Bölüm 13
Chapter 13

Akıllı Video Gözetiminin Temel Hak ve Özgürlükler Bağlamında Değerlendirilmesi: KGYS'den Vücut Kameralarına

Evaluation of Smart Video Surveillance in the Context of Fundamental Rights and Freedoms: From CCTV to Body Cameras

Buket Abanoz Öztürk [1]

[1] İstanbul Ticaret Üniversitesi, Hukuk Fakültesi, İstanbul, Türkiye

Öz

Bu çalışmada, Türkiye'de suçun önlenmesi amacıyla kullanılan akıllı video gözetimi temel hak ve özgürlükler bağlamında incelenmektedir. Suçla mücadelede kameraların kullanılmasına, Mobil Elektronik Sistem Entegrasyonu (MOBESE) adı altında 2000'li yılların başında İstanbul başta olmak üzere pek çok şehirde meydanlar, caddeler, parklar, metrolar ve toplu taşıma araçları gibi kamusal alanların yedi gün yirmi dört saat izlenmesiyle başlanmıştır. İlerleyen süreçte MOBESE, Kent Güvenlik Yönetim Sistemi (KGYS) adını almış ve Plaka Tanıma Sistemleri (PTS) ile entegre edilmiştir. Böylece kamera üzerinden alınan araç fotoğrafları ve plaka karakterleri tanımlaması, istenildiğinde plakası okunan araçların plaka bilgileri ve fotoğrafları ile beraber sorgulanması ve alarm üretilmesi sağlanabilmiştir. 2019 yılından itibaren de İstanbul'da trafik polisleri vücut kameralarını test etmektedir ve 2025 yılından itibaren tüm polislerin yüz tanıma teknolojisi ile entegre olan vücut kameralarıyla donatılması planlanmaktadır. Yüz ve iris taraması yapabilen vücut kameraları ile dar alanda biyometrik veriler toplanarak merkezi sunuculara aktarılmaktadır. Dolayısıyla tüm bu araçların sensörleri aracılığıyla çevrelerindeki neredeyse tüm nesnelere ilişkin çok sayıda veri topladığı ve birbirlerine entegre olduğu akıllı video gözetim sistemi karşımızdadır. Akıllı video gözetimi suçun önlenmesinde etkili bir araç olabilir. Fakat bireylerin temel hak ve özgürlükleri bağlamında ciddi endişeleri beraberinde getirmektedir. Bu nedenle akıllı video gözetiminin hukuki ve etik standartlarının oluşturulması ve bu kurallara uyulması büyük önem taşımaktadır. Çalışmada, Türkiye'de akıllı video gözetiminin gelişimi ve bu kameraların kullanımına izin vermek için hukuki şartların neler olduğu incelenmektedir. Ülkemizdeki kamera sistemlerinin ve yapay zekâ destekli modern önleyici polislik uygulamalarının hukuki alt yapısındaki eksiklikler ele alınırken, Almanya'daki video gözetim düzenlemeleri de incelenecek ve bu düzenlemelerin Türkiye için yol gösterici olup olamayacakları değerlendirilecektir.

Abstract

The aim of this study is to evaluate the smart surveillance used to prevent crime in Türkiye from the perspective of fundamental rights and freedoms. With the City Security and Management System (KGYS), public spaces such as squares, streets, parks, subways and public transportation vehicles in many cities, especially in Istanbul, have been monitored 24 hours a day, seven days a week, for about 20 years. In the future, the cameras were integrated with the License Plate Recognition System (PTS). In this way, it is possible to identify vehicle photos and license plate characters taken via the camera, to query the vehicles whose license plates are read, together with their license plate information and photos, and to generate alarms. Traffic police in Istanbul have been testing body cameras since 2019, and it is planned that all police officers will be equipped with body cameras integrated with facial recognition technology as of 2025. Biometric data is collected in narrow areas with body cameras that can scan faces and irises and transferred to central servers. Therefore, we have smart camera systems where all these vehicles collect a lot of data about almost all objects in their environment through their sensors and integrate with each other. Camera

Abanoz Öztürk, B. (2025). Evaluation of smart video surveillance in the context of fundamental rights and freedoms: from CCTV to body cameras. in Esen, A., Yayla, M., Ayhan, U., Arslan, A. C. & Erbaş, B. (Eds.), *Metropol ve Güvenlik: İnsan Hakları ve Sivil Toplum Perspektifi* (p. 152-176). İstanbul University Press. https://doi.org/10.26650/B/SSc6SSc14SSc24.2025.007.13

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License.

© 2025. Abanoz Öztürk, B.

Buket Abanoz Öztürk baozturk@ticaret.edu.tr

images, license plate numbers and data from the facial recognition system provide important information to the police in preventing crime. On the other hand, it also brings with it serious concerns in terms of the right to privacy of individuals and the right to protection of personal data. Therefore, it is of great importance to establish legal and ethical standards for video surveillance and to comply with these rules. The study examines the development of smart camera systems in Türkiye and the legal conditions for permitting the use of these cameras. While addressing the deficiencies in the legal infrastructure of camera systems and AI-supported modern preventive policing practices in our country, video surveillance regulations in Germany will also be examined and whether these regulations can be a guide for Türkiye will be evaluated.

Anahtar Kelimeler Kamerali Gözetim · Vücut Kamerasi · Yüz Tanima Teknolojisi · Özel Hayat · Kişisel Veri · Türkiye

Keywords Smart Surveillance · Body Cam · CCTV · Facial Recignition System · Privacy · Personal Data · Türkiye

Extended Summary

The importance of camera systems in combating crime is increasing day by day with the advancement of technology. Following the terrorist attacks on September 11, 2001, the use of cameras in the field of security in the United States has gained an important place. In addition to transportation centers such as airports, subways, and train stations, streets, squares, and parks are also monitored and recorded with cameras, and these records are stored. The use of cameras quickly spread to European countries such as England, Germany, France, and Italy, as well as to densely populated countries such as China and India. Today, China and England are referred to as surveillance society due to the large number of cameras they use compared to their populations. Since the early 2010s, the scope and function of security cameras such as unmanned aerial vehicles (UAVs), drones, and body cameras, which have become widespread in America, China, Russia, and some European countries, have been greatly expanded.

In Türkiye, the use of cameras in the fight against crime began in the early 2000s with the monitoring of public areas such as squares, streets, parks, subways and public transportation vehicles 24/7 in many cities, especially in Istanbul. In the following process, MOBESE was renamed as the Urban Security Management System (KGYS) and integrated with License Plate Recognition Systems (PTS). Thus, vehicle photographs and license plate characters taken from the camera can be identified and alarms can be generated by querying the license plate information and photographs of vehicles whose license plates are read. Since 2019, traffic police have been testing body cameras as part of a pilot project in Istanbul. It is planned that all police officers will be equipped with body cameras starting in 2025. Biometric data is collected in narrow areas with body cameras that can scan faces and irises and transferred to central servers. Police also use drones and unmanned aerial vehicles (UAVs) for crowd control and surveillance, especially at large events and social incidents. Therefore, the scope of video surveillance, which started with the monitoring of public areas such as squares, parks, and public transportation vehicles in order to ensure traffic safety and prevent crime, has expanded considerably with facial recognition technologies, unmanned aerial vehicles, drones, and body cameras. Nowadays, we have AI-supported smart video surveillance, where all these vehicles collect a lot of data about almost all objects in their environment through their sensors and integrate with each other. Smart video surveillance is a type of surveillance that goes beyond traditional surveillance systems and uses advanced technologies and algorithms. Smart surveillance systems integrate data from various sensors (cameras, motion detectors, sound sensors, etc.) and analyze this data to provide more comprehensive surveillance. In doing so, they usually use artificial intelligence (AI), machine learning, big data analytics, and sensor technologies to enable more effective and detailed monitoring. While smart video surveillance is used as an important tool in security and combating crime, it also brings with it important discussions in terms of the fundamental rights and freedoms of individuals.

Every new technology is like a double-edged sword. This wide-scale use of technology also brings with it important discussions in terms of the fundamental rights and freedoms of individuals. For this reason, it is of great importance to establish the legal and ethical standards of video surveillance and to comply with these rules. The study examines the development of smart camera systems in Türkiye and the legal conditions for permitting the use of these cameras. There are deficiencies in the legal infrastructure of camera systems and modern preventive policing practices supported by artificial intelligence in our country. There is no regulation that allows video surveillance in public areas for the purpose of preventing crime. Therefore, cameras used in public areas are against the law. Therefore, a legal regulation that makes the monitoring, recording, storage and

usage of video surveillance systems in Türkiye, including the use of body cameras, clear, specific and auditable should be made. For the legal regulation to be made, the video surveillance regulations in Germany will also be examined and it will be evaluated whether these regulations can be a guide for Türkiye.

1. GİRİŞ

Suçla mücadelede kamera sistemlerinin önemi, teknolojinin ilerlemesiyle birlikte her geçen gün daha da artmaktadır. 11 Eylül 2001'deki terör saldırılarının ardından, Amerika Birleşik Devletleri'nde güvenlik alanında kamera kullanımı önemli bir yer edinmiştir. Havaalanları, metrolar, tren garları gibi ulaşım merkezlerinin yanı sıra caddeler, meydanlar ve parklar da kameralarla izlenmekte, kaydedilmekte ve bu kayıtlar saklanmaktadır. Kamera kullanımı başta İngiltere, Almanya, Fransa, İtalya gibi Avrupa ülkelerine ve Çin, Hindistan gibi nüfusu yoğun ülkelere de kısa sürede yayılmıştır. Günümüzde, Çin ve İngiltere nüfuslarına oranla kullandıkları kamera sayısının fazlalığı nedeniyle gözetim toplumu (surveillance society) olarak anılmaktadır. Araştırmalara göre, Londra'da bir kişi günde ortalama 300 kez kapalı devre televizyon kameraları[1] tarafından kaydedilmektedir (Associated Press, 2007). Çin'in Tajuan şehrinde ise her bin kişiye 120 kamera düşmektedir (Aktan, 2024).

2010'lu yılların başlarından itibaren, Amerika, Çin, Rusya ve bazı Avrupa ülkelerinde yaygınlaşmaya başlayan yüz tanıma teknolojileri, insansız hava araçları (İHA'lar), dronlar, vücut kameraları gibi araçlarla video gözetiminin kapsamı ve işlevi oldukça genişletilmiştir. Günümüzde, sensörleri aracılığıyla çevrelerindeki neredeyse tüm nesneler hakkında büyük miktarda veri toplayan ve birbirine entegre olan yapay zekâ destekli *akıllı video gözetimi* karşımıza çıkmaktadır. Akıllı video gözetimi, geleneksel gözetim sistemlerinin ötesine geçen, gelişmiş teknolojiler ve algoritmalar kullanarak yapılan gözetim türüdür. Akıllı gözetim sistemleri, çeşitli sensörlerden gelen verileri (kameralar, hareket dedektörleri, ses sensörleri vb.) entegre eder ve bu verileri analiz ederek daha kapsamlı bir gözetim sağlar (Wood, 2021, s. 150). Bunu yaparken genellikle yapay zekâ (YZ), makine öğrenimi, büyük veri analitiği ve sensör teknolojileri kullanarak daha etkin ve detaylı bir izlemeyi mümkün kılar. Akıllı video gözetimi güvenlik ve suçla mücadelede önemli bir araç olarak kullanılırken, aynı zamanda bireylerin temel hak ve özgürlükleri bakımından önemli tartışmaları da beraberinde getirmektedir[2].

Kameralı gözetim sistemlerinin arka planında suç işlendikten sonra değil, suç henüz işlenmeden önce etkin tedbirlerin alınması gerekliliği ve önleyici ceza hukuku anlayışı yatar. Suçları işlenmeden önleyebilmek amacıyla başvurulan önleyici polis tedbirleri de bunun bir görünümüdür. Önleyici bu yaklaşımda, suç işleme potansiyeli olan, suç işlemeye yönelik hazırlık hareketlerini gerçekleştiren veya suç işleyeceği yönünde ihbar ya da istihbari bilgi gelen kişilerin tespit edilebilmesi hedeflenir (İçer, Dönmez, 2020, s. 447). Ön alan soruşturmaları ile polise gelecekteki tehlikeleri önleyebilmek amacıyla birtakım yetkiler verilmekte ve bireylerin temel hak ve özgürlüklerine yönelik müdahalenin sınırları genişletilmektedir (Abanoz, 2018). Bu kapsamda suçla mücadelede güvenliğin sağlanması ve suçun önlenmesi gibi makro konuların yanı sıra, topluma uyum ve toplum içerisinde nasıl davranıldığı gibi bireyler nezdinde mikro analizlere de odaklanılmıştır (Töngür ve diğerleri, 2022, s. 40) Böylece suç

[1] Closed Circuit Television veya CCTV olarak bilinen kapalı devre kamera sisteminin ilk kez Almanya'da, Nazi ordusu için geliştirilen V2 roketlerinin gelişim sürecini kontrol etmek ve olası teknik sorunları saptamak amacıyla kullanıldığı ifade edilmektedir. Suçla mücadelede ise ilk kez özel sektörde İngiltere'de bir perakendede ve Amerika'da bir bankada kullanılmıştır (Yıldırım, 2013: 11).

[2] 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 2024'te kabul edilen Yapay Zekâ Tüzüğü'ne açıkça aykırı olduğu belirtilmektedir. (European Center for Not-for-Profit Law, 2024).

davranışı dış dünyaya yansıtılmadan, kişilere müdahale etmek ve gelecekte yol açacakları tehlike ve zararları bugünden önleyebilmek amaçlanmıştır. Bu amaç giderek yaygınlaşmış, suçun işlenmesini önlenemek ceza hukukunun kutsal amacı haline gelmiştir (Keçelioğlu, 2015)

Belirtilen bu süreç, suçun önlenmesinde akıllı video gözetimini kritik bir konuma getirmiştir. Teknolojik gelişmeler, suçla mücadelede önemli araçlar sağlamakla birlikte, bu araçların sınırsız ve koşulsuz kullanılması hukuka aykırı olacaktır. Gerçekten de önleyici polis tedbirleri, ceza muhakesinde koruma tedbirleri ile idari tedbirler arasında gri bir alan oluşturarak bireylerin temel hak ve özgürlüklerine müdahale etmektedir (İçer, Dönmez, 2020, s. 435). Bu nedenle, yapısı itibariyle önleyici tedbir yönü baskın olan kamusal alanda kamera kullanımının hukuki koşullarını belirleyerek sınırlandırmak, hukuk devletinin de bir gereğidir. Birçok ülkede kameralı gözetim sistemlerinin şeffaflığı, hesap verilebilirliği, kurulum amacına hizmet etmesi, ölçülü olması ve özgürlükleri ihlale yönelmemesini sağlamak amacıyla önemli yasal düzenlemeler yapılmıştır. Bu bağlamda çalışmada, Türkiye'de suçun önlenmesinde kullanılan kamera sistemlerinin nerelerde kullanıldığı, bu kameraların kullanımına izin vermek için hukuki şartların neler olduğu ve bireylerin temel hak ve özgürlüklerinin korunması için kamera kullanımında karşımıza çıkan hukuki zorluklar ele alınacaktır. Türkiye'de kamera sistemlerinin hukuki alt yapısında eksiklikler söz konusudur. Fakat Almanya'da kamuya açık alanlarda video gözetimi için çeşitli düzenlemeler bulunmaktadır. Bu düzenlemeler, temel olarak Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz, BDSG), Avrupa Birliği Genel Veri Koruma Tüzüğü (European General Data Regulation, GDPR) ve çeşitli eyalet polis kanunlarıyla belirlenmiştir. Çalışmada bu düzenlemelerin Türkiye için yol gösterici olup olamayacakları değerlendirilecektir.

2. KAMUSAL ALANDA AKILLI VİDEO GÖZETİMİNİN GELİŞİMİ: KGYS'DEN VÜCUT KAMERALARINA

Suçla mücadelede kameralar, Türkiye'de kamusal alanlarda[3] ilk kez 2001 yılında Diyarbakır'da Mobil Elektronik Sistem Entegrasyonu (MOBESE) kapsamında kullanılmaya başlanmıştır (Çoban, 2005, s. 36). Diyarbakır İl Emniyet Müdürlüğü'nde başlatılan bu system, başlangıçta araç takip ve suç analizi amacıyla kullanılmıştır. Altmış beş ekip üzerinde denenen ve suç oranlarını *yüzde elli* (%50) oranında azalttığı iddia edilen sistemin başarısı, şehirdeki tüm emniyet ekipleri ve araçlarının bulundukları noktaların sayısal harita üzerinde gösterilmesiyle suçluları takip eden ekiplerin haritadan izlenmesine ve suçluların kaçması olası tüm yolların hemen kapatılmasına dayanmaktadır (Temel, 2009, s. 95). Başlangıçta Emniyet Genel Müdürlüğü araçları için tasarlanan ve iletişim altyapısı olarak GPRS teknolojisini kullanan bu sistem, yazılım ve mobil donanım birimlerinden oluşmakta olup coğrafi bilgi sistemleri ile bilgi yönetim sistemlerinin entegrasyonu ile çalışmaktadır. Öncelikle büyük şehirlerin ana caddeleri ve meydanlarında kullanılmaya başlanan sistem, zamanla diğer şehirlere ve şehirlerin giriş-çıkışları ile kritik noktalarına da kurulmuştur.

2005 yılından bu yana da İstanbul'da kameralar ile meydanlar, caddeler, parklar, metrolar ve toplu taşıma araçları gibi kamusal alanlar yedi gün yirmi dört saat izlenmeye başlanmıştır. İlerleyen süreçte MOBESE, Kent Güvenlik Yönetim Sistemi (KGYS) adını almış ve Plaka Tanıma Sistemleri (PTS) ile entegre edilmiştir. Böylece kamera üzerinden alınan araç fotoğrafları ve plaka karakterleri tanımlanabilmekte ve plakası okunan araçların plaka bilgileri ve fotoğrafları sorgulanarak alarm üretilebilmektedir (Emniyet

[3]Jürgen Habermas, kamusal alanı "açıklık" unsuru ile tanımlar. Yazara göre, bir alanın kamusal alan olarak kabul edilebilmesi için söz konusu alanın herkese açık olması gerekir (Torun, 2020: 222). Venedik Komisyonu ise kamusal alanı herkesin her zaman ve her şart altında özgür ve ayrıcalıksız bir şekilde erişilebildiği yerler olarak tanımlamıştır. (Venedik Komisyonu'nun Kamu Görevlileri Tarafından Kamusal Alanlarda Kameralı İzleme ve İnsan Haklarının Korunması Hakkında Görüşü, 23 Mart 2007, s. 4.) Doktrinde kamusal alan kavramı ile konut dışında kalan yerlerin ifade edildiği belirtilmiştir (Öztürk ve diğerleri, 2014: 559). Dolayısıyla görünür konut çatıları, bahçesi, balkonu veya özel bir restoranın arka odası MOBESE kameraları ile denetlenemez.

Genel Müdürlüğü, 2024). Başlangıçta araç takip uygulaması olarak geliştirilen bu sistem, İstanbul Emniyet Müdürlüğü bünyesinde kullanılmaya başladıktan sonra, komuta kontrol merkezi, araç takip sistemi, mobil araç sorgulama sistemi, bölge görüntüleme sistemi ve emniyet müdürlüğü bilgisayar ağı gibi çeşitli alt birimlerle entegre çalışacak şekilde geliştirilmiştir. Dolayısıyla, sistem sadece şehrin kameralarla izlenmesini değil; muhtarlıklardaki otomasyon sistemlerinden, gezici güvenlik ekiplerinin olay yerinde yaptıkları inceleme ve raporların kaydedilmesine kadar geniş bir takip sürecini kapsar hale gelmiştir (Kesin, 2007, s. 67).

2019 yılından itibaren İstanbul'da bir pilot proje kapsamında trafik polisleri vücut kameralarını kullanmaktadır. Bu kameralar, sadece EGM tarafından da değil, aynı zamanda Jandarma Genel Komutanlığına (JGK) bağlı karakol ve trafik birimlerinde, Sahil Güvenlik Komutanlıklarında (SaGK), Belediyelerin Zabıta birimlerinde, Adliye Bakanlığına bağlı Ceza infaz kurumlarında bulunan gardiyanlarda, Kamu ve Özel Güvenlik Birimlerinde de kullanılmaktadır. Yüz ve iris taraması yapabilen vücut kameraları ile dar alanda biyometrik veriler toplanarak merkezi sunuculara aktarılmaktadır. Bu kameraların açılıp kapanması veya durdurulması genellikle kamerayı kullanan yetkilinin takdirine bağlıdır (Nelson, Cunningham, 2015; Turgut Bilgiç, 2023, s. 424). Vücut kameraları genellikle acil bir durumda kayıt alır ve bu esnada kırmızı bir kayıt ışığı yanar (Grünwald, 2015). Bakanlığın yaptığı açıklamada, yüz tanımlama sistemine entegre çalışacak vücut kameralarından gelen görüntülerin komuta merkezinden anbean izlenebileceği ifade edilmiştir.

Yüz tanıma teknolojisinin kamera sistemine entegrasyonu ile birlikte, değişmez nitelikte olan biyometrik verilerin de toplanması mümkün olmuştur. Yüz tanıma teknolojileri, görüntülerdeki yüzleri tanımlama ve karşılaştırma işlemlerini gerçekleştiren yapay zekâ ve makine öğrenmesi sistemleridir. Yüz tanıma teknolojisi genel olarak şu şekilde çalışır: İlk adımda, yüz tanıma sistemi, bir görüntüde yüzleri yüz tespit algoritmaları ile tespit eder. Yüz tespit edildikten sonra, gözler, burun ve ağız gibi yüzün önemli bölgeleri tanımlanır ve hizalanır. Yüzden, yüzün özelliklerini tanımlayan bir dizi veri (veya özellik vektörü) çıkarılır. Bu özellikler, yüzün benzersiz biyometrik özelliklerini temsil eder. Çıkarılan özellikler, veri tabanında kayıtlı yüzlerin özellikleriyle karşılaştırılır. Bu karşılaştırma genellikle mesafe metrikleri (örneğin, euclidean distance) veya benzerlik ölçütleri kullanılarak yapılır (Elmas, 2018, s. 128). Yüzlerin karşılaştırılması sonucunda, en benzer veya en yakın eşleşmeler belirlenir ve bir kimlik tahmini yapılır. Böylece belirli bir bölgede yaşayan çok sayıda insanın yüzünün tanıtıldığı sistem, şüpheli şahısları tespit edebilir ve haklarında yakalama kararı bulunan kişilere rast gelinmesi halinde alarm üretebilir ve polisin olaya müdahale etmesi sağlanabilir (İçer, Dönmez, 2020, s. 423).

Türkiye'de 2024 yılı itibariyle sadece İstanbul'da 10 bin MOBESE kamerası, 20 bin vücut kamerası Emniyet Genel Müdürlüğü tarafından kullanılmaktadır. Polis, özellikle büyük etkinliklerde ve toplumsal olaylarda, kalabalık kontrolü ve gözetim amacıyla dronlar ve İHA'ları da kullanmaktadır. İçişleri Bakanlığı tarafından yapılan açıklamada, bu sayıların yeterli olmadığı, sadece ana arterlerde değil şehrin her yerinde olmak üzere 75 bin güvenlik kamerasının hedeflendiği ve kurumsal firmaların kameralarından gelen görüntülerin de sisteme entegre edileceği ifade edilmiştir. Ayrıca yüz tanıma sistemi ve biyometrik verilerinin kullanılması suretiyle insanların kimliklerinin tespit edilmesi, Polis Bilgi Sistemi (PolNet) üzerinden gerekli güvenlik kontrollerinin yapılması ve gerçekleştirilen tüm işlemlerin kayıt altına alınmasını sağlayan veri tabanı yönetim sistemi bulunmaktadır.

Sonuç olarak, kamusal alanlarda kullanılan kamera sistemi, sadece trafik güvenliğinin sağlanması ve suçun önlenmesi amacıyla meydanlar, parklar, toplu taşıma araçları gibi kamusal alanların izlenmesinden ibaret değildir[4]. Yapısı itibariyle önleyici ceza hukuku aracı olan kamera sistemleri, polisin belirli bir suç kapsamında bireysel bir adli izin olmaksızın pek çok kişisel veriye erişmesini sağlar. Bu veriler

[4] Emniyet Genel Müdürlüğü, TÜBİTAK aracılığıyla Kent Güvenlik Yönetim Sistemlerinden (KGYS) elde edilen video görüntülerinden anlamlı sonuçlar çıkarmaya yarayacak akıllı destek yazılımları geliştirilmesi için 2013 yılında açık çağrıya çıkmıştır. KGYS operaörlerine destek olacak video analiz sisteminin oluşturulması amacıyla çıkılan çağrıda, davranış

kişinin nerede, kiminle ve ne kadar süreyle konuştuğu, ne yaptığı, ne satın aldığı, ne okuduğu ve hatta ne düşündüğü de olabilir. Bunlardan bazıları özel nitelikli sağlık verileri de olabilir. Örneğin, hastalıklar yakın gelecekte termal ışık görüntüsünden, IRIS taramasından veya diğer davranış kalıplarından teşhis edilebilecektir (Conrad, 2017). Herhangi bir suç faaliyeti ile ilgili olmasa bile kamusal alanlar yedi gün yirmi dört saat izlenir ve kaydedilir. Bu yönüyle akıllı kamera sistemleri, koruma tedbirlerinin özellikleriyle bağdaşmaz. Koruma tedbirlerinde genellikle tedbire maruz kalan somut bir şüpheli veya sanık vardır. Fakat gelişmiş akıllı kamera sistemleri, özellikle dronelar gibi uçabilen nesnelerin kullanımı ile çok daha geniş alanları izleyebilir (algoritmik gözetim) ve kamera sistemlerine entegre çalışan yüz tanıma teknolojisi ile bölgedeki insanların kimlik tespiti yapılabilir. Veri tabanında eşleşme olduğunda sistem alarm üretebilir ve uyarıyı alan polis, proaktif bir şekilde olaya müdahale edebilir.

3. AKILLI VİDEO GÖZETİMİNİN TEMEL HAK VE ÖZGÜRLÜKLER BAĞLAMINDA DEĞERLENDİRİLMESİ

Kameralar ile kaydedilen bireylerin görüntüleri, kişisel verileri arasında yer almakta olup onların özel hayatına (AY m. 20) dair bilgileri içerir. Özel hayat kültürden kültüre ve bir hukuk sisteminden diğerine değişkenlik gösterse de global ölçekte asgari bir standart sağlanması gereklidir. Bu noktada, Avrupa İnsan Hakları Mahkemesi (AİHM), Sözleşme'nin 8. maddesi ile alakalı vermiş olduğu içtihatlarla bu standardı oluşturmaya hizmet eden önemli araçlardan biridir (Zafer, 2010, s. 32). AİHM, özel hayatın korunması hakkının kapsamını değerlendirirken, sadece doğrudan özel hayatla ilgili olanları değil, aynı zamanda bu hakkın amacına hizmet eden ve kamuya mal olmuş yansımaları da bu koruma alanına dahil etmektedir. Bu açıdan özel hayat mahremiyet hakkından daha geniştir ve herkesin özgür olarak kişiliğini oluşturmasını ve geliştirmesini sağlayan bir alanı kapsamaktadır (Kilkelly, 2001, s. 16).

Türk Anayasa Mahkemesi de özel hayatın, kişinin fiziksel ve ruhsal bütünlüğünü kapsayan eksiksiz bir tanımı yapılamayacak kadar geniş olduğunu belirterek bir kişinin görüntüsünün kayıt altına alınmasını veya yayınlanmasını özel hayatı ile ilgili olduğunu kabul etmektedir (AYM, Orhan Kayahan Kararı, 22/11/2014). Ayrıca Anayasa Mahkemesi bir kişinin diğer kişilerle etkileşime geçtiği alan, kamuya açık olup olmamasına bakılmaksızın, kişinin "mahremiyet meşru beklentisine"[5] sahip olduğunu gösteren koşulların var olması hâlinde "özel hayat" kapsamına gireceğini belirtmektedir (AYM, Orhan Kayahan Kararı, 22/11/2014, p. 28; P.G. and J.H./Birleşik Krallık, App. No: 44787/98, 25/9/2001, § 56; Peck/Birleşik Krallık, App. No: 44647/98, 28/01/2003, § 57). Kamusal alanda da kişilerin özel hayat alanı olabileceğine dikkat çeken yazarlar, parkta kız arkadaşına sarılan veya plajda güneşlenen bir kimsenin görüntüsünün alınmasından rahatsız olabileceği gibi örneklerle meseleyi somutlaştırmaktadır (Karakehya, 2009, s. 345). Kamuya açık alanlarda bireylerin hareketlerinin ve yaşadıklarının izlenmesi, özel hayatlarına müdahale teşkil etmese de bu bilgilerin düzenli veya kalıcı olarak kaydedilmesi özel hayatla ilgili sorunlara yol açabilir. Yani eğer izleme sistemli bir şekilde yapılıyorsa ve kayıt altına alınıyorsa bireyin özel yaşamına müdahale söz konusu olabilir. Bu nedenle, polis tarafından toplanan dosyalar, müdahaleci veya gizli bir yöntemle toplanmamış olsa bile kişinin özel hayatına dahil bilgileri içermektedir (AİHM, P. G. ve J. H./Birleşik Krallık Kararı, § 57).

Kişinin görüntüsünün yanı sıra yüz tanıma sistemi ile yüz verilerinin, özellikle vücut kameraları ile de göz ve iris taramasının yapılması biyometrik veri toplandığı anlamına gelir. Kişisel verilerin korunması

analizi yapan bir yazılımın sisteme eklenmesi ile şüpheli araç ve kişilerin tespiti hedeflenmektedir. Bkz. https://tubitak.gov.tr/sites/default/files/1007-egm-2013-01.pdf, (Erişim: 27.08.2024)

[5] Özel hayat alanının belirlenmesinde, "makul/meşru özel hayat beklentisi" testi, ilk kez Amerika Federal Yüksek Mahkemesi'nin Katz v. United States kararında kullanılan bu test, kişinin özel hayatına müdahaleyi bekleyip beklemediği, bu beklentinin makul olup olmadığı ve müdahaleye hazırlıklı olup tedbir alabilecek durum- da olup olmadığı akıl yürütmesine dayanmaktadır. Eğer söz konusu müdahale, hayatın olağan akışı içinde beklenilebilecek nitelikte ise ve kişi, bu makul beklentiye rağmen tedbir almıyorsa, bu alanı başkaları ile paylaşmakta sakınca görmediği anlamına gelmektedir (Üzeltürk, 2004: 10).

hakkı, Anayasa'nın özel hayatın gizliliği hakkını düzenleyen 20. maddesi içerisinde düzenlenmiştir[6]. Kişisel verilerin korunması, özel hayatın gizliliğinin bir parçasıdır. Kişisel verilerin gizliliği, bu verilerin kaderini tayin etme hakkını da içerir (İçer, Dönmez, 2020, s.443). Kişisel veri, *kimliği belirli veya belirlenebilecek bir bireye ait her türlü bilgi* olarak tanımlanırken; biyometrik veriler ise *özel nitelikli kişisel veri*lerdir (Kaya, 2011, s. 318). KVKK m. 6/1-e göre, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak kabul edilmektedir. Bu verilerin işlenmesi kural olarak yasaktır. Ancak düzenlemede belirtilen istisnai durumlarda işlenebilir[7]. Avrupa Genel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR) madde 4/14'e göre de biyometrik veriler, özel teknik süreçler kullanılarak elde edilen ve bir kişinin fiziksel, fizyolojik veya tipik davranışsal özelliklerine ilişkin olan ve kişinin açıkça tanımlanmasına olanak sağlayan kişisel verilerdir. Parmak izi, iris, DNA gibi yüz verisi de biyolojik verileri arasında yer almaktadır. Biyometrik veriler, GDPR madde 9/1'e göre özel kategorilerdeki kişisel veri olduğundan, bunların işlenmesi ancak m. 9/2'de belirtilen istisnai durumlarda mümkün olabilir[8].

[6] AY m. 20: "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Mülga üçüncü cümle: 3/10/2001-4709/5 md.)

(Değişik fıkra: 3/10/2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

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

[7] KVKK m. 6-Özel nitelikli kişisel verilerin işlenmesi şartları: (3) Özel nitelikli kişisel verilerin işlenmesi yasaktır. Ancak bu verilerin işlenmesi;

a) İlgili kişinin açık rızasının olması,

b) Kanunlarda açıkça öngörülmesi,

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

ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,

d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,

e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,

f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,

g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde mümkündür.

[8] Madde 9- Özel Kategorilerdeki Kişisel Verilerin İşlenmesi: 1. Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.

paragraf aşağıdakilerden birinin geçerli olması halinde uygulanmaz:

Birlik veya üye devlet hukuku çerçevesinde 1. paragrafta belirtilen yasağın veri sahibi tarafından kaldırılamayacağına ilişkin bir hüküm sağlanması haricinde, veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi;

Birlik veya üye devlet hukuku çerçevesinde ya da üye devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece, kontrolörün

13 Haziran 2024 tarihinde Resmî Gazete'de yayımlanan Avrupa Birliği Yapay Zekâ Yasası'nın (EU AI Act) 51. maddesi uyarınca, bir fotoğrafın kişinin kimliğini teşhis amacıyla teknik araçlarla işlenmesi halinde, basit bir fotoğraftan farklı bir biyometrik veri ortaya çıkar ve bu sistemik risk taşıyan genel amaçlı bir yapay zekâ modeli olarak sınıflandırılır. Bu sistemler, sadece yüz verilerini depolanmakla kalmaz, aynı zamanda yapay zekâ kullanarak veri tabanındaki yüzleri değerlendirip kimlik bilgilerini eşleştirebilir, böylece hakkında yakalama kararı bulunan kişiler ve hatta potansiyel suçlular bile tespit edilebilir (İçer, Dönmez, 2020, s. 429). Fakat Avrupa Birliği Yapay Zekâ Yasası'nın 5. maddesinin 1-d bendinde, bir gerçek kişinin suç işleme riskini değerlendirmek veya tahmin etmek amacıyla profilinin çıkarılmasına veya kişilik özelliklerinin ve niteliklerinin değerlendirilmesine dayalı olarak gerçek kişilerin risk değerlendirmelerini yapmak için bir yapay zekâ sisteminin kullanılması yasaklanmıştır. Dolayısıyla öngörücü polislik uygulaması kapsamında profilleme yapılması Yapay Zekâ Yasası tarafından yasaklanmış bir yapay zekâ uygulamasıdır.

Yapay Zekâ Yasası'na göre, CCTV görüntülerinden hedefsiz yüz görüntüleri toplanarak gerçek (eş) zamanlı biyometrik veri tanımlaması yapılması yasaktır (m. 5/1-e). Bu tür sistemler, kitlesel gözetim ve mahremiyet ihlali risklerini arttırdığı için yasaklanmıştır. Ancak *i)* insan kaçırma, insan ticareti veya cinsel sömürü mağdurlarına yönelik hedefli aramalar ile kayıp kişilerin aranması; *ii)* gerçek kişilerin yaşamına veya fiziksel güvenliğine yönelik belirli, önemli ve yakın bir tehdidin veya gerçek ve mevcut ya da gerçek ve öngörülebilir bir terör saldırısı tehdidinin önlenmesi*; iii)* En az dört yıllık azami bir süre için bir hapis cezası veya tutuklama emri ile cezalandırılabilen suçlar için bir ceza soruşturması

---

veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi;

veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması;

işleme faaliyetinin bir vakıf, birlik veya kar amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi;

işleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması;

yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi;

gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi;3e

koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca ve 3. paragrafta atıfta bulunulan koşullar ve güvencelere tabi olarak çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;

özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması veya sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartları sağlanması gibi halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;

gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, 89(1) maddesi uyarınca kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.

1. paragrafta atıfta bulunulan kişisel veriler Birlik ya da üye devlet hukuku kapsamındaki mesleki gizlilik yükümlülüğü veya ulusal yetkin organlar tarafından konan kurallara tabi olarak bir profesyonel tarafından veya söz konusu profesyonelin sorumluluğu altında ya da Birlik ya da üye devlet hukuku kapsamındaki mesleki gizlilik yükümlülüğü veya ulusal yetkin organlar tarafından konan kurallara tabi olarak başka bir kişi tarafından işlendiğinde, söz konusu veriler 2. paragrafın (h) bendinde atıfta bulunulan amaçlara yönelik olarak işlenebilir.

Üye Devletler genetik veriler, biyometrik veriler veya sağlık ile ilgili veriler ile alakalı olarak sınırlamalar da dahil olmak üzere ek koşullar uygulamaya devam edebilir ya da ek koşullar getirebilir.

veya kovuşturması yürütmek veya bir ceza infazı yapmak amacıyla bir suç işlediğinden şüphelenilen bir kişinin yerinin belirlenmesi veya kimliğinin belirlenmesi amaçlarıyla polis kamuya açık alanlarda gerçek zamanlı biyometrik tanımlama sistemi kullanabilir (m. 5/1-h). Gerçek zamanlı biyometrik veri tanımlaması sadece bu amaçlar için, özel olarak hedeflenen kişinin kimliğini doğrulamak amacıyla kullanılabilir[9]. Kullanımın gerçekleşeceği üye devlet için bağlayıcı kararı olan bir yargı makamı veya bağımsız idari makam tarafından verilen, gerekçeli bir talep üzerine ulusal hukukun ayrıntılı kurallarına uygun olarak verilen bir ön izne tabidir. Yetkili adli makam veya kararı bağlayıcı olan bağımsız bir idari makam, yalnızca kendisine sunulan somut deliller temelinde, söz konusu 'gerçek zamanlı' uzaktan biyometrik tanımlama sisteminin kullanımının, talepte belirtilen 1-h'de yer alan amaçlardan birine ulaşmak için gerekli ve orantılı olduğuna kanaat getirdiğinde ve özellikle zaman dilimi, coğrafi ve kişisel kapsam açısından kesinlikle gerekli olanla sınırlı kaldığında yetkiyi verir. Fakat yalnızca gerçek zamanlı uzaktan biyometrik tanımlama sisteminin çıktısına dayanarak bir kişi üzerinde olumsuz bir hukuki etki yaratan hiçbir karar alınamaz (m. 5/3) Eşleştirme ve tanımlama zamanlarının aynı olmadığı uzaktan biyometrik veri tanımlaması bu yasağın dışında tutulmuştur. Uzaktan biyometrik tanımlama sistemleri "yüksek riskli" yapay zekâ sistemi olarak kabul edilmiştir (m. 6). Bu tür sistemlerin sadece çok sınırlı ve önceden yetkilendirilmiş birimler tarafından kullanılmasına izin verilmiştir[10]. Ayrıca Yasanın 70. maddesinde yapay zekâ sistemlerindeki ön yargıdan kaynaklanabilecek ayrımcılığa karşı başkalarının haklarını korumak için, yapay zekâ sağlayıcılarının belirli nitelikleri haiz kişisel verileri de işleyebilmesinin önünün açılması gerekliliği ifade edilmiştir. Dolayısıyla yüz tanıma teknolojisinin eğitildiği veri setinin, sistemin tasarlandığı amaç açısından yeterli temsil kabiliyetine sahip nitelikte ve mümkün olan en iyi ölçüde hatasız ve eksiksiz olması gerekir.

Kişinin kamusal alanda kamelara yansıyan verilerin toplanması sürecinde olduğu gibi yok edilmemesi de bireylerin temel hak ve özgürlüklerine müdahale teşkil edebilir. Hakkında herhangi bir suç isnadı bulunmayan veya beraat kararı alan kişilerin kişisel verilerinin silinmemesi masumiyet karinesini ihlal edebilir. Türk Ceza Kanunu'nun "*verileri yok etmeme*" başlıklı 138. maddesi *"kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemesini"* suç olarak düzenlemektedir. AİHM kamu yetkililerini gözetim teknolojilerinin geniş kapsamlı ve ayrım gözetmeksizin kullanımına karşı uyarmakta ve bu uygulamaların sadece özel hayatın gizliliğinin korunması hakkını değil, aynı zamanda *masum sayılma hakkı* gibi diğer insan haklarını da etkileyebileceğini vurgulamaktadır. Mahkemeye göre, masumiyet karinesi aynı zamanda bir kişinin itibarını korumayı amaçlar ve bu nedenle AİHS m. 8'de koruma altına alınan özel hayatın gizliliğinin korunması hakkı ile ilgilidir. Sözleşmenin 6/2 ve 8. maddeleri arasındaki bağlantı ve masumiyet karinesinin ahlaki önemi, *S ve Marper/Birleşik Krallık* davasında ortaya konmuştur. Dava konusu olayda

[9] Yasaklanmış Yapay Zekâ Uygulamaları (m. 5/2): "...kolluk kuvvetleri tarafından kamuya açık alanlarda 'gerçek zamanlı' uzaktan biyometrik tanımlama sistemlerinin kullanımı, yalnızca söz konusu bentte belirtilen amaçlar için, özel olarak hedeflenen kişinin kimliğini doğrulamak amacıyla kullanılacak ve aşağıdaki unsurları dikkate alacaktır:

(a) olası kullanıma yol açan durumun niteliği, özellikle sistemin kullanılmaması durumunda ortaya çıkacak zararın ciddiyeti, olasılığı ve ölçeği;

(b) sistemin kullanımının ilgili tüm kişilerin hakları ve özgürlükleri üzerindeki sonuçları, özellikle bu sonuçların ciddiyeti, olasılığı ve ölçeği. Ayrıca, bu maddenin 1. paragrafının birinci alt paragrafının (h) noktasında belirtilen amaçlardan herhangi biri için kolluk kuvvetlerinin amaçları doğrultusunda kamuya açık alanlarda 'gerçek zamanlı' uzaktan biyometrik tanımlama sistemlerinin kullanımı, özellikle zamansal, coğrafi ve kişisel sınırlamalar açısından, bunların kullanımını yetkilendiren ulusal yasaya uygun olarak kullanımla ilgili olarak gerekli ve orantılı güvencelere ve koşullara uymalıdır. 'Gerçek zamanlı' uzaktan biyometrik tanımlama sisteminin kamuya açık alanlarda kullanımı, yalnızca kolluk kuvveti makamının 27. maddede belirtildiği şekilde temel haklar etki değerlendirmesini tamamlaması ve sistemi 49. maddeye göre AB veri tabanına kaydetmesi halinde yetkilendirilir. Ancak, usulüne uygun olarak gerekçelendirilmiş acil durumlarda, bu tür sistemlerin kullanımı, söz konusu kaydın gereksiz gecikme olmaksızın tamamlanması koşuluyla AB veri tabanına kaydedilmeden başlatılabilir."

[10] Yüksek riskli yapay zekâ sistemlerinin sağlayıcı ve dağıtıcıları ile kullanıcıların yükümlülükleri Yasa'nın üçüncü bölümünde 6-49. maddeler arasında detaylı olarak düzenlenmektedir.

Bay S, 2011 yılının Ocak ayında 11 yaşındayken tutuklanmış ve aynı yılın Haziran ayında beraat etmiştir. *Bay Marper* ise 2011 yılının Mart ayında tutuklanmış, ardından Haziran ayında davası reddedilmiştir. İki şüphelinin de tutuklandıktan sonra, 1984 tarihli Polis ve Suç Delil Yasası hükümlerine göre parmak izleri ve DNA örnekleri alınmıştır. Başvurucular, parmak izlerinin, hücre örneklerinin ve DNA profillerinin Polis ve Suç Delil Yasası'nın 64. bölüm (1A) uyarınca saklanmasının İHAS'nin 8. maddesinde korunan özel hayatlarının gizliliği hakkını ihlal ettiğini iddia etmişlerdir. Başvurucular, Sözleşme'nin 6/2 maddesi ileri sürmemiş olsalar da Mahkeme, masumiyet karinesine, yargılama sonrası aşamada, yani başvurucular hakkında verilen beraat kararı ve davanın reddi kararı bağlamında atıfta bulunmuştur[11]. Mahkeme, davanın koşulları göz önüne alındığında, başvurucuların parmak izlerinin, hücre örneklerinin ve DNA profillerinin süresiz olarak saklanmasının, başvuruculara hüküm giymiş kişiler gibi davranılmasına neden olduğuna ve onların masum olmadığı algısına yol açtığına karar vermiştir. Bununla birlikte, Mahkeme, söz konusu alıkoymanın özel hayata orantısız bir müdahale oluşturduğuna da karar vermiştir (AİHM Kararı, S. ve Marper v. Birleşik Krallık, par. 122, 125).

Bu bağlamda, suçla mücadele amacıyla kamusal alanda kamera kullanımında Türk Hukuku bakımından temel hak ve özgürlüklerinin sınırlandırılma usulünü düzenleyen Anayasa m. 13 ile özel hayatın gizliliği hakkını koruma altına alan m. 20'nin yanı sıra, kişisel veriler de dikkate alınarak 6998 sayılı Kişisel Verilerin Korunması Kanunu kapsamında veri işlemenin şartlarına (KVKK m. 6) riayet edilmesi gerekir. Anayasa m. 13'e göre, özgürlükler ancak kanunla, meşru bir nedene dayanarak, hakkın özüne dokunmadan, ölçülü bir şekilde ve demokratik toplum düzeninin gereklerine aykırı olmadan sınırlanabilir. Dolayısıyla özgürlüklerin güvence ve sınırlama ölçütlerine riayet edilebilmesi için ilk şart, polis tarafından kullanılan kamera sistemlerinin usul ve esaslarını kanunla düzenlemektir. Fakat Türkiye'de kamera sistemlerinin ve yapay zekâ destekli modern önleyici polislik uygulamalarının hukuki alt yapısında eksiklikler söz konusudur. Kent Güvenlik Yönetim Sistemi kapsamında kamusal alanda kişilerin görüntülerini düzenli olarak kaydeden, bu kayıtları depolayan ve saklayan kameralı gözetim faaliyetinin usul ve esaslarını düzenleyen herhangi bir kanuni düzenleme bulunmamaktadır. Benzer şekilde, polisin vücut kamerası ile bireylerin biyometrik verilerinin hangi durumlarda toplayacağı, nerede depolanacağı, ne kadar süre saklanacağı ve bu verilere kimlerin erişebileceğinin usul ve esaslarını düzenleyen herhangi bir yasal düzenleme de yapılmamıştır (Töngür ve diğerleri, s. 43). Kannatimizce kamusal alanda suçun önlenmesi amacıyla kullanılan ve teknolojik gelişmelerle kapsamı oldukça genişleyen video gözetim sistemlerinin usul ve esasları kanunla düzenlenmelidir. Bu noktada tespit edebildiğimiz kadarıyla *kanuni düzenleme yapılması* gerekliliğine karşı öne sürülen üç görüş bulunmaktadır. Birinci görüş, kamera sisteminin kamusal alanlarda kullanılması nedeniyle bir kanuni düzenlemeye ihtiyaç olmadığı yönündeyken; ikinci görüş, mevzuatımızda yeterli düzenleme olduğu yönündedir. Üçüncü görüş ise kamera sisteminin hukuka uygunluğunu ilgilinin rızasına dayandırmaktadır. Aşağıda bu görüşler değerlendirilecektir.

4.1. Kanuni Düzenlemeye İhtiyaç Olmadığı Görüşü

Kamera sistemleriyle izlenen alanların kamusal alan olduğunu ve kamusal alanda herşeyin aleni olması nedeniyle herhangi bir yasal düzenlemeye gerek olmadığını ifade edenler bulunmaktadır (Çolak, 2007, s. 676). Ancak kamusal alanda kullanılıyor olmaları yüz tanıma teknolojisini ve kamera sistemlerini hukuka uygun hale getiremez. Anayasa m. 13'e göre, özgürlükler ancak kanunla, meşru bir nedene dayanarak, hakkın özüne dokunmadan, ölçülü bir şekilde ve demokratik toplum düzeninin gereklerine aykırı olmadan sınırlanabilir. Özgürlüklerin güvence ve sınırlama ölçütleri gerek Anayasa'da gerek taraf

[11] Section 64 (1A) of the Police and Criminal Evidence Act prescribed that fingerprints or samples taken from a person in connection with the investigation of an offence might be retained after they had fulfilled the purposes for which they were taken.

olduğumuz uluslararası sözleşmelerde açıkça düzenlenmektedir. Kamusal alanda özgürlükler sınırlanabilir; fakat kamusal alanın kendisi bir hakkın sınırlama nedeni olamaz (Eren, 2005, s. 96).

Anayasa Mahkemesi, kişinin diğer kişilerle etkileşime geçtiği alan, kamuya açık olsa bile kişinin "mahremiyet meşru beklentisine" sahip olduğunu gösteren koşulların var olması hâlinde bu alanda özel hayatın gizliliğinin korunacağını belirtmektedir (AYM, Orhan Kayahan Kararı, 22/11/2014, p. 28). AİHM de kamusal alanda kullanılan kapalı devre televizyon kameralarına yaklaşımını ortaya koyan kararlar verniştir. 2003 yılında verilen Peck v. Birleşik Krallık kararında, özel hayata ait beklentilerin zayıf olduğu kamusal alanda kişinin sadece filme alınmasının özel hayata müdahale olmadığını, fakat bu tür bilgilerin düzenli ve kalıcı olarak kaydedilmesi durumunda özel hayata müdahalenin ortaya çıktığını kabul etmektedir. Dava konusu olayda, depresyonda olan başvurucu, elinde bıçakla Brentwood caddesinde yürürken kapalı devre kameralarına yakalanmıştır (AİHM, Peck v. UK, 44647/98, § 57). Başvurucunun bu görüntüleri, birçok gazete ve televizyon programında *"CCTV ve polis ortaklığı ile potansiyel tehlikeli bir durum etkisiz hâle getirildi"* ifadeleriyle başvurucunun yüzü gizlenmeden yayınlanmıştır. Kamera sisteminin başarısının kamuoyuna duyurulması amacıyla suçlu gibi yansıtılan başvurucu, Yayın Standartları Komisyonu ve Basın Şikayet Komisyonu'na şikayette bulunmuş ve başvurusu reddedilmiştir. İç hukuk yollarını tüketen başvurucu, AİHM'ne başvurmuştur. Mahkeme, özel hayata ait beklentilerin zayıf olduğu kamusal alanda kişinin sadece filme alınmasının özel hayata müdahale olmadığı, ancak; verilerin *sistematik kaydedilmesi*nin ve *geçici* olarak *saklanması*nın özel hayata müdahale olduğu, kayıtların *alenileşmesi*nin özel hayata saygı hakkına *ciddi* bir müdahale olduğu ve müdahalenin gerekliliği şartının yerine getirilmediğinden AİHS m. 8'in ihlal edildiğine karar vermiştir.

4.2. Kanuni Dayanağı Olduğu Görüşü

Kamusal alanda kişilerin görüntülerin kaydedilmesi konusunda, 5271 sayılı Ceza Muhakemesi Kanunu'nun 160. maddesinde[12] düzenlenen Cumhuriyet Savcısının genel araştırma yetkisi, 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun birinci maddesinde[13] düzenlenen önleyici tedbir alma yetkisi, PVSK yedinci ek maddesinde[14] ve 2803 sayılı Jandarma, Teşkilat, Görev ve Yetkileri Kanunu'nu beşinci ek maddesinde düzenlenen önleyici teknik araçla izleme ve istihbarat toplama yetkisi dayanak olarak gösterilemez. Bu düzenlemeler suçun önlenmesi amacıyla bazı tedbirlerin alınmasını öngörse de sistematik ve süreklilik arz eden bir görüntü kaydına izin vermez.

2559 sayılı Polis Vazife ve Salahiyet Kanunu (PVSK) yedinci ek maddesinde[15] ve 2803 sayılı Jandarma, Teşkilat, Görev ve Yetkileri Kanunu'nu (JTGYK) beşinci ek maddesinde düzenlenen önleyici teknik araçla izleme ve istihbarat toplama yetkisi kapsamında suçun önlenmesi amacıyla hâkim kararı ile teknik araçla izleme yapılabileceği düzenlenmiştir. Dolayısıyla suçun önlenmesi amacıyla kameralı gözetlemeye maruz kalacak kişilerin, kendilerine ne zaman ve hangi kapsamda müdahale edileceğini,

[12] CMK m. 160: "(1) Cumhuriyet savcısı, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmaya başlar. (2) Cumhuriyet savcısı, maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, emrindeki adlî kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür."

[13] PVSK m. 1/1: "Polis, asayişi amme, şahıs, tasarruf emniyetini ve mesken masuniyetini korur. Halkın ırz, can ve malını muhafaza ve ammenin istirahatini temin eder."

[14] PVSK Ek madde 7/6: "İstihbarat faaliyetlerinde, bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir. Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir."

[15] PVSK Ek madde 7/6: "İstihbarat faaliyetlerinde, bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir. Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir."

görüntülerinin ne kadar süre saklanabileceğini, kimlerin bu görüntülere ulaşabileceğini bilinebilir veya öngörülebilir kılan bir düzenleme değildir. Önleyici teknik araçla izleme, kamusal alanda kullanılan kamera sistemine benzer yönleri olmakla birlikte belirli kimselerin görüntülerinin alınmasına imkân vermesi, sistematik ve süreklilik arz etmemesi ve yüz tanıma sistemine entegre olmaması nedenleriyle farklılık arz eder.

Bununla birlikte, 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunu'nun 5. Maddesinin 5. fıkrasında *"Müsabaka ve seyir alanlarında; güvenliğin sağlanması ve bu Kanuna aykırı davrananların tespiti amacıyla, gerekli teknik donanımlar kurulur. Kameralar ve benzeri teknik donanımların yerleştirilecekleri yerler ve sayıları il veya ilçe spor güvenlik kurulları tarafından belirlenir."* denilmek suretiyle spor alanlarında güvenlik gerekçesiyle kamera kurulumuna kanuni dayanak sağlanmıştır. Fakat bu kameralar ile de nasıl bir izleme yapılacağı, usul ve şartları ayrıca düzenlenmemesi eksiklik teşkil ettiği gibi kamera sistemleri ile tüm kamusal alanların sürekli olarak izlenmesine ve kaydedilmesine izin vermez.

Bu düzenlemeler dışında, PVSK m. 5'te "parmak izi ve fotoğrafların kayda alınması" madde başlığı altında polisin hangi hallerde parmak izlerinin yanı sıra fotoğraflarının alınarak, ait olduğu kişinin kimlik bilgileri ile sisteme kaydedilmesine imkân tanıyan bir düzenleme bulunmaktadır. Bu madde uyarınca; a) Gönüllü, b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, ç) Türk vatandaşlığına başvuruda bulunan, d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, e) Gözaltına alınan, f) 5271 sayılı CMK m. 81 kapsamında hakkında fizik kimliği tespiti işlemi uygulanan, g) 5275 sayılı CGYİHK m. 21 kapsamında hakkındaki mahkumiyet hükmü kesinleşerek infaz kurumuna alınan kimselerin parmak izleri ve fotoğrafları alınarak sisteme kaydedilir. Polis, kimlik tespiti yapmak veya olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilmektedir. Bu düzenleme de akıllı kamera sistemleriyle kamusal alanların yedi gün yirmi dört saat izlenmesine, kaydedilmesine ve görüntülerin depolanmasına izin veren bir düzenleme değildir.

Mevzuatımızda PVSK'da yalnızca belirli kimselerin fotoğraflarının çekilmesi, kaydedilmesi (PVSK m. 5), istihbari amaçlarla (PVSK ek madde 5, JTGYK ek madde 7) ya da ceza muhakemesi süreçlerinde delil elde etmek amacıyla sınırlı olarak da kişilerin teknik araçlarla izlenmesi (CMK m. 140) mümkündür. Fakat bu düzenlemelerin sistematik ve sürekli olarak bireylerin görüntülerinin kaydedilmesine ve saklanmasına, biyometrik verilerinin depolanmasına, bu verilerin yapay zekâ ile davranış analizinde kullanılmasında izin vermez[16]. Kamusal alanda akıllı kamera sistemi kullanımı yapısı itibariyle önleyici bir tedbirdir. Bu tedbirin usul ve esaslarını düzenleyecek bir kanuni düzenleme yapılmalıdır.

Düzenlemede, kamusal alanda akıllı kamera kullanımının, kural olarak "canlı izleme" ile sınırlı olduğu belirtilmelidir[17]. Fakat suçüstü hali gibi istisnai bazı hallerde "kayıt altına almaya" izin verilebilir. Dolayısıyla sistemde kayıt yapabilecek donanım ve yazılım mevcut olmalı, suçüstü hali, yani suçu işlerken veya suça konu fiilin pek az önce işlendiğini gösteren bir görüntüye rastlanması durumunda aniden kayıt altına alınmalıdır. Karayollarında araçların belli mesafeler arasındaki ortalama hızlarının hesaplanması yönteminde de sadece hız sınırını aşan kişilerin sisteme kaydedildiği görülmektedir. Bu yönüyle orantılı bir müdahale söz konusudur, tüm araçların ortalama hızının sisteme kaydedilmesi

[16] Yargıtay 10. Ceza Dairesi de 23.10.2023 tarihinde kamusal alanda kullanılan kameralarla ilgili önemli bir karar vermiştir. Kararda, *"Usulüne uygun şekilde teknik araçlarla izleme kararı alınmaksızın (CMK 140), sanığın MOBESE kameraları ile izlenip suç delillerine ulaşılması durumunda, elde edilen deliller hukuka aykırıdır ve hükme esas alınamaz."* ifadelerine yer vermiştir. Bu kararda, hakkında bir suç isnadı olmayan sıradan bir vatandaşın önleyici amaçla kullanılan güvenlik kamerasına yansıyan görüntüsünün aleyhine kullanılamayacağı kabul edilmiştir ve eğer bir suç şüphesi varsa teknik araçla izleme koruma tedbirinin koşullarını düzenleyen CMK m. 140'a başvurulması gerektiği ifade edilmiştir. Yargıtay 10. Ceza Dairesi, E. 2022/1846, K. 2023/8954, T. 23.10.2023.

[17] Aynı yönde bkz. Özkan, s. 83; Karakeyha, s. 325.

hukuka aykırı olur. Fakat plaka tanıma sisteminin de bir tedbir olarak kapsamı ve koşulları hukukumuzda düzenlenmemiştir[18]. Suçla mücadele amacıyla tüm kamusal alanların süresiz kaydedilmesi, suç şüphesinin varlığından bağımsız olarak önleyici tedbir adı altında tüm toplumun kişisel verilerinin kaydedilmesi şeklinde temel hak ve özgürlüklere ağır bir müdahale teşkil eder. Ayrıca sürekli kayıt altına alınması ve belirsiz bir süre boyunca bu kayıtların muhafaza edilmesi, daha sonra geriye dönük incelemelerle polisin istediği zaman bir kimse hakkında soruşturma başlatabilmesi tehlikesini ortaya çıkaracaktır. Yapay zekâ destekli akıllı kamera sistemi ile otomatik olarak incelenen ve işlenen veriler, kanunla belirlenecek suçlarla ilgili değilse kayıt altına alınmamalıdır. Örneğin, terör olaylarının yoğun yaşandığı bir şehirde varil yüklü kamyonu tespit eden akıllı kamera, aracın bir süt kamyonu olduğunu algılandığında suç işleneneceğini gösteren bir emare bulunmuyorsa veri işlemeyi sona erdirmeli ve sistemdeki veriyi de silmelidir (Özkan, 2016, s. 84). Önerimiz, bu sistemlerin önleyici tedbirler olarak kanunla düzenlenmesi ve birbirine entegre yapılarının dikkate alınmasıdır. Doktrinde bu sistemin, optik ve teknik araçlarla veri toplanması şeklinde ifade edilmesi önerilmektedir (Özbek ve diğerleri, 2023, s. 645).

[18] Baden-Württemberg Polis Kanunu §22a otomatik plaka okuma sisteminin kullanılmasını düzenlemektedir: *"(1) Polis bir tehlikenin önlenmesi veya suçların önlenmesi için yaptığı çalışmalarda 26'ncı maddenin 1'nci fıkrası uyarınca yaptığı kontrollerde saklı teknik araçlar kullanarak araçların otomatik olarak resimlerini bunların plaka numaralarını kaydedebilir. Aracın içinde oturan kişiler kaçınılamaz bir şekilde kayıt altına alınmış olurlarsa, kayıtlar buna rağmen kullanılabilir. Birinci ve ikinci cümle uyarınca yapılan kayıtlar;*

Bütün alanı kapsayacak şekilde yapılamaz.

26'ncı maddenin birinci fıkrasının iki ve üç numaralı bentlerine giren hallerde sürekli olarak yapılamaz.

26'ncı maddenin birinci fıkrasının dört ve beş numaralı bentlerine giren hallerde, kontrol noktasında suç işlendiğine ilişkin veya konrol edilen çevrede Alman Ceza Muhakemesi Kanununun 100a maddesine giren suçların işlendiği veya bu suçların önlenebileceği polisin bilgisi dahilinde ise, ve

26'ncı maddenin birinci fıkrasının altı numaralı bendine giren hallerde uzun süreli olarak gerçekleştirilemez. Birinci fıkraya göre teknik araçlarla kaydedilmesi sırasında denetim amacıyla uygun bir şekilde tutanak düzenlenir.

(2) Elde edilen plaka numaraları federal adli kolluk bürosundaki kanuna göre kayıt altında tutulmuş bulunan polis bilgisayar kayıtlarıyla karşılaştırılabilir. Polis bilgisayarındaki veriler Şengen Sözleşmesi uyarınca arandıkları için şengen bilgi bankasına kaydedilmiş bulunan verilerle de karşılaştırılabilir. Birinci cümle uyarınca yapılan karşılaştırma sadece aşağıda sayılan araç plaka numaraları hakkında uygulanabilir.

1. Görüldüğü yerde polis tarafından kayıt altına alınmasıı gizli kayıt yapılması veya bu kanunun 25'nci maddesi, Ceza Muhakemesi Kanunun 163e ve 463a maddesi, Şengen Sözleşmesinin 99'uncu maddesi veya federal anayasayı koruma kanunun 17/3 maddesinin hükümleri gereğince amaca bağlı kontrol edilen araçlar,

2. Ağır bir tehlike bulunan hallerde, tehlikenin önlenmesi amacıyla,

3. Suç şüphesi bulunan hallerde ceza soruşturma ve kovuşturması yapılması amacıyla veya,

4. Cezanın infazı amacıyla, Karşılaştırma plakanın içerdiği bütün harf ve numaralarının aranan araçların plaka numaraları ile karşılaştırılması yoluyla yapılır.

(3) Birinci fıkranın birinci cümlesi uyarınca kayıt edilen veriler, aranan plaka numaraları arasında yer almıyorsa, karşılaştırmanın hemen ardından, geciktirilmeksizin, otomatik olarak silinir. Birinci cümleye giren hallerde, veri toplandığı ve bunların karşılaştırıldığı konusunda tutanak düzenlenemez.

(4) Elde edilen plaka numarası aranan araçların listesinde bulunduğu takdirde, palaka numarası aracın resmi, resmin çekildiği yer seyir istikameti tarih ve zamana ilişkin kayıtlar saklanır. Aracın içindekiler uyum sağlanan hallerde durdurulur. Daha sonraki işlemler mevcut aranan araçlar kayıt listesinden yapılacak inceleme üzerine elde edilen güncel bilgiye dayanılarak yapılır. Birinci cümle uyarınca kaydedilen veriler ile diğer tedbirlerden yola çıkılarak ulaşılan kişisel veriler;

1. Plaka numarasının arananlar bilgisayarına kaydedilmesine yol açan amaç açısından gerekli değil ise,

2. Suç soruşturma ve kovuşturması için gerekmiyorsa veya,

3. Bir tehlikenin önlenmesi açısından gerekli değil ise, silinir."

4.3. Müdahaleyi İlgilinin Rızasına Dayandıran Görüş

Kameralı gözetleme alanının dışına yerleştirilmiş uyarıcı işaretlerle haberdar edilmelerine rağmen söz konusu alana giren bireylerin, o alanda görevliler tarafından izlenmelerine ve görüntülerinin kaydedilmelerine örtülü de olsa rıza verdikleri düşünülmektedir. Benzer şekilde, vücut kameralarını kullanan görevliler yaka, omuz veya sırt bölgelerinde *"Ses ve Görüntü Kaydı Alınmaktadır."* ifadesini içeren yazıları taşırlar. Polis memurlarının sözlü olarak vücut kamerası ile karşısındaki kişinin görüntüsünü kayda aldıklarını ilettikleri örnekler de bulunmaktadır. Sürekli olarak görüntünün kaydedilmediği uygulama örneklerinde, ihtiyaç anında polis memurların karşısındaki vatandaşa *"Sizi kameraya kaydediyorum şu andan itibaren yaptığımız görüşmeler kayıt altına alınır."* şeklindeki açıklamasından sonra kayıt başlatılmaktadır. Bu örneklerde kameralı gözetleme faaliyetini hukuka uygun hale getiren şeyin, uyarıcı levhaların varlığına rağmen söz konusu alana giriş yapılması olduğu düşünülmektedir.

İlginin rızası, TCK m. 26, f. 2'de "*Kişinin üzerinde mutlak suretle tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez.*" denilmek suretiyle açıkça bir hukuka uygunluk nedeni olarak düzenlenmiştir (Mahmutoğlu, 2005, s. 54). Rızanın bir fiili hukuka uygun hale getirebilmesi için üç temel şartın varlığı aranır. İlki, kişinin mutlak surette tasarrufta bulunabileceği bir hakkın varlığı; ikincisi, söz konusu haktan vazgeçmenin anlamını, kapsamını ve önemini bilebilecek durumda olması, bir başka ifadeyle rıza ehliyetine sahip olması ve üçüncüsü rızanın açıklanmasıdır (Ekici Şahin, 2012, s. 177). Rıza açıklaması, kural olarak belli bir şekle bağlı değildir. Rıza yazılı veya sözlü olarak açıklanabileceği gibi, somut koşullardan ve kişinin davranışlarından anlaşılarak da açıklanmış kabul edilebilir (Koca, Üzülmez, 2010, s. 286). Buna *örtülü rıza* denilir. Eğer kişi, uyarıcı işaretlerin varlığına rağmen kameralı gözetleme alanına giriyorsa, görüntüsünün izlenmesi ve kaydedilmesine rıza verdiği kabul edilir. Fakat uyarıcı işaretlerin varlığı da tek başına yeterli değildir. Söz konusu rızanın geçerli olabilmesi için neye rıza verildiği konusunda yeterli bilgi sahibi olunması ve özgür bir şekilde rızanın verilmiş olması gerekir. Bir başka ifadeyle, kişi rıza verdiği müdahalenin kapsamı konusunda bilgilendirilmeli ve rıza vermeme ihtimalinde alternatif bir seçeneği de mevcut olmalıdır.

Kişisel Verilerin Korunması Kanunu'na göre, kişisel veriler ancak açık rıza veya kanunlarda öngörülmesi ile işlenebilir (m. 6). Bununla birlikte, biyometrik verilerin işlenmesi halinde "özel nitelikli kişisel veriler" kapsamında değerlendirme yapmak gerekir. Düzenlemeye göre: *"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."* Bu nedenle vücut kameraları ile kişilerin biyometrik verileri işlenmek isteniyorsa kural olarak açık rızalarının alınması gerekir.

KVVK m. 3/1-a bendine göre, *açık rıza* belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle verilen rızayı ifade eder. Bu konuda rızanın geçerli olabilmesi için neye rıza verildiği konusunda yeterli bilgi sahibi olunması ve özgür bir şekilde rızanın verilmiş olması gerekir (Koca, Üzülmez, 2023, s. 294). Rıza açıklaması, kural olarak belli bir şekle bağlı değildir. Rıza yazılı veya sözlü olarak verilebilir. Fakat bu konuda açık rıza arandığından, somut koşullardan ve kişinin davranışlarından anlaşılarak açıklanmış, yani örtülü rıza kabul edilemez (Ekici Şahin, 2012, s. 177). Aydınlatma için ise kameralı

gözetleme yapan alanlara yerleştirilen uyarıcı işaretlerin veya polisin yaka kamerasını çalıştırmadan önce yapacağı sözlü uyarının yeterli olmadığı söylenmelidir. Aydınlatma yükümlülüğünün hangi şekilde yerine getirilebileceği konusunda KVKK'da özel bir düzenleme bulunmamaktadır. Örneğin, her kameranın yanına bir QR kodun yer alması ve bu kodun internete bağlı bir cihazın kamerasına okutulması ile aydınlatma metnine ulaşılabildiği bir yöntemin aydınlatma için kullanılabileceği düşünülmektedir.

Bununla birlikte, KVKK m. 28'de düzenlenen önleyici, koruyucu ve istihbari faaliyetler kapsamında veri işlenmesi, veri koruma kanunu kapsamı dışında tutulmuştur. Düzenlemede kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler veya yargısal süreçler kapsamında veri işlenmesi durumunda veri koruma kanunun dışında tutulduğu görülmektedir. Örneğin, Millî İstihbarat Teşkilâtı (MİT) ve emniyet istihbarat bu düzenlemeyle kanun dışında tutulur[19]. Bu bağlamda, tam istisnadan yararlanacak faaliyetlerin milli güvenlik, kamu güvenliği, kamu düzeni gibi unsurları korumaya yönelik makro ölçekteki süreçleri kapsadığı söylenebilir (Kızılırmak, 2019, s. 254). Dolayısıyla bireysel ya da doğrudan kamu güvenliğine etki edecek nitelikte olmayan bir suçun önlenmesi kapsamındaki faaliyetler bu hüküm kapsamında değildir. Fakat inceleme konumuzla bağlantılı olarak suçla mücadele kapsamında "önleyici faaliyetler" bu istisna kapsamında sayılmıştır. Önleyici faaliyetlere örnek olarak PVSK ile polise tanınan kimlik sorma, kimlik tespiti, parmak izi ve fotoğrafların sisteme kaydedilmesi gösterilebilir. Plaka tanıma sistemi, şehir güvenlik kameraları veya vücut kameraları da polis tarafından önleyici kolluk faaliyeti kapsamında kullanılmaktadır. Bu kameralar, üstelendiği fonksiyon itibariyle "önleyici tedbir" niteliğindedir (Özbek ve diğerleri, 2023, s. 194; Özkan, 2016, s. 65). Her ne kadar suç önleme amacıyla kullanılıyor olsalar da bu faaliyete ilişkin ne PVSK'da ne farklı bir kanunda herhangi bir düzenleme yer almamaktadır. Dolayısıyla kamusal alanda kullanılan akıllı kamera sistemi, kanunla düzenlenmediği için kanunla görev ve yetki verilmiş bir kurum tarafından yürütülen faaliyet kapsamında değerlendirilemez. Belirtilen bu nedenlerle, kamusal alanda kullanılan kamera sistemleri veri koruma kanununa uyması gereken faaliyetler kapsamı dışında -kanuni düzenleme yapılana kadar- tutulamaz. Fakat kanuni düzenleme yapıldığında, önleyici bir tedbir olarak kullanılan akıllı kamera sistemleri ile işlenen kişisel veriler KVKK m. 28 hükmü uyarınca istisna kapsamında olabilir. Yine de kamera sistemlerinin gizli olarak kullanılması hukuka aykırı olacağı için uyarıcı işaretler konulmalıdır.

5. ALMANYA'DA KAMUSAL ALANDA VİDEO GÖZETİMİ: YASAL DÜZENLEMELER VE UYGULAMA ÖRNEKLERİ

Almanya'da kamuya açık bir alanlarda video gözetimi için çeşitli düzenlemeler bulunmaktadır. Bu düzenlemeler, temel olarak Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz, BDSG), Avrupa Birliği Genel Veri Koruma Tüzüğü (European General Data Regulation, GDPR) ve çeşitli eyalet polis kanunlarıyla belirlenmiştir. Aşağıda bu düzenlemeler ve uygulamadan örnekler incelenecektir.

4.1. Veri Koruma Mevzuatı

Federal Veri Koruma Kanunu'nun § 6b hükmü, kamuya açık alanlarda kapalı devre televizyon kame-

[19] Bu durum madde gerekçesinde *"Milli İstihbarat Teşkilatı ile diğer istihbarat birimlerinin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetler kapsamında işlendiği veriler Kanun kapsamı dışında tutulmaktadır. Aynı şekilde belirtilen amaçlarla, suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda; yetkişi birim tarafından yürütülen faaliyetler kapsamında işlenen veriler de bu istisna kapsamındadır. Bu konulardaki yetkili birimin; milli savunmayı, milli güvenliği kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği veriler de kapsam dışında tutulmaktadır."* şeklinde ifade edilmiştir.

ralarının kullanımı düzenler[20]. *Kamuya açık alanların **o**ptik-elektronik araçlarla gözetlenmesi* başlıklı bu düzenlemeye göre, video gözetimine yalnızca, ***i)*** Kamu kurumlarının görevlerini yerine getirmeleri, ***ii)*** Ev kurallarının uygulanması, bir başka ifadeyle bir kimsenin bir yere girişine izin verilmesi ya da verilmemesi amacıyla karar verme hakkını kullanması, ***iii)*** Verisi işlenen kişinin özel olarak tanımlanmış meşru bir menfaatin korunması adına gerekli ve etkilenenlerin meşru menfaatlerinin bundan daha ağır bastığına dair hiçbir belirti olmadığında izin verilir. Özellikle spor tesisleri, toplanma alanları, eğlence merkezleri, alışveriş merkezleri ve otoparklar gibi kamuya açık büyük tesisler veya tren, gemi ve otobüs taşımacılığına yönelik araçlarda video gözetimi için kişilerin yaşamının, sağlığının veya özgürlüğünün korunması açısından önemli menfaatler olarak kabul edilir. Elde edilen verilerin saklanması ve kullanılması ancak belirlenen amacın yerine getirilmesi ve verisi işlenen kişinin meşru ve daha üstün çıkarının bulunmaması halinde mümkündür. Elde edilen verinin sonraki bir amaç doğrultusunda işlenmesi sadece devlet ve kamu güvenliğine karşı bir tehdidin önlenmesi ve suçların kovuşturulması için gerekli olması durumunda mümkündür.

Kamuya açık alanların suçun önlenmesi amacıyla optik-elektronik araçlarla izlenmesi mümkündür, ancak tedbirin bu amaca ulaşmak için gerekli olması ve etkilenenlerin korunmaya değer mefaatlerinin bundan daha ağır bastığına dair hiçbir göstergenin bulunmaması gerekir. Genellikle ikinci koşulda bazı ihtilaflar ortaya çıkabilmektedir. Bu bağlamda, bireylerin temel hak ve özgürlükleri üzerindeki etkileri göz önüne alındığında, operatörün menfaati ile video gözetiminden etkilenenlerin hakları arasında bir denge kurulması önemlidir. Kişiyi açıkça gösteren fotoğraflar, BDSG 3. Bölüm 1. fıkra kapsamında kişisel veridir. Kişinin kendi verilerinin kaderini tayin hakkı da anayasal olarak korunan bir haktır. İlgili kişinin iradesi dışında görüntüsünün alınması anayasal haklarına müdahale teşkil eder. Müdahalenin yoğunluğu kameranın kurulduğu alana, kurulum açısına ve teknik özelliklerine bağlıdır.

Avrupa Birliği Genel Veri Koruma Tüzüğü video gözetimi konusunda özel bir düzenleme getirmese de veri işlemede menfaatler dengesine dayalı bir değerlendirme yapılmasını gerektirir (m. 6/1/f). Düzenleme, Federal Veri Koruma Kanunu'nun (BDSG) Bölüm 28 Paragraf 1 Cümle 1 No. 2 ile oldukça benzerdir ve sorumlu organın veya üçüncü bir tarafın, herhangi bir öncelikli menfaatle çatışmayacak meşru bir menfaatinin varlığını şart koşar (Karper, 2016). Ayrıca Veri Koruma Tüzüğü, etkilenenlerin hakları bakımından şeffaflık yükümlülüğü arar. Benzer şekilde, BDSG Bölüm 6b Paragraf 2'ye göre, gözetimin koşulları ve sorumlu kuruluş belirtilmelidir. Fakat GDPR madde 12 ve madde 13 ile birlikte şeffaflık yükümlülüğünü önemli ölçüde genişletmektedir. Veri işlemeden sorumlu kişinin iletişim bilgilerine ek olarak, onun temsilcisi, şirket veri koruma görevlisinin iletişim bilgileri, amaçlar ve yasal dayanakları da en geç veri toplama sırasında iletilmelidir (GDPR m. 6/1). Adil ve şeffaf video gözetimini sağlamak için depolama süresi, düzeltme ve silme hakları da belirtilmelidir (GDPR m. 13/2). Bu bilgiler kesin, şeffaf, anlaşılır olmalı ve özellikle çocuklara yönelik olduğunda, açık ve basit bir dil kullanılarak, kolay erişilebilir bir biçimde iletilmelidir. Ne yazık ki GDPR, videoyla yakalanan alana girmeden önce tüm bu hususların pratikte nasıl sunulabileceğini açıklamaz. Yine çocukların kameralı gözetim alanlarından geçtiklerinde görüntülerinin kayıtta kalıp kalamayacakları dikkate alınmalıdır. GDPR madde 6 Paragraf 1, bu durumlarda özellikle dikkatli olunmasını gerektirir. Bununla beraber, video gözetiminde yalnızca kişilerin görüntüleri kişisel veri olarak işlenmez, aynı zamanda, örneğin yüz tanıma sistemiyle biyometrik verileri ve bireysel hareket profilleri de toplanır ve saklanır. Biyometrik veriler, Avrupa Genel Veri Koruma Tüzüğü m. 9'a göre yalnızca istisnai durumlarda işlenebilir[21].

[20] https://dejure.org/gesetze/BDSG_a.F./6b.html, Bu düzenleme, en son 25 Şubat 2015 yılında aşağıdaki cümleler eklenerek genişletilmiştir. "*1. spor, toplantı ve eğlence mekanları, alışveriş merkezleri veya **otoparklar gibi kamuya açık büyük ölçekli tesisler veya 2. Kamuya açık demiryolu, gemi ve otobüs taşımacılığına yönelik araçlar ve kamuya açık büyük ölçekli tesisler, orada kalan insanların yaşamının, sağlığının veya özgürlüğünün korunması açısından özellikle önemli bir menfaat olarak değerlendirilmektedir.***"

[21] Özel kategorideki kişisel verilerin işlenemsi, Madde 9: 1. Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla

GDPR madde 17 (1) (a) uyarınca veri denetleyicisi, toplanma amaçları için artık gerekli olmaması durumunda verileri makul olmayan bir gecikme olmaksızın silmekle yükümlüdür. Federal Veri Koruma Kanunu'nda yer alan ifadeler biraz daha katı olsa bile, veri ekonomisi ilkesi dikkate alınarak, görüntü verilerinin amaca ulaşıldıktan hemen sonra silinmesi zorunluluğunun yine de mevcut olması gerekir. Bu noktada, video verilerinin değerlendirilmesinin makul bir şekilde gerçekleştirilebileceği süre ayrı ayrı kontrol edilmeli ve 72 saatlik maksimum saklama süresi aşılmamalıdır (Karper, 2016).

Akıllı video gözetim sistemlerinin yaygın kullanımı için, veri işlemenin kapsamını ve amacını açıkça tanımlayan, ayrıca mekansal ve zamansal bir sınır ile birlikte kısa saklama süreleri öngören yeni bir yasal dayanak gerekebilir. Ayrıca video gözetiminden etkilenen kişilerin haklarına da açıkça atıfta bulunulmalıdır. Ev kurallarına veya tehlikelere karşı yasanın genel maddesine başvurmak yargısal denetim karşısında yeterli olmabilir.

---

genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.

2. Paragraf aşağıdakilerden birinin geçerli olması halinde uygulanmaz:

Birlik veya üye devlet hukuku çerçevesinde 1. paragrafta belirtilen yasağın veri sahibi tarafından kaldırılamayacağına ilişkin bir hüküm sağlanması haricinde, veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi;

Birlik veya üye devlet hukuku çerçevesinde ya da üye devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece, kontrolörün veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi;

veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması;

işleme faaliyetinin bir vakıf, birlik veya kar amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi;

işleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması;

yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi;

gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi;3e

koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca ve 3. paragrafta atıfta bulunulan koşullar ve güvencelere tabi olarak çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;

özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması veya sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartları sağlanması gibi halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;

gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, 89(1) maddesi uyarınca kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.

1. paragrafta atıfta bulunulan kişisel veriler Birlik ya da üye devlet hukuku kapsamındaki mesleki gizlilik yükümlülüğü veya ulusal yetkin organlar tarafından konan kurallara tabi olarak bir profesyonel tarafından veya söz konusu profesyonelin sorumluluğu altında ya da Birlik ya da üye devlet hukuku kapsamındaki mesleki gizlilik yükümlülüğü veya ulusal yetkin organlar tarafından konan kurallara tabi olarak başka bir kişi tarafından işlendiğinde, söz konusu veriler 2. paragrafın (h) bendinde atıfta bulunulan amaçlara yönelik olarak işlenebilir.

Üye Devletler genetik veriler, biyometrik veriler veya sağlık ile ilgili veriler ile alakalı olarak sınırlamalar da dahil olmak üzere ek koşullar uygulamaya devam edebilir ya da ek koşullar getirebil

4.2. Federal Polis Kanunu ve Eyalet Polis Kanunları

Almanya'da polislerin vücut kamerası kullanmasına ilişkin düzenlemeler eyalet polis kanunlarında ve Federal Polis Kanunu'nda yer almaktadır[22]. Vücut kameralarının kullanımı, ilk olarak Hessen, Hamburg ve Bavyera eyaletlerinde pilot projeler kapsamında başlamıştır[23]. Daha sonra Federal Meclis de polislerin vücut kamerası kullanmalarına Federal Polis Kanunu'na yaptığı düzenlemelerle izin vermiştir[24].

[22] Örneğin, Baden Württembetg Polis Kanunu'nun 21. maddesinde kamuya açık alanların kameralarla kaydedilmesinin koşulları düzenlenmiştir. Aleni yerlerde yapılan görüntü ve ses kayıtları başlıklı maddeye göre: *"(1) Polisin fiili görevlerini yerine getiren birimleri, Toplantı ve Gösteri Yürüyüşleri Kanunu kapsamına girmeyen aleni organizasyonlar ve topluluk oluşması sırasında veya bunlar vesilesi ile, bunlar sırasında önemli ağırlığı olan kabahatler veya suçlar işlenebileceklerini kabul etmeyi haklı gösterecek fiili olgular bulunan kişilerin resimlerini veya seslerini kayda alabilir. Üçüncü kişiler, kaçınılmaz bir şekilde, etkilenecek olsalar dahi, kayıt yapma işlemi sürdürülür. (2) 26'ncı maddenin 1'nci fıkrasının 3'üncü bendinde tanımlanan objelerde veya bunların yakınında, bu objelere karşı veya bunların içinde suç işleneceğini kabul etmeyi haklı gösteren bulgular varsa, ve bu şekilde kişiler, bu objeler veya bunların içinde bulunan eşyanın tehlikeye düştüğü hallerde fiili polis hizmetini gören memurlar kişilerin resimlerini çekebilirler ve ses kaydı alabilirler. (3) Fiili polis hizmeti gören memurlar ve yerel polis makamları kamu güvenliğini tehdit eden tehlikeleri önlemek üzere veya 26'ncı maddenin 1'nci fıkrasının 2 no'lu bendinden tanımlanan yerlerde, bunlar kamuya açık yer niteliğinde oldukları sürece kamu güvenliğini bozmuş olan halleri ortadan kaldırmak üzere aleni ve açık bir şekilde görüntü kaydı nakli yapmak suretiyle izleyebilirler ve kişilerin resimlerini çekebilirler. (4) Suçların veya kabahatlerin kovuşturulması kamu hukukuna ilişkin taleplerin ileri sürülmesi veya bu kanunun 2'nci maddesinin 2'nci fıkrası uyarınca, bireylerin özel haklarının korunması, özellikle başka türlü delil bulunmamasından dolayı ispat zorunluluğunun ortadan kaldırılması için somut olayda kullanılmaları gerekli olmadıkları takdirde resim ve ses kayıtları geciktirilmektesizin ancak en geç iki ayın geçmesi ile silinir. Üçüncü fıkra uyarınca yapılan resim kayıtları, bu fıkranın 1'nci cümlesi uyarınca kullanma koşulları oluşmamışsa, 48 saat sonra silinir. (5) Açıkça yapılmadığı hallerde, resim nakli ve resim ve ses kaydı şekilde gerçekleşen izlemede uygun bir şekilde bilgilendirme yapılır. Resim ve ses kayıtları somut olayda suç soruşturma veya* kovuşturmasında veya önemli *kabahatlerin yaptırıma bağlanmasında gerekli olduğu haller dışında, geciktirilmeksizin, ancak en geç dört hafta sonra silinir, bunlar kamu hukuka ilişkin talep haklarının ileri sürülmesi veya ikinci maddenin ikinci fıkrasında öngörülen özel hakların korunması, bilhassa başka delil bulunmaması nedeniyle ispat zorluğu yaşandığı hallerde kullanılabilir. Kaçınılmaz bir şekilde üçüncü kişiler hakkında da kayıt yapılmışsa, bu kayıtların kullanılması buna rağmen mümkündür. Eğer somut olaydaki duruma göre önemli bir hukuki menfaat açısından bir zarar doğması veya diğer hukuki menfaatler açısından önemli ölçüde tehlike varsa veya ilgili hüküm toplumun sair önemli bir yararını koruyor ise, belli bir kabahatin önemli olduğu kabul edilir."*

[23] Hessen'de: Madde 14 Paragraf 6 HSOG; Hamburg'da: Madde 8 Paragraf 5 PolDvG HH; Bavyera'da konumun büyüklüğü veya net olmaması nedeniyle video gözetimi (Madde 33 Paragraf 1 Nr. 2 BayPAG), ön kayıt işlevine sahip vücut kameralarının kullanılması (Madde 33 Paragraf 4 BayPAG), otomatik kullanımı tanıma ve değerlendirme sistemleri (Madde 33 Paragraf. 5 BayPAG),

[24] **§27a- Mobil görüntü kaydetme ve ses kayıt cihazları:**

(1) Federal Polis, gerekli olduğuna dair fiili emarelerin bulunması halinde, vücuda yakın olarak takılan görüntü ve ses kayıt cihazlarını kullanarak, kamuya açık yerlerde görüntü ve ses kayıtları yapmak suretiyle kişisel verileri toplayabilir.

1. Federal polis memurlarını veya üçüncü şahısları hayat, beden, özgürlük veya mülkiyete yönelik tehlikelere karşı korumak veya 2. a) ceza gerektiren suçlar veya b) Bireysel vakalarda dahi oldukça önemli olan idari suçları takip etmek.

(2) Kişisel verilerin toplanması, üçüncü kişilerin kaçınılmaz olarak etkilenmesi durumunda da gerçekleşebilir.

1. paragraf uyarınca önlemler uygun bir biçimde belirtilmelidir; Yakın bir tehlike varsa, bildirim atlanabilir.

(3) Görüntü ve ses kayıt cihazları, bekleme modundayken ara belleklerine kısa süreliğine veri kaydedebilir. Bu veriler, paragraf 1'e uygun olarak kayıt yapılmadığı sürece, maksimum 30 saniye sonra iz bırakmadan otomatik olarak silinmelidir. Bu durumda, paragraf 1'e uygun olarak kaydedilen veriler,

paragraf 1'e uygun olarak kayıt başlamadan önce 30 saniyeye kadar kaydedilebilir.

(4) Kişisel verilerin birinci fıkra uyarınca kaydedilmesi halinde görüntü ve ses kayıtlarının 30 gün süreyle saklanması gerekir. Aşağıdaki durumlar için gerekli olmadıkça kayıtlar derhal imha edilmelidir:

1. a) ceza gerektiren suçlar veya b) Bireysel vakalarda dahi önemli önem taşıyan idari suçları takip etmek için,
2. bireysel durumlarda tehlikeyi önlemek veya
3. Bireysel durumlarda, özellikle ilgili kişinin talebi üzerine, yasallığın kontrol edilmesi

kaydedilen polis eylemleri için.

§ 27b- Olaya bağlı otomatik plaka tanıma: (1) Federal Polis, 2. maddenin 2. fıkrası uyarınca görevlerini yerine getirmek amacıyla, kamuya açık trafik alanlarındaki araçların plakalarını, teknik araçlar kullanarak, kişinin bilgisi dışında, geçici ve kapsamlı olmayan bir şekilde otomatik olarak toplayabilir, eğer 1. Bunun, kişinin vücut bütünlüğüne, hayatına veya

İlk kez 2013 yılında, Hessen eyaletinde Frankfurt, Wiesbaden ve Offenbach'taki pilot projeler kapsamında polisler vücut kameralarını kullanmıştır (Grünwald, 2015). Hem Hessen'de hem Hamburg'da polisin neyi ve ne zaman kaydedeceğine bileğindeki uzaktan kumandayı kullanarak kendisi karar vermiştir. Polislerin vücut kameralarıyla sürekli görüntü kaydı yapmasına izin verilmez, yalnızca olayla ilgili olarak kayıt yapabilirler. Kaydın bitiminden sonra, kolluk kuvvetleri açısından gerekli olmadıkça kayıtların silinmesi gerekir. Hessen'de kanun, verilerin artık güvenlik ve kovuşturma amaçları için gerekli olmaması halinde "derhal" silinmesi gerektiğini şart koşar (HSOG Bölüm 14 Paragraf 6). Hamburg'da ise görüntü ve ses kayıtlarının cezai kovuşturma açısından gerekli olmadıkça en geç dört gün sonra silinmesi gerekir (PolDvG HH § 8 paragraf 5). Kayıtların silinmesi işlemi polis memuru tarafından değil, amiri tarafından başlatılır. Hessen'de kameralar yalnızca yaya bölgeleri, parklar veya kapalı otoparklar gibi kamusal alanlarda kullanılmaktadır ve ses kaydı alınmaz. Olaydaki hareketlerin daha iyi anlaşılması için ses kaydının da alınması planlanmaktadır. Eyaletlerde vücut kameralarının kullanımına başladıktan sonra, polislerin kurallara riayette daha titiz davranıkları ve vatandaşların ise polise karşı direnme davranışlarının azaldığı ifade edilmiştir (Karper, 2016).

Fakat Saksonya eyaletinde 2020 yılından bu yana polis "Kişi Kimlik Tespit Sistemi" (Peronen-Identifikations-System/PerIS) ile uzaktan biyometrik tanımlama yapmaktadır. Savcılık tarafından, biyometrik gözetimin yasal dayanağı olarak Ceza Muhakemesi Kanunu'nun 98a maddesi gösterilmektedir (Wörner, 2024). Diğer yöntemlerin "önemli ölçüde daha az umut verici veya önemli ölçüde daha zor" olacağı büyük öneme sahip bir suç durumunda bir tarama ağı soruşturmasına izin veriyor. Bu düzenlemeye göre, teknoloji tarafından kaydedilen tüm kişiler "otomatik olarak diğer verilerle karşılaştırılabilir. Saksonya eyaletinde vücut kameraları polis kanununda düzenlenmeden kullanılmıştır ve bu nedenle hukuka aykırı kullandığına ilişkin eleştiriler söz konusudur (Conrad, 2017-b). Bu eleştirilerden ilki; kamusal alanda kullanılan diğer kameralarda olduğu gibi büyük uyarı levhalarıyla bireylere bilgilendirme yapılmamasına dayanır. Ayrıca kişinin kendisi hakkındaki verileri kaderini belirleme hakkı ile polisin güvenliği sağlama ve belgeleme konusundaki menfaati arasında uygun bir denge oluşturulması gerektiği ifade edilmiştir. Son olarak, yeni teknik sistemlerin kullanımına ilişkin bir ön kontrol yapılması zorunluluğu varken eyalette deneme amaçlı doğrudan kullanılması hukuka aykırı olarak nitelendirilmiştir[25]. Vücut kameraların polis memurlarına yönelik saldırıların azaltılmasına gerçekten katkıda bulunup bulunmadığının ortaya koyulması talep edilmiştir.

özgürlüğüne yönelik mevcut bir tehlikeyi önlemek için gerekliyse, 2. Sınır güvenliğine yönelik ciddi önem taşıyan suçlara ilişkin fiili delillere dayanarak meydana gelmesi veya 3. Bir kişi veya bir araç Federal Polis veya başka bir makam tarafından uyarılmış ve bu kişi tarafından veya uyarı verilen araç aracılığıyla ciddi önem taşıyan bir suçun işlenmesi tehlikesi yakın veya devam ediyorsa.

(2) 1. fıkra uyarınca toplanan veriler, 34. maddenin 1. fıkrasının 2. cümlesine uygun olarak arananlar listesiyle otomatik olarak karşılaştırılabilir.

(3) Bir isabet durumunda, kaydedilen veriler ile arama veri tabanından alınan veriler arasındaki uygunluk derhal kontrol edilmelidir. Eşleşen veriler, elde edilen bilgilerle birlikte işlenebilir ve düzenleyen makama iletilebilir.

(4) Herhangi bir isabet olmaması durumunda veriler derhal ve iz bırakmadan silinmelidir.

(5) Toplanan verilerin, 34. Maddenin 1. Fıkrasının 2. Cümlesine uygun olarak arama sonuçlarıyla karşılaştırılması sonucunda eşleşme çıkması durumunda, ancak arananlar listesindeki uyarının Paragraf 1'in 1'den 3'e kadar olan sayılarının amaçları doğrultusunda, önemli bir suçun kovuşturulmasını sağlamak amacıyla gerekli olmadıkça veriler derhal ve iz bırakmadan silinmelidir.

§ 27c- Arama Kaydı: (1) Federal Polis, görevlerini yerine getirmek için gerekli olması halinde, operasyonel kontrol merkezlerine gelen telefon görüşmelerini kaydedebilir.

(2) Kayıtlar, ceza gerektiren suçların kovuşturulması veya tehlikenin önlenmesi için bireysel vakalarda hala bunlara ihtiyaç duyulmazsa, görevi yerine getirmek için artık gerekli olmadıkları anda ve en geç 30 gün içinde derhal ve iz bırakmadan silinmelidir.

Bkz. https://dserver.bundestag.de/btd/18/109/1810939.pdf

[25] vgl. § 7 Abs. 3 NDSG

Alman Federal Polisi özellikle Berlin'de tren istasyonunda, 2017 yılından bu yana yüz tanıma sistemlerini kullanmaktadır. Başlangıçta, Deutsche Bahn (DB) (Alman Tren İstasyonu), demiryolu görevlilerine yönelik şiddeti önlemek amacıyla yaklaşık 3700 güvenlik personeli ile vücut kamerası kullanımına başlamıştır. Berlin'de tren istasyonu çalışanları, sürekli kayıt yapan ve canlı görüntüyü üniformalarına iliştirilen küçük bir monitöre aktaran vücut kameralarıyla donatılmıştır (Conrad, 2017-a). Daha önceki uygulamalarda, polisin görüntü kaydına başlaması için bileğine bağlı bir düğmeye dokunması gerekiyordu. Fakat DB uygulamasında vücut kamerası sürekli aktif haldedir ve görevliler üniformlarının üzerinde açıkça "kamera gözetimi" ibaresini taşırlar. Daha sonra 2017 yılında Deutsche Bahn, bir adım daha ileri giderek İçişleri Bakanlığı ve Federal Polis ile birlikte Berlin'in Südkreuz tren istasyonunda "akıllı video gözetimi" için biyometrik yüz tanıma pilot projesi başlatmak istemiştir. Berlin Südkreuz istasyonunda yasal dayanağı olmadığı halde polis tarafından biyometrik yüz tanıması sistemi bir yıl boyunca test edilmiştir.

Bu pilot proje kapsamında, yapay zekâ ile yüz tanıma sistemine entegre kameralar tren istasyonunda kullanılarak, insanların hareket şekillerini değerlendirebilmek ve şüpheli bagajları tespit edebilmek amaçlanmıştır. Yazılım, yankesicilerin tipik hareketlerini tanıyabilmeli ve güvenlik güçlerini uyarabilmelidir. Akıllı video gözetim sistemi, kişilerin örneğin "Sporda Şiddete Uğrayan Failler" veri setiyle karşılaştırılmasına olanak tanıyan yüz tanıma yazılımıyla donatılmıştır (Conrad, 2017-a). Fakat zayıf aydınlatma gibi teknik veya trene gecikmemek için koşan kişinin davranışlarının yanlış alarmı tetiklemesi endişeleri kamuoyunda tartışılmıştır. Nitekim daha önce 2007 yılında Mainz tren istasyonunda benzer bir pilot proje yürütülmüş ama başarısızlıkla sonuçlanmıştır (Conrad, 2017-a; Kannenberg, 2017).

Vücut kameraları hem tren istasyonlarında hem de trenlerde ve dolayısıyla kamuya açık alanlarda kullanılmaktadır Deutsche Bahn şirketi Alman devletine ait olan bir özel hukuk şirketidir ve vücut kameralarını kullanırken Federal Veri Koruma Yasası'nın (BDSG) 6b düzenlemesine uyulması gerekir. Bu tesislerin sahibi olarak Deutsche Bahn da genellikle ev kurallarına (Hausrecht) tabidir. Kameralı kontrol önlemleri, bu ev kurallarına dayanarak veya biletin uygun şekilde satın alınması koşuluyla bireysel yolcuyla yapılan sözleşmeye dayalı ilişki yoluyla da oluşturulabilir. Şirketin, vücut kameraları aracılığıyla Deutsche Bahn personeline yönelik saldırıları önleme veya belgeleme konusundaki menfaati, polis memurlarının suçun önlenmesi kapsamındaki (önleyici) tedbirleriyle aynı değildir. Devletin suçun önlenmesi kapsamında alacağı tedbirler, özel güvenlik güçlerinin başvuramayacağı düzenleyici kanunlara dayanmaktadır. Bu çerçevede, DB görevlilerinin vücut kamerası kullanımında bireylerin kişisel haklarına ilişkin meşru menfaati, Deutsche Bahn'ın menfaatinden daha ağır basabilir. Hem fail/mağdur olduğu iddia edilen kişilerin hem de görüntünün kaydedildiği ortamda olayla ilgisi olmayan üçüncü kişilerin verileri kaydedilmektedir. DB uygulamasında kayıtların saklanıp saklanmayacağı da bilinmemektedir. Kayıtların saklanması gerekiyorsa, saklama süreleri BDSG Bölüm 6b Paragraf 5'e uygun olmalıdır; buna göre veriler, amaca ulaşmak için artık gerekli değilse veya etkilenen kişilerin menfaati varsa derhal silinmelidir.

Akıllı video gözetimi, bireysel temel haklara yönelik tehditlerin yoğunluğunu ve kapsamını artırmaktadır. Almanya'da video gözetimi konusunda çeşitli yasal düzenlemeler bulunmakla birlikte eksiklikler de söz konusudur. Belirtilen bu nedenlerle, kişilerin eş zamanlı mı geriye dönük mü tespit edildiğinden ziyade, akıllı video gözetim uygulamaları arasında ayrım yapmak (kimlik tespiti, izleme, gözaltı ve yakalama için görüntü kaydı gibi), her bir duruma özgü riskleri dikkate alarak usul ve esaslarını düzenlemek gerekecektir.

5. SONUÇ

Bu çalışmada, Türkiye'de suçun önlenmesi amacıyla kullanılan akıllı video gözetimi temel hak ve özgürlükler bağlamında ele alınarak hukuki koşulları ve sınırları gösterilmiştir. Ülkemizde suçla müca-

delede kamera kullanımı, 2000'li yılların başında İstanbul başta olmak üzere pek çok şehirde meydanlar, caddeler, parklar, metrolar ve toplu taşıma araçları gibi kamusal alanların yedi gün yirmi dört saat izlenmesiyle başlamıştır. İlerleyen süreçte MOBESE, Kent Güvenlik Yönetim Sistemi (KGYS) adını almış ve Plaka Tanıma Sistemleri (PTS) ile entegre edilmiştir. Böylece kamera üzerinden alınan araç fotoğrafları ve plaka karakterleri tanımlanabilmekte ve plakası okunan araçların plaka bilgileri ve fotoğrafları sorgulanarak alarm üretilebilmektedir. 2019 yılından bu yana da İstanbul'da bir pilot proje kapsamında trafik polisleri vücut kameralarını test etmektedir. 2025 yılından itibaren tüm polislerin vücut kameralarıyla donatılması planlanmaktadır. Yüz ve iris taraması yapabilen vücut kameraları ile dar alanda biyometrik veriler toplanarak merkezi sunuculara aktarılmaktadır. Polis, özellikle büyük etkinliklerde ve toplumsal olaylarda, kalabalığın kontrolü ve gözetimi amacıyla dronları ve insansız hava araçlarını (İHA) da kullanmaktadır. Dolayısıyla trafik güvenliğinin sağlanması ve suçun önlenmesi amacıyla meydanlar, parklar, toplu taşıma araçları gibi kamusal alanların izlenmesi ile başlayan video gözetiminin kapsamı, yüz tanıma teknolojileri, insansız hava araçları, dronlar ve vücut kameraları ile oldukça genişlemiştir. Günümüzde tüm bu araçların sensörleri aracılığıyla çevrelerindeki neredeyse tüm nesnelere ilişkin çok sayıda veri topladığı ve kendi aralarında birbirlerine entegre olduğu yapay zekâ destekli *akıllı video gözetimi* karşımızdadır. Akıllı video gözetimi, geleneksel gözetim sistemlerinin ötesine geçen, gelişmiş teknolojiler ve algoritmalar kullanarak yapılan gözetim türüdür. Akıllı gözetim sistemleri, çeşitli sensörlerden gelen verileri (kameralar, hareket dedektörleri, ses sensörleri vb.) entegre eder ve bu verileri analiz ederek daha kapsamlı bir gözetim sağlar (Wood, 2021, s. 150). Bunu yaparken genellikle yapay zekâ (YZ), makine öğrenimi, büyük veri analitiği ve sensör teknolojileri kullanarak daha etkin ve detaylı bir izlemeyi mümkün kılar.

Her yeni teknoloji iki ucu keskin bir kılıç gibidir. Akıllı video gözetimi güvenlik ve suçla mücadelede önemli bir araç olarak kullanılırken, aynı zamanda bireylerin temel hak ve özgürlükleri bakımından önemli tartışmaları da beraberinde getirmektedir. Yapısı itibariyle önleyici ceza hukuku aracı olan kamera sistemleri, polisin belirli bir suç kapsamında bireysel bir adli izin olmaksızın pek çok kişisel veriye erişmesini de sağlar. Kişinin nerede, kiminle ve ne kadar süreyle konuştuğu ne yaptığı ne satın aldığı ne okuduğu ve hatta ne düşündüğü de bu verilere dahildir. Herhangi bir suç faaliyeti ile ilgili olmasa bile kamusal alanlar yedi gün yirmi dört saat izlenir ve kaydedilir. Bu yönüyle akıllı kamera sistemleri, koruma tedbirlerinin özellikleriyle bağdaşmaz. Koruma tedbirlerinde genellikle tedbire maruz kalan somut bir şüpheli veya sanık vardır. Fakat gelişmiş akıllı kamera sistemleri ile -özellikle dronelar gibi uçabilen nesnelerle-çok daha geniş alanlar kameralar tarafından izlenebilir ve yüz tanıma teknolojisi ile bölgedeki tüm insanların kimlik tespiti yapılabilir, veri tabanında eşleşme olduğunda sistem alarm üretebilir ve uyarıyı alan polis olaya müdahale edebilir.

Bir kişinin hareketlerinin ve yaşadıklarının kamuya açık alanda izlenmesi özel hayatın kendisine bir müdahale teşkil etmese de kamusal alandaki bu tür bilgilerin düzenli veya kalıcı olarak kaydı söz konusu olunca özel hayatla ilgili konular ortaya çıkabilir. Yani eğer izleme sistemli bir şekilde yapılıyorsa ve kayıt altına alınıyorsa bireyin özel yaşamına müdahale söz konusudur. Bu nedenle polis tarafından toplanan veriler, söz konusu bilgi müdahaleci veya gizli bir yöntemle toplanmamış olsa bile kişinin özel hayatına dahil bir bilgidir. Kişinin görüntüsünün yanı sıra yüz tanıma sistemi ile yüzünün, vücut kameraları ile de göz ve iris taramasının yapılması biyometrik veri toplandığı anlamına gelir. Bireyin kimliğini belirlemeyi sağlayan parmak izi, iris, DNA gibi biyolojik verileri gibi yüz verisi de biyometrik verilerden biridir. Bu sistem sadece yüz verilerini depolanmaz, aynı zamanda yapay zekâ sayesinde veri tabanında bulunan yüzleri değerlendirerek kimlik bilgileri eşleştirmesi yapılabilir, böylece hakkında yakalama kararı bulunan kişiler ve hatta potansiyel suçlular bile tespit edilebilir. Kişinin kamusal alanda kamelara yansıyan verilerinin toplanması kadar yok edilmemesi de bireylerin temel hak ve özgürlüklerine müdahale teşkil edebilir. Hakkında herhangi bir suç isnadı bulunmayan veya beraat kararı alan kişilerin kişisel verilerinin silinmemesi masumiyet karinesini ihlal edebilir. Bu nedenle, vücut kamerası

kullanımı da dahil olmak üzere Türkiye'de kameralı gözetim sistemlerinin izleme, kaydetme, saklama ve kullanılma sürecine ilişkin **açık**, **belirli** ve **denetlenebilir** kılan kanuni bir düzenleme yapılması gerekir. Bu çalışmada varılan sonuçlara göre yapılacak kanuni düzenlemede, aşağıdaki hususlara dikkat edilmesinde fayda bulunmaktadır:

(I) Kamusal alanda akıllı video gözetimi, kural olarak "izleme" ile sınırlı olmalıdır. Hem kapalı devre televizyon kameraları hem de vücut kameraları ile kural olarak sürekli kayıt yapılmamalıdır. Fakat suçüstü hali gibi istisnai bazı hallerde "kayıt altına almaya" izin verilebilir. Önleyici kayıt altına alma tedbirinin hangi alanda kullanılacağı, hangi katalog suçlar bakımından kaydın başlatılabileceği, tedbiri uygulayacak yetkili makam, görüntülerin saklama süresi ve yok edilme süreci düzenlemede belirtilmelidir. Ayrıca yapılacak bir kanunun ardından, bu kanuna dayanılarak çıkarılacak yönetmelikte de kameranın duruş ve izleme açılarına bağlı olarak görüntü alanına, gece-gündüz izleme zamanlarına, izlenecek alanıp aydınlatılıp aydınlatılmayacağına, insansız hava aracı, drone veya mobil araçlarla kayıt yapılıp yapılamayacağı hususlarına da yer verilmelidir. Ayrıca bu hususta bir denetleme kurulunun oluşturulması da gerekir. Kamu kurum ve kuruluşları, belediyeler ve üçüncü kişilerin kameralı gözetleme faaliyeti ile ilgili kurallara uyup uymadıkları bu kurul tarafından denetlenmelidir.

(II) Suçun önlenmesi amacıyla kamuya açık her alana kamera sistemi kurulması ölçülü bir müdahale değildir. Kamera sistemi kurulacak bölgedeki suç oranları ve suç türleri dikkate alınmalı, pilot uygulaması yapılarak kameranın bölgedeki suç oranlarını nasıl etkilediği takip edilmelidir. Kameralar "sınırlı alan uygulaması" ilkesine göre kurulmalıdır. Örneğin, bir tren garının veya havalimanının kamera sistemi ile takibi hukuka uygun olabilirken, bir mesire alanın takibi hukuka aykırı olabilir.

(III) Kamera yerleştirilen alanlara "Bu alan kamera sistemi ile izlenmekte, kaydedilmekte ve bu kayıtlar belirli bir süre saklanmaktadır." şeklinde uyarıcı levhalar yerleştirilmelidir. Akıllı kamera sistemlerine ilişkin kanuni düzenleme yapıldığında, önleyici bu tedbir kapsamında işlenen kişisel veriler KVKK m. 28 hükmü uyarınca istisna kapsamında olabilir. Yine de kamera sistemlerinin gizli olarak kullanılması hukuka aykırı olacağı için uyarıcı işaretler konulmalıdır ve yapılacak kanuni düzenlemede kameralı gözetim alanlarına yerleştirilen uyarı tabelaları ile vücut kamerası taşıyan polis memurlarının sırtlarında ve göğüslerinde kameralı gözetim yapıldığına dair uyarı yazısı taşımaları gerekliliği düzenlenmelidir.

(IV) Yüz tanıma teknolojisi akıllı video gözetiminin kritik bir parçasıdır. Görüntülerdeki kişilerin kimlik tespitine imkân veren bu teknolojisi, kitlesel gözetim tehlikesi ve yapay zekâ ön yargısı sebebiyle bireylerin temel hak ve özgürlüklerine müdahale teşkil edebilir. Bu nedenle Yapay Zekâ Yasası'na göre, CCTV görüntülerinden hedefsiz yüz görüntüleri toplanarak gerçek (eş) zamanlı biyometrik veri tanımlaması yapılması yasaklanmıştır (m. 5/1-e). Ancak *i)* insan kaçırma, insan ticareti veya cinsel sömürü mağdurlarına yönelik hedefli aramalar ile kayıp kişilerin aranması; *ii)* gerçek kişilerin yaşamına veya fiziksel güvenliğine yönelik belirli, önemli ve yakın bir tehdidin veya gerçek ve mevcut ya da gerçek ve öngörülebilir bir terör saldırısı tehdidinin önlenmesi; *iii)* en az dört yıllık azami bir süre için bir hapis cezası veya tutuklama emri ile cezalandırılabilen suçlar için bir ceza soruşturması veya kovuşturması yürütmek veya bir ceza infazı yapmak amacıyla bir suç işlediğinden şüphelenilen bir kişinin yerinin belirlenmesi veya kimliğinin belirlenmesi amaçlarıyla polis kamuya açık alanlarda gerçek zamanlı biyometrik tanımlama sistemi kullanabilir. Gerçek zamanlı biyometrik veri tanımlaması sadece bu amaçlar için, özel olarak hedeflenen kişinin kimliğini doğrulamak amacıyla kullanılabilir. Fakat yalnızca gerçek zamanlı uzaktan biyometrik tanımlama sisteminin çıktısına dayanarak bir kişi üzerinde olumsuz bir hukuki etki yaratan hiçbir karar alınamaz (m. 5/3). Eşleştirme ve tanımlama zamanlarının aynı olmadığı uzaktan biyometrik

veri tanımlaması bu yasağın dışında tutulmuştur. Uzaktan biyometrik tanımlama sistemleri "yüksek riskli" yapay zekâ sistemi olarak kabul edilmiştir (m. 6). Bu tür sistemlerin sadece çok sınırlı ve önceden yetkilendirilmiş birimler tarafından kullanılmasına izin verilmiştir.

(V) Ayrıca Yapay Zekâ Yasasının 70. maddesinde yapay zekâ sistemlerindeki ön yargıdan kaynaklanabilecek ayrımcılığa karşı başkalarının haklarını korumak için, yapay zekâ sağlayıcılarının belirli nitelikleri haiz kişisel verileri de işleyebilmesinin önünün açılması gerekliliği ifade edilmiştir. Dolayısıyla yüz tanıma teknolojisinin eğitildiği veri setinin, sistemin tasarlandığı amaç açısından yeterli temsil kabiliyetine sahip nitelikte ve mümkün olan en iyi ölçüde hatasız ve eksiksiz olması gerekir.

(VI) Kamera görüntülerinin veri aktardığı kontrol merkezlerinin denetimi kanunda düzenlenmelidir. Ana komuta merkezi ve veri kontrol merkezleri görüntülü olarak kayıt altına alınmalı, kayıtlara kimlerin ulaşabileceği ve tüm elektronik işlemlerin log kayıtları tutulmalıdır. Bu konuda yetkili personelin yetki ve sorumlulukları düzenlenmelidir.

(VII) Sadece kamu kurumlarının değil özel kişiler tarafından bireysel kullanım için kamusal alana kamera yerleştirebilme koşulları da kanunda açıkça düzenlenmelidir. Bu hususta Alman Federal Veri Koruma Kanunu § 6b hükmü yol gösterici olabilir. Düzenlemede kamuya açık alanlarda bireysel kamera kullanımına ancak doğrudan korunan bir hukuki menfaati bulunuyorsa izin verilebilir. Kamunun kullanımına açık alanlarla sınırlı bir şekilde güvenlik gerekçesiyle kamera sistemi kurulabilir. Fakat kamuya açık bu alan özel mülkiyete ait ortak kullanım alanı ise (örneğin, bir sitenin otoparkı) ilgili kişilerin (örneğin, tüm komşuların) rızaları alınmalıdır. Dolayısıyla bir apartman girişine güvenlik gerekçesiyle kurulan kamera sisteminin tüm sokağı izleyecek şekilde yerleştirilmesi hukuka aykırıdır.

Son olarak, teknik gelişmelerin hızı ve Türkiye'nin jeopolitik konumu da dikkate alındığında akıllı video gözetiminin suçla mücadelede etkili bir yöntem olabilir. Fakat güvenlik pahasına özgürlüklerin kısıtlanması da kabul edilemez. Bu nedenle, kamusal alanda akıllı video gözetimi ve yapay zekâ sistemlerinin kullanımı için gereken hukuki düzenlemelerin yapılması atılması gereken ilk adımdır.

Yazar Bilgileri Buket Abanoz Öztürk
[1] İstanbul Ticaret Üniversitesi, Hukuk Fakültesi, İstanbul, Türkiye
0000-0002-1886-2595 baozturk@ticaret.edu.tr

Kaynakça | References

Abanoz, B. (2018). *Kamusal Alanda Kameralı Gözetlemenin Suçun Önlenmesindeki Etkisi ve Elde Edilen Delillerin Hukuka uygunluğu Sorunu*, On İki Levha Yayıncılık.

Aktan, S. (2020). Dünyada en fazla güvenlik kamerasına sahip şehirler: İstanbul ilk 50'de, *Euronews*, Erişim: https://tr.euronews.com/2020/07/25/dunyada-en-fazla-guvenlik-kameras-na-sahip-sehirler-istanbul-ilk-50-de, 24.06.2024.

Bilgiç, E. T. (2023). Halka Açık Alanlarda Video Gözetim Bağlamında Kişisel Verilerin Korunması: Fransa Örneği. *Hacettepe Üniversitesi Hukuk Fakültesi Dergisi*, 13 (2), 414-457.

Bunn N., Cunningham, B. (2015). Which Data Should Police Body Cams Collect?. *The Atlantic*. https://www.theatlantic.com/politics/archive/2015/10/which-data-should-police- body-cams-collect/433197/. (Erişim: 30.06.2024).

Conrad C. S. (2016). Deutsche Bahn testet Body-cams. *Datenshutz Notizen*. https://www.datenschutz-notizen.de/deutsche-bahn-testet-body-cams-4415298/, (Erişim: 24.06.2024).

Conrad, C. S. (2017-a). Videoüberwachung 2.0- Neue Technik, Neue Probleme?. *Datenschutz Notizen.* https://www.heise.de/news/Deutsche-Bahn-will-intelligente-Videoueberwachung-testen-3631191.html, (Erişim: 24.06.2024).

Condrad, C. S. (2017-b). Rechtswidriger Bodycam-Einsatz der Polizei in Niedersachsen?, *Datenshutz Notizen*, https://www.datenschutz-notizen.de/rechtswidriger-bodycam-einsatz-der-polizei-in-niedersachsen-4217272/, (Erişim: 24.06.2024).

Çoban, E. (2005). Ülkemizin Modern Bilgi ve Güvenlik Konsepti MOBESE, *Çağın Polisi Dergisi*, 4(47, 36-38.

Çolak, H., Taşkın, M. (2007). *Ceza Muhakemesi Kanunu Şerhi*. Ankara. Seçkin Yayınevi.

Elmas, Ç. (2018). *Yapay Zekâ Uygulamaları. Yapay Sinir Ağı, Makine Öğrenmesi-Derin Öğrenme, Derin Ağlar-Bulanık, Mantık, Sinirsel Bulanık Mantık- Genetik Algoritma*. Seçkin Yayıncılık, Ankara.

Erdoğan, I., (2021). *Yapay Zekâ Teknolojilerinin Ceza Muhakemesinde Kişisel Veri Toplanmasına Etkileri*, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Doktora Tezi, İstanbul.

Eren, A. (2005). Özgürlükler Mekânı Olarak Kamusal Alan. *AÜEHFD*. IX (3-4), 95-124.

Grünwald, C. (2015). Vorsicht-die Polizei filmt mit. *Datenschutz Notizen*. https://www.datenschutz-notizen.de/vorsicht-die-polizei-filmt-mit-0910385/, (Erişim: 30.06.2024).

İçer, Z., Dönmez, E. (2020). Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları. *Ceza Hukuku Dergisi*, 15(43), 321-461.

Kannenberg, A. (2017). Deutsche Bahn will intelligente Videoüberwachung testen. *Heise Online*. https://www.heise.de/news/Deutsche-Bahn-will-intelligente-Videoueberwachung-testen-3631191.html, (Erişim Tarihi: 30.06.2024).

Karakehya, H. (2009). Gözetim ve Suçla Mücadele: Gözetimin Tarihsel Gelişimi ile Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*. 58(2), 319-358.

Karper, I. (2016). Datenschutz-Grundverordnung-Videoüberwachung. *Datenschutz Notizen*. https://www.datenschutz-notizen.de/datenschutz-grundverordnung-videoueberwachung-0014293/, (Erişim Tarihi: 02.09.2024)

Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*. Prof. Dr. İlhan Özay'a Armağan. 69 (1-2), 317-334.

Keçelioğlu, Elvan. (2015). Risk Toplumunda Ceza Hukukunun Değişen Yüzü. *AÜHF Prof. Dr. Nevzat Toroslu'ya Armağan*. Vol. 1. 627-638.

Kempe, L. (2024). Navigating the AI Employment Bias Maze: Legal Compliance Guidelines and Strategies. *American Bar Association*, https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-april/navigating-ai-employment-bias-maze/, (Erişim Tarihi: 17.08.2024).

Kesim, S., (2007). *Gözetim Toplumu ve Toplumsal Meşruiyet*, Mimar Sinan Güzel Sanatlar Üniversitesi, Yayınlanmamış Doktora Tezi.

Kızılırmak, B. (2019). Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi. *Kadir Has Üniversitesi Hukuk Fakültesi Dergisi*. 7(2). 225-261.

Kilkelly, U. (2001). *Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi'nin Uygulanmasına İlişkin Kılavuz*. İnsan Hakları El Kitapları. No. 1. Almanya.

Koca, M., Üzülmez, İ. (2023). *Türk Ceza Hukuku Genel Hükümler*. Ankara, Seçkin Yayıncılık.

Konukapay, C. (2023). Kişisel Verilerin Korunmasının Sınırları: İstisna Kapsamında Yer Alan Faaliyetler. *Kişisel Verilerin Korunması Çalışma Kitabı*. Ed. Gizem Gültekin Varkonyi, Kübra İslamoğlu Bayer. Seçkin Yayıncılık. Ankara.

Lobo, S. (2017). In fünf Jahren ist Ihe Gesicht Ihr Personalausweis. *Spiegel Netzwelt*, https://www.spiegel.de/netzwelt/web/kameraueberwachung-wird-zur-verhaltenskontrolle-a-1135744.html, (Erişim, 03.09.2024)

Mahmutoğlu, F. S. (2005). 5237 Sayılı Türk Ceza Kanunu'nda Hukuka Uygunluk Nedenleri. *Hukuk ve Adalet Eleştirel Hukuk Dergisi*, 2 (5). 42-60.

Murakami Wood, D., Steeves, V. (2021). Smart Surveillance. *Surveillance & Society*. 19 (2). 150-153.

Özbek, V. Ö., Doğan, K., Bacaksız, P. (2023). *Ceza Muhakemesi Hukuku*. Ankara. Seçkin Yayıncılık.16. Baskı.

Özkan, H. (2016). MOBESE izleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi. *CHD*. 30. 63-103.

Öztürk, B., Tezcan, D., Erdem, M., Sırma, Ö., Kırıt, Y., Özaydın, Ö., Alan, E., Erden, E. (2014). *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, Ankara.

Salzmann M., Schindler, S. (2018). Polizeiliche Gesichtserkennung in Strafverfahren in Deutschland. *ZD-Aktuell*. Heft 18. 06344.

Stahie, S. (2020). AI-controlled Camera Follows Bald Referes's Head Instead of the Ball. *Bitdefender*. https://www.bitdefender.com/blog/hotforsecurity/ai-controlled-camera-follows-bald-referees-head-instead-ball/, (Erişim, 03.09.2024).

Temel, A. (2009). *Suçun Önlenmesinde MOBESE Uygulaması*, Gazi Üniversitesi, Yüksek Lisans Tezi.

Torun, T., (2020). Jurgen Habermas'ın Kamusal Alan Kavrayışı: Rasyonel Politik İrade Oluşumu, *Kaygı. Bursa Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi*, 19 (1).

Töngür, A., İşbir, K., Öztürk, M., Alkan, Ö., Bilgin, H., Beşgül, B., Ayhan, Z. (2022). *Önleyici Polislik Tedbirleri*, Polis Akademisi Yayınları: 176, Rapor No: 79.

Şahin, M. E. (2012). *Ceza Hukukunda Rıza*. İstanbul, On İki Levha Yayınları.

Üzeltürk, S. (2004). *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı,* İstanbul, Beta Basım.

Wörner, L. (2024). "AI and Prevention of Crime, The German Perspective", The experimental French legal system fort he 2024 Paris Olympic and Paralympic Games, Article 10 of Law no. 2023-380 of 19 May 2023 on the 2024 Olympic and Paralympic Games, Konuşma Metni, s. 1-5, s. 2.

Yıldırım, E., (2013). *CCTV: Dünü, Bugünü, Yarını*. Ankara, Arkadaş Basım.

Zafer, H. (2010). *Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK 132-134),* İstanbul, Beta Yayıncılık.