri işlemede uyulması gereken temel ilkeler, 108 sayılı Sözleşme'ye paralel olarak; *"kişisel verilerin verilerin doğru ve hukuka uygun işlenmesi, belirli, açık ve meşru amaçlarla işlenme, işlendiği amaçlar bağlantılı ve sınırlı olarak işlenme, güncel veya güncel duruma uygun olma, gerektiğinden fazla süre saklanmama"* şeklinde ifade edilmiştir.

Direktifte, veri işlemenin yasal sayılması için gereken şartlar yani işlenme şartları, hassas nitelikli verilerin işlenmesi, verisi işlenecek veri sahibini aydınlatma zorunluluğu, veri sahibinin hakları, veri güvenliği, kişisel verilerin üçüncü ülkelere aktarılması gibi

---

[319] Council of Europe,2018, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series No.223.s.1-2. (Erişim Tarihi: 05.09.2022) https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

pek çok husus bulunur. Veri Koruma Direktifi 6698 sayılı Kişisel Verilerin Korunması Kanunu hazırlanırken örnek alınmış, Anayasa Mahkemesi'nce de KVKK ile ilgili görülen bir iptal davasında ölçüt olarak kullanılmış, pek çok ABAD kararına konu olmuştur[320].

Kişisel verilerin korunmasını isteme hakkı 2000 yılında kabul edilip 2009 yılında bağlayıcılık kazanan Avrupa Birliği Temel Haklar Şartı'nda da yer almış, hakka "özel ve aile hayatına saygı" başlığından farklı bir başlıkta yer verilmiştir. Bu yorumlayış ve uygulama, özel hayatın gizliliği şemsiyesinden çıkarılan hakkın AB tarafından müstakil şekilde tanındığını açıkça göstermiştir. AB'de sektörel bazda da çeşitli direktif ve yönergeler çıkarılmaya devam etmektedir. Başlık altındaki maksat temel düzenlemelere değinmek olduğundan, bu özel düzenlemelere yer verilmemiştir.

"2016/679 sayılı ve 27 Nisan 2016 Tarihli Gerçek Kişilerin Kişisel Verilerin İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 95/46/EC sayılı AB Yönergesini Yürürlükten Kaldıran Avrupa Parlamentosu ve Avrupa Konseyi Tüzüğü -*Regulation EU 2016/679 Of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*" kısa anılışı ile GDPR, 2018 yılında yürürlüğe girdiğinden beri kişisel verilerin korunması alanı pek çok sahada yükselişe geçmiştir. GDPR, kişisel verilerin gizliliğini tüm Avrupa halkının temel hakkı olarak tanımlar, kişisel verilerin yaşam döngüsünü düzenler ve Veri Koruma Direktifi modernize ederek onu güncel koşullar ile harmonize hale getirmeyi amaçlar[321]. Bu sebeple hem özel sektör hem de kamu sektörünün kullandığı yeni teknolojilerin ve modellerin, büyük miktarda kişisel veriyi toplarken, kullanırken kısacası işlerken GDPR'da belirtilen kurallara uygun hale getirilmesi gerekir[322].

Oldukça kapsamlı olan düzenlemede; Veri Koruma Direktifi'nde yer alan kişisel verilerin işlenmesinde uyulması gereken temel ilkelere ek olarak uygun uygun teknik veya organizasyonel önlemler kullanılarak yetkisiz veya yasa dışı işlemeye ve sair

---

[320] DÜLGER, M. V. (2020) Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi, 3. Baskı, s. 96-97.
[321] ŠIDLAUSKAS, A. (2019). "Video Surveillance and the Gdpr. Social Transformations in Contemporary Society", 7, s.56.
[322] Ibid.

ihlallere karşı hukuka uygun işlemeyi temin eden "bütünlük ve gizlilik" ilkesi eklenmiştir[323]. Ayrıca 17. maddede yer alan unutulma hakkı, veri koruma etki değerlendirmesi, belirli ve ayrıksı veri işleme durumları hakkındaki hükümler, kişisel verilerin ihlali durumunda uygulanacak yaptırımlar, üçüncü ülkelere aktarım konusunda prensipler gibi pek çok yeni belirleme yer almaktadır. GDPR, insan müdahalesi olmadan kullanılan yapay zekâ uygulamaları için de bazı kısıtlamalar ve ölçütler getirmektedir[324]. Her ne kadar GDPR ile veri koruma alanında AB ülkeleri arasında uygulama yönünden bir yeknesaklık sağlanması amaçladıysa da gerçek korumanın yalnızca yasal çerçeveye değil aynı zamanda mevzuatın fiili olarak uygulanması, yorumlanması, mahkemeler ve Veri Koruma Otoriteleri (*Data Protection Authorities*) tarafından uygulanma biçimlerine de bağlı olduğu ifade edilmektedir[325].

Gerçekten, Avrupa Konseyi ve AB düzenlemeleri mahremiyet ve kişisel verilerin korunmasına ilişkin hem genel hem de sektörel pek çok norm içermekteyse de kuralların uygulanması hukuk sistemleri ve kültürlerdeki farklılıklar nedeniyle AB ülkeleri arasında farklılık göstermektedir[326]. Bir eleştiri de GDPR'ın davranışsal verilerin veri ekonomisi pazarında engellenmeden işlemeye devam etmesini mümkün kıldığı hakkındadır[327]. Buna göre; GDPR'a rağmen hem veri piyasasının doğası hem de bu tür verilerin ticaretinde bireylerin belirli (özel olarak) seçilen verilerinin kullanılarak yeni stratejilerin üretilmeye devam ettiği, düzenlemenin verilerin kötüye kullanılmasına karşı oldukça minör bir etki getirebileceği, büyük verinin şirketlerce yönetimi ve gözetiminin yarattığı sorunların devam ettiği ortadadır[328]. Kişisel verilerin korunması alanındaki en kapsamlı düzenleme olan GDPR'ın dahi bu sorunları çözmek açısından yeterliliğe sahip olmadığı iddiaları, kontrolörlerin temel ilkelere uyması ve açık rıza koşulunu sağlaması durumunda bile

---

[323] GDPR, md.5/1-f.
[324] LAYBATS, C., & DAVIES, J. (2018). "GDPR: Implementing the regulations". Business Information Review, 35(2), s.81. "
[325] CUSTERS, B., DECHESNE, F., SEARS, A. M., TANI, T., & VAN DER HOF, S. (2018). "A comparison of data protection legislation and policies across the EU". Computer Law and Security Review, 34(2), s.235.
[326] Ibid.
[327] ANDREW, J., & BAKER, M. (2021). "The General Data Protection Regulation in the Age of Surveillance Capitalism". Journal of Business Ethics, 168, ,s.576.
[328] Ibid.

orantısız gözetimin, kişisel verilerin amaçsal yönetiminin devam ettiği görüşünü beslemektedir.

3.1.3.4. Amerika Birleşik Devletleri'nin Duruşu

1890 yılında Harvard Üniversitesi Hukuk Fakültesi Dergisi'nde yayınlanan *"mahremiyet hakkı-right to privacy"* isimli makalelerinde Warren ve Brandeis; mahremiyete veya özel hayata yönelik yapılan ihlalleri haksız fiillere benzetir[329]. Dolayısıyla bu fiiller kötü niyetle işlenmiş olmasalar da yanlıştır ve sorumluluk gerektirir[330]. Çalışmanın ilk bölümünde yer verildiği üzere, bu yayın Amerika'da mahremiyetin savunulması ve hukuk tarafından korunması açısından oldukça ses getirmiştir. Yine William L. Prosser'ın 1960'ta yayınlanan Privacy Torts isimli çalışması da böyledir. Öte yandan Westin'in 1967 tarihli Mahremiyet ve Özgürlük (*Privacy and Freedom*) isimli kitabında[331], mahremiyet hakkında bugün de devam eden pek çok soru işareti yer almaktadır.

ABD'de esas değişimi yapan ise 1974'te kabul edilen "*Gizlilik Yasası- the Privacy Act*" olmuştur. Yasa federal kurumlar tarafından kayıt sistemlerinde tutulan bireyler hakkındaki bilgilerin toplanmasını, muhafaza edilmesini, kullanılmasını ve dağıtılmasını yöneten bilgi uygulamalarını içerir[332]. Gizlilik Yasası, kurumların verilerin tutulduğu kayıt sistemleri hakkında kamuya bildirimde bulunmalarını gerektirir ve yasada yer alan on iki yasal istisnadan birine uygun olmadığı sürece, bireyin yazılı rızası olmadan bir kayıt sisteminden bir birey hakkındaki kaydın açıklanmasını yasaklar[333]. Bunlar dışında düzenleme ile bireylere kendileri hakkındaki kayıtlara erişim ve bu kayıtlarda değişiklik yapmaları için çeşitli haklar sağlanıp, verileri kaydedenlere bazı gerekliliklere uyma yükümlülüğü getirilir. Belirtmek gerekir ki ülkede tek bir veri koruma yasası olmayıp hem federal hem de eyalet düzeyinde çıkarılan pek çok yasa bulunur. Federal düzeydeki

---

[329] WARREN ve BRANDAIS, 1890, s.219.
[330] Ibid.
[331] WESTIN, A. (1967). Privacy and Freedom. New York: Ig Publishing.
[332] The United States, Department of Justice, Privacy Act of 1974.
[333] Ibid.

yasalar daha temel hususlara değinirken, eyalet yasaları çok daha detaylı, çeşitli ve sektörlere yöneliktir.

ABD'de kişisel verilerin korunmasına yönelik özellikle 1996 tarihli sağlık sektöründe mahremiyet ve güvenliği düzenleyen *"Sağlık Sigortası Taşınabilirlik ve Hesap Verebilirlik Yasası-Health Insurance Portability and Accountability Act-HIPAA"*, 1999 tarihli tüketicilerin kamuya açık olmayan gizlilik bilgilerinin finans endüstrisinde nasıl toplandığını ve kullanıldığını yöneten *"Gramm-Leach-Bliley Yasası"*, *"2000 tarihli Çocukların Çevrimiçi Gizliliğini Koruma Yasası-Children's Online Privacy Protection Act"* önemli adımlar olarak görülmekteyse de; hala GDPR eşdeğeri koruma sağlayan bir düzenleme ile karşılaşılamamaktadır.

3.1.3.5. APEC

Asya Pasifik ülkelerinin ekonomik iş birliğini sağlamak için 1989'da kurulan APEC[334], 2004 yılında "Gizlilik Çerçeve Belgesi"ni (*Privacy Framework*) kabul etmiştir. Belgenin kabul edilme gerekçesi bilgi akışının önündeki engellerden kaçınmak, ticaretin devamını sağlamak ve APEC bölgesinde ekonomik büyümeye destek olmak şeklinde ifade edilmiştir[335]. Düzenleme oldukça detaylı olup, zararın önlenmesi, bildirim, verileri elde etmeye yönelik sınırlamalar, kişisel verilerin kullanımı, seçim, kişisel verinin bütünlüğü, veri güvenliği önlemleri, erişim ve düzeltme, hesap verebilirlik gibi ilkeleri içermektedir. APEC Gizlilik Çerçeve Belgesi üzerinde OECD Rehber İlkeleri'nin etkisinin oldukça bariz olduğu belirtilmekle birlikte, ilkelerin zorlayıcı olmadığı, hangi oranda uyum sağlanacağının devletlerin inisiyatifinde olduğu belirtilmektedir[336].

---

[334] Asia-Pacific Economic Cooperation, About APEC.
[335] APEC Privacy Framework (2005).
[336] KÜZECİ,2021.s.166.

3.1.3.6. ECOWAS

Batı Afrika Ülkeleri Ekonomik Topluluğu olan ve 15 üye devletten oluşan ECOWAS, 2010 kurucu anlaşmaya ek olarak bağlayıcılığı olmayan Kişisel Verilerin Korunması Ek Yasası'nı kabul etmiştir. Yasa'nın Veri Koruma Direktifi'nden güçlü bir şekilde etkilendiği ve üye devletleri bir veri koruma otoritesi kurmaya sevk ettiği görülmektedir. Örgüt 2011 yılında ise bölgede artan siber suç seviyesi karşısında bölgesel mevzuatın uyumlaştırılması veya oluşturulmasına yönelik artan ihtiyacı vurgulayan Siber Suçlarla Mücadeleye İlişkin Direktifi de kabul etmiştir[337].

3.1.4. Korunan Hak ve Menfaatler

Kişisel verilerin korunmaya "değer" kılınışı, mahremiyetin bir hak olarak ortaya çıkışı ile aynı kaynaktan ilerler. Bu doğrultuda çalışmanın birinci bölümünde yer verilen mahremiyetin gelişimi, kişisel verilerin korunması hukukunun temelindedir. Veri koruma yasaları genel olarak kişilere ait verilerin işlenmesindeki aşamaları düzenleyerek kişisel verilerin toplanma, kaydedilme, saklanma, kötüye kullanılma ve aktarım yollarını ele alır. Elbette kişilere ilişkin her türlü veri değil yalnızca onların tanımlanmasına veya çeşitli özellikler ile belirli hale gelmelerine sebep olan veriler, belirli sınırlama ve denetimlere tabi olacaktır. Bu açıdan kişisel verilerin korunmasına ilişkin düzenlemeler, bireylerin mahremiyetini ve özel hayatlarını kişisel verilerin "zarar görmesi" olasılığı açısından, bu durumun sonuçlarına karşı korumaya çalışır.

Bir görüşe göre; veri koruma yasalarının sağlamaya çalıştığı sistem, büyük veri ile fazlaca ilişkilidir. Özellikle dijital ortamda tıklamalar, yorumlar, işlemler ve fiziksel hareketlerin bu bilgileri piyasaların ve seçmenlerin duygularını ve faaliyetlerini izlemek için kullanan büyük veri işlemcileri tarafından giderek daha fazla kaydedildiği, analiz edildiği bir küresel ortamda bu uygulamaların birtakım sosyal maliyetleri bulunur[338]. Bunun yanında büyük verinin gözetim amaçlarıyla kullanılabilmesi, bireylere ciddi

---

[337] CCDCOE. Economic Community of West African States. (Erişim Tarihi: 01.10.2022) https://ccdcoe.org/organisations/ecowas/

[338] ANDREW & BAKER, 2021,s.565.

zararlar verebilme potansiyeli, güvenli kullanımının denetiminin zorluğu karşısında bir "risk dengesi" yaratmak için devletlerce getirilen kişisel verilerin korunması kurallarının gerçekten bir denge kurup kurmadığı konusu tartışmaya açıktır[339]. Zuboff'un fikirleriyle de uyumlu biçimde ilerleyen bu tartışmada, özel hayatın gizliliğini ve mahremiyetin korunmasını amaçlayan veri koruma yasalarının getirmiş olduğu ve veri güvenliğine ilişkin olan anonimleştirme, gizlilik taahhütnameleri düzenleme, maskeleme gibi yöntemlerin kişisel verileri büyük şirketlere karşı korunan hak ve menfaatler yönünden koruyamayabileceği fikirleri yer alır.

Kişisel verilerin ekonomik değer taşıması, nesnelerin interneti *(IOT-Internet of Things)* büyük veri, bulut sistemleri gibi yeni uygulamalar, veriler ile oluşturulan "yeni" ekonomi modelleri, farklı veri işleme teknikleri, bireylerin hak ve özgürlükleri ile kişisel verilerin edinilip işlenmesi ve veri akışı (*data flow*) sağlanması arasında bir dengeleme yapılmasına sebep olmuştur[340]. Öyle ki bu tabloda elde edilen bazı hassas verilerin korunması, kişilerin özel hayatlarını açıkça ve tehlikeli şekilde ihlal edebilecek yapıda olmalarından ötürü daha gerekli hale gelmiştir. Ayrıca kişisel verilerin hatta bilgi güvenliğinin ve yönetiminin sağlanmasının, iletişim ortamının kendisinin korunmasının öneminin de bilinen yöntem ve kuralların yenilenmesi ihtiyacını doğurduğu ifade edilmektedir[341]. Böylece kişisel verilerin korunması hukukunun kapsamına bilginin yönetişimi ve bilgi güvenliği politikası da dahildir demek yanlış olmayacaktır.

Kişisel verilerin korunmasına ilişkin her geçen gün hızla artan düzenlemelerin kapsamında, günümüz modernleşmesinde kişisel verilere duyulan gereksinimin bir kabulü vardır. Bu gereksinimin ise yalnızca devletlerin olmadığı açıktır zira devletlerin, alandaki düzenlemeler oluşmadan önce "kamu güvenliği, kamu düzeni, istihbarî" gibi gerekçeler ile bireylerin bilgilerini kaydetme yetkisi bulunmakta idi. Ancak dijitalleşme ile oluşan ve bilindik yöntemlere "hem yakın hem yabancı" olan tekniklerin[342] dünyadaki

---

[339] Ibid, s. 576.
[340] "AŞIKOĞLU, Ş.İ. (2018) Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri. Onikilevha: İstanbul." s.1.
[341] HENKOĞLU, T. (2015) "Bilgi Güvenliği ve Kişisel Verilerin Korunması". Ankara: Yetkin Yayınları. s.19.
[342] RYAN, J. (2010) "A History of the Internet and the Digital Future". London: Reaktion Books.

tüm bireylere ilişkin yeni bir gözetim biçimi yaratması ile "özel yaşamın gizliliği ve genel olarak kişilik hakkının kendisi, düşünceyi açıklama özgürlüğü, bilgi edinme hakkı, mahremiyet" gibi konseptler bambaşka bir risk gölgesi altına girmiştir.

Dolayısıyla verilerin sahipleri ile bu verileri elde edenler arasındaki menfaat dengesinin veri sahipleri aleyhine bozulması, bireylerin maddi ve manevi bütünlüklerini koruma ihtiyacını gözler önüne sermiş[343], kişisel verilere ulaşmak her zamankinden çok daha kolay hale gelmiş[344], bu durum devletlere insan haklarına verilen önem doğrultusunda bireylerin verilerini koruma görevi yüklemiştir. Diğer taraftan kişisel veriler kullanılarak işlenen suçların artması (bilişim sistemlerine girilmesi, parmak izi veya göz retinasının hukuka aykırı kullanımı, yeni hırsızlık dolandırıcılık ve şantaj türleri, özel hayata dair verilerin haksız kullanımı) da[345] veri güvenliğinin sağlanmasını elzem kılmıştır.

Dijitalleşmenin -birbiri ile eşit olmayan şekilde- hem olumlu fırsatları hem de riskleri beraberinde getirmesi ile gücün sosyal anlamdaki paylaşımı, çıkarlar dengesi, toplumun norm ve değerleri de değişmiştir[346]. En başa dönüldüğünde her toplum bilginin değişimi üzerine kuruludur[347]. Günümüzde ise bilgi alışverişine eklenen yeni aktörler bireylere yönelik belki de devletlerden fazla bilgi sahibidir. Bu sebeple kişisel veri koruma mevzuatı ile oluşturulması amaçlanan çerçevede, kişinin verilerinin izole edilmesinden çok bu verilerin doğru aktarımı ve kullanımı ile diğer seçeneklerin masaya yatırılması yer alır. Kişilere verilerinin hangi kanallara aktarıldığını öğrenme hakkı (verilerin geleceğini tayin hakkı), verilerin silinmesini isteme hakkı, bazı şartlar dahilinde unutulma hakkı[348] gibi fırsatlar tanınarak hem bir temel hak olan kişisel verilerin korunmasını isteme hakkı sağlanmış olur hem de devletler dev veri ekonomisi karşısında

---

[343] AYÖZGER ÖNGÜN, Ç. (2019) "Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil". İstanbul: Beta Basım Yayın. Genişletilmiş 2. Baskı. s.1.
[344] DÜLGER, 2020, s.67.
[345] BÜK, A. (2018) "Bilişim Alanında Kişisel Verilerin Korunması". Ankara: Seçkin Yayıncılık. s.15-16.
[346] "SCHÜNEMANN, W. J.; BAUMAN, M. O. (2017) Privacy, Data Protection and Cybersecurity in Europe". Switzerland: Springer International Publishing.s.1.
[347] Ibid, s.2.
[348] "YAVUZ, C. (2018) İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması: Unutulma Hakkı". Ankara: Seçkin Yayıncılık.2. Baskı.

bilginin sağladığı gücü elinde bulundurma ve belirleyici rolünü sürdürme imkanını elde eder.

3.2. KAMUSAL ALANDA VİDEO GÖZETİME İLİŞKİN DÜZENLEMELER

3.2.1.Avrupa Birliği'ndeki Düzenlemeler

3.2.1.1.Genel Veri Koruma Tüzüğü (GDPR)

GDPR video gözetim cihazlarına ilişkin özel bir hüküm içermez fakat kamusal alanlarda kullanılan kameralar aracılığı işlenen kişisel verilere ilişkin elbette genel düzenleme olan GDPR uygulanacaktır. Ayrıca GDPR'ın uygulanmasını sağlamakla görevlendirilen *"EDPB-European Data Protection Board-Avrupa Veri Koruma Kurulu*" ve *"EDPS-European Data Protection Supervisor-Avrupa Veri Koruma Denetçisi"* düzenlemeleri, sair AB ve Avrupa Konseyi düzenlemeleri ile devletlerin ulusal mevzuatları bu tür veri işlemeler açısından da geçerlidir. Fakat belirtilmelidir ki; video kameraların kullanımına dair karşımıza genellikle "soft law" olarak da ifade edilen rehberler, direktifler, kararlar ve görüşler gibi ikincil hukuk düzenlemeleri çıkmaktadır.

Öncelikle çalışmanın ikinci bölümünde belirtildiği üzere ABAD kararlarına göre halka açık alandaki her kameralı gözetim kişisel verilerin işlenmesine sebep olmaz. Bunun için kişisel verilerin "sürekli ve sistemli" bir izleme ile elde edilmesi gerekir. Öte yandan video kayıt cihazları ile elde edilen kayıtlardan, biyometrik ve sair özel yapıda (hassas nitelikli) veri elde edilmesi durumları dışında, klasik kamera kayıt sistemleri tarafından toplanan kişisel verilerin korunması açısından hem GDPR'da hem 2016/680 sayılı Polis-Adalet Direktifinde[349] hem de ulusal mevzuatlarda çeşitli koruma önlemleri ve kuralları yer alır. Bu kapsamda GDPR'ın 5. maddesinde belirtilen *"(a) hukuka uygun*

[349] "2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İş birliği Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Direktif".

adil ve şeffaf olma, (b) belirli, açık ve meşru amaç doğrultusunda veriyi elde etme ve işleme, (c) işlendikleri amaç ile alakalı ve gereken ölçüde olma, (d) doğru ve güncel olma, (e)amacın gerektirdiği süre kadar muhafaza edilme, (f) bütünlüğün ve gizliliğin sağlanması için uygun tedbirlerin alınması" şeklindeki genel işleme kurallarına uygun bir veri işleme faaliyeti yürütülmesi gerekir.

Bunun dışında kamu otoritelerince video gözetim ile yapılan işleme faaliyetinin hukuka uygunluğu, GDPR'ın 6. maddesine belirtilen işleme koşullarından en az birinin mevcut olup olmadığına bakılarak saptanabilecektir. Video gözetim yönünden bu şartlardan özellikle rıza, yasal yükümlülüğe uygunluk, "kamu yararına" ifa edilen bir görev veya bu kapsamdaki resmi bir yetkilendirmenin sonucunda hasıl olan gereklilik hususlarının sağlanması beklenecektir. Devletlerce GDPR'a uyum sağlama maksadıyla alınacak tedbirlerin ve hukukun kamu yararına yönelik bir amacı karşılaması ve izlenen meşru amaçla orantılı olması gereği ise aynı maddenin üçüncü fıkrasında belirtilir.

Video görüntüleri GDPR kapsamında temel olarak kişisel verilerin işlenmesi için geçerli ilkeler altında korunur. Bu sebeple başta "adil işleme" olmak üzere, GDPR'ın altı temel ilkesine uyulması gerekir ki bu ilkeler video gözetim ile verilerinin toplanması ve işlenmesi söz konusu olduğunda ilgili kişilerin mahremiyetlerinin korunmasına dair çok yönlü bir koruma sağlama amacını taşır. Bununla birlikte video kayıt sistemlerinin genel kullanımı için GDPR'dan kaynaklanan öneriler pek çok kaynakta; kameraların yalnızca özel olarak tanımlanmış güvenlik sorunlarını hedefleyerek alakasız görüntülerin toplanmasının en aza indirmesi, CCTV'lerin bulunduğu alanda gözetim ve veri işleme konusunda bilgilendirme yapılması, amaca hizmet etmeyen CCTV kayıtlarının silinmesi, verilerin belirtilen bir saklama süresi ile ihtiyaç duyulan minimum süre boyunca saklanması ve ihtiyaç duyulmadığında silinmesi, yalnızca meşru amaçlarla ve yasal dayanak ile gözetim yapılması, izlemeye ilişkin politikalar ve kuralların açık ve kolayca erişilebilir olması, veri koruma görevlisi atanması, gizlilik etki değerlendirmesi

yapılması, kayıtların ve CCTV sistemlerinin güvenli bir şekilde saklanması ve erişimin yetkili personelle sınırlandırılması şekilde yer almaktadır[350].

Halka açık alanlarda kamu otoritelerince yapılan video gözetim açısından GDPR'da yer alan istisna hükümlerinin de değerlendirilmesi gerekir. 23. maddede "kısıtlamalar" (*restrictions*) olarak başlıklandırılan maddeye göre; maddede sayılan bazı durumlarda GDPR'da yer alan hak ve yükümlülüklere ilişkin hükümlerin uygulanması kısıtlanabilecektir. Ancak bu istisnai durumlar dahi tüm GDPR hükümlerini dışlamayıp, temel veri koruma kurallarına olay veya faaliyetle örtüştüğü ölçüde uyulmaya devam edilmelidir[351].

Kısıtlama sebepleri arasında, kamusal alanlardaki video gözetim için bazı hallerde dayanak olarak ortaya çıkması mümkün olan *"kamu güvenliğine ilişkin tehditlere karşı koruma ve önlemeyi de kapsayan şekilde, suçların önlenmesi (...)"* hususunun da yer aldığı görülür. Ancak bu kısıtlama sebebi video gözetim açısından düşünüldüğünde, çok sınırlı bazı durumlar için bir istisna halinden bahsedilmesi söz konusu olacaktır. Örneğin, bir konuda yapılan veri işleme hakkında soruşturma sahiplerine bilgi verilmesinin ya da kişilerin haklarını kullanmasının olası soruşturmaya engel olabileceği durumlarda GDPR açısından istisna olma durumu gündeme gelecektir[352]. Burada kamu güvenliği ile anlaşılması gerekenin, insan hayatını ilgilendiren acil durumlara ilişkin olması gerektiği EDPB tarafından pek çok farklı düzenlemede özellikle belirtilir.

Dolayısıyla gerek ABAD'ın veri işlemeye ilişkin istisnaların dar yorumlanması hakkındaki kararları gerekse "kamu güvenliği" sebebinin oldukça sınırlı bir gereklilik ile kullanılması, kamusal alandaki video gözetimler açısından bazı sonuçlara varılmasına yol açar. Öyle ki, bu durumda kamusal alandaki her izleme istisna kapsamında değerlendirilemeyecek, soruşturma gibi bazı özel durumlar açısından ancak yapılan işlemi tehlikeye düşürmemek adına istisna kapsamına dahil olunabilecek, bu durumda

---

[350] ŠİDLAUSKAS, 2019,s.62-63.
[351] EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, s.6.vd.
[352] Ibid, s.9.

dahi bireylere belirli hakları sağlanacak ve gereklilik durumu sona erdiğinde veri sorumlusunun tabi olduğu yükümlülüklere uyulacaktır[353].

GDPR'ın 35. maddesinde belirtilen *"veri koruma etki değerlendirmesi-data protection impact assessment"* kimin tarafından kullanıldığına bakılmaksızın video gözetim süreçlerine uygulanmalıdır. Maddenin birinci fıkrasında bilhassa yeni teknolojilerin kullanımında, bu kullanımın bireylerin hak ve özgürlüklerine dair yüksek bir risk oluşturmasının olası olması durumunda, veri işleme faaliyetine başlamadan önce kontrolör tarafından bir değerlendirme yapılacağından bahsedilir. Bu değerlendirme, faaliyetin kişisel verilerin korunmasına yönelik etkisi ile ilgili olacaktır. Yani GDPR'a göre; klasik video gözetim cihazları dışında özellikle biyometrik veri elde edebilen veya yapay zekâ kullanan kameraların kullanımında veri koruma etki değerlendirmesi yapılmasının bir gereklilik olduğu belirtilebilir. Burada özellikle kameraların kurulmasından sorumlu ve yetkili kamu kurumlarında veri koruma görevlisi bulunmasının da önemi ortaya çıkmaktadır.

Veri koruma etki değerlendirmesine şu üç halde özellikle ihtiyaç duyulacağı belirtilir: gerçek kişilere ilişkin profil çıkarmayı da kapsayan şekilde yapılan ve hukuki sonuçlar doğurabilen otomatik işlemeler, hassas nitelikli kişisel verilerin ya da ceza gerektiren suçlar hakkındaki işlemeler, kamusal bir alanın geniş çaplı ve sistematik biçimde izlenmesi. Ayrıca yapılacak değerlendirmede; işleme faaliyetine ve amaçlarına ilişkin sistematik açıklama, amaçla bağlılık ve orantılılığa dair izah, veri sahiplerine yönelik olası riskler ve bunlara karşı alınan tedbirler gibi hususların yer alması gerekir.

3.2.1.2. 2016/680 sayılı Polis-Adalet Direktifi

"2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İşbirliği Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı

---

[353] Ibid, s.6.

Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Direktif"[354] veya kısa adıyla Polis-Adalet Direktifi ise; temelde kamu otoritelerinin veya polisin veri işleme aracılığıyla elde ettiği menfaat ile bireylerin kişisel verilerinin korunması hakları arasında bir denge mekanizması kurmayı, polis ve adalet alanındaki veri işlemeleri diğer veri işlemelerden ayırmayı amaçlar[355]. Bu noktada ceza soruşturma ve kovuşturmasında uygulanacak olan devletlerin ulusal hukuklarının, Polis-Adalet Direktifi'nde yer alan ilkelere uygun şekilde oluşturulması beklenir[356].

Kamusal alandaki video gözetim, bir kolluk uygulaması olarak ve aynı zamanda ceza adaletinin sağlanması için suç soruşturması, suçun önlenmesi, kamu güvenliğinin tesisi, kamunun tehlikelerden korunması amaçlarıyla yapıldığında bu düzenleme devreye girecektir[357]. Polis-Adalet Direktifi'ne göre, belirtilen hallerde dahi AB Şartı, AİHS ve sair düzenlemeler ile uyumlu hareket edilmeli ve hakların sınırlanması dar yorumlanarak, veri sahiplerine kişisel verilerin korunmasını isteme hakkının özüne saygı duyularak belirli taleplerde bulunma fırsatı verilmelidir[358].

Direktif kapsamına giren veri işlemeler açısından ayrıca, ekonomik kaygılardan bağımsız olarak uygun teknik ve organizasyonel önlemlerin alınması gerekliliği, "tasarımda *(privacy-by-design)"* ve "varsayılan *(privacy-by-default)"* olarak veri koruma ilkelerine uygun biçimde iç politika oluşturulması, önlemler alınıp prosedürler geliştirilirken veri koruma etki değerlendirmesi yapılması, kategorik bazda kayıtlar tutulması, kayıtların talep üzerine sunulması, mümkünse veri işlemeden önce denetim

---

[354] "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA".

[355] BOSTANCI BOZBAYINDIR, G. (2018) "Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler". Galatasaray Üniversitesi Hukuk Fakültesi Dergisi- 2018/2.s.71.

[356] Ibid.

[357] Ibid, s.72.

[358] "Official Journal of the European Union, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, para.48".

makamına danışılması, olası veri güvenliği zafiyeti yaşanan durumların en kısa sürede bir denetim makamına bildirilmesi, veri koruma görevlisi atanması, aktarım konusunda güvenceler ve kısıtlamalar getirilmesi şartlarının sağlanması gerekecektir.

Polis-Adalet Direktifi'nde yer alan temel ilkeler GDPR'da yer alan veri işleme ilkeleri ile hemen hemen aynıdır. Dolayısıyla bu düzenleme kapsamında örneğin suç işlenmesinin önlenmesi amacıyla kamusal alanda yapılan video gözetimler açısından, birer kontrolör olan yetkili kamu otoritelerinin, amaçta sınırlama, verilerin doğruluğunu ve güvenliğini sağlama, gerekli süre kadar muhafaza etme, yasallık, şeffaflık, orantılılık gibi ilkelere uygun hareket etmesi beklenecektir.

Bu konuda AB ülkeleri arasında Polis-Adalet Direktifine uygunluk bakımından bütünüyle bir yeknesaklık sağlanması elbette ulusal mevzuatların devreye girişinden dolayı mümkün değildir. Ancak başlı başına bu düzenlemenin yapılması, kolluk birimlerince belirli amaçlarla adli veya idari görevler yürütülürken kişisel verilerin işlenmesinin ayrıca değerlendirilmesine gerek duyulması yönünden önemlidir. Nihayetinde, suç işlenmesinin önlenmesi veya kamu güvenliğinin sağlanması gibi sebepler ile kişisel veriler işlenirken hiçbir sınıra bağlı kalınmaksızın hareket edilmesi, hakkın korunmasındaki temel kaygıya aykırı bir tablo ortaya çıkaracaktır.

3.2.1.3.EDPB-EDPS Düzenlemeleri

GDPR'ın 68 ve devamı maddelerinde, EDPB'nin tüzel kişiliğe sahip, bağımsız bir AB organı olduğu, GDPR ve sair kişisel verilerin korunması mevzuatının doğru uygulanmasını sağlamak ile görevli ve yetkili kılındığı belirtilir. EDPB video kayıt cihazları ile kişisel verilerin işlenmesine ilişkin 2020 yılında bir rehber yayınlamıştır. Burada amaç GDPR hükümlerinin konu ile bağlantısını kurmak, açıklanan ilke ve kuralların -kimi zaman genel akıl yürütme yöntemleri kullanılarak- tüm potansiyel

kullanım alanlarına nasıl genellenebileceğini göstermek olarak ifade edilmektedir (hem geleneksel hem akıllı/yapay zekâ kullanabilen/artırılmış video kayıt sistemleri için)[359].

Rehberde video kayıt sistemlerinin kişileri belli biçimde davranmaktan kaçınmaya itebileceği kabul edilmişse de hem kamu otoritelerince kullanımda hem de özel sektörde özellikle yüksek performanslı kayıt cihazlarının "verilerin ikincil kullanımı (*secondary use*)" gibi riskleri de artırdığının altı çizilmiş ve amaca ulaşmanın kayıt cihazları ile gözetim dışında farklı yolları olması durumunda video kayıtlarının varsayılan olarak (*by default*) bir zorunluluk olmayacağı belirtilmiştir[360].

EDPB'nin rehberinde kamusal alanların kamu otoritelerince gözetiminden çok, araç kamerası, mülk kameraları, iş yeri kameraları gibi sistemlerin üzerinde durulmuştur. Ancak çıkarların dengelenmesi, bireylerin hak ve özgürlüklerine müdahalenin yoğunluğu, toplanan bilginin türü ve içeriği, coğrafi kapsam yani ne kadar alanın gözetlendiği, veri öznelerinin sayısı, veri öznelerinin çıkarları, teknik tedbirlerin alınması, alternatif yolların olup olmadığı gibi hususların, bu tür gözetimler açısından da ele alınması gerektiği söylenebilecektir.

AB'nin bağımsız veri koruma otoritesi olan *"EDPS-European Data Protection Supervisor- Avrupa Veri Koruma Denetçisi",* video kayıt sistemlerine ilişkin, bu sistemlerin iyi tasarlanmış veya seçici şekilde uygulanmasının sağlanması halinde veri güvenliği sorununun da üstesinden gelinebileceği, aksi halde bireysel gizliliğin dolayısıyla temel hakların ihlal edilmesi durumunun ortaya çıkma tehlikesinin altını çizer. Kamera sistemleri aracılığıyla kişisel verilerin işlenmesinde temel olarak ele alınması gerekenler ise; veri kalitesi (*data quality*), bilgi edinme hakkı (*right of information*), veriyi tutma süresi (*retention period*) olarak ifade edilmiştir[361].

---

[359] WAHL, T. (04.05.2020), "Eucrim, EDPB: Data Protection Guidelines on Video Surveillance". (Erişim Tarihi 17.01.2022) https://eucrim.eu/news/edpb-data-protection-guidelines-video-surveillance/.
[360] Ibid.
[361] Ibid.

Bunlardan veri kalitesi, alakasız veya yeterince gerekli olmayan görüntülerin toplanmasının en aza indirilmesini kapsarken (*data minimisation*), aynı zamanda video kayıtlarının daha belirgin veya açık maksatlar ile yapılmasını gerekli kılar. Diğer taraftan, kamera kaydı yapıldığına dair çeşitli uyarılar konulmalı, sistemdeki görüntülerin kim tarafından ve ne kadar süre ile tutulacağına ilişkin bilgi verilmeli, görüntü kayıtlarının tutulacağı süre de dahil kamera kayıt sisteminin kullanımına yönelik açık ve belirli politikalar oluşturulmalıdır[362].

Konu hakkında EDPS tarafından 2010 yılında oluşturulan raporun genel çerçevesi; "privacy by design" adı verilen ve işleme yapan araçların oluşumundan, arzına ve işleyişine kadar her aşamasında yani tasarımında kişisel verilerin korunmasına-gizliliğe uygun bir işleyişin sağlanması gerektiğini ifade eden ilke, video gözetiminin yasal gerekçelendirmesinin önemi, video gözetimi kullanma ihtiyacının açıkça gösterilmesi gereği, video gözetiminin taşıdığı amacın gerçekleştirilmesi için elverişli bir araç olup olmadığı, daha az zararlı alternatifler olup olmadığı gibi hususlar ile kayıtların saklanma süresi, alınabilecek teknik güvenlik önlemleri, kayıtların transferine ilişkin maddelerden oluşur[363].

Raporda güvenlik amacıyla kurulan video kayıt sistemlerinde; özellikle kurumların (kamu otoritelerinin) dikkatli olması gerektiği, sistemlerin kurulma amacının yalnızca "güvenlik çevresi kapsamındaki anormallikleri gözetlemek" veya "güvenlik olaylarıyla ilgilenmek" şeklinde belirtilmesinin yeterli olmayacağı, aynı zamanda gözetim altına alınacak alanda meydana gelmesi beklenen ve caydırıcılık istenen güvenlik olaylarının detayına inilmesinin bir gereklilik olduğu ifade edilmiştir[364].

Bunların yanında oluşabilecek güvenlik risklerinin basit bir biçimde tanımlanmaması, gerçekçi ve doğrulanabilir biçimde güvenlik risklerinin varlığının ve kapsamının (spesifik tehlikeler, suç oranları vb.) ortaya konulması, sadece spekülatif nitelikte veya anektodal kanıtların algılanmasıyla video gözetimi yapmanın haklı

---

[362] Ibid.
[363] Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines, s.10 vd.
[364] Ibid, s.20.

çıkarılmaması, video kayıt sisteminin kurulduğu bölgedeki güvenlik risklerinin türü, geçmişte bölgede yaşanan olaylar ve güncel risklerin yaşanma olasılığının belirlenmesi gibi sağlamalar yapılarak netleştirme yapılması gerektiği belirtilmiştir[365].

Hem EDPB hem de EDPS'nin yaptığı düzenlemeler esasen video gözetim bakımından "gereklilik" ve "çıkarlar dengesi"nin altını çizer. Her ne kadar ilk bakışta "kamu güvenliği" gibi oldukça geniş bir konsepte dayanarak video gözetim yapılması veri işleme açısından "istisnai" bir durum gibi gözükse de bu tür gözetimler için de somut durum elverdiği sürece temel veri işleme ilkelerine uyulması gerekir. Elbette kanundan kaynaklanan veya spesifik bir cezai soruşturma veya adli faaliyet kapsamında talep edilen CCTV verileri bu tespitin dışında kalacaktır. Ancak kamusal alanların sistemli ve sürekli gözetiminde tabiri caizse, uyuyan kurallar uyanarak bireylere sahip oldukları hakların kullandırılması beklenir.

3.2.1.4. Avrupa Konseyi 108 + Konvansiyonu

Yürürlüğe girmemiş olsa da Avrupa Konseyi tarafından kabul edilen ve pek çok AB ülkesi tarafından imzalanan 108+, yapay zekâ temelli sistemlerin kullanımının yaygınlaşması ile bu doğrultuda alınması veri korumaya yönelik alınması gereken tedbirleri ve modernleştirilmiş kuralları içerir. Öyle ki veri işleme tanımında verileri elde etmek, saklama, değiştirme gibi faaliyetlerin yanında kişisel verilere mantıksal ve/veya aritmetik işlemler yapılması da işleme faaliyeti kabul edilmiştir. Düzenlemenin olabilecek en geniş katılım ile imzalanması, imzacı ülkelerin 108+'ın üç sene içimde yürürlüğe girmesi için derhal önlem alması, ülkelerindeki veri koruma mekanizmalarını güncellemeleri gerektiği AB Bakanlar Komitesince vurgulanmıştır[366].

Video gözetime ilişkin de kimi maddelerinde çeşitli yönleriyle yer verilen düzenlemede özel nitelikli veriler başlığı altında; görüntülerin işlenmesinde, bu

---

[365] Ibid, s.21.
[366] Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data. Decision of the Committee of Ministers. 128th session of the Committee of Ministers, Elsinore, 18 May 2018. s.5.

görüntülerin neye ilişkin olduğuna dair hassasiyet barındırabilecek unsurların belirlenmesi gerektiği, benzersiz tanımlamaya izin veren belirli bir teknik araçla işlemeyi içeren faaliyetin, özel nitelikli kişisel veri işleme olacağı belirtilir[367]. Bunun dışında faaliyetlerin tamamen kişisel amaçlarla mı yapıldığı, özel alanın dışında kalan kişilere verilip verilmediği (örneğin halka açık bir web sitesi) saklanıp saklanmadığı veya hangi ortamlarda saklandığı, kamusal alanı kapsayıp kapsamadığı gibi hususların ayrımına varılmasının önemli olduğu gibi hususlar yer alır.

Düzenlemenin 11. maddesinde istisnalar ve sınırlamalar başlığı altında ise; yasallık, adillik, şeffaflık ve belirlilik ilkelerinin altı çizilerek bu temel ilkelerin, kolluk kuvvetlerinin video gözetim gibi faaliyetler yürütmesine tek başına engel olmadığı, bu tür faaliyetlerin ceza gerektiren suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ile cezai yaptırımların infazı amacıyla ulusal güvenlik ve kamu güvenliğinin korunması ve önleme faaliyetleri de dahil olmak üzere, hukukilik ve veri sahiplerinin meşru menfaatleri dikkate alınarak demokratik toplumda gerekli ve orantılı bir önlem teşkil ederek yapılabileceği belirtilmiştir[368]. Bu hükümle birlikte, yine hükümde yer alan sebepler ile kamusal alanlarda yapılan video gözetim faaliyetleri genel olarak veri işlemek için aranan şartlardan muaf olacak fakat her durumda yasallık, adillik, şeffaflık ve belirlilik ilkelerine riayet edilmesi gerekecektir.

Bunlarla birlikte belirtilen kısıtlamaların gerekliliğinin olay bazında, kamusal menfaatteki temel hedefler ışığında incelenmesi gerektiği, devletin veya uluslararası örgütün kamu yararına olan bazı amaçları için istisnaların gerekli kılabileceği ifade edilmiş, "ulusal güvenlik" kavramının AİHM'in ilgili içtihatları ile yorumlanacağı, ulusal güvenlik ve savunma amaçları için dahi işleme faaliyetine ilişkin bağımsız inceleme ve denetim mekanizmalarının işletileceği vurgulanmıştır[369]. 108 + ile veri işleme faaliyeti, kişisel veri, kontrolör-alıcı (*recipient*)-veri işleyen (*data processor*) kavramlarının kapsamını çağın gerekliliklerine uygun şekilde modernize edilmiş, video gözetim faaliyeti açık şekilde veri işleme kapsamına alınmış, kamusal alanların kamu

[367] Ibid, s.108.
[368] Ibid, s.26.
[369] Convention 108 +, s.26.

otoritelerince video gözetiminin belirli haller ile sınırlı olarak veri işlemeye dair bazı kurallardan istisna tutabileceği belirtilmiş, bu haller kısaca tanımlanmıştır.

Dolayısıyla Polis-Adalet Direktifinin yanında 108 + ile birlikte, bu faaliyetlerin genel olarak suç ceza gerektiren suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması, cezai yaptırımların infazı amacıyla ulusal güvenlik ve kamu güvenliğinin korunması, kamu güvenliği, milli güvenlik gibi sebeplerle yürütülebileceği ancak meşruiyet, adil işleme, şeffaflığın sağlanması ve veri işleme amacının belirli ve sınırlı olmasına dikkat edilmesi gerektiği ortadadır. Adil işleme ise veri işlemeden elde edilecek fayda, menfaat, bireysel ve toplumsal özgürlüklerin, verisi işlenen ve veriyi kullanan taraflarca dengelenmesini ifade eder.

3.2.2.Biyometrik Verilerin Önemi

Bilişim çağının geldiği bu noktada kişilerin hemen her hareketlerinde üzerinde işlem yapılan "verileri" hukuk ile korunmadığında aslında ortada bir kişilik hakkı ihlali olduğu kabul edilir. Bu sebeple bugün kişisel verileri korumak için pek çok ülkede veri koruma yasaları çıkarılmış, düzenlemeler yapılmış ve bağımsız veri koruma otoriteleri kurulmuştur[370]. Kişilere ait bazı veriler ise kendilerine has kimi özelliklerden dolayı daha "hassas" kabul edilir ve özel olarak korunur. Nitekim çeşitli işlemler yapılırken kişilerce verilen bu hassas, özel veriler kimi zaman rıza unsurunu aşan şekilde, "farkında olunmadan" dahi verilebilmektedir. Bu durum özellikle yüz tanıma sistemlerinin uygulandığı sosyal alanlarda karşımıza çıkmaktadır.

Biyometrik veriler, kişilerin kendi hafızalarında kimlik doğrulama amacıyla tuttukları kullanıcı adı veya parola gibi veriler olmayıp, doğuştan sahip olunan ve her insan için biricik olan fiziksel ve davranışsal özellikleri kapsayan verilerdir. Bu veriler,

---

[370] "Bugün 194 ülkeden 128 tanesinin veri koruma ve mahremiyete ilişkin çeşitli düzenlemeleri bulunmaktadır". Data Protection and Privacy Legislation Worldwide, (Erişim Tarihi 25.04.2022) https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
Data protection around the World, (Erişim Tarihi 18.11.2022)
https://www.cnil.fr/en/data-protection-around-the-world

kişileri tanımlamak için kullanılan ayırt edici özelliklere dayanarak ortaya çıkar. Bunlardan yüz gibi insan vücudunun değişmez fiziksel özellikleri, kişiye ait biyometrik verileri oluşturur.

Özel nitelikli yani hassas kişisel veriler, diğer kişisel verilere kıyasla farklı bir koruma usulüne göre işlenir. Hassas(özel) nitelikli verilerin diğer verilerden başkalaşan tarafı, bu tür verilerin bünyelerinde barındırdığı ve ihlali durumunda kişilere toplumda önyargıyla yaklaşılma, ayrımcılık gibi özellikle sosyal risk barındırmalarıdır[371]. GDPR'ın 4. maddesindeki tanıma göre biyometrik veri; "*yüz görüntüleri veya daktiloskopik[372] 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*" şeklinde ifade edilmiştir. Görüldüğü üzere, biyometrik veriden bahsedebilmek için kişisel verilerin işlenmesinde kişinin "fizyolojik, fiziksel veya davranışsal özellikleri gibi ayırt edici özellikleri"nin ortaya çıkması, kişinin bu şekilde tanınır hale getirilmesi beklenir.

Ülkemizde KVKK'nın biyometrik veriyi "özel nitelikli kişisel veriler" arasında belirtmesinden önce bir Danıştay Kararı'nda biyometrinin kullanıldığı yöntemlerin tanımlanabilir biçimsel ve bireye has özellikleri nitelediği, otomatik doğrulamayı sağlayan kimlik eşleştirme yöntemlerini kullandığı ifade edilmiş ve bu yöntemlere örnek olarak parmak izi ve el geometrisi tanıma, iris-retina-yüz-DNA tanıma gibi biyometrik veri türleri sayılmıştır[373]. Biyometrik veriler yapısal olarak kişilere ait değişmeyen, bazen onlar öldükten sonra dahi değişmeden kalabilen, basitçe elde edilebilen türdedir[374]. Bu türde verilerin kullanımı, diğer veriler ile karıştırılma risklerinin çok düşük olması ve kolay şekilde elde edilip sonradan bir değişikliğe uğramamaları sebepleriyle tercih edilir.

---

[371] "TAŞTAN, F. G. (2017) Türk Sözleşme Hukukunda Kişisel Verilerin Korunması. İstanbul: On İki Levha Yayıncılık, 1. Baskı", s.41.
[372] "Daktiloskopi: Parmak izine dayanarak kimlik belirleme yöntemi" (https://sozluk.gov.tr/)
[373] "Danıştay 15. Dairesinin 2014/4562 esas sayılı kararı., Danıştay'ın tanımına ek olarak belirtmekte fayda görülmektedir ki; yüz geometrisi de el geometrisi gibi işlem görmektedir".
[374] "SATAPATHY S. C. & JOSHI A. (2017). Information and Communication Technology for Intelligent Systems (ICTIS 2017), Bhatnagar S. Cooperative Multimodal Approach for Identification – Volume 1, s. 13-18."

Yüz tanıma özelliği bulunan video kameraların kolaylıkla elde ettiği kişinin yüzüne ait biyometrik verileri fizyolojik niteliklidir ve genellikle değişmeyen, vücudumuzda taşıdığımız özelliklerin bütününü oluşturan verilerdir. Bir görüşe göre, fizyolojik nitelikli biyometrik verileri morfolojik ve biyolojik olmak üzere iki kategoriye ayırmak mümkündür[375]. Bu çerçevede, yüz geometrisi gibi özellikleri ortaya çıkaran tanımlayıcılar morfolojik analiz yapmış olmaktadır[376]. Buradan yola çıkarak biyometrinin biyolojik nitelikli verileri ölçme ve analiz etme teknolojisi veya bilimi içinde yer aldığı ortaya çıkmaktadır[377]. Esasen kimlik sahibinin "kendisini oluşturan" veriler, biyometrik verilerdir.

Bir görüşe göre; biyometrik yöntemler kullanılarak elde edilen veriler zaman içinde değişmediğinden, kişinin vücut bütünlüğü kapsamındadır ve bu sebeple özellikle değiştirilme açısından güvenilirlik sağladığından geleneksel usullere kıyasla daha az sakıncalıdır[378]. Teknolojinin gelişmesiyle birlikte kimlik doğrulama yöntemlerinde de birtakım güncellemeler gerçekleşmiştir. Biyometri, bireylerin kimliklerini doğrulamak maksadıyla onların fizyolojik veya davranışsal durum/yapılarını kullanır ve bu veriler bireylerin hayatları boyunca değişmez[379]. Kişilerin biyometrik verilerini şifrede olduğu gibi unutması mümkün değildir çünkü bu veriler bizzat kişinin bir parçası olup onun üzerinde taşınmaktadır. Bu özellikleri dolayısıyla uygulamada biyometrik verilerin güvenilirlik düzeyi de "yüksek ve pratik" olarak kabul edilmektedir.

Bu noktada belirtmekte fayda görülmektedir ki, ses, görüntü, fotoğraf gibi veriler her zaman biyometrik veri niteliğini teşkil etmeyebilir. GDPR'ın 51 numaralı resital hükmü uyarınca, fotoğraflardaki kişisel veriler direkt olarak biyometrik türde kişisel veri kabul edilmeyip, böyle bir kabul için özel bir teknik kullanarak biyometri elde edecek şekilde işleme yapılması, bu şekilde biyometrik özelliklerin ortaya çıkarılması ve kişinin

---

375 Thales Group, "What is biometrics". (Erişim Tarihi: 29.04.2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics
376 Ibid.
377 STRECKFUS, C.H. & GUAJARDO EDWARDS, C. (2011). "The Use of Salivary as a Biometric Tool to Determine the Presence of Carcinoma of the Breast Among Women" (Biometrics- In Tech). s.249.
378 SEVİNÇER, S. (2015) "Biyometrik yöntemlerle elde edilen kişisel verilerin site konutların güvenlik sistemlerinde kullanımı", İstanbul Barosu dergisi, 92(2), 234.
379 "SATAPATHY S. C. & JOSHI A. (2017)", s. 13-18.

bu şekilde tanımlanması gerekir[380]. Ayrıca kişisel verilerin işlenmesi, kişiyi kimliği ile belirlemek değil de sadece tanımlanabilir hale getirmek için yapılıyorsa bu durumda da biyometrik veri elde edilmesi gündeme gelmez[381].

Yüz tanıma (*facial recognition*) tekniğinde; kişilerin ağız biçimi, göz çevreleri gibi yapıları alınarak bunlar dijital ortamda karşılaştırmalı şekilde eşleştirilmeye tabi tutulur[382]. Dolayısıyla bu yöntem ile yüz yapısı benzeyen insanlar aynı kişi gibi algılanıp, yanlış sonuçlar doğabilir. Davranışsal özellikli biyometrik veri olarak ses tanıma da oldukça sık kullanılmaktadır. Ses tanımanın biyometrik veri olarak kullanılma sebebi her bireyin sesinde ton, perde, ahenk farklılığı olmasıdır nitekim kişilerin konuşurken ağzını kıpırdatma biçimleri de bambaşkadır[383] . Hızlı, güvenli ve kolay bir yöntem olarak ses tanıma da bireylerin ayırt edilmesine yarayan bir biyometrik veridir[384]. Bu yöntem bilhassa yaka kameraları açısından söz konusu olabilir.

3.2.2.1. Hukuki Açıdan Biyometrik Verilerin Önemi

Biyometrik verilere yönelik siber yöntemlerle yapılan güvenlik tehditleri arttıkça, hassasiyetleri sebebiyle daha kritik bir noktada olan bu verilerin güvenliğini sağlamak elzem olmuştur. Burada kişilerin biyometrik verilerini kullanarak çeşitli alanlara (özellikle bilişimsel) giriş yapmaları güvenliği sağlama noktasında önemlidir fakat "ölçülülük" ilkesi nazara alınmadan veri güvenliği doğru şekilde tesis edilmiş sayılamaz.

Biyometrik verilerin kişilere has ve kopyalanması mümkün olmayan yapıda olması, hukuken düzenleme yapılmasını gereksiz kılmaz. Bilakis bu türden verilerin

---

[380] Official Journal of the European Union (2016/679).
[381] "YÜCEDAĞ, N. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 75(2), 765-790."
[382] HAN F. & HU J. & KOTAGİRİ R. (2011) "Advanced Topics In Biometrics, Chapter 19 Biometric Authentication For Mobile Computing Applications", s.461-478.
[383] "WILSON T.V. (t.y.), How Stuff Works: How Biometrics Works: Voiceprints". (Erişim Tarihi: 29.04.2021), http://science.howstuffworks.com/biometrics3.htm
[384] Fingerprinting Criticisms. (t.y.), http:// www.fingerprinting. com/fingerprinting-criticism.php ve ARSLAN B. ve SAĞIROĞLU Ş. (2016). "Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme, Politeknik Dergisi", 19 (2), s. 101-114.

kullanımında yanlış eşleştirmeler yapılması kişilerin ciddi ayrımcılığa maruz kalmasına sebep olur. Özellikle ABD'nin San Francisco eyaletinde yüz tanıma sisteminin genellikle siyahî ve düşük gelirli vatandaşların olduğu bölgelerde kullanıldığı tespit edilmiş, ortaya çıkan aleni insan hakları ihlalleri ve açılan davalar ile bazı kullanımların durdurulmasına karar verilmiştir[385]. Yine güvenlik sağlama aracı olarak kullanılan yüz tanıma sistemlerinin yanlış tespitleri ile haksız yere yargılanan pek çok kişi bulunur.

Bunlardan başka biyometrik verilerin kullanımının hukuki çerçevesinin açıkça çizilmemesi, kitlesel işaretlemeleri ve güvenlik ihlallerini doğurur. Bu sebeple özenle korunması ve yasal kapsamın oluşturulması çok önemlidir. Özellikle Çin'de her alanda yüz tanıma (bazı bölgelerde ek olarak ses tanıma) sistemleri kullanılmakta ve bu sistemler muhalif kişilerin sosyo-politik açıdan damgalanmasını sağlamaktadır. Hukuki çerçeve oluşturulmadığında ortaya çıkacak sonuçlar oldukça vahimdir. Yüz tanıma sisteminin yaygın kullanımı, kamusal alanlarda anonimliğe son verir ve bireylerin sistemli bir şekilde izlenmesine izin verir.

Biyometrik verilerin kullanımı ile veri girişi yapılan veri tabanlarına (*databases*) ilişkin her gün çok fazla veri ihlali haberi gündeme gelmektedir. Forbes dergisinin web adresinde bilişim üzerine yazılan bir köşe yazısında; milyonlarca yüz tanıma kaydı verisinin ihlaline ilişkin bir rapordan bahsedilir[386]. Güvenlik araştırmaları yapan Vpnmentor dergisinde yayınlanan rapora göre; ihlalin ve saldırının büyüklüğünü ifade eden en büyük husus; siber saldırı yapılan sistemin veri tabanının hükümetler, bankalar ve polis dahil 83 ülkede 5,700 kuruluş tarafından kullanılan sistem ile entegre halde olmasıdır[387]. Bunun anlamı böylesine geniş çaptaki bir sistemde milyonlarca biyometrik verinin hukuk dışı kullanımlar için çalındığı ve her an pek çok yerde kullanılabileceğidir.

---

[385] Conger, K. vd. (14.05.2019). San Francisco Bans Facial Recognition Technology. The New York Times. (Erişim Tarihi:18.11.2022). https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[386] DOFFMAN, Z. (14.08.2019). "New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report". (Erişim Tarihi:06.05.2021), https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=2e2d575046c6 .

[387] Ibid.

3.2.2.2. Biyometrik Verilerin Korunmasına İlişkin Düzenlemeler

Öncelikle yüz tanıma özelliğine sahip akıllı kameralar ile biyometrik verilerin işlenmesi sırasında temel hak ve özgürlüklerin özüne dokunulamayacaktır ve ölçülülük, yöntemin (biyometrik veri işleme) amaç bakımından uygun olması gibi ilkelere riayet edilecektir. Biyometrik verilerin işlenmesinde işleme eyleminin ulaşılmak istenen amaç için elverişli olması gerekir-ki burada aracın elverişliliği, istenen neticeye yaklaşılıp yaklaşılmadığına göre ölçülür[388]. Bunların yanında biyometrik veri işlemenin elde edilmesi planlanan maksat açısından "kaçınılmaz" olması beklenir.

Anayasa Mahkemesi'nin 28.09.2017 tarihli ve 2016/125 esas, 2017/143 karar numaralı kararında da gerekliliğin, getirilen kuralın amaca hizmet etmesi yönünden aranacağı vurgulanmıştır. Ayrıca; her somut olayda farklı bir yorum getirilebileceği hususu vurgulanarak, gereklilik ilkesine göre *"en az müdahaleci aracın seçilmesi",* sınırlamanın daha az olduğu yöntem ile de aynı amacın elde edilmesi durumunda bu yöntemin seçilmesi, mecburi ve kaçınılamaz şekilde biyometrik veri elde edildiğinde ise bunun gerekçelerinin, açık sebeplerinin ortaya konulması gerektiği ifade edilmiştir[389]. Aksi durumlarda bu ilkenin gözetildiğinden bahsedilemez.

Gereklilik ilkesinin yanında biyometrik veri işlenmesinde varılmaya çalışılan amaç ile kullanılan yöntemler arasında bir orantının bulunması beklenir. Kullanılan araç ve elde edilmek istenen maksat arasında bulunması gereken denge veya ölçü, orantılılık ilkesine uygun hareket edilmesi için elzemdir[390]. Biyometrik verilerin işlenmesinde, yapılan sınırlamanın ölçüsü ile bu sınırlamayı gerekli kılan nedenler bakımından ölçülülük ilkesine uygun hareket edilerek; kullanılan araç vasıtasıyla veri sahiplerine orantısız müdahalelerde bulunulmaması gerekir[391]. Bunlar dışında belirlenen süre kadar muhafaza edilme, sebep ortadan kalkınca imha gerçekleştirme gibi kurallara da riayet edilmelidir.

---

[388] YÜKSEL, M (2017) "Temel Hakların Sınırlandırılması ve Ölçülülük". SDÜHFD, Cilt:7, Sayı:1, s. 8-9.
[389] Ibid.
[390] Ibid, s.13.
[391] Ibid, s.14.

Avrupa Birliği madde 29 Çalışma Grubunca[392] oluşturulan "Facial Recognition WP 192" başlıklı dokümanda kişilerin yüz tanıma amacıyla dijital görüntüleri çevrimiçi ve mobil hizmetlere yüklendiğinde, kontrolörlerin veri sahiplerinin yüz tanıma amacıyla gerçekleşebilecek görüntülerinin işlenmesine açık rıza verdiğinden emin olması gerektiği vurgulanmıştır[393]. Buna göre kontrolör, dijital görüntülerin ve şablonların yalnızca belirtilen amaç için kullanılmasını sağlamalıdır, kişinin açık rıza vermediği amaçlar için dijital görüntülerin üçüncü şahıslar tarafından daha fazla işlenmesi riskini azaltmak amacıyla teknik kontrolleri uygulamaya koymalıdır ve üçüncü şahısların erişimini kısıtlamak için araçlar geliştirmelidir.

Ek olarak kontrolör, hizmetin kayıtlı kullanıcısı olmayan veya başka bir şekilde bu tür işlemeye açık rıza vermeyen kişilerin dijital görüntülerinin yalnızca kendisinin bu tür bir işlem için meşru bir menfaati olduğu sürece işlenmesine dikkat etmeli, veri aktarımının güvenliğini sağlamak için şifrelenmiş iletişim kanallarını veya alınan görüntünün kendisini şifrelemeyi, görüntü aracılığıyla elde edilen verilerin ölçülü/gerekli miktarda olmasını sağlamalıdır[394].

Kontolör, verilerin depolanması için en uygun yeri (veri tabanını) tercih etmeli ve depolanan verilerin güvenliğini sağlamalıdır. Özellikle doğrulama amacıyla yüz tanıma durumunda, biyometrik şifreleme teknikleri kullanılabilir; bu tekniklerle, kriptografik anahtar doğrudan biyometrik verilere bağlanır ve yalnızca doğru canlı biyometrik örnek doğrulamada sunulursa yeniden oluşturulur, hiçbir görüntü veya şablon saklanmaz (böylece bir tür "izlenemez biyometri" oluşturur)[395]. Ayrıca kişilere hem orijinal görüntülere hem de yüz tanıma bağlamında oluşturulan şablonlara erişim haklarını kullanmaları için uygun başvuru mekanizmalarının temin edilmesi önemlidir.

---

[392] The Article 29 Working Party, The Working Party on the Protection of Individuals with regard to the Processing of Personal Data.
[393] Article 29 Data Protectıon Working Party (2012), Opinion 02/2012 on facial recognition in online and mobile services,
[394] Ibid.
[395] Ibid.

Bunun yanında 108 Sayılı Sözleşme Danışma Komitesi tarafından yakın tarihte benimsenen 28 Ocak 2021 Tarihli "Yüz Tanıma Rehberi"ne göre ise; biyometrik veri işleme teknolojilerin kullanımları çok ve çeşitlidir, bunlardan bazıları ciddi şekilde veri sahiplerinin haklarını ihlal edebilir, bu açıdan bireylerin kapsamlı gözetimine izin veren mevzuatlar, bireylerin özel hayata saygı hakkına aykırı olabilecektir[396]. Yüz tanıma özelliğini kullanan teknolojilerinin hali hazırda kullanılan gözetim sistemlerine entegrasyonu, kişisel verilerin korunması ile özel hayatın gizliliği ve diğer temel haklarına yönelik ciddi riskler oluşturabileceği gibi internette bireylerin dijital görüntülerine erişim imkânı düşünüldüğünde bu teknolojilerin kullanımı her zaman kişilerin farkındalığını veya biyometrik verileri işlenen kişilerin iş birliğini sağlayamayacaktır[397].

Yüz tanıma teknolojilerinin kullanımının gerekliliği ile amaca orantılılık ve veri sahiplerinin hakları üzerindeki etkileri birlikte değerlendirilmelidir, farklı kullanım durumları kategorize edilmeli ve ilgili yasal çerçeveye göre yüz tanıma yoluyla biyometrik verilerin işlenmesi yerinde olmalıdır. Bu yasal çerçeve her farklı kullanıma göre özellikle; özel kullanımın ve amacının ayrıntılı açıklaması, kullanılan algoritmanın minimum güvenilirliği ve doğruluğu, kullanılan fotoğrafların saklama süresi, bu kriterleri denetleme olasılığı, sürecin izlenebilirliği, korumaların neler olduğunun belirtilmesi gibi kriterleri karşılamalıdır[398].

Yine Avrupa Birliği madde 29 Çalışma Grubu'nun *"opinion 3/2012 on developments in biometric technologies"* başlıklı görüşünde; biyometriyi kullanmanın bir ön koşulunun bireylerin temel hak ve özgürlüklerinin korunmasına yönelik riskleri hesaba katarak biyometrik verilerin toplandığı ve işlendiği amacın açık bir tanımının yapılmış olması olduğu, bir kişinin göründüğü yerdeki fotoğrafların kendisini yüz tanıma algoritmasına sahip bir çevrimiçi fotoğraf albümünde otomatik olarak etiketlemek için işlenebileceğine açık rıza verdiyse, bu işlemin veri korumaya uygun bir şekilde

---

[396] Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data Convention 108(2021), Guidelines on Facial Recognition, s.1-16. (Erişim Tarihi: 11.09.2022) https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

[397] Ibid.

[398] Ibid.

gerçekleştirilmesi gerektiği ve etiketlemeden sonra biyometrik verilere artık ihtiyaç olmayacağı belirtilmiştir[399]. Rapora göre; biyometrik verilerin tanımlama amacıyla kullanılmasında kişinin yüzünü analiz eden sistemler, suçla mücadeleye çok verimli bir şekilde katkıda bulunabilir ve ciddi bir suçtan şüphelenilen bilinmeyen bir kişinin kimliğini etkili bir şekilde ortaya çıkarabilirse de büyük ölçekten bakıldığında kullanılan bu sistemler aynı zamanda ciddi yan etkilere de neden olabilir[400].

Doğruluk prensibine göre; işlenen biyometrik veriler doğru ve toplandıkları amaç ile orantılı olmalıdır ve veriler kayıt sırasında ve veri sahibiyle biyometrik veriler arasında bağlantı kurulduğu esnada doğru olmalıdır. Açık rıza, bu prensibinin bir yansıması olarak aranacaktır. Veri minimizasyonu ise daha önce de belirtildiği üzere, biyometrik veriler genellikle eşleştirme işlevleri için gerekenden daha fazla bilgi içerdiğinden kontrolör tarafından uygulanması gereken ve tüm mevcut bilgilerin işlenmemesi, iletilmemesi veya depolanmaması gerektiği anlamına gelen bir ilkedir. Bu ilke yüz tanıma gibi algoritmalar içeren sistemlerde saklanan biyometrik veriler açısından her an geçerliliği sağlanması gereken bir kuraldır. Ayrıca biyometrik verilerin işlenmesinin yalnızca önemli bir riskin somut varlığına dair objektif ve belgelenmiş koşullar temelinde kanıtların olduğu durumlarda, mülkleri veya bireyleri güvence altına alan gerekli bir araç olarak gerekçelendirilebileceği ifade edilmektedir[401].

Bu yaklaşımdan ötürü kontrolörün, hangi koşulların biyometrik verilerin işlenmesini gerektiren somut ve önemli bir risk oluşturduğunu kanıtlaması gerekir. Elbette anılan risklerin devam edip etmediğine düzenli aralıklarla bakılması beklenir. Burada amaç hassas nitelikli bu tür verilerin işlenmesini gerektiren önemli risklerin ortada olup olmadığını anlamak, bununla birlikte hala elde başka daha az müdahaleci seçenekler varsa bu alternatif seçenekleri tercih etmektir. Eğer biyometrik verilerin neden

---

[399] Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric Technologies, s.1-9.
[400] Ibid, s. 10.
[401] Ibid.

işlendiği yeterince (gerekçeyle orantılı şekilde) ifade edilemiyorsa, veri işleme faaliyeti derhal sona erdirilmeli veya en azından bir süreliğine bekletilmelidir.

Bireyselleşmenin teknolojiye bağlı olarak boyut değiştirmesiyle birlikte, kişisel verilerin öneminin ve değerinin artmasına bağlı olarak biyometrik veriler de kişisel mahremiyet kapsamında gündeme alınmış olup, bu konuda hem bilimsel hem de hukuki çalışmalar yoğunlaşmıştır[402]. Bu amaçla birçok ülkede yasal düzenlemeler yapılmış ve veri ihlali durumlarında çeşitli yaptırımlar uygulanmaya başlanmıştır. Fakat elde edilen ve dijital olarak veya başka yöntemlerle saklanan biyometrik verilerin uygun şekilde korunması, gerektiğinde silinmesi veya yok edilmesi zorunludur. Bu türden veriler, kişiyle doğrudan örtüşen ve ona sıkı sıkıya bağlı olan, onu diğer bireylerden ayrırt eden bir veri eşleştirmeyi sağlar ki böyle hassas bir alanın hukuken sıkı şartlara tabi olarak korunması gerekir[403]. Bireylerin yüz geometrisi gibi bilgilerin kuralsızca dağıtılması çok ciddi tehlikeler meydana getirecektir[404].

Günümüzde yapay zekâ teknolojisinin entegre olduğu veri girişi yapılan sistemler oldukça yaygın kullanılmaktadır. Biyometrik verilerin ihlali halinde karşılaşılabilecek tehditler ise; önce bireylere sonra kitlelere/topluma yönelik tehditleri de barındıran boyutlara varabilecek ciddiyettedir. Bu türden veriler kendilerine has yapıları sebebiyle çok daha sıkı koşullar ile korunmalıdır ve olası ihlallerin neticeleri konusunda hem bireylerde hem de kamuda bilinç yaratılmalıdır. Bu ise; salt hukuk kurallarının uygulanması ile değil idarenin birimlerine sirayet eden bir kültür ve hukukun sosyal kavrayış ile yorumlanması yoluyla sağlanabilecektir.

---

[402] Biyometrik Yöntemlere İlişkin Uygulama Yöntemleri ve Örnekleri Hakkında Kapsamlı Bir Çalışma İçin bkz. "KESER BERBER L., LOSTAR, M. (2006) Bilişimde Biyometrik Yöntemler". Ankara: Yetkin Yayınları.

[403] BULUT, M. (2020). "Özel Bir Hukuki Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler". Ankara Barosu Dergisi, 2020(3), s.114.

[404] Ibid.

3.3. VİDEO GÖZETİMİN UYGULANIŞI YÖNÜNDEN İKİ ÜLKE ÖRNEĞİ: FRANSA VE TÜRKİYE

Mahremiyetin korunması yönünden Fransa, kamusal alanda video gözetime ilişkin hukuki düzenlemeler ve bunların doğurduğu tartışmalar bakımından oldukça ilgi çekicidir. Bunun ilk sebebi en geniş çaplı hukuki düzenleme kabul edilen GDPR'ın uygulandığı bir ülke olmasıdır. Ülkede bir taraftan GDPR ve sair ulusal düzenlemeler ile video gözetime karşı meşru bir zemin bulunurken, diğer taraftan CNIL'in özellikle "akıllı" kamera sistemlerine karşı uyarıları[405] ve sivil toplum örgütlerinin CCTV'lere yönelik söylemleri ile bunlara rağmen yapılan tartışmalı yeni düzenlemeler dikkat çekmektedir.

Bu sebeplerle Fransa'nın video gözetim konusunda durduğu yer, kişisel verilerin korunması alanında pek çok iyi uygulama örneğine sahip olması, GDPR korumasında olması bunlara rağmen hukuk normları-meşruluk ve normlar ile korunmak istenen fayda üçgeninde eleştirilere matuf olması sebepleriyle örnek mahiyetinde ele alınmak istenmiştir. Başlık altında video gözetim sistemlerinin kamusal alanlardaki kullanımı bakımından Türkiye'deki genel durum ele alınmış, genel hukuki düzenlemelerin dışında hangi özel koşullara dayalı olarak kamusal alanda video gözetim yapıldığı sorgulanmıştır.

3.3.1. Fransa'da Kamusal Alanlarda Uygulanan Video Gözetim

3.3.1.1. Genel Bilgi

Fransa'da halka açık alanlarda yapılan video gözetim, uzun süredir çeşitli tartışmalara sebep olan bir konudur[406]. Öyle ki; Anti-Video Gözetim Kolektifi tarafından Fransa

---

[405] CNIL.19.06.2022. Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position. (Erişim Tarihi: 08.08.2022). https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position

[406] PEYRON, J., "Debate swirls as Paris embraces video surveillance", France 24. (Erişim Tarihi: 10.01.2022) https://www.france24.com/en/20120117-debate-swirls-around-paris-new-high-surveillance-system-cameras-cctv-police

Belediye Başkanlarına yönelik henüz 2004 yılında yayınlanan açık mektupta; analog kameralardan bilgisayarlı kameralara geçiş sonrasında Toulouse gibi bölgelerde "zenginler" için kameralarla korunan mahallelerin oluşturulmasının amaçlandığı, video gözetimin suçluluk oranını düşürme üzerindeki etkilerinin kanıtlanamadığı, kameraların Fransa'yı bir istihbarat ağı altında ezerek bireysel ve kolektif özgürlüklere zarar verdiği belirtilmiştir[407].

CNIL'in zaman zaman çeşitli alanlara yönelik yapılan izlemeler konusunda aşırı video kayıt cihazı kullanımının altını çizdiği ve bu tür uygulamaların GDPR eksenine girmesine ilişkin yaptığı kamuoyu duyuruları da dikkat çekmektedir[408]. Bunun yanında, yıllar içinde video kameraların sayısı, kameralı izlemeye yönelik yazılımlar, kamera üreten şirketler ve devletin video kayıt sistemlerine ayırdığı bütçe gibi video gözetim ekonomisine dahil olan unsurların dikkat çekici seviyede arttığı iddialarının olduğu bilinmektedir[409]. Ülkede halka açık alanlardaki video gözetiminin 2007 yılından itibaren ciddi bir atış gösterdiği, bu izleme biçiminin öncelikli amaç haline getirildiği, daha önce konu ile ilgilendirilen politikacı İçişleri Bakanı iken 15 Mayıs 2007 tarihli kararnamenin kabul edilmesiyle teknik konularda İçişleri Bakanına görüş bildirmekten sorumlu bir Ulusal Video Gözetim Komisyonu (*La Commission Nationale de la Vidéoprotection*) oluşturulmuştur[410].

Fransa'nın veri koruma paketi iki aşamalıdır. Ulusal ve AB düzenlemeleri şeklinde iki hukukun tatbiki ile şekillenen kişisel verilerin korunması, verilerin işlenmesini gerektiren sebepler, faaliyetler ve hatta cihazlar bakımından farklı hükümlere tabi olacaktır. Dolayısıyla Fransa özelinde kişisel verilerin korunmasına ilişkin yapılacak bir inceleme, öncelikle bütüncül bir bakış ile temel AB düzenlemeleri baz alınarak yapılmalı, sonrasında veri işlemenin biçimine veya özel sebebine göre ulusal düzenlemelere

---

[407] "Does Video Surveillance Have a Limit? An open letter to the Mayors of France". The Anti-Video Surveillance Collective of France. 2004. (Erişim Tarihi: 08.08.2022). http://www.notbored.org/limits-of-surveillance.html

[408] CNIL, "Mises en demeure de plusieurs établissements scolaires pour vidéosurveillance excessive". Konu hakkında genel bilgi için bkz. OVALIOĞLU, S. (2021) Avrupa Birliği Hukukunda Kişisel Verilerin Korunması (Yüksek Lisans Tezi) s.103 vd.

[409] The Local Fr, Drones and surveillance cameras: France's new security bill explained

[410] MUCCHIELLİ, L. (2016). "À Quoı Sert La Vidéosurveillance De L'espace Public ? Le cas français d'une petite ville «exemplaire ». Deviance et Societe", 40(1), s. 25. https://doi.org/10.3917/ds.401.0025

bakılmalıdır. Fransa'da halka açık alanlarda yapılan izlemeye ilişkin bir değerlendirme yapabilmek için, aşamalı şekilde hareket edilerek video gözetime sebep ve konu yönünden yaklaşılmalıdır.

Nitekim ülkede hem ulusal mevzuat hem de AB mevzuatı aynı anda yürürlüktedir ve bu sebeple yapılan hukuki düzenlemeler uygulamada, katmanlı şekilde yorumlanmaktadır. Bundan dolayı video gözetim yapılma sebebinin ne olduğu ve hangi yasal dayanak ile video kayıt sisteminin kurulduğu belirlenmeli, buna göre AB mevzuatı veya Fransa'da yürürlükte olan mevzuattan hangisinin uygulanacağı ortaya konulmalı, ardından gözetim ile elde edilen kişisel verilerin aktarımı da tespit edilen kurallara uygun şekilde yapılmalıdır. Bu açıdan deyim yerindeyse "iki başlı" olan Fransız veri koruma hukukunda, uygulanacak kuraldan önce, hangi hukukun öncelikli olduğu konusu önemlidir. Bununla birlikte özellikle GDPR'da yer verilen temel ilkelerin uygulanması, aynı anda hem AB mevzuatının hem ulusal mevzuatın uygulandığı veri işlemelerde söz konusu olabilecektir.

İfade edildiği üzere Fransa'da video gözetim ile elde edilen kişisel verilerin korunması ve işlenmesinin düzenlemesi, hem GDPR ve Polis-Adalet Direktifi ile diğer AB düzenmeleri; hem de başta temel kanun olarak "6 Ocak 1978 tarihli ve 78-17 sayılı Veri Koruma Yasası"[411](78-17 sayılı Yasa), 1 Mayıs 2012'de yürürlüğe giren İç Güvenlik Yasası[412], 2021-646 sayılı Kapsamlı Güvenlik Koruma Özgürlükleri İçin 25 Mayıs 2021 Yasası[413] (25 Mayıs 2021 Yasası) ve diğer Fransız hukuku düzenlemeleri ile sağlanmaktadır. Bunun yanında EDPB, EDPS gibi AB otoriteleri ile CNIL, Ulusal Video Koruma Komisyonu gibi ulusal resmi oluşumlar bulunmakta ve kişisel verilerin korunmasına ilişkin hakkın bu yapı ile korunması amaçlanmaktadır.

[411] La Loi Informatique et Libertés.
[412] Code de la Sécurité Intérieure.
[413] Loi no 2021-646 du 25 Mai 2021 Pour Une Sécurité Globale Préservant les Libertés.

3.3.1.2. Kişisel Verilerin Korunması Yönünden Video Gözetimin Şartları

78-17 sayılı Yasa ile idari yönden bağımsız bir statü tanınarak kurulan CNIL, bireylerin mahremiyet haklarının tesisi için çeşitli düzenleme ve denetleme faaliyetleri yürütmektedir. 78-17 sayılı Yasa ise; kişisel verilerin korunması bakımından ülkenin iç serbestliğini tesis eden hükümler ile Polis-Adalet Direktifinin GDPR ile birlikte Fransız hukukuna aktarılmasını sağlayan yapıya kavuşmuştur. GDPR ve Polis-Adalet Direktifinden oluşan "Avrupa Kişisel Verileri Koruma Paketi"nin yürürlüğe girmesi, Fransa'da veri sorumlularının uyması gereken yasal çerçeveyi değiştirmiş ve İç Güvenlik Yasası hükümlerine tabi ve uygun olarak video koruma sistemleri kurulmasını gerektirmiştir[414].

Bu kapsamda video gözetim ile yapılan veri işlemenin yasal olması gerektiği ve bu yasallığın koşulları 78-17 sayılı Yasanın 5. maddesinde belirtilmiş ve kişisel verilerin işlenmesinin hangi koşullarda hukuka uygun olacağı ifade edilmiştir. İlgili madde GDPR'da yer alan veri işleme şartları ile benzer niteliktedir ve video kayıt sistemleri ile kişisel verilerin işlenmesi, yalnızca sayılan koşullardan en az birinin karşılaması halinde yasal olacaktır.

Bu sebepler kısaca;

> *"GDPR'a uygun rıza, işlemenin veri sahibinin taraf olduğu bir sözleşmenin ifası için, veri sahibinin talebi üzerine alınan sözleşme öncesi tedbirlerin ifası için veya kontrolörün tabi olduğu yasal bir yükümlülüğe uygunluk için gerekli olması, işlemenin veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerini korumak için veya kamu yararına bir görevin yerine getirilmesi ile kontrolöre verilen resmi yetkinin uygulanması için gerekli olması, işlemenin kamu makamları tarafından görevlerinin ifası sırasında gerçekleştirilen işlemeler hariç olmak üzere özellikle veri sahibinin çocuk olduğu durumlarda veri sahibinin menfaatleri veya özgürlükleri ve temel hakları ihlal edilmediği sürece veri sorumlusu veya üçüncü bir kişi tarafından izlenen meşru menfaatlerin amaçları için gerekli olması"*

[414] CNIL, Vidéoprotection: quelles sont les dispositions applicables?.

olarak ifade edilir[415] .

Yasanın 42. maddesinde ise GDPR hükümlerinin uygulama alanı "bulmayacağı" haller belirtilmiştir. Buna göre; AB hukuku kapsamına girmeyen bir faaliyet bağlamında, (…) devlet adına uygulanan ve devlet güvenliği veya savunmasını ilgilendiren kişisel verilerin işlenmesi için geçerli olan *"devlet güvenliği ve savunmasını içeren işleme faaliyetleri"*, Avrupa Birliği Antlaşması'nın V. başlık II. bölümünde yer alan *"Birliğin Dış Eylemine İlişkin Genel Hükümler ve Ortak Dış ve Güvenlik Politikasına İlişkin Özel Hükümler"* kapsamına giren faaliyetler, *"kamu güvenliğine yönelik tehditlere karşı koruma ve bu tür tehditlerin önlenmesi de dahil olmak üzere ceza gerektiren suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması veya cezaların infazı"* amacıyla yetkili makamlar tarafından yapılan işlemeler GDPR hükümlerini dışlayacaktır. Dolayısıyla belirtilen hallerde GDPR ve Polis-Adalet Direktifi kapsamından çıkılmış olacak, AB mevzuatında sayılan güvenlik sebepleri ile yapılan video gözetimler bakımından uygulama alanı bulmayacaktır.

Diğer taraftan İç Güvenlik Yasasının 251-1 ila 255-1 maddelerini kapsayan "video koruma" (*video protection*) başlığında yer alan hükümler özellikle konunun genel çerçevesini belirlemektedir. 251-2. maddesine göre; kamuya açık yollarda çekilen görüntülerin video koruması aracılığıyla iletilmesi ve kaydedilmesi ancak;

> *"kamu bina ve tesisleri ile çevrelerinin korunması, ulusal savunma için faydalı güvenlik teçhizatlarının korunması, taşıma akışlarının düzenlenmesi, trafik kuralları ihlallerinin gözlemlenmesi, saldırganlık, hırsızlık veya uyuşturucu kaçakçılığı riskine maruz kalan yerlerde kişilerin ve malların güvenliğine yönelik saldırıların önlenmesi ile özellikle bu suçlara maruz kalan alanlarda son fıkrada öngörülen gümrük yolsuzluğunun önlenmesi ve Gümrük Kanununda ifade edilen diğer suçlar, Kanunda belirtilen koşullar altında terör eylemlerinin önlenmesi, doğal veya teknolojik risklerin önlenmesi, kişilerin kurtarılması ve yangına karşı korunma, lunaparklarda halka açık tesislerin güvenliği, hukuki sorumluluğu garanti eden bir sigorta ile motorlu bir kara taşıtının işletilmesi için kapsanması gereken yükümlülüğe uygunluk sebeplerinin sağlanması"*

[415] La loi Informatique et Libertés:md.5.

amaçlarıyla yetkili kamu makamları tarafından uygulanabilir. Aynı maddede saldırı veya hırsızlık riskine maruz kalan yer ve kuruluşların can ve mal güvenliğini sağlamak amacıyla halka açık yer ve kuruluşlarda video gözetim yapılabileceği ifade edilmiştir. İç Güvenlik Yasasının 251-3 maddesinde ise; *"halka açık yollardaki CCTV işlemleri, konut binalarının içinden veya özellikle girişlerinden gelen görüntüleri göstermeyecek şekilde gerçekleştirilir. Kamuoyu, CCTV sisteminin varlığından ve sorumlu makam veya kişi hakkında açık ve kalıcı olarak bilgilendirilir"* düzenlemesi yer almaktadır. Avrupa Birliği'nin veri korumaya yönelik GDPR veya sair düzenlemeleri kapsamına girmeyen video gözetlemeler yönünden, başta İç Güvenlik Yasası olmak üzere konu hakkındaki ulusal düzenlemeler uygulama alanı bulacaktır.

26 Mayıs 2021 tarihinde Fransız Resmî Gazetesi'nde yayımlanarak yürürlüğe giren 2021-646 sayılı Kapsamlı Güvenlik Koruma Özgürlükleri İçin 25 Mayıs 2021 Yasası ihdas edilmiştir. Bu yeni yasa; zabıta, özel güvenlik şirketleri, yaka kameraları ve video koruması gibi gözetim araçları ve kolluk kuvvetlerinin korunmasını kapsamakta olup, Anayasa Konseyi (*Conseil Constitutionnel*) tarafından özellikle polis memurlarının kimliğinin tespitine dair tahrik suçunu oluşturan 52. maddesi yönünden kısmen "sansürlenmiş" ve pek çok tartışmaya konu olmuştur[416]. 25 Mayıs 2021 Yasasında, belediyeye bağlı çalışan polisler, özel güvenlik personelleri gibi güvenlik güçlerine yönelik hükümler, video koruma, araç içi kameralar, yaka kameraları ve dronlara ilişkin hükümler, güvenlik personellerinin kimlik tespit etmek için saldırganlık veya provokasyon durumunda uygulayabileceği önlem ve işlemler yer almaktadır[417].

2016/680 sayılı Polis-Adalet Direktifi; 78-17 sayılı Fransız Veri Koruma Yasası'nda yer verilerek Fransız iç hukukuna aktarılmıştır. Nitekim 78-17 sayılı Yasanın, Direktifin iç hukuka tatbik edildiği 3. başlığında yer alan 87. maddeye göre; Direktifin amacı, ceza gerektiren suçların önlenmesi ve tespiti, bu alandaki soruşturma ve kovuşturmalar veya kamu güvenliğine ve kamu güvenliğine yönelik tehditlere karşı koruma ile birlikte cezai yaptırımların infazı için uygulanan kişisel verilerin işlenmesidir.

---

[416] Amnesty International, France: New security law risks dystopian surveillance state.
[417] Vie Publique, Loi du 25 mai 2021 pour une sécurité globale préservant les libertés.

Veri işlemenin direktif kapsamında kabul edilmesi için veri işleme sebeplerinin "kamu güvenliğine yönelik tehditlere karşı koruma" içeren nitelikte ve aynı zamanda bu "tehditlerin önlenmesi" de dahil olmak üzere adli makamlarca verilen cezai yaptırımlarla ilgili icraî eylemlere izin veren işleme faaliyetleri olması gerekir. Diğer bir deyişle, Polis-Adalet Direktifi kapsamında olan işleme faaliyetleri, bir suçun işlenmesinden önce yürütülen polis faaliyetleri ile ilgili caydırıcı, tehditleri tespit eden amaçlarla gerçekleşen faaliyetleri kapsayabilir.

Daha önce de belirtildiği üzere, Polis-Adalet Direktifinde yer alan türden bir video gözetimi yoksa doğrudan GDPR hükümleri devreye girecektir. Yani video gözetimi yetkili makamlarca cezai soruşturma ve kovuşturmanın yapılması amacıyla ifa edilen görevler çerçevesinde ise veya yine yetkili makamlarca suçların önlenmesi veya tespiti amacını taşıyorsa faaliyet direktif kapsamında olacak, aynı zamanda genel nitelikli GDPR hükümleri de uygulanacaktır. Ancak veri işleme faaliyeti devlet güvenliğini veya ulusal savunmayı sağlamak için yapılıyorsa, AB düzenlemeleri kapsamına girmeyip, sadece ulusal Veri Koruma Yasası hükümlerine tabi olmaya devam edecektir[418].

3.3.1.3. Konu, Kişi ve Sebep Yönünden Video Gözetim

Fransa'da kamusal alanlarda yapılan gözetimde kişi yönünden yetkiyi belirleyebilmek için özellikle gözetim yapılacak alan, bu alanda kullanılan video kamera cihazının yapısı ve hangi hukuk sistemine tabi olunduğu hususlarının belirlenmesi önem taşımaktadır. Zira ancak bu şekilde hangi mevzuata (Avrupa Birliği ile eşgüdümlü uygulanan mevzuat veya yalnızca ulusal mevzuat) tabi olunacağı ve gözetimin yapılma amaçlarının hukuka uygunluğu denetlenebilir hale gelecektir. Örneğin; video kayıt sistemi ulusal güvenlik-kamu güvenliği gibi bir sebebe dayanılarak kurulmuş ve bu şekilde kişisel veri elde edilmeye başlanmış ise; Fransız Veri Koruma Yasası, İç Güvenlik Yasası ve 25 Mayıs 2021 Yasası (ve sair özel nitelikli düzenlemeler) hükümlerine bakılarak video izlemeye ilişkin yetkili kişi-makam-kurum-kuruluşlar tespit edilmelidir.

---

[418] CNIL, Directive « Police-Justice » : de quoi parle-t-on?.

İç Güvenlik Yasasının yetkilendirme konusunu düzenleyen 252-1 maddesinde düzenlendiği üzere yasa kapsamında bir video koruma sisteminin kurulması, ilgili departmandaki Devlet temsilcisinin ve Paris'te ulusal savunma konuları dışında, Bakanlığın bildiriminden sonra verilen Emniyet Müdürü'nün (*préfecture de police*) iznine tabi olacaktır. Sistem, birden fazla departman bölgesinde kurulu kameralar içerdiğinde izin, başvuranın genel merkezinin bulunduğu departmandaki Devlet temsilcisi ve bu merkez ofisi Paris'te bulunuyorsa, video koruması için departman komisyonuna danıştıktan sonra Emniyet Müdürü tarafından verilir ve kameraların takıldığı bölümlerdeki Devlet temsilcileri bilgilendirilir.

Yasanın 252-2 maddesi ise Emniyet Müdürlüğü yetkilendirmesinin, özellikle video koruma sistemini çalıştırmaktan veya görüntüleri izlemekten sorumlu kişilerin niteliği ve yasa hükümlerine uygunluğu sağlamak için alınması gereken önlemler ile ilgili tüm yararlı önlemleri belirleyeceğini, görüntülerin izlenmesinin yalnızca ulusal polis ve jandarma teşkilatları ile zabıta teşkilatlarının münferit olarak belirlenmiş ve yetkili temsilcileri ile münferit olarak atanan kişiler tarafından sağlanabileceğini belirtir. 25 Mayıs 2021 Yasasında belirtilen pek çok video kamera kayıt sisteminin kuruluşunun, ilgili maddelerde belirtilen yetkilerle donatılan belediye başkanlarının önceden yapacakları talebe tabi olduğu ifade edilir[419].

Öyle ki; yine İç Güvenlik Yasasının 522-2 gibi bazı hükümlerinin işlerlik kazanacağı hallerde video kayıt sistemleri kurulması hakkındaki taleplerin, görevlendirilen belediye başkanları tarafından "müştereken" yapılması durumu söz konusu olmaktadır. Ek olarak, kırsal bölgelerde polis tarafından yapılan genel nitelikli kayıtlara ilişkin mezkûr Yasanın 46. maddesinin birinci fıkrasında yer alan video kamera sistemlerinin uygulama şartları ve toplanan verilerin kullanımının, CNIL'in yayınlanmış ve gerekçeli görüşünden sonra alınan Conseil d'État (Fransız Danıştayı) kararnamesiyle belirleneceği hüküm altına alınmıştır[420].

---

[419] Loi 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés:md. 46.
[420] Ibid.

25 Mayıs 2021 Yasası ile birlikte Fransa'da CCTV görüntülerini alabilen servisler genişletilmiş, zabıta ekiplerine mağazaların yakınındaki kameralardan alınan görüntüleri izleyebilme yetkisi verilmiş, toplu taşımayı güvence altına almak için bazı RATP ve SNCF (*Régie Autonome Des Transports Parisiens ve Société Nationale Des Chemins De Fer Français*- şehir içi ulaşımı sağlayan kuruluşlar) görevlilerine, Devletin sorumluluğu altında halka açık yolların video gözetimine erişebilme yetkisi verilmiştir. Bunların yanında polis ve jandarma tarafından kullanılan yaya kameralarının, belirtilen bazı güvenlik riski teşkil eden durumlarda görüntüler hem komuta merkezine hem de müdahalenin yürütülmesine dahil olan yetkililere canlı olarak iletilebileceği bir yapı tasarlanmıştır.

Mezkûr Yasanın "Video Koruma ve Görüntü Yakalama" (Vidéoprotection Et Captation D'images) başlığı altında düzenlenen 40 ila 49. maddelerinde genel olarak;

> *"(...)Belediyeler arası işbirliğine yönelik olarak bir kamu kuruluşunun, yerel suç önleme sistemleri üzerindeki yetkisini kullandığında (...)CCTV cihazlarının satın alınması, kurulması ve bakımına karar verebileceği, (...)kırsal kesimde güvenlik görevlerini yerine getirirken, kırsaldaki muhafızlara (Jandarma), Bakanlıktaki (İçişleri Bakanlığı) Devlet temsilcisi tarafından, -her yerde- bireysel kameralar aracılığıyla, müdahalelerinin görsel-işitsel kaydına devam etmeleri için yetki verilebileceği, (...)bireysel kameraların verildiği personelin, yaptıkları kayıtlara doğrudan erişemeyeceği, kişisel verileri içeren kayıtların, hukuki, idari veya disiplin kovuşturması kapsamında kullanıldığı durumlar dışında altı ay sonra silineceği"*

ifade edilmektedir. Görüldüğü üzere konu, kişi ve sebep yönünden yetkilendirmenin gerekli yasal düzenlemelerin yapılması ile gerçekleşmesi mümkün olsa da GDPR'da yer alan temel ilkelerin her koşulda sağlanması, bireylerin özel hayatlarının ve mahremiyet haklarının korunması açısından önemlidir. Ayrıca video gözetim sistemlerinin kullanılması konusunda tercih edilmesi gereken yaklaşımın, salt güvenlik veya

mahremiyet sağlama değil aynı zamanda ülkenin öznel koşulları gözetilerek oluşturulması gerekir.

3.3.1.4. Eleştiriler

Fransa'da kamusal alanlarda yapılan video gözetimin uygulama alanının oldukça geniş olduğu ve izlemelerde daha çok kamu güvenliği sebebinin dayanak alındığı gözlemlenmektedir. Bu sebeple AB mevzuatının yanında, ulusal hukukta video izlemeye ilişkin çeşitli düzenlemeler yapılmış, CNIL, Ulusal Video Koruma Komisyonu ve kamu kurumları içinde yer alan konu ile ilgilendirilen departmanlar aracılığı ile bir denetim ya da fren mekanizması tasarlanmıştır. Böylece GDPR kapsamı dışında kalan sebepler ile yapılan video gözetimler açısından da seyrinin izlenmesi mümkün bir düzenlemeler bütünlüğü göze çarpmaktadır. Ayrıca özellikle emniyet birimlerinin vermiş olduğu video gözetim sistemi kurulmasına dair kararların, gözetimden sorumlu olarak yetkilendirilen departmandaki devlet temsilcisinin onayına tabi olması, faaliyetlerin ayrıca resen harekete geçme yetkisi verilen CNIL ve Ulusal Video Gözetim Komisyonu tarafından doğrudan denetlenmesi hususları önem arz etmektedir.

Video gözetim konusunun bireylerin mahremiyetlerinin tesisi ve korunması yönünden hassas olması sebebiyle, ülkedeki 25 Mayıs 2021 Yasası yoğun şekilde eleştirilmiştir. Öyle ki; Anayasa Konseyi ilgili düzenleme hakkında bir çekince yayınlamış, güvenlik güçlerinin veya belediyelere bağlı bulunan zabıtaların yetkili bulundukları bölgeler dışında bulunan video kayıtlarına erişme hakkını sakıncalı bulmuştur[421]. Ayrıca video izleme konusunda güvenlik aktörlerinin bazı ayrıcalıklı yetkilerinin güçlendirilmesi, görevlerinin yerine getirilmesi için kurulumu ve yetkilendirmesi "kolay" araçlar tahsis edilmesi, yaka kamerası gibi yeni teknolojik donatılara sahip video cihazlarının kullanımı ve halka açık yollar gibi alanlarda belediye polisi, ulaşım yetkilileri (RATP,SNCF) aktörlerinin de yetkilendirilmesi hususlarının

[421] Vie Publique.

bireylerin mahremiyetlerinin hukuka aykırı şekilde ihlal edilmemesi için özenle kullanılması gerekecektir.

Ülkede ayrıca -yoğun kamera kullanımına rağmen- video gözetime dair çalışmaların oldukça az hatta "kayıp" olduğu belirtilir[422]. Video gözetim literatüründeki çalışmaları ile bilinen Eric Heilmann; video gözetimin 2007 yılına kadar belediye başkanlarının elindeki veya yönetimindeki bir araç olduğunu, cihazları polisin çalışmalarını desteklemek için kullanmaya (ya da kullanmamaya) karar verme yetkisinin belediye başkanlarında olduğunu, 2007 yılında Nicolas Sarkozy devlet başkanı olduktan sonra git gide artan CCTV kullanımı ile İçişleri Bakanlığı'nın ulusal bir strateji dahilinde hareket etmeye başladığını belirtir[423]. Bununla birlikte Heilmann tarafından ülkede merkezi otorite ile yerel birimler arasında CCTV'lerin kurulumu ile ilgili bir gerilim olduğu, devletin daha çok kamera kurulumu arzu ederken, video gözetim cihazları kurma/kurdurma konusunda bazı yetkileri olduğu görülen belediyeler gibi yerel birimlerin buna direndiği ifade edilir[424].

Belirtmek gerekir ki; yakın tarihte 19 Temmuz 2022'de CNIL'in akıllı ya da arttırılmış *(caméras augmentées)* kameraların kamusal alanlarda kullanımına ilişkin yayınladığı dokümanda; bu tür otomatik görüntü işleyen yazılımlara sahip kameraların sadece kişileri kayıt altına almayı değil kişilere ilişkin bilgileri otomatik şekilde analiz etmeyi amaçladığı, kişilerin görüntüsünün alınmasının onlara ait kıyafet, maske gibi çeşitli özellikleri ön plana çıkaracağı, kameraların doğaları gereği müdahaleci olduğu ve bu cihazların kontrolsüz bir şekilde genelleştirilmesinin kamusal alanda bireylerin davranışlarına etkiyen bir riskli gözetime yol açacağı belirtilmiştir[425].

---

[422] KLAUSER, F.R. (2009). "Lost surveillance studies: a critical review of French work on CCTV". Surveillance & Society 6(1). s.23

[423] HEILMANN, E. (2011). "Video surveillance and security policy in France: From regulation towidespread acceptance". (Galley Proof çev.) Information Polity 16.s.9.

[424] Ibid, s.1.

[425] CNIL (19.07.2022), Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position. (Erişim Tarihi: 11.09.2022) https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position

CNIL'in amaçladığı, kamusal alandaki kullanımların "meşru da olsa" adil ve orantılı kullanımı konusunda çağrı yapmaktır. Nitekim her meşru kullanım adil kullanım anlamına gelmemektedir. CNIL, bu kameraların hiçbir zaman insanların "puanlanması" için kullanılmamasını sağlayan kırmızı çizgiler konulması gerektiğini savunur ve Fransız yasalarının, suçların tespiti ve kovuşturulması için, önceden var olan CCTV kameralarının kullanımına cevaz veren hükümler hariç, kamu makamları tarafından "arttırılmış" kameraların kullanılmasına izin vermediğini iddia eder[426].

CNIL'in çalışma konusuna doğrudan temas eden bu çağrı içerikli doküman ile "akıllı" kameraların kullanımında bireylerin menfaatini temel alan ve yasa ile konan hükümler ve yetkilendirme yapılması, kullanımların yine ayrı bir makamın denetimine tabi olması, anonim veriler ile istatistik üretilmesi gibi alternatiflerin ele alınması gibi hedeflere yönelik bir çağrı yapmış, deyim yerindeyse pozisyonunu belli etmiştir[427]. Akıllı kameraların kamusal alanda kullanımı ve kullanımın sınırlanması, CNIL'in 2022-2024 stratejik planına da girmiş bir konudur[428]. Duyulan endişenin sebebi ise; artan akıllı kamera kullanımının, hukuk ile meşru bir zemin yaratılması rağmen bugün Çin'in geldiği vatandaşların skorlanması seviyesinde bir totaliterlik riskini bünyesinde barındırmasıdır.

Heilmann'ın 2011 yılında yayınlanan çalışmasından itibaren pek çok ülkede olduğu gibi Fransa'da da video gözetim cihazlarının sayısının arttığı aşikardır. Burada çalışmada ortaya konmaya çalışılan sav doğrultusunda ifade edilmek istenen, Hailmann'ın da belirttiği üzere devletlerin CCTV'leri kullanımın politik değişimlerden etkilenen bir güvenlik stratejisi ekseninde sağlandığıdır. Halbuki güvenlik ihtiyacı hükümetlerin değişiminden etkilenmeyen, politik kararlardan ari bir durum olarak her zaman mevcuttur.

---

[426] Ibid.
[427] CNIL (19.07.2022), Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position.
[428] CNIL, Plan Stratégique 2022-2024, axe 3.s.7. (Erişim Tarihi: 11.09.2022) chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cnil.fr/sites/default/files/atoms/files/cnil_plan_strategique_2022-24.pdf

Fransa'da 2007 yılına kadar hem insanlara hem de mülklere yönelik saldırılara karşı en savunmasız olan kentsel yerlerde seçici olarak kullanılan CCTV'nin, 2007 yılından sonra her koşulda ve her yerde kullanılması gereken bir araç olarak görülmeye başlanması[429] yalnızca CCTV'lerin değil genel olarak gözetim kavramının girift yapısının ve sebep olduğu tartışmaların da bir tezahürüdür. Kişisel verilerin korunması yönünden günümüzde GDPR, GDPR öncesinde de Veri Koruma Direktifi koruması altında olan dolayısıyla konu bağlamında iyi uygulama örneği addedilebilecek Fransa'da dahi hukuki düzenlemelerin eksiksiz bir koruma sağlayabileceğini iddia etmenin doğru olmadığı kanaatindeyim.

3.3.2. Ülkemizde Kamusal Alanlarda Uygulanan Video Gözetim

Ülkemizde kamusal alanda gözetleme KGYS veya MOBESE ile yapılır. MOBESE gibi kamusal alanları görüntüleme sistemleri veya ALPR'ler gibi plaka okuma cihazları KGYS'ye dahildir. MOBESE esasen İstanbul Emniyet Müdürlüğü çatısı altında ve İstanbul Valiliği'nin desteği ile yürütülen bir KGYS unsuru olarak, İçişleri Bakanlığı teşkilatı çatısında, suçun azaltılması, kamu hizmetlerinin ve yönetiminin kolaylaştırılması amacıyla kullanılmaya başlanmış, elde edilen görüntülerin önce küçük birimlerin veri tabanlarına daha sonra ana komuta kontrol merkezlerinde toplanması ve sistemin genel işleyişinin ise İçişleri Bakanlığı bünyesindeki Emniyet Genel Müdürlüğü'nce yapılması kararlaştırılmıştır[430]. İhtiyaç duyulan bölgelere jandarma komutanlıkları, belediye başkanlıkları hatta muhtarlıklar tarafından dahi video gözetim sistemi kurulabildiği belirtilmektedir[431].

Ülkemizde video gözetim sistemlerinin kamusal alanda kullanımına, bunlar ile elde edilen kişisel verilerin muhafazasına, aktarımına, kullanımına ilişkin ayrıca bir kanuni dayanak ya da spesifik bir ikincil düzenleme bulunmamaktadır. Bu sebeple MOBESE'lerin kullanımı; kamu düzeninin ve kamu güvenliğinin sağlanması, suç

---

[429] Ibid, s.1-2.
[430] ÇAPAR,2011.s.81-82.
[431] BAŞAR, C. (2017). Devletin Kitlesel Gözetleme Araçlarının Özgürlükler ve Hukuk Güvenliği Üzerindeki Etkileri ile Bunların Yasal Dayanakları Üzerine Bir İnceleme. Türkiye Barolar Birliği Dergisi, 133, s.105-106.

işlenmesinin önlemesi, emniyetin tesisi hakkındaki genel sebep veya koşullara dayandırılmaktadır[432]. MOBESE'lerin kullanımına gerekçe yapılan dolaylı ve dağınık bazı hukuki düzenlemelere bakıldığında; 2559 sayılı Polis Vazife ve Salahiyet Kanunu (PVSK), 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanun (JTGYK), 5442 sayılı İl İdaresi Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) karşımıza çıkmaktadır. PVSK'nın ek 7. Maddesinde yine maddede yer alan bazı suçlar kapsamında istihbarî faaliyet yürütülürken suç işlenmesinin önlenmesi maksadıyla teknik araçlarla izleme yapılabileceği belirtilmektedir.

JTGYK'nın ek 5. maddesinde de "belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme" yapılabileceği hüküm altına alınmıştır. Teknik araçlarla izlemenin 5271 sayılı Ceza Muhakemesi Kanununa (CMK) göre kamuya açık alanlarda şüpheli veya sanığın ses ve görüntü izlemesine tabi olması olarak tanımlandığı düşünüldüğünde; PVSK ve JTGYK'da yer alan hükümlerin belirli suçlar için yalnızca şüpheli veya sanık açısından yapılan kamusal alandaki video gözetim sistemi kullanımları için gündeme geleceği ifade edilebilir. Dolayısıyla bunun dışındaki faaliyetler açısından şüpheli veya sanık dışında kalan kişilerin izlenmesi açısından bu hüküm uygulama dışı kalacaktır.

Yine "İl İdaresi Kanunu'nun 11 A maddesi kapsamında" valilerin, 32 B maddesi kapsamında ise kaymakamların "kamu düzeni ve güvenini korumak ile suç işlenmesini önlemek için gerekli tedbirleri alacağına" dair hükümlerin, kamusal alanlarda video kamera sistemleri kurulmasına hizmet eden düzenlemeler olup olmadığı açık değildir. Öyle ki; vali ve kaymakamların bu düzenlemelere dayalı şekilde kamusal alanların kameralı gözetimi konusunda yetkili sayılamayacakları, bahis konusu edilen hükümlerdeki mülki amirlerin genel olarak kamu düzenini sağlama görevlerinin genel bir

[432]Ibid, s.114.

görev olmayıp, spesifik olarak belirli an ve olaylar için olduğu, hasıl olan ihtiyaçlar ortadan kalktıktan sonra sona ereceği ifade edilmektedir[433].

KVKK'nın 3. maddesinin (d) bendine göre *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanan kişisel veri; aynı maddenin (e) bendine göre Kanunda sayılan şekilde elde edilme, kaydedilme, depolanma, aktarılma gibi işlemlere tabi tutulduğunda işlenmiş kabul edilmektedir. Bu sebeple önceki başlıklarda da izah edildiği üzere, bireylerin görüntülerinin alınması, depolanması veya bu görüntülerin tekrar tekrar izlenebilmesi veri işleme olarak kabul edilmelidir ve bu sebeple görüntülerin gizlilik ve bütünlüğünün sağlanması zorunlu olmalıdır[434].

KVKK'da sayılan istisna halleri de dahil her durumda uyulması gereken temel ilkeler ise 4 üncü maddede: *"hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"* şeklinde ifade edilmiştir. Bu ilkeler "95/46/EC sayılı Veri Koruma Direktifi'nde ve daha kapsamlı şekilde GDPR"da da yer almaktadır. Bu ilkelerden kişisel verilerin ancak geçerli bir sebebe dayanarak işleneceğini düzenleyen belirlilik ilkesi; kişisel verilerin işlenmesine ilişkin hususların net bir biçimde ilgili kişilerce idrakine ve kişisel veri işleme faaliyetinin hangi yasal dayanak kapsamında gerçekleştirildiğinin tespit edilmesine yarayacaktır.

Bir diğer önemli gerekliliği doğuran olan ölçülülük ilkesine göre ise; veri işleme eyleminin kendisi, işleme amacı ile uyumlu ve örtüşen yapıda olmalıdır ve hali hazırda var olmayan sebeplerin daha sonra ortaya çıkacağını düşünerek veri işleme yapılmamalıdır. Buradaki önemli nokta yeterli verinin ötesinde veri işlemekten imtina edilmesidir. Ölçülülük ilkesi, kişisel verilerin işlenmesi ile bu işlemeyi gerektiren sebep arasında uygun bir denge kurulması gerekliliğini ifade eder. Ölçülülük ilkesinin

---

[433] KÜÇÜK, T. S. (2018). "Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı ile Önleyici Amaçla İzlenmesi". Yeditepe Üniversitesi Hukuk Fakültesi Dergisi Cilt: Xv Sayı 1, s.73-74.

[434] ALKAN, M., MENTEŞ, T., İNCEEFE, M.A. (2020). "Kişisel Verileri Koruma El Kitabı Teknik Uygulama ve Uyumluluk". Ankara: Nobel Yayıncılık.s.142.

yorumlanmasında Anayasa Mahkemesi'nin 28.09.2017 tarihli ve E.2016/125, K.2017/143 numaralı kararlarında yer alan ölçülülük kriterlerinin kullanılması önem arz edecektir. Anayasa Mahkemesi kararında "elverişlilik, gereklilik ve orantılılık" unsurları ölçülülüğün temel üç unsuru arasında değerlendirilmektedir.

KVKK'nın 5 inci maddesi ise kişisel verilerin kişilerce verilmiş açık rıza olmaksızın işlenemeyeceğini belirterek, hangi hallerde açık rıza aranmaksızın veri işleyebilmenin mümkün olabileceğini düzenler. Bu haller;

> *"a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."*

şeklinde ifade edilmiştir. Dolayısıyla kanaatimce video kameraların kullanılmasında KVKK'nın istisna hallerine dayanılmayan veri işlemeler açısından, kanunlarda açıkça öngörülme veya hukuki yükümlülüğün yerine getirilmesi için zorunluluk sebeplerinden birine dayanılması gerekecektir.

Kamera sisteminin belirli, açık ve meşru zemini sağlaması için; kamera kayıtları alınırken verileri işlenen kişilerin durumu açık ve kolay bir şekilde anlaması, faaliyetin hangi işleme şartına dayanarak gerçekleştiğinin "tespit edilebilir" olması, kamera kaydı alınmasının amacının belirli bir biçimde-belirliliği sağlayacak kapsamda sunulması gerekecektir. Bu sebeple kameraların yerleştirildiği yerlere uyarıcı-açıklayıcı levhalar asılması önemlidir. Bu levhaların kolay bir biçimde anlaşılabilir olması, dürüstlük ilkesine uyulması bakımından da aranacaktır[435]. Yargıtay kararlarında da kameraların

---

[435] Kişisel Verileri Koruma Kurumu, Rehberler, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s.9.

açık alanda bulunmasının kişilerin rıza vermiş sayılması anlamını taşımayacağı, güvenlik kamera sistemlerinin kurulduğu bölgelerde uyarıcı levhalar vb. mekanizmalar olması gerektiği ifade edilmiştir[436]. Amacın meşru olması ise, verilerin işlenmesinin ve kamera kaydının alınmasının, "gerekli" olması manasına gelecektir. Diğer taraftan 12 nci maddenin gereği olarak Kişisel Verileri Koruma Kurulu tarafından belirlenen teknik-idari tedbirler de alınmak durumunda olduğundan, periyodik ve otomatik silme ya da imha gibi hususlar yerine getirilmelidir.

Bunun yanında yasa koyucular tarafından gerek ulusal gerek uluslararası düzenlemelerde görüntü kaydeden sistemlerce işlenen kişisel verilere ilişkin ayrıksı ve daha belirleyici kuralların oluşturulması aktarım konusunun da çerçevesini netleştirecektir. Bu kapsamda gözetleme sistemleri ile kaydedilen görüntüleri gösteren ekranların herhangi bir güvenlik görevlisi ya da CCTV işletme odasından geçen herkes tarafından değil, yetkili kişilerce izlenmesi, görüntülerin formattan bağımsız olarak korunması, elektronik formatta şifrelenmesi, fiziksel ortamda kilitleme işlemine tabi tutulması, güvenlik ortamına alınıp bu şekilde izlenmesi, veri sahiplerinin mahremiyetlerinin meşru bir gerekçe olmaksızın ifşa edilmemesi, tüm taraflar yararına adil ve dengeli bir teknoloji kullanımı oluşturulması gibi bir dizi teknik ve idari ilkeye riayet edilmesi önem arz etmektedir[437].

KVKK açısından kamusal alandaki video gözetimlere yönelik yapılacak değerlendirmede "istisnalar" başlıklı 28. maddeye dayanılması olasılığı akla gelmektedir. Maddenin birinci fıkrasının (ç) bendine göre; "*millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini"* tesis etmek maksadıyla kanun ile görevlendirilmiş veya yetkilendirilmiş kamu kurum ve kuruluşlarınca yürütülen *"önleyici, koruyucu ve istihbarî faaliyetler"* KVKK'nın kapsamı dışında kalacaktır. KVKK'nın kapsamı ise 2. maddede belirtildiği üzere *"kişisel verileri işlenen gerçek kişiler"* yani kameralar aracılığı ile görüntüleri kayıt altına alınan vatandaşlar ve *"kişisel verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik*

[436] Yar. 12. CD. E. 2015/4413 K.2016/4086 15.03.2016
[437] ALKAN, MENTEŞ, İNCEEFE, 2020, s.143.

olmayan yollarla işleyen gerçek ve tüzel kişiler" yani kamu tüzel kişiliği veya görüntüleri kaydeden idari kuruluşlara ilişkindir.

İfade edilmelidir ki KVKK'nın 28. Maddesinin (ç) bendinde bahis konusu edilen işlem ve eylemler; *"istihbarat birimleri tarafından maddede belirtilen amaçlar güdülerek yürütülen çeşitli operasyonlar, suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda yetkili birimlerce veri toplamak, mali istihbarat elde etmek, şüpheli işlem bildirimleri almak ve analiz ederek ilgili kurumlarla paylaşmak amacıyla yürütülen"* faaliyetlerdir[438]. Kanun hükümlerinin tamamen uygulanmayacağı birinci fıkrada sayılan hallerde bu muafiyet yalnızca işlemenin yapıldığı faaliyete yönelik olacak, farklı bir sebebe yönelik işleme yapıldığında KVKK'ya uyulması zorunluluğu tekrar canlanacaktır.

Dolayısıyla kamusal alanlardaki video gözetim aracılığı ile kişisel verilerin elde edilmesinde yani işlenmesinde, bu gözetimin bir an için *"önleyici, koruyucu ve istihbarî faaliyetler"* maksadıyla yapıldığı düşünülse de 28. maddenin dar ve olayla sınırlı olarak yorumlanması gereği göz önüne alındığında bu düşünce anlamını yitirecektir. Ayrıca kanun gerekçesinde ve komisyon raporlarında da kamusal alandaki video gözetim cihazlarının kullanımından bahsedilmemektedir.

KVKK'nın 28. maddesinin ikinci fıkrası ise dışlamak suretiyle kanunun bazı maddelerinin uygulanmayacağı, "kısmi" istisna hallerini belirtir. Burada kural, ikinci fıkrada sayılan hallerde KVKK hükümlerine uyulmasıdır. Yalnızca belirtilen kimi hususlarda bu zorunluluk ortadan kalkar. İkinci fıkraya göre; *"veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. madde, zararın giderilmesini talep etme hakkı hariç olmak üzere ilgili kişinin haklarını düzenleyen 11. madde ve veri sorumluları siciline kayıt yükümlülüğünü düzenleyen 16. madde hükümleri"*, belirtilen hallerde uygulanmayacak, kanunun diğer maddelerine aynı şekilde uyulmaya devam edilecektir.

---

[438] Kişisel Verileri Koruma Kurumu (2019). Örneklerle Kişisel Verilerin Korunması. Ankara: Kvkk Yayınları No:29.s.53.

Bahis konusu dört halden biri; *"kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması"*, diğeri ise *"kişisel veri işlemenin 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"* dır. Ancak kısmi istisnalar kapsamında yapılacak uygulamalar, olay bazında veya münhasır bir faaliyet çerçevesinde olmalıdır-ki sürekli yapılan MOBESE faaliyetlerinin bu şartı karşıladığı söylenememektedir.

Ayrıca kanunen aranan "gereklilik" örneğin suçun önlenmesi amacıyla kişisel verilerin işlenmesi yönünden de geçerlidir. Dolayısıyla bu kapsamda somut bir suç şüphesi oluşmaksızın kamusal alanlara kurulan sistemler tarafından elde edilen kişisel verilerin emniyet birimlerindeki komuta merkezlerine aktarılmasının, suç işlenmesinin önlenmesi veya suç soruşturması yönünden hasıl olan bir gereklilik veya kanunen verilen belirli bir görev-yetki sonucu yapılması beklenir.

Diğer taraftan "suç işlenmesinin önlenmesine ilişkin gereklilik" hususunun geniş bir yoruma tabi tutularak değerlendirme yapıldığı bir ihtimalde dahi, 28. maddenin ikinci fıkrasına göre KVKK'dan muaf tutulacak hükümler "aydınlatma yükümlülüğüne, ilgili kişinin haklarını düzenleyen maddeye ve veri sorumluları siciline" ilişkindir. Nihayetinde KVKK'nın genel kapsamına ve temel ilkelerine, işleme şartlarına, aktarıma ilişkin uyulması gereken hususlar yine geçerli olacak ve kanuni şartların sağlanması gerekecektir.

Daha önce de belirtildiği üzere, kamusal alanda yapılan video gözetimin temel hak ve hürriyetlerin sınırlanması olduğu gerek ülkemizde gerek uluslararası literatürde kabul edilir. Öyle ki Yargıtay 12. Ceza Dairesi'nin 2012 yılında verdiği bir kararda aşağıdaki şekilde hüküm kurulmuştur:

> *"…Özel hayat kavramının; kişinin sadece gözlerden uzakta, başkalarıyla paylaşmadığı, kapalı kapılar ardında, dört duvar arasındaki yaşantısı ve mahremiyetinden ibaret değil, herkesin bilmediği veya bilmemesi gereken, istenildiğinde başka kişilere açıklanabilen, tamamen kişiye özel hayat*

olayları ve bilgilerin tamamını içermesi karşısında, kamuya açık alanda bulunulduğunda 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(...)" [439].

Yine aynı Daire'nin 2016 yılında vermiş olduğu kararda ise şu hususlar yer alır:

"kamuya açık alandaki kişinin, gün içerisinde yapıkları, gittiği yerler, kiminle niçin, nasıl, nerede ve ne zaman görüştüğü gibi hususları tespit etmek amacıyla sürekli denetim ve gözetim altına alınması sonucu elde edilmiş bilgileri ya da onun başkalarınca görülmesi ve bilinmesini istemeyeceği, özel yaşam alanına girdiğinde şüphe bulunmayan faaliyetleri özel hayat kapsamına dahildir; ancak, süreklilik içermeyen ve özel yaşam alanına dahil olmayan olay ve bilgiler ise bu kapsamda değerlendirilemez"[440].

Bu karardan anlaşıldığı üzere kamusal alandaki sistemli ve sürekli kameralı izlemelerin özel hayatın gizliliğinin sınırlanması olduğu, bireylerin sosyal hayata entegre olmalarının neticesinin mahremiyetin tamamen feda edilmesi anlamına gelmeyeceği, kalabalık içinde bilinmeme ihtiyacının hukuken tanındığı konularında herhangi bir tartışma olmadığı söylenebilir.

Ayrıca Anayasa'nın 20. Maddesinde "özel hayatın gizliliği" alt başlığında düzenlenen "kişisel verilerin korunmasını isteme hakkı"na video gözetim ile getirilen sınırlamanın yine Anayasa'nın 13. Maddesine uygun şekilde yapılması, hakkın özüne dokunmadan, Anayasal sebeplere dayanılarak ve kanunla yapılması gerekecektir. Bu durumda kamusal alanlardaki video gözetimi doğrudan ve açık şekilde düzenleyen bir kanun maddesi olmadığı gibi, hali hazırdaki dolaylı hükümler içeren kanuni dayanakların da çok geniş ve belirsiz ibarelerden oluştuğunu söylemek yanlış olmayacaktır. Bunlarla birlikte; temel hak ve hürriyetlerin sınırlandırılmasında bir an için kanunla sınırlama şartının yerine gelmesi ihtimalinde de kişisel verilerin korunması hakkının

---

[439] Yargıtay 12. Ceza Dairesi 2011/7345 E. 2012/8936 K. 03.04.2012 T.
[440] Yargıtay 12. Ceza Dairesi 2015/4413 E. 2016/4086 K. 15.03.2016 T.

sınırlandırılmamış bir özünün muhakkak kalması, araç ile amaç arasında daima bir "ölçü" olması gerekecektir[441].

KVKK'nın 28. maddesinin sınırlı yorumlanmasına ilişkin 23 Ocak 2018 tarihli ve 30310 sayılı Resmî Gazetede yayınlanan "28.09.2017 tarihli ve E. 2016/125, K. 2017/143 sayılı Anayasa Mahkemesi kararında"[442] Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendine ilişkin yapılan incelemede; Anayasa'nın 13. maddesine uygun yorum yapılması, temel hak ve hürriyetler sınırlanırken hakların özüne dokunulmaması, hak ile korunan amacın etkisinin bertaraf edilmesi sonucunu doğuran nitelikte sınırlamalar yapılmaması gerektiğinin altı çizilmiştir[443].

Dolayısıyla kamusal alanda yapılan sürekli izlemeler yönünden, her koşulda gerçekleştirilmesi beklenen, demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacının sağlanması, hakkın özüne dokunulmaması, ölçülülük ilkesine riayet edilmesi, KVKK gereği veri güvenliğine ilişkin tedbirlerin alınması suretiyle kameralı gözetimin gerçekleştirilmesidir. Nihayetinde gerek Anayasa gerekse ilgili Kanun hükümleri kameraların kullanılmasındaki esas amaç olan "güvenlik sağlama" maksadının, bireylerin özel yaşamlarının izlenmesine araç kılınmasına müsaade etmemektedir.

Diğer taraftan KVKK'nın 28 inci maddesi kapsamında istisna olarak değerlendirilen "*millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini"* tesis etmek maksadıyla kanun ile görevlendirilmiş veya yetkilendirilmiş kamu kurum ve kuruluşlarınca yürütülen *"önleyici, koruyucu ve istihbarî faaliyetler"* hallerinin; Anayasa'dan 2001 yılında çıkartılan "tüm" temel hak ve hürriyetlere ilişkin genel

---

[441] GÖZLER, K. (2020) İnsan Hakları Hukuku. Bursa: Ekin Basım Yayın Dağıtım. 3. Baskı. s.392.

[442] Anayasa Mahkemesi E. 2016/125, K. 2017/143 28.09.2017 T. (Erişim Tarihi:12.08.2022)https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2017-143-nrm.pdf

[443] Kişisel Verileri Koruma Kurumu, "Ses kayıt özelliği bulunan güvenlik kamerası kullanılması" ile ilgili Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli ve 2020/212 sayılı Karar Özeti, (Erişim Tarihi:12.08.2022). https://www.kvkk.gov.tr/Icerik/6892/2020-212

sınırlama sebepleri de düşünüldüğünde, Anayasa'nın 13 üncü maddesine uygun bir sınırlama içerip içermediği tartışmalı hale gelecektir.

Mülga maddenin ilk fıkrası *"temel hak ve hürriyetler, Devletin ülkesi ve milletiyle bölünmez bütünlüğünün, millî egemenliğinin, Cumhuriyetin, millî güvenliğin, kamu düzeninin, genel asayişin, kamu yararının, genel ahlâkın ve genel sağlığın korunması amacı ile... sınırlanabilir"* olup, 9 adet genel sınırlama sebebini (milli güvenlik, kamu düzeni, genel asayiş, kamu yararı…) barındırmakta idi. KVKK'nın 28 inci maddesinde de yine bu sebeplerin her ne kadar kapsamı *"önleyici, koruyucu ve istihbarî faaliyetler"* ile sınırlandırılarak da olsa yer alması, Anayasa'nın hali hazırdaki 13. ve 20. maddeleri bakımından sorgulanabilir durumdadır. Ketizmen 2006 yılında yazmış olduğu doktora tezinde, kişisel verilerinin işlenmesinde 2001 yılında Anayasa'dan çıkarılan genel sınırlama sebeplerine dayanılmasını Anayasa'nın 13 ve 20. maddelerine aykırı bulmuş, kişisel verilerin işlenmesi hakkındaki hukuki düzenlemeler açısından hiçbir sınırlamanın yer almadığı Anayasa'nın 20. maddesine uygun hareket edilmesi gerektiğini belirtmiştir[444].

Uygulamada cihazların kurulma gerekçelerinin, kamu düzeni ve güvenliğini sağlama, suç işlenmesinin önlenmesi gibi genel sebepler ile gerekçelendirildiği görülmekle birlikte, video gözetim cihazlarına birer delil toplama vasıtası olarak yaklaşıldığı da göze çarpmaktadır. Bu açıdan da yine CMK'nın 140. maddesine göre "somut delillere dayanan kuvvetleri şüphe sebeplerinin olması" ve "başkaca biçimde delil elde edilememesi" durumlarında şüpheli veya sanığın görüntü altına alınabilmesi hususu bahis konusu olacaktır. Belirtilmelidir ki; kamusal alanlarda yapılan sürekli izlemelerde dolaylı olarak geçerli olabilecek hükümlere başvurularak, temel hak ve özgürlükler aleyhine genişletici veya kıyasa yol açan yorumlamalar yapılamaz[445]. Bu durumda da

---

[444] KETİZMEN, M. (2006). "Türk Ceza Hukukunda Bilişim Suçları" (doktora tezi). Yök Tez Merkezi. (191474) s. 265,268.

[445] AKTAN, H.Y. (29.01.2022). "MOBESE'lerin Hukuki Durumu". Cumhuriyet. (Erişim Tarihi:12.08.2022) https://www.cumhuriyet.com.tr/yazarlar/olaylar-ve-gorusler/mobeselerin-hukuki-durumu-hamdi-yaver-aktan-1903580

ülkemizde bu türden izlemeler için bir hukuki dayanak bulabilmek şu an için mümkün görünmemektedir[446].

MOBESE sistemlerinin CMK'ya göre teknik araçlarla izleme olarak değerlendirilme ihtimali karşısında, bu koruma tedbirine ancak kanun maddesinde belirtilen koşullarda, katalog suçların işlenmesinden ve belirli bir şüphe derecesinin oluşmasından sonra başvurulabileceği, MOBESE sistemlerinin ise henüz suç işlenmeden kullanıldığı, bunun bir "önleyici" tedbir olduğu ifade edilmektedir[447]. Gerçekten de adli amaçlarla kullanılmayan ve yalnızca suç işlenmesini önleme ve kamusal alanlar içinde caydırıcılığı hedefleyen kameralar açısından CMK'da yer alan "teknik araçlarla izleme" tedbirinin söz konusu olamayacağı kanaatindeyim. Yine konu hakkındaki bir çalışmada; kanuni bir dayanağa sahip olmayan MOBESE kayıtları ile elde edilen kişisel verilerin ceza muhakemesinde kullanılmasının, kişisel verilerin korunmasını isteme ve adil yargılanma haklarının ihlali olacağı ifade edilmiştir[448].

Vücut kameraları için de aynı boşluk söz konusu olmakla birlikte kanuni bir dayanağa rastlanmamaktadır. Bu tür kameraların genellikle ses kaydetme özellikleri de bulunduğu için, kullanımları açısından Anayasa'nın 20 ve 22. maddelerinde yer alan sınırlama sebepleri, adli kolluğun CMK'da belirtilen teknik araçlarla izleme halleri gibi hukuki şartların mevcut olması gerekecektir[449]. Ses kaydetme özelliği bulunan güvenlik maksatlı kullanılan kameralara ilişkin Kişisel Verileri Koruma Kurulu'nun 2020 yılında vermiş olduğu kararda da Anayasa'nın 13. maddesinde yer alan hususlar vurgulanmış, devletin haklara ölçüsüz biçimde müdahale edilmesi manasına gelebilecek faaliyetlerden imtina etmesi gerektiği belirtilmiştir[450]. Ketizmen de aynı hususu ifade etmiş, kişisel

---

[446] Ibid.
[447] ABANOZ, B. (2015). "Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi eve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu İlişkisi" (yüksek lisans tezi). İstanbul Üniversitesi, İstanbul. s.66.
[448] CAN, N. (2020). "Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması" (yüksek lisans tezi). Yök Tez Merkezi. (653565) s. 167.
[449] ŞEN, E. (24.01.2016). "Mobese ve Kamera Sistemi ile İzleme. Hukuki Haber". (Erişim Tarihi:12.08.2022) https://www.hukukihaber.net/mobese-ve-kamera-sistemi-ile-izleme-makale,4576.html
[450] Kişisel Verileri Koruma Kurumu, "Ses kayıt özelliği bulunan güvenlik kamerası kullanılması" ile ilgili Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli ve 2020/212 sayılı Karar Özeti, (Erişim Tarihi:12.08.2022). https://www.kvkk.gov.tr/Icerik/6892/2020-212

verilerin işlenmesinin temel haklara ilişkin Anayasal sınırlandırma kurallarına tabi olacağının altını çizmiştir[451].

Basit görünüşlerinin aksine karmaşık bir ağ yapısına sahip olan MOBESE sistemleri artık ülkemizde güvenliğin sağlanmasının yanı sıra trafik akışının kontrolü, afet koordinasyon merkezi gibi izleme merkezleri ve sair sebeplerle kullanılan çok fonksiyonlu bir entegrasyon aracı haline gelmiştir[452]. Öyle ki MOBESE sistemlerinin bir süreklilik arz eden emniyet birimi olduğu ifade edilir[453]. Esas kullanım amacının dışına çıkılarak bireylerin özel yaşamlarına müdahale niteliği taşımalarından ötürü, kamusal alanda kameraların kullanımının kanun ile düzenlenmesi şarttır.

Güvenliğin sağlanması bakımından caydırıcılık ve tespit şeklinde iki önemli fonksiyonu olan kameraların, bilhassa belirli bir olayın takibi veya süreklilik arz etmeyen durumlarda kullanımı kanunla öngörülmüş olması halinde hukuka aykırı olmasa da sürekli ve kanun ile öngörülmemiş olan video gözetim faaliyetleri hukuka aykırı olacak ve bu suretle elde edilen kişisel veriler yargılamada hukuk uygun delil niteliği teşkil etmeyecektir[454]. Uygulamada dayanılan PVSK, JTGYK, CMK'da yer alan düzenlemelerin sürekli olmayan izlemeleri kapsadığı ancak MOBESE faaliyetlerinin sürekli devam ettiği dikkate alındığında[455], hem kanuni boşluk hem de dayanak hükümlerin doğru şekilde uygulanmaması durumu ortaya çıkmaktadır. Ayrıca KVKK bakımından dayanıldığı düşünülen 28. madde de kişisel verilerin sürekli olarak MOBESE'ler ile kaydı yönünden doğru bir dayanak gibi gözükmemektedir. Zira bu kez

---

[451] KETİZMEN, M. (2006). "Türk Ceza Hukukunda Bilişim Suçları" (doktora tezi). Ankara Üniversitesi Sos, Ankara.s. 262.

[452] "ÖZKAN, H., Mobese İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi, Ceza Hukuku Dergisi, 11(30)", s. 63-64.

[453] TAŞCI, U. (2016). Güvenlik Amaçlı Gözetim Aracı Olarak Türkiye'de Mobese ve Eleştiriler. Cbü Sosyal Bilimler Dergisi, 14(2), s.169. https://doi.org/10.18026/cbusos.18498

[454] ŞEN, E. (21.11.2019). "MOBESE ve Güvenlik Kameralarının Özel Hayata Müdahalesi ve Delil Vasfı". Hukuki Haber. (Erişim Tarihi:12.08.2022). https://www.hukukihaber.net/mobese-ve-guvenlik-kameralarinin-ozel-hayata-mudahalesi-ve-delil-vasfi-makale,7202.html

[455] ÖZER, H. D. (2022). "Mobese İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme". Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 24(1), s.485.

de KVKK'nın ölçülülük, belirlilik gibi genel ilkelerinin yerine getirilmesinde bir uyuşmazlık ortaya çıkmaktadır.

Ülkemizde terörizm, göç ve işsizlik kaynaklı suç gibi pek çok güvenlik kaygısı ile çeşitli gözetim projeleri[456] oluşturulmakta, bu şekilde genel asayiş ve güvenliğin sağlanmasında anlık müdahale kabiliyeti gibi kolaylıklar aranmaktadır. Ülkemizin somut koşulları kapsamında belirli bölgelerde video gözetim sistemlerine yaygın şekilde başvurulması anlaşılır olmakla birlikte; kişisel veriler yönünden hukuk güvenliğinin tesisi için kamusal alanlarda gözetim cihazlarının kullanımının kanun ile düzenlenmesi gerekir. Bu bir anayasal gereklilik olduğu gibi, AB uyumu doğrultusunda ülkemizde gelişmekte olan kişisel verilerin korunması hukukunun çerçevesinin de netleşmesini sağlayacaktır.

3.3.3. Fransa ve Türkiye Uygulamalarının Değerlendirilmesi

Hukuk devletlerinin, suçların aydınlatılması, güvenliğin sağlanması, suçların azaltılmasına yönelik politikalar üretilmesi, vatandaşların veya kamunun huzur ve barış içinde yaşamasını sağlayan pek çok görevi bulunur. Hatta bu görevlerin yerine getirilmesi devletlerin varlık sebeplerindendir. Teknoloji de sağladığı imkanlar ile günümüzde hemen her alanda fayda sağlamaktadır. Fakat günümüzde kamuya açık alanlarda da kişilerin özel hayatın gizliliği, mahremiyetin sağlanması, kişisel verilerin korunmasını isteme gibi temel hak ve hürriyetlerinin korunmasının bir gereklilik olduğu konusunda uzlaşı mevcuttur.

Bu sebeple video gözetim cihazlarının ihlal etmesi muhtemel kişisel verilerin korunmasını isteme ve özel hayatın gizliliği haklarının öncelikle hukuk yoluyla korunması gerekir. Zira hukuki düzenlemeler olmaksızın teknik koruma yöntemleri de "sahipsiz" kalmaktadır. Çalışmada iddia edilen, hali hazırdaki hukuk normlarının bireyleri kamusal alandaki gözetime karşı korumada yetersiz olduğu iken; bu hukuk

---

[456] Bkz. İçişleri Bakanlığı. Gamer Projesi. (Erişim Tarihi:12.08.2022). https://www.icisleri.gov.tr/bilgiteknolojileri/gamer-projesi

normlarının dahi bulunmaması elbette temel hak ve hürriyetlerin ihlali anlamına gelecektir.

Fransa ile ülkemizdeki kamusal alanda video gözetim uygulamaları karşılaştırıldığında birtakım önemli farklılıklar olduğu gözlemlenebilir. Öncelikle Fransa'da kameralara karşı kişisel veriler hem GDPR hem de ulusal mevzuat tarafından düzenleme altına alınmıştır. Ülkede GDPR hükümlerinin dışında kalan ve ulusal kanunlarca ayrıksı bırakılan terör gibi durumlara yönelik yapılan izlemeler dışında, GDPR'daki boşlukları doldurmak için 78-17 sayılı Veri Koruma Yasası, İç Güvenlik Yasası, 25 Mayıs 2021 tarihli Yasa gibi düzenlemeler mevcuttur.

Bu düzenlemelerde video gözetim konusunun ayrıca düzenlendiği, yargısal denetimin aktif şekilde yapıldığı, bazı hallerde kamusal alanlara kurulacak cihaz (tesisat) türlerinin, Conseil d'Etat tarafından kararname ile belirlendiği göze çarpmaktadır. Ülkemizde ise bir temel hak olan kişisel verilerin korunmasını isteme hakkı ile ilişkilendirilecek ve münhasıran video gözetim konusunun düzenlendiği bir kanun bulunmamakla birlikte, KVKK'da da hususa ilişkin bir özel hüküm ihdas edilmemiştir.

Diğer taraftan, Fransa'da video gözetim yapan cihazların etkinliğini değerlendirme ve tavsiye misyonunu yerine getiren, video koruma sistemlerinin teknik özellikleri, çalışması veya kullanımı ile ilgili olarak İçişleri Bakanına yönelik tavsiyeler yayınlayan, sistemlerin çalışmasıyla ilgili herhangi bir zorluğu veya bir ihlal teşkil etmesi muhtemel herhangi bir durumu kendi inisiyatifiyle üstlenebilen, hükümet tarafından her yıl kendisine video gözetime ilişkin rapor gönderilen bir Ulusal Video Koruma Komisyonu (*La Commission Nationale de la Vidéoprotection*) bulunmaktadır[457]. Yirmi kişiden oluşan komisyonda, İçişleri Bakanı tarafından atanan üyeler olmakla birlikte, milletvekilleri, hâkim savcılar ve CNIL üyesi de bulunur[458]. Doğrudan video gözetime

[457] Code de la Sécurité Intérieure, md. L-251-1 ila L-251-8.
[458] Code de la Sécurité Intérieure, md. R-251-1.

yönelik böyle bir oluşumun, hukuk kurallarının uygulanmasında etkinlik ve objektiflik sağlanması bakımından önemli olduğu kanaatindeyim.

Son olarak ülkemize MOBESE'ler için ayrı kontrol odalarının olmadığı ve komuta kontrol merkezinin içinde polisin de bulunduğu, tüm gözetim işlemlerinin polis idare ve kontrolünde olduğu ifade edilmektedir[459]. Fransa'da ise mevzuat gereği görüntülerin izlenmesi polis ve jandarma teşkilatları ile zabıta teşkilatlardan münferit olarak tayin edilmiş ve yetkilendirilmiş görevliler ve münferit olarak atanmış diğer kişiler tarafından sağlanabilecektir[460]. Bu şekilde video gözetim ile edinilen kişisel verilerin kontrolü polis dışında belirli sivil otorite ve birimlerce de sağlanarak, hakların korunması bakımından daha güvenli şekilde hareket edilmiş olmaktadır[461].

3.4. HUKUKUN İŞLEVSELLİĞİNE DAİR SORGULAMALAR

3.4.1. Kişisel Verilerin Korunması Hukukuna Sosyal Yaklaşım

Hamide Topçuoğlu'nun 1969 yılında yayınlanan "Hukuk Sosyolojisi" kitabının başında, pozitif hukuk kurallarının ve düzenlerinin, insan aklının ürünü olan yaratımların, kapalı bir sistem değil, gerçeklerin sistemi olduğu, bu sistemin ise diğer düzenler veya sektörler ile iletişim halinde, onlardan etkilenen ve onları etkileyen bir yapıda olduğu, hukukun hukuk dışı ile olan ilişkisinin kurulmasının hukuk disiplininin zorunlu bir ögesi olduğunu anlatan bir pasaj yer alır[462]. Çalışma boyunca da ifade edilmeye çalışılan, mahremiyet kavramının ve mahremiyet ile özel hayatın gizliliğini koruma temelinde gelişen kişisel verilerin korunması hukukunun kapalı bir kurallar sistemi şeklinde ele alınmasının yeterli olmayacağıdır.

---

[459] ÇAPAR,2011.s.87.
[460] Code de la Sécurité Intérieure, md. L-252-2.
[461] ÇAPAR,2011.s.87.
[462] TOPÇUOĞLU, H. (1969) Hukuk Sosyolojisi (Sosyoloji Açısından Hukuk). İstanbul: Cezaevi Matbaası. 3. Baskı.

Kişisel verilerin korunması hukukunun özellikle veri güvenliği konusunda teknik detayları da fazlaca olduğundan, hem ceza hukuku, idare hukuku, medeni hukuk, borçlar hukuku, ticaret hukuku gibi temel hukuk dalları ile hem de bilişim, siber güvenlik gibi farklı alanlar ile etkileşimi çok fazladır. Yani bu oldukça dinamik ve yeni hukuk dalı, mahremiyetin çalışmanın ilk bölümünde açıklanan tarihsel ve geniş perspektifli yapısı, teknik alanların hukuka entegrasyonu, hukukun teknolojik gereksinimlere yetişme çabası ve sair pek çok "aşina olunmayan" yeniliği bünyesinde barındırır. Örneğin; büyük veri gizliliği, kameraların etkisini anlamak için anomi kuramı, sosyal kontrol teorisi, kültürel çatışma teorisi ve sosyal değişim teorisi, anonimlik teknolojisi, veri şifreleme teknolojisi[463] gibi pek çok unsur veya konu mahremiyet ile kişisel verilerin korunması konseptine dahildir.

Mahremiyet ve sosyal çevre birbirleri ile etkileşim içinde olduğundan, kişisel veriler ihlal edilmeleri durumunda sosyal alanda veya dış dünyada doğuracakları sonuçlar nedeniyle de önemlidir. Ancak mahremiyetin ve kişisel verilerin korunması hakkının yasal yansımalarının etkileşimli bir bağlamı reddettiği iddia edilir[464]. Buna göre; dijitalleşmenin ve teknolojinin ticari ve siyasi etkileri doğrultusunda gelişen veri koruma yasaları tam da bu sebepler ile asıl hedeflerini kaçırmış, bir üretim biçimi olarak kişisel verilerin korunması mevzuatına dair onca düzenlemede sosyolojik yaklaşım ihmal edilmiştir[465]. Bu yaklaşıma göre yasama organlarının koyduğu kurallar ekseninde verilen rızaların, toplumsal hayatta bir karşılığı yoktur, mevzuat ile sosyal yaşam birbirinden kopuk kalmakta ve içselleştirilememektedir.

Mahremiyetin ve onu tesis etmek üzerine oluşturulan hukukun diğer -daha önemli addedilen- haklar ile denge içinde uygulanabilmesi için sosyo-hukuki bir çerçeveden, bazı ön kabullerin yapılması, veri koruma yasalarının özel hayatın sürekli gözetim altında olduğu, basında tartışıldığı, kişisel verilerin toplama ve işleme altında olduğu gerçeğini

---

[463] YUXUAN Y., XİANYU Z., YUANJİE J. (2020). Sociological Aspects of Big Data Privacy. In Proceedings of the 2020 12th International Conference on Machine Learning and Computing (ICMLC 2020). Association for Computing Machinery, New York, NY, USA, s. 230–235. https://doi.org/10.1145/3383972.3384075

[464] LEITH, P. (2006). The socio-legal context of privacy. International Journal of Law, 2(2), s.105.

[465] Ibid, s.106.

değiştirmediğinin anlaşılması gerekir[466]. Bunun için ise oluşan mevzuatın ve veri koruma otoritelerinin düzenlemelerinin ele alması gereken, teknik detayların yanında mahremiyetin aleyhindeki durumlar, teknik uygulamaların yanı sıra vatandaşlara gizliliğin korumasına niçin ihtiyaç duyulduğu, gizliliğin veya aleniliğin sosyal fonksiyonları gibi meselelerdir.

Debbie V.S. Kasper'a göre; mahremiyetin keşfinin kapsamını genişletmek için, onun sosyal hayatın düzenlenmesinde oynadığı ek roller ve mahremiyetin sosyal etkilerine dair farkındalığın geliştirilmesi için sosyolojik yaklaşımlara ağırlık verilebilir[467]. Bununla birlikte mahremiyetin ve kişisel verilerin toplumda anlaşılma şeklinin; kişisel gelişim, grup dayanışması, tabakalaşma ve sosyal kontrol alanlarında sosyal hayatı derinden etkilemesinden kaynaklı olarak öncelikle bu sosyal fenomenlerin anlaşılması da önemli birer araç olabilir[468].

Bu açıdan kişisel verilerin korunması hukukunda kurulacak bir sosyolojik yaklaşım, gizliliğin toplum tarafından doğru anlaşılmasına, bu alanda getirilen hukuk kurallarının mantığının sorgulanmasına imkân sağlayabilir. Zira bu haliyle, veri güvenliğine niçin gerek duyulduğu, tasarımda gizlilik, veri minimizasyonu gibi ilkelerin ne anlama geldiği ve ne işe yaradığı, açık rızanın tam olarak neyi sağladığı gibi konuların bireylerce doğru şekilde kavranıp kavranmadığı şüphelidir.

Mahremiyeti ve kişisel verileri sosyal bir konu ve davranışsal bir kavram olarak ele almak, bu mefhumları elde etmenin ne işe yaradığını ve kaybetmenin maliyetlerinin gözden geçirilmesini sağlar[469]. Örneğin kamusal alanlarda video gözetim cihazlarının gizliliği nasıl ihlal ettiği, bu cihazlarca elde edilen görüntülerin niçin kişisel veri olduğu, kişisel verilerin kuralsızca elde edilmesinin ne gibi riskler barındırdığının kavranması ancak konunun sosyal yönüyle hukuk kuralları arasındaki ilişkinin anlaşılmasına ve anlatılmasına bağlıdır. Bu açıdan kişisel verilerin korunmasında deyim yerindeyse

---

[466] Ibid.
[467] KASPER DEBBIE V.S. (2007). Privacy as a Social Good. Social Thought & Research, 28 ,s.186.
[468] Ibid, s.185-186.
[469] MARGULIS, S. T. (2003). Privacy as a social issue and behavioral concept. Journal of Social Issues, 59(2), s.243. https://doi.org/10.1111/1540-4560.00063

lokomotif rolü üstlenen veri koruma otoritelerinin, video gözetime yönelik düzenleme, rehber gibi araçları kullanırken temelde ihlal edilen hal ve menfaatleri bireylere sosyal perspektiften ifade edebilmesi önemlidir.

3.4.2. Video Gözetim Açısından Tek Başına Hukuki Korumanın Yeterliliğinin Sorgulanması

Rona Serozan, "amaca uygunluk yani yerindelik, adalet ve hukuki güvenlik" mefhumlarının bir hukuk devletinin ölçütleri ve temel unsurları olan uygulama şartları olduğunu, bu parametrelerin kuralları yorumlama, boşluk doldurma, kural dışlama faaliyetlerinde de kullanıldığını ifade eder[470]. Hukukun uygulanabilmesi için ise çoğulcu demokrasinin de gereği olarak toplum tarafından özümsenip benimsenmesi gerekir ki bu durum eylemli bir katılım ile kurallara gönüllü olarak uyulmasını sağlar[471].

Bu açıdan tüm dünyada her geçen gün başka bir ülke tarafından üzerine düzenleme yapılan kişisel verilerin korunması hukukunda adilliğin, verilere doğal olarak sahip olan bireyler ile bu verileri sonradan elde edip bir amaç doğrultusunda kullanan gerçek veya tüzel kişiler arasında menfaat dengesinin sağlanması olarak ifade edebiliriz. Öyleyse amaca uygunluk; kişisel verilerin korunması hukukunun var olma amacı olan bireylerin temel hak ve hürriyetlerini koruma işlevini tam olarak yerine getirebilmesi, bireylerin kişisel verilerini veya özel hayat ve mahremiyetlerini korumak olacaktır.

AB'nin özellikle GDPR ile veri koruma yükümlülüğü bakımından oldukça ciddi bir adım atmış olduğu gerçeğine rağmen bu durumun gizliliğin veya ifade özgürlüğünün teminatı olmadığı, üye devletlerin veri gizliliğini korurken GDPR kapsamında ifade özgürlüğünü ve bilgiyi korumaya yönelik yasal yükümlülüklerini yeterince dikkate alıp almadıklarının açık olmadığı belirtilmektedir[472]. Diğer taraftan AB'nin yeni düzenlemeler getirmekle birlikte veri toplama ve işleme ile ilgili ortaya çıkan etik

---

[470] SEROZAN, R. (2017) Hukukta Yöntem-Mantık. İstanbul: Vedat Kitapçılık. 2. Bası. s.73-74.
[471] Ibid, s.73.
[472] REVENTLOW, N. J. (2020). Symposıum On The Gdpr And Internatıonal Law Can The Gdpr And Freedom Of Expressıon Coexıst? 114, s.34. https://doi.org/10.1017/aju.2019.77

kaygıları ele alma yönünde yol kat etmesi gerektiği, yasa koyucuların düzenlemeye çalıştıkları geniş davranışsal veri ekosistemlerini anlamadığı takdirde bu kaygıların da kolay giderilemeyeceği, veri koruma alanındaki düzenlemelerin bu haliyle büyük şirketlerin yasaların kısıtlamalarından kaçabilecekleri bir geçit oluşturacağı da ifade edilmektedir[473].

Spesifik olarak video gözetim alanında ortaya konan genel ve özel kuralların, kamu otoritelerinin faaliyeti ölçüsüz kullanmasının önüne geçebileceğini iddia etmek yerinde olmayacaktır. Zira temel veri koruma ilkeleri, veri işleme şartları idareyi veri sorumlusu (kontrolör) olmak konusunda daha bilinçli hale getirse de uygulamada verilerin kötüye kullanımının önüne geçilmesi daha farklı ve geniş bir perspektif gerektirir. Bu açıdan Fransa'da olduğu gibi kamu gücü kullanan birimlerin hem bağımsız kurullarca hem de caydırıcı bir mekanizma kurularak denetimi, video gözetime ilişkin yetkilendirme gibi önemli koşullar içeren düzenlemelerin ayrı bir komisyon veya yargı tarafından denetimi elzemdir. Bunun dışında teknik tedbirlerin alınması hali hazırda bir ön koşul olarak sağlanmalıdır.

Kişisel verilerin elektronik ortamlarda korunmasında hukuk kuralları ile çözüm üretilebilmesi, dijital ortamdaki risk ve ihlal tespitini yapmak bakımından daha zordur[474]. Kamera kayıtlarının ölçülü, belirli sebeplere dayalı, belirli bir süre ile sınırlı şekilde genel ilkelere riayet edilerek yapılması önem arz etmekle birlikte; bu kayıtlar bir kez elde edildikten sonra dijital ortamda saklama aşamasında veri güvenliğin de ayrıca sağlanması şarttır. Dolayısıyla kişisel verilerin özellikle elektronik ortamlarda hukuk kuralları ile korunması açısından, teknolojik gelişmeler ile uyumlu hareket edilmesi, ikincil düzenlemelerin rehberlik ettiği bir uygulama kanımca faydalı olacaktır.

Bir veri kapitalizmi yaklaşımı olarak, veri piyasasının doğasının, kişisel verilerin ticareti aracılığıyla bireylerin davranışlarını etkilemek için uygulanacak yeni stratejilere

---

[473] ANDREW, J., & BAKER, M. (2021). The General Data Protection Regulation in the Age of Surveillance Capitalism. Journal of Business Ethics, 168, s.576. https://doi.org/10.1007/s10551-019-04239-z

[474] TURAN, M. (2021) Karşılaştırmalı Hukukta Kişisel Verilerin Korunması. Ankara: Seçkin Yayıncılık. 4. Baskı. s. 24.

açık halde olduğu fikri[475] somut koşullarla örtüşmektedir. Zira veri piyasasında tekelleşmenin, büyük veri yönetiminin etkisiyle bu bilgi ticaretinin bireysel menfaatler açısından olası olumsuz sonuçları artık görülmüş ve kabul edilmiştir. Ancak yasal düzenlemeler karşısında kamu otoriteleri de birer veri sorumlusu olduğundan, video gözetime dair gizlilik endişelerinin kamu aktörlerince de özel şirketler ile eşit seviyede uygulanması gerekir.

Topçuoğlu doktora tezinde şöyle belirtir: *"Kanunu koyan ve tatbik eden makamların, bu hususta ki titizlik derecesi ne kadar fazla olursa, ferdin cemiyetten edineceği emniyet hissi de o kadar kuvvetli olur ki, hukuk nizamının da esas itibariyle gayesi budur[476]".* Kişisel verilerin korunmasına ilişkin oluşturulan ve hâlâ inşa edilen hukuk video gözetim açısından da elbette geçerlidir. Ancak kamusal alanların önemine binaen bizatihi kamu otoritelerinin konulan kurallara uygun önlemler alarak işleme faaliyeti yürütmesi gerekecektir.

Solove, özellikle güvenlik-mahremiyet ikileminde hukukun çıkarlar arasında gerekli dengeyi sağlayamadığını, devletlerin mahremiyetin sağlanması ve kişisel verilerin korunmasına yönelik getirilen kuralları kötüye kullanmamalarının hukuk tarafından temin edildiği ancak pek çok kez bunun gerçekleşmediğini belirtir[477]. Bilhassa kamusal alanlardaki video gözetim faaliyetleri açısından hukuki düzenleme ve "bakış açısı" eksikliği söz konusu iken; var olan özel veya somut olaya göre uygulanan genel veri koruma kuralların eksiksiz uygulanması gerekir[478].

Kamusal alanların izlenmesi yönünden, istihbarat bilgisi toplama ve sair güvenlik amaçları gündeme gelmektedir. Bu sebeple de caydırıcı amaçla yapılan süreklilik arz eden video gözetim faaliyetleri dahi "istisnai faaliyet" olarak yorumlanabilmektedir. Bu noktada veri korumaya yönelik hukuk kurallarına uyulmadığı takdirde kamu otoritelerine

---

[475] ANDREW ve BAKER, 2021, s.576.
[476] TOĞÇUOĞLU, H. (1950) Kanuna Karşı Hile (doktora tezi). Ankara Üniversitesi Akademik Arşiv Sistemi. s.4.
[477] SOLOVE, D. J. (2011). Nothing to Hide: the False Tradeoff Between Privacy and Security. Yale University Press.s.13.
[478] SOLOVE, 2011, S. 180-181.

veya yetkili/görevli personele uygulanabilecek yaptırımlar ise ayrı bir tartışma konusudur. Zira bir veri koruma otoritesinin denetleme makamı olarak örneğin İçişleri Bakanlığı'na idari para cezası uygulaması anlamlı olmayacaktır. Personellere uygulanabilecek disiplin cezaları ise uygulanan orantısız video gözetimin önünü kesme noktasında yetersiz kalabilir. Devletlerin özellikle kitlesel izlemeler açısından kendi koydukları kurallara uymalarını sağlamak için de[479], katılımlı ve sosyal yaklaşımı benimseyen bir veri koruma hukuku anlayışı geliştirmek önemlidir.

Kamusal alandaki video gözetimin yüz tanıma gibi akıllı sistemler entegre edilmiş biçimi ile uygulanmasında sosyal kavrayış ve katılım noktasında eksiklikler bulunmaktadır[480]. Bu sistemler hukukun açıkça ve belirli olarak cevaz verdiği durumlar için, güvenlik gerekçeleri ile elbette uygulanabilir. Ancak sistemlerin kurulumunda halkın güvenini etkileyebilecek bu teknolojilerin kullanımı noktasında "akıllı yönetişim, şeffaflık, izleme, denetleme" gibi unsurların ele alınması gerekir[481]. Video gözetim uygulamaları sosyal alana ve hayata da etki ettikleri için bu açıdan aynı zamanda sosyal uygulamalardır. Dolayısıyla halkın bilgisi, desteği ve katılımı olmaksızın salt hukuki düzenlemelere dayanarak kullanımları, veri koruma hukukunun temel maksadının sağlanması bakımından "havada kalan" veya anlaşılamayıp sürekli eleştirilen ve sorgulanan bir zemin yaratacaktır.

Solove'ye göre, kişisel verilerin ve mahremiyetin bir hak olarak korunmasını tesis eden kurallar üç açıdan yeterli değildir. Bu yetersizliklerden birincisi kuralların bireylere çok fazla sorumluluk yüklemesi, ikincisi bireylerin kurallar hakkında karar vermek için yeterli zamanı ve bilgisi olmaması, üçüncüsü ise bu kuralların görünürde tek tek bireylere yönelik olsa da daha bütüncül olarak etki doğurmasıdır[482]. Yani bireylerin kişisel verilerinin korunmasına yönelik verdikleri kararlar diğer bireylerin mahremiyetleri

---

[479] MANANCOURT, V. (06.07.2022) Europe's state of mass surveillance. Politico. (Erişim Tarihi: 02.10.2022) https://www.politico.eu/article/data-retention-europe-mass-surveillance/
[480] GUO, Z. ve KENNEDY, L. (2022). Policing based on automatic facial recognition. Artif Intell Law . s. 42.
[481] Ibid.
[482] SOLOVE, D. J. (February 1, 2022- Forthcoming 2023). The Limitations of Privacy Rights. 98 Notre Dame Law Review. GWU Legal Studies Research Paper No. 2022-30.s.1.

üzerinde de etki doğuracaktır[483]. Ayrıca kurallar verilerin gizliliğini sağlamayı amaçladığı kadar onların doğru aktarımını, güncel şekilde saklanmasını ve edinilmesini, kısacası temel ilkelere uygun şekilde işlenmesini de amaçlar. Ancak kişisel verilerin korunması hukukunun kapsamına bakıldığında esas amaç gizliliğin sağlanması olarak görünmesine rağmen bu sağlanamamakta, diğer amaç olan verilerin kurallara uygun şekilde işlenmesi ise "kuralların dizayn ediliş maksadı" ile örtüşmemektedir[484].

Kişisel verilerin korunması ile işlenmesi arasında bir denge unsuru olarak hukuk kurallarının uygulanmasında, toplumsal faydanın da göze ardı edilmemesi gerekir[485]. Bu ise düzenlemelerin amaçsal yorumlanmasını, birey ve toplum menfaatleri arasında denge kurulmasını, belirsiz durumlarda veri koruma otoritelerinin aydınlatıcı rolünü, hukuk kurallarının açıklığını ve aynı zamanda yenilikçi yaklaşımlara yol açılmasını gerekli kılmaktadır[486]. Video gözetim bakımından toplumsal faydanın gerekli kıldığı hallerde, veri güvenliğine ilişkin teknik kuralları ve hukuk kurallarına riayet edilerek yapılan izlemelerin de bu kapsamda yorumlanması gerekir.

Hukuk kurallarının yapılış amacı ile uygulanma amacının tartışılır bir durumda olması, kişisel verilerin korunması yönünden daha kapsayıcı ve yapısal çözümleri gerekli kılar. Video gözetimin kamusal alanlarda yapılması bakımından meşru bir yetkilendirme, belirliliğin hukuk kuralları ile sağlanması, müstakil bir temel hak veya özel hayatın gizliliği hakkının yansıması olarak kabul edilen kişisel verilerin korunmasını isteme hakkının sınırlanmasının yasalar ile yapılması birinci basamak olarak önemlidir.

Bununla birlikte ikinci basamak ise hukuk kurallarının işlerliğinin sağlanmasına, dönüştürücülüğüne ve uygulanmasına yöneliktir ki kişisel verilerin korunması

---

[483] Ibid.
[484] Ibid. Ayrıca siber alan ve hukuk tartışmaları ile dijital dünyadaki kurallara yönelik tartışmalar için bkz. KAHIN, B. Ve NESSON, C.(ed.) (1999) Borders in Cyberspace: Information Policy and the Global Information Infrastructure. Harvard Information Infrastructure Project-MIT Press: Cambridge, Massachusetts.
[485] KAYA, M.B. (2019) Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge. KESER BERBER, L., BİLGİLİ, A.C.(Ed.) (2019) Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku Marmara Hukuk Bilimsel Toplantılar Serisi-1. İstanbul: onikilevha yayıncılık. s.64.
[486] Ibid.

hukukunun karma yapısından ötürü tek başına hali hazırdaki hukuk kurallarının uygulanması bu amaçlar için yeterli olmayacaktır. Yukarıdaki başlıkta ele alındığı üzere, sosyal yaklaşım ile toplumsal ve bireysel menfaatler de dikkate alınarak veri işlemeye gidilmemesi, var olan kurallara rağmen veri ihlallerinin oluşmasına zemin hazırlayacaktır. Video gözetime hatta genel olarak gözetime yönelik ihdas edilen hukuk kurallarının uygulanmasında, hâkim bakış açısının hukuki merkeziyetçilikten hukuki çoğulculuğa kayması kişisel verilerin korunmasının idrakinde faydalı olacaktır. Kanımca uygulanagelen devlet-hukukunun, pozitivist anlayış veya pozitivist muhafazakarlık aşılarak sosyal yaklaşım ile zenginleştirilmesi, bütüncül bir hukuki koruma tesis edilmesi için gereklidir[487].

[487] Hukuki çoğulluk tartışmaları, devlet hukuku/devlet dışı hukuk, hukuki merkeziyetçilik hakkında bkz. HATİPOĞLU AYDIN, D. (2014). HUKUKİ ÇOĞULLUKTA İKTİDAR PROBLEMİ. Journal of Istanbul University Law Faculty , 72 (1) , 487-505 .

SONUÇ

Devletlerin gözetimi, tarihsel açıdan teknolojik ve teknik gelişmeler ile birlikte farklı şekillerde ve farklı araçlar ile boyut değiştirmiştir. Mahremiyet de gözetim ile beraber dönüşmüş, önceleri oldukça sınırlı olan gizlilik beklentisi daha sonra yavaş yavaş bireyselleşmenin ve liberal değerlerin yükselmesiyle artmıştır. Öyle ki mahremiyet algılamaları evlerin koridorlarından dini alanlara sirayet etmiş, şehir yaşamında bir "merkezden çekilme" doğurmuştur. Diğer taraftan; artan nüfus, savaşlar, devletlerin iç politikalarında oluşturdukları sosyal kontrol stratejileri, şehirlerin büyüdükçe daha zor denetlenebilir ve gözlenebilir hale gelmesi ve nihayetinde dijitalleşme gibi sebepler ile gözetim sistemli şekilde başvurulan bir faaliyet haline gelmiştir.

Teknolojik imkanların da artmasıyla birlikte bir gözetim aracı olarak kameralar kullanılmaya başlanmış, bu şekilde şehirlerdeki kamusal alanların denetimi sağlanmaya çalışılmıştır. Nitekim kameralar kamusal alanlarda olan olayların anlık şekilde izlenebilmesine, bu görüntülerin arşivlenmesine, arşiv kayıtlarının uzun süreler saklanabilmesine imkân tanımaktadır. Böylece kameralar bir güvenlik ve kontrol sağlama aracı haline gelmiş, olaylara daha hızlı şekilde müdahale edilmesi, suçlu takibi, bazı suçlar açısından caydırıcılık avantajları elde edilmiştir. Artık günümüzde video gözetimin ve video gözetimde kullanılacak cihazların kamusal alanlarda özellikle güvenliği sağlama noktasındaki kolaylaştırıcı ve destekleyici rolü sebebiyle kamu otoritelerince artan şekilde kullanıldığı açıktır. Bu kullanımın orantılı olup olmadığı, devletlerin güvenlik sağlama rolünü kameralara yüklediği, her yerde gözetim yapan kameraların bulunmasının bireysel özgürlüklere yönelik tehdit olduğu gibi eleştiriler de kullanımın artmasıyla yükselmeye başlamıştır.

Güvenliğin sağlanması amacıyla gözetimin artırılması bizi özgürlük-güvenlik ikilemine götürür. Bir taraftan modern devletler, diğer hak ve hürriyetlerin karşısında güvenlik sağlamayı önceleme politikası güderken; diğer taraftan özgürlüklerin de sağlanmasını amaçlamak durumundadır. Bu şekilde kameralarla dolu meydanlar ve şehirlerde, güvenliğin bekçisi olma görevinin yerine getirildiği vatandaşlarca da

görülecek, her ne kadar sürekli bir izleme olsa da güvende hissetmenin konforu yaşanılacaktır. Ancak eğer kişisel veriler, özel hayat gibi kavramlar da hukuki koruma altına alındıysa -ki kişisel verilerin korunması hukukunun var oluş amacının budur- bunun gereği salt şirketlere değil her aktöre karşı yerine getirilmelidir. Aksi halde bu kuralların meydana getirilme amacı konusunda pek çok sorgulamaya kapı açılmış olacaktır.

Kamusal alanlar, bireylerin demokratik hayata katılımı, sosyalleşmesi ve şehir hayatına entegre olabilmesi gibi yönlerden önemlidir. Devletlerin gözetimi gerçekleştirme boyutu değiştikçe, kamusal alanlar da başkalaşmış, şehir yaşamı meydan ve bulvarlardan çevrelere doğru genişlemiş, merkezler bir ticaret ve alışveriş alanı haline gelmiş; bireyler ise bir parça mahremiyet ve özellikle güvenlik beklentisi ile kenarı çekilmiştir. Burada video gözetimin hem büyüyen şehirlerdeki güvenliği sağlama anlamında bir "çare" olarak görülmesi hem de bireylerde her an "gözetlenen" olmaktan kaynaklı bir güvende olma hissi ve aynı zamanda mahrem alanı yitirme durumu yaşanmaktadır.

Tam da mahremiyetin dönüşümü ve dijitalizasyon adı verilen bilgi toplumunun yükselişi ile birlikte, geçmişten farklı olarak bilginin gücü dijital dünya ile birleşmiş, veriler artık ekonomik bir değer haline gelmiş, kişisel veriler kullanılarak yeni bir piyasa yaratılmıştır. Bu şekilde oldukça yoğun etki altında kalan insan davranışı ve tercihleri, sürekli olarak gözetim altındaki yaşamlar artık temel hakları sorgulanır hale getirmiş, devletler ise gerek bilgiye tahakkümü büyük şirketlere bırakmamak, gerek kendi yapılarını ve egemenliklerini korumak, gerekse ciddi düzeyde bozulan menfaat dengesini daha makul hale getirmek için kişisel verilerin kullanılmasına yönelik düzenlemeler getirmiştir. Bu düzenlemeler ile hem bizatihi kamu organları hem de özellikle büyük şirketler sınırlanmaktadır.

Bugün en kapsamlı uygulamanın AB'de uygulanageldiği kişisel verilerin korunması hukukunun temel aldığı "orantılılık, ölçülülük, meşruluk, verilerin doğruluğu, güncelliği ve güvenliği, veri minimizasyonu" gibi ilkelerin video gözetim açısından da uygulanması beklenir. Ayrıca video gözetimin sistemli ve sürekli şekilde kamusal alanda

yapılmasının etkileri ile potansiyel riskleri sebebiyle bu konuya ilişkin özel düzenlemeler yapılmaya başlanmış, bireyleri devletlerin ölçüsüz kameralı gözetiminden korumak için kamusal alandaki gözetimin gerekliliğine vurgu yapılmıştır.

Burada özellikle belirli bir suç soruşturması kapsamının, suçlu takibinin veya belli bir amaç için yapılan ve sürekli olmayan gözetim faaliyetleri aracılığı ile kişisel verilerin işlenmesinin ayrıksı tutulduğunu belirtmek gerekir. Zira bu tür işlemeler istisna veya kısıtlama sebebi sayılmakta, bir kısım veri işleme kurallarından ari tutulmaktadır. Ancak bu faaliyetlerde dahi olay ile uygun düştüğü ölçüde bazı temel kurallar yerine getirilmeli, kişilere başvuru haklarını kullanma hakkı tanınmalıdır.

Öte yandan bahis konusu edilen belirli maksatla yapılan gözetim faaliyetleri dışındaki izlemelerin muhakkak kanun ile yapılması, temel hal ve hürriyetlerin sınırlanmasının hukuka uygun yapılması zorunluluğunun tezahürüdür. Kanun ile sınırlama durumu elbette mahremiyetin veya özel hayatın sınırlanmadığı anlamına gelmeyecek yalnızca bu sınırlamanın meşru bir şekilde yapılması sağlanacaktır. Bu meşruiyetin sağlanması asgari düzeydeki temel koşuldur.

Belirtildiği üzere; video gözetimin salt hukuka uygun şekilde yapılmış olması, onun orantılı ve ölçülü olduğu anlamına gelmeyecek, kişisel verilerin güvenliği sağlanmış olmayacaktır. Nitekim veri güvenliği tıpkı mahremiyet gibi çok yönlü bir düzenek ile sağlanmalıdır. Teknik, hukuki, sosyal ve ilgili sair bakış açıları bir arada değerlendirilerek sistemli yapılacak izlemelerde cihaz kurulumlarına ancak belirli güvenlik aşamaları geçildikten sonra karar verilmelidir. Bunun yanında özellikle sosyal yaklaşım, verilerinin korunması amaçlanan bireylerin, mahremiyeti, özel hayatı veya kişisel verilerin önemini anlaması bakımından önemlidir. Veri koruma yasalarının uygulanışı noktasında, aynı amaçla kurulan bağımsız otoritelerin hak ihlalleri durumundaki olumsuz sosyal kayıpların da altını çizmesi gerekir. Böyle bir yaklaşım benimsenmediği takdirde salt kişisel verilerin korunması hukuku, video gözetim karşısındaki özel hayat ve mahremiyetin korunması savunularını etkin kılmak açısından yeterli olmayacaktır.

KAYNAKLAR

BASILI KAYNAKLAR

ABANOZ, B. (2015). Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi eve Elde Edilen Delillerin Hukuka Uygunluğu Sorunu İlişkisi (yüksek lisans tezi).

AKGÜL, M.ve HEKİMOĞLU TOPRAK, H. Sosyal Ağlarda Mahremiyetin Dönüşümü: Instagram Örneği. Online Academic Journal of Information Technology 2019 Yaz/Summer– Cilt/Vol: 10 - Sayı/Num: 38. s.75-114.

AKINLAR, C. (2012). *Kapalı Devre Görüntü ve Kayıt Sistemleri*. Güvenlik Sistemleri. (Yusuf OYSAL, Ed.; 1). Anadolu Üniversitesi Yayınları. 82-109.

ALKAN, M., MENTEŞ, T., İNCEEFE, M.A. (2020). Kişisel Verileri Koruma El Kitabı Teknik Uygulama ve Uyumluluk. Ankara: Nobel Yayıncılık.

ANDREW, J., & BAKER, M. (2021). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*, *168*, 565–578. https://doi.org/10.1007/s10551-019-04239-z

ARENDT, H. (1979) The Origins of Totalitarianism. Harvest Book: New York.

ARIEL, B., FARRAR, W. A., & SUTHERLAND, A. (2015). The effect of police body-worn cameras on use of force and citizens' complaints against the police: A randomized controlled trial. *Journal of Quantitative Criminology*, 31(3), 509–535.

ARIK, E. (2018) Dijital Mahremiyet Yeni Medya ve Gözetim Toplumu. Konya: Literatürk Akademia.

ARSLAN B. & SAĞIROĞLU Ş. (2016). Mobil Cihazlarda Biyometrik Sistemler Üzerine

Bir İnceleme, Politeknik Dergisi, 2016; 19 (2).

ARSLANTAŞ TOKTAŞ, S., MUTLU, B., DİKMEN, E.Ş., FİDANER, I.B., KÜZECİ, E. ve ÖZAYGEN, A. (2012) Türkiye'de Dijital Gözetim: T.C. Kimlik Numarasından E-Kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi. İstanbul: Alternatif Bilişim Derneği.

ARTUÇ, M. (2015) Mahremiyet Açısından Birey ve Devlet İlişkisi (yüksek lisans tezi). Adnan Menderes Üniversitesi, Aydın.

ASSANGE, J. (2012) Cypherpunks New York and London: OR Books.

AŞIKOĞLU, Ş.İ. (2018) Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri. Onikilevha: İstanbul.

AYÖZGER ÖNGÜN, Ç. (2019) Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil. İstanbul: Beta Basım Yayın. Genişletilmiş 2. Baskı.

BALL, K., GRAHAM, S., GREEN, N., & LYON, D. (2006). A Report on the Surveillance Society. In *Polity* (Vol. 70, Issue September). http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

BALL, K., HAGGERTY, K., LYON, D. (Ed.) (2012) Routledge Handbook of Surveillance Studies. Routledge: London and New York.

BALL, J. (2021) Sistem. (Yasin Konyalı çev.) İstanbul: Timaş Yayınları. (Orijinal eserin yayın tarihi 2020).

BASKIN, O. (2021) Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması. Ankara: Seçkin Yayıncılık.

BAŞAR, C. (2017). Devletin Kitlesel Gözetleme Araçlarının Özgürlükler ve Hukuk Güvenliği Üzerindeki Etkileri ile Bunların Yasal Dayanakları Üzerine Bir İnceleme. *Türkiye Barolar Birliği Dergisi*, *133*, 97–131.

BAŞTÜRK, E. (2018). Post Yapısalcı Teori Bağlamında Post-Panoptik Gözetimin Küresel Politikası. *SİYASAL: Journal Political Sciences*, *27*(1), 47–68. https://doi.org/10.26650/siyasal.2018.27.1.0001

BAUMAN, Z., & LYON, D.(ed.) (2016). *Akışkan Gözetim* (Elçin Yılmaz Çev. 2nd ed.). Ayrıntı Yayınları.

BAYRA, E. (2019). "Güvenlik Devleti: Leviathan'dan Hukuk Devletine, Hukuk Devletinden Leviathan'a. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 6(1), 93-129.

BENTHAM, J., Pease-Watkin,C., Werret,S., Çoban,B. ve Özarslan,Z. (2019)Panoptikon: Gözün İktidarı(3. Baskı). (Barış Çoban, Zeynep Özarslan Çev.). İstanbul: Su Yayınları.

BERK, M. E. (2020). Dijital Çağın Yeni Tehlikesi "Deepfake". OPUS International Journal of Society Researches , 16 (28) , 1508-1523 . DOI: 10.26466/opus.683819

BÉTİN, C., MARTİNAİS, E., & RENARD, M.-C. (2003). Sécurité, vidéosurveillance et construction de la déviance : l'exemple du centre-ville de Lyon. *Déviance et Société*, *27*(1), 3. https://doi.org/10.3917/ds.271.0003

BİTİRİM OKMEYDAN, S. (2017) 'Postmodern Kültürde Gözetim Toplumunun Dönüşümü: "Panoptikon" Dan "Sinoptikon" ve "Omniptikon" A', AJIT-e: Online Academic Journal of Information Technology, 45–69.https://doi.org/10.5824/1309

BOSTANCI BOZBAYINDIR, G. (2018) Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet

Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler. Galatasaray Üniversitesi Hukuk Fakültesi Dergisi- 2018/2.s.51-103.

BOZBEYOĞLU, A.Ç. (2012) The Electronic Eye Of The Police:The provincial information and security system in Istanbul. Doyle, A. Lippert, R. Lyon, D. (ed.) Eyes Everywhere:The global growth of camera surveillance. (s.139-156) Routledge:London and New York.

BOZOVIC, M. (1995). *Jeremy Bentham the panopticon writings*. Verso: London and New York.

BULUT, M. (2020). Özel Bir Hukuki Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler. Ankara Barosu Dergisi, 2020(3), 100-150.

BÜK, A. (2018) Bilişim Alanında Kişisel Verilerin Korunması. Ankara: Seçkin Yayıncılık.

BRENTON, M. (1964) The Privacy Invaders, New York: Coward-McCann.

BROWN, B. (1995). CCTV in Town Centres: Three Case Studies. In *Crime Detection and Prevention Series*. London: Police Research Group Crime Detection And Prevention Series: Paper No 68.

CAN, N. (2020). Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması (yüksek lisans tezi). Yök Tez Merkezi. (653565)

CECCATO, V., & NALLA, M. K. (Eds.). (2020). *Crime and fear in public places : towards safe, inclusive and sustainable cities*. London and New York:Routledge.

COLEMAN, R. (2004). *Reclaiming the Streets surveillance, social control and the city*. Oregon: Willan Publishing.

CROLL, A. (1999). Street Disorder, Surveillance and Shame: Regulating Behaviour in the Public Spaces of the Late Victorian British Town. In *Social History* (Vol. 24, Issue 3). https://www.jstor.org/stable/4286578

CUSTERS, B., DECHESNE, F., SEARS, A. M., TANI, T., & VAN DER HOF, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law and Security Review*, *34*(2), 234–243. https://doi.org/10.1016/j.clsr.2017.09.001

ÇAPAR, S. (2011) Birleşik Krallıkta CCTV, Türkiye'de Mobese Caddelerde Güvenlik Nöbetindeki Kameralar. Ankara:Turhan Kitabevi Yayınları.

ÇEKİN, M. S. (2020) Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu. İstanbul: On İki Levha Yayıncılık. 3. Baskı.

ÇETİN, M., & ASIL, S. (2017). GÜNÜMÜZ TOPLUMUNDA GÖZETİM OLGUSU. *Third Sector Social Economic Review*, *52*(1), 180–205.

DAMJANOVSKI, V. (2014). *CCTV From Light to Pixels* (3rd ed.). Elsevier.

DANDEKER, C. (1990) Surveillance, Power and Modernity: Bureaucracy and Discipline From 1700 to the Present Day. Polity Press: Cambridge.

DE CEW, J. (Spring 2018 Edition) "Privacy" The Stanford Encyclopedia of Philosophy Edward N. Zalta (ed.).

DEVELİOĞLU, H.M. (2017) 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku. İstanbul: Onikilevha.

DIAMOND, B. (2010). Safe Speech: Public Space as a Medium of Democracy. *Journal of Architectural Education*, *64*(1). https://about.jstor.org/terms

DOLGUN, U. (2004), ‘Gözetim Toplumunun Yükselişi: Enformasyon Toplumundan Gözetim Toplumuna’, Yönetim Bilimleri Dergisi, 1(3), 55–74.

DOLGUN, U. (2015). Şeffaf Hapishane yahut Gözetim Toplumu: Küreselleşen Dünyada Gözetim, Toplumsal Denetim ve İktidar İlişkileri (3. Baskı). İstanbul: Ötüken Neşriyat.

DOYLE, A., LIPPERT, R., & LYON, D. (Eds.). (2012). Eyes Everywhere The global growth of camera surveillance Edited. Routledge.

DURKHEİM, É., SPAULDING, J. and SIMPSON, G. (2005). *Suicide: A Study in Sociology*. Routledge. https://doi.org/10.1097/00001504-200003000-00002

DÜLGER, M. V. (2020) Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi, 3. Baskı.

DWORKIN, G. (1973). The Younger Committee Report on Privacy. *The Modern Law Review*, *36*(4), 399–406. http://www.jstor.org/stable/1093890

EMEKLİER, B. (2011). Thomas Hobbes ve John Locke’un Güvenlik Anlayışının Karşılaştırmalı Bir Analizi. *Güvenlik Stratejileri Dergisi*, *7*(13), 99–123. https://dergipark.org.tr/en/pub/guvenlikstrtj/issue/7530/99185

FOUCAULT, M. (2015) Hapishanenin Doğuşu. (Mehmet Ali Kılıçbay çev.) Ankara: İmge Kitabevi, 6. Baskı. (Orijinal eserin yayın tarihi: 1992)

FUSTER, G.G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. Brussel: Springer.

FYFE N.R. and FYFE J. B. (1998) ‘the eyes upon the street’ closed-cırcuit televısıon surveillance and the city.N. Fyfe (edited) (1998) Images of the Street: Planning, Indentity and Control in the Public Space. Routledge: London and New York.

FYFE, N.R.(Ed.) (2006) Images of the street: Planning, identity and control in public space. London and New York: Routledge. https://doi.org/10.4324/9780203026496

GELLMAN, B. (2020) Dark Mirror: Edward Snowden and the American Survaillance State. Penguin Press: New York.

GOOLD, B., LOADER, I., & THUMALA, A. (2013). The banality of security: The curious case of surveillance cameras. *British Journal of Criminology, 53*(6), 977–996. https://doi.org/10.1093/bjc/azt044

GUMPERT, G., & DRUCKER, S. J. (2001). Public boundaries: Privacy and surveillance in a technological world. *Communication Quarterly*, *49*(2), 115–129. https://doi.org/10.1080/01463370109385620

GUO, Z., KENNEDY, L. (2022). Policing based on automatic facial recognition. *Artif Intell Law* . s. 1-47. https://doi.org/10.1007/s10506-022-09330-x

GÖZLER, K. (2020) İnsan Hakları Hukuku. Bursa: Ekin Basım Yayın Dağıtım. 3. Baskı.

GURİNSKAYA, A. (2020). Young Citizens Attitudes Towards CCTV and Online Surveillance in Russia. In book: Digital Transformation and Global Society (pp.61-74) 10.1007/978-3-030-65218-0_5.

GÜVEN, O. Ö. (2014) 'Gözetim Tekniklerinin Güç İlişkileri Bağlamında Dönüşümü ve Toplumsal Denetim', Atatürk İletişim Dergisi, 7, s. 79-112.

HALL, E. T. et.al. (1968) Proxemics (and Comments and Replies) Current Anthropology . 9:2/3, s. 83-108.

HAN, B.C. (2020) Şeffaflık Toplumu. (Haluk Barışcan çev.) İstanbul: Metis Yayınları. 6. Baskı.

HAN F. & HU J. & KOTAGİRİ R. (2011) Advanced Topics In Biometrics, Chapter 19 Biometric Authentication For Mobile Computing Applications, www.worldscientific.com .

HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2018) Poland: Drukarnia Interak Printing House.

HATİPOĞLU AYDIN, D. (2014). HUKUKİ ÇOĞULLUKTA İKTİDAR PROBLEMİ. Journal of Istanbul University Law Faculty , 72 (1) , 487-505 .

HATİPOĞLU AYDIN, D. (2022) Siber Alan ve Hukuk. İstanbul: Onikilevha yayınları.

HAZAR, E. (2012) Gözetleme Toplumu Bağlamında Çağdaş Sosyal Kontrol Araçları: Kapalı Devre Kamera Sistemleri ve Toplumsal Fayda ve Maliyetleri: Ankara İli Örneği (yüksek lisans tezi). Yök Tez Merkezi. (347549)

HEILMANN, E. (2011). Video surveillance and security policy in France: From regulation to widespread acceptance. (Galley Proof çev.) Information Polity 16. s.1-9.

HENKOĞLU, T. (2015) Bilgi Güvenliği ve Kişisel Verilerin Korunması. Ankara: Yetkin Yayınları.

HOBBES, T. (1651). *Leviathan Or The Matter, Forme, & Power Of A Common-Wealth Leviathan Or The Matter, Ecclesiastical And Civill: Vol. 2009.* The Project Gutenberg E-Book of Leviathan.

İÇER, Z., & DÖNMEZ, E. (n.d.). Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları. *CHD*, *15*(43), 421–461.

INNES, M. (2003). *Understanding Social Control: Deviance, Crime and Social Order*. Open University Press. https://doi.org/10.1177/026455050505200216

JASANOFF, S. (2021) Teknoloji ve İnsanın Geleceği. İstanbul: Bgst Yayınları, 1.Baskı.

KAHIN, B. ve NESSON, C.(ed.) (1999) Borders in Cyberspace: Information Policy and the Global Information Infrastructure. Harvard Information Infrastructure Project-MIT Press: Cambridge, Massachusetts.

KARADAĞ, U. Süreklilik mi Kopuş mu? Thomas Hobbes ve John Locke'un Toplum Sözleşmesi Teorilerinin Sınırlı Bir Mukayeses, *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi*, 15(185), s. 107-136.

KARADAĞ, U. "Kamu Hukuku Açısından Otokratik Yönetim-Gayrişahsi Devlet İktidarı İlişkisi ve 'Staatsgewalt' Kavramı, *SÜHFD.*, C. 28, S. 3, 2020, s. 1429-1464.

KARAGÜLLE, A. E. (2015) Günümüzde Değişen Mahremiyet Algısının Sosyal Ağlar Bağlamında İncelenmesi İlişkisi (yüksek lisans tezi). İstanbul Ticaret Üniversitesi, İstanbul.

KASPER DEBBIE V.S. (2007). Privacy as a Social Good. *Social Thought & Research, 28*, 165–189.

KESER BERBER L., LOSTAR, M. (2006) Bilişimde Biyometrik Yöntemler. Ankara: Yetkin Yayınları.

KESER BERBER, L., BİLGİLİ, A.C.(Ed.) (2019) Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku Marmara Hukuk Bilimsel Toplantılar Serisi-1. İstanbul:onikilevha yayıncılık.

KETİZMEN, M. (2006). Türk Ceza Hukukunda Bilişim Suçları (doktora tezi). Yök Tez Merkezi. (191474)

KETİZMEN, M., KART, A. (2019). Kişisel Veri ve Rekabet Hukuku Kapsamında "Big

Data", Kişisel Verileri Koruma Dergisi. 1(1), 64-76.

KLAUSER, F.R. (2009). Lost surveillance studies: a critical review of French work on CCTV. *Surveillance & Society* 6(1). s.23-31.

KLING, R., & LYON, D. (1994). The Electronic Eye: The Rise of the Surveillance Society. In *Contemporary Sociology* (Issue 4). University of Minnesota Press. https://doi.org/10.2307/2077688

KILINÇ ÖZÜÖLMEZ, P. (2019) 'Michel Foucault'nun İktidar ve Özne Kavramsallaştırmasına Gözetim Sorunu Üzerinden Bakmak: Black Mirror – Arkangel', Selçuk Üniversitesi İletişim Fakültesi Akademi Dergisi, 12(2), 630–655.

KÖSEOĞLU, Özgür (2012). Sosyal Ağ Sitesi Kullanıcılarının Motivasyonları: Facebook Üzerine Bir Araştırma, Selçuk İletişim Dergisi.

KÜÇÜK, T. S. (2018). Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı ile Önleyici Amaçla İzlenmesi. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi Cilt:Xv Sayı 1*, 49–89. www.armoninuans.com

KÜZECİ, E. (2021) Kişisel Verilerin Korunması. İstanbul: On İki Levha Yayıncılık, 4. Baskı.

LACOMBE, D. (1996). Reforming Foucault: A Critique of the Social Control Thesis. *The British Journal of Sociology, 47*(2), 332–352.

LAYBATS, C., & DAVIES, J. (2018). GDPR: Implementing the regulations. *Business Information Review*, *35*(2), 81–83. https://doi.org/10.1177/0266382118777808

LEITH, P. (2006). The socio-legal context of privacy. *International Journal of Law*, *2*(2),

105–136.

LOCKE, J. (1680). *Second Treatise Of Government*. The Project Gutenberg E-Book of Second Treatise of Government.

LOKKE, E. (2020) Mahremiyet: Dijital Toplumda Özel Hayat (Dilek Başak çev.) İstanbul: Koç Üniversitesi Yayınları. (Orijinal eserin yayın tarihi:2017)

LUM C, KOPER CS, WILSON DB vd. (2020). Body-worn cameras' effects on police officers and citizen behavior: A systematic review. Campbell Systematic Reviews. Volume 16. Issue 3. S.1-40.

LYON, D. (1997). Elektronik Göz- Gözetim Toplumunun Yükselişi (Dilek Hattatoğlu Çev.) Sarmal Yayınevi.

MONAHAN, T. (Ed.). (2006). *Surveillance and Security Technological Politics and Power in Everyday Life*. Routledge.

MARGULIS, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243–261. https://doi.org/10.1111/1540-4560.00063

MARX, G. T. (2015). International Encyclopedia of the Social & Behavioral Sciences. *International Encyclopedia of the Social & Behavioral Sciences*, *23*, 733–741. http://www.sciencedirect.com/science/article/pii/B9780080970868640254

MATCZAK, P., WÓJTOWİCZ, A. vd. (2021): Effectiveness of CCTV systems as a crime preventive tool: evidence from eight Polish cities. International Journal of Comparative and Applied Criminal Justice.

MATTELART, A. (2012) (Onur Gayretli ve Su Elif Karacan Çev.) Gözetimin Küreselleşmesi: Güvenlikeştirme Düzeninin Kökeni. İstanbul: Kalkedon Yayınları.

(Orijinal eserin yayın tarihi:2007)

MC GRAVEN, W. (2016) Privacy and Data Protection Law. USA: Foundation Press.

MONAHAN, T. (2010). Surveillance as governance. Social inequalities and the pursuit of democratic surveillance. In Kevin D. Haggerty and M. Samatas (eds) Surveillance and Democracy. New York: Routledge- Cavendish, pp. 91–110.

MOORE, A.D. (2016) Privacy, Security and Accountability: Ethics, Law and Policy. Rowman & Littlefield International: London&New York.

MOROZOV, E. (2011). The Net Delusion: The Dark Side of Internet Freedom. In *New York* (Vol. 9, Issue 04). Public Affairs. http://www.amazon.com/Net-Delusion-Morozov/dp/1846143535

MUCCHIELLİ, L. (2016). À Quoı Sert La Vidéosurveillance De L'espace Public ? Le cas français d'une petite ville « exemplaire ». *Deviance et Societe*, *40*(1), 25–50. https://doi.org/10.3917/ds.401.0025

NORRIS, O. ve ARMSTRONG, G. (1999) The Maximum Survaillance Society. Oxford-New York:Berg.

NORRIS, C. (2012) The success of failure: Accounting for the global growth of CCTV. Routledge Handbook of Surveillance Studies. (K. Ball,K. Haggerty, D. Lyon ed.) Routledge: London and New York.

OVALIOĞLU, S. (2021) Avrupa Birliği Hukukunda Kişisel Verilerin Korunması (Yüksek Lisans Tezi) Yök Ulusal Tez Merkezi. Dokuz Eylül Üniversitesi, İzmir.

ÖNAL M**.** (2013). RFID Mimarisi ve Programlama, (1. Baskı, s. 241- 253), İstanbul: Kodlab, (Erişim Tarihi: 29.04.2021), https:// books. google. com.tr/

books?id=DT6nBAAAQBAJ&pg=PA246&dq=biyometrik+veri&hl=tr&sa=X&ved=0ahUKEwjBm6qLyKfXAhUKKcAKHRG1A7gQ6AEIOzAE#v=onepage&q=biyometrik%20veri&f=false

ÖZKAN, H., (2016) Mobese İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi, *Ceza Hukuku Dergisi*, 11(30), 63-103.

ÖZER, H. D. (2022). Mobese İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *24*(1), 459–500.

PACKARD, V. (1964). The Naked Society. New York: Ig Publishing.

PARLAK BÖRÜ, Ş. (2013) Fotoğraf Üzerindeki Haklar (doktora tezi). Yök Tez Merkezi. (330323)

PAŞAOĞLU, C. & ADJE, K H. & DEMİRTAŞ, O. (2019). A Review On Privacy Preserving Biometric Authentication Methods. Kişisel Verileri Koruma Dergisi, 1(1).

PATTON, J. W. (2000). Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology*, *2*, 181–187.

PIZA, E. L., WELSH, B. C., FARRINGTON, D. P., & THOMAS, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology and Public Policy*, *18*(1), 135–159. https://doi.org/10.1111/1745-9133.12419

REVENTLOW, N. J. (2020). *Symposıum On The Gdpr And Internatıonal Law Can The Gdpr And Freedom Of Expressıon Coexıst? 114*, 31–34. https://doi.org/10.1017/aju.2019.77

RULE, J. B. (2012). Privacy in Peril: How We Are Sacrificing a Fundamental Right in

Exchange for Security and Convenience. *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, 1–256. https://doi.org/10.1093/acprof:oso/9780195307832.001.0001

RULE, J. B., & GREENLEAF, G. (2008). Global privacy protection: The first generation. In J. B. Rule & G. Greenleaf (Eds.), *Global Privacy Protection: The First Generation*. Edward Elgar Publishing. https://doi.org/10.4337/9781848445123

ROSENBERG, J. (1969) The Death of Privacy. New York: Random House.

RYAN, J. (2010) A History of the Internet and the Digital Future. London: Reaktion Books.

SATAPATHY S. C. & JOSHI A. (2017). Information and Communication Technology for Intelligent Systems (ICTIS 2017). Bhatnagar S. Cooperative Multimodal Approach for Identification , Volume 1.

SCHUİLENBURG, M., PEETERS, R. (2018) Smart cities and the architecture of security: pastoral power and the scripted design of public space. *City Territ Archit* 5**,** 13.s.1-9. https://doi.org/10.1186/s40410-018-0090-8.

SCHÜNEMANN, W. J.; BAUMAN, M. O. (2017) Privacy, Data Protection and Cybersecurity in Europe. Switzerland:Springer İnternational Publishing.

SCHOEMAN, F. D. (1992). Privacy and Social Freedom. Cambridge University Press.

SEROZAN, R. (2017) Hukukta Yöntem-Mantık. İstanbul: Vedat Kitapçılık. 2. Bası.

SEVİNÇER, S. (2015). Biyometrik Yöntemlerle Elde Edilen Kişisel Verilerin Site Konutların Güvenlik Sistemlerinde Kullanımı. İstanbul Barosu Dergisi, 92(2), 233-245.

ŠIDLAUSKAS, A. (2019). Video Surveillance and the Gdpr. *Social Transformations in Contemporary Society*, *7*, 55–65.

SIMON, J., & FEELEY, M. M. (1992). The new penology: Notes of the emerging strategy of corrections and its implications. *Criminology*, *30*(4), 449-474. https://doi.org/10.4324/9781315095288

SKOGAN, W. G. (2019). The future of CCTV. *Criminology and Public Policy*, *18*(1), 161–166. https://doi.org/10.1111/1745-9133.12422

SMITH, M., & MILLER, S. (2022). The ethical application of biometric facial recognition technology. *AI and Society*, *37*(1), 167–175. https://doi.org/10.1007/s00146-021-01199-9.

SNOWDEN, E. (2019) Permanent Record. London: Metropolitan Books.

SOLOVE, D. J. (2002) Conceptualizing Privacy.California Law Review, 90(4), 1087-1155.

SOLOVE, D. J. (2011). *Nothing to Hide : the False Tradeoff Between Privacy and Security*. Yale University Press.

SOLOVE, D. J. (February 1, 2022- Forthcoming 2023). The Limitations of Privacy Rights. 98 Notre Dame Law Review. GWU Legal Studies Research Paper No. 2022-30.s.1-50.
SSRN: https://ssrn.com/abstract=4024790 or http://dx.doi.org/10.2139/ssrn.4024790

SPRIGGS, A., & GILL, M. (2006). CCTV and Fight Against Retail Crime: Lessons from a National Evaluation in the U.K. *Security Journal*, *19*(4), 241–251. https://doi.org/10.1057/palgrave.sj.8350023

STRECKFUS, C.H. & GUAJARDO EDWARDS, C. (2011). The Use of Salivary as a Biometric Tool to Determine the Presence of Carcinoma of the Breast Among Women (Biometrics- In Tech).

TAŞCI, U. (2016). Güvenlik Amaçlı Gözetim Aracı Olarak Türkiye'de Mobese ve Eleştiriler. *Cbü Sosyal Bilimler Dergisi*, *14*(2), 159–190. https://doi.org/10.18026/cbusos.18498

TAŞTAN, F. G. (2017) Türk Sözleşme Hukukunda Kişisel Verilerin Korunması. İstanbul: On İki Levha Yayıncılık, 1. Baskı.

URQUHART, L., & MIRANDA, D. (2021). Policing faces: the present and future of intelligent facial surveillance. *Information and Communications Technology Law*, 1–26. https://doi.org/10.1080/13600834.2021.1994220

THOMAS, A. L., PIZA, E. L., WELSH, B. C., & FARRINGTON, D. P. (n.d.). The internationalisation of cctv surveillance: Effects on crime and implications for emerging technologies. *International Journal of Comparative and Applied Criminal Justice*, *46*(1), 1–22. https://doi.org/10.1080/01924036.2021.1879885

TOĞÇUOĞLU, H. (1950) Kanuna Karşı Hile (doktora tezi). Ankara Üniversitesi Akademik Arşiv Sistemi.

TOPÇUOĞLU, H. (1969) Hukuk Sosyolojisi (Sosyoloji Açısından Hukuk). İstanbul: Cezaevi Matbaası. 3. Baskı.

TURAN, M. (2021) Karşılaştırmalı Hukukta Kişisel Verilerin Korunması. Ankara: Seçkin Yayıncılık. 4. Baskı.

TURTIAINEN, H.T. (2020). State-of-the-art object detection model for detecting CCTV and video surveillance cameras from images and videos.(Master's Thesis in Information

Technology). University of Jyväskylä. http://urn.fi/URN:NBN:fi:jyu-202005253430 (Erişim Tarihi 04.12.2021)

VAN DER SLOOT, B.; GROOT, A. D. (2018) The Handbook of Privacy Studies. Amsterdam: Amsterdam University Press.

VINCENT, D. (2017) Mahremiyet Kısa Bir Tarih. (Deniz Cumhur Başaraner çev.) Ankara: Epos Yayınları.

WARREN, S. D., BRANDEIS L.D. (15.12.1890) 'The Right to Privacy', Harvard Law Review, Vol.4.No.5, 193–220.

WELSH, B. C., & FARRINGTON, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, *26*(4), 716–745. https://doi.org/10.1080/07418820802506206

WESTIN, A. (1967). Privacy and Freedom. New York: Ig Publishing.

WILLIAMS, C. A. (2003). Police surveillance and the emergence of CCTV in the 1960s. *Crime Prevention and Community Safety*, *5*(3), 27–37. https://doi.org/10.1057/palgrave.cpcs.8140153

YAVUZ, C. (2018). İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması: Unutulma Hakkı. Ankara:Seçkin Yayıncılık.2. Baskı.

YEŞİL, B. (2006). Watching ourselves: Video surveillance, urban space and self-responsibilization. *Cultural Studies*, *20*(4–5), 400–416. https://doi.org/10.1080/09502380600708770

YUXUAN Y., XIANYU Z., YUANJIE J. (2020). Sociological Aspects of Big Data Privacy. In Proceedings of the 2020 12th International Conference on Machine Learning

and Computing (ICMLC 2020). Association for Computing Machinery, New York, NY, USA, s. 230–235. https://doi.org/10.1145/3383972.3384075

YÜCEDAĞ, N. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanununun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 75(2), 765-790.

YÜKSEL, M. (2009), 'Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar', Ankara Üniversitesi SBF Dergisi, 64(1), 275 98.

YÜKSEL, M. (2017) Temel Hakların Sınırlandırılması ve Ölçülülük. SDÜHFD, Cilt:7, Sayı:1.

YÜKSEL, S. (2012) Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale. İstanbul: Beta Yayıncılık.

ZHANG, H., Lİ, P., DU, Z., & DOU, W. (2020). Risk entropy modeling of surveillance camera for public security application. *IEEE Access*, *8*, 45343–45355. https://doi.org/10.1109/ACCESS.2020.2978247

ZUBOFF, S. (2019). *The Age of Surveillance Capitalism*. Public Affairs. www.publicaffairsbooks.com

ELEKTRONİK KAYNAKLAR

AKTAN, H.Y. (29.01.2022). MOBESE'lerin Hukuki Durumu. Cumhuriyet. (Erişim Tarihi:12.08.2022)
https://www.cumhuriyet.com.tr/yazarlar/olaylar-vegorusler/mobeselerin-hukuki-durumu-hamdi-yaver-aktan-1903580

American Civil Liberties Union. (July 2013). You Are Being Tracked. (Erişim Tarihi:12.08.2022) www.aclu.org

American Convention on Human Rights, (Erişim Tarihi:20.09.2022).https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm

Amnesty International, France: New security law risks dystopian surveillance state. (Erişim Tarihi: 10.02.2022). https://www.amnesty.org/en/latest/news/2021/03/france-new-security-law-risks-dystopian-surveillance-state/

ANDREW, E. (15.01.2019), Town halls cut services but spend millions on CCTV, The Times. (Erişim Tarihi: 07.07.2022). https://www.thetimes.co.uk/article/town-halls-cut-services-but-spend-millions-on-cctv-bx2rsb9kb

APEC Privacy Framework (2005). (Erişim Tarihi:05.08.2022) https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

APEC Privacy Framework (2015). (Erişim Tarihi:05.08.2022).http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf

Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric Technologies, s.1-9. (Erişim Tarihi:05.08.2022) https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2012/wp193_en.pdf

Asia-Pacific Economic Cooperation, About APEC, (Erişim Tarihi:05.08.2022). https://www.apec.org/about-us/about-apec .

BOWCOTT, O. (06.05.2008). CCTV boom has failed to slash crime, say police. The Guardian, (Erişim Tarihi:05.08.2022). https://www.theguardian.com/uk/2008/may/06/ukcrime1

BUNN, N. And CUNNINGHAM B. (23.10.2015), Which Data Should Police Body Cams Collect? The Atlantic. (Erişim Tarihi:29.07.2022) https://www.theatlantic.com/politics/archive/2015/10/which-data-should-police-body-cams-collect/433197/

BRANDL, R. (03.02.2022) The world's most surveilled citizens. Tooltester. (Erişim Tarihi:30.07.2022) https://www.tooltester.com/en/blog/the-worlds-most-surveilled-countries/

Cambridge International AS & A Level Information Technology 9626 For examination from 2017, Data, information and knowledge, (Erişim Tarihi:29.07.2022) chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cambridgeinternational.org/images/285017-data-information-and-knowledge.pdf

République Française, Caméras de surveillance sur la voie publique et dans les lieux ouverts au public. (Erişim Tarihi:18.11.2022) https://www.service-public.fr/particuliers/vosdroits/F2517

CNIL, Cookies: GOOGLE fined 150 million euros. (Erişim Tarihi:18.11.2022) https://www.cnil.fr/en/cookies-google-fined-150-million-euros

CNIL, Data protection around the World. (Erişim Tarihi:18.11.2022) https://www.cnil.fr/en/data-protection-around-the-world

CNIL, Directive « Police-Justice » : de quoi parle-t-on ?, (Erişim Tarihi: 07.02.2022). https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t

CNIL, La CNIL publie 8 recommandations pour renforcer la protection des mineurs en ligne, (Erişim Tarihi: 28.01.2022). https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne

CNIL, La loi Informatique et Libertés, (Erişim Tarihi: 10.02.2022). https://www.cnil.fr/fr/la-loi-informatique-et-libertes

CNIL, La vidéosurveillance – vidéoprotection sur la voie publique(03.12.2019), (Erişim Tarihi: 19.11.2022) https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique

CNIL, Mises en demeure de plusieurs établissements scolaires pour vidéosurveillance excessive, (Erişim Tarihi: 10.02.2022). https://www.cnil.fr/fr/mises-en-demeure-de-plusieurs-etablissements-scolaires-pour-videosurveillance-excessive

CNIL, Plan Stratégique 2022-2024, (Erişim Tarihi: 11.09.2022) axe 3.s.7. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cnil.fr/sites/default/files/atoms/files/cnil_plan_strategique_2022-24.pdf CNIL (19.07.2022), Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position. (Erişim Tarihi: 11.09.2022) https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position

CNIL (13.12.2019), Vidéoprotection: quelles sont les dispositions applicables? (Erişim Tarihi: 11.09.2022) https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables

Conger, K. vd. (14.05.2019). San Francisco Bans Facial Recognition Technology. the New York Times. (Erişim Tarihi:18.11.2022). https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Consolidated version of the Treaty on the Functioning of the European Union, Part I, Title II, art.16. (Erişim Tarihi: 11.09.2022) https://www.legislation.gov.uk/eut/teec/article/16

Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data Convention 108(2021), Guidelines on Facial Recognition, s.1-16. (Erişim Tarihi: 11.09.2022) https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data. Decision of the Committee of Ministers. 128th session of the Committee of Ministers, Elsinore, 18 May 2018. (Erişim Tarihi: 05.09.2022) https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Council Of Europe (1981), Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, (Erişim Tarihi: 05.09.2022) https://rm.coe.int/1680078b37.

Council of Europe (2018), Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series No.223. (Erişim Tarihi: 05.09.2022) https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-theconvention-fo/16808ac91a

Cornell Law School, Legal Information Institute, Surveillance. (Erişim Tarihi: 22.09.2022) https://www.law.cornell.edu/wex/surveillance

DASCALESCU, A. (20.09.2022) The Controversial Clearview AI Was Used By Florida Man's Lawyer to Clear Him Of Vehicular Homicide Charges. Techthelead. (Erişim Tarihi: 22.09.2022) https://techthelead.com/the-controversial-clearview-ai-was-used-by-florida-mans-lawyer-to-clear-him-of-vehicular-homicide-charges/

DOFFMAN, Z. (14.08.2019). *New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report.* (Erişim Tarihi:06.05.2021), https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fing.

Economic Community Of West African States (Ecowas) Revised Treaty. (Erişim Tarihi: 01.10.2022)https://www.ecowas.int/wp-content/uploads/2015/01/Revised-treaty.pdf

EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, (Erişim Tarihi: 10.09.2022) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en

Electronic Frontier Foundation, Street Level Surveillance, (Erişim Tarihi:29.07.2022) https://www.eff.org/tr/issues/street-level-surveillance

Electronic Frontier Foundation, Automated License Plate Readers (ALPRs), (Erişim Tarihi:29.07.2022) https://www.eff.org/tr/issues/street-level-surveillance

European Commission, Data protection-Rules for the protection of personal data inside and outside the EU. (Erişim Tarihi 01.10.2022) https://ec.europa.eu/info/law/law-topic/data-protection_en

European Data Protection Supervisor, video-surveillance, (Erişim Tarihi 18.06.2022). https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices (Version 2.0) Adopted on 29 January 2020, (Erişim Tarihi 17.12.2021). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf

Eye Biometrics (t.y.), MIS Biometrics, (Erişim Tarihi: 29.04.2021). http:// misbiometrics.wikidot.com/eye

FERRON, E. (28.04.2021), Should You Give The Police Access To Your Home Security Camera?, (Erişim Tarihi 04.08.2021). https://www.safety.com/police-access-home-security-camera/

Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines, (Erişim Tarihi 18.06.2022).https://edps.europa.eu/sites/default/files/publication/12-02-13_report_cctv_en.pdf

Govenment U.K., Guidance Amended Surveillance Camera Code of Practice (accessible version) Updated 3 March 2022, (Erişim Tarihi:01.08.2022) https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

Greenwald, G., MacAskill,E.(07.06.2013), NSA Prism program taps in to user data of Apple, Google and others, The Guardian (Erişim Tarihi: 19.11.2022) https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

HARE, S. (10.11.2019). These new rules were meant to protect our privacy:they don't work. The Observer. (Erişim Tarihi: 10.08.2022). https://www.theguardian.com/commentisfree/2019/nov/10/these-new-rules-were-meant-to-protect-our-privacy-they-dont-work

Harvard Business Review(2022), "The New Rules of Data Privacy", (Erişim Tarihi: 19.11.2022) https://hbr.org/2022/02/the-new-rules-of-data-privacy

HARWELL, D. (18.05.2021) Amazon extends ban on police use of its facial recognition technology indefinitely. The Washington Post. (Erişim Tarihi: 05.08.2022)

https://www.washingtonpost.com/technology/2021/05/18/amazon-facial-recognition-ban/

HILL, K. (24.06.2020). Wrongfully accused by an algorithm, The Seatlle Times. (Erişim Tarihi: 05.08.2022) https://www.seattletimes.com/business/technology/wrongfully-accused-by-an-algorithm/

HILL K. (18.09.2022) Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands. The New York Times. (Erişim Tarihi: 22.09.2022) https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html?s=03

Iran International. (06.02.2022). Tehran's 5,000 Surveillance Cameras, 150 Sites Hacked. (Erişim Tarihi: 09.08.2022) https://www.iranintl.com/en/202206025165

İçişleri Bakanlığı. Gamer Projesi. (Erişim Tarihi:12.08.2022). https://www.icisleri.gov.tr/bilgiteknolojileri/gamer-projesi

KEMPF-LEONARD, K. and MORRIS, N.A. (2012). Social Control Theory. , (Erişim Tarihi: 30.06.2022). https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-97801953966070091.xml#:~:text=Durkheim's%20view%20of%20social%20control,%E2%80%9D%20(Durkheim%201951%2C%20p.

Kişisel Verileri Koruma Kurumu Yayınları (Haziran 2019). Örneklerle Kişisel Verilerin Korunması, No 29. (Erişim Tarihi:25.04.2021). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a23bfe08-9b3a-4c2f-8a97-a259dcc0e667.PDF.

Kişisel Verileri Koruma Kurumu, Kurul Kararları, *"Ses kayıt özelliği bulunan güvenlik kamerası kullanılması"* ile ilgili Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli

ve 2020/212 sayılı Karar Özeti, (Erişim Tarihi:12.08.2022). https://kvkk.gov.tr/Icerik/6892/2020-212 .

Kişisel Verileri Koruma Kurumu, Rehberler, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, (Erişim Tarihi 14.08.2021). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf

KLIEM, V. (17.09.2020). Body-Worn Cameras and Memory. Force Science. (Erişim Tarihi:09.08.2022) https://www.forcescience.com/2020/09/body-worn-cameras-and-memory/

KLOSOWSKI, T., (15.07.2021), Facial Recognition Is Everywhere. Here's What We Can Do About It. Wirecutter, (Erişim Tarihi: 05.08.2022) https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/

Les Caméras de Vidéosurveillance Peuvent Désormais "Vidéo-Verbaliser". (Erişim Tarihi:28.09.2022) https://toulouse.soussurveillance.net/spip.php?page=article&id_article=132&connect=sosu

MANANCOURT, V. (06.07.2022) Europe's state of mass surveillance. Politico. (Erişim Tarihi: 02.10.2022) https://www.politico.eu/article/data-retention-europe-mass-surveillance/

MIT Technology Review(2016), Capitalizing on the data economy, (Erişim Tarihi: 19.11.2022) https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/

Nişanyan Sözlük, (Erişim Tarihi:23.06.2022) https://www.nisanyansozluk.com/kelime/g%C3%B6zetim

OECD, Who we are, (Erişim Tarihi 18.08.2022) https://www.oecd.org/about/

OECD Legal Instruments, Background Information, (Erişim Tarihi 18.08.2022) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OECD Legal Instruments, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, (Erişim Tarihi 18.08.2022) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Oxford Learner's Dictionaries. (Erişim Tarihi 18.08.2022) https://www.oxfordlearnersdictionaries.com/definition/english/security?q=security

Official Journal of the European Communities Directive 95/46/EC Of The European Parliament And Of The Council (1995), on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (Erişim Tarihi: 25.04.2021) https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5

Official Journal of the European Union, Regulation (Eu) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), (Erişim Tarihi: 25.04.2021). https://eur-lex.europa.eu/eli/reg/2016/679/oj .

Official Journal of the European Union, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council

Framework Decision 2008/977/JHA, (Erişim Tarihi: 10.09.2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680

ÖNAL M. (2013). RFID Mimarisi ve Programlama, (1. Baskı, s. 241- 253), İstanbul: Kodlab, (Erişim Tarihi: 24.04.2021), https:// books. google. com.tr/ books?id=DT6nBAAAQBAJ&pg=PA246&dq=biyometrik+veri&hl=tr&sa=X&ved=0ahUKEwjBm6qLyKfXAhUKKcAKHRG1A7gQ6AEIOzAE#v=onepage&q=biyometrik%20veri&f=false

PEYRON, J., Debate swirls as Paris embraces video surveillance, France 24. (Erişim Tarihi: 10.01.2022) https://www.france24.com/en/20120117-debate-swirls-around-paris-new-high-surveillance-system-cameras-cctv-police

République Française, Code de la sécurité intérieure (Version en vigueur au 28 février 2022), (Erişim Tarihi: 28.02.2022) https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505404

République Française, Loi 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, (Erişim Tarihi: 10.02.2022). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043530276

Security Magazine (12.04.2018), Pro's and Cons for IP vs. Analog Video Surveillance, (Erişim Tarihi:29.07.2022) https://www.securitymagazine.com/articles/88854-pros-and-cons-for-ip-vs-analog-video-surveillance

Security Magazine. (01.05.2020). Automatic Number-Plate Recognition System Exposes 9 Million Records. (Erişim Tarihi: 09.08.2022) https://www.securitymagazine.com/articles/92287-automatic-number-plate-recognition-system-exposes-9-million-records

Schneier on Security (2014), Surveillance is the Business Model of the Internet: Bruce Schneier.(Erişim Tarihi: 19.11.2022) https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html

Surfshark, Surveillance Cities, (Erişim Tarihi: 28.07.2022) https://surfshark.com/surveillance-cities

ŞEN, E. (24.01.2016). Mobese ve Kamera Sistemi ile İzleme. Hukuki Haber. (Erişim Tarihi:12.08.2022) https://www.hukukihaber.net/mobese-ve-kamera-sistemi-ile-izleme-makale,4576.html

ŞEN, E. (21.11.2019). MOBESE ve Güvenlik Kameralarının Özel Hayata Müdahalesi ve Delil Vasfı. Hukuki Haber. (Erişim Tarihi:12.08.2022). https://www.hukukihaber.net/mobese-ve-guvenlik-kameralarinin-ozel-hayata-mudahalesi-ve-delil-vasfi-makale,7202.html

Thales Group, "What is biometrics" (Erişim Tarihi:29.04.2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

The World Bank, Individuals using the Internet (% of population), (Erişim Tarihi: 02.07.2022) https://data.worldbank.org/indicator/IT.NET.USER.ZS

The Wall Street Journal, NSA Officers Spy on Love Interests, (Erişim Tarihi: 03.07.2022). https://www.wsj.com/articles/BL-WB-40005

Türk Dil Kurumu Sözlükleri, Güncel Türkçe Sözlük, (Erişim Tarihi:23.06.2022) https://sozluk.gov.tr/

The Local Fr, Drones and surveillance cameras: France's new security bill explained, (Erişim Tarihi: 10.12.2021). https://www.thelocal.fr/20201120/drones-and-surveillance-cameras-frances-new-security-bill-explained/

TRAICHUK, A. (12.11.2021) CCTV and Facial Recognition: Where Do the Two Technologies Overlap, Data Science Central. (Erişim Tarihi: 05.08.2022) https://www.datasciencecentral.com/cctv-and-facial-recognition-where-do-the-two-technologies-overlap/

Türkiye Cumhuriyeti İçişleri Bakanlığı (11.10.2017) "Valiler Buluşması", (Erişim Tarihi:01.08.2022) https://www.icisleri.gov.tr/valiler-bulusmasi11102017

UNCTAD, Data Protection and Privacy Legislation Worldwide. (Erişim Tarihi 25.04.2022) https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

United Nations Digital Library, (1988) Guidelines for the Regulation of Computerized Personal Data Files: final report / submitted by Louis Joinet, Special Rapporteur. (Erişim Tarihi:19.08.2022) https://digitallibrary.un.org/record/43365?ln=en

United Nations Human Rights. International Covenant on Civil and Political Rights. (Erişim Tarihi:19.08.2022) https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Universal Declaration of Human Rights, (Erişim Tarihi: 19.11.2022) https://www.un.org/en/about-us/universal-declaration-of-human-rights

University of Minnesota, Human Rights Library, (Erişim Tarihi:19.08.2022). http://hrlibrary.umn.edu/gencomm/hrcom16.htm

Vie Publique, Loi du 25 mai 2021 pour une sécurité globale préservant les libertés, (Erişim Tarihi: 10.02.2022). https://www.vie-publique.fr/loi/277157-loi-pour-une-securite-globale-preservant-les-libertes

Voa, İstiklal Caddesi Saldırısı Failinin Kimliği Açıklandı. (Erişim Tarihi: 18.11.2022) https://www.voaturkce.com/a/istiklal-caddesi-saldirisi-failinin-kimligiaciklandi/6833192.html

WAHL, T. (04.05.2020), EDPB: Data Protection Guidelines on Video Surveillance, (Erişim Tarihi 17.08.2021). https://eucrim.eu/news/edpb-data-protection-guidelines-video-surveillance/

WILSON T.V. (t.y.), How Stuff Works: "How Biometrics Works: Voiceprints". (Erişim Tarihi: 29.04.2021). http://science.howstuffworks.com/biometrics3.htm

Wired (2022), How GDPR is Failing?, (Erişim Tarihi 07.07.2022). https://www.wired.com/story/gdpr-2022/

York, J. the harms of surveillance to privacy, expression and association, Global Information Society Watch. (Erişim Tarihi: 17.11.2022). https://giswatch.org/en/communications-surveillance/harms-surveillance-privacy-expression-and association#:~:text=Surveillance%20affects%20us%20in%20myriad,from%20progressing%20as%20a%20society

MAHKEME KARARLARI

AİHM. Peck ve Birleşik Krallık Kararı. Başvuru No: 44647/98. Karar Tarihi: 28 Ocak 2003. (Erişim Tarihi: 13.08.2022) https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]}

AİHM. Herbecq ve diğer v. Belçika Kararı. Başvuru No: 32200/96 ve 32201/96. Karar Tarihi: 14 Ocak 1998. (Erişim Tarihi: 13.08.2022) https://hudoc.echr.coe.int/

AİHM. Vukota-Bojić v. Switzerland Kararı. Başvuru No: 61838/10. Karar Tarihi: 18.10.2016. (Erişim Tarihi: 13.08.2022). https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-11261%22]}

AİHM. Antovic ve Mirkovic v. Karadağ, Başvuru No: 70838/13, Karar Tarihi: 28.11.2017, (Erişim Tarihi: 13.08.2022) https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-11757%22]}

Anayasa Mahkemesi E. 2016/125, K. 2017/143 28.09.2017 T. (Erişim Tarihi:12.08.2022) https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2017-143-nrm.pdf

Prince Albert v.Strange (Erişim Tarihi: 13.07.2022) https://www.casemine.com/judgement/uk/5a8ff8d260d03e7f57ecdced

Prince Albert v. Strange, High Court of Chancery. (1849) 1 Mac & G 25, [1849] EWHC Ch J20, 41 ER 1171, (1849) 18 LJ Ch 120. (Erişim Tarihi: 19.09.2022) http://www.bailii.org/ew/cases/EWHC/Ch/1849/J20.html

Yargıtay 12. Ceza Dairesi 2011/7345 E. 2012/8936 K. 03.04.2012 T.

Yargıtay 12. Ceza Dairesi 2015/4413 E. 2016/4086 K. 15.03.2016 T.