YÜZ TANIMA TEKNOLOJİLERİNİN ÖNLEYİCİ CEZA HUKUKU VE CEZA MUHAKEMESİ SÜREÇLERİNDEKİ KULLANIMI VE SINIRLARI(*)

Dr. Öğr. Üyesi Zafer İÇER(**)
Elif DÖNMEZ(***)

Öz: Suç işlemek ya da daha genel bir ifadeyle üstün bir erk tarafından konulmuş norma karşı gelmek insanlık tarihi kadar eski bir davranış modelidir. İnsanoğlu yüzyıllardır suç işleyenleri cezalandırma yoluna giderek cezanın genel önleme amacını gerçekleştirmeyi hedeflemektedir. Bu hedef, potansiyel suçluların gözünü korkutmayı da içermektedir. Yaşanan tecrübeler ve gelişmeler, korunan hukuki değerleri ihlale yönelen eylemlerin, henüz gerçekleşmeden engellenmesinin önemini ortaya koymuştur. Önleyici sahada devletin suçla mücadelesinde en etkili enstrümanı teknolojidir. 20. yüzyıl sonlarında suçlunun teşhisi için kullanılmaya başlanan DNA testi; kapalı alanlara suç aleti sokulmamasını sağlayan x-Ray cihazları; gözetleme yoluyla suçu engellemeye ve suçluyu tespite yarayan CCTV, Mobese gibi kamera sistemleri cezai süreçlerde kullanılan teknolojilerin önde gelenleri olarak sayılabilir. Günümüzde ise önleme ve tespit faaliyetlerinde hızı artırmak ve hata payını en aza indirmek amacıyla başvurulan yüz tanıma teknolojileri, önleyici ceza hukukunun hatta ceza muhakemesi süreçlerinin önemli bir basamağı haline gelmiştir. Bu çalışmada yüz tanıma teknolojilerinin temel çalışma prensipleri, hukuki niteliği, temel hak ve hürriyetlerle ilişkisi, bu teknolojilerin kamu gücü tarafından kullanılmasına ilişkin göz önünde bulundurulması gereken ilkeler ve koşullar inceleme konusu yapılmıştır.

Anahtar Kelimeler: Yüz Tanıma, Yapay Zekâ, Hukuk, Önleyici Ceza Hukuku, Ceza Hukuku.

THE USE OF FACE RECOGNITION TECHNOLOGIES IN PREVENTIVE CRIMINAL LAW AND CRIMINAL PROCEDURE PROCESS AND LEGAL LIMITS

Abstract: It is an act as old as human history to commit a crime or to act against the norm set by a superior power. For centuries, mankind has been trying to achieve the aim of general prevention of crime. This aim also includes the indimidation of potential criminals. All experiences and developments have shown the importance of the obstruction of actions which breach protected legal values. In preventive area the most effective instrument of the state in its struggle against crime is technology. The DNA test, which was used in late 20th century for the identification of criminals; x-Ray devices which ensure that no crime tools are

(*) Makalenin Gönderim Tarihi: 09.05.2020,
Makalenin Kabul Tarihi: 21.07.2020.

(**) Marmara Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Usul Hukuku Anabilim Dalı,
E-posta: zafericer@marmara.edu.tr; Orcid no: https://orcid.org/0000-0002-2628-9055.

(**) Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku, Yüksek Lisans Programı Öğrencisi,
E-posta: ahevik@yahoo.com; Orcid no: https://orcid.org/0000-0002-2421-6434.

inserted into confined spaces; and camera systems such as CCTV or Mobese, which prevent crime and detect the criminal through surveillance can be counted as the leading technologies used in criminal processes. Today, face recognition technologies which are used in order to accelerate prevention and detection activities and to minimize the margin of error are becoming an important step in preventive criminal law and even criminal procedure processes. In this study, the basic working principles of facial recognition technologies, the legal nature of facial recognition, its relation with fundamental rights, and principles and conditions to be taken into consideration regarding the use of these technologies by the public power are subject to review.

Keywords: Face Recognition, Artificial Intelligence, Preventive Criminal Law, Criminal Law.

I. Giriş

Günümüzde hukuk devletlerinin temel amacı, toplumu oluşturan bireylerin huzur ve güvenlik içinde yaşamalarını temin etmektir. Bu doğrultuda devlete düşen pek çok ödev bulunmaktadır. Bunların başında da toplumu oluşturan bireylerin uyması gereken kuralları belirlemek; bireylerin hak ve hürriyetleri ile kamu düzen ve güvenliğini korumaya ve suç işlenmesinin önüne geçmeye yönelik tedbirleri hayata geçirmek yer almaktadır.

Esasen, rasyonel toplumu oluşturmak için koyduğu kurallara uyulup uyulmadığını ve kendi öngördüğü toplum düzenine karşı yasadışı birtakım faaliyetler yürütülüp yürütülmediğini denetlemek bu gerekliliğin doğal bir sonucudur. Bu nedenle devlet, belirtilen amaçlarla geçmişten bugüne her zaman bireyleri gözetleme eğiliminde olmuş[1], istihbarat ve espiyonaj faaliyetlerinde bulunmuştur. Teknolojinin gelişmediği eski dönemlerde bu denetleme, istihbari faaliyetler aracılığıyla "insan unsuru" temel alınarak hayata geçirilmiştir. Teknolojideki gelişmeler arttıkça, bu faaliyetlerde insan unsuru yanında çeşitli teknik araçların (örneğin ses ve görüntü kaydeden cihazlar) kullanımı da söz konusu olmuştur.

Günümüzde ise gelişen teknoloji ile birlikte bireylerin izlenmesi ve denetlenmesi; Mobese kameralar, uzaktan ses ve görüntü kaydına imkân veren teknik araçlar, yapay zekâ destekli sistemler, özellikle yüz tanıma teknolojileri, insansız hava araçları gibi teknik olanaklarla daha kolay bir hale gelmiştir. Teknolojinin gelişimi, temel hak ve hürriyetlere müdahaleyi kolaylaştırmakla birlikte, bu teknik imkanların sınırsız ve koşulsuz kullanılabilmesi mümkün değildir. Bu sebeple, yeni müdahale tarzlarının hukuki açıdan çerçeve içine alınarak sınır ve şartlarının tespit edilmesi, hukuk devleti olmanın bir gereğidir[2].

---

1 **Karakehya, Hakan,** "Gözetim ve Suçla Mücadele": Gözetimin Tarihsel Gelişimi ile Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme, Ankara Üniversitesi Hukuk Fakültesi Dergisi, c: 58, y: 2009, s. 2.

2 **Özbek, Veli Özer - Doğan, Koray - Bacaksız, Pınar,** Ceza Muhakemesi Hukuku, Ankara, 2019, s. 175.

Teknolojinin getirdiği olanaklar, suçla mücadele açısından devletin imkanlarını artırmış ve bunu oldukça basitleştirmiştir. Bunun bir yansıması olarak teknoloji, bilhassa önleyici ceza hukuku faaliyetleri açısından yaygın ve artan düzeyde bir kullanım alanına sahip olmaya başlamıştır. Keza ceza muhakemesi süreçlerinde de (bir takım koruma tedbirlerinde) bu imkanlardan belli ölçüde yararlanıldığını söylemek mümkündür.

Devletin suçla mücadele amacıyla kullanmaya başladığı yeni teknolojiler arasında yapay zekâ destekli yüz tanıma teknolojileri de bulunmaktadır. Yüz tanıma teknolojisi, yapay zekâ desteğiyle insan yüzünü tespit edip işleme koyarak sistem içerisinde var olan veriler ile karşılaştırmakta ve derin öğrenme *(deep learning)* metodu ile birtakım sonuçlar ortaya koyabilmektedir. Bu teknoloji, biyometrik[3] bir veri *(biometrische daten)* olan insan yüzünün makine tarafından okunabilir hale getirmesi ve böylelikle çok çeşitli kullanım alanları oluşturması sebebiyle, beden ve kimlik arasındaki bağlantı üzerinde geri dönülmez bir etki bırakmaktadır[4]. Bunun için sisteme belirli bir bölgede yaşayan milyonlarca insanın yüz verileri tanıtılmakta, sonrasında sistem derin öğrenme metoduyla çeşitli algoritmalar ışığında belirlenen parametreleri dikkate alarak şüpheli, tehlikeli şahısları tespit etmekte yahut hakkında yakalama kararı bulunan bir şüpheliyi belirleyerek kolluk güçlerinin harekete geçebilmesini sağlamaktadır.

Almanya'da 2007 yılından bu yana, Federal Kriminal Polis Bürosu, bilinmeyen kişileri tanımlamaya yarayan yüz tanıma sistemlerini test etmektedir[5]. Hamburg kentinde 2017 yılında yapılan G20 zirvesinde çıkan olaylarda yasal bir dayanağı olmadığı halde polis tarafından göstericilerin yüzleri kayıt altına alınmış ve biyometrik referans veri tabanı ile karşılaştırılmıştır. 2018 yılında ise "Berlin Südkreuz Güvenlik İstasyonu" pilot projesinin "Biyometrik Yüz Algılama" alt projesi kapsamında, Berlin Südkreuz istasyonunda polis aramalarını desteklemeye yönelik biyometrik yüz algılamanın uygunluğu, bir yıl boyunca gerçekçi koşullar altında test edilmiştir. Ancak bu esnada mevcut yasal duruma göre biyometrik yüz tanımaya normal operasyonlarda izin verilmemiştir[6].

G20 zirvesi sonrasında yüz tanıma sistemlerinin kullanımı yasadışı kabul edilerek, Alman Ceza Muhakemesi Yasası (StPO) çerçevesinde, herhangi bir sebep olmaksızın çok sayıda insanın uygulamaya muhatap edilmesi ve bunun

---

3 Biyometri, bireylerin davranışlarına ve biyolojik özelliklerine göre otomatik tanınması olarak tanımlanmaktadır. Bkz. **Coester, Ulla - Fuhlert, Bernd,** "Gesichtserkennung - eine Frage der Ethik?" Datenschutz und Datensicherheit, 2020/1, s. 48, 49.

4 **Thiel, Markus,** "Die Vermessung der Welt? - Zur Nutzung biometrischer Identifikationssysteme durch die Sicherheitsbehörden", Zeitschrift für Rechtspolitik, Heft 8, 2016, s. 220.

5 **Wendt, Kai,** "Rechtsgrundlage zur automatisierten Gesichtserkennung in Strafverfahren", ZD-Aktuell, Heft 19, 2018, 06364.

6 **Salzmann, Miriam - Schindler, Stephan,** "Polizeiliche Gesichtserkennung in Deutschland", ZD-Aktuell, Heft 18, 2018, 06344; **Thiel,** s. 219.

koruma tedbirlerinin belirli bir şüpheye dayanması ve ölçülülüğü gibi kriterlere uygun olmaması sebebiyle uygulamanın meşru kabul edilemeyeceği ifade edilmiştir. Yine de eyalet polis yasasında (BPolG § 23 Abs 4[7]; § 27 Satz 1 Nr. 2[8]) video kayıtlarının otomatik değerlendirilmesine yönelik spesifik düzenlemelerin olduğu, ancak bu düzenlemelerin de terörist saldırılar ya da savunmasız nesnelerin, suç odakları tarafından tehdit edilen olaylar gibi suç teşkil eden belirli davranış kalıplarının varlığı durumunda görüntülerinin otomatik değerlendirilmeye tabi tutulabilmesine imkân tanıdığı belirtilmiş ve bu düzenlemelerin yeterliliği tartışmaya açılmıştır[9].

Yukarıda da ifade ettiğimiz gibi, devletin uyguladığı bu gibi tedbirler ve özellikle bireylerin temel hak ve hürriyetlerine müdahale oluşturan uygulamalar, bir hukuk devletinde sınırsız ve koşulsuz olamayacağından, önleyici ceza hukuku ve ceza muhakemesi hukuku açısından gerek elverişliliği, gerekse işlevselliği ile kolluk güçlerinin, adli mercilerin işini kolaylaştırabilecek olan bu teknolojinin kullanımının hukuki açıdan belirli bir çerçeve içine alınması kaçınılmaz bir gereklilik olarak ortaya çıkmaktadır. Bununla beraber gerek dünyada, gerek Türkiye'de konuyla ilgili kapsayıcı hukuki düzenlemelerin bulunmadığı görülmektedir. Teknolojinin gelişme hızı göz önüne alındığında, teknolojik kurumlara hukuki düzlemde dayanak oluşturacak düzenlemelerin ivedilikle yapılması gerektiği açıktır. Bu çalışmada, yüz tanıma teknolojisinin kullanım alanları önleyici ceza ve ceza muhakemesi hukuku boyutuyla değerlendirilerek temel hak ve hürriyetler çerçevesinde bu teknolojinin kullanımının sınırları ve şartlarına ilişkin temel ilkeler tespit edilmeye çalışılacaktır.

II. Yüz Tanıma Teknolojileri, Avantaj ve Dezavantajları

Yüz tanıma, dijital bir görüntü ya da videodan bir insanın kimliğini teşhis etmeyi ya da doğrulamayı sağlayan, kişinin yüzünün bir kamera kullanılarak kaydedildiği ve daha önce kaydedilmiş bir veya daha fazla yüz görüntüsüyle karşılaştırıldığı sistemlerin genel adıdır[10].

---

7 "(...) Eğer bir kişi Federal Polis kurumunda, demiryolları kurumunda, hava taşımacılığı kurumu veya ticari havalimanında, anayasal bir kurumda veya Fedaral Bakanlıkta ya da sınır geçiş noktasında ya da hemen yakınında bulunuyorsa ve bu yerlerdeki kişi ya da nesnelerin doğrudan tehlike altında olduğu suçların işleneceği varsayımını haklı çıkaracak olgular varsa ve kişinin kimliğini risk durumuna veya kişiye dayalı kanıtlara dayanarak tespit etmek gerekirse, Federal Polis, bu kişinin kimliğini belirleyebilir."

8 "Federal Polis, otomatik görüntü kayıt ve kayıt cihazlarını, yasadışı geçişler veya sınırda güvenlik tehditleri veya § 23 Paragraf 1 No. 4'te atıfta bulunulan nesneler veya orada bulunan kişiler veya şeyler bakımından ortaya çıkan tehlikeleri tanımak için kullanabilir (...)".

9 **Heldt, Amelie P.,** "Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raums", MMR, Heft 5, 2019, s. 287; **Salzmann - Schindler,** 06344; **Dweres,** s. 24.

10 **Heldt,** s. 286; **Drewes, Michael,** "Videoüberwachung 2.5 - Biometrische Gesichtserkennung und intelligence Videoanalyse", Deutsches Polizeiblatt, 2020/1, s. 22.

Yüz tanıma sistemleri, Mobese sistemlerin çok daha gelişmiş versiyonları olup Mobese *(mobil elektronik sistem entegrasyonu)* sistemler; şehrin kalabalık yerlerine, kamusal alanlara, cadde ve meydanlara kurulan kameralar aracılığıyla güvenliğin sağlanması, suç işlenmesinin önlenmesine yönelik olarak kişilerin görüntülerini kayıt altına alır[11]. Bununla birlikte sistem, sabit ya da hareketli şekilde bizatihi görüntü ve ses kaydına ve bu verilerin otomatik olarak belirli bir merkezde toplanmasına imkân sağlar. Bu sistemlerin kullanılmasıyla elde edilen görüntü ve kayıtlar, gerektiğinde anlık ya da geriye dönük olarak yetkililer tarafından analiz edilerek kullanılır[12]. Buna karşılık aşağıda detaylı olarak inceleyeceğimiz üzere yüz tanıma sistemleri, yapay zekâ destekli sistemler olup yalnızca veri deposunda kayıtlı yüz verileri ile elde edilen referans verileri mukayese etmekle kalmaz, aynı zamanda sistem, oluşturulmuş algoritmalar sayesinde makine öğrenmesi metoduyla, istenen konularda belirli bir çıktı sağlar. Mobese sistemlere göre çok daha fonksiyonel olan bu teknolojinin en önemli avantajı, veri analizinin yapay zekalı sistem tarafından yapılabilmesidir.

Yüz tanıma, özü itibariyle üç basamaklı bir işlemler silsilesini içerir. Bunlardan ilki kayıttır *(enrolment)*. Uygulama ilk etapta, yüzleri kaydederek bir referans seti oluşturur. Çekilen görüntü yüz ifadeleri, göz yuvalarının üst kenarları, elmacık kemiklerinin etrafındaki alanlar ve ağzın yan kısımları gibi sürekli değişmeyen yüz özellikleri kullanılarak sayısallaştırılır. İkinci aşama tanımlama *(identifikation)* olup sistem tarafından elde edilen referans veri ile stoktaki veriler karşılaştırılır. Tanıma sırasında yüz belirlenerek karakteristik özellikleri hesaplanır. Karakteristik yüz özelliklerinin karşılık gelen referans özelliklerle karşılaştırılması, klasik görüntü işleme ve görüntü analiz yöntemleri kullanılarak gerçekleştirilir. Son aşamada ise bu eşleşmelerin doğrulaması *(verifikation)* gerçekleştirilerek sistem bir çıktı sağlar[13].

Yüz tanıma sistemlerinin en yaygın çalışma metotları, verilen görüntüden seçilen belli özellikleri bir veri tabanındaki yüzlerle karşılaştırmak olmakla beraber farklı yöntemler izleyen programlar da mevcuttur. Yüz tanıma, günümüzde bilgisayarlar tarafından hiçbir insanın yapamayacağı kadar hızlı yapılmaya başlanmış; başlangıçta bilgisayar uygulaması olarak ortaya çıkan yüz tanıma sistemleri mobil platformlarda ve robotikte de kullanılmaya başlanmıştır[14]. Dünyanın dört bir yanında yüz tanıma teknolojisi kullanan yazılımlar geliştirilmekle beraber ABD, Rusya, Çin, Japonya, İsrail ve Avrupa ülkeleri bu alanda öncü durumdadır[15].

---

11 **Özkan, Halid,** "Mobese İzleme ve Kayıtlarının Ceza Muhakemesi hukuku Açısından Değerlendirilmesi", Ceza Hukuku Dergisi, c: 11, s: 30, 2016, 63, 64; **Özbek - Doğan- Bacaksız,** s. 174.

12 **Özkan,** s. 64, 65.

13 **Drewes,** s. 23.

14 https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html, https://www.+nicid.eu/face-recognition/ (e.t.: 26.03.2020)

15 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (e.t.: 22.04.2020)

Günümüzde çok basamaklı kod kullanan güvenliğe ek olarak, her insanda mevcut olan ve zamanla değişmeyen biyometrik verilere dayalı biyometrik şifreleme seçenekleri giderek yaygınlaşmaktadır. Kimlik doğrulamasını ve güvenliği sağlamak amacıyla yapılan ve biyometrik verilerin kullanıldığı bu uygulamaların, her insanda mevcut olan bir karakteristiği konu edinmesi *(evrensellik),* bu karakteristiğin kişiyi açıkça tanımlaması *(teklik)* ve zaman içinde değişmeden kalabilmesi *(dayanıklılık)* ölçülerini taşıması gerektiği ifade edilmiştir[16].

Biyometrik verilere dayalı olarak ortaya çıkan bu teknolojilerin kullanımı daha çok, belirli yerlere girilmesi ya da belirli sistemlere erişim esnasında söz konusu olmaktadır. Uygulama çoğu zaman güvenliği sağlamaya yöneliktir. Örneğin hastanelerde, enerji santrallerinde, bankalarda, şirketlerde, askeri tesislerde, kuruma erişimi kontrol etmek için iris, yüz ve hatta damar taramasının şifreleme yöntemi olarak kullanıldığı bilinmektedir[17].

Günümüzde bu uygulamalardan en yaygın olanı parmak izi taraması olup çeşitli yerlere erişimin dışında mobil iletişim cihazlarında dahi parmak izi kullanımı yaygınlaşmış durumdadır[18]. Son dönemlerde mobil cihazlarda yüz tanıma (Face ID) teknolojilerine de yer verilmeye başlanmıştır[19]. Bu yolla cihaz sahibinin sisteme güvenli ve hızlı bir şekilde girişi sağlanmakta ve kişisel veriler koruma altına alınmaktadır.

Günümüzde giderek yaygınlaşan ve pek çok kişinin kullanımında bulunan bu cihazlarda, yüz tanıma teknolojisinin işleyişi ana hatlarıyla şu şekilde gerçekleşmektedir: Sisteme bir defa girişi sağlanacak yüz verisi doğrudan kullanıcı tarafından tanıtılır ya da sistem futbol maçları gibi kalabalık alanlarda yüzleri ayıklayarak kaydetmek suretiyle kendi veritabanını oluşturacak şekilde programlanır[20]. Elde edilen yüz verileri sistem tarafından gözler arasındaki mesafe, çene şekli gibi ayrıntılar analiz edilip matematiksel bir gösterime dönüştürülerek veritabanına kaydedilir ve giriş izni için kodlanır. Sonraki kullanımlarda, cihaz farklı bir yüzle karşılaşırsa, sistem erişim izni vermez.

Eğer, sonraki kullanım sırasında görüntülenen yüz verisi, daha önce tanıtımı yapılan yüz ile eşleşiyorsa, sistem cihaza ya daha önce belirlenmiş uygulamaya otomatik giriş izni verir. Böylelikle, cihaz ya da uygulama açısından güvenlik sağlanmış olur. Bu metot, güvenlik açısından oldukça elverişli olduğu gibi, hak sahibinin sisteme erişimini hızlandırması, kolaylaştırması ve bilhassa veri güvenliğinin maksimum

---

16 **Thiel,** s. 218.

17 **Rottmeier, Christian - Eckel, Philipp,** "Die Entschlüsselung biometrisch gesicherter Daten im Strafverfahren", NStZ., Heft 4, 2020 s. 194; **Thiel,** s. 218.

18 **Rottmeier - Eckel,** s. 194; **Coester - Fuhlert,** s. 49.

19 https://support.apple.com/en-us/HT208108 (e.t.: 22.04.2020)

20 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (e.t.: 22.04.2020).

düzeyde sağlanması bakımından oldukça işlevseldir. Bu teknik, ayrıca özel nitelikteki iş yerlerine, belirli odalara, bilgisayarlara giriş açısından da kullanılabilmektedir.

Bazı sistemler ise sisteme ilk kez gösterilen kişi ile sistemin veritabanında kayıtlı olan kişiler arasındaki eşleşme olasılığını hesaplamak üzere geliştirilmiştir. Bu sistemler tek bir eşleşmeye işaret etmez ve kullanıcıya birkaç potansiyel eşleşme sunar[21]. Bu durumda sistemin tespit ettiği potansiyel eşleşmelerin manuel olarak ayıklanması gerekir.

Yüz tanımada belirli özelliklerin tespit edildiği örüntü tanıma, farklı değişkenler arasındaki ilişkiyi gösteren ve yüzlerin bireysel olarak sınıflandırılabilmesine imkân tanıyan fizyo(g)nomiye dayanan ayrım analizi gibi çeşitli yöntemler kullanılabilmektedir. Makine öğrenimi yoluyla yüzlerde tekrar eden kalıpları bağımsız olarak tanımlamayı öğrenmek için farklı insanların on binlerce görüntüsünün kullanılması sayesinde son yıllarda önemli gelişmeler kaydedilmiştir[22].

Yüz tanıma, iki boyutlu ya da üç boyutlu olarak gerçekleştirilebilir. İki boyutlu yöntemler, yüzün önemli kısımlarının boyutlarını ve birbirinden uzaklığını kaydeder. Sonrasında bu veriler, bir algoritma ile analiz edilerek üç boyutlu hale getirilir; bu yolla maliyet azalır ve güvenilirlik artar[23]. Yüzler, bir veri tabanıyla mukayese edilerek gerçek zamanlı tanımlama için yüz tanıma ve veri analizinin birleştirildiği *Viola Jones*[24] algoritması kullanılır. Bu sistem, yüzler arasındaki benzerlikleri bulmak için makine öğrenmesi metodunu kullanır[25].

Üç boyutlu çekimin yapılabildiği ilk dönemlerde, yüzün önden görülemediği durumlarda tespitin başarı oranının düşebileceği ve hata payının daha fazla olduğu ifade edilmişse de sistemin mükemmelleştirilmesine yönelik olarak frontal görüntü olmamasına rağmen tanımayı sağlayabilecek multibiyometrik yönteme ilişkin çalışmaların devam ettiği ifade edilmektedir[26].

Büyük kalabalıklar içindeki bireylerin tanımlanması otomatik olarak yapılabilmektedir. Bu amaçla, bireylerin hali hazırda elde edilmiş biyometrik referans verileri ile daha önce veri tabanına kaydedilmiş olan çok sayıda biyometrik arasında karşılaştırma yapılmaktadır. Bu karşılaştırmanın amacı, biyometrik referans veri kaydı kaydedilmiş verilerle eşleşen bireyi filtrelemektir[27].

21 https://www.eff.org/pages/face-recognition (e.t.: 26.03.2020).

22 **Coester - Fuhlert,** s. 49.

23 **Streed, Michael W.,** Creating Digital Faces for Law Enforcement, Amsterdam, 2017, s. 301-311.

24 2001 yılında Paul Viola ve Michael Jones tarafından geliştirilmiş bir yüz algılama teknolojisidir. Bu algoritmanın diğer algoritmalardan farkı doğruluk oranı yüksek bir tanımlama yapabilmesi ve saniyede 15 kare ile insan gözünün yakalamayacağı bir süratle gerçek zamanlı çalışabilmesi olarak ifade edilmektedir. Ayrıntılı bilgi için bkz. https://medium.com/patron-ai/viola-jones-algoritması-ile-yüz-tespiti-türkçe-38ea73c910e3 (e.t. 24.04.2020)

25 **Heldt,** s. 286.

26 **Heldt,** s. 286.

27 **Coester - Fuhlert,** s. 49.

Yüz tanıma teknolojisinin, kamu gücü tarafından kullanıldığı en önemli alan suçla mücadeledir. Tüm dünyada ülkelerin iç güvenliklerini sağlama amacı, özellikle son yıllarda terör eylemlerinde meydana gelen artış, önleyici ceza hukukunun *(preventive criminal law)* gelişmesi[28] ve suç işlendikten sonra değil, suç işlenmeden önce etkin tedbirlerin alınması yönündeki genel eğilim, bu teknolojilerin güvenlik alanında kullanılması gerekliliğini beraberinde getirmiştir. İngiltere yüz tanıma teknolojilerini "hayati" ve "mükemmel bir silah" olarak tanımlamakta[29], Amerika ise sistemin "kolluk süreçlerinde paha biçilemez" olduğunu ifade etmektedir[30].

Kamu gücü tarafından yüz tanıma teknolojileri aracılığıyla alınacak tedbirler, her şeyden önce kamu güvenliği ve kamu düzeninin sağlanmasıyla ilgilidir. Bununla birlikte, masum bireyler, yüz görüntülerinin kamusal alanlarda biyometrik olarak kaydedilmesi dolayısıyla bu uygulamadan etkilenmektedir[31]. Uygulamayla özellikle kamuya açık alanlarda, işlek cadde ve kalabalık meydanlarda, önemli geçiş güzergâhlarında, insanların toplu olarak bulundukları yerlerde, ulaşım istasyonlarında, büyük alışveriş merkezlerinde ve buna benzer diğer dış mekânlarda yüksek çözünürlüklü kameralar aracılığıyla öncelikle güvenliğin sağlanması hedeflenmektedir[32]. Kamusal merciler bakımından önlemeden sonraki hedefin bu teknolojiler yoluyla suç şüphelisinin tespit edilebilmesi, bunun da ötesinde potansiyel suçluların tespit edilmesi olacağında şüphe yoktur[33].

Bu amaçlara özgülenmiş yüz tanıma teknolojisinin işleyişi de temelde aynı olup, belirli bir kamusal alana yerleştirilen sabit ya da hareketli (mobil) kameralar, o yerden geçmekte olan kişilerin yüz verilerini işleyerek veri tabanına aktarmakta ve sisteme daha önceden tanıtılmış yüz verisiyle bu veriler mukayese edi-

---

28 **Bozbayındır, Ali Emrah,** "The Advent of Preventive Criminal Law: An Erosion of the Traditional Criminal Law?" Criminal Law Forum-The Official Journal of the Society fort he Reform of Criminal Law, vol: 29, no: 1, 2018, s. 35-48.

29 https://www.gov.uk/government/speeches/surveillance-camera-commissioners-ifsec-speech (e.t.: 26.03.2020).

30 **Ashby, Matthew P.J.,** "The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis", European Journal on Criminal Policy and Research, y. 2017, vol. 23, s. 1.

31 **Heldt,** s. 286, 287.

32 **Piza, Eric L. - Welsh, Brandon C. - Farrington, David P. - Thomas, Amanda L.,** CCTV Surveillance for Crime Prevention, vol. 18, issue: 1, 2019, s. 135-159.

33 Günümüzde de pek çok farklı alanda kullanılan yüz tanıma sistemlerinin, teknolojideki gelişmelerle birlikte özellikle "suç işlenmesinin önlenmesi" konusunda kullanımının dünya çapında giderek yaygınlaştığı görülecektir. 2020 yapımı bir Netflix bilimkurgu dizisi olan "The Omniscient" bu konuya yönelik distopik bir anlatı yaratmakta ve her bireyin yüz tanıma teknolojisiyle geliştirilmiş çok küçük drone'lar aracılığıyla takip edildiği, bireyin yapay zekâ üzerinde tanımlı suça yönelik hareketlerden birinde bulunması halinde drone'unun harekete geçerek ilgili makamları haberdar ettiği ve böylelikle kişilerin suç işlemesinin engellendiği, suç işleyenlerin ise doğrudan suçüstü yakalandığı bir evrenden bahsetmektedir. Dizide bahsedilen teknolojilerden çoğu yakın geçmişte geliştirilmiş olduğundan böyle bir düzenin hayata geçmesi teknik olarak imkânsız değildir, dolayısıyla hukuki regülasyonların bu teknolojilerin kullanımı göz önüne alınarak geliştirilmesi gerekecektir.

lerek eşleşme olması ya da sistemin şüpheli bir durum tespit etmesi halinde, ilgili şahıs ya da şahıslar hakkında önleyici/adli tedbirler ilgili mercilerce hayata geçirilebilmektedir. Veriler sisteme kullanıcı tarafından aktarılabileceği gibi sistem doğrudan yapay zekâ desteğiyle sosyal medyadaki görseller, trafik kameraları ve doğrudan sahada çekilen fotoğraflar üzerinde de araştırma yapabilmektedir[34].

Yüzleri karşılaştırabilmek için, yüzdeki kişisel özelliklerin birbiriyle mukayese edilmesi gerekir. Bu mukayese, ilk etapta yüzün ölçülmesi, özelliklerin ağırlığının, derinliğinin ve genişliğinin tespit edilmesiyle mümkün olmaktadır. Bu amaçla kullanılan yazılım, görüntü veya videodaki yüzleri ilk adımda tanıyan ve sonrasında bunları ölçerek makine tarafından okunabilen şablonlar olarak isimlendiren bir "desen tanıma" sistemini kullanır. Bu veriler sonrasında mevcut ve ayrıca makine tarafından okunabilir görüntülerle mukayese edilir. Sistemin yaptığı analiz belirli bir isabet oranıyla rapor edilerek, son değerlendirme için uzmana sunulur[35].

Öte yandan, sistemler yalnızca yüz verilerini kullanmamakta, ayrıca yapay zekâ desteği ile yüz verileriyle kimlik bilgilerini eşleştirerek, sistemde mevcut olan bu kimselere ilişkin tüm verileri değerlendirmekte, bu doğrultuda potansiyel bir suçluyu tespit ederek kolluk güçlerine bu konuda bir uyarı dahi yapabilmektedir.

Yukarıda da belirtildiği üzere yüz tanıma sistemlerinden pek çok farklı alanda yararlanılmasına rağmen sistemlerin hala güvenilmeyen veya eksik bulunan yanları da mevcuttur. Bu dezavantajlı alanlar şöyle sıralanabilir:

i) Hata riski: Güvenilir yüz algılama, bir görüntüdeki konum, çözünürlük, boyut, ölçeklendirme, harici aydınlatma efektleri gibi temel faktörlerin değişmez olmasını gerektirir. Bu sebeple, yaş, ten rengi, cinsiyet, farklı yüz ifadeleri, çeşitli aksesuarların varlığı algılama ve tanımayı zorlaştırır[36]. Yüz tanıma sistemlerinin henüz teknik olarak kesin nitelikli analizler yapabilecek ölçüde gelişmediği ve bu sebeple parmak izi, şifre gibi diğer güvenlik unsurlarından farklı olarak yüz tanımanın kesin veriler ortaya koymadığı ifade edilmiştir. Bilhassa, görüntünün ön taraftan alınamadığı, ışık ya da hava koşulları gibi dış faktörlerin yeterli olmadığı durumlarda sistemdeki hata payının daha fazla olacağı belirtilmiş, yine kişilerin yüzlerini atkı, fularla kapatmaları, ceket yakasını dik tutmaları gibi, yüzü kısmen ya da tamamen kapatan aksesuarların kullanılmasının tanımayı zorlaştırabileceği kaydedilmiştir[37]. 2018 yılında Almanya'da yapılan pilot uygulama kapsa-

---

34 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (e.t.: 26.03.2020).

35 **Wendt,** 06364; **Thiel,** s. 219.

36 **Dweres,** s. 23.

37 European Union Agency, Facial Recognition Technology: Fundamental Rights Considerations in the Contect of Law Enforcement, s. 4; Coester - Fuhlert, s. 50.

mında Federal Polis tarafından hazırlanan raporda, yüz tanıma sistemlerinin polis faaliyetlerinde önemli bir destek aracı olabileceği belirtilmekle birlikte, yüz tanıma sisteminin dış faktörlerden etkilenebildiğine ve hata payının olabileceğine dikkat çekilmiş, özellikle aydınlatmanın, olumsuz ışığın neden olduğu gölgelerin ve arka aydınlatmaların, sistemin başarısını olumsuz yönde etkilediği tespitine yer verilmiştir. Bununla beraber Raporda, en isabetli sonuçların ön yüz çekimlerinden elde edildiğine vurgu yapılmıştır[38]. Yapılan araştırmalar görüntü üzerinde birkaç piksellik küçük değişikliklerin bile yapay zekanın gördüğünü tamamen farklı bir şekilde yorumlaması için yeterli olduğunu göstermektedir. Zira yapay zekâ, insanlardan farklı olarak görüntüyü işlerken detaylarla temel yapıyı eşdeğer önemli kabul edebilmekte, ayrıca harfleri veya rakamları okumaksızın sadece görüntülerdeki pikseller arasında iletişim kurmaya çalışmakta; örneğin oldukça büyük karışıklıklara yol açabilecek şekilde üzerine birkaç kısa çizgi eklenmiş "dur" işaretini hız sınırı olarak algılayabilmektedir[39]. Bu sorunların çözümü için yapay zekâ algoritmalarının daha iyi geliştirilmesi gerekmektedir. Bu alandaki çalışmalarda hızla aşama kaydedildiği ve sürekli yeni tekniklerin ortaya çıktığı göz önünde bulundurulduğunda hata payının her geçen gün azalacağına şüphe bulunmamaktadır.

ii) Biyometrik verilerin sisteme alınması: Sistem, tanımayı veya tespiti yapabilmek için yüz verisini öncelikle kaydetmekte, bu durum da bir güvenlik açığı halinde veriyi ulaşılabilir hale getirmektedir[40]. Sistem veriyi kaydettiğinden ve depoladığından, sisteme dışarıdan yapılacak hukuka aykırı müdahaleler, bu verilere kötü niyetli kimselerin erişmesi tehlikesini beraberinde getirmektedir.

iii) Önyargılı analizler: Yaygın kanı, yüz tanıma sistemlerine ait veri tabanlarının ilk etapta beyaz ırktan insanların yüzleriyle oluşturulduğu ve sistemin sonradan diğer ırkları tanımakla ilgili daha fazla hata yaptığı yönündedir[41]. Bilhassa kamuoyunda son dönemlerde, bazı büyük şirketler (Google, Amazon, Uber gibi) tarafından çeşitli amaçlarla kullanılan yüz tanıma uygulamalarının ırkçı analizlerde bulunduğu yönünde iddialar gündeme gelmiştir[42].

---

38 **Salzmann - Schindler,** 06344; **Thiel,** s. 219.

39 **Szegedy, Christian - Zaremba, Wojciech - Sutskever, Ilya - Bruna, Joan - Erhan, Dumitru - Goodfellow, Ian - Fergus, Rob**, Intriguing Properties of Neural Networks, International Conference on Learning Representations, 2014, (https://arxiv.org/abs/1312.6199); **Ocak, Mahir E.,** "Yapay Zekayı Kandırmak", Bilim ve Teknik, y: 53, s: 62, Aralık, 2019, s. 28-36.

40 https://www.electronicid.eu/en/blog/post/biometric-facial-recognition/en (e.t.: 30.03.2020)

41 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (e.t.: 30.03.2020).

42 https://www.bbc.com/turkce/haberler-dunya-39599214 (e.t.: 07.05.2020); https://nayn.co/amazona-irkcilik-suclamasi-yuz-algilama-servisi-cinsiyetci-ve-irkci/ (e.t.: 07.05.2020); https://www.sabah.com.tr/dunya/2018/07/31/abdde-yuz-tanima-teknigi-irkci-cikti (e.t.: 07.05.2020).

iv) Kesin olmayan (ihtimale dayalı) analizler: Yüz tanıma algoritmaları, tanınan yüzün sistemdeki yüzle eşleştiği ya da eşleşmediği yönünde iki olasılık üzerinden hareket etmekte olup kesinlik arz etmemektedir. Bu noktada karşılaşılan iki temel hata "yanlış pozitif" ve "yanlış negatif" durumlarıdır. "Yanlış pozitif" halinde sistem algıladığı yüzü veri tabanında bulunan bir başka yüzle eşleştirmektedir. "Yanlış negatif" halinde ise sistem gerçekte bir eşleşme bulunmasına rağmen eşleşme olmadığı yönünde karar vermektedir[43]. Hata oranları fotoğraf kalitesinin de etkisi bulunmaktadır. Bu bağlamda algoritmaların hiçbir zaman kesin sonuç ortaya koymadığı, hata payının olduğu, bu nedenle en azından günümüzdeki teknolojik seviyede insan kararının devreye girmesinin zorunlu olduğu ifade edilmektedir[44]. Algoritma ile insan kararını bir araya getirebilmek adına kullanılacak yöntem, bir sayısal eşik belirleyerek algoritmanın eşleşme için verdiği kesinlik oranının bu eşiğin altında kalması halinde insan faktörünü devreye sokmak olabilir.

III. Yüz Verisinin Hukuki Niteliği

Toplumu oluşturan insanlar, sosyal yaşamda belirli bir öneme ve değere sahiptir. Bu değer, kişilerin toplum nezdinde "birey" olarak ortaya çıkmasından ileri gelmektedir. Toplumları oluşturan ve düşünsel, duygusal, iradeyle ilgili nitelikleri toplum içinde belirlenen insanların her birini ifade eden[45] birey kavramı, insanın kendine özgü ayırıcı özelliklerine vurgu yapan bir kavramdır. Aynı zamanda bu kavram, hukukun ve demokrasinin egemen olduğu toplumlarda, kendini ifade edebilme, hukukun kendisine tanıdığı hak ve imkânları özgürce kullanabilme yetisine sahip olan insanların, birbirleriyle ve devletle ilişkilerinde konumlandırıldığı statüyü de ifade eder.

Bireyi esas alan demokratik bir hukuk devletinde, bireyi bireyden ayırmaya yarayan, bireyin diğer bireylerle olan şahsi, sosyal, ticari, mesleki ilişkilerine ve devletle olan ilişkilerine esas teşkil edecek, bireyin kim olduğunu ortaya koyabilecek, onu diğer bireylerden ayırt edebilecek bir "kimliğe" ihtiyaç duyulduğu kuşkusuzdur. Esasen bireyi diğer bireylerden ayıran bu kimlik ve bu kimliği sembolize eden bireye ait tüm bilgiler, kişisel verilerin özünü oluşturmaktadır[46].

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3'üncü maddesi, Türkiye'nin 1981'de imzaladığı ve Türkiye bakımından 2016'da yürürlüğe giren

---

43 **Dweres,** s. 23.

44 European Union Agency, Facial Recognition Technology: Fundamental Rights Considerations in the Contect of Law Enforcement, s. 4.

45 Güncel Türkçe Sözlük, https://sozluk.gov.tr/?kelime= (e.t.: 30.03.2020).

46 **Göçmen Uyarer, Sinem,** Kişisel Verilerin Korunması, Ankara, 2019, s. 104; **Bük, Alaattin,** Bilişim Alanında Kişisel Verilerin Korunması, Ankara 2018, s. 33; **Sert, Şeyma,** Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara, 2019, s. 21-25; **Korkmaz, İbrahim,** Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara, 2019, s. 25-30.

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne[47] (108 no.lu sözleşme) paralel olarak kişisel veriyi *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlamıştır. Kişisel veri, Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GDPR) ise; *"tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tarif edilmiştir. Tüzüğe göre, tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir. Bu tanımlardan hareketle, "kişisel veri" kavramını; "bireyin şahsi, ailevi, mesleki durumlarını, özelliklerini içerisinde barındıran, bireyi diğer bireylerden ayırt etmeye elverişli her türlü bilgi" olarak tanımlamak mümkündür.

Kişisel veriye ilişkin yapmış olduğumuz bu tanımlamalar çerçevesinde, bireye ilişkin yüz hatlarının, yüz yapısının, jest ve mimiklerin kişisel veri niteliğinde olduğuna şüphe yoktur. Yüz verisi, bireyin biyolojik yapısına ilişkin bir veri olduğundan, bu veri *"biyometrik veri"* olarak adlandırılmaktadır. Biyometrik, ilgilinin fizyolojik ve davranışsal niteliklerini işleyip değerlendirerek, kimliği belirleyebilmek amacıyla oluşturulmuş program ya da sistemlerin bütünü için kullanılan çerçeve bir terimdir[48]. Bireyin kontrolü ve kimliğinin belirlenmesini sağlayan yöntemler, bireye ait retina, parmak izi, iris, DNA gibi biyolojik verileri esas almaktadır. Yüz verisi de bu biyolojik verilerden biri olup, bireyi belirlemeye yarayan en önemli araçlardan biridir. Avrupa Birliği'nin, kişisel verilerin korunmasına ilişkin regülasyonlarında yüz verisinin biyometrik veri olduğu belirtilmektedir[49]. GDPR[50] uyarınca bir fotoğrafın, fotoğrafı çekilen kişinin teşhisi amacıyla teknik araçlarla işlenmesi halinde basit fotoğraftan farklı bir "biyometrik veri" ortaya çıkmaktadır[51]. Avrupa Birliği Adalet Divanı da bir kimsenin kamera ile kaydedilen görüntüsünün ilgili kişinin teşhis edilmesine olanak sağlaması sebebiyle kişisel veri teşkil ettiğine hükmetmektedir[52].

---

47 Sözleşmenin tam metni için: https://humanrightscenter.bilgi.edu.tr/media/uploads/2016/03/29/KisiselVerilerinOtomatikIslemeTabiTutulmasiKarsisindaBireylerinKorunmasiSozlesmesi.pdf (e.t.: 02.04.2020)

48 **Akgül, Aydın,** Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı, Türkiye Barolar Birliği Dergisi, y. 2015, sayı: 118, s. 201.

49 Data Protection Working Party, Article 29, 00720/12/EN WP193, Opinion 3/2012 on developments in biometric technologies.

50 The General Data Protection Regulation.

51 GDPR, Recital 51.

52 Rynes v. Romanya, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212 (e.t.: 30.03.2020).

Biyometrik veriler, bireyin kimliğini belirmeye doğrudan yarayan, biyolojik, fizyolojik ve davranışsal özelliklerini oluşturan veriler olduğundan, özel bir kategori altında incelenmektedir. Nitekim 6698 sayılı Kanun'un 6'ncı maddesi, kişiye ait biyometrik verileri özel nitelikli kişisel veriler olarak kabul etmiş ve bu nitelikteki verilerin işlenmesini daha ağır koşullara tabi tutmuştur[53].

Buna göre, özel nitelikleri itibariyle biyometrik verilerin işlenmesi kural olarak ilgilinin açık rızasının alınmış olması şartına bağlanmış, ancak maddenin 3. fıkrasında sağlık ve cinsel hayata ilişkin olanlar dışındaki kişisel verilerin kanunlarda öngörülen hallerde açık rıza bulunmaksızın da işlenebileceği düzenlenmiştir. Örneğin, kolluk tarafından bir suç soruşturması sebebiyle, 2559 sayılı PVSK'nın 5. maddesi uyarınca şüphelilerin parmak izlerinin alınması, 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığı'nın kişilerin ceza mahkûmiyetlerine ilişkin verilerini işlemesi gibi durumlarda açık rıza aranmayacaktır[54]. Buradan hareketle bir mevzuatta öngörülmüş olması durumunda biyometrik veri niteliğindeki yüz görüntüsünün de kişinin açık rızası alınmadan işlenebileceği söylenmelidir.

Almanya'daki uygulamalar yönünden, StPO. §§ 161[55], 163[56], 483[57]'üncü paragraflarının verilerin işlenmesi için yeterli bir yasal dayanak teşkil ettiği Emniyet ve Savcılık Teşkilatı tarafından yapılan açıklamalarda ifade edilmiştir. Özellikle,

---

53 *"Özel nitelikli kişisel verilerin işlenme şartları*

MADDE 6- (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."

54 https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu (e.t.: 28.03.2020)

55 Maddenin birinci fıkrası, savcının genel soruşturma yetkisinin düzenlemektedir. Maddeye göre, savcı tüm makamlardan bilgi talep edebilir, her türlü soruşturmayı kendisi ya da kolluk güçleri marifetiyle yapmaya yetkilidir. (Karş. CMK m.160, 161). Maddenin 3. fıkrasına göre, Kanun uyarınca bir önleme sadece belirli suçlardan şüphe edilmesi dolayısıyla izin verilirse, diğer yasalar uyarınca karşılık gelen bir önlem temelinde elde edilen kişisel veriler, cezai süreçlerde, kişilerin rızası olmadan bu tür suçları araştırmak için kullanılabilir. 4. fıkraya göre, teknik araçların kullanımından elde edilen kişisel veriler, yalnızca orantılılık ilkesine uygun olarak kanıt amacıyla kullanılabilir.

56 163. madde, polisin soruşturma süreçlerindeki yetkisine ilişkin düzenlemeler içermektedir.

57 483. madde kişisel verilerin işlenmesine ilişkin olup mahkemelerin, kolluk kuvvetlerinin, denetimli serbestlik görevlilerinin, yönetim denetimi altındaki denetim makamlarının ve adli yardım da dahil olmak üzere, cezai işlemler için gerekli olduğu sürece dosya sistemlerindeki kişisel verileri işleyebileceği düzenlenmiştir. Maddenin 2 ve 3'üncü fıkrası ise, verilerin kullanılabilirliği ve saklanmasına ilişkin düzenlemeler içermektedir.

makine tarafından okunabilen veri şablonlarının kişisel bir referansının olmadığı ve bu nedenle veri koruma yasasının bu gibi durumlarda ihlal edilmiş olmayacağı, yüz tanıma sistemlerinin yalnızca bir yardım olduğu ve bireyin temel hakkına yönelik yoğun bir tecavüzün söz konusu olmadığı ifade edilmiştir[58]. Bununla birlikte Hamburg Veri Koruma ve Bilgi Özgürlüğü temsilciliği tarafından yapılan hukuki incelemede, polis ve savcılık tarafından belirtilen yasal dayanakların yalnızca sanıklar hakkında uygulanabileceğinden bahisle yeterli olmadığı görüşü dile getirilmiş, görüntü ve video dosyalarının otomatik değerlendirilmesine imkân tanıyan bir yasal dayanağın mevcut olmadığı belirtilerek, uygulamanın bu haliyle Veri Koruma Yasası'nı ihlal ettiği bildirilmiştir[59].

İngiliz hukukunda ise Police and Criminal Evidence Act § 64-A uyarınca polisin kural olarak polis merkezinde fotoğraf çekme yetkisinin bulunduğu, polis merkezi dışında fotoğraf çekilebilmesinin ise ancak kişinin tutuklanması, gözaltına alınması gibi belirli hallerde mümkün olduğu hüküm altına alınmış olup bu haller dışında polisin kamusal alanda çekim yapabilmesine olanak tanınmamıştır. İngiltere'deki uygulama bakımından ise, İngiliz polisinin 2017'de yüz tanıma sisteminin veri tabanına koruma amacıyla zihinsel sağlık sorunları bulunan kişileri dahil etmiş olması hassas nitelikli kişisel verilerin işlenmesi tartışmasını beraberinde getirmiştir[60]. Bu sebeple ICO[61], yüz tanıma teknolojisinin kullanımıyla ilgili regülasyonlar yapılarak hukuki zemin oluşturulana kadar İngiliz polisini teknolojilerin kullanımını yavaşlatmaya davet etmiştir[62].

IV. Yüz Tanıma Teknolojisinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Uygulama Alanları

Büyük şehirlerdeki nüfusun artışıyla birlikte, suçla mücadele gitgide zorlaşmıştır. Özellikle 21. yüzyılın başında yaşanan global terör hadiseleri pek çok ülkede yeni güvenlik önlemlerinin hayata geçirilmesini zorunlu kılmıştır. Pek çok ülke bu çerçevede yasal düzenlemeler getirmiştir. Son birkaç yılda ise yapay zekâ teknolojisindeki gelişmeler bu alandaki güvenlik tedbirlerinde de değişime ve çeşitliliğe yol açmıştır. Bu değişimin getirdiği en önemli uygulamalardan biri de yüz tanıma teknolojisidir.

Yüz tanıma, bireyin doğrudan kişisel verileriyle ilgilidir. Bir kimsenin yüz hatları, burun, ağız, kulak şekli, göz rengi gibi yüze ait unsurlar ve özellikler hiç

---

58 **Wendt,** 06364.

59 **Wendt,** 06364.

60 Big Brother Watch, Face Off: The Lawless Growth of Facial Recognition in UK Policing, 2018, s. 16.

61 International Communities Organisation.

62 https://www.research-live.com/article/news/police-should-slow-down-facial-recognition-says-ico/id/5061042 (e.t.: 30.03.2020).

şüphesiz kişisel veri niteliğini taşımaktadır. Bu açıdan yüz tanıma teknolojisinin kullanımının hukuki açıdan incelenmesi önem arz etmektedir. Bu kullanımın çeşitli sınırlandırmalara tabi olmadan hayata geçirilmesi, her şeyden önce bireyin temel haklarına ve özel olarak kişisel verilerine ölçüsüz bir müdahale oluşturabilir. Dolayısıyla yüz tanıma teknolojisinin nasıl ve hangi amaçlarla kullanıldığı kadar, bu kullanımın hangi koşullara tabi olması gerektiği de önem arz etmektedir.

21. yüzyılda devletlerin suçla mücadelede kullandığı en önemli enstrümanlarından biri de önleyici ceza hukuku uygulamalarıdır. Önleyici ceza hukukunun temel amacı, suçun henüz işlenmeden önce engellenmesi olup suç işlendikten sonra önleyici ceza hukuku tedbirleri devre dışı kalmaktadır. Bu andan itibaren, bir suç şüphesine dayalı olarak ceza muhakemesi süreci başlamakta ve bu sürece ait işlem ve tedbirler uygulanabilir hale gelmektedir. Gerek geçmişte gerekse günümüzde, suç politikasındaki değişimlere bağlı olarak, ülkelerin zaman zaman kişi hak ve özgürlüklerine müdahaleyi olabildiğince öteleyen özgürlükçü devlet anlayışını ikinci plana alabildikleri ve bunun yerine toplumun, bireylerin güvenliğini sağlama adına vatandaşların potansiyel risk faktörü olarak muhatap alındığı önleyici ceza hukuku uygulamalarına ağırlık verebildikleri gözlemlenmektedir[63].

Önleyici ceza hukukunun başlıca görünüş biçimlerinden biri olan ve henüz işlenmemiş suçları önlemek amacıyla başvurulan önleyici polis tedbirlerinin, istihbari veya önleme amacıyla idare tarafından gerçekleştirilen benzer faaliyetlere yaklaştığı ve idarenin faaliyetleri ile muhakeme tedbirleri arasındaki sınırı belirsizleştirdiği söylenebilir[64]. Gerçekten de, önleyici polis tedbirleri, ceza muhakemesi tedbirleri ile idari tedbirler arasında gri bir alan oluşturan ve kişi hak ve hürriyetleri bakımından çeşitli müdahale biçimlerini beraberinde getiren tedbirlerdir. Bu özellikleri dolayısıyla, önleyici uygulamaların, ceza takibini "polisleştirdiği" ve "özelleştirdiği" ifade edilmiştir[65].

Önleyici ceza hukuku faaliyetleri, özellikle son on yıldır kayda değer biçimde artış göstermiş ve pek çok ülkenin güvenlik stratejilerinde önleyici faaliyetlerin etkinliğinin artırılması ilk sırayı almıştır. Bu gelişim, sadece devlet güvenliğinin bireyin haklarına nazaran daha ön planda tutulduğu Çin, Dubai gibi ülkelerde değil, aynı zamanda hukuk devleti ilkesinin geçerli olduğu İngiltere, Amerika Birleşik Devletleri gibi liberal ülkelerde de yaşanmıştır. Amerikalı yetişkinlerin yüzde 59'u kolluk kuvvetlerinin kamusal alanlardaki potansiyel güvenlik tehditlerini değerlendirmek için yüz tanıma teknolojisini kullanmasını kabul edilebilir bulmaktadır[66].

63 Özellikle, 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri'nde yaşanan ikiz kule saldırısından sonra pek çok ülkede ulusal ve uluslararası düzeyde terörizme karşı başlatılan mücadele kapsamında, önleyici ceza hukuku uygulamalarına ağırlık verilmeye başlandığını ifade etmek mümkündür.

64 **Dönmezer - Erman,** s. 141.

65 **Dönmezer, Sulhi - Erman, Sahir,** Nazari ve Tatbiki Ceza Hukuku, Cilt I, İstanbul, 2016, s. 132-140.

66 https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ (e.t.: 30.03.2020).

İfade edilmelidir ki, önleyici ceza hukuku kapsamında geliştirilen yeni güvenlik önlemlerinin en yaygın olanı yüz tanıma teknolojisidir. Bu teknoloji sayesinde, idari kolluk faaliyeti yürüten güvenlik kuvvetleri, yapay zekâ destekli sistemin verdiği sonuçlara göre, durdurma, kimlik sorma, arama gibi işlem ve tedbirleri uygulayabilmektedir. Bu teknolojinin desteği olmaksızın yapılan uygulamalarda, durdurma, kimlik sorma, arama gibi önleyici tedbirler, güvenlik güçlerinin inisiyatifinde gerçekleşmekte ve onların mesleki bilgi, birikim ve tecrübesine dayalı olarak yapılmaktadır. Yüz tanıma teknolojisi sayesinde, söz konusu tedbirlerin uygulanabilirliğiyle ilgili analizler, oluşturulan algoritmalar vasıtasıyla, akıllı sistem tarafından kendiliğinden yapılabilmekte, algoritmalarla belirlenen ölçütlerle eşleşme ya da sisteme kayıtlı milyonlarca insan yüzü ile sistem tarafından anlık olarak elde edilen yüz verisinin mukayesesi sonucu olası bir eşleşme ya benzeşme durumunda, sistem uyarı vererek önleyici işlemlerin uygulanması konusunda güvenlik güçlerini harekete geçirebilmektedir. Bu uygulama, özellikle kamusal alanlarda, caddelerde, meydanlarda yüksek çözünürlüklü kameralar vasıtasıyla elde edilen veriler çerçevesinde gerçekleştirilmektedir. Daha önce de ifade ettiğimiz gibi, yüz tanıma teknolojilerinin önleyici ceza hukukundaki kullanımı, tamamen suçun önlenmesi amacına yöneliktir. Dolayısıyla, suç işlemiş bir kimsenin yakalanması, izlenmesi amacıyla yapılan uygulamaların niteliği önleyici ceza hukuku faaliyeti olmaktan çıkarak adli bir işlem (soruşturma işlemi, koruma tedbiri) mahiyetine bürünür.

Yapılan çalışmalar, görünür şekilde kameralar konularak gözetleme yapıldığında caydırıcılık bakımından faydalar sağlandığını, örneğin halka açık alanlarda mülkiyet ve şiddet suçlarında kayda değer düşüşler olduğunu ortaya koymaktadır[67]. Ayrıca yapılan araştırmalar, kamusal alanlarda kamera ile yapılan izlemelerin kişilerin sosyo-psikolojik durumları üzerinde olumlu etkilerde bulunduğunu ve özellikle suç korkusunu azalttığını göstermektedir[68].

Bu doğrultuda pek çok ülkede yüz tanıma teknolojileri, suç işlenmesinin önlenmesi amacıyla aktif olarak kullanılmakta veya test edilmektedir. İngiltere'de sokaklara gerçek zamanlı yüz tanıma kameraları yerleştirilmiş, Macaristan'da "szitakötö (yusufçuk)" adlı bir projeyle ülkeye 35.000 yüz tanıma kamerası yerleştirilerek sürücülerin yüzlerinin plaka numaralarıyla eşleştirilmesi hedeflenmiştir[69]. Güney Galler polisi yüz tanımayı aktif bir şekilde kullanmakta ve şüpheli-

67 **McLean, Sarah J.-Worden, Robert E.-Kim, MoonSun,** Here's Looking at You: An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder, s. 319; **Ashby, Matthew P.J.,** age, s. 448, 455. Suçluların kameralara dair farkındalığı suç oranları üzerinde etki yarattığı için kameraların görünür ve gözetlemenin bilinir olması önem arz etmektedir.

68 **Derdiman, R. Cengiz - Tataroğlu, Nihal,** "Devlet Gözetimi ile İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri", İnönü Üniversitesi Hukuk Fakültesi Dergisi, c: 7, y: 2016, sayı: 1, s. 257.

69 European Union Agency, Facial Recognition Technology: Fundamental Rights Considerations in the Contect of Law Enforcement, s. 3.

lerin, potansiyel mağdurların ve korunmasız (kaybolma eğilimi veya demansı olan) kişilerin tanınması amacıyla oluşturulan kapsamlı bir veri tabanı üzerinde çalışmayı sürdürmektedir[70].

Öte yandan, Interpol tarafından geliştirilen Interpol Yüz Tanıma Sistemi, yüz özelliklerini temel alarak kişiyi teşhis eden veya doğrulayan bir biyometrik yazılımdır. Kasım 2016'da kullanılmaya başlanan yazılım pek çok ülkede halen başlangıç aşamasında olup Interpol'ün de katkısıyla geliştirilmeye devam etmektedir. Yüz tanıma sistemleri parmak izi ve DNA gibi diğer teşhis yöntemlerinden farklı olarak yaşlanma, plastik cerrahi, makyaj, görüntü kalitesi, uyuşturucu ve sigaranın yan etkileri, incelenen kişinin duruş açısı gibi faktörleri de dikkate almak durumundadır. Bu nedenle sistemin sağladığı verilerin doğrulanması için manuel bir süreç yürütülmektedir[71].

Temelde sistemin çalışma prensibi, bir yüz görüntüsü girildiğinde kayıtlı olan profiller arasından en olası eşleşmelerin aday listesini üretmeye dayanır. Bu listeler, görüntüyü "Muhtemel Aday", "Aday Değil" veya "Sonuçsuz" olarak kategorize etmek amacıyla yüzde benzersiz özellikler arayan deneyimli Interpol uzmanlarına gönderilir ve uzmanlar tarafından görüntü, listedeki her bir adayla manuel olarak karşılaştırılır. Elde edilen bilgiler görüntüyü sağlayan ülkelerle de paylaşılır. Sistemin sağlıklı çalışabilmesi adına öncelikle kaliteli görüntülere ihtiyaç duyulmaktadır. Bu bağlamda ideal fotoğraf; yüzün aydınlatıldığı ve nötr bir arka plana sahip olan ve şahsın önden tam görüntüsünü içeren ICAO standart pasaport fotoğrafı[72] olacaktır.

Üye ülkelerden gelen Bildirim ve Difüzyon taleplerindeki tüm yüz görüntüleri, kalite kriterlerini sağlamaları koşuluyla yüz tanıma sisteminde aranır ve saklanır. Ayrıca üye ülkeler, örneğin havalimanları ve sınır kapıları için "yalnızca arama" talebinde de bulunabilir[73].

Yüz tanıma teknolojileri, "Next Generation Identification Interstate Photo System (NGI IPS)" kapsamında FBI tarafından da kullanılmaktadır. Sistem kapsamında kolluk kuvvetleri, kolluk süreçleri içinde çekilmiş 30 milyonun üstünde fotoğraf arasından arama yapmak için fotoğraf gönderebilir ve potansiyel soruşturma araçları olarak listelenen adayların isimlerine ulaşabilir. Burada dikkat edilmesi gereken husus şudur; sistem yalnızca soruşturma adaylarını

---

70 Universities' Police Science Institute-Crime and Security Research Institute-Cardiff University, An Evaluation of South Wales Police's Use of Automated Facial Recognition, Eylül 2018.

71 https://www.interpol.int/How-we-work/Forensics/Facial-Recognition (e.t.: 26.03.2020)

72 ICAO (International Civil Aviation Organisation-Uluslararası Sivil Havacılık Örgütü) tarafından pasaportlarda ortak olarak kullanılmak üzere getirilen ölçü ve kurallara uygun fotoğraflardır.

73 Interpol halen yeni teknolojileri, kimlik tespiti süreçlerini, eğitim ihtiyaçlarını tartışmak ve üye ülkeleri uygulamanın iyileşmesi adına desteklemek amacıyla yılda iki kez "Yüz Uzmanları Çalışma Grubu" toplantılarına ev sahipliği yapmaktadır. https://www.interpol.int/How-we-work/Forensics/Facial-Recognition (e.t.: 26.03.2020).

tespit etmekte, soruşturmanın sonucuna ilişkin kesin bir tespitte bulunamamaktadır[74]. 2016 yılında Georgetown'da yapılan bir araştırmada tüm Amerikalıların yarısına ait yüz verisinin polisin yüz tanıma sistemlerinde kayıtlı olduğu tespit edilmiştir[75].

Benzer biçimde Çin'de trafik düzeninin sağlıklı işlemesi, trafiğe çıkan insanların suçu işlemelerinin önüne geçilmesi, caydırıcılık oluşturması amacıyla, tümüyle yapay zekâ destekli sistemle donatılmış bir polis istasyonu uygulaması geliştirilmiş ve test uygulamalarına başlanmıştır. Bu istasyona çevredeki çeşitli kameralar aracılığıyla görüntüler aktarılmakta ve suç işleyen, trafik kurallarını ihlal eden kimseler, sistem tarafından otomatik bir şekilde tespit edilmektedir[76].

Hukuk sistemi içinde soruşturma-kovuşturma evrelerinde şüpheli ve sanıkla ilgili çeşitli tedbirler uygulanabilmektedir. Koruma tedbiri olarak adlandırılan bu tedbirler, delillerin toplanması, muhafazası, şüpheli veya sanığın hazır bulundurulması ve nihayetinde adil bir yargılama yapılarak maddi gerçeğin ortaya çıkarılması amacına özgülenmiştir. Bu süreçlerde yüz tanıma teknolojisinin çok çeşitli amaçlarla uygulanabileceğini söylemek mümkündür. Hakkında yakalama kararı olan bir kişinin tespit edilmesi, şüpheli, sanık, tanık gibi kimselerin beyanlarının doğruluğunun denetlenmesi gibi amaçlarla bu teknolojinin kullanılabileceği ifade edilmelidir. Elbette tüm bu süreçlerde bu uygulamanın ceza muhakemesi faaliyetinin etkinliğini artıracağı ve gerek zaman gerekse iş yükü anlamında adli mercilerin işini kolaylaştıracağı rahatlıkla söylenebilir.

Yüz tanıma teknolojisinin ceza muhakemesindeki kullanım alanlarının en önemli örneğini şüpheli şahısların yakalanması oluşturmaktadır. Çin'deki yapay zekâ polis istasyonları yalnızca suçun önlenmesini amaçlamamakta, aynı zamanda şüpheli şahısların yakalanması amacına da hizmet etmektedir. Şüpheli şahsın yüz verisi sisteme girilmekte ve uygulama noktasında tespit edilen yüzler bu veriyle mukayese edilerek şüpheli şahsa benzeyen ya da doğrudan bu kişi olduğu belirlenen kimseler raporlanarak şüpheli kimselerin yakalanması sağlanmaktadır.

Yüz tanıma teknolojilerinin kolluk kuvvetleri tarafından kullanıldığı bir diğer alan kayıp kişilerin bulunması faaliyetleridir. Hindistan'da kayıp çocukları bulmak için geliştirilen "TrackChild" uygulaması yoluyla 4 gün içinde yaklaşık 3000 çocuk bulunmuş ve kayıp çocukların ciddi bir sorun olduğu ülkede yüz tanıma teknolojileri ilgiyle karşılanmıştır[77].

---

74 https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (e.t.: 26.03.2020).

75 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (e.t.: 30.03.2020).

76 https://www.log.com.tr/cin-yapay-zeka-tarafindan-yonetilen-insansiz-polis-istasyonu-hazirliginda/ (e.t.: 26.03.2020).

77 https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html (e.t.: 26.03.2020).

Yüz tanıma teknolojisini etkin bir şekilde kullanan ülkelerin başında gelen İngiltere'de WeSee firması tarafından geliştirilen yapay zekâ yazılımı sayesinde kişilerin yüz ifadeleri, bakışları, jest ve mimikleri, duygu durumu ve vücut ısısı analiz edilmekte; bu veriler sisteme önceden aktarılmış olan fotoğraflardan elde edilen mevcut verilerle karşılaştırılarak potansiyel suçlular icra faaliyetine geçmeden tespit edilebilmektedir. Yine İngiltere'nin West Midlands bölgesinde polis teşkilatının kullandığı Ulusal Veri Analiz Çözümü (NDAS) sistemi kişinin yüzünü tanıyarak bu kişiye ait devlet kayıtlarında mevcut olan tüm kişisel verileri (genel bilgi tarama kaydı, yaş, eğitim durumu, adli sicil, ikamet bölgesi gibi) taramakta ve bu yolla kişinin suç işleme potansiyelini değerlendirmektedir. Böylelikle suç işleme potansiyeli bulunan kişiler güvenlik güçlerine bildirilerek bu kimseler nezdinde önleyici ceza hukuku faaliyetlerinin gerçekleştirilmesine imkân tanınmaktadır. Bu sistem kişinin mevcut verilerini ve belirli bölgelerdeki suç işleme istatistiklerini de değerlendirmekte ve sistem algoritması tarafından risk analizi yapılmaktadır[78].

Yüz tanıma teknolojilerinden maksimum verimin alınabilmesi için bu sistemlerin farklı teknolojilerle senkronize edilerek kullanılması gerekmektedir. Zira farklı sistemlerden destek alınması halinde yüz tanıma sistemlerinin harekete geçirilmesi, veri tabanlarının geliştirilmesi ve elde edilen verilerin ayıklanması, çok daha kolay ve düşük maliyetli şekilde gerçekleştirilebilecektir. Nitekim yapılan araştırmalar, aynı amaca hizmet etmek üzere kamera ve polis memuru sayısını artırmak yerine silah seslerini algılayarak polise raporlayan ShotStopper gibi GDT teknolojilerinin[79] yüz tanıma sistemine entegre edilmesinin çok daha hızlı ve uygun maliyetli olduğunu ortaya koymuştur[80].

Bu noktada üzerinde durulması gereken bir diğer konu, özellikle Amerikan hukukunda potansiyel suçluları teşhis edebilmek adına risk değerlendirmesi yapmak üzere tasarlanan algoritmaların daha önceden insanlar tarafından verilmiş kararları analiz ederek kendi puanlama sistemlerini oluşturmasıdır. İnsan eliyle verilmiş kararların hiçbir zaman tam anlamıyla objektif olamaması, çok yüksek miktarda karar bir araya geldiğinde kişilerin yaşadığı bölge veya eğitim durumlarıyla suç potansiyelleri arasındaki korelasyonun ciddi biçimde hatalı teşhis edilmesine yol açmaktadır. Bu sebeple benzer yazılımların objektifliğiyle ilgili tartışmalar meydana gelmektedir. Örneğin Massachusetts eyaletinin Brookline, Northampton, Somerville ve Cambridge Şehir Konseyleri aldıkları kararlarla yüz

78 https://www.bbc.com/turkce/haberler-dunya-44865198; http://www.milliyet.com.tr/teknoloji/ingiliz-polisi-sucu-onlemek-icin-yapay-zeka-kullanacak-2786584 (e.t.: 26.03.2020). Bu gelişme sonrasında, basında, sinema tarihinin önemli filmler arasında yer alan "Azınlık Raporu" filmindeki teknolojinin gerçeğe dönüştüğü yorumları dile getirilmiştir. Bkz. http://www.hurriyet.com.tr/avrupa/azinlik-raporu-filmi-gercek-oluyor-sucu-islenmeden-onleme-donemi-basliyor-41035280 (son erişim tarihi: 26.03.2020).

79 Gunshot Detection Technology, Amerika'nın bazı eyaletlerinde kullanılan, silah seslerini akustik sensörler yoluyla algılayarak ateş edilen konumu en yakın polis merkezine ihbar eden uygulamalardır.

80 **Piza - Welsh - Farrington - Thomas,** s. 17.

tanıma teknolojilerinin kullanımını sınırlandırmış, bu kararlarına "hukuki düzenlemelerin hızının teknolojik gelişmelere yetişemediğini, gerekli düzeltmeler yapılana kadar teknolojilerin kullanımının geçici olarak durdurulması gerektiğini" gerekçe göstermişlerdir. Sınırlandırma taraftarları ayrıca yüz tanıma yazılımlarının yaş, cinsiyet ve ırk faktörleriyle ilgili önyargılı olduğunu; bu teknolojileri kullanan veri tabanlarının ırksal önyargılarla karşılaştığını ifade etmektedir. Yüz tanıma teknolojilerinin kullanımının geçici olarak durdurulmasına ilişkin eyalet meclisi karar tasarılarında da ilgili yazılımların kadınların, gençlerin ve siyahilerin yüzlerini algılamakta daha başarısız olduğu ve bu tür yanlışlıkların zararlı "yanlış pozitif" teşhislere yol açtığından bahsedilmektedir. Bu durum genel olarak algoritmaların geliştirilme aşamasında kadınlar ve siyahilere oranla daha yüksek oranda beyaz erkekler üzerinde denenmesine[81] ve ışıklı ortamlarda beyazların, karanlık ortamlarda siyahların daha zor tanınması gibi teknik problemlere dayandırılmaktadır[82]. Bu bağlamda Massachusetts Eyalet Meclisi Haziran 2019'da "Yüz Tanımayı Durdur" temalı bir kampanya başlatarak "bu teknolojilerin temel insan haklarını ihlal etmesini engellemek için" adım atmıştır[83]. Amerikan insan hakları örgütü Liberty ve Essex Üniversitesi de benzer girişimlerde bulunmuştur[84]. Benzer şekilde ACLU[85], Amazon'un "Rekognition" adlı yüz tanıma yazılımının Kongre'den 28 kişiyi yanlış tanıdığını, bu kişilerin büyük bölümünün Afro-Amerikanlar ve Latinler olduğunu iddia etmiştir[86]. Yakın zamanda ABD'de George Floyd'un polis tarafından öldürülmesine ilişkin protestolarda da yüz tanıma teknolojisinin Afro-Amerikalılara yönelik haksız muamelelere yol açabileceği iddia edilmiş; bunun üzerine Amazon, Rekognition teknolojisinin polis tarafından kullanımını bir yıl erteleyerek hükümetlerin yüz tanıma teknolojisinin etik kullanımı için daha güçlü düzenlemeler yapması gerektiğini ifade etmiştir[87]. Amazon'a paralel şekilde IBM de teknolojilerin beyaz olmayan insanlara karşı önyargılı olduğunun ispatlandığını ifade ederek polise satışını durdurmuştur[88].

---

81 https://www.perpetuallineup.org/ (e.t.: 30.03.2020)

82 European Union Agency, Facial Recognition Technology: Fundamental Rights Considerations in the Contect of Law Enforcement, s. 27.

83 https://www.masslive.com/news/2020/01/cambridge-bans-facial-recognition-technology-becoming-fourth-community-in-massachusetts-to-do-so.html (son erişim tarihi: 26.03.2020)

84 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (e.t.: 30.03.2020)

85 American Sivil Liberties Union.

86 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it (e.t.: 30.03.2020)

87 https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html#:~:text=SEATTLE%20%E2%80%94%20Amazon%20said%20on%20Wednesday,unfair%20treatment%20of%20African-Americans. (e.t.: 24.07.2020)

88 https://www.forbes.com/sites/thomasbrewster/2020/06/11/microsoft-urged-to-follow-amazon-and-ibm-stop-selling-facial-recognition-to-cops-after-george-floyds-death/#7dddc385b6b4 (e.t.: 24.07.2020)

Konuyla ilgili Amerika'da yapılan bir diğer araştırma, yüz tanıma teknolojisinin kullanımı bakımından kolluk kuvvetlerine güvenen beyazların oranı %60 iken siyahlarda bu oranın %43 olduğunu tespit etmiştir[89]. Big Brother Watch, İngiltere'deki durumun Amerika'daki sürece çok benzer olduğunu belirtmekte ve İngiliz polis kuvvetleri tarafından kullanılan yazılımın demografik önyargılar için test edilmediğini, ayrıca sistemin özellikle siyahi kadın bireyler üzerinde yanıltıcı sonuçları olabildiğini ifade etmektedir[90].

Yüz tanıma teknolojilerinin kullanımıyla ilgili olarak İngiltere'nin Romford bölgesinde polisin bazı vatandaşların yüz tanıma kameraları tarafından taranmayı reddetmeleri nedeniyle haklarında idari para cezası uygulanması üzerine yaşanan olayda kişilerin yüzünü örtme hakkı olup olmadığı tartışılmış ve polisin yaptığı açıklamada yüz tanımanın reddedilmesinin kişiyi şüpheli haline getirmeyeceği belirtilmiştir[91].

İngiltere'de yüz tanıma teknolojisinin kullanımıyla ilgili yaşanan bu olaylar etik ve hukuki tartışmaları beraberinde getirmiş; bazı insan hakları savunucuları yüz tanıma teknolojisinin kamusal alanlarda kullanımının kişisel verileri ihlal ettiği, uygulamanın rıza dışı parmak izi alma ya da DNA analizi yapma ile eşdeğer olduğu ve kişilik haklarını ihlal ettiği yönünde eleştiriler dile getirmişlerdir[92]. Eleştirilerde de bahsedildiği üzere yüz tanıma ve benzeri önleme faaliyetleri toplum güvenliği ve suçla mücadele açısından fayda sağlasa da kişisel veriler, özel hayatın gizliliği, hareket serbestisi ve kişi hürriyeti başta olmak üzere temel hak ve hürriyetler yönünden sakıncaları da beraberinde getirmekte; bu sebeple uygulamanın belli şartlarla sınırlandırılması büyük önem arz etmektedir[93].

Bu noktada gündeme gelen bir diğer tartışma da yüz tanıma kameralarının Covid-19 virüsü nedeniyle tüm dünyada kullanılmaya başlanan yüz maskeleri karşısındaki durumudur. Söz konusu maskeler kişilerin kamera yoluyla tanınması imkanını ortadan kaldırarak yüz tanıma teknolojilerini etkisiz hale getirmektedir. Bu nedenle tanımayı sadece gözler üzerinden gerçekleştirmeye yönelik yeni teknolojiler üzerinde dahi çalışılmaktadır[94].

---

89 https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ (e.t.: 30.03.2020). Araştırma ayrıca siyahilere benzer şekilde gençler ve Demokratların da teknolojinin kullanımı açısından daha az güvenli olduğunu ortaya koymaktadır.

90 Big Brother Watch, Face Off: The Lawless Growth of Facial Recognition in UK Policing, 2018, s. 16.

91 https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html (e.t.: 26.03.2020).

92 https://www.bbc.com/news/uk-48315979 (e.t.: 26.03.2020).

93 **İçer, Zafer - Buluz, Başak,** "Yapay Zekanın Ceza Muhakemesindeki Rolü ve Geleceği", 9. Suç ve Ceza Film Festivali, http://cdn.istanbul.edu.tr/FileHandler2.ashx?f=9uscff-teblig.pdf (e.t.: 03.05.2020), s. 17.

94 https://www.govtech.com/question-of-the-day/Question-of-the-Day-for-05122020.html; https://www.biometricupdate.com/202004/israeli-military-grade-biometric-facial-recognition-works-with-face-masks (e.t.: 24.07.2020)

Türkiye, yüz tanıma teknolojilerinin ülke çapında uygulanması bakımından çeşitli avantajlara sahiptir. Özellikle Türkiye'de tüm suç tipleriyle ilgilenen tek bir ulusal polis teşkilatı olması ve aynı teşkilatın havalimanları ve otoyolların güvenliği, ehliyet ve pasaportların verilmesi gibi çok farklı alanlarda faaliyet göstermesi; ehliyet ve pasaport fotoğraflarından ülke nüfusunun büyük bir kısmını kapsayan bir veri tabanı oluşturularak bu veri tabanından teşhis ve yakalama yapılmasını kolaylaştıracaktır. Bunun yanında Türk polis teşkilatı herhangi bir geliştirme gerekmeksizin simultane olarak video ve fotoğraf aktarılabilen POLNET adlı bir sistemi ülke çapında kullanmaktadır. Halihazırda mevcut olan POLNET'in kullanımı yüz tanıma sisteminin uygulanmasını kolaylaştıracak ve ek bir bütçe gerektirmeyecektir[95].

V. Yüz Tanıma Teknolojisinin Kamu Gücü Tarafından Kullanımının Temel Hak ve Hürriyetlerle İlişkisi

Bilişim ve teknoloji alanındaki teknik gelişmelerin, günümüz olanaklarına ve ihtiyaçlarına uygun şekilde kullanılabilirliği, kamu gücünün fırsat olarak ele aldığı bir konudur. Biyometrik verilerin güvenlik alanında kullanılması, hem insan faktöründen bağımsız olarak sistemlerin güvenilirliği yönünden avantajlı olarak değerlendirilmekte, hem de personel ihtiyacını ortadan kaldırdığından pratik ve ekonomik kabul edilmektedir. Bu açıdan, siyasi arenadaki genel eğilim, modern teknolojinin güvenlik alanında kullanılmasıdır. Bu eğilimin kamuoyu ve toplum tarafından da olumlu karşılandığı yönünde politik bir algı bulunsa da, bazıları yüz tanıma ile ilişkili video gözetimini topluma karşı "genel bir şüphe" tezahürü olarak görmektedir[96]. Gerçekten de halka açık alanlarda kişisel verilerin düzenli ve sınırsız bir şekilde elde edilebilmesine olanak tanıyan bu teknolojinin, kamu gücü tarafından bir "otomatik güvenlik hizmeti" olarak değerlendirilmemesi gerekmektedir[97].

Yüz tanıma teknolojisi, kişinin yüz verisinin elde edildiği ve işlendiği bir teknoloji olması sebebiyle temel haklarla ilişkilidir. Yüz hatları özel nitelikli kişisel veri niteliğini taşıdığından bu teknolojinin kamu gücü tarafından kullanımı kural olarak kişisel verilere yönelik bir müdahale oluşturmaktadır[98].

---

95 **Yayla, Ahmet S. - Hastings, Samantha K.,** "An Exploration of Using Face Recognition Technologies for National Security", Polis Bilimleri Dergisi, c: 6, sayı: 1-2, 2004, s. 7-8.

96 **Thiel,** s. 218, 219.

97 **Thiel,** s. 220.

98 **Thiel,** s. 219. Bu noktada, yüz tanıma sistemlerinin hukuka aykırı şekilde uygulanmasının Türk Ceza Kanunu'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenen suçları gündeme getirebileceği ifade edilmelidir. İlgili bölümde "özel hayatın gizliliğinin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi", "kişisel verilerin hukuka aykırı olarak kaydedilmesi", "kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi", "kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemesi" suç olarak tanımlanmış ve bu suçların

Kişisel verilerin korunması hakkı, kişisel verilerin hukuka uygun kaydedilmesi ve hukuka uygun kaydedilen kişisel verilerin yine hukuka uygun olarak kullanılması ve saklanmasını içermektedir. Hatta yüz verilerinin karşılaştırma için kullanılmasının da kaydetme ve işleme dışında yüz verisine yönelik ek bir müdahale türü olduğu ifade edilmiştir[99].

Kişisel verilerin korunması, özel hayatın gizliliğinin bir parçasıdır[100]. Bireyin kendini yönetme hakkı kapsamında, kendi tercihleri doğrultusunda şekillendirebileceği; *"dingin ve rahat bırakılma hakkına sahip olduğu kendine özgü alanı"* olarak tanımlanabilecek[101] özel hayatı kural olarak başkalarının ve devletin ilgi alanı dışında kalmalıdır[102]. Anayasa Mahkemesi'ne göre, özel hayatın gizliliği, kişi hürriyetinin bir devamıdır[103]. Anayasa'nın 20. maddesi, özel hayatın gizliliği hakkını düzenlenmiş ve bu madde içinde kişisel verilerin korunması hakkına da yer verilmiştir[104]. Özel hayatın gizliliği, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde koruma altına alınmış olup, kişisel verilerin gizliliği ayrıca koruma altına alınmamış olsa da bu madde kapsamında Avrupa İnsan Hakları Mahkemesi'nin kararlarına konu olmaktadır.

Kişisel verilerin gizliliği, bu verilerin kaderini tayin etme hakkını da beraberinde getirmektedir. Esasen, kişinin kendisinin ve kişisel verilerinin kaderini tayin etme hakkı, genel kişilik hakkının kendi içerisinde değerlendirilebilecek

---

kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi halinde cezanın ağırlaştırılacağı belirtilmiştir. Yüz tanıma amacıyla yerleştirilen kameraların, bu sistemlerin uygulanma koşullarını ve yerleştirilme amacını aşan şekilde kullanılması halinde, ilgili suçların temel şeklinin ve ayrıca bu kameraların başında bulunan polis veya diğer idari birimler tarafından da ağırlaştırılmış halinin işlenmesinin mümkün olduğuna dikkat çekilmelidir. İlgili suçlar için bkz. **Sert,** s. 99 vd.; **Korkmaz,** s. 385 vd.; **Uyarer,** s. 169 vd.

99 **Heldt,** s. 287.

100 **Ersoy,** s. 3, 4.

101 **Kalabalık, Halil,** İnsan Hakları Hukuku, Ankara 2015, s. 427.

102 **Eryılmaz, M. Bedri,** Türk ve İngiliz Hukukunda ve Uygulamasında Durdurma ve Arama, Ankara 2003, s. 65.

103 **Armağan, Servet,** Temel Haklar ve Ödevler, İstanbul 1980, s. 19.

104 Anayasa'nın 20. maddesi şu şekildedir: *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. 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.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."*

alt kategorilerinden biridir. Alman Anayasa Mahkemesi bir kararında[105], bireyin özgür kişisel gelişiminin korunmasının, bireyin kişisel verilerinin sınırsız toplanması, depolanması, kullanılması ve aktarılmasına karşı korunmasını da içerdiğini belirtmiştir. Bu bağlamda, kişinin kendi kaderini tayin etme, maddi ve manevi varlığını geliştirme hakkının, kişisel verilerin ifşası ve kullanımı açısından da geçerli olduğu ifade edilmiştir[106]. Anayasamızın 17. maddesinde, herkesin yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahip olduğu belirtilmiş olup kişisel verilerin kaderini tayin etme hakkının, bu hak çerçevesinde değerlendirilmesi mümkündür.

Kamusal alanlarda yüksek teknoloji içeren yüz tanıma sistemlerinin belirgin bir amaç ve somut tehlike olmaksızın kullanılması, temel hak ve hürriyetlere ilişkin temel gereksinimleri karşılamadığından orantısız kabul edilmelidir. Kişinin kendi kaderini belirleme ve kişisel verilerinin akıbetini tayin etme hakkı, halka açık olarak anonim hareket etme hakkını da içerdiğinden, kişinin hareket serbestisiyle (AY. m.19) doğrudan irtibatlıdır[107].

Bu kullanımın, barışçıl açık hava toplantılarını da kapsaması durumunda, toplantı ve gösteri yürüyüşü düzenleme hakkı (AY. m.34) ve eğer bu müdahale kişilerin görüşlerini açıklamamasına yol açıyorsa ifade hürriyeti (AY. m.25, 26) ile dahi ilişkilendirilebileceği söylenebilir[108].

Tüm temel hak ve hürriyetlerde olduğu gibi, kişisel verilere yönelik müdahaleler de belirli koşullar altında mümkün olabilmektedir. Esasen devletin ve toplumun var olabilmesi, kamu düzen ve güvenliğinin tesis edilebilmesi, toplumda huzur ve barışın sağlanabilmesi için hak ve hürriyetlerin belirli koşullar altında sınırlandırılması kaçınılmaz bir zorunluluk teşkil eder[109]. Ancak bir hukuk devletinde temel hak ve hürriyetler sınırlandırılsa dahi, bu sınırlandırmanın sınırsız, keyfi olmaması, özünün ortadan kaldırılmaması, ancak yasanın açıkça belirttiği sebeplere bağlı olarak kanunla sınırlama yapılması ve bu sınırlamanın demokratik toplum düzeninin gerekliliklerine ve ölçülülük ilkesine aykırı olmaması gerekir (AY m.13)[110].

Nitekim, Anayasa'nın özel hayatın gizliliği (ve bu çerçevede kişisel verilerin gizliliği hakkı) bakımından öngördüğü sınırlandırma sebepleri, 20. maddenin 2. fıkrasında, "millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması" şeklinde belirtilmiş, keza AİHS'in 8. maddesinde de benzer şekilde, özel

105 BVerfGE 65, 1, 43.

106 **Heldt,** s. 287; **Thiel,** s. 219.

107 **Heldt,** s. 288.

108 **Heldt,** s. 288.

109 **Kapani, Münci,** Kamu Hürriyetleri, op.cit., s. 282.

110 **Gözler, Kemal,** Anayasa Hukukunun Genel Esasları, Bursa, 2013, s. 419.

hayatın gizliliği hakkının kullanılmasının ancak bir kamu müdahalesinin "yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması" için gerekli bir tedbir olması durumunda söz konusu olabileceği ifade edilmiştir.

Toplumsal yaşamın sürdürülebilmesi, insanların diğer insanlarla ve devletle olan ilişkilerinin tesis edilebilmesi, bireye ait verilerin farklı şekillerde kullanımını gündeme getirir. Devlet, bazı kurumlarının görev ve yetkilerinin gereği olarak, bireylerin şahsına ait bilgileri kaydetme ya da mevcut bilgileri saklama, kullanma gereği duyabileceği gibi, gerçek veya özel hukuk tüzel kişileri de, mesleki yetkilerini kullanırken kişilere ait verileri kaydetme, kullanma, işleme, saklama gibi bazı işlemleri gerçekleştirebilecektir. Bununla birlikte, verilerin aidiyeti ve şahsi verilerin sadece o kişiyi ilgilendirmesi esasına bağlı olarak, tüm bu işlemlerin kötüye kullanmalara, suistimallere, hak ihlallerine karşı hukuki güvencelerle donatılması gerekir. Esasen kişisel verilerin kullanılması değil, gizliliği ve korunması kural olduğundan, bu verilerin kaydedilmesi, saklanması, verilmesi, aktarılması, işlenmesi gibi davranış modellerinin çağdaş demokratik hukuk devleti ilkelerine uygun şekilde regüle edilmesi, şartlarının ve istisnalarının açık bir şekilde yasal düzenlemelere bağlanması ve müdahalelere ilişkin denetim mekanizmalarının öngörülmesi kaçınılmaz bir gerekliliktir. Zira, kişi güvenliği, hürriyeti, kişi dokunulmazlığı ne denli önemliyse kişisel verilerin korunması da özel hayatın gizliliğinin bir parçası olarak birey için o kadar önem taşımaktadır. Hatta, özel hayatın ve kişisel veri gizliliğinin en etkili şekilde korunması için her bireyin hangi kişisel bilgilerinin hangi amaçlarla otomatik veri dosyalarında tutulduğunu bilme, verilerinin yasada öngörülen amaçlarla kullanılıp kullanılmadığını öğrenme hakkı da bulunmakta olup bu hak ülkemizde Anayasal düzeyde güvence altına alınmıştır (m.20/3)[111].

Teknolojinin son derece hızlı geliştiği günümüzde bireye ait bilgilerin saklanması daha kolay olmakla birlikte, bu bilgilerin ilk elden ulaşılabilirliği de artmaktadır. Bu durum, kişinin kişisel verilerinin korunması hakkına müdahaleler oluşturabilmekte[112] ve temel bir hak olan özel hayatın gizliliği hakkının ihlal edilip edilmediği sorusunu gündeme getirebilmektedir[113]. Bu noktada belirtmek gerekir ki, Anayasa ve AİHS'de yer alan özel hayatın gizliliğine ilişkin hükümler, kişinin diğer insanlar ve dış dünya ile ilişki kurma hakkını da korumaya yöneliktir. Bu görüşe paralel bir yaklaşımda olan Danıştay da "personelden kişisel veri alınması kapsamında olan yüz tanıma sistemi ile mesai takibi uygulamasının

---

111 **Kalabalık,** a.g.e., s. 430.

112 **Dedeoğlu, Gözde,** "Gözetleme, Mahremiyet, İnsan Onuru", TBD Bilişim Dergisi, Mart 2004, sayı: 8, s. 1-3.

113 **Şimşek, Oğuz,** Anayasa Hukukunda Kişisel Verilerin Korunması, 2008, s. 1, 2; **Ersoy, Eren,** "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", ab.org.tr/ab06/bildiri/6.doc; s. 1-2.

kamusal alanda da olsa özel hayatın gizliliği kapsamında bulunması ve bu uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması göz önüne alındığında yüz tanıma işleminin hukuka aykırı olduğu" yönünde içtihatta bulunmuştur[114].

Bir kişinin diğerleri ile kamusal alanda dahi özel yaşam sahasına girebilecek bir etkileşim bölgesi bulunmaktadır. Sokakta yürüyen bir kişi, başkaları tarafından görüntülenmeyi kabullenmiş demektir; bir alanın teknolojik aletlerle izlenmesi de aynı türden bir olay niteliğindedir. AİHM de buradan hareketle, "bir kişinin kamusal alandaki faaliyetlerinin fotoğraflanmasının özel yaşama müdahale yaratmayacağını",[115], bununla beraber "bir kişinin kamu kurumlarınca *sistematik ve daimî* olarak kaydedilmesi noktasında özel yaşama müdahale ortaya çıkacağını"[116] kabul etmektedir.

Wood davası, kamusal gözetimde hangi insan haklarına tehdit oluşturulduğuyla ilgilenen ilk hukuki testtir. Silah karşıtı protestoya katılan ve protesto bitiminde polis tarafından fotoğrafları çekilen başvurucu AİHS m.8'e yönelik saldırı olduğunu iddia etmiş; İngiliz Yüksek Mahkemesi, olayla ilgili olarak dışarıda çekilen fotoğrafın ilgili maddeye aykırı olabilmesi için; ***i)*** Polisin aldığı tedbirin ciddi olması ve özel hayata saldırı niteliği taşıması, ***ii)*** Fotoğrafı çekilen kişinin mahremiyet beklentisinin makul olması, ***iii)*** 8. maddenin uygulanmasının kanunlarca kısıtlanmış olması gerektiği yönünde şartlar getirmiştir. Dava sonucunda polisin aldığı önlem orantısız bulunarak demokratik bir toplumda uygulanamayacağı bildirilmiş ve 8. maddenin ihlali yönünde hüküm verilmiştir[117].

Sonuç olarak, yüz tanıma uygulamasına ilişkin bir yasa hükmü bulunmaksızın, yine Anayasa ya da AİHS'te belirtilen sınırlandırma sebepleri olmaksızın, bireylerin yüz verilerinin kamu gücü müdahalesine maruz kalmasının, yukarıda ifade ettiğimiz çerçevede "özel hayatın gizliliği hakkı", "kişisel verilerin gizliliği ve korunması hakkı", "kişinin maddi ve manevi varlığını geliştirme hakkı bağlamında kişisel verilerinin kaderini tayin etme hakkı", "toplantı ve gösteri yürüyüşü düzenleme hakkı", "ifade özgürlüğü", "kişinin diğer insanlar ve dış dünya ile ilişki kurma hakkı" ile ilişkilendirilebileceği ve yapılan uygulamaların bu haklara yönelik müdahale koşulları çerçevesinde irdelenmesi gerektiği ifade edilmelidir[118].

---

[114] Danıştay 5. Dairesi, 2013/7949 E., T: 15.11.2013.

[115] Herbecq v. Belçika, http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-88070&filename=001-88070.pdf. (e.t.: 30.03.2020).

[116] Peck v. Birleşik Krallık, https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-687182-694690%22]}; Amann v. İsviçre, https://www.legal-tools.org/doc/6e49ed/pdf/ (e.t.: 30.03.2020). Ayrıca bkz. P.G. & J.H. v. Birleşik Krallık.

[117] The Law Society Commission on the Use of Algorithms in the Justice System - The Law Society of England and Wales, Algorithms in the Criminal Justice System, Haziran 2019.

[118] **Jayawickrama, Nihal,** The Judicial Application of Human Rights Law, Cambridge, 2002, s. 610.

VI. Yüz Tanıma Uygulamasının Hukuki Niteliği, Mevzuatımızdaki Durum

Kamu gücü tarafından uygulamaya konulan yüz tanıma teknolojisi bir yandan önleyici ceza hukukuna hizmet ederken diğer yandan da ceza muhakemesi süreçlerinde bazı işlevleri yerine getirebilen adli nitelikte bir faaliyet olarak değerlendirilmelidir. Bu yönüyle yüz tanımanın karma nitelikte bir işlem mahiyeti taşıdığını ifade etmek gerekir.

Yüz tanıma bilhassa suçun önlenmesi ve suçla mücadele açısından kamu gücünü kullanan makamların işini kolaylaştıran, bu amaçları elde edebilmeye elverişli olan bir faaliyettir. Bu faaliyet yoluyla henüz suç işlenmeden suç işleme potansiyeli olan, suç işlemeye yönelik hazırlık hareketlerini gerçekleştiren ya da daha önceden suç işleyeceği yönünde ihbar ya da istihbarat bilgisi elde edilen kişilerin tespit edilmesi mümkün olabilecektir. Bahsedilen uygulamalar; ön alan soruşturmaları olarak da adlandırılmakta olup bu süreçte belirlilik, oranlılık, insan haysiyetinin korunması ilkelerinin geçerli olması gerektiği ifade edilmekte, bunun yanında ön alan soruşturmalarının, savcının kolluk kuvvetleri üzerindeki hakimiyetini kaybetmesi, delil elde etmenin idari bir nitelik kazanması, polis teşkilatının "gizli polis" teşkilatına dönüşmesi gibi birtakım riskler barındırdığı ileri sürülmektedir[119].

Ceza muhakemesi hukukunda, tehlikeli hallere karşı müracaat edilebilecek tedbirler, "önleme tedbirleri" ve "koruma tedbirleri" olarak iki başlık altında incelenebilir[120]. Önleme tedbirleri, tehlikenin mevcut olup henüz suçun işlenmediği hallerde başvurulan tedbirlerdir. Bu tedbirlerin alınmasında kural olarak suçun işlenmesini önlemekle görevli olan idari makamlar yetkilidir. Bir suç şüphesinin ortaya çıkmasından itibaren ise, koruma tedbirlerinin uygulanması gündeme gelir[121].

Genel kabule göre koruma tedbirlerinin ortak özellikleri; tedbirin yasayla düzenlenmesi, belirli bir suç şüphesinin bulunması, tedbirin hükümden önce temel bir hakkı sınırlaması, geçici olması, gecikmede tehlike bulunması ve tedbirin orantılı olmasıdır[122].

Yüz tanıma uygulamalarının muhatabı belirsiz kimseler olup suç şüphesinin ya da bir suç tehlikesinin mevcut olmadığı durumlarda, süreklilik arz ede-

---

119 **Özbek - Doğan- Bacaksız,** s. 153-160.

120 **Yenisey, Feridun - Nuhoğlu, Ayşe,** Ceza Muhakemesi Hukuku, Ankara, 2019, s. 267.

121 **Özbek - Doğan- Bacaksız,** s. 153, 154; **Şahin, Cumhur,** Ceza Muhakemesi Hukuku - I, Ankara, 2019, s. 269, 270, 275; **Yenisey - Nuhoğlu,** s. 267.

122 **Centel, Nur - Zafer, Hamide,** Ceza Muhakemesi Hukuku, İstanbul, 2017, s. 281; **Öztürk, Bahri - Kazancı, Behiye Eker - Güleç Sesim Soyer,** Ceza Muhakemesi Hukukunda Koruma Tedbirleri, Ankara, 2019, s. 26 vd.; **Öztürk, Bahri - Tezcan, Durmuş - Erdem, Mustafa Ruhan - Gezer, Özge Sırma - Kırıt, Yasemin F. Saygılar - Akcan, Esra Alan - Tütüncü, Efser Erden - Özaydın, Özdem - Villemin Derya Altınok - Tok, Mehmet Can,** Ana Hatlarıyla Ceza Muhakemesi Hukuku, Ankara 2019, s. 267 vd.; **Yenisey - Nuhoğlu,** s. 306 vd.; **Şahin,** s. 273 vd.

cek biçimde uygulanmaması gerekir. Bu bakımdan, bu faaliyetin yapısı itibariyle önleyici ceza hukuku vasıtalarına daha yakın olduğu söylenebilirse de, koruma tedbirlerinin özelliklerini taşıdığında da şüphe bulunmamaktadır.

Bununla birlikte, belirli bir suç şüphelisinin tespit edilmesi ve yakalanması amacıyla genele yönelik uygulanan yüz tanımanın hukuki mahiyeti üzerinde de durulmalıdır. Her ne kadar bu uygulama belirli bir suç şüphelisini yakalamak amacıyla faaliyete konulabilirse de, genele yönelik yüz tanıma uygulamasının koruma tedbirlerinin özellikleriyle bağdaşmadığı açıktır. Zira koruma tedbirlerinde çoğu zaman muhatap somut bir şüpheli veya sanıktır. Bazı tedbirler dışında (iletişimin denetlenmesi, elkoyma gibi) soruşturma konusu olmayan, ilgisiz üçüncü kişiler muhatap alınmaz. Buna karşın yüz tanıma sistemleri, pek çok vatandaşı muhatap almakta ve tedbir uygulanırken "ayıklayıcılık" yapılamamaktadır.

Bu noktada belirtilmelidir ki, Türk hukukunda özel olarak yüz tanıma uygulamasına ilişkin bir yasal düzenleme yer almamaktadır.

Bununla birlikte, PVSK'nın 5. maddesinde; ***i)*** Nüfusa kayıtlı olmadığı için kimliği tespit edilemeyen (m.4), ***ii)*** Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, ***iii)*** Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, ***iv)*** Türk vatandaşlığına başvuruda bulunan, ***v)*** Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, ***vi)*** Gözaltına alınan, ***vii)*** CMK'nın 81. maddesi[123] kapsamında hakkında fizik kimliğinin tespiti işlemi uygulanan, ***viii)*** 5275 sayılı CGTİHK'nın 21. maddesi[124] uyarınca, hakkındaki mahkumiyet hükmü kesinleşerek infaz kurumuna alınan kimselerin parmak izlerinin yanı sıra fotoğraflarının alınarak, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilebilmesine imkan tanınmıştır.

---

[123] CMK madde 81: "(1) Üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur. (2) Kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus tutanağa geçirilir."

[124] CGTİHK madde 21: "Haklarında kesinleşmiş hapis cezasını içeren mahkûmiyet ve ödenmeyen adlî para cezalarının hapse çevrilmesine ilişkin karar bulunanlar, Cumhuriyet Başsavcılığının yazılı emriyle ceza infaz kurumuna gönderilirler. Üstleri ve eşyaları arandıktan sonra kabul odalarına konulur ve hekim muayenesinden sonra kuruma yerleştirme işlemleri yapılır. (2) Ceza infaz kurumuna alınan hükümlülerin adı ve soyadı, işledikleri suç, cezalarının türü ve süresi, mahkûmiyet ilâmının tarih ve numarası ve infaza başlandığı gün "hükümlü defteri"ne kayıt olunur. Bu defterdeki sıra numarası, hükümlünün numarasını oluşturur. (3) Tanıya yönelik olarak hükümlülerin parmak ve avuç içi izleri alınır, fotoğrafları çekilir, kan grupları, vücutlarının dış özellikleri ve ölçüleri belirlenir. Kayıt altına alınan söz konusu bilgiler hükümlünün kişisel dosyasında veya elektronik ortamda saklanır. Bu bilgiler, Kanunun zorunlu kıldığı hâller dışında hiçbir kurum ve kişiye verilemez."

PVSK'nın 5. maddesi uyarınca, bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir. Kolluk birimleri, kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir. Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur. Sistemde yer alan kayıtlar gizlidir ve madde belirlenen amaçlar dışında kullanılamaz. Sisteme kayıtlı olan fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir.

Diğer yandan, PVSK'nın Ek 6. maddesinde polisin olaydaki failin gözaltındaki şüpheli ile aynı kişi olup olmadığının belirlenmesi bakımından zorunlu olması halinde ve savcı talimatı doğrultusunda teşhis yaptırabileceği ve teşhise tabi tutulan kişilerin bu işlem sırasında fotoğrafları çekileceği belirtilmiştir.

Bu düzenlemeler dışında, mevzuatımızda teknik araçlarla izleme tedbirine ilişkin bir kısım düzenlemeler yer almaktadır. Bu tedbirin, istihbari amaçlarla ve koruma tedbiri olarak uygulanan türleri bulunmaktadır. PVSK (Ek 7. madde) ve 2803 sayılı Jandarma, Teşkilat, Görev ve Yetkileri Kanunu'nda (Ek 5. madde) istihbarat faaliyetlerinde ve sadece istihbari amaçlarla kullanılmak üzere belirli suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabileceği düzenlenmiştir. Yine, katalog halinde yer verilen belirli suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilememesi hâlinde, hakim ya da gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından karar verilebilen, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyerinin teknik araçlarla izlenmesine, ses veya görüntü kaydının alınmasına imkan veren teknik araçlarla izleme koruma tedbirine ise, CMK'nın 140'ıncı maddesinde yer verilmiştir.

Mevzuatımızdaki bu sınırlı düzenlemeler dışında, bizatihi yüz tanıma teknolojilerinin önleyici ceza hukuku ve ceza muhakemesi süreçlerinde kullanılmasına ilişkin düzenlemelerin bulunmadığı, mevcut düzenlemelerin yalnızca bazı hallerde, belirli, müşahhas kimselerin fotoğrafının çekilmesi, bir kısım kişilerin istihbari amaçlarla ya da koruma tedbiri mahiyetindeki teknik araçlarla izlenmesiyle sınırlı olduğu, bu açıdan yüz tanıma teknolojisinin kamusal alanlarda genele yönelik uygulanabilirliğine imkan veren, kapsayıcı yasal düzenlemelere ihtiyaç olduğu açıktır.

VII. Yüz Tanıma Uygulamasında Göz Önünde Bulundurulması Gereken Temel İlkeler

Yüz verisi, özel nitelikte bir veri olduğundan işlenme koşulları diğer kişisel verilerden farklı bir şekilde ortaya konulmalıdır. Her ne kadar 6698 sayılı Kanun'un 6. maddesinin 2. fıkrası özel nitelikli kişisel verilerin ilgilinin

açık rızası olmaksızın işlenmesinin yasak olduğunu düzenlese de, Anayasa ve AİHS'in 8. maddesinde öngörülen sınırlandırma sebepleri arasında yer alan suçun önlenmesi, kamu güvenliğinin sağlanması gibi amaçlarla yüz tanıma uygulaması icra edildiğinden bu uygulamaya muhatap olanların rızasına ihtiyaç duyulmayacağı tartışmasızdır. Zira önleyici-adli nitelikte karma bir tedbir mahiyetinde olan yüz tanımanın, kişilerin rızasına bağlı tutulması fiilen mümkün olmayacağı gibi, amaca da uygun düşmeyecektir. Nitekim 6698 sayılı Kanunun 6. maddesinin 3. fıkrasında bazı veriler hariç olmak üzere özel nitelikteki verilerin kanunlarda öngörülen hallerde ilgili kişinin açık rızası olmadan da işlenebilmesine imkân tanınmıştır. Yine de, rızası meselesinden bağımsız olarak, yüz tanıma teknolojisinin kullanılmasında belirli ilkelerin göz önünde bulundurulması gerekmektedir.

Yüz tanıma sistemlerinin kullanımı, kişinin yüz verisinin işlenmesi anlamına geleceğinden, kişisel verilerin işlenmesinde göz önünde bulundurulan ilkeler yüz tanıma açısından da geçerlidir. Bu bağlamda 6698 sayılı Kanun'un 4. maddesinde ifade edildiği üzere yüz tanıma uygulamasının hukuka ve dürüstlük kurallarına uygun olması, belirgin, açık ve meşru amaçlar için uygulanması, amaçla bağlantılı, sınırlı ve ölçülü olması, uygulamanın getirdiği verilerin ancak amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir[125]. Aşağıda bu çerçevede, yüz tanıma sistemlerinin kullanımına ilişkin göz önünde bulundurulması gereken ilkeler ve koşullar üzerinde durulacaktır[126].

1. Yasal Düzenleme Gerekliliği

Yüz tanıma, yüz verisinin kaydedilmesi, aktarılması ve işlenmesi gibi işlemleri içerdiğinden kişisel verilere ve özel hayatın gizliliğine müdahale oluşturan bir uygulamadır. Anayasa'nın 13. maddesine göre, temel hak ve hürriyetler ancak kanunla sınırlanabilir. Keza, 6698 sayılı Kanun'da verinin işlenme şartları arasında kanunda açıkça düzenlenme yer almaktadır. Bu açıdan, yüz tanımanın gü-

---

[125] Kişisel verilerin korunması ve işlenmesinde, bazı temel ilkelerin göz önünde bulundurulması gerekir. Verilerin işlenmesinde, bazı temel ilkelerin esas alınması, hukuk devletinin bir gereğidir. Her şeyden önce verilerin işlenebilmesi için, buna ilişkin yasal bir düzenlemeye ihtiyaç vardır. Böyle bir yasal düzenleme olmaksızın yapılan müdahaleler hukuka uygun kabul edilemez. Kişisel verilerin işlenebilmesinin belirli amaçlarla gerçekleştirilmesi gerekir. Bu amacın yalnız başlangıçta değil, kaydedilen verilerin işlenmesi, aktarılması sırasında da bulunması esastır. Kişisel verilerin kaydedilmesinde, işlenmesinde, ilgilinin iradesi veya bilgisinin bulunması aranmalıdır. Meşru olmayan bir şekilde, kişinin iradesi veya bilgisi dışında kişisel verilerin kaydedilmesi, işlenmesi hukuka uygun değildir. Yasaya uygun yapılan müdahalelerin, ölçülü olması, amacı aşmaması ve kullanımın denetiminin etkin bir organ tarafından gerçekleştirilmesi gerekir. Kişisel verilerin etkin bir şekilde korunmasını sağlamak amacıyla bireyin, şikâyet, tazminat gibi her türlü yasal hakları güvence altına alınmalı, kötüye kullanıma karşı etkili (idari, hukuki veya cezai) başvuru yolları öngörülmelidir. **Kilkelly, Ursula,** Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Kılavuz, İnsan Hakları El Kitapları No: 1, Almanya, 2001, s. 58.

[126] Krşz. mobese sistemlerinin kullanımına ilişkin koşullar hakkında bkz. **Özkan,** s. 67 vd.

venlik alanında kamu gücü tarafından kullanımı bakımından yasal düzenlemeye ihtiyaç olduğunda tereddüt yoktur[127]. Düzenlemenin yer aldığı kanunun detaylı, uygulamanın koşul ve sınırlarının açık, belirgin olması da uluslararası hukuka uygunluk açısından aranan diğer özelliklerdir[128].

Kanunilik ilkesi kapsamında değerlendirilmesi gereken diğer bir durum da kişisel ve özellikle biyometrik verilerin kullanılmasıyla ilgili temel bir prensip olan elde edilen verinin kanuni sınırlar içinde kullanılması, kullanım amacının ortadan kalkması veya kanunun cevaz verdiği sürenin dolması halinde verinin derhal sistemlerden silinmesidir. Bu uygulama kapsamında, amaca ulaşmayı sağlayacak ilgili ve gerekli verilerin kullanılması sağlanmalıdır. Bu bağlamda, karşılaştırma için gerekli olmayan bilgi ve verilerin toplanması söz konusu olmuşsa, bu verilerin "veri minimizasyonu ilkesi" çerçevesinde yok edilmesi gerekir[129]. Bu verilerin hangilerinin, hangi koşullar altında silinmesi ya da yok edilmesi gerektiği yasada ayrıca düzenlenmelidir.

TCK'nın 138. maddesinde de "kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemesi" suç olarak düzenlenmiştir. Bu bağlamda yüz tanıma kameraları yoluyla elde edilen verilerin kanunda belirlenecek süre sonunda ortadan kaldırılması hukukilik açısından büyük önem arz etmektedir. AİHM de biyometrik verilerin sınırsız olarak kayıt altında tutulmasının ve kişilerin ilgili verilerin silinmesi için talepte bulunmalarının belli şartlara bağlanmasının AİHS'in 8. maddesindeki özel hayata saygı hakkına aykırı olduğu yönünde karar vermiştir[130].

2. Meşru Bir Amaca Dayanma

Yüz tanıma teknolojisinin kullanımında da en hassas konulardan biri uygulamanın amaçsallığıdır. Yüz tanımanın belli ve meşru amaçlarla uygulanması gerekir[131]. Bu amaç kamu güvenliğinin sağlanması, suçun işlenmesinin önüne geçilmesi, suçluların yakalanması olabilir. Avrupa İnsan Hakları Mahkemesi de somut olayın özellikleri göz önünde tutulmak şartıyla "başvurucunun özel hayata saygı hakkı ve suçlunun yakalanması arasındaki denge korunduğu sürece" video

---

127 Allan v. Birleşik Krallık, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-122859%22]}; Data Protection Directive for Police and Criminal Justice Authorities, §8, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680.

128 Szabo and Vissy v. Macaristan, https://policehumanrightsresources.org/szabo-and-vissy-v-hungary-37138-14; Vukota-Bojic v. İsviçre, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-167490%22]}; **Özbek - Doğan- Bacaksız,** s. 178.

129 **Thiel,** s. 220.

130 S. and Marper v. Birleşik Krallık, https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-2571936-2784147%22]}; Karabeyoğlu v. Türkiye, https://www.echr.coe.int/Documents/CP_Turkey_ENG.pdf.

131 Data Protection Directive for Police and Criminal Justice Authorities, §9, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680; **Özbek - Doğan- Bacaksız,** s. 178.

kayıt teknolojilerinin kullanımını hukuka uygun bulmaktadır[132]. Bu amaçlar dışında, yüz tanıma uygulamasının gelişigüzel, keyfi amaçlarla kullanılması hukuka aykırı olacaktır.

Bu noktada ifade edilmelidir ki, kameraların belli ve meşru amaç dahilinde kurulmasının yanı sıra, kameralar yoluyla elde edilen yüz verilerinin de amaca uygun kullanılması zorunludur[133]. Avrupa Parlamentosu ve Avrupa Konseyi, verilerin kameraların konulma amacı dışında bir konuda kullanılmasının ancak bunun gerekli, orantılı ve kanuni olması durumunda mümkün olduğunu kabul etmektedir[134].

3. Süreklilik Arz Etmeme

Yüz tanımanın süreklilik arz edecek şekilde uygulanması, hak ve hürriyetler açısından orantılı bir müdahale tarzı değildir. Yüz tanıma için yetkilendirmenin sebepsiz olmaması, uygulamanın somut tehlike ya da artan tehdit veya ihlal riskine dayandırılması aranmalıdır[135]. Böylelikle uygulamanın, kanunlarla sınırları çizilmiş belirli koşullar altında, süreklilik arz etmeyecek şekilde uygulanabilirliği temin edilebilecektir. Yetkili merciler tarafından kanundaki koşullar dâhilinde alınan kararlarda, yüz tanıma uygulamasının yapılacağı yer ve kapsamının önceden belirlenmiş olması ve yine hangi sürelerle uygulamanın yapılacağının tayin edilmiş olması önemli bir gerekliliktir. Bu uygulamayla, suçun önlenmesi ve suçluların tespiti amaçlandığından belirli risk ve tehditlerin varlığına ilişkin şüphe sebeplerine dayalı olarak yer, kapsam ve zaman bakımından önceden belirlenmiş mahallerde uygulamanın hayata geçirilmesi elzemdir.

4. Ölçülü Olma

Temel hak ve hürriyetlerin sınırlanmasında teknolojinin kullanılması ve inceleme konumuz kapsamında kamusal alanlarda video gözetiminin sınırlarının belirlenmesine ilişkin tartışmaların büyük çoğunluğu özgürlük ve güvenlik arasındaki denge bakımından yapılmaktadır[136]. Bu durum, hak ve özgürlükler arasında denge kurulmasının, temel hak ve hürriyetlere müdahale yönünden önemini ortaya koymakta ve bu ölçütün güncelliğini yitirmediğini göstermektedir[137].

---

[132] Karin Köpke v. Almanya, http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-101536&filename=001-101536.pdf.

[133] Karabeyoğlu v. Türkiye, https://www.echr.coe.int/Documents/CP_Turkey_ENG.pdf.

[134] Data Protection Directive for Police and Criminal Justice Authorities, §4, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680

[135] **Thiel,** s. 220; **Özbek - Doğan- Bacaksız,** s. 182.

[136] Yüz tanıma teknolojilerinin sosyal hayattaki kullanımının özel hayatın gizliliği hakkına potansiyel bir müdahale niteliğinde olduğu söylenebilir. Zira bu teknolojilerin kullanıma geçmesiyle ortak yaşam alanlarında görüntü takibi yapılarak kişilerin yüzlerinin tespiti yoluna gidilecek, kişinin gün içinde nerede ve kiminle olduğu, ne yaptığı gibi pek çok bilginin takibini yapmak mümkün hale gelecektir. Bu müdahalenin orantılı olabilmesi ise ancak sayılan sınırlama sebeplerinden birinin mevcut olması durumunda mümkün olacaktır.

[137] **Thiel,** s. 219.

Yüz tanıma teknolojileri suçun önlenmesinde ve şüphelilerin yakalanmasında önemli bir rol icra etmektedir. Ayrıca gelişen teknolojik standartlar dâhilinde bu teknolojilere başvurulması, oldukça ağır işleyen ceza muhakemesi süreçlerinin yükünü hafifletecek ve adli mercilerin işini kolaylaştıracak niteliktedir. Bu noktada bu teknolojilerin kontrolsüz kullanımı tehlikesi gündeme gelmektedir. Ceza muhakemesi hukukunda koruma tedbirlerine hâkim olan orantılılık (ölçülülük) ilkesinin bir sonucu olarak yüz tanıma teknolojilerinin kullanımı, ancak uygulamanın belli bir amaca yönelik yapılması ve daha hafif başka bir tedbirin bu amacı gerçekleştirmeye muktedir olmaması halinde mümkün olabilmelidir[138]. Teknolojilerin en yaygın kullanım amacının suçun önlenmesi olduğu göz önünde bulundurulduğunda, orantılılığın sağlanması için yüz tanımanın "bir suç şüphesinin ya da suçun işleneceğine ilişkin somut tehlike ve ihlal risklerinin kıyasen daha yoğun olduğu yer, zaman ve durumlarda" yapılması gerektiği ifade edilebilir. Örneğin, havalimanlarında, tren istasyonlarında bir terör saldırısı tehdidinin varlığı halinde bu uygulamanın orantılı olduğu söylenebilecektir. Keza, merkezi bir caddenin özellikle yılbaşı akşamı gibi kalabalık bir zaman diliminde izlemeye tabi tutulması, terör tehlikesi, hırsızlık ve taciz gibi suçların işlenmesinin engellenmesine katkıda bulunabilecektir. Buna karşılık, konutların ağırlıklı olduğu bir muhitte, sokak arasında yapılacak bir izlemenin amaca hizmet bakımından gerekli ve orantılı olmayacağı ifade edilebilir[139].

Orantılılıkla ilgili önemle üzerinde durulması gereken bir diğer nokta da izlemenin bireyleri suç işlemekten alıkoymanın yanı sıra, özgürlük duygularını kısıtlayarak toplumsal gelişimi sınırlandırması gibi daha geniş kapsamlı ve olumsuz etkiler ortaya koyması ihtimalidir[140]. Doktrinde algoritmaların irade üzerinde etkili olduğu ve bireyi gerçekte olmadığı biri olmaya yönlendirdiği yönünde görüşler mevcuttur. Sürekli gözetim ve denetim fikri kişiyi daha "kurallara uygun" yaşayan biri haline getirerek sadece hukuk kurallarına değil, ahlaki normlara da uygun yaşamaya yönlendirebilecek ve hareket serbestisini kısıtlayabilecektir[141]. Şüphesiz, uygulamanın bu tip dezavantajları, demokratik ve çoğulcu bir toplum tarafından olumlu karşılanmayacaktır. Bu tip olumsuz etkileri en aza indirmek adına izleme esnasında orantılılık ve kanunilik şartlarının tam olarak sağlanmış olması büyük önem taşımaktadır.

---

138 **Thiel,** s. 220; **Özbek - Doğan- Bacaksız,** s. 178.

139 **Yenisey, Feridun,** "Aleni Alanların Video Kamera ile Denetlenmesi", http://www.caginpolisi.com.tr/eski_sitemiz/120/8-9.htm (son erişim tarihi: 26.03.2020)

140 **Karakehya,** s. 346; Nlets the International Justice and Public Safety Network, Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf, s. 17.

141 **Yeung, Karen,** Hypernudge: Big Data as a Mode of Regulation by Design, Information, Communication & Society, y: 2016, 20/1, 1-19, s. 14.

5. Yetkili Merciler Tarafından Karar Alınması ve Uygulanması

Yüz tanıma uygulaması kanunda açıkça düzenlenmiş olmalı ve bu uygulama yine kanunun açıkça yetkilendirdiği kişilerin kararlarına dayanmalıdır. Bu uygulamanın hangi alanlarda, ne tür teknik vasıtalarla (sabit ya da mobil sistemlerle) yapılacağı hususunda karar verme yetkisinin de sınırsız olmaması, kanunda belirtilen koşullara dayanması gerekmektedir. Bu durum hukuki güvenlik ilkesinin doğal bir sonucudur. Ayrıca hukuka uygun şekilde alınan kararların, yine kanun tarafından yetkilendirilmiş kamu görevlileri ve yetkili birimler tarafından icra edilmesi gerekir.

6. Denetlenebilirlik

Yüz tanıma uygulaması kanunla belirlenen, kanunun yetki verdiği kişiler tarafından uygulanan bir faaliyet olduğundan bu faaliyetin hukuka uygun yapılıp yapılmadığının denetlenebilir olması, buna yönelik bir denetim mekanizmasının oluşturulmuş olması gerekmektedir. Bir hukuk devletinde, yetkili merciler tarafından alınan kararların denetime tabi olması temel bir prensiptir. Denetim mekanizması hem uygulama öncesinde karar aşamasında hem de uygulama yapıldıktan sonraki evrede söz konusu olmalıdır. Örneğin biyometrik yüz tanıma sisteminin kullanımına karar vermeden önce, her somut durumda bunun gerekli olup olmadığı kontrole tabi tutulmalıdır[142]. Böylelikle, yüz tanıma teknolojisinin, amaç dışı, keyfi ve ölçüsüz şekilde kullanılabilmesi engellenmiş ve kanun tarafından verilen yetkinin suistimal edilmesinin önüne geçilmiş olur. Bu sebeple mevzuatta bu uygulamaya karşı denetim ve yasal başvuru yollarının açık tutulması, bu teknolojinin meşruiyeti bakımından önemli bir kriterdir.

7. Uygulamanın Kamuya Açık Alanlarda Yapılması

Yüz tanıma teknolojilerinin asıl kullanım amacı kamu güvenliği ve düzenini sağlamak ve suç işlenmesini önlemek olup önleyici tedbir olarak kullanılmaları esastır. Bu bağlamda bu teknolojiler yoluyla ancak kamu gücü tarafından denetim yapılabilecektir. Bu sebeple özel alanlarda, konutlarda, iş yerlerinde, özel araçlarda uygulama yapılmaması; ancak kamuya açık alanlarda, açık bir rızaya ihtiyaç duyulmadan girilebilecek alanlarda, kamu binalarında, ulaşım merkezlerinde, limanlarda, havaalanlarında, istasyonlarda, alışveriş merkezlerinde, caddelerde, meydanlarda uygulama yapılabilmesi gerekir[143]. Ancak bu durumda dahi uygulamanın belirtilen alanlarda yapılması ölçülülük prensibine ve amaca uygunluk koşuluna hizmet etmek zorundadır[144].

---

142 **Thiel,** s. 220.

143 **Özbek - Doğan- Bacaksız,** s. 181.

144 Bu koşul ile ilgili olarak üzerinde durulması gereken diğer bir nokta, kişilerin yüz tanıma kameralarından gizlenme hakkı bulunup bulunmadığıdır. İngiltere'nin Romford kentinde meydana gelen olayda İngiliz polisi, vatandaşların yüzlerini kameradan saklayamayacakları yönünde açıklamada bulunmuştur.

8. Bilinebilirlik

Yüz tanıma teknolojisinin uygulandığı alanlarda bu uygulamanın yapıldığının herkesçe görülebilir şekilde belirtilmesi, uygulamanın bilinirliğinin sağlanması gerekmektedir. Yüz tanıma gizli olarak uygulanan bir faaliyet olmamalı, tedbirin uygulandığı birey tarafından bilinebilir olmalıdır. Uygulama yapılmadan önce, uyarı levhaları ve tabelalarla hangi bölgede yüz tanımanın yapıldığı belirtilmeli ve bu bildirim herkesçe görülebilecek şekilde izleme alanına konulmalıdır.

Bildirimin belirsizlik taşımaması gerekir. Örneğin belirli bir ilçede yüz tanımanın uygulandığı yönünde bir uyarı yeterli olmayacaktır. Uygulamanın yapıldığı tüm yerlerde o alan içerisinde görünürlüğün ve bilinebilirliğin sağlanması önem arz etmektedir. Bu nedenle kameralı denetimlerin suçların sıklıkla işlendiği yerlerde yapılması amaca uygundur. Buradaki temel kriter "tehlikeli yerler" kriteridir. Bu yerler, geniş kalabalıkların bulunması sebebiyle suç işlenme sıklığının yüksek ya da işlenme tehlikesinin yoğun olduğu bölgelerdir. Ancak, video kamera ile denetlenecek yerin herkesin girebileceği, aleni bir yer olması şarttır. Mesela, bir gece kulübünün arka tarafındaki bir oda, kamera ile denetlenemez[145]. AİHM de kararlarında konuyla ilgili olarak "gözetimin açık olmadığı durumlarda insanların gözetlendiklerine dair bilgilendirilmesi" ve "gözetleme yapıldığı ayrıca belirtilmesine gerek olmayacak düzeyde açık olmadıkça gözetlenenin rızası alınması" gerekliliğine vurgu yapmaktadır[146].

Bu bağlamda değinilmesi gereken bir başka nokta, denetimin hareketli (mobil) kameralarla yapıldığı durumlardır. Yüz tanıma sistemlerinin insansız hava araçları vasıtasıyla uygulamaya konulması, sistemin işlevselliğini ve verimini şüphesiz arttıracaktır. Ancak bu hallerde, hangi alanlarda uygulama yapılacağının belirli olması ve alanın dışına taşınmamasına, belirlilik ve ölçülülük kuralının ihlal edilmemesi açısından dikkat edilmelidir.

VIII. Sonuç

Yüz tanıma teknolojisi, çeşitli amaçlarla bireylerin yüzlerinin kaydedildiği ve veri stoğundaki verilerle mukayese edilerek belirli bir eşleşmenin hedeflendiği sistemlerdir. Bu sistemlerin işleyişi; verinin kaydedilmesi, tanımlanması ve doğrulanması aşamalarından oluşur.

Yüz tanıma teknolojilerinin kullanımı, suçla mücadele bakımından son derece elverişli ve işlevseldir. Kamu gücü tarafından bu teknolojilerin kamuya açık alanlarda, havaalanlarında, liman ve istasyonlarda, gümrük sahalarında kullanılması, önleyici ceza hukuku ve ceza muhakemesi süreçleri açısından idari ve adli mercilerin işini kolaylaştırmakta, güvenliğin sağlanması noktasında önemli bir

[145] **Yenisey,** age., http://www.caginpolisi.com.tr/eski_sitemiz/120/8-9.htm (son erişim tarihi: 26.03.2020).

[146] Lopez Ribalda v. İspanya, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-197098%22]}.

fonksiyon icra etmektedir. Tüm bu faydalarına rağmen, bu sistemlerin kullanımı temel hak ve hürriyetlere müdahale oluşturduğundan, belirli koşullara tabi tutulmalıdır.

Yüz tanıma teknolojilerinin işleyişi temelde aynı olup, belirli bir alana yerleştirilen sabit ya da hareketli (mobil) kameralar, o yerden geçmekte olan kişilerin yüz verilerini işleyerek veri tabanına aktarmakta ve sisteme daha önceden tanıtılmış yüz verisiyle bu veriler mukayese edilerek eşleşme olması ya da sistemin şüpheli bir durum tespit etmesi halinde, ilgili şahıs ya da şahıslar hakkında önleyici/adli tedbirler ilgili mercilerce hayata geçirilebilmektedir.

Yüz tanıma sistemleriyle elde edilen yüz verisi, hukuki niteliği itibariyle kişisel veri özelliğini taşımaktadır. Yüz verisi biyometrik özellikler taşıdığından, özel nitelikli kişisel veriler kategorisindedir.

Kamu gücü tarafından suçun önlenmesi, suçluların tespiti ve yakalanması amaçlarıyla gerek önleyici ceza hukuku gerekse ceza muhakemesi süreçlerinde uygulanabilen bu sistemler, İngiltere, ABD, Almanya, Çin gibi ülkelerde fiilen kullanılmaya başlanmış ya da test aşamasında hayata geçirilmiştir.

Yüz tanıma uygulaması, temel hak ve hürriyetlere müdahale oluşturmaktadır. Anayasa ya da AİHS'te belirtilen sınırlandırma sebepleri olmaksızın, bireylerin yüz verilerinin kamu gücü müdahalesine maruz kalması, bilhassa "özel hayatın gizliliği hakkı", "kişisel verilerin gizliliği ve korunması hakkı", "kişinin maddi ve manevi varlığını geliştirme hakkı bağlamında kişisel verilerinin kaderini tayin etme hakkı", "toplantı ve gösteri yürüyüşü düzenleme hakkı", "ifade özgürlüğü", "kişinin diğer insanlar ve dış dünya ile ilişki kurma hakkı" ile ilişkilendirilebilecektir. Fiili uygulamaların, bu haklara yönelik müdahale koşulları çerçevesinde değerlendirilmesi gerekmektedir.

Kamu gücü tarafından uygulamaya konulan yüz tanıma teknolojisi bir yandan önleyici ceza hukukuna hizmet etmekte, diğer yandan da ceza muhakemesi süreçlerinde bazı işlevleri yerine getirebilecek özellikleri taşımaktadır. Bu yönüyle sistem, suçun önlenmesi amacıyla uygulanabildiği gibi, bir suç şüphelisinin yakalanması amacıyla da kullanılabilmektedir. Koruma tedbirlerinin genel özelliklerinden bazılarına uygun olmasa da yüz tanıma uygulamasının, hukuki niteliği itibariyle önleyici-koruyucu tedbirler kategorisinde değerlendirilebileceği ve bu yönüyle karma nitelikte bir işlem mahiyeti taşıdığını ifade etmek gerekir.

Mevzuatımızda, PVSK'da yalnızca bazı hallerde belirli kimselerin fotoğrafının çekilmesi, kaydedilmesinin yanında, istihbari amaçlarla (PVSK. Ek m.5, JTGYK. Ek m.7) ya da ceza muhakemesi süreçlerinde delil elde edebilmek amacıyla (CMK m.140) kişilerin kamusal alandaki faaliyetlerinin teknik araçlarla izlenmesi ile sınırlı düzenlemeler olmakla birlikte, güvenliğin sağlanması ve suçun önlenmesi amacıyla yüz tanıma teknolojisinin uygulanmasına olanak sağlayan

açık bir düzenleme yer almamaktadır. Uygulamanın kamusal alanlarda genele yönelik uygulanabilirliğine imkân veren kapsayıcı yasal düzenlemelere ihtiyaç olduğu şüphesizdir.

Bu konuya ilişkin yasal düzenlemeler yapılırken, birtakım koşul ve prensiplerin göz önünde bulundurulması gerekmektedir. Yüz tanıma teknolojilerinin önleyici ceza hukuku ve ceza muhakemesi süreçlerinde uygulanması temel hak ve hürriyetlere müdahale oluşturduğundan, bu müdahale yasal düzenlemeye dayanmalı, meşru bir amaç için uygulanmalı, süreklilik arz etmemeli, ölçülü olmalı, yetkili merciler tarafından alınan kararlara istinaden uygulanmalı, denetlenebilirliği ve bilinebilirliği sağlanmalı, kamuya açık alanlarda uygulanmalıdır. Ancak, bu ilke ve prensipler çerçevesinde hayata geçirilecek yasal düzenlemelerin ve uygulamaların hukuka uygun olabileceği gözden uzak tutulmamalıdır.

Kaynakça

Akgül, Aydın, "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", Türkiye Barolar Birliği Dergisi, y: 2015, sayı: 118.

Armağan, Servet, Temel Haklar ve Ödevler, İstanbul, 1980.

Ashby, Matthew P.J., "The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis", European Journal on Criminal Policy and Research, y. 2017, vol. 23.

Big Brother Watch, Face Off: The Lawless Growth of Facial Recognition in UK Policing, 2018.

Bozbayındır, Ali Emrah, "The Advent of Preventive Criminal Law: An Erosion of the Traditional Criminal Law?" Criminal Law Forum-The Official Journal of the Society fort he Reform of Criminal Law, vol: 29, no: 1, 2018.

Bük, Alaattin, Bilişim Alanında Kişisel Verilerin Korunması, Ankara, 2018.

Centel, Nur - Zafer, Hamide, Ceza Muhakemesi Hukuku, İstanbul, 2017.

Coester, Ulla - Fuhlert, Bernd, "Gesichtserkennung - eine Frage der Ethik?" Datenschutz und Datensicherheit, 2020/1.

Data Protection Directive for Police and Criminal Justice Authorities, Official Journal of the European Union.

Dedeoğlu, Gözde, "Gözetleme, Mahremiyet, İnsan Onuru", TBD Bilişim Dergisi, Mart 2004, sayı: 89.

Derdiman, R. Cengiz - Tataroğlu, Nihal, "Devlet Gözetimi ile İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri", İnönü Üniversitesi Hukuk Fakültesi Dergisi, y: 2016, c: 7, sayı: 1.

Dönmezer, Sulhi - Erman, Sahir, Nazari ve Tatbiki Ceza Hukuku, Cilt I, İstanbul, 2016.

Drewes, Michael, "Videoüberwachung 2.5 - Biometrische Gesichtserkennung und intelligence Videoanalyse", Deutsches Polizeiblatt, 2020/1.

Ersoy, Eren, Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması, 4. Bilgi Teknolojileri Kongresi, Akademik Bilişim 2006.

Eryılmaz, M. Bedri, Türk ve İngiliz Hukukunda ve Uygulamasında Durdurma ve Arama, Ankara, 2003.

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, 2018.

Göçmen Uyarer, Sinem, Kişisel Verilerin Korunması, Ankara, 2019.

Gözler, Kemal, Anayasa Hukukunun Genel Esasları, Bursa, 2013.

Heldt, Amelie P., "Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raums", MMR, heft: 5, 2019.

İçer, Zafer-Buluz, Başak, "Yapay Zekanın Ceza Muhakemesindeki Rolü ve Geleceği", 9. Suç ve Ceza Film Festivali, 2019, (http://cdn.istanbul.edu.tr/FileHandler2.ashx?f=9uscff-teblig.pdf).

Jayawickrama, Nihal, The Judicial Application of Human Rights Law, Cambridge, 2002.

Kalabalık, Halil, İnsan Hakları Hukuku, Ankara, 2015.

Karakehya, Hakan, "Gözetim ve Suçla Mücadele: Gözetimin Tarihsel Gelişimi ile Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme", Ankara Üniversitesi Hukuk Fakültesi Dergisi, c: 58, y: 2009.

Kilkelly, Ursula, Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Kılavuz, İnsan Hakları El Kitapları No: 1, Almanya, 2001.

Korkmaz, İbrahim, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara, 2019.

McLean, Sarah J. - Worden, Robert E. - Kim, MoonSun, "Here's Looking at You: An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder", Criminal Justice Review, vol. 38, issue: 3, 2013.

Ocak, Mahir E., "Yapay Zekayı Kandırmak", Bilim ve Teknik, Aralık 2019, y: 53, sayı: 62.

Özbek, Veli Özer - Doğan, Koray - Bacaksız, Pınar, Ceza Muhakemesi Hukuku, Ankara, 2019.

Özkan, Halid, "Mobese İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi", Ceza Hukuku Dergisi, c: 11, sayı: 30, 2016.

Öztürk, Bahri - Eker Kazancı, Behiye - Soyer Güleç, Sesim, Ceza Muhakemesi Hukukunda Koruma Tedbirleri, Ankara, 2019.

Öztürk, Bahri - Tezcan, Durmuş - Erdem, Mustafa Ruhan - Gezer, Özge Sırma - Kırıt, Yasemin F. Saygılar - Akcan, Esra Alan - Tütüncü, Efser Erden - Özaydın, Özdem - Altınok Villemin, Derya - Tok, Mehmet Can, Ana Hatlarıyla Ceza Muhakemesi Hukuku, Ankara, 2019.

Piza, Eric L. - Welsh, Brandon C. - Farrington, David P. - Thomas, Amanda L., "CCTV Surveillance for Crime Prevention", Criminology and Public Policy, vol. 18, issue: 1, 2019.

Rottmeier, Christian - Eckel, Philipp, "Die Entschlüsselung biometrisch gesicherter Daten im Strafverfahren", NStZ., heft: 4, 2020.

Salzmann, Miriam - Schindler, Stephan, "Polizeiliche Gesichtserkennung in Deutschland", ZD - Aktuell, heft: 18, 2018, 06344.

Sert, Şeyma, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Ankara, 2019.

Streed, Michael W., Creating Digital Faces for Law Enforcement, Amsterdam 2017.

Szegedy, Christian - Zaremba, Wojciech - Sutskever, Ilya - Bruna, Joan - Erhan, Dumitru - Goodfellow, Ian - Fergus, Rob, Intriguing Properties of Neural Networks, International Conference on Learning Representations, 2014.

Şimşek, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, 2008.

The Law Society Commission on the Use of Algorithms in the Justice System - The Law Society of England and Wales, Algorithms in the Criminal Justice System, Haziran 2019.

Thiel, Markus, "Die Vermessung der Welt? - Zur Nutzung biometrischer Identifikationssysteme durch die Sicherheitsbehörden", Zeitschrift für Rechtspolitik, heft: 8, 2016.

Universities' Police Science Institute - Crime and Security Research Institute - Cardiff University, An Evaluation of South Wales Police's Use of Automated Facial Recognition, Eylül 2018.

Wendt, Kai, "Rechtsgrundlage zur automatisierten Gesichtserkennung in Strafverfahren", ZD-Aktuell, heft: 19, 2018, 06364.

Yayla, Ahmet S. - Hastings, Samantha K., "An Exploration of Using Face Recognition Technologies for National Security", Polis Bilimleri Dergisi, c: 6, sayı: 1-2, 2004, s. 141-157.

Yenisey, Feridun - Nuhoğlu, Ayşe, Ceza Muhakemesi Hukuku, Ankara, 2019.

Yenisey, Feridun, "Aleni Alanların Video Kamera ile Denetlenmesi", (http://www.caginpolisi.com.tr/eski_sitemiz/120/8-9.htm).

Yeung, Karen, "Hypernudge: Big Data as a Mode of Regulation by Design", Information, Communication & Society, yıl: 2016, 20/1, 1-19.

Çevrimiçi Kaynaklar

http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-101536&filename=001-101536.pdf

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

http://www.caginpolisi.com.tr/eski_sitemiz/120/8-9.htm

http://www.ceza-bb.adalet.gov.tr/makale1-2.htm

http://www.hurriyet.com.tr/avrupa/azinlik-raporu-filmi-gercek-oluyor-sucu-islenmeden-onleme-donemi-basliyor-41035280

https://en.wikipedia.org/wiki/Facial_recognition_system#cite_note-47

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680

https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-687182-694690%22]}

https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-122859%22]}

https://medium.com/patron-ai/viola-jones-algoritması-ile-yüz-tespiti-türkçe-38ea73c910e3

https://nayn.co/amazona-irkcilik-suclamasi-yuz-algilama-servisi-cinsiyetci-ve-irkci/

https://sozluk.gov.tr/?kelime=

https://support.apple.com/en-us/HT208108

https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

https://www.+nicid.eu/face-recognition/

https://www.bbc.com/news/uk-48315979

https://www.bbc.com/turkce/haberler-dunya-39599214

https://www.bbc.com/turkce/haberler-dunya-44865198

https://www.biometricupdate.com/202004/israeli-military-grade-biometric-facial-recognition-works-with-face-masks

https://www.echr.coe.int/Documents/CP_Turkey_ENG.pdf

https://www.eff.org/files/2013/11/07/09-facial_recognition_pia_report_final_v2_2.pdf

https://www.eff.org/pages/face-recognition

https://www.electronicid.eu/en/blog/post/biometric-facial-recognition/en

https://www.electronicid.eu/face-recognition/

https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

https://www.forbes.com/sites/thomasbrewster/2020/06/11/microsoft-urged-to-follow-amazon-and-ibm-stop-selling-facial-recognition-to-cops-after-george-floyds-death/#7dddc385b6b4

https://www.gov.uk/government/speeches/surveillance-camera-commissioners-ifsec-speech

https://www.govtech.com/question-of-the-day/Question-of-the-Day-for-05122020.html

https://www.guvenlikonline.com/makale/564/-kalabalikta-yuz-tanima-nasil-calisir.html

https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html

https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

https://www.interpol.int/How-we-work/Forensics/Facial-Recognition

https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu

https://www.legal-tools.org/doc/6e49ed/pdf/

https://www.log.com.tr/cin-yapay-zeka-tarafindan-yonetilen-insansiz-polis-istasyonu-hazirliginda/

https://www.masslive.com/news/2020/01/cambridge-bans-facial-recognition-technology-becoming-fourth-community-in-massachusetts-to-do-so.html

https://www.milliyet.com.tr/teknoloji/ingiliz-polisi-sucu-onlemek-icin-yapay-zeka-kullanacak-2786584

https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html#:~:text=SEATTLE%20%E2%80%94%20Amazon%20said%20on%20Wednesday,unfair%20treatment%20of%20African-Americans.

https://www.perpetuallineup.org/

https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/

https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/

https://www.research-live.com/article/news/police-should-slow-down-facial-recognition-says-ico/id/5061042

https://www.sabah.com.tr/dunya/2018/07/31/abdde-yuz-tanima-teknigi-irkci-cikti

https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it