HALKA AÇIK ALANLARDA VİDEO GÖZETİM BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI: FRANSA ÖRNEĞİ

PERSONAL DATA PROTECTION IN THE CONTEXT OF VIDEO SURVEILLANCE IN PUBLIC AREAS: THE CASE OF FRANCE

Araştırma Makalesi

Ezgi TURGUT BİLGİÇ*

ÖZ

Halka açık alanlar yalnızca günlük faaliyetlerin yürütüldüğü değil aynı zamanda sosyalleşmenin ve toplumsal hayata katılımın da sağlandığı yerlerdir. Video gözetim cihazları ise halka açık alanlarda hem çeşitli güvenlik kaygıları hem de gelişen teknolojinin etkisiyle yaygın şekilde kullanılmaya başlanmıştır. Yapay zekâdaki gelişmeler de bu ivmelenmeye eklenmiş, yüz tanıma gibi özelliği olan kameralar değişmez nitelikte kişisel veri elde ettiklerinden pek çok açıdan çeşitli faydalar sağlamaya başlamıştır. Diğer taraftan halka açık alanlarda video gözetim cihazlarının yaygın kullanımı kişisel verilerin korunması yönünden birtakım kaygılar doğurmuş, video kayıt cihazları ile yapılan gözetime ilişkin hukuk kurallarının yeterliliği, güvenlik amacıyla elde edilen kişisel verilerin hukuka uygunluğu gibi konular tartışılmaya başlanmıştır. Kişisel verilerin korunması konusunda pek çok temel ve ikincil nitelikli hukuki düzenleme bulunan Avrupa Birliği ve Avrupa Konseyi üyesi bir ülke olarak Fransa'da video gözetimin geniş bir uygulama alanı vardır. Ülkede ayrıca konu hakkında düzenlenen kanun hükümleri, Ulusal Video Gözetim Komisyonu *(Commission Nationale de la Vidéoprotection)* gibi resmi birimler, Veri Koruma Otoritesi'nin *(CNIL)* tavsiye niteliğindeki rehber ve kararları ile ikincil nitelikteki düzenlemeler mevcuttur. Ancak yine de video gözetimin caydırıcılık, etkililik gibi işlevleri tartışılmakta, kişisel verilere ilişkin hukuki düzenlemelerin

DOI: 10.32957/hacettepehdf.1295271

Makalenin Geliş Tarihi: 10.05.2023 **Makalenin Kabul Tarihi:** 30.09.2023

* Hacettepe Üniversitesi Kamu Hukuku Doktora Öğrencisi, Kişisel Verileri Koruma Kurumu Uzman Yardımcısı.

E-posta: ezgiturgut.int@gmail.com

ORCID: 0000-0001-9667-3637.

Bu makale yazarın Hacettepe Üniversitesi Kamu Hukuku Bölümü'nde hazırlanan Yüksek Lisans Tez Çalışması'ndan üretilmiştir.

Bu makale Hacettepe Üniversitesi Hukuk Fakültesi Dergisi Araştırma ve Yayın Etiği kurallarına uygun olarak hazırlanmıştır.

varlığı, ülkede uygulanan sürekli video gözetim faaliyetlerine yönelik eleştirilerin ve hukuka aykırılık iddialarının önüne geçememektedir.

Çalışmada Fransa'da halka açık alanlarda yapılan video gözetim ele alınmış, video kayıt cihazları karşısında kişisel verilerin korunmasını temin eden yasal zemine ve kameralı gözetim uygulaması hakkındaki mevcut eleştirilere yer verilmiştir. Bununla birlikte Fransa örneği üzerinden video gözetim ile kişisel verilerin korunması arasındaki ilişki belirtilmiş, özellikle yapay zekâ kullanabilen kameralar gibi yeni teknolojik gelişmelerin yaratabileceği hukuki ve etik zorlukların altı çizilmiş, güvenlik sağlama ile veri koruma arasındaki ölçülülüğün önemine değinilmiştir. Son olarak çalışmada, Fransa'da mevcut yasal düzenlemelere rağmen video gözetime dair bazı uygulamaların kişisel veriler yönünden endişelere sebep olduğu, daha etkin bir mekanizma oluşturulması gerektiği ifade edilmiştir.

Anahtar Kelimeler: Video Gözetim, CCTV, Kişisel Verilerin Korunması, Fransa, GDPR

ABSTRACT

Public spaces play a crucial role in facilitating everyday activities, social interactions, and community engagement. The integration of video surveillance devices in these areas has become increasingly common, driven by advancing technology and heightened security concerns. The advent of artificial intelligence, particularly facial recognition features, has further accelerated this trend, offering several benefits through the capture of unchangeable personal data. However, the widespread deployment of such devices has given rise to concerns regarding the protection of personal data, leading to debates about the adequacy of legal regulations governing video surveillance and the legality of obtaining personal data for security purposes.

In France, a member of both the European Union and the Council of Europe, where numerous primary and secondary legal regulations on personal data protection exist, video surveillance finds broad applications. The country has enacted specific laws on this subject, established official bodies like the National Video Surveillance Commission (Commission Nationale de la Vidéoprotection), and implemented secondary regulations such as advisory guides and decisions by the Data Protection Authority (CNIL). Despite these measures, debates persist around the functions of video surveillance, including deterrence and effectiveness. The existence of legal regulations pertaining to personal data has not been entirely successful in preventing criticism and allegations of illegality directed towards ongoing video surveillance activities in the country.

This study delves into the landscape of video surveillance in public areas in France, shedding light on the legal safeguards for personal data and acknowledging criticisms of camera surveillance. It explores the intricate relationship between video surveillance and personal data protection, underscoring the challenges posed by advanced technologies such as AI-enabled cameras. Despite the existing legal framework in France, the study posits that certain video surveillance practices give rise to concerns regarding personal data, advocating for the implementation of more effective mechanisms to address these issues.

Keywords: video surveillance, CCTV, personal data protection, France, GDPR

EXTENDED ABSTRACT

Background

Video surveillance has evolved into an indispensable tool for ensuring public safety, maintaining social order, and monitoring criminal activities in today's world. It is increasingly rare to encounter public spaces without an array of surveillance devices, each equipped with various types and features. The integration of artificial intelligence has further propelled this trend, especially with the deployment of cameras endowed with facial recognition capabilities, offering significant benefits such as enhanced security measures and the identification of potential criminals through the capture of unalterable biometric data. This technology empowers public authorities to monitor public spaces more efficiently, facilitating rapid responses when intervention is needed.

Public spaces serve not only as venues for daily activities but also as hubs for socialization and participation in socio-democratic life. Individuals establish a social context with their communities by being present in these areas. While it is acknowledged that individuals in public spaces expose themselves to some degree of visibility, concerns arise when personal data privacy is violated by cameras in certain situations. The extensive use of video surveillance devices, coupled with the introduction of artificial intelligence-enabled smart cameras in public spaces, raises legitimate concerns about the protection of personal data.

Critiques against the proliferation of video surveillance technology generally revolve around its perceived ineffectiveness in achieving intended purposes such as enhancing security and reducing crime. Additionally, concerns are raised about the potential misuse of personal data acquired by surveillance devices, either by state or non-state actors. There is apprehension about the potential violation of fundamental rights and freedoms, including privacy and freedom of expression, due to widespread surveillance. The questioning of legal security is also a pertinent issue. In light of these critiques, the relevance and effectiveness of legal regulations for the protection of personal data against video surveillance, as well as the delicate balance between security and freedom, become crucial. Failure to address these concerns may lead to the disregard of the fundamental data protection principle of proportionality.

Purpose

The aim of this study is to discuss the implications and significance of video surveillance in public spaces in France, focusing on the protection of personal data, and to examine how the balance between the desire for security and the right to privacy is established from a personal data perspective.

Research Questions

What are the legal and social consequences of extensive video surveillance in public spaces?

What are the concerns, criticisms, and risks related to the protection of personal data against video surveillance?

How is personal data protected in the face of societal interests or security concerns?

Is the legal framework for video surveillance practices in public spaces in France sufficient in terms of protecting personal data?

What are the implications of the extensive use of CCTV in France in terms of personal data?

Methodology

The study employed a qualitative research approach to examine the legal implications of video surveillance in public spaces for safeguarding personal data, using France as an illustrative example. Legal regulations, encompassing both European Union legislation and French national legislation, as well as other secondary rules related to video surveillance and personal data protection, were utilized. The research also encompassed a review of the general framework and multidimensionality of surveillance, academic literature on video surveillance and personal data protection, and current developments in the field.

The first section of the study delves into the concept and history of video surveillance, a topic with far-reaching implications for areas such as law enforcement, urban planning, and social psychology. This section explores perspectives that consider surveillance essential for maintaining social order, juxtaposed with counterarguments that view it as a manifestation of state control infringing upon individual rights.

In the second section, the study addresses the types of personal data acquired by video surveillance devices in public spaces and critiques of widespread video surveillance. Criticisms are categorized around four main arguments questioning the effects of video surveillance, namely functionality, susceptibility to authoritarianism or misuse, and concerns regarding legal security (legal certainty).

France, as a member of the European Union with numerous legal regulations governing the protection of personal data, extensively applies video surveillance. Apart from fundamental EU regulations, there exist national laws, official bodies like the National Video Surveillance Commission (Commission Nationale de la Vidéoprotection), advisory guides, decisions from the Data Protection Authority (CNIL), and secondary regulations. However, despite the existence of legal frameworks concerning personal data, debates persist on the functions of video surveillance, such as deterrence and effectiveness. These regulations have not completely addressed criticisms and allegations of illegality directed at video surveillance practices in the country.

In the third and final section of the study, video surveillance in public spaces in France is discussed, emphasizing the legal framework ensuring the protection of personal data against video recording devices and current criticisms of camera surveillance practices. The study also explores the relationship between video surveillance and the protection of personal data, using the example of France. It highlights legal and ethical challenges posed by new technological developments, especially cameras utilizing artificial intelligence, and discusses the importance of proportionality between ensuring security and protecting data.

Conclusion and Results

In light of technological and technical advancements, it has become imperative to address the discourse surrounding the protection of personal data by elucidating the legal and practical dimensions of the rapidly expanding video surveillance practices. This study, using France as a case study, has elucidated the intricate relationship between video surveillance and data protection law. Despite the presence of current legal regulations in the country, it has been noted that specific practices associated with video surveillance raise

concerns regarding personal data. Consequently, there is a call for the establishment of a more effective mechanism to safeguard personal data.

GİRİŞ

Video kayıt cihazları, halka açık alanlarda gözle görülmesi güç gözetmenler olarak, her hareketimizi titizlikle kaydetmektedir. Kapalı devre televizyonlar, genel kullanımıyla CCTV *(Closed-circuit television),* tek veya çoklu kameralar kullanarak belirli bir bölgeyi gözetlemek, bu gözetim sonucunda elde edilen görüntüleri kaydetmek ve video formatında oynatmak amacıyla kullanılmaktadır[1]. Teknolojinin ilerlemesi, bu sistemlerin kurulum ve işletme maliyetlerini düşürmüş, bu durum kamu otoritelerinin özellikle yoğun kalabalığın olduğu sokak ve caddeler gibi halka açık yerlerde bu tür sistemleri sıkça kullanmaya başlamasına neden olmuştur.

2021 yılının sonlarına doğru dünya genelinde yaklaşık 1 milyar kamera bulunmaktadır ki bu da her 8 kişiyi izlemek için bir kamera mevcudiyeti anlamına gelir[2]. Kameraların daha gelişmiş ve geniş alanları kapsayabilen özelliklere sahip olmaları, onları güvenlik önlemlerinin uygulanması açısından da etkili hale getirmiştir. Ancak özellikle şehirlerde halka açık alanlarda kurulan CCTV sistemlerinin sayısındaki artış, güvenliği sağlama amacı dışında, sosyal denetim oluşturma, yaşam kalitesi ile güvencesi yaratma ve bilgi toplama gibi çeşitli nedenlere de dayandırılmaktadır.

Halka açık alanlar, sadece basit birer sosyalleşme mekânları değil, aynı zamanda sivil toplumun temelini oluşturan, insanların özgürce bir araya gelebildiği yaşamsal arenalardır. Bir görüşe göre bu mekanlar toplumsal anlaşmayı ve topluluk kimliklerini destekleyen, insanların günlük aktivitelerini sürdürebileceği yerlerdir[3]. Diğer bakış açısına göre halka açık alanlar, kimliklerin oluşturulduğu ve tartışıldığı, toplumsal eylemler ve bireylerin bir araya gelmesiyle aynı zamanda demokratik bir platform olan

---

1 Cüneyt Akınlar, "Kapalı Devre Görüntü ve Kayıt Sistemleri", Yusuf Oysal (ed.), Güvenlik Sistemleri (1. Baskı, Anadolu Üniversitesi Yayınları, Eskişehir 2012), 83.

2 Surfshark, "Surveillance Cities" <https://surfshark.com/surveillance-cities>

3 Jason W Patton, "Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places" (2000) Ethics and Information Technology, 181.

bölgelerdir[4]. Bu nedenle halka açık alanların, sosyal ritüellerin ve kültürel davranışların gerçekleşmesi, sosyal rollerin üstlenilmesi ve toplumsal dönüşümlerin yaşanması açısından önemli mekanlar olduğu açıktır[5]. Ayrıca bu alanlar, insanların suç mağduru olabileceği veya suç korkusu ve diğer güvenlik endişelerinin tetiklenebileceği yerler olarak da tanımlanabilir[6]. Nihayetinde halka açık alanlar, özel yaşamın dışa vurulduğu, toplumsal katılımın sağlandığı alanlardır. Bu bağlamda halka açık alanlarda yoğun olarak kullanılan gözetim araçlarının, bireyler ve topluluklar üzerinde önemli etkileri bulunur.

Video gözetim, uygulandığı halka açık alanları temelden değiştirmekle kalmayıp aynı zamanda bu alanlarda kişisel verilerin ve özel yaşamın gizliliğinin korunması gerekliliğini de beraberinde getirmektedir. Ayrıca kamu otoritelerinin yürüttükleri video gözetim faaliyetleri için kendilerine de sınır koymalarını gerektiren hukuk normları oluşturulması gereği ortaya çıkar. Özellikle belirli toplumsal gruplar açısından uygun koruma ve denetim olmaksızın uygulandığında ortaya çıkabilecek ayrımcılık meydana getirme riski, bu tür kameralı izleme yaklaşımlarının ölçülü ve dikkatli bir şekilde hayata geçirilmesini gerektirir[7].

Çalışmanın amacı, Fransa'da kişisel verilerin korunmasını odağa alarak halka açık alanlardaki video gözetimin kişisel verilerin korunması yönünden sonuçlarını ve anlamını tartışmak, güvenlik sağlama ve özel hayatın gizliliğinin korunmasını isteme hakkı arasındaki dengenin nasıl kurulduğunu -kişisel veriler yönünden- incelemektir. Bu amaç doğrultusunda çalışmanın ilk bölümünde genel olarak gözetimin tarihsel ve kavramsal temelleri ile video gözetimin anlamına bir giriş yapılmıştır. Çalışmanın ikinci bölümünde yaygın gözetime yönelik temel eleştiriler ve son bölümünde Fransa'daki mevcut yasal çerçeve ele alınarak kişisel verilerin güvenlik sağlama ve sair amaçlar karşısında ne şekilde korunduğu ifade edilmeye çalışılmıştır.

---

4 Beth Dıamond, "Safe Speech: Public Space as a Medium of Democracy" (2010) Journal of Architectural Education,105.

5 Ibid.

6 Vania Ceccato And Mahesh Nalla (eds), Crime and Fear in Public Places: Towards Safe, Inclusive and Sustainable Cities (1. Baskı, Routledge, London 2020), 8.

7 Ibid.

Fransa video gözetim bağlamında birkaç önemli nedenden ötürü çalışmanın odağında yer almıştır. Özellikle saldırı, terörizm gibi güvenlik gereklilikleri doğuran eylemler sebebiyle[8] ülkede bilhassa büyük şehirlerde oldukça fazla CCTV kullanılmaktadır[9]. Diğer taraftan bir Avrupa Birliği *(AB)* ülkesi olarak Fransa'da kişisel verilerin korunmasını temin etmeyi amaçlayan AB Genel Veri Koruma Tüzüğü *(General Data Protection Regulation-GDPR)* ile sair düzenlemeler ve ulusal-yasal mekanizma bulunmaktadır. Fakat klasik CCTV'lerin yoğun kullanımı dışında yapay zekâ kullanabilen kameralara da başvurulması gibi durumlar, ülkede video gözetim yönünden kişisel verilerin korunması konusunu kimi zaman kuşkulara sebep olan bir saha haline getirmektedir.

Son yıllarda kapsamı günden güne genişleyen veri koruma hukuku ise kameraların bazı durumlarda kişisel veri elde etmesi, depolaması kısacası veri işlemesi gerekçesiyle kullanımlarında devreye girmektedir. Bu durumda kamu otoritelerince halka açık alanlarda video gözetim cihazları kullanılırken kişisel verilerin korunması düzenlemeleri ile korunan amaca uygun hareket edilmesi beklenir. Çalışma, konusu itibarıyla toplumsal, hukuki ve teknolojik unsurların iç içe geçtiği oldukça kapsamlı ve hızla güncellenen bir mahiyete sahiptir. Dolayısıyla video gözetimin kişisel verilerin hukuken korunması ve veri güvenliğinin sağlanması açısından doğuracağı zorlukları anlamak, konunun karmaşık ve nispeten yeni doğasını da anlamak için gereklidir.

I. VİDEO GÖZETİM VE KİŞİSEL VERİLER ARASINDAKİ İLİŞKİ

A. Gözetimin Kavramsal Boyutu

Gözetim sadece fiziksel alanları değil, dijital ayak izlerimizin takip edildiği siber mecraları da kapsamaktadır. Bu izleme, her bir siber platformda farklı bir "biz"

---

[8] République Française, "Caméras de surveillance sur la voie publique et dans les lieux ouverts au public", <https://www.service-public.fr/particuliers/vosdroits/F2517>

[9] Örneğin 1 km2 başına düşen kamera sayısının belirlendiği bir kıyasta İstanbul'da toplam 109.000 CCTV bulunurken Paris'te 26.834 adet CCTV olduğu saptanmıştır. Ancak suç indeksleri birbirlerine yakın gözüken bu iki metropolde İstanbul'da km2 başına düşen CCTV sayısı 42,3 iken Paris'te rakam 254,59'a yükselmektedir. Konu ile ilgili kaynak: Surfshark, "Surveillance Cities: Who Has The Most CCTV Cameras In The World?", <https://surfshark.com/surveillance-cities>

oluşturacak kadar kapsamlıdır. Gözetim konusundaki tartışmalar, sadece yapay zekâ destekli kamera sistemlerinin sağladığı izlemenin ötesine geçmektedir. Bu tartışmalar, gözetimin yasal boyutlarını, tarihsel gelişimini ve toplumsal etkilerini de içermekte bu konuları da detaylı bir şekilde ele almamızı gerektirmektedir. TDK sözlüğüne göre gözetim kavramı, gözetme işi, nezaret, himaye anlamlarında kullanılmaktadır[10]. Etimolojik inceleme yapıldığında, "közet" sözcüğünün "beklemek" veya "korumak" anlamlarında bir fiilden türemiş olduğu, benzer şekilde "gözetmek" fiilinin de eski Türkçe'de "göz" anlamına gelen "köz" kelimesinden "-at" takısı ile oluşturulmuş olabileceği karşımıza çıkar[11]. Kavramın İngilizce'deki karşılığı olan "surveillance" kelimesi, Fransızca'da "üzerinde" anlamına gelen "sur" ile "izlemek" anlamındaki Latince "vigilare" kelimesinden türetilmiş "veiller" fiilinin bir araya gelmesiyle oluşmuştur[12]. Ancak gözetim kavramının sadece kelime anlamı ve etimolojik kökeniyle sınırlı olmadığı, daha derin ve karmaşık anlamlar taşıdığı da söylenmelidir.

B. Video Gözetimin İşlevi

Devletlerin gözetim faaliyetleri temelde güvenlik odaklıdır. Dijital platformlardan şehirlerdeki CCTV kameralarına veya sınır kontrollerine kadar hem kendi güvenlik stratejilerini gerçekleştirmek hem de küresel güvenlik ilkelerini uygulamak adına birçok karmaşık ilişki içine girerler[13]. Fakat gözetim uygulamaları sadece güvenlikle de sınırlı kalmamakta toplumda kabul görmüş sosyal normları yeniden şekillendirmekte ve farklı toplumsal sapma biçimlerinin oluşmasına zemin hazırlamaktadır[14]. Video gözetim sistemleri, elde edilen görüntülerin yönetilmesi ve kullanılması işine hizmet etmek için kullanılan bir dizi teknik araçtan oluşur, diğer deyişle gözetime aracı kılınır. Bir video

---

10 Türk Dil Kurumu Sözlükleri, "Güncel Türkçe Sözlük", https://sozluk.gov.tr/ "gözetim".

11 Nişanyan Sözlük, <https://www.nisanyansozluk.com/kelime/g%C3%B6zetim>"gözetim".

12 Oxford Learner's Dictionaries, <https://www.oxfordlearnersdictionaries.com/definition/english/security?q=security> "security".

13 "Duygu Hatipoğlu Aydın, Siber Alan ve Hukuk (2022) Onikilevha Yayınları İstanbul" 184.

14 Christophe Bétın and Emmanuel Martınaıs, "Sécurité, vidéosurveillance et construction de la déviance : l'exemple du centre-ville de Lyon" (2003) 27(1) Déviance et Société, 3.

gözetim sistemi analog ve dijital cihazlar ile bir yazılımdan oluşur, burada amaç belirli bir sahnenin görüntülerini yakalama, görüntü işleme ve bunları bir operatöre göstermektir[15].

Kamera ile video kaydı alınması, fotoğrafın suç önleme ve kontrol amacı için kullanılmasıyla doğrudan ilişkilidir[16]. 1850'lerde Amerika'da, gözaltına alınan mahkumların fotoğraflarının çekilmesiyle başlayan bir uygulama, ilk olarak ulusal ölçekte ve daha sonra geniş bir coğrafyada benimsenmiştir[17]. Uygulama, fotoğrafın suç kontrolü ve önleme amacıyla stratejik bir şekilde kullanılmasının erken bir örneğidir.

1960'lar, video gözetim tarihinde bir dönüm noktası oluşturmaktadır. Bu dönemde video kaset kaydedici (*videocassette recorder-VCR*) piyasaya sürüldüğünde, kameradan alınan görüntülerin kimyasal işlemeye ihtiyaç duymadan doğrudan filme kaydedilebilmesi mümkün hale gelmiştir. Bu teknolojik gelişme, daha ekonomik ve basit bir kayıt yöntemini mümkün kılarak görüntülerin tek bir kişi tarafından uzaktan izlenmesine olanak sağlamıştır. 1960'larda suç önleme ve hırsızları caydırmak amacıyla geliştirilen CCTV, 1970'lerde daha yaygın bir şekilde kullanılmaya başlanmıştır. Örneğin, henüz o dönemde bile ABD polisi tarafından caddelerde 24 saatlik gözetim sağlayacak kameraların konumlandırıldığı belirtilmektedir[18]. Neticede teknolojik ilerlemeler sayesinde 1980'lerde video gözetim sistemleri ivme kazanmış, bu gelişme 1990'lar ve sonrasında bu sistemlerin kullanımında önemli bir artışa yol açmıştır.

---

15 European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices (Version 2.0)" (adopted 29 January 2020), 29

<https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf.>

16 Clive Norrıs and Gary Armstrong, The Maximum Surveillance Society (Berg, Oxford and New York 1999), 3.

17 Ibid.

18 Selim Çapar, Birleşik Krallıkta CCTV, Türkiye'de Mobese Caddelerde Güvenlik Nöbetindeki Kameralar (Turhan Kitabevi Yayınları, Ankara 2011), 13.

C. Video Kayıt Sistemleri Tarafından İşlenen Kişisel Veriler

CCTV'ler tarafından elde edilen görüntüler, doğrudan bireylerle ilişkilendirilebildiği için kişisel veri olarak kabul edilir ve sistemlerce elde edilen görüntüler hukuki inceleme konusu haline gelir. Kişisel verinin uluslararası düzenlemelerde genel kabul gören tanımı *"…tanımlanmış veya tanımlanabilir bir gerçek kişiye (data subject, veri öznesi veya ülkemizdeki 6698 sayılı Kişisel Verilerin Korunması Kanununa 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…"* şeklindedir[19]. Fakat video gözetim cihazları aracılığıyla kişisel veri elde edilmesi, her zaman için "veri işleme" olarak kabul edilmemektedir. Hangi durumların veri işleme faaliyeti sayılacağı, somut olayın detaylarına, hukuki düzenlemelere ve mahkeme kararlarına bağlı olarak belirlenmektedir.

Kamu otoriteleri tarafından halka açık alanlarda kullanılan gözetim kameraları arasında otomatik plaka tanıma sistemleri *(Automatic License Plate Recognition-ALPR),* vücut kameraları, yüz ve iris tanıma yetenekli kameralar, geleneksel kapalı devre televizyonlar *(CCTV)* ve gün ışığında ya da kızılötesi modda video veya fotoğraf çekebilen insansız hava araçları bulunmaktadır[20]. Güvenlik güçleri tarafından yaygın olarak kullanılan otomatik plaka tanıma sistemleri *(ALPR),* sokak direkleri veya otoyol üst geçitleri gibi yerlere monte edilmiş kameralardır. Bu sistemler plaka numaralarını, konum ve zaman bilgisiyle birlikte otomatik olarak kaydeder ve bu verileri bir merkezi sunucuda saklar[21]. Bu sistem sayesinde, sabit veya hareketli ALPR kameraları, plaka numaraları, araç rengi ve markası gibi bilgileri, tarih ve konum verileriyle birleştirerek saklar. Bu veriler, şüpheli araçların hareketini izlemek ya da suç mahalline yakın araçları

---

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

[20] Electronic Frontier Foundation, "Street Level Surveillance" <https://www.eff.org/tr/issues/street-level-surveillance>

[21] Electronic Frontier Foundation, "Automated License Plate Readers (ALPRs)" <https://www.eff.org/cases/automated-license-plate-readers >

belirlemek için güvenlik birimlerine iletilir[22]. Plaka verileri aracılığıyla, araç tescili ve ehliyet veri tabanlarına erişilerek, plaka sahiplerine ait hassas kişisel verilere de (örneğin sabıka kaydı) ulaşılabilmektedir.

Yaka kameraları *(Body Worn Camera-BWC)*, polisler ve yetkili diğer kişilere gerçek zamanlı bilgi sağlar ve saha ile kontrol merkezi arasında sürekli bir veri akışı oluşturur. Bu sayede saha operasyonları daha merkezi bir şekilde koordine edilmiş olur[23]. BWC'ler, özellikle dar alanlarda sıkça kullanılır ve genellikle video ile ses verilerini merkezi sunuculara aktarır. Bu kameraların açılıp kapanması veya durdurulması genellikle kullanan yetkilinin takdirine bağlıdır[24]. Yüz ve iris taraması yapabilen bu kameralar, değişmez nitelikteki biyometrik verileri de elde ederler. Bu sebeple ölçüsüz kullanımları eleştiri konusudur.

II. HALKA AÇIK ALANLARDAKİ VİDEO GÖZETİME YÖNELİK GENEL ELEŞTİRİ ODAKLARI

A. CCTV'lerin İşlevine İlişkin Tartışmalar

Kameraların işlevselliğiyle ilgili ana tartışma, halka açık alanlardaki kameraların suç oranlarını azaltıp azaltmadığı ve eğer azaltıyorsa, hangi tür suçlarda daha etkili oldukları üzerinedir. CCTV'lerin etkinliğini inceleyen bir çalışmada, bu kameraların farklı suç türlerine değişen etkileri olabileceği belirtilmekte, suçların kameraların bulunmadığı bölgelere kayabileceği ve CCTV'nin geniş anlamda olumlu bir etkisinin olmadığının altı çizilmektedir[25]. Ancak bu çalışmanın incelediği bölgede insanlar genellikle kameralar sayesinde daha güvende hissettikleri için kamera izlemesini desteklese de bu desteğin ne zamana kadar süreceği veya ölçüsüz kullanımın sonuçları öngörülerek mi verildiği oldukça belirsizdir.

---

[22] Wesley G Skogan, "The Future of CCTV" (2019) 18(1) Criminology and Public Policy, (s.161-166), 164.

[23] Ibid.

[24] Nelson Bunn and Bryan Cunnıngham, "Which Data Should Police Body Cams Collect?" The Atlantic (14 October 2015) <https://www.theatlantic.com/politics/archive/2015/10/which-data-should-police-body-cams-collect/433197/>

[25] Çapar (n 18) 63.

Welsh ve Farrington'un meta-analizi ise CCTV'nin Birleşik Krallık'ta (özellikle otoparklarda) işlenen araç suçlarını etkili bir şekilde azalttığını ancak diğer suç türlerine önemli bir etkisi olmadığını göstermektedir[26]. Ayrıca analizde, CCTV'nin suçluları tespit etme kapasitesinin, suçluları caydırmada sağladığı faydalardan daha etkili olduğu, bu kameraların yaya ve trafik güvenliğini artırabileceği, terör eylemlerinin önlenmesine yardımcı olabileceği de ifade edilmektedir. Zira 11 Eylül saldırıları sonrasında, terörle mücadele amacıyla Amerika ve Avrupa'da CCTV sistemlerinin kullanımı ciddi şekilde artmıştır.

Sosyal medya kullanıcılarının fotoğraflarını izinsiz bir şekilde kullanarak yüz tanıma algoritmasını geliştiren Clearview AI gibi yazılımlar, bu tür teknolojilerin tartışmalı yönlerini gündeme getirmektedir[27]. Ancak yüz tanıma özelliği olan kameraların işlevselliği konusundaki tüm eleştirilere rağmen bu tür cihazların belirli olayların çözümünde oldukça etkili olabildiği de söylenmelidir. Örneğin Floridalı bir kişi araç ile insan öldürmekle suçlandığında, kişinin avukatı bu yazılımı özel erişim izni ile kullanmış ve kaza yerinde çekilmiş görüntülerle 20 milyar yüz verisini karşılaştırmıştır[28]. Böylelikle Clearview AI yazılımı, suçlanan kişinin aracı kullanan kişi olmadığını saptamış, bu saptama suç isnadına ilişkin yapılan savunma için kritik bir delil olabilmiştir.

B. Kötüye Kullanılma Potansiyeline İlişkin Tartışmalar

Güvenlik ile özgürlük arasındaki denge, otoriter uygulamalara ve kötüye kullanıma açık olma riski taşıyan yöntemlerin kullanımı konusunda önem arz eden bir konudur. Suç ve güvenlik endişeleri, devletleri daha fazla gözetim ve kontrol mekanizmaları oluşturmaya itebilir. Kimi zaman devletin kendisi tarafından da güvensizlik yaratabilen bu izleme uygulamaları, otoriterliği destekleyen bir güç dinamiği oluşturabilir ve bireyleri

---

[26] Brandon C Welsh and David P Farrıngton, "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis" (2009) 26(4) Justice Quarterly, 735-742.

[27] Ana Dascălescu, "The Controversial Clearview AI Was Used By Florida Man's Lawyer to Clear Him Of Vehicular Homicide Charges" Techthelead <https://techthelead.com/the-controversial-clearview-ai-was-used-by-florida-mans-lawyer-to-clear-him-of-vehicular-homicide-charges/ >

[28] Kashmir Hıll, "Wrongfully accused by an algorithm", The Seattle Times <https://www.seattletimes.com/business/technology/wrongfully-accused-by-an-algorithm/>

sürekli şekilde devam eden bir gözetim altında tutabilir. Bu bağlamda, devletlerin hangi yöntemleri kullanarak güvenlik sağlayacakları ve bireysel özgürlükleri nasıl koruyacakları önemlidir.

Yüz tanıma ve diğer biyometrik veri elde eden teknolojilerin kullanıldığı kameraların sayısının artması, bu alanda eleştirilerin de çeşitlenmesine yol açmıştır. Bu cihazlar, suç önleme ve suçlu takibi amacıyla kullanılan yapay zekâ algoritmaları ile donatılmıştır. Algoritmalar, topladığı yüz verilerini mevcut veri tabanları ile karşılaştırabilir, derin öğrenme (*deep learning*) teknikleriyle çeşitli analizler yapabilir ve hassas nitelikteki biyometrik verileri işleyebilir[29]. Bu durum yalnızca suç önleme kapasitesini değil aynı zamanda bireylerin özgürlük ve gizliliğine yönelik endişeleri de doğurur.

Biyometrik veriler, kişiye özgü ve değişmez karakteristiğe sahip oldukları için yüz tanıma sistemlerine olan endişeler özellikle devletler bu sistemleri kullanmaya başladığında artar. Bu tür sistemlerin yanıltıcı sonuçlar üretebilmesi, verilerin silinemediği ve böylece güvenlik riski yaratabileceği durumlar, yapay zekânın yanlış veya önyargılı değerlendirmeler yapabilmesi ve yetkisiz erişim riskleri, bu teknolojileri kullanımları açısından hem teknik hem de etik açıdan eleştiri konusu yapmaktadır[30].

C. Hukuki Güvenceye İlişkin Tartışmalar

Bir görüşe göre CCTV'ler aracılığıyla güvenliğin sağlandığına olan inanç artık o kadar yaygındır ki sıradanlaşmış durumdadır[31]. Bu sıradanlaşma esasen, güvenliği sadece teknolojik araçlarla değil aynı zamanda hukuki düzenlemeler ve toplumsal güven unsurlarıyla sağlamanın önemini ortaya çıkarır. Zira bireylerin güvenliğini sağlama

---

29 Zafer İçer ve Elif Dönmez "Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları" (2021) 15(43) Ceza Hukuku Dergisi, 423.

30 Ibid 430-431.

31 Benjamin Goold, Ian Loader and others, "The Banality of Security: The Curious Case of Surveillance Cameras" (2013) 53(6) British Journal of Criminology, 992-994.

iddiasındaki bu tür cihazların her yere yerleştirilmesi, paradoksal bir şekilde, arzu edilen güvenlik seviyesini zayıflatabilecek koşulları da oluşturabilecektir[32].

Norris ve Armstrong'un belirttiği gibi CCTV'nin yalnızca suçu azaltıp azaltmadığına odaklanmak yerine, bu cihazların nasıl ve neden konuşlandırıldığına dair daha geniş bir perspektife ihtiyaç vardır[33]. Operatörlerin hangi kriterlere göre kararlar aldığı, kameraların hangi tür "şüpheli" davranışlar veya kişileri izlemek için, hangi lokasyonlarda yer aldığı ve bu konuşlandırmanın sadece suçla ilgili endişelere mi hizmet ettiği yoksa daha geniş bir sosyal düzenleme ve belirli kişi topluluklarını takip etme amacına mı hizmet ettiği konuları bu tür bir değerlendirmenin kapsamında olmalıdır. Bu bağlamda gözetimin bir tür iktidar mekanizması olarak değerlendirilmesi gerekir. Bu tür bir iktidara ne tür sınırlamaların ve neden bu sınırlamaların konduğunu açıklığa kavuşturmak, hukuki düzenlemelerin yalnızca kitaplarda yazılı kurallar olmaktan çıkıp pratiğe nasıl yansıdığını anlamak için önemlidir. Hukukun sadece teorik bir yapı olarak değil, eylem ve uygulama olarak da incelenmesi, bu sınırların ne kadar etkili olduğunu ve kurallara ne derece uyulduğunu anlamak için kritik önemi haizdir[34].

AB üyesi ülkelerde bağlayıcı bir düzenleme olan GDPR (*Genel Veri Koruma Tüzüğü*) kişisel verilerin korunmasına yönelik temel kuralları belirlemekte ve bireylerin doğrudan kendilerine mündemiç bilgileri üzerinde kontrol sahibi olmasını amaçlamaktadır. Bu doğrultuda kişisel verilerin ait olduğu veri öznelerine (*data subjects*) çeşitli hukuki güvenceler sağlanmıştır. Bunlar kısaca, bilgilendirme hakkı (*right to be informed*), erişim hakkı (*right of access*), düzeltme hakkı (*right to rectification*), silme veya unutulma hakkı (*right to erasure-right to be forgotten*), veri taşınabilirliği hakkı (*right to data portability*), genel olarak kişisel verilerin işlenmesine itiraz hakkı (*right to object*), otomatik karar alma ve profil oluşturmaya itiraz hakkıdır (*right to object to automated decision making and profiling*)[35]. Ayrıca kontrolörler tarafından GDPR'da yer

---

[32] Ibid.

[33] Norrıs and Armstrong (n16) 10.

[34] Norrıs and Armstrong (n16) 10-11.

[35] 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

alan veri işleme koşullarına veya yükümlülüklerine aykırı davranılması durumunda uygulanacak yüksek idari para cezaları (kuruluşların yıllık küresel gelirleri üzerinden) belirlenmiştir[36].

Belirtilmelidir ki GDPR'ın kişisel verileri işlenen gerçek kişilere sağladığı hukuki güvenceler, günümüzde artık yapay zekâyı kapsamına alan kameraların kullanımı yönünden eksik kalmaktadır. Nitekim şeffaflık, düzeltme ve silme hakkı, itiraz hakkı gibi temel veri koruma ilkelerinin yapay zekâ kullanabilen sistemler karşısındaki etkinliği tartışmalıdır[37]. Yapay zekânın karmaşık doğası (verdiği kararların/çıktıların oluşturulduğu sürecin anlaşılması bakımından) GDPR'da garanti altına alınan açıklanabilirlik, şeffaflık gibi ilkeleri sarsmakta yanlış sonuçlar üretilmesi gibi durumlarda bireylere silme hakkının kullandırılmasının teknik açıdan nasıl mümkün olacağı şeklindeki sorular belirsizliğini korumaktadır. Örneğin yapay zekâ kullanabilen kameraların gerçekleştireceği algoritmik işleyiş neticesinde yanlış kişiler ile eşleştirme yapılması durumunda çeşitli hak ihlallerinin doğması ihtimal dahilindedir.

GDPR'ın gözetim toplumunu yasallaştırdığı fakat durdurmadığı, kural olarak yüz tanıma ve diğer biyometrik veri toplama teknolojilerinin genellikle vatandaşın açık rızası olmadan yasaklandığı ancak kamu yararı ve suçla mücadele gibi istisnaların zamanla bunun istisnası olmayı aşarak genel kural haline geldiği ifade edilir[38]. Özellikle GDPR'da tanımlanan istisnaların geniş ölçekte uygulanabilirliği, CCTV'lerin sadece istihbarat ve kolluk kuvvetleri tarafından değil, aynı zamanda birçok şirket ve mülk sahibi tarafından da kullanılabilir hale gelmesi gibi riskleri beraberinde getirmektedir[39]. Bu sebeple mevcut veri koruma ve insan hakları düzenlemeleri kameralı gözetimin getirdiği mahremiyet ve

---

of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) md. 13,14,15,16,17,20,21 ve 22. <https://eur-lex.europa.eu/eli/reg/2016/679/oj >

36 Ibid md. 83.

37 Frederike Ufert, "AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?" (2020) 5(2) European Papers 1094.

38 Stephanie Hare, "These new rules were meant to protect our privacy: they don't work", The Observer <https://www.theguardian.com/commentisfree/2019/nov/10/these-new-rules-were-meant-to-protect-our-privacy-they-dont-work >

39 Stephanie Hare, "These new rules were meant to protect our privacy: they don't work", The Observer <https://www.theguardian.com/commentisfree/2019/nov/10/these-new-rules-were-meant-to-protect-our-privacy-they-dont-work >

güvenlik sorunlarını ele alsa da salt bu yasal düzenlemelerin varlığı, gözetim sistemlerinin kişisel veriler yönünden güvenilir olduğu anlamına gelmeyecektir[40].

Hukuki düzenlemelerin sadece kişisel verilerin elde edildikten sonra nasıl korunacağını değil özellikle elde edilme sürecini ele alması ve bu yolla temel hak ve özgürlükleri evrensel bir şekilde koruması beklenir. Veri koruma konusunda lider bir role sahip olan AB'de mevcut yasalara rağmen hükümetlerin kitlesel gözetim uygulamalarına devam etmesi, kişisel verilerin korunmasına yönelik belirli sebep, ölçülülük, gereklilik gibi temel ilkeleri sorgulamak için anlamlı bir neden oluşturmaktadır. Bu durum özellikle Avrupa Birliği Adalet Divanı *(ABAD)* ve AİHM kararlarının uygulama bakımından ulusal yasalarla çeliştiği durumlar için geçerlidir[41].

III. FRANSA'DA HALKA AÇIK ALANLARDA UYGULANAN VİDEO GÖZETİM

A. Genel Bakış

Fransa halka açık alanlarda video gözetim, kamera kullanımına ilişkin hukuki düzenlemeler ve bunların doğurduğu tartışmalar bakımından oldukça ilgi çekicidir. Bunun temel nedeni kişisel verilerin korunması yönünden en geniş çaplı hukuki düzenleme kabul edilen GDPR'ın ve ikincil nitelikli düzenlemelerin uygulandığı bir AB ülkesi olmasıdır. Ülkede bir taraftan GDPR ve ulusal düzenlemeler ile video gözetime yönelik meşru bir zemin bulunurken, diğer taraftan ülkenin bağımsız veri koruma otoritesi olan CNIL'in[42] özellikle "akıllı" kamera sistemlerine karşı uyarıları[43] ve sivil toplum örgütlerinin CCTV'lere yönelik söylemleri ile bunlara rağmen yapılan tartışmalı

---

[40] Aaron DOYLE, Randy K LIPPERT and David LYON (eds), Eyes Everywhere: The Global Growth of Camera Surveillance (Routledge, London and New York 2012), 14.

[41] Vincent Manancourt, "Europe's state of mass surveillance", Politico <https://www.politico.eu/article/data-retention-europe-mass-surveillance/ >

[42] La Commission nationale de l'informatique et des libertés, Ulusal Bilgi İşlem ve Özgürlükler Komisyonu (Fransız Veri Koruma Otoritesi).

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

yeni düzenlemeler dikkat çekmektedir. Bu sebeple Fransa, kişisel verilerin korunması bakımından oluşturulan güncel yasal zemin ve özellikle terör veya şiddet faaliyetlerinin kontrolü sebebiyle kitlesel şekilde kişisel verilerin işlenmesinin yarattığı güvenlik-özgürlük ikilemini gözlemlemek bakımından bir uygulama örneği olarak ele alınmıştır. Zira ülkenin yapay zekâ destekli kamera kullanımına izin veren ilk AB ülkesi olması[44], yoğun CCTV kullanımı gibi konular kişisel verilerin korunmasından beklenen faydanın sorgulanmasına sebep olmaktadır.

Fransa'da video gözetim, farklı tartışmalara yol açan bir konu olarak dikkat çekmektedir[45]. 2024 yılında Paris'te yapılacak olan Olimpiyat ve Paralimpik Oyunları'nda Fransız Parlamentosu tarafından yapay zekâ kullanabilen kameraların kullanılmasına karar verilmesi kamuoyunda büyük yankı uyandırmıştır. İmzacıların arasında Uluslararası Af Örgütü ve İnsan Hakları İzleme Örgütü gibi oluşumların da bulunduğu otuz sekiz sivil toplum örgütünce oluşturulan açık mektupta, bahis konusu kamera kullanımının insan haklarına ve Avrupa Parlamentosu tarafından Haziran 2023'te kabul edilen Yapay Zekâ Tüzüğü (*Artificial Intelligence Act*[46]) olarak bilinen taslak düzenlemeye açıkça aykırı olduğu belirtilmektedir[47]. Konuya dair daha detaylı bilgiye aşağıdaki başlıklarda yer verilmiştir.

CNIL, belirli alanlarda yapılan gözetimle ilgili olarak aşırı video kayıt cihazı kullanımını vurgulamakta ve bu tür uygulamaların GDPR kapsamına girmesiyle ilgili

---

[44] The Brussels Times, "All-out assault on privacy': France is first EU country to legalise AI-driven surveillance", <https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance >

[45] Julien Peyron, "Debate swirls as Paris embraces video surveillance", France 24 <https://www.france24.com/en/20120117-debate-swirls-around-paris-new-high-surveillance-system-cameras-cctv-police >

[46] Proposal for a Regulation Of The European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legıslative Acts <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 >

[47] European Center for Not-for-Profit Law, "Civil Society Open Letter On The Proposed French Law On The 2024 Olympic And Paralympic Games" <https://ecnl.org/news/civil-society-open-letter-proposed-french-law-2024-olympic-and-paralympic-games>

kamuoyu duyuruları yapmaktadır[48]. Ek olarak, yıllar içinde video kameraların sayısı, gözetim yazılımları, kamera üretici firmalar ve devletlerin bu tür gözetim sistemlerine ayırdığı bütçe gibi video gözetim ekonomisine dahil olan faktörlerin, önemli ölçüde arttığı ifade edilmektedir[49]. Bu doğrultuda 2007 yılından itibaren ülkede video gözetim bir güvenlik sağlama hedefi olarak belirlenmiş ve dönemin İçişleri Bakanı tarafından 15 Mayıs 2007 tarihinde bir kararname kabul edilmiş, kararnameyle teknik konularda İçişleri Bakanı'na danışmanlık yapmak üzere bir Ulusal Video Koruma Komisyonu *(Commission Nationale de la Vidéoprotection)* kurulmuştur[50].

Fransız veri koruma sistemi iki kaynaktan şekillenir. Ulusal düzenlemeler ve AB düzenlemeleri şeklinde iki mevzuatın tatbiki ile sağlanan kişisel verilerin korunması, verilerin işlenmesini gerektiren sebepler, faaliyetler ve hatta cihazlar bakımından farklı hükümlere tabi olacaktır. Bu nedenle Fransa'ya odaklanan veri koruma değerlendirmesinde, ilk etapta geniş kapsamlı bir yaklaşımla temel AB düzenlemeleri ele alınmalı, ardından veri işleme yöntemleri veya spesifik amaçlar gözetilerek ulusal mevzuata odaklanılmalıdır.

B. Kişisel Verilerin Korunması Hakkında Uygulanacak Yasal Çerçeve

Kişisel verilerin korunması veya işlenmesi Fransa'da öncelikli olarak Avrupa İnsan Hakları Sözleşmesi *(AİHS)* ve Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi *(108 Sayılı Sözleşme)* gibi temel Avrupa Konseyi düzenlemeleri, GDPR, 2016/680 sayılı Polis ve Ceza Adaleti Direktifi[51] ile diğer

---

48 CNIL, "Mises en demeure de plusieurs établissements scolaires pour vidéosurveillance excessive" <https://www.cnil.fr/fr/mises-en-demeure-de-plusieurs-etablissements-scolaires-pour-videosurveillance-excessive>

49 The Local Fr, "Drones and surveillance cameras: France's new security bill explained" <https://www.thelocal.fr/20201120/drones-and-surveillance-cameras-frances-new-security-bill-explained>

50 Laurent Mucchielli, "À Quoı Sert La Vidéosurveillance De L'espace Public? Le cas français d'une petite ville «exemplaire»" (2016) 40(1) Deviance et Societe, 25.

51 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 "2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İş birliği

AB düzenlemeleri, "6 Ocak 1978 tarihli ve 78-17 sayılı Veri Koruma Kanunu"[52], 1 Mayıs 2012'de yürürlüğe giren İç Güvenlik Kanunu[53], 2021-646 sayılı Özgürlükleri Koruyan Küresel Güvenlik Kanunu[54] ve diğer ulusal düzenlemeler tarafından temin edilmektedir. Kişisel verilerin korunması için Avrupa Veri Koruma Kurulu (*European Data Protection Board-EDPB*) ve Avrupa Veri Koruma Denetçisi *(European Data Protection Supervisor-EDPS)* gibi AB seviyesindeki kurumlar, CNIL ve Ulusal Video Koruma Komisyonu gibi Fransa'ya özgü resmî kurumlar ve otoriteler de görev yapmaktadır. Bu yasal yapı, kişisel verilerin korunması için bir dizi önlem ve denetim mekanizması oluşturmayı hedeflemektedir.

1. Temel Sözleşmeler

AİHS'in 8. maddesine göre bir bireyin kişisel verilerinin işlenmesi, "özel ve aile hayatı, konutu ve yazışmalarıyla ilgili saygı hakkı"nın bir uzantısını teşkil eder[55]. Avrupa Birliği Temel Haklar Şartı 2000 yılında kabul edilmiş ve 2009 yılında bağlayıcı hale gelmiş olup bu şartta da kişisel verilerin korunmasını isteme hakkına ayrı bir başlık altında yer verilmiştir. Bu yenilik, hakkın AB tarafından özel hayatın gizliliği çerçevesinin dışına çıkarılarak bağımsız bir şekilde tanındığını göstermektedir. 1970'lerin ortasından itibaren Avrupa Konseyi Bakanlar Komitesi, AİHS'in 8. maddesini referans alarak kişisel verilerin korunması konusunda çeşitli kararlar almış ve düzenlemeler yapmıştır. 1981 yılında kabul edilen 108 Sayılı Sözleşme[56], veri koruma

---

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". <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>

52 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ("La Loi Informatique et Libertés"). <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460>

53 Code de la Sécurité Intérieure.

54 Loi no 2021-646 du 25 Mai 2021 Pour Une Sécurité Globale Préservant les Libertés.

55 "Handbook On European Data Protection Law" (Poland, 2018), 17.

56 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data <https://rm.coe.int/1680078b37>

hukukunda yasal bağlayıcılığı olan ilk uluslararası belge olarak bu şekilde ortaya çıkmıştır[57].

Teknolojideki ilerlemelerin sebebiyet vereceği olası veri koruma problemleri hakkında devam eden çalışmalar sonucunda 2018 yılında uygulamada 108+ olarak bilinen "Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Modernize Edilmiş Sözleşme"[58] henüz yürürlüğe girmese de Bakanlar Komitesi'nce kabul edilmiştir. 55 ülke ile birlikte Fransa da 108+'ın ilk imzacılarından olmuştur[59].

Avrupa Konseyi'nin onayladığı ve birçok ülkenin katıldığı 108+, yapay zekâ uygulamalarının giderek artan kullanımıyla birlikte ortaya çıkan gereksinimleri karşılamak için veri koruma konusunda alınması gereken yeni önlemleri ve güncellenmiş yönergeleri kapsamaktadır. Düzenleme, veri işleme kavramını sadece veri elde etme, saklama ve değiştirmeyi içeren faaliyetler olarak sınırlamamakta aynı zamanda kişisel verilere yapılan mantıksal ve/veya aritmetik işlemleri de veri işleme faaliyeti olarak kabul etmektedir.

11. madde altında "İstisnalar ve Sınırlamalar" başlığıyla yasallık, adillik, şeffaflık ve belirlilik gibi kritik ilkeler vurgulanmaktadır. Bu ilkeler, kolluk güçlerinin video gözetim gibi yöntemleri kullanmasına doğrudan bir engel oluşturmayacaktır. Ancak bu tür gözetim eylemleri suçların önlenebilmesi, araştırılması, belirlenmesi ve suçluların yargılanabilmesi ayrıca ulusal ve kamusal güvenliğin sağlanabilmesi amaçlarıyla yapılabilir. Bunlar, demokratik bir toplumda, hukuki uygunluk ve veri sahiplerinin hakları gözetilerek gerektiği ölçüde ve orantılı bir biçimde uygulanabilir[60]. Bu hüküm doğrultusunda, belirtilen nedenlerle halka açık yerlerde gerçekleştirilen video gözetim uygulamaları, genellikle veri işleme için gereken standart koşullardan muaftır. Ancak bu

---

57 "Handbook On European Data Protection Law" (Poland, 2018), 24 vd.

58 Council of Europe, "Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Convention 108 and Protocols" <https://www.coe.int/en/web/data-protection/convention108-and-protocol>

59 Council of Europe, Chart of signatures and ratifications of Treaty 223 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>

60 Ibid 26.

tür uygulamalarda dahi yasallık, adillik, şeffaflık ve belirlilik ilkelerine uyulması zorunludur.

Düzenlemede ayrıca, belirtilen sınırlamaların gerekliliğinin olaya özgü olarak ve kamusal menfaatin temel hedefleri doğrultusunda değerlendirilmesi gerektiği belirtilmiştir. "Uluslararası güvenlik" ve "kamu yararı" gibi kavramlar için istisnaların yapılması gerekebilir ancak bu istisnalar Avrupa İnsan Hakları Mahkemesi'nin *(AİHM)* ilgili içtihatlarına uygun olarak yorumlanmalıdır. Hatta ulusal güvenlik ve savunma amaçlı veri işleme faaliyetlerinde dahi bağımsız denetim ve inceleme mekanizmalarının devreye sokulması gerektiği özellikle vurgulanmaktadır[61].

2. AİHM Kararları Işığında Normatif Çerçeve

Kişisel verilerin korunmasını isteme hakkı, temel haklar arasında yer alır ve özel hayatın gizliliğinin bir uzantısı olarak hukuk eliyle sağlanır. Halka açık alanlarda gerçekleştirilen gözetim faaliyetleri söz konusu olduğunda ise bu hak yine belirli şartlar dahilinde korunabilecektir. Kişisel verilerin korunması için müstakil bir hüküm ihdas edilmemiş olsa da kişisel veriler AİHS'in 8. maddesinde yer alan özel hayata saygı hakkını düzenleyen madde kapsamında korunmaktadır. Diğer ifadeyle kişisel verilerin işlendiği durumları için 8. madde uygulanacaktır. Maddenin ikinci fıkrası, kamu otoritelerinin özel yaşama yalnızca *"müdahalenin kanun öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda[62]"* sınırlı şekilde müdahale edebileceğini belirtmektedir.

AİHM tarafından, halka açık alanlarda gerçekleşen tüm aktivitelerin özel hayatın ihlali olarak kabul edilmediği ancak CCTV kameraları gibi sürekli gözetim unsurlarının özel yaşamın bir parçası olarak değerlendirildiği anlaşılmaktadır. AİHM'in mevcut içtihadına göre bu tür kameralar tarafından toplanan kişisel veriler, 8. madde altında

---

61 Convention 108 +, m.11, para. 91,92 ve 94.

62 Avrupa İnsan Hakları Sözleşmesi 11., 14. ve 15. Protokoller ile değiştirilen metin <https://www.echr.coe.int/documents/d/echr/convention_tur >

korunan haklara dahildir. Bu madde sadece bireyin özel yaşamını korumakla kalmayıp halka açık alanlarda sosyal etkileşim ve dış dünya ile bağlantı kurma gibi özgürlüklerini de güvence altına alır[63]. Bu nedenle kamu otoriteleri tarafından sürekli ve sistemli şekilde halka açık bir alanın gözetlenip verilerin saklanması ile ara sıra fotoğraf çekilmesi arasında önemli bir fark olacaktır[64]. Ayrıca kişilerin halka açık bir alanda olması durumunda bile kişisel verilerin 8. madde kapsamındaki özel yaşamın gizliliği çerçevesinde korunmasına engel olunamayacaktır[65].

Diğer yandan CCTV'lerin kişisel veri işlediğinden bahsedebilmek için bu kameraların bireylerin kimliklerini belirleyebilecek şekilde görüntülerini toplarken bu görüntülerin anlık depolanması veya kaydedilip saklanması hususu oldukça önemli hale gelir[66]. Eğer elde edilen görüntüler kaydedilirse ve bu süreç kalıcı ya da sistematik bir biçimde yürütülüyorsa, kişisel verilerin korunması mevzuatı devreye girecektir. Yüz tanıma kabiliyetine sahip kameralar ise bireylerin değişmeyen kişisel verilerini topladığı için daha müdahaleci kabul edilir. Bu tür kameraların orantısız kullanımı, bireyler arasında eşitsizliğe yol açabileceğinden, bu teknolojinin daha ölçülü ve sınırlı şekilde kullanılması gerekir[67].

---

63 Peck v United Kingdom, App No 44647/98 (ECHR, 28 January 2003), para. 57, <https://hudoc.echr.coe.int/eng#{%22appno%22:[%2244647/98%22],%22itemid%22:[%22001-60898%22]}>

Ayrıca kişisel verilerin korunması ve kişilik hakkı arasındaki ilişki hakkında bkz. Onur BASKIN, Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması (Seçkin Yayıncılık, Ankara 2021), 67-108.

64 Herbecq and Others v Belgium, App No 32200/96 & 32201/96 (ECHR, 14 January 1998), 97, <https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-88070&filename=001-88070.pdf>

Sistemli ve sürekli izlemenin özel hayata müdahale olduğuna dair karar için bkz. Vukota-Bojić v Switzerland, App No 61838/10 (ECHR, 18 November 2016), para. 67 &77, <https://hudoc.echr.coe.int/eng#{%22appno%22:[%2261838/10%22],%22itemid%22:[%22001-167490%22]}>

65 Satakunnan Markkinapörssi Oy And Satamedia Oy V. Finland, App No 931/13 (ECHR, 27 June 2017), para. 131. < https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175121%22]}>

66 Elif Küzeci, Kişisel Verilerin Korunması (4. Baskı, On İki Levha Yayıncılık, İstanbul 2021), 508.

67 Lachlan Urquhart and Diana Lourdes Mıranda, "Policing Faces: The Present and Future of Intelligent Facial Surveillance" (2021) Information and Communications Technology Law 1, 8.

AİHM, AİHS'in 8. maddesinin 2. fıkrasında belirtilen özel yaşama müdahale hakkını, bir dizi kriteri göz önünde bulundurarak değerlendirir. Bu kriterler arasında müdahalenin toplumsal bir ihtiyaca yanıt olup olmadığı, müdahalenin meşru amaçlarla orantılı olması, uygulanan tedbirin amaca uygun ve geçerli olması, müdahale olmaksızın toplumda oluşabilecek zararlı etkilerin varlığı veya yokluğu gibi faktörler bulunmaktadır[68].

Terörle mücadele ve ulusal güvenlik bağlamında AİHM, güvenlik birimlerinin terör bağlantılı kişilerin kişisel verilerini kullanmasını özel yaşamın korunması açısından bir müdahale olarak kabul etmektedir. Ancak bu tür bir müdahalenin, acil bir toplumsal ihtiyaca yanıt verdiği durumlarda, orantılılık ilkesine uygun bir şekilde yapılması gerekmektedir[69]. Yani müdahale, meşru bir amacı yerine getirmek için gerekenden fazla olmamalıdır. Bu bağlamda, müdahalenin kapsamı, etkilenen birey sayısı ve bireylere sunulacak güvenceler gibi faktörler dikkatle değerlendirilmelidir[70].

3. Genel Veri Koruma Tüzüğü (GDPR)

AB'de kişisel verilerin korunmasına yönelik temel yasal belge 1995 yılından 2018'e kadar "95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi" *(Veri Koruma Direktifi)* olmuştur. Direktif kabul edildiğinde, yürürlükte olan 108 Sayılı Sözleşme'de bulunan veri koruma ilkelerini esas almış ve bunları genişletmiştir.

ABAD kararlarına göre de halka açık alanlardaki tüm video gözetimi sistemlerinin faaliyetleri, doğrudan kişisel veri işleme olarak kabul edilmez, durumun koşullarına ve gözetimin amacına bakılmalıdır. Bu sebeple kişisel verilerin "sürekli ve sistemli" bir izleme sonucu elde edilmesi beklenir. Özellikle biyometrik veya diğer hassas veri

---

68 "Handbook On European Data Protection Law" (Poland: Drukarnia Interak Printing House, 2018), 40.

Leander v. Sweden, App No 9248/81, (ECHR, 26 March 1987), para. 49-50-51. <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}>

69 Handbook On European Data Protection Law, 40.

70 Ibid.

türlerinin toplanmadığı genel amaçlı video izleme sistemleri için GDPR, 2016/680 sayılı Polis ve Ceza Adaleti Direktifi ve ulusal düzenlemeler bir dizi koruma önlemi ve kuralı içerir. Bu bağlamda GDPR'ın 5. maddesinde belirtilen genel işleme ilkelerine uyulması esastır. Bu ilkeler; *"(a) hukuka uygun 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"* şeklindedir.

Ayrıca GDPR'ın "kısıtlamalar" (*restrictions*) başlıklı 23. maddesi, veri koruma hükümlerinin uygulanmasının belirli durumlarda kısıtlanabileceğini düzenler. Bu kısıtlamalar, genellikle suçların önlenmesi veya kamu güvenliğine ilişkin tehditlere karşı koruma ve önleme gibi "belirli" meşru amaçlara dayalı olarak, temel hak ve özgürlüklerin özüne saygı gösterildiğinde ve demokratik bir toplumda gerekli ve orantılı olduğunda uygulanabilir. Örneğin milli güvenlik, savunma, kamu güvenliği, afetlere karşı insan hayatının korunması, suçların önlenmesi ve halk sağlığı gibi konular meşru amaçlar olarak kabul edilir.

Bu kısıtlamalar veri öznelerinin temel hak ve özgürlüklerini riske atmamalıdır. Ayrıca ilgili yasal tedbirler kötüye kullanım ve yasa dışı erişimi engelleyecek güvenceleri de içermeli, bu tür kısıtlamaların ne zaman ve hangi şartlar altında uygulanabileceği, veri öznelerinin bu kısıtlamalardan haberdar olma hakkı da belirtmelidir. İfade edilmelidir ki bu haller genellikle tüm GDPR hükümlerini dışlamaz ve temel veri koruma ilkelerine somut durumun koşulları çerçevesinde uyulmaya devam edilir[71].

Bununla birlikte suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması veya ceza yaptırımlarının infazı dahil kamu güvenliğine yönelik tehditlere karşı koruma ve önleme gibi belirli durumlarda, soruşturma altındaki veri öznelerine bilgi vermek, bu soruşturmanın başarısını tehlikeye atabilecektir[72]. Bu nedenle, para aklama gibi suçların takibi bakımından GDPR'ın 23(1)(d) maddesi uyarınca bilgiye erişim hakkının veya veri

---

[71] EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, 6 vd.

[72] Ibid 9.

öznelerine tanınan hakların da ayrıca kısıtlanması gerekebilir[73]. Elbette bu kapsamda yürütülmekte olan soruşturmayı tehlikeye atmaması kaydıyla, erişilmesi kısıtlanan bilgilerin veri öznelerine verilmesi gerekecektir.

Neticede itibarıyla halka açık alanlarda video gözetim için uygulanan istisnalar genellikle oldukça sınırlı bir kapsamda uygulanır ve yalnızca belirli meşru amaçlar çerçevesinde geçerlidir. Yani halka açık alandaki her izleme istisna kapsamında değerlendirilemeyecek, soruşturma gibi bazı özel durumlar açısından ancak yapılan işlemi tehlikeye düşürmemek adına istisna kapsamına dahil olunabilecek, bu durumda dahi bireylere belirli hakları sağlanacak ve gereklilik durumu sona erdiğinde veri sorumlusunun tabi olduğu yükümlülükler canlanacaktır[74].

GDPR kapsamında, biyometrik veri toplama yeteneğine sahip veya yapay zekâ teknolojilerinden faydalanan kameraların kullanılması durumunda, 35. maddeye göre bir Veri Koruma Etki Değerlendirmesi *(Data Protection Impact Assessment-DPIA)* yapılması da zorunludur. Bu konuda, yetkili kamu kurumlarında özellikle kameraların yerleştirilmesinden sorumlu olan bir veri koruma görevlisinin bulunması gerekmektedir. Bu görevli, etki değerlendirmesi sürecini koordine etmeli ve veri koruma ilkelerinin düzenlemelerle uyumlu şekilde uygulanmasını sağlamalıdır.

4. 2016/680 sayılı Polis ve Ceza Adaleti 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 Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Direktif veya kısa adıyla Polis ve Ceza Adaleti Direktifi ise temel olarak bireylerin kişisel veri güvenliği ile kamu kurumları veya polis tarafından veri işleme yoluyla sağlanan faydalar arasında bir denge oluşturmayı, adalet ve polislik alanlarında gerçekleştirilen veri işleme

[73] Ibid.

[74] Ibid 6.

faaliyetlerini, diğer türden veri işleme faaliyetlerinden farklı bir şekilde ele almayı hedefler[75].

Bu bağlamda Polis ve Ceza Adaleti Direktifi'ne uygun olarak üye devletlerin ulusal düzenlemelerinin, ceza soruşturma ve kovuşturma süreçlerini düzenlerken belirtilen ilkeleri gözetmesi gerekmektedir[76]. Eğer video gözetim, kamu güvenliğinin sağlanması, suçların önlenmesi ve soruşturulması gibi kolluk kuvveti uygulamaları ve ceza adaleti amaçları için gerçekleştiriliyorsa, bu Direktif'in kapsamına girecektir[77]. Yine Direktif'te yer alan durumlarda da AB Şartı, AİHS ve sair düzenlemeler ile uyumlu hareket edilmeli ve hakların sınırlanması dar yorumlanarak, kişisel verilerin korunmasını isteme hakkının özüne saygı duyularak veri öznelerine talepte bulunma hakları kullandırılmalıdır.

Polis ve Ceza Adaleti Direktifi'nin temel ilkeleri, GDPR ile büyük oranda örtüşmektedir. Bu durumda, örneğin halka açık alanlarda suçun önlenmesi amacıyla video gözetim yapan kontrolör olarak görevli kamu otoritelerinin, amaç belirleme, veri doğruluğu, güvenlik, belirli bir süre saklama, yasallık, şeffaflık ve orantılılık gibi ilkeleri gözetmesi beklenmektedir. Ancak Direktif'e uygunluğun tam anlamıyla AB üye ülkeleri arasında standartlaştırılması, ulusal düzenlemelerinin varlığı sebebiyle güç olabilir.

5. EDPB *(Avrupa Veri Koruma Kurulu)*- EDPS (*Avrupa Veri Koruma Denetçisi*) Düzenlemeleri

EDPB tarafından 2020 yılında video kayıt cihazları ile kişisel verilerin işlenmesine dair yayınlanan rehberin amacı, GDPR'ın bu konuyla olan ilişkisini ortaya koymak ve belirtilen ilkeler ve kuralların, farklı türdeki video kayıt sistemleri (geleneksel veya yapay zekâ destekli) için nasıl genelleştirilebileceğini açıklamaktır[78].

---

75 Gülşah Bostancı Bozbayındır, "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" (2018) Galatasaray Üniversitesi Hukuk Fakültesi Dergisi 51, 71.

76 Ibid.

77 Ibid 72.

78 Thomas Wahl, "EDPB: Data Protection Guidelines on Video Surveillance", Eucrim, <https://eucrim.eu/news/edpb-data-protection-guidelines-video-surveillance/ >

EDPS ise video kayıt sistemlerinin dikkatli bir şekilde tasarlanması ve uygulanması durumunda, veri güvenliği sorunlarının çözülebileceğini vurgular. Aksi takdirde gizliliğin ve dolayısıyla temel hakların ihlal edilme riski ortaya çıkabilir. Bu tür sistemlerin kullanımında ana odak noktaları; veri kalitesi *(data quality),* bilgi edinme hakkı *(right of information),* veriyi tutma süresidir *(retention period).* Veri kalitesi, gereksiz veya alakasız görüntülerin toplanmasını minimize etmeyi *(veri minimizasyonu)* ve kayıtların belirgin ve açık amaçlar için yapılmasını içerir. Ayrıca kamera kayıtlarının yapıldığına dair duyurular yapılmalı, kayıtların kim tarafından ne kadar süreyle saklanacağı konusunda bilgi verilmeli ve bu tür veri işleme faaliyetleri için belirgin politikalar oluşturulmalıdır[79].

Raporda belirtildiği üzere güvenlik amaçlı video kayıt sistemlerinin kurulmasında kamu otoritelerinin çok özenli olmaları gerekmektedir. Sadece "anormallikleri izleme" ya da "güvenlikle ilgili olaylara müdahale etme" gibi genel ifadelerle sistemin amacını belirtmek yetersiz kalacaktır. Gözetim yapılacak alanda karşılaşılabilecek ve önlem veya caydırıcılık amaçlanan spesifik güvenlik senaryolarına detaylı bir şekilde yer verilmesi zorunludur[80].

Rapor, güvenlik risklerinin sadece yüzeysel ifadelerle belirlenemeyeceğini de vurgulamaktadır. Spesifik tehlikeler, suç oranları gibi somut ve doğrulanabilir verilere dayanarak güvenlik risklerinin net bir şekilde tanımlanması gerekmektedir. Buna göre salt anektodal bilgiler veya varsayımlar, video gözetim sistemi kurmak açısından yeterli bir gerekçe olmayacaktır. Raporda, video kayıt sistemlerinin kurulduğu bölgedeki güvenlik risklerinin türü, bu bölgede geçmişte meydana gelen olaylar ve gelecekte olabilecek risklerin olasılığının dikkatli bir şekilde değerlendirilmesi gerektiğinin de altı çizilmiştir[81].

EDPB ve EDPS'nin düzenlemeleri, video gözetiminin "gereklilik" ve "çıkarlar dengesi" koşullarını vurgulamaktadır. "Kamu güvenliği" gibi geniş bir kavram, video gözetimi veri işleme açısından "istisnai" bir durum gibi gösterebilir fakat bu tür

---

79 Ibid.

80 Ibid 20.

81 Ibid 21.

gözetimlerde de mümkün olduğunca temel veri işleme ilkelerine sadık kalınması beklenir. Elbette yasal zorunluluklar veya belirli bir cezai soruşturma ve adli işlem sebebiyle elde edilen CCTV kayıtları bu genel değerlendirmenin dışında kalabilir. Ancak halka açık alanlarda yapılan sürekli ve sistemli gözetimde, uygun koşullar sağlanarak bireylerin sahip olduğu hakların korunması ve kullanılabilir olması önemlidir.

6. Ulusal Düzenlemeler

78-17 sayılı Veri Koruma Kanunu, Fransa'da kişisel verilerin korunması açısından önemli bir yere sahiptir ve Polis ve Ceza Adaleti Direktifi ile birlikte GDPR'ı Fransız hukukuna entegre etmektedir. "Avrupa Kişisel Verileri Koruma Paketi"nin yürürlüğe girmesi, Fransa'da veri sorumluları için yasal çerçeveyi yeniden şekillendirmiş ve İç Güvenlik Kanunu'na uygun olarak video gözetim sistemlerinin kurulmasını zorunlu kılmıştır. Bu çerçevede 78-17 sayılı Kanun'un 5. maddesi video gözetimle kişisel veri işlemenin hangi koşullarda yasal olacağını açıkça belirtir. Bu madde GDPR'da belirtilen veri işleme koşulları ile büyük oranda örtüşmektedir. Dolayısıyla video kayıt sistemleri aracılığıyla kişisel verilerin işlenmesi, belirtilen koşullardan en az birinin mevcut olması halinde yasal kabul edilecektir.

Bu sebepler özetle *"GDPR'a uygun rıza, işlemenin veri öznesinin taraf olduğu bir sözleşmenin ifası, veri öznesinin talebi üzerine alınan sözleşme öncesi tedbirlerin ifası için veya kontrolörün tabi olduğu yasal bir yükümlülüğe uygunluk için gerekli olması, işlemenin veri öznesinin 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 öznesinin çocuk olduğu durumlarda veri öznesinin menfaatleri veya özgürlükleri ve temel hakları ihlal edilmediği sürece veri sorumlusu veya üçüncü bir kişi tarafından izlenen meşru menfaatlerin amaçları için gerekli olması"*dır[82].

[82] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, md.5.

Kanun'un 42. maddesinde ise GDPR hükümlerinin uygulama alanı bulmayacağı durumlara yer verilmiştir. Bu doğrultuda *"(...) devlet adına uygulanan ve devlet güvenliği veya savunmasını ilgilendiren kişisel verilerin işlenmesi için geçerli olan devlet güvenliği ve savunmasını içeren işleme faaliyetleri, AB 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 maksadıyla yetki verilmiş mercilerce yürütülen veri işleme faaliyetleri"* GDPR hükümlerinin dışında kalacaktır.

Kanun'da yer alan 251-1 ila 255-1 maddeleri ise "video koruma"nın (*video protection*) temel kapsamını belirlemektedir. Örneğin 251-2. maddeye göre halka açık alanlarda alınan görüntülerin video gözetim cihazları ile kayıt altına alınması;

> *"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 (...) 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, halka açık tesislerin güvenliği, hukuki sorumluluğu garanti eden bir sigorta ile motorlu bir kara taşıtının işletilmesi için kapsanması gereken yükümlülüğe uygunluk sebeplerinin sağlanması"*

şeklinde belirtilen maksatlarla yetkili kamu otoriteleri tarafından yapılabilir. İç Güvenlik Kanunu'nun 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"* hükmü bulunmaktadır. AB'nin GDPR ve

sair düzenlemeleri kapsamının dışında kalan video gözetlemeler yönünden başta İç Güvenlik Kanunu olmak üzere konu hakkındaki ulusal düzenlemeler uygulanacaktır.

Fransız Resmî Gazetesi'nde 26 Mayıs 2021 tarihinde yayımlanarak yürürlüğe giren 2021-646 sayılı Özgürlükleri Koruyan Küresel Güvenlik Kanunu, zabıta, özel güvenlik şirketleri, yaka kameraları ve video koruması gibi gözetim araçları ve kolluk kuvvetlerinin korunmasını kapsamakta olup pek çok tartışmaya konu olmuştur[83]. Özgürlükleri Koruyan Küresel Güvenlik Kanunu geniş bir yelpazede güvenlikle ilgili konuları ele almakta, belediye polisleri ve özel güvenlik personeli gibi farklı güvenlik güçleri için çeşitli düzenlemeler getirmektedir. Ayrıca video gözetim sistemleri, araç içi kameralar, yaka ya da vücut kameraları ve dronlar gibi teknolojik gözetim araçlarına dair hükümler de yer almaktadır. Kanun, güvenlik personelinin saldırganlık veya provokasyon durumlarında kimlik tespiti yapabilmesi için uygulayabileceği çeşitli önlemler ve işlemleri de kapsamaktadır[84].

2016/680 sayılı Polis ve Ceza Adaleti Direktifi, Fransız iç hukukuna 78-17 sayılı Veri Koruma Kanunu aracılığıyla entegre edilmiştir. Bu Kanun'un 3. başlığı altında yer alan 87. madde, Direktif'in ana amacının, cezai işlemlerle ilgili olarak kişisel verilerin işlenmesi olduğunu belirtmektedir. Bu ceza gerektiren suçların önlenmesi, tespiti, soruşturma ve kovuşturma süreçlerini, ayrıca kamu güvenliğini ve bu alandaki tehditleri önceden belirlemeyi amaçlayan yaptırımların uygulanmasını da içerir. Direktif, suç işlenmeden önce gerçekleştirilen polis faaliyetlerini ve tehditleri erken bir aşamada belirlemeyi amaçlayan faaliyetleri de kapsamına almaktadır.

İfade edilmelidir ki eğer video gözetim yetkili organlar tarafından cezai inceleme veya suç önleme amacıyla gerçekleştiriliyorsa, bu tür aktiviteler Polis ve Ceza Adaleti Direktifi çerçevesinde değerlendirilecektir. Bu durumda genel GDPR hükümleri de geçerli olacaktır. Ancak eğer video gözetim veya diğer veri işleme uygulamaları devlet

---

[83] Amnesty International, "France: New security law risks dystopian surveillance state" <https://www.amnesty.org/en/latest/news/2021/03/france-new-security-law-risks-dystopian-surveillance-state/ >

[84] Vie Publique, "Loi du 25 mai 2021 pour une sécurité globale préservant les libertés" <https://www.vie-publique.fr/loi/277157-loi-pour-une-securite-globale-preservant-les-libertes >

güvenliği ya da ulusal savunma ile ilgiliyse, bu tür işlemeler AB'nin veri koruma düzenlemeleri dışında kalacak ve yalnızca ilgili ulusal düzenlemeye tabi olacaktır[85].

Özgürlükleri Koruyan Küresel Güvenlik Kanunu'nun yürürlüğe girmesiyle birlikte, Fransa'da video gözetim sistemine erişim yetkisi olan kuruluşlar da genişlemiştir. Zabıta ekipleri artık mağazaların yakınlarındaki kameralardan alınan görüntüleri izleme yetkisine sahiptir. Ayrıca toplu taşıma güvenliğini artırmak amacıyla Paris'te faaliyet gösteren RATP (*Régie autonome des transports parisiens)* ve Fransa genelinde demiryolu taşımacılığı yapan SNCF'nin *(Société nationale des chemins de fer français)* görevlileri de halka açık yolların video gözetim sistemlerine erişebilecektir. Yeni düzenlemelerle, polis ve jandarmanın kullanımı için tasarlanmış yaka kameralarının görüntüleri, belirli güvenlik riski taşıyan durumlarla karşılaşıldığında hem merkezi komuta noktalarına hem de olay yerindeki yetkililere canlı olarak iletilebilecektir.

7. 2024 Olimpiyat ve Paralimpik Oyunlarına İlişkin Kanun ve Fransız Anayasa Konseyi Kararı

2024 Olimpiyat ve Paralimpik Oyunlarına ilişkin oldukça tartışma yaratan kanun tasarısının Fransız Anayasa Konseyi'nin kararı ile uygun bulunmasından, ayrı bir başlık altında bahsetmek faydalı olacaktır. İlk olarak 22 Aralık 2022'de Fransız Senatosuna sunulan ve ilk yardımda bakım, doping ile mücadele ve güvenlik konularını içeren tasarı Anayasa Konseyi'nin de uyum kararından sonra 9 Mayıs 2023'te yayımlanmıştır[86]. Bahis konusu Kanunun 10. maddesinde 31 Mart 2025 tarihine kadar ciddi saldırı riskine maruz kalan spor, eğlence veya kültür etkinliklerinin güvenliğinin sağlanması amacıyla, İç Güvenlik Kanunu'nun L. 252-1 maddesi uyarınca izin verilen video koruma sistemlerinin maddede belirtilen (belirli etkinliklerin düzenlendiği yerlerde ve çevresinde, toplu taşıma araçlarında ve bunlara hizmet veren yollarda) halka açık alanlarda deneysel olarak

---

85 CNIL, "Directive « Police-Justice » : de quoi parle-t-on?", <https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t >

86 Sénat, "Projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions",<https://www.senat.fr/travaux-parlementaires/textes-legislatifs/la-loi-en-clair/projet-de-loi-jeux-olympiques-et-paralympiques-de-2024.html >

algoritmik işlem (*traitements algorithmiques*) yapabileceği hususları yer almaktadır[87]. Kamera sistemleri aynı zamanda hava araçlarına da monte edilebilecektir. Bu gerçek zamanlı algoritmik işlemenin amacı, ortaya çıkarması muhtemel riskli olayları tespit etmek ve bunları polis, jandarma gibi güvenlik görevlilerine rapor etmek olarak belirtilmiştir.

Yine maddenin kapsamında GDPR ve sair kişisel verilerin korunması düzenlemelerine bağlı olunduğu, algoritmik işleme yapılan video gözetim faaliyetlerinde herhangi bir biyometrik tanımlama (yüz tanıma tekniği kullanılarak) yapılmayacağı dolayısıyla biyometrik veri işlenmeyeceği, münhasıran olay bazında hareket edileceği, GDPR'ın 35. maddesinde belirtilen veri koruma etki değerlendirmesinin yapılacağı yer alır.

Anayasa Komisyonu ise algoritmik işleme ile elde edilen görüntülerin, terör eylemleri, kişilerin güvenliğine ciddi zarar verme riskleri taşıyan veya ortaya çıkacağı önceden belirlenebilen olayları gerçek zamanlı olarak tespit etmek ve bildirmek amacıyla elde edileceğini, kamusal düzeni koruma hedefine yönelik anayasal değerler ile 1789 Beyannamesi'nin 2. maddesiyle korunan özel hayata saygı hakkı arasında denge kurma görevinin yasamada olduğunu, kamusal düzeni koruma hedefine yönelik anayasal değeri karşılamak için kanun koyucunun eleştiri konusu olan maddede belirtilen "görüntülerin algoritmik işleme tabi tutulması" faaliyetine izin verme yetkisine sahip olduğunu belirtmiştir[88]. Komisyon algoritmik gözetimde görüntülerin sistemli ve otomatik bir analizinin gerçekleştirileceğini ve bu sayede elde edilebilecek bilgilerin sayısının ve hassasiyetinin önemli ölçüde artacağının kabulüyle, bu tür gözetim sistemlerinin uygulanmasında özel hayatı koruyacak özel güvencelerin sağlanması gerektiğini de eklemiştir[89].

---

[87] République Française, LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1), <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974 >

[88] Conseil Constitutionnel, "Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions",<https://www.conseil-constitutionnel.fr/actualites/loi-relative-aux-jeux-olympiques-et-paralympiques-de-2024-et-portant-diverses-autres-dispositions >

[89] Ibid.

CCTV'lerin yapay zekâya dayalı algoritmik gözetim yapması, klasik CCTV sistemlerine kıyasla depolama ve iletim bant genişliği, insan kaynağının azaltılması gibi avantajlar sağlar[90]. Bunun yanında bu akıllı gözetim sistemleriyle hemen hemen hiç insan müdahalesi olmadan geniş çaplı izleme, otomatik algılama, belirli nesne veya kişinin izlenmesi, elde edilen görüntüler üzerinde daha fazla analiz yapabilmek mümkündür[91]. Bu sayede -özellikle yapay zekâ kullanan kameraların uçabilen nesnelerde de eklenmesiyle- çok daha geniş alanlar kameralarca izlenmiş olacak, daha fazla video veya görüntü kaydedilebilecek, anormal davranışlar ya da nesneler kolayca tespit edilebilecektir. Bunun anlamı doğal olarak çok daha fazla miktarda kişisel verinin işlenmesidir.

Anayasa Komisyonu kararında da belirtildiği üzere konu hakkındaki hükümler yalnızca kişisel verilerin korunması hakkındaki düzenlemeleri değil özellikle serbest dolaşım hakkı, protesto hakkı, düşünce özgürlüğü ve özel hayata saygı hakkı gibi temel sözleşmeler ile korunan hakları ihlal ettikleri gerekçesiyle milletvekilleri tarafından da yoğun şekilde eleştirilmiş, algoritma işlemlerinin yeterli güvencelerle sınırlanmadığı, hükümlerin uygulama alanının sadece olimpiyat ve paralimpik oyunları ile ilgili etkinliklerle sınırlı olmadığı ve belirli olayların tespitinde biyometrik verilerin işlenmesini zorunlu kılacağı belirtilmiştir[92].

C. Eleştirel Değerlendirme

Fransa'da halka açık alanlardaki video gözetim uygulamaları oldukça yaygındır ve genellikle kamu güvenliğini esas almaktadır. Bu nedenle GDPR dışındaki durumlarda uygulanması için kişisel verileri koruyan ulusal hukuki düzenlemeler getirilmiştir. Ülkede veri koruma otoritesi olan CNIL, Ulusal Video Koruma Komisyonu ve konuya özgü kamu kurumları aracılığıyla çok yönlü bir denetim mekanizması oluşturulmuştur. Bu yapı, GDPR'ın kapsamadığı video gözetim faaliyetlerinin de denetlenmesini

---

90 Minh T. NGUYEN vd. "Artificial intelligence based data processing algorithm for video surveillance to empower industry 3.5" (2020) Computers & Industrial Engineering 148 106671, 1.

91 Ibid 2.

92 Conseil constitutionnel, "Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions".

sağlamaktadır. Özellikle video gözetim sistemleri için emniyet birimlerince alınan sistem kurulum kararlarının bu konuda yetkili devlet departmanının onayına tabi tutulması ve faaliyetlerin CNIL ile Ulusal Video Gözetim Komisyonu tarafından ayrıca denetlenmesi, kapsamlı ve işlevsel bir düzenlemeler bütünlüğü oluşturur.

Bununla birlikte Özgürlükleri Koruyan Küresel Güvenlik Kanunu video gözetim konusunda ciddi eleştirilere sebebiyet verir. Anayasa Konseyi ilgili Kanuna ilişkin belediyelere bağlı zabıta gibi yetkililerin belirlenen bölgelerin dışındaki video kayıtlarına erişmesini kişisel verilerin korunması yönünden sakıncalı bulmuştur[93]. Güvenlik otoritelerine sağlanan geniş yetkiler, teknolojik olarak gelişmiş gözetim araçlarının kullanılması ve polisin yanı sıra ulaşım otoriteleri *(RATP, SNCF)* gibi farklı aktörlerin de gözetim yetkisi alması, bireysel mahremiyetin hukuki açıdan da risk altında olduğu anlamına gelebilir. Bu nedenle, bu tür gözetim faaliyetlerinde iç denetimin önemli bir rolü vardır.

Fransa'da yüksek seviyede kamera gözetimi olmasına karşın, bu konuda yeterli akademik çalışmanın yapılmadığı da ifade edilir[94]. Video gözetim, güvenlik, kamu otoritelerince CCTV kullanımı, video gözetimin suç işlenmesine etkileri konularında çalışmaları bulunan Eric Heilmann[95] 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 gitgide artan CCTV kullanımı ile İçişleri Bakanlığı'nın ulusal bir strateji dahilinde hareket etmeye başladığını belirtir[96]. Ayrıca ülkede CCTV kameralarının yerleştirilmesi konusunda merkezi hükümet ile yerel yönetimler arasında bir tür çekişme yaşandığı, devletin kamera sayısını artırmayı arzularken kamera kurulumu konusunda belirli

---

93 Vie Publique, "Loi du 25 mai 2021 pour une sécurité globale préservant les libertés".

94 Francisco R Klauser, "Lost Surveillance Studies: A Critical Review of French Work on CCTV" (2009) 6(1) Surveillance & Society , 23.

95 Bahis konusu edilen çalışmalara ulaşmak için bkz. Université de Bourgogne, CIMEOS (Eric Heılmann) <https://cimeos.u-bourgogne.fr/3-equipes/enseignants-chercheurs/96-eric-heilmann.html >

96 Eric Heılmann, "Video Surveillance and Security Policy in France: From Regulation to Widespread Acceptance" (2011) 16 Information Polity , 9.

yetkileri olan yerel birimlerin (özellikle belediyeler) bu yöndeki taleplere karşı çıktığı ifade edilmektedir[97].

19 Temmuz 2022 tarihinde CNIL, halka açık alanlarda kullanılan akıllı ya da arttırılmış kameralara *(caméras augmentées)* dair bir doküman yayınlamıştır. Dokümanda, bu tür kameraların sadece insanları görsel olarak kaydetmekle kalmayıp otomatik analizler de yapmayı hedeflediği, kameraların kişilerin kıyafetleri, maskeleri gibi özel özelliklerini de ön plana çıkardığı belirtilmiştir[98]. Bu tür kameralar doğaları gereği müdahaleci olduklarından, bunların kontrolsüz şekilde yaygınlaşmaları, halka açık alanlarda bireylerin davranışlarını olumsuz etkileyebilecek riskli bir gözetim oluşturabilecektir.

Halka açık alanlarda akıllı kameraların kullanımına ilişkin olarak CNIL'in "meşruiyet" ve "adillik" kavramları arasında bir ayrıma gittiği göze çarpar. Kamera kullanımının meşru olması, onun aynı zamanda adil ve orantılı olacağı anlamına gelmemektedir. CNIL, bu tür teknolojilerin insanların "puanlanması" gibi etik olmayan uygulamalarda kullanılmaması için net sınırlar çizilmesi gerektiğini vurgulayarak Fransız kanunlarının mevcut CCTV kameralarını suç tespiti ve kovuşturulması amacıyla kullanılmasına cevaz verdiğini fakat bunun akıllı kameraların kamu otoriteleri tarafından ölçüsüzce kullanılması için sebep oluşturmadığını belirtir[99].

CNIL'in konu hakkında yayınladığı doküman, akıllı kameraların kullanımı konusunda ciddi etik ve yasal düşünceleri gündeme getirmekte bireylerin hak ve menfaatlerinin korunmasını esas alarak, bu tür teknolojilerin kullanımının özenli bir şekilde yetkilendirilmesi ve denetlenmesi gerektiğini vurgulamaktadır[100]. Asıl endişe

---

97 Ibid 369.

98 CNIL, "Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position"

CNIL'in bu pozisyonuna rağmen 2024'te Paris'te yapılacak olimpiyatlar için Fransız senatosunun büyük çoğunluğu tarafından olumlu oy verilmesi hk. Kayalı, Laura, "French Senate backs AI-powered video surveillance for Paris 2024 Olympics" (31 January 2023) Politico <https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/french-senators-back-ai-powered-video-surveillance-for-paris-2024-olympics/amp/ >

99 Ibid.

100 CNIL, "Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position"' (19.07.2022)<https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position >

kaynağı ise bu tür kameraların biyometrik veri toplaması ve yapay zekâ destekli olması, yanlış uygulamalar söz konusu olduğunda Çin'deki gibi, vatandaşların "skorlanması" şeklinde totaliter uygulamalara yol açabilecek potansiyeli barındırmasıdır. CNIL, teknolojinin hızla geliştiği bu dönemde, hukuki ve etik normların bu gelişmelerle uyumlu hale getirilmesi gerektiğini savunmaktadır. Yapay zekâ kullanabilen kameralar karşısında kişisel verilerin korunması CNIL'in 2022-2024 stratejik planının bir parçası olarak da öne çıkmaktadır[101].

Avrupa Parlamentosu tarafından kabul edilen ve yürürlüğe girmesi beklenen, üye devletlerin yapay zekâ sistemlerini kullanmasına sınırlar getiren AB Yapay Zekâ Tüzüğü Taslağı'nın 38 numaralı gerekçe paragrafında yapay zekâ sistemlerinin kolluk tarafından kullanmasının bir güç dengesizliğine sebep olabileceği, temel haklar üzerinde olumsuz etkiler doğurabileceği, bu sistemler açıklanabilir (*explainable artificial intelligence-XAI*[102]) olmadıkça masumiyet karinesi, savunma ve adil yargılanma hakkı gibi önemli temel hakların kullanımını engelleyebileceği belirtilir[103].

Teknolojik gelişmelerin pek çok ülkede olduğu gibi Fransa'da da video gözetim cihazlarının sayısının artmasına sebep olduğu aşikardır. Kamu otoritelerince CCTV kullanımı, teknolojik gelişmelerin yanında politik değişimlerden de etkilenen bir güvenlik stratejisi ekseninde sağlanmaktadır. Fransa'da 2007 yılına kadar özellikle banliyöler gibi kentsel yerler ile şehir merkezlerinde yoğunlukla kullanılan CCTV'nin, 2007 yılından sonra her koşulda ve her yerde, güvenlik sağlanması için kullanılması gereken bir araç

Kişisel verilerin elde edilme sebebi olarak dayanak oluşturabilen istatistik elde etme konusunda, istatistiklerin anonim veriler üzerinden üretilmesi gibi alternatif çözüm yollarına başvurulması önerilmektedir.

[101] CNIL, "Plan Stratégique 2022-2024" <https://www.cnil.fr/sites/default/files/atoms/files/cnil_plan_strategique_2022-24.pdf >

[102] Yapay zekânın algoritmik işleyişinde opaklık, kara kutu (black box), ön yargılı veya yanlış (kurgusal) sonuçlar üretme gibi sorunların aşılması için ortaya konan ve kısaca yapay zekâ modellerinin işleyişinin analiz edilebilmesini hedefleyen "açıklanabilir yapay zekâ" konseptinin kendisinin de tartışmalı olduğu belirtilmelidir. Konu hakkındaki eleştirel bir çalışma için bkz. Kiana Alikhademi vd. "Can Explainable AI Explain Unfairness? A Framework for Evaluating Explainable AI" (2021) *ArXiv*. /abs/2106.07483

[103] Proposal for a Regulation Of The European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legıslative Acts,

olarak görülmeye başlanması[104] yalnızca video gözetimin değil genel olarak gözetim konusunun güvenlik-özgürlük ikileminin bir tezahürüdür.

SONUÇ

Halka açık alanlarda video gözetime 1970'lerden başlayarak artan yönelim, 11 Eylül saldırılarından sonra farklı bir dönemece girmiştir. Kamu otoriteleri asayiş sağlamak, hızlı müdahale kabiliyeti geliştirmek, suç işlenmesine yönelik caydırıcılık oluşturmak, suçlu takibi yapmak gibi kısaca "güvenlik" çatısı altında ele alınabilecek amaçlarla kameralı gözetime yaygın şekilde başvurmaktadır. Güvenlik sağlama amaçlarının yanında konunun gözetim kapitalizmi, halka açık alanların dönüşümü, sosyal kontrol sağlama gibi çeşitli boyutları da gözetimin amaçları konusuna eklemlendirilerek tartışılmaktadır.

Bireylerin halka açık alanlarda bulunmasının, özel hayatı ve kişisel verilerin korunmasını isteme hakkını ortaya koymayı engellemediği, sistemli ve sürekli izlemeler ile kameralarca elde edilen görüntülerin kaydedilmesi sonuçları ortaya çıkan faaliyetler bakımından kabul edilmektedir. Dolayısıyla bu tür durumlarda kişisel verilerin korunması hukuku devreye girecek, özellikle ölçülülük, veri kalitesi, veri minimizasyonu, belirli, açık ve meşru bir amaç ile izleme yapılması, kişisel verilerin kayıt altında tutulacağı sürenin kayıt amacı doğrultusunda sınırlanması gibi çeşitli temel ilkelere uyulması beklenecektir. GDPR kapsamındaki istisna ve kısıtlamalar çerçevesinde yapılacak izlemeler bakımından da olay ile örtüştüğü sürece bu temel ilkelere riayet edilmesi, her bir somut durumda güvenlik-özgürlük dengesinin kurulması, CCTV kullanımının ölçülü ve sınırlı olması gerekir.

Video gözetim karşısında kişisel verilerin hem ulusal hem de AB ve Avrupa Komisyonu düzenlemeleriyle korunduğu Fransa'da, konu ile ilgili bir taraftan GDPR, Polis ve Ceza Adaleti Direktifi, EDPB ve EDPS'nin düzenlemeleri gibi genel nitelikli mevzuat, diğer taraftan başta 78-17 sayılı Fransız Veri Koruma Kanunu ve İç Güvenlik Kanunu başta olmak üzere ulusal mevzuat bulunur. Bununla birlikte ülkede özellikle yaka

[104] Ibid 1-2.

kameralarının yaygın kullanımı, yapay zekâ kullanabilen kameralara yönelik kaygılar, genel olarak CCTV'lerin yoğun kullanımları gibi konular kişisel verilerin korunmasını isteme hakkına ve dolayısıyla özel hayatın gizliliğine bir müdahale olarak eleştirilmektedir. Nitekim video gözetim yönünden hukuki meşruiyetin sağlanması, yapılan izlemeleri kişisel verilerin korunması yönünden hukuka uygun hale getirmeyecek, hukuk güvenliği sağlanmış olmayacaktır.

Şiddet eylemlerinin kontrolü, suçlu ve suç takibi, toplumsal olayları gözleme gibi ihtiyaçların giderilmesi için eski CCTV'lere nazaran daha ucuz ve gelişmiş olan video kamera sistemleri birer destek aracı olarak kullanılmaktadır. Diğer taraftan kişisel verilerin korunması düzenlemelerine uyulması gerekliliği etkin bir denge kurulmasını elzem kılar. Fransa örneğinde görüldüğü üzere, yeni teknolojik gelişmelerin etkisiyle ortaya çıkan daha gelişmiş, yapay zekâ kullanabilen kameraların halka açık alanlarda kullanımı, kişisel veriler yönünden yepyeni hukuki ve etik güçlükler yaratmaya başlamıştır. Teknolojik ve teknik gelişmeler karşısında konu hakkındaki hukuki düzenlemeler de sık sık gözden geçirilmek, güncellenmek durumundadır. Ancak salt hukuki düzenlemelerin bulunması ve güncel olması da video gözetim ve kişisel verilerin korunması dengesinin sağlanması için yeterli olmayacaktır. Bunun yanında toplumsal farkındalık, kamu otoritelerinin mevzuat ile uyumlu hale getirilmesi, kişisel verilerin korunmaması durumlarının potansiyel etkilerinin tüm aktörlerce anlaşılması gibi çok boyutlu bir veri koruma anlayışı geliştirilmelidir.

Fransa'da video gözetime yönelik var olan ulusal-bölgesel mevzuat ve ülkedeki uygulama birlikte ele alındığında, kişisel verilerin korunması perspektifinden güvenlik sebeplerinin oldukça geniş yorumlandığı, hukuki düzenlemelerin ötesinde bir CCTV kullanımı olduğu, yapay zekâ kullanabilen kameraların halka açık alanlarda geniş çapta kullanımının bireysel özgürlükler yönünden endişe verici olduğu ifade edilmelidir. Nitekim algoritmik işleyişin sebep olması ihtimal dahilinde olan ön yargılı veya yanlış (kurgusal) sonuçlar verme gibi henüz çözüm getirilememiş problemler, kameralarla elde edilen görüntüler diğer deyişle kişisel veriler söz konusu olduğunda daha kritik bir hale gelmektedir.

KAYNAKÇA

Akınlar C, "Kapalı Devre Görüntü ve Kayıt Sistemleri", Yusuf Oysal (ed.), Güvenlik Sistemleri (1. Baskı, Anadolu Üniversitesi Yayınları, Eskişehir 2012).

Baskın O, *Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması* (Seçkin Yayıncılık, Ankara 2021)

Bétin C and Martınaıs E, "Sécurité, vidéosurveillance et construction de la déviance : l'exemple du centre-ville de Lyon" (2003) 27(1) Déviance et Société (3) 3-24.

Bostancı Bozbayındır G, "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" (2018) Galatasaray Üniversitesi Hukuk Fakültesi Dergisi (51) 51-103.

Ceccato V and Nalla M (eds), *Crime and Fear in Public Places: Towards Safe, Inclusive and Sustainable Cities* (1st edn, Routledge, London 2020).

Çapar S, Birleşik Krallıkta CCTV, *Türkiye'de Mobese Caddelerde Güvenlik Nöbetindeki Kameralar* (Turhan Kitabevi Yayınları, Ankara 2011).

Dıamond B, "Safe Speech: Public Space as a Medium of Democracy" (2010) Journal of Architectural Education.

Dolgun U, *Şeffaf Hapishane yahut Gözetim Toplumu: Küreselleşen Dünyada Gözetim, Toplumsal Denetim ve İktidar İlişkileri* (3rd edn, Ötüken Neşriyat, İstanbul 2015).

Doyle A, Lippert R K and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge, London and New York 2012).

Goold B, Loader I and others, "The Banality of Security: The Curious Case of Surveillance Cameras" (2013) 53(6) British Journal of Criminology 977-996.

Hatipoğlu Aydın D, *Siber Alan ve Hukuk* (On İki Levha Yayıncılık, İstanbul 2022).

Heilmann E, "Video Surveillance and Security Policy in France: From Regulation to Widespread Acceptance" (2011) 16 Information Polity 1-9.

İçer Z ve Dönmez E "Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku Ve Ceza Muhakemesi Süreçlerindeki Kullanımı Ve Sınırları" (2021) 15(43) Ceza Hukuku Dergisi 421-461.

Klauser F R, "Lost Surveillance Studies: A Critical Review of French Work on CCTV" (2009) 6(1) Surveillance & Society 23-31.

Küzeci E, *Kişisel Verilerin Korunması* (4. Baskı, On İki Levha Yayıncılık, İstanbul 2021).

Mucchielli L, "À Quoı Sert La Vidéosurveillance De L'espace Public ? Le cas français d'une petite ville «exemplaire »" (2016) 40(1) Deviance et Societe 25-50.

Nguyen M T. vd. "Artificial intelligence based data processing algorithm for video surveillance to empower industry 3.5" (2020) Computers & Industrial Engineering 148 106671 1-15.

Norris C and Armstrong G, *The Maximum Surveillance Society* (Berg, Oxford and New York 1999).

Patton J W, "Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places" (2000) Ethics and Information Technology .

Skogan W G, "The Future of CCTV" (2019) 18(1) Criminology and Public Policy 161-166.

Ufert F, "AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?" (2020) 5(2) European Papers 1094.

Urquhart L and MIRANDA D L, "Policing Faces: The Present and Future of Intelligent Facial Surveillance" (2021) Information and Communications Technology Law (1) 1-26.

Welsh B C and Farrington D P, "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis" (2009) 26(4) Justice Quarterly 716-745.

Faydalanılan İnternet Kaynakları:

Anti-Video Surveillance Collective of France, "Does Video Surveillance Have a Limit? An Open Letter to the Mayors of France" (2004) <http://www.notbored.org/limits-of-surveillance.html >

Bunn N and Cunningham B, "Which Data Should Police Body Cams Collect?" The Atlantic (14 October 2015) <https://www.theatlantic.com/politics/archive/2015/10/which-data-should-police-body-cams-collect/433197/ >

CNIL, "Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position" (19 July 2022) <https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position>

CNIL, "Directive « Police-Justice » : de quoi parle-t-on?" <https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t >

CNIL, "Mises en demeure de plusieurs établissements scolaires pour vidéosurveillance excessive" <https://www.cnil.fr/fr/mises-en-demeure-de-plusieurs-etablissements-scolaires-pour-videosurveillance-excessive >

CNIL, "Plan Stratégique 2022-2024, axe 3, 7"

<https://www.cnil.fr/sites/default/files/atoms/files/cnil_plan_strategique_2022-24.pdf >

CNIL, "Vidéoprotection: quelles sont les dispositions applicables?" <https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables>

Conseil Constitutionnel, "Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions" <https://www.conseil-constitutionnel.fr/actualites/loi-relative-aux-jeux-olympiques-et-paralympiques-de-2024-et-portant-diverses-autres-dispositions>

Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" <https://rm.coe.int/1680078b37 >

Council of Europe, "Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Convention 108 and Protocols" <https://www.coe.int/en/web/data-protection/convention108-and-protocol >

Dascălescu A, "The Controversial Clearview AI Was Used By Florida Man's Lawyer to Clear Him Of Vehicular Homicide Charges" Techthelead <https://techthelead.com/the-

controversial-clearview-ai-was-used-by-florida-mans-lawyer-to-clear-him-of-vehicular-homicide-charges/>

European Center for Not-for-Profit Law, "Civil Society Open Letter On The Proposed French Law On The 2024 Olympic And Paralympic Games" <https://ecnl.org/news/civil-society-open-letter-proposed-french-law-2024-olympic-and-paralympic-games>

Electronic Frontier Foundation, "Automated License Plate Readers (ALPRs)" <https://www.eff.org/cases/automated-license-plate-readers >

Electronic Frontier Foundation, "Street Level Surveillance" <https://www.eff.org/tr/issues/street-level-surveillance >

European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices (Version 2.0) Adopted on 29 January 2020" <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf >

Hare S, "These new rules were meant to protect our privacy: they don't work", The Observer <https://www.theguardian.com/commentisfree/2019/nov/10/these-new-rules-were-meant-to-protect-our-privacy-they-dont-work>

Herbecq and Others v Belgium, App No 32200/96 & 32201/96" (ECHR, 14 January 1998) 97.

<https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-88070&filename=001-88070.pdf >

Hill K, "Wrongfully accused by an algorithm", The Seattle Times <https://www.seattletimes.com/business/technology/wrongfully-accused-by-an-algorithm/>

Kayalı L, "French Senate backs AI-powered video surveillance for Paris 2024 Olympics" (31 January 2023) Politico

<https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/french-senators-back-ai-powered-video-surveillance-for-paris-2024-olympics/amp/ >

Leander v. Sweden, App No 9248/81, (ECHR, 26 March 1987), para. 49-50-51. <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}>

Manancourt V, "Europe's state of mass surveillance", Politico

<https://www.politico.eu/article/data-retention-europe-mass-surveillance/ >

Nişanyan Sözlük, <https://www.nisanyansozluk.com/kelime/g%C3%B6zetim >

Oxford Learner's Dictionaries,

<https://www.oxfordlearnersdictionaries.com/definition/english/security?q=security >

Peck v United Kingdom, App No 44647/98 (ECHR, 28 January 2003), para. 57.

<https://hudoc.echr.coe.int/eng#{%22appno%22:[%2244647/98%22],%22itemid%22:[%22001-60898%22]} >

Peyron J, "Debate swirls as Paris embraces video surveillance", France 24 <https://www.france24.com/en/20120117-debate-swirls-around-paris-new-high-surveillance-system-cameras-cctv-police >

République Française, "Caméras de surveillance sur la voie publique et dans les lieux ouverts au public", <https://www.service-public.fr/particuliers/vosdroits/F2517 >

République Française, LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1),

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974 >

Satakunnan Markkinapörssi Oy And Satamedia Oy V. Finland, App No 931/13" (ECHR, 27 June 2017), para. 131.

<https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175121%22]} >

Sénat, "Projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions", <https://www.senat.fr/travaux-parlementaires/textes-legislatifs/la-loi-en-clair/projet-de-loi-jeux-olympiques-et-paralympiques-de-2024.html >

Surfshark, "Surveillance Cities"< https://surfshark.com/surveillance-cities >

The Brussels Times, "All-out assault on privacy': France is first EU country to legalise AI-driven surveillance", <https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance>

The Local Fr, "Drones and surveillance cameras: France's new security bill explained" <https://www.thelocal.fr/20201120/drones-and-surveillance-cameras-frances-new-security-bill-explained>

Traichuk A, "CCTV and Facial Recognition: Where Do the Two Technologies Overlap", Data Science Central <https://www.datasciencecentral.com/cctv-and-facial-recognition-where-do-the-two-technologies-overlap/>

Türk Dil Kurumu Sözlükleri, "Güncel Türkçe Sözlük" <https://sozluk.gov.tr/> "gözetim"

Vie Publique, "Loi du 25 mai 2021 pour une sécurité globale préservant les libertés" <https://www.vie-publique.fr/loi/277157-loi-pour-une-securite-globale-preservant-les-libertes>

Vukota-Bojić v Switzerland, App No 61838/10 (ECHR, 18 November 2016) , para. 67 &77.

<https://hudoc.echr.coe.int/eng#{%22appno%22:[%2261838/10%22],%22itemid%22:[%22001-167490%22]}>

Wahl T, "EDPB: Data Protection Guidelines on Video Surveillance", Eucrim <https://eucrim.eu/news/edpb-data-protection-guidelines-video-surveillance/>