

GLUKHIN v RUSYA: KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA CEZA ADALET SİSTEMİNDE KİMLİK TESPİTİ AMACIYLA YÜZ TANIMA

Glukhin v Russia:

*Facial Recognition for Identification Purposes in the Criminal Justice System
in the Context of Protection of Personal Data*

Emre Oğuz MERİÇ*

Özet

Kameralı gözetim araçlarının yaygınlaşması ve teknolojideki gelişim, daha fazla görüntünün elde edilmesine ve yüz tanıma sistemlerinin yaygınlaşmasına zemin hazırlamıştır. Kişilerin benzersiz veya ayırt edici özelliği niteliğindeki yüz şablonlarını işleyen yüz tanıma sistemleri, biyometrik teknolojiler kullanır. Nitekim işlenen yüz şablonları da biyometrik kişisel veri niteliğindedir. Dolayısıyla yüz tanıma sistemlerinin yüz şablonlarını işleyebilmesi, veri korumaya dair temel ilke ve kurallara uyulmasına ve özel nitelikli veriler için öngörülen ek güvencelerin sağlanmasına bağlıdır. Kişisel verileri Sözleşmenin 8. maddesi bağlamında değerlendiren Avrupa İnsan Hakları Mahkemesi de biyometrik verilerin elde edilmesi, saklanması ve işlenmesine dair içtihadında uluslararası mevzuatta ortaya konan temel ilke ve kuralları kabul etmektedir. Türkiye'nin ulusal mevzuatına bakıldığında benzer anlayışın benimsendiği görülür. Dört bölümden meydana gelen çalışmada sırasıyla, *Glukhin* kararı özetlenmiş, ardından yüz tanıma sistemlerinin kapsamı ve ceza adalet sistemindeki kullanım biçimleri açıklanmış, sonrasında Mahkemenin içtihat gelişimine değinilerek Türk hukuku bağlamında değerlendirme yapılmıştır. Sonuç kısmında ise yakın gelecekte kolluğun yaka kameraları vasıtasıyla Türkiye'de kullanılması planlanan yüz tanıma teknolojisinin hukuki dayanağı ve uygulamasına dair önerilerde bulunulmuştur.

Anahtar Kelimeler: Yüz tanıma, biyometrik veri, özel nitelikli veri, kişisel veri, özel hayata saygı, veri koruma, yaka kamerası, kapalı devre televizyon

Abstract

The proliferation of video surveillance tools and advances in technology have paved the way for the acquisition of more images and the widespread use of facial recognition systems. Facial recognition systems that process facial templates that are unique or distinctive features of individuals use biometric technologies. As a matter of fact, the processed facial templates are also biometric personal data. Therefore, the ability of facial recognition systems to process facial templates depends on compliance with the basic principles and rules of data protection and the additional

➤ Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.

➤ Makale Geliş Tarihi/Article Received Date: 17.03.2025

➤ Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 22.07.2025

* Arş. Gör., İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Doktora Öğrencisi, Fatih Sultan Mehmet Vakıf Üniversitesi Hukuk Fakültesi Araştırma Görevlisi, Ceza ve Ceza Muhakemesi Hukuku, comeric@fsm.edu.tr, <https://orcid.org/0000-0003-2102-715X>



safeguards provided for special categories of data. The European Court of Human Rights, which evaluates personal data in the context of Article 8 of the Convention, also recognizes the basic principles and rules set out in international legislation in its jurisprudence on the acquisition, storage and processing of biometric data. Turkey's national legislation adopts a similar approach. In the study, which consists of four parts, the *Glukhin* judgment is summarized, followed by an explanation of the scope of facial recognition systems and their use in the criminal justice system, and then the development of the Court's jurisprudence and an evaluation in the context of Turkish law. In the conclusion, recommendations are made regarding the legal basis and implementation of facial recognition technology, which is planned to be used in Turkey in the near future through the body cameras of the police.

Keywords: Facial recognition, biometric data, sensitive data, personal data, respect for private life, data protection, body camera, CCTV

GİRİŞ

Kendisine suç isnat edilen kişinin kimlik tespiti, ceza muhakemesinin sağlıklı işleyişi için önemli ve yargılamada kural olarak gereklidir. Maddi gerçeğe ulaşılması amacına yönelik olarak sadece şüpheli veya sanığın değil, mağdurun da kim olduğunun belirlenmesi ayrıca önem taşır. Ceza yargılamasında kural olarak duruşmada hazır olması gereken sanığa ulaşılabilmesi veya mağdurun tanımlanması, çoğu zaman suç şüphesini doğuran olayın gerçekleştiği yerde bulunan iz, emare ve delillerle mümkün olur. Bu bağlamda 20. yüzyılda adli tıptaki gelişmelerle DNA bilgileri ile parmak izi, kimlik tespitinde önemli bir rol oynamaya başlamıştır. Parmak izi ve DNA üzerinden yapılan bir tespitin, nesnel niteliği, daha az hataya açık olması, hızlı ve başarılı sonuçlar üretmesi, DNA ve parmak izini uzunca bir süre değerli kılmıştır¹.

Günümüz teknolojileri ise kimlik tespitinde yeni bir yöntemi ve yeni bir bilgi türünü cazip hale getirmektedir. Yüz tanıma teknolojisindeki gelişim ile kameraların yaygınlaşması, görüntüler üzerinden kişileri tanımlayabilen oldukça verimli sistemlerin kurulmasına imkân sağlamaktadır.

Yüz görüntülerinden elde edilen ve kişinin benzersiz veya ayırt edici özelliklerini gösteren yüz şablonlarının eşleştirilmesiyle kimlik tespiti yapabilen yüz tanıma sistemleri, biyometrik teknolojiler² kullanır³. Biyometrik teknolojiler kullanan yüz tanıma sistemlerinin işlediği yüz şablonlarının niteliğinin belirlenmesi, veri koruma bağlamında önemlidir. Avrupa veri koruma mevzuatı, kişisel verilerin işlenmesine dair temel ilke ve kurallar öngörmekte, biyometrik verileri hassas veya özel nitelikli veri olarak sınıflandırarak ek güvencelere tabi tutmak-

¹ Simon A. Cole, *Suspect Identities A History of Fingerprinting and Criminal Identification* (Harvard University Press 2002) 217.

² Biyometrik teknolojiler, kişinin kimliğinin tespiti için benzersiz veya ayırt edici insan özelliklerinin toplanması, ölçülmesi ve saklanmasıyla ilgilenir., Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications A Comparative Legal Analysis* (Springer 2013) 19.

³ Roman Amelin and Sergey Channov, 'On the Legal Issues of Face Processing Technologies' in Daniel A. Alexandrov and others (eds), *Digital Transformation and Global Society 5th International Conference* (Springer Nature 2020) 223, 225.

tadır. Avrupa İnsan Hakları Mahkemesi de kişisel verileri özel hayata saygı hakkı bağlamında yorumlarken, Avrupa veri koruma mevzuatında belirtilen temel ilke ve kuralları benimsemektedir. Dolayısıyla yüz tanıma teknolojinin ceza adalet sisteminde kullanımı için kişisel verilerin korunması bağlamında takip edilmesi gereken ilke ve kuralların tespiti, işlenecek verinin niteliğinin belirlenmesi ile verilerin toplanması, işlenmesi ve saklanması şartlarına bağlıdır.

Çalışmada öncelikle ceza muhakemesi sürecinde yüz tanıma teknolojinin kullanımının Avrupa İnsan Hakları Mahkemesi tarafından ilk defa ayrıntılı olarak değerlendirildiği *Glukhin* kararı özetlenmiştir. Takip eden bölümde yüz tanıma sistemlerinde kullanılan teknoloji ve yöntemler açıklanmıştır. Sonrasında Avrupa veri koruma mevzuatına göre yüz şablonlarının biyometrik veri olup olmadığı tespit edilmiş ve bu bağlamda esas alınması gereken ilke ve kurallar ortaya konmuştur.

Üçüncü bölümde Avrupa İnsan Hakları Mahkemesinin içtihat gelişimi üzerinde durularak; Mahkemenin çıkarımları, kişisel verilere dair temel ilke ve kurallar bakımından irdelenmiştir. Son bölümde karar, Türk Hukuku bağlamında değerlendirilmiştir.

Sonuç kısmında ise yakın gelecekte ülkemizde kolluğun yaka kameraları üzerinden uygulamaya konulması planlanan yüz tanıma sistemleri için, olması gereken hukuk ve uygulama bağlamında izlenmesi gereken hususlara dair önerilerde bulunulmuştur.

I. İNCELEME KONUSU KARAR

Çalışmada incelenen karar, Avrupa İnsan Hakları Mahkemesi tarafından 4 Temmuz 2023 tarihinde verilen 11519/20 numaralı karardır⁴.

A. Olaylar

Moskova Belediye Başkanlığının resmi internet sitesi üzerinden verilen bilgilere göre Mayıs 2017 itibarıyla Moskova’da 3500’den fazla CCTV⁵ kamerası kurulmuştur. Aynı yılın Eylül ayında 3000’den fazla CCTV kamerası canlı yüz tanıma⁶ sistemiyle donatılmıştır. 2018 yılında Moskova metrosuna yüz tanıma

⁴ İçtihat gelişiminin değerlendirildiği üçüncü bölümdeki Mahkeme çıkarımlarını tekrar etmemek amacıyla ve çalışmanın hacmi dikkate alınarak kararın tamamına yer verilmemiş; yalnızca olayların ve Mahkemenin değerlendirmesindeki yeni ve önemli hususların aktarılmasıyla yetinilmiştir.

⁵ “CCTV”, kapalı devre televizyon (“closed-circuit television”) kavramının kısaltması olarak kullanılmaktadır ve aynı zamanda video gözetim ya da kameralı gözetim (“video surveillance”) olarak da adlandırılmaktadır. Belirli bir alanı izleyen bir kamera veya bir dizi kameradan oluşan ve elde edilen görüntüleri izlemek ve/veya saklamak için kullanılan ek ekipmana sahip bir televizyon sistemidir. Kapalı devre olması sebebiyle sınırlı sayıda izleyicisi olur. <https://www.edps.europa.eu/data-protection/data-protection/glossary/c_en#cctv> erişildi 3 Şubat 2025.

⁶ Canlı yüz tanıma (“live facial recognition”), bir kamera tarafından yakalanan yüzlerin, izleme listesinde yer alan ilgili kişilerin yüz görüntüleriyle karşılaştırılarak gerçek zamanlı olarak eşleştirme yapılmasını ifade eder. The European Commission, *Summary Report of the project “Towards the*

sistemine uyumlu CCTV kameralar yerleştirilmiştir ve canlı yüz tanıma sistemi 2019 yılında test edilmiştir. 1 Eylül 2020 itibariyle yaklaşık 175 bin adet olan Moskova'daki tüm CCTV kameralar, canlı yüz tanıma teknolojisi kullanabilir hale getirilmiştir⁷.

İnternetin rutin olarak izlenmesi sırasında polis, bir çevrimiçi sosyal paylaşım ve sohbet platformu olan *Telegram*'da herkese açık bir kanalda yayınlanan başvurunun yer aldığı fotoğraflar ve bir video keşfetmiştir. Polis, fotoğraf ve videolardan ekran görüntüleri alarak muhafaza etmiş ve iddiaya göre başvurunun kimliğini belirlemek için bunlara yüz tanıma teknolojisi uygulamıştır. Videodaki yerin Moskova metrosunun istasyonlarından biri olduğunu tespit eden polis, bu istasyonda ve başvuranın geçiş yaptığı diğer iki istasyonda bulunan CCTV kameralarından video kayıtları toplamıştır. Video kayıtlarından da ekran görüntülerini almış ve muhafaza etmiştir. İddiaya göre ayrıca kabahat işlediğinden bahisle başvuru- cuyu tespit etmek ve yakalamak için Moskova metrosuna yerleştirilen ve canlı yüz tanıma sistemi kullanan CCTV kameralarından yararlanılmıştır. Telegram kanalı ile CCTV kameralarından alınan video kayıtlarının ekran görüntüleri, daha sonra başvuru aleyhinde yürütülen kabahat⁸ yargılamasında delil olarak kullanılmıştır⁹.

Moskova Meshchanskiy Bölge Mahkemesi, başvurucuya isnat edilen suçun işlendiğini sabit görürken; diğer delillerin yanı sıra, *Telegram*'dan elde edilen ekran görüntüleri ile CCTV kameralarından alınan video kayıtlarının ekran görüntülerine dayanmıştır¹⁰.

B. Mahkeme'nin Değerlendirmesi ve Kararı

Mahkeme, Sözleşme'nin 8. maddesi bağlamında başvuruyu kabul edilebilir bulduktan sonra yerleşik inceleme yöntemine göre önce müdahalenin varlığını araştırmış ve sonrasında müdahalenin ilgili maddeye göre ihlal meydana getirip getirmediğini değerlendirmiştir.

1. Müdahalenin Varlığı

Bireyin özel hayatına ilişkin verilerin yalnızca depolanması, 8. madde bağlamında bir müdahale doğurur. Saklanan bilgilerin daha sonra kullanılmasının, bu tespit üzerinde bir etkisi yoktur¹¹.

European Level Exchange of Facial Images” 7 <<https://www.telefi-project.eu/telefi-project/results>> erişildi 26 Kasım 2024.

⁷ *Glukhin v Rusya* App no 11519/20 (ECtHR, 4 Temmuz 2023) para 5.

⁸ “*Administrative offence*” kavramı kabahat olarak çevrilmiştir.

⁹ ibid 68.

¹⁰ ibid 15.

¹¹ ibid 65.

Mevcut davada, Mahkeme'nin konuyla ilgili özel sorusuna rağmen başvurunun kimliğini ve yerini tespit etmek için yüz tanıma teknolojisinin kullanıldığı iddiaları hakkında Hükümet yorum yapmamıştır. Ulusal hukukun yüz tanıma teknolojisinin kullanımına ilişkin kayıt veya bildirim öngörmemesi nedeniyle başvurunun iddialarını ispat etmesinin zorluğunu, başvurunun kimliğinin hızlı bir şekilde tespit edilmesine ilişkin başka bir açıklama bulunmamasını ve Hükümet tarafından canlı yüz tanıma teknolojisinin kullanıldığının zımnen kabul edilmesini dikkate alan Mahkeme, mevcut davanın özel koşullarında yüz tanıma teknolojisinin kullanıldığını kabul etmiştir¹².

Mahkeme önceki kararlarında fotoğrafların polis tarafından saklanması ve bu fotoğraflara yüz tanıma teknikleri uygulanma olasılığının, özel yaşam hakkına müdahale teşkil ettiğine karar vermiştir. Mevcut davada da Mahkeme, yüz tanıma teknolojisiyle fotoğraf ve videolardan kimlik ve yer tespiti yapılarak aleyhindeki idari ceza yargılaması çerçevesinde başvurunun kişisel verilerinin işlenmesinin, Sözleşmenin 8 § 1 maddesi anlamında özel hayatına saygı hakkına bir müdahale teşkil ettiği sonucuna varmıştır¹³.

2. Müdahalenin Haklılığı

Mevcut davada Mahkeme, kanunilik ve meşru bir amacın varlığı kistaslarının, müdahalenin “*demokratik bir toplumda gerekli*” olup olmadığı kistasından ayrı tutulamayacağı sonucuna varmış ve tümünü birlikte değerlendirmiştir¹⁴.

Mahkemeye göre yüz tanıma teknolojisinin uygulanması bağlamında, tedbirlerin kapsamını ve uygulanmasını düzenleyen ayrıntılı kuralların yanı sıra kötüye kullanım ve keyfilik riskine karşı güçlü güvencelere sahip olunması gerekir. Canlı yüz tanıma teknolojisinin kullanımı söz konusu olduğunda ise güvencelere duyulan ihtiyaç artar. Mevcut davada gösterilen iç hukuk düzenlemeleri yeterli nitelikte değildir. “*Adalet yönetimi*”¹⁵ ile bağlantılı olarak (“*in connection with the administration of justice*”) biyometrik kişisel verilerin işlenmesine izin veren hüküm geniş bir biçimde formüle edilmiştir. Hükümetin bu hükümle

¹² ibid 69-72.

¹³ ibid 72-73.

¹⁴ ibid 78.

¹⁵ Adalet yönetimi, devletlerin cezai, idari ve medeni yönden adalet dağıtımında hakkaniyet ve verimlilik sağlamaya çalıştıkları, normları, kurumları ve sistemleri içeren geniş bir terimdir. Adalet yönetimine uygulanacak kurallar çok çeşitli olmakla birlikte özellikle adil yargılanma, masumiyet karinesi, mahkemenin bağımsızlığı ve tarafsızlığı ile hak arama özgürlüğünü içerir. Ceza adalet sistemi bağlamında ayrıca soruşturma ve kovuşturma yapılması, tutuklama ve hüküm kurma gibi işlem ve faaliyetler adalet yönetime ilişkindir. David Weissbrodt, ‘The Administration of Justice and Human Rights’ (2009) 1 City University of Hong Kong Law Review 23, 23. Sözleşmenin 6. maddesi bağlamında değerlendirme yapan Avrupa İnsan Hakları Mahkemesine göre demokratik bir toplumda, adalet yönetimi o kadar önemli bir yere sahiptir ki, 6. maddenin 1. paragrafının kısıtlayıcı bir şekilde yorumlanması, bu hükmün amacına ve hedefine uygun olmaz. *Delcourt v Belçika* App no 2689/65 (ECtHR, 17 January 1970), para 25.



ilgili herhangi bir yüksek mahkeme yorumuna atıfta bulunmaması, idari ve adli uygulamada kısıtlayıcı bir yoruma dair örnek sunmaması dikkate alındığında; herhangi bir adli işlemle bağlantılı olarak yüz tanıma teknolojisinin kullanımı da dahil olmak üzere biyometrik kişisel verilerin işlenmesine izin verildiği görülmektedir. İç hukuk, yüz tanıma teknolojisinin kullanımını gerektirecek hallerin niteliği, izlenen amaçlar, hedef alınabilecek kişi kategorileri veya hassas kişisel verilerin işlenmesine ilişkin herhangi bir sınırlama içermemektedir. Ayrıca Hükümet, yetkilendirme, elde edilen verilerin incelenmesi, kullanılması ve saklanmasıyla ilgili düzenlemeler, herhangi bir denetim kontrol mekanizması veya kanuni çareler gibi Rusya’da yüz tanıma teknolojisinin kullanımına eşlik eden herhangi bir usuli güvenceye atıfta bulunmamıştır¹⁶.

Kişisel verilerin soruşturmalar bağlamında işlenmesinin “*demokratik bir toplumda gerekliliği*” değerlendirilirken, söz konusu suçların niteliği ve ağırlığı dikkate alınması gereken unsurlardan biridir. Mevcut davada iç hukuk, niteliğine ve ağırlığına bakılmaksızın, herhangi bir suçun soruşturulması ve kavuşturulmasıyla bağlantılı olarak biyometrik kişisel verilerin işlenmesine izin vermektedir. *Telegram*’da yayınlanan fotoğraf ve videolardan başvurunun kimliğini tespit etmek ve bunun da ötesinde Moskova metrosunda seyahat ederken yerini tespit ederek yakalamak için canlı yüz tanıma teknolojisinin kullanılması “zorlayıcı bir toplumsal ihtiyaca” (“*pressing social need*”) karşılık gelmemiştir¹⁷.

Tüm değerlendirmeler sonucunda Mahkeme, başvurunun Sözleşmeyle korunan ifade özgürlüğü bağlamında son derece müdahaleci yüz tanıma teknolojisinin kullanılmasının, Sözleşmenin korumak ve geliştirmek için tasarladığı hukukun üstünlüğüyle yönetilen demokratik bir toplumun idealleri ve değerleri ile bağdaşmadığı sonucuna varmıştır. Başvurunun kişisel verilerinin idari ceza yargılaması çerçevesinde yüz tanıma teknolojisi kullanılarak işlenmesi “demokratik bir toplumda gerekli” olarak kabul edilemez¹⁸.

Sonuç olarak Sözleşmenin 8. maddesi ihlal edilmiştir¹⁹.

II. YÜZ TANIMA SİSTEMLERİ

Suçların önlenmesi ve ceza muhakemesi sürecinin tamamlanabilmesi için şüpheli, sanık veya ilgili diğer kişilerin kimlik tespiti önem taşır. Kimlik tespiti amacıyla bilimsel tekniklerin ve uzmanlıkların ortaya çıkışı ve kullanımı özellikle 20. yüzyılla birlikte oldukça artmıştır²⁰.

¹⁶ Glukhin v Rusya (n 7) paras 82-83.

¹⁷ ibid 87-89.

¹⁸ ibid 90.

¹⁹ ibid 91.

²⁰ Sertel Şıracı, ‘Yüz Tanıma Teknolojilerinin Kişisel Verilerin Korunması Hukuku Açısından İncelenmesi’ (2023) 5 [1] Kişisel Verileri Koruma Dergisi 23, 24.

Adli tıptaki gelişmelerle kimlik tespiti için ortaya çıkarılan yeni yöntemler, çeşitli bilgilerin özel teknik usullerle kullanılmasını gerektirmiştir. Parmak izi, DNA profilleri, dövmeler veya ses bu bilgilere örnek gösterilebilir²¹. Değerlendirilen diğer bir bilgi ise yüz görüntüleri ve bu bağlamda kullanılan teknik ise yüz tanımadır.

Yüz tanımaya dair ilk çalışmalar olan vücut şeklinin ölçülmesi ve yüz karşılaştırması 19. yüzyılın ortalarında yapılmaya başlanmış olsa da fotoğraf ve videoların yaygınlaşmasıyla diğer bir ifadeyle görüntülerin fiziksel bir nesne halinde veya dijital ortamda veri şeklinde saklanabilecek hale gelmesiyle yüz görüntülerinin kimlik tespitinde kullanımı artmıştır. Örneğin bir fotoğraf veya güvenlik kamerasının çektiği videodaki kişinin, kendisine suç isnat edilen kişi olup olmadığının tespitinde mağdur ve tanığın yanı sıra yüz görüntüsü analizi uzmanlığı olan bilirkişinin görüşünden yararlanılabilmesi mümkün hale gelmiştir. Geleneksel sayılabilecek bu yöntem esasında insanın zihinsel kapasitesi veya bilgi birikiminin başarısına dayanırken kimlik tespitinde sıklıkla kullanılan diğer yöntemler olan parmak izi veya DNA analizinden farklılık gösterir. Parmak izi üzerinden veya DNA analiziyle yapılan kimlik tespiti, insanlar tarafından gerçekleştirilen geleneksel yüz tanımaya göre daha hızlı ve daha az hataya açıktır, daha az donanım ve eğitim gerektirir. Bu sebeple vücut şeklinin ölçülmesi ve yüz karşılaştırması daha eski tarihlerde ortaya çıkarılmasına rağmen 20. yüzyılın başından itibaren parmak iziyle tanımlama yaygınlık kazanmış; benzer biçimde DNA profillemeye de sıklıkla tercih edilen bir yöntem olarak benimsenmiştir. Diğer taraftan öznel görüşlerin baskın olduğu geleneksel yüz görüntüsü analizinin güvenilirliğine dair endişeler ortaya çıkmıştır. Yapılan araştırmalara göre, insanlar tanıdık yüzleri oldukça iyi tespit ederken, tanımadıkları insanların yüzlerini tespit etmede oldukça hatalı sonuçlara varmaktadırlar²².

Mevcut yüz tanıma teknikleri ise bu durumu tersine çevirebilecek bir sistem vadetmektedir. Nitekim yüz görüntülerinin artık yeni teknolojiler kullanılarak²³ bilgisayarlar tarafından işlenmesi mümkündür. Günümüzde yüz görüntülerinin elde edilmesi, depolanması ve bunların hızlı bir biçimde işlenerek sonuç çıkarması

²¹ William J. Tilstone, 'Scientific Basis of the Forensic Process' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer Science Business Media 2014) 4672, 4676.

²² Martin Paul Evison, 'Forensic Facial Analysis' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer Science Business Media 2014) 1713, 1713-24.

²³ Optik alanındaki gelişmelerle yüksek çözünürlüklü görüntü yakalayabilen kameraların yaygınlaşmasının, yüz tanıma teknolojilerinin verimliliğini artırarak yaygınlaşmasına zemin hazırladığı söylenebilir. Şıracı (n 20) 24. Açık, ölçek ve aydınlatma gibi değişkenlerden kaynaklanan görüntüler arasındaki farkları en aza indirmek için geliştirilen yeni teknikler için ayrıca bakınız Amelin and Channov (n 3) 224.



ılması noktasındaki yeni gelişme ve imkânlar, yüz tanıma sistemlerinin yaygınlaşmasına zemin hazırlamaktadır.

Yüz tanıma sistemlerini ve görüntüleri, parmak izi ve DNA analizinden üstün kılabilecek temel husus ise elde edilebilecek veri sayısıdır. Otomatik veri işleyen sistemlerin verimliliğinin, veri sayısı ile doğru orantılı artması²⁴ yüz tanıma sistemlerini öne çıkarır. Sürücü belgesi veya pasaport başvurusunda bulunulması gibi çeşitli işlemlerde yüz görüntüleri alınıp saklanabilmektedir. Bunun yanı sıra görüntü ve video yakalayan cihazların, kamu alanlarında yaygınlaşmaya devam etmesi, polis yaka kameralarıyla mobil hale gelmesi, yüz tanımayı diğer yöntemlerin önüne geçirebilir. Nitekim, uzun yıllar güvenilir bir yöntem olarak görülen parmak izi ve DNA profileme için ilgili bilgilerin olay yerinde bulunması gerekirken; yüz görüntüleri her geçen gün artan bir hızla toplanmaya devam edilmekte ve yüz tanıma için yeterli veriyi oluşturmaktadır.

A. Yüz Tanımadaki Kullanılan Teknoloji ve Yöntemler

Günümüz teknolojileri bağlamında yüz tanıma sözlükte “bilgisayarın, bir kişinin yüzünün dijital²⁵ görüntüsünü tanımasını mümkün kılan teknoloji” biçiminde ifade edilmektedir²⁶. Kullanılan teknoloji, bir fotoğraf veya videodan yüzün farklı özelliklerinin dijital bir temsilini çıkarır ve bu şablon (“*template*”) olarak adlandırılır²⁷. Sonrasında bir veya daha fazla farklı şablonla karşılaştırma yapılarak yüzün tanınması sağlanır²⁸.

Yüz tanıma, fotoğraf ve video görüntüsü işleme tekniklerinin bir parçasıdır. Nitekim video kameralar belirli bir alandaki insanların görüntülerini kaydetse de her kamerada yüz tanıma sistemi bulunmaz. Biyometrik veri toplayan ve iş-

²⁴ Yüz tanımanın verimli sonuçlar üretmesi yararlanılan teknoloji kadar kullanılabilir mevcut verinin hacminde bağlıdır. ibid 224.

²⁵ Dijital, bilginin 1 ve 0 sayılarından oluşan bir dizi olarak kaydedilmesi veya saklanması anlamına gelir. <<https://dictionary.cambridge.org/dictionary/english/digital>> erişildi 16 Ocak 2025; Bilgisayarlar tarafından kullanılan bu bilgiyi muhafaza etme biçimi, dijitalleşebilen her türlü bilginin işlenmesini kolaylaştırıp yaygın hale getirmiştir. Ethem Alpaydın, *Machine Learning* (The MIT Press 2021) 2-3.

²⁶ <<https://dictionary.cambridge.org/dictionary/english/facial-recognition>> erişildi 16 Ocak 2025.

²⁷ European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* 7 <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en> erişildi 20 Ocak 2025; Biyometrik şablon, biyometrik bir örnekten çıkarılan ve biyometrik bir veri tabanında saklanan benzersiz özelliklerin dijital bir temsildir. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on Facial Recognition* (2021) 9 <<https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html>> erişildi 20 Ocak 2025.

²⁸ European Data Protection Board (n 27) 7.

leyen yüz tanıma sistemlerinin video veya fotoğraf çeken araçlara ayrıca entegre edilmesi gerekir²⁹.

Günümüzde yararlanılan yüz tanıma teknolojisi bir biyometrik görüntü yakalama aracıdır³⁰. Yüz tanıma sistemlerinin kullandığı biyometrik teknolojiler, bir kimliğin otomatik olarak doğrulanması veya bir kişinin tanımlanması için bireylerin benzersiz veya ayırt edici biyolojik ve/veya davranışsal özelliklerini toplar ve genellikle saklar³¹. Yararlanılan bu teknoloji üç temel yöntem kullanır. Bunlar doğrulama (“*verification*”/“*authentication*”), tanımlama (kimlik tespiti/“*identification*”) ve sınıflandırma (“*categorisation*”) olarak adlandırılır³². Doğrulama ve tanımlama, bireylerin benzersiz özelliklerini karşılaştırırken; sınıflandırma, bir bireyin biyometrik özelliklerine dayanarak belirli bir gruba ait olup olmadığını belirlemeye çalışır³³. Doğrulama ve tanımlama arasındaki ayrım ise, ihtiyaç duyulan biyometrik veriler ile bunların kullanımına dair ortaya çıkan sorunların çözümü için önem arz eder³⁴.

Doğrulama, sisteme sunulan biyometrik özelliği belirli bir biyometrik özelliklerle karşılaştırır. Genellikle aynı kişiye ait olduğu varsayılan iki özelliğin eşleştirilmeye çalışıldığı bu yöntem, “bire bir (1:1) karşılaştırma” olarak da adlandırılır³⁵.

Doğrulamanın farklı kullanım alanları vardır. Kullanıcıların tam kontrole sahip olduğu akıllı telefon gibi cihazların kilidini açmak, kamu veya özel hizmetlerden faydalanmak amacıyla dijital kimlik oluşturmak, bina girişleri veya belirli sınırlardan ya da noktalardan geçmek için yüz tanımayla doğrulama ya-

²⁹ ibid 7.

³⁰ Ian Berle, *Face Recognition Technology Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images* (Springer Nature 2020) 9.

³¹ Kindt (n 2) 36.

³² European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* 7-8 <<https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law#publication-tab-7>> erişildi 21 Ocak 2025; Avrupa Birliği bünyesinde 1995 tarihinde ortaya çıkarılan 95/46/EC sayılı Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif’in 29. maddesi uyarınca kurulan Çalışma Grubu’nun (“*Article 29 Data Protection Working Party*”) “çevrimiçi ve mobil hizmetlerde yüz tanıma hakkında 02/2012 sayılı görüş” yazısına göre yüz tanıma, bireylerin yüzlerini içeren dijital görüntülerin, bu bireylerin tanımlanması, doğrulanması veya sınıflandırılması amacıyla otomatik olarak işlenmesidir. Article 29 Data Protection Working Party, *Opinion 2/2012 on facial recognition in online and mobile services* 2 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> erişildi 21 Ocak 2025.

³³ European Union Agency for Fundamental Rights (n 32) 7; Sınıflandırmada amaç, bireyi tanımlamak veya doğrulamak değil onu bir sınıfa dahil ederek belirli bir fiil veya işlemde bulunmaktır. Örneğin bir reklam ekranı, kendisine bakan bireyin yaşına veya cinsiyetine bağlı olarak farklı reklamlar gösterebilir. Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies* 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> erişildi 28 Ocak 2025.

³⁴ Kindt (n 2) 36.

³⁵ ibid 36.



pılabilir³⁶. Hava limanlarına veya ceza infaz kurumlarına girişlerde yolcunun veya müdafinin kimliği doğrulanarak geçiş yapmasına izin verilebilir³⁷. Otomatik Sınır Kontrol (“*Automated Border Control*” - ABC) sistemleri, doğrulamanın günümüzde en yaygın kullanım biçimlerinden biridir. Sınırı geçmek isteyen kişi pasaportta yer alan fotoğrafı taratırken aynı zamanda kendisinin yüz görüntüsü alınır. Yüz tanıma teknolojisi kullanan sistem, elde edilen iki yüz görüntüsünü karşılaştırır ve bunların aynı kişiyi gösterme olasılığı belirli bir eşiğin üzerindeyse kimlik doğrulanır. Verilen bu örnekte bir veri tabanından bilgi çekilmez, her iki yüz görüntüsü de karşılaştırma öncesi toplanır. Dolayısıyla doğrulama yapan çoğu sistem biyometrik özelliklerin merkezi bir veri tabanında depolanmasını gerektirmez. Doğrulanacak kişiden eşleştirmenin hemen öncesinde alınan yüz görüntüsü, kimlik veya seyahat belgesi gibi bir taşıyıcıda saklanan biyometrik verilerle karşılaştırılarak sonuca ulaşılır³⁸.

Doğrulamanın aksine tanımlama veya kimlik tespiti yönteminde ise sisteme sunulan biyometrik özellik, bir veya daha fazla veri tabanında depolanmış olan biyometrik verilerin tümüyle karşılaştırılır. Yüz tanıma sistemleri bağlamında söylemek gerekirse bir yüz görüntüsü veri tabanında yer alan birçok yüz görüntüsüyle eşleştirilmeye çalışılır. Bu sebeple “bire çok (1:N) karşılaştırma” ismini de taşır. Kullanılan teknoloji iki görüntünün aynı kişiye ait olma olasılığını gösteren bir puan verir. Doğrulamada olduğu gibi puan belirli bir eşiğin üzerindeyse kullanıcıya olası bir eşleşme olduğu bilgisi verilir³⁹.

Tanımlamanın çeşitli uygulama biçimleri vardır. Bireylerin kamusal alanda tanımlaması yapıp hareketleri izlenebilir, sosyal ağdaki ilişkilerini belirlemek için kullanılabilir veya bir bankamatikte yapılan tanımlamayla kişinin banka hizmetlerine kolayca erişimi sağlanabilir⁴⁰.

Her iki yöntemin işlevini ve ortak yönünü kısaca tekrar etmek gerekirse, hem doğrulama hem de tanımlama biyometrik şablonlar arasında tahmini bir eşleştirme yapar ve çıktı olarak bir olasılık sunar. Hesaplanan bu olasılık, karşılaştırılan yüzlerin aynı kişiye ait olma ihtimalidir. Olasılık, kullanıcı veya sistemin geliştiricisi tarafından belirlenen bir eşiği aşarsa, sistem bir eşleşme olduğunu varsayar ve bu eşleştirmeyi kullanıcıya sunar⁴¹.

Yöntemlerin farklılıkları ise farklı yapıda sistemlerin kurulmasını gerekli kılar. Doğrulama çoğu durumda veri tabanı gerektirmez ve sadece istisnai hallerde belirli bir biyometrik özellik setinin merkezi veya yerel olarak depolan-

³⁶ European Data Protection Board (n 27) 9.

³⁷ Şıracı (n 20) 24.

³⁸ European Union Agency for Fundamental Rights (n 32) s. 7.

³⁹ Kindt (n 2) s. 37; European Union Agency for Fundamental Rights (n 32) 7-8.

⁴⁰ European Data Protection Board (n 27) 9-10.

⁴¹ ibid 7-8.

masına ihtiyaç duyarken; tanımlama, biyometrik verilerin muhafaza edildiği bir veri tabanını gerektirir⁴².

Çalışmaya esas alınan *Glukhin* kararında Mahkemenin özel hayata saygı ve kişisel verilerin korunması bağlamında yüz tanıma teknolojisini değerlendirirken üzerinde durduğu hususlardan bir tanesi verilerin elde edilme, saklanma ve işleme koşullarıdır. Diğer bir husus ise yüz tanıma sistemlerinin kullandığı verilerin, biyometrik veri niteliğidir. Zira kişisel verilerin korunmasına dair ortaya çıkarılan ulusal ve uluslararası mevzuatta biyometrik veriler, hassas veya özel nitelikli veri olarak adlandırılır ve işlenmesine karşı ek güvenceler öngörülür. Bu bağlamda da yüz tanıma sistemleri tarafından kullanılan verilerin, uluslararası veri koruma mevzuatında yer alan tanımlara göre biyometrik veri niteliğinde kabul edilip edilemeyeceğinin belirlenmesi önem taşır.

B. Biyometrik Veri

El, ayak veya parmak izi gibi benzersiz özelliklerin insanı tanımlamak için kullanılabileceği, içinde bulunduğumuz yüzyılın çok daha öncesinde fark edilmiştir. Bununla birlikte yakın geçmiş ve günümüzde bilgisayar teknolojisindeki gelişmelerle bilgilerin veri biçiminde depolanabilmesi ve hızlı bir biçimde işlenebilmesi, kimlik tespitinin otomatikleşmesini sağlamıştır⁴³. Biyometrik kavramının, “*otomatik tanıma için kullanılabilen ölçülebilir bir biyolojik (anatomik ve fizyolojik) ve davranışsal özellik*” olarak yapılan tanımı da bu otomatikleşmeye vurgu yapmaktadır⁴⁴. İnsanın ölçülebilir özelliklerinin otomatik olarak işlenerek sonuç çıkarılabilmesiyle yirminci yüzyılın sonunda Avrupa ve Amerika Birleşik Devletleri’nde biyometrik özellikleri kullanan çeşitli büyük ölçekli sistemler kurulmuştur⁴⁵.

Biyometrik terimi Yunanca “*βίος*” (yaşam) ve “*μέτρον*” (ölçü) kelimelerine dayanır ve “*canlı türlerinin ölçümü*” anlamına gelir⁴⁶. Biyometrik teknolojiler ise ayrıntılı bir tanımlamayla, bir kişi tarafından yapılan bir iddianın otomatik olarak doğrulanması veya o kişinin kimliğinin tespiti için benzersiz veya ayırt edici insan özelliklerinin toplanması, ölçülmesi ve saklanması anlamına gelir⁴⁷.

⁴² Kindt (n 2) 37-39.

⁴³ National Science and Technology Council, *Biometrics History* (2006) 1 <<https://www.hsdl.org/c/view?docid=463907>> erişildi 24 Ocak 2025.

⁴⁴ <<https://www.dhs.gov/biometrics>> erişildi 24 Ocak 2025.

⁴⁵ Sığınmacılar ve yabancılar için parmak izi veri tabanı, vize bilgi sistemi ve Schengen bilgi sistemi gibi sistemler hakkında ayrıntılı bilgi için bakınız Kindt (n 2) 65-73; National Science and Technology Council (n 43) 9-24.

⁴⁶ Kindt (n 2) 19; National Science and Technology Council (n 43) 1.

⁴⁷ Kindt (n 2) 19; Avrupa Birliği’nin bağımsız veri koruma otoritesi olarak nitelendirilen Avrupa Veri Koruma Denetçisi’nin (“*The European Data Protection Supervisor*”-EDPS) benzer yöndeki tanımı için bakınız <https://www.edps.europa.eu/data-protection/data-protection/glossary/b_en#biometrics> erişildi 3 Şubat 2025.



Biyometrik veri⁴⁸ kavramı ise, biyometrik teknolojilerin kullandığı, kişiye özgü ve benzersiz nitelikteki biyolojik/fizyolojik ve davranışsal özelliklerden elde edilen kişisel veriler biçiminde tanımlanabilir. Parmak izi, damar veya retina deseni, avuç içi geometrisi, yüz yapısı, el şekli, fizyolojik biyometrik veri niteliğindedir. Davranışsal biyometrik verilere ise kişinin yürüyüş veya konuşma biçimi, akıllı telefon kullanırken ekranı kaydırış biçimi, klavyeye basış biçimi, araba sürüş biçimi örnek gösterilebilir⁴⁹.

1. Uluslararası Metinlerde Biyometrik Veri Kavramı

Avrupa'daki uluslararası veri koruma mevzuatında yer alan biyometrik veri tanımları şunlardır:

- Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde imzalanan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (Sözleşme 108) 2018 yılında kabul edilen bir protokolle güncellenmiştir ve artık Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Sözleşmesi veya Sözleşme 108+ olarak adlandırılmaktadır. Sözleşmeyi güncelleyen çalışmanın açıklayıcı raporunda yer alan tanıma göre biyometrik veri, “*bir bireyin fiziksel, biyolojik veya fizyolojik özelliklerine ilişkin verilerin belirli bir teknik işlemde geçirilmesinden kaynaklanan ve bireyin benzersiz bir şekilde tanımlanmasına veya kimlik doğrulamasına olanak tanıyan verilerdir*”⁵⁰.
- Avrupa Birliği bünyesinde ortaya çıkarılan Genel Veri Koruma Tüzüğü'nün (GDPR) 4. maddesinde yer alan tanıma göre biyometrik veri, “*yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin kimliğinin benzersiz şekilde tespitini sağlayan veya bunu doğrulayan fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak belirli teknik işleme ile ortaya çıkan kişisel verilerdir*”⁵¹. Ceza adalet sistemi içerisinde suçların önlenmesi, ceza muhakemesi süreci ve cezaların infazında kişisel verilerin işlenmesine yönelik uygulama alanı bulacak, polis ve ceza adalet sistemi otoriteleri için

⁴⁸ Avrupa kurum ve kuruluşlarının çoğunun “biyometrik”, “biyometrik veri” ve “biyometrik teknoloji” kavramlarını birbirleri yerine kullandıklarına dair çıkarımlar için ayrıca bkz. Catherine Jasseraud-Breeman, ‘Reprocessing of biometric data for law enforcement purposes: Individuals’ safeguards caught at the Interface between the GDPR and the ‘Police’ directive?’ (PhD thesis, University of Groningen 2019) 55 <<https://research.rug.nl/en/publications/reprocessing-of-biometric-data-for-law-enforcement-purposes-indiv>> erişildi 4 Şubat 2025.

⁴⁹ Kişisel Verileri Koruma Kurumu, *Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber* 5-6 <<https://www.kvkk.gov.tr/Icerik/2030/Rehberler>> erişildi 24 Ocak 2025; Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* 8 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> erişildi 28 Ocak 2025.

⁵⁰ <<https://www.coe.int/en/web/data-protection/convention108-and-protocol>> erişildi 3 Şubat 2025.

⁵¹ <<https://gdpr-info.eu/>> erişildi 4 Şubat 2025; Genel Veri Koruma Tüzüğü'nün resmi olmayan Türkçe çevirisi için ayrıca bakınız <https://www.ab.gov.tr/ab-genel-veri-koruma-tuzugu-gdpr-turkceye-cevrildi_53650.html> erişildi 4 Şubat 2025.

veri koruma alanındaki temel Avrupa Birliği aracı niteliğindeki Avrupa Parlamentosu ve Konsey'in 2016/680 Sayılı Direktifinin⁵² 3. maddesinde de aynı tanım yer almaktadır⁵³.

Tanımlar insanın benzersiz özelliklerine atıf yapsa da biyometrik veriden bahsedebilmek için verinin belirli bir teknik işleme ile ortaya çıkması gerekir⁵⁴. Bu husus Genel Veri Koruma Tüzüğü'nün gerekçe kısmında da ortaya konmaktadır. Örneğin işlenen fotoğraflar her durumda biyometrik ve dolayısıyla hassas veri niteliğinde kabul edilmemelidir. Ancak bunlar biyometrik veri tanımlarında da vurgulandığı üzere bir gerçek kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına olanak tanıyan belirli bir teknik araçla işlendiğinde bu kategori içerisine alınmalıdır.

Günümüzde kimlik tespiti ve kimlik doğrulama için kullanılan yüz tanıma sistemlerinin teknik bir işlemle yüz görüntülerini elde ettiğini kabul etmek gerekir. Sistemlerin kullandığı biyometrik teknolojiler, bir kimliğin otomatik olarak doğrulanması veya bir kişinin tanımlanması için bireylerin benzersiz veya ayırt edici biyolojik ve/veya davranışsal özelliklerini toplar ve genellikle saklar⁵⁵. Diğer bir ifadeyle doğrulama veya tanımlama için yüz biyometrisi çıkarılır⁵⁶. Bu şekilde elde edilen, depolanan ve işlenen yüz görüntüleri de biyometrik veri niteliğindedir⁵⁷.

2. Yüz Tanıma Sistemleri Tarafından Kullanılan Biyometrik Verilerin İşlenmesinde Esas Alınacak İlke ve Kurallar

Biyometrik verilerin toplanması ve işlenmesinin, kişisel verilerin korunması bağlamında ortaya çıkardığı önemli bir husus kişilerin benzersiz özellikleri ile kimlikleri arasındaki ilişkinin kullanım yoğunluğudur. Nitekim biyometrik

⁵² <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>> erişildi 12 Ocak 2025; İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü tarafından hazırlanan Türkçe çeviri için bakınız <<https://itlaw.bilgi.edu.tr/tr/haberler/turkce-tercume-ve-bilgi-notu-27-nisan-2016-tarihli-84/>> erişildi 12 Ocak 2025.

⁵³ Avrupa Birliği bünyesinde Genel Veri Koruma Tüzüğü ceza adalet sisteminde doğrudan uygulama alanı bulmaz. Suçların önlenmesi, tespiti, soruşturulması ve kovuşturulması veya cezaların infazı amacıyla polis ya da adli merciler tarafından yürütülen faaliyetler ve işlemler bakımından 2016/680 Sayılı Direktif uygulanır. Bu sebeple Direktifte yer alan bu tanım ceza adalet sisteminde yüz tanıma teknolojilerinin kullanımı bakımından önem taşır.

⁵⁴ Biyometrik verinin yasal tanımı yapılırken herhangi bir formattan veya verilerin teknik olarak işlenmesinden bahsedilmemesi gerektiği yönündeki görüş ile kavramın uluslararası mevzuat ve öğretilerdeki tanımlarının ayrıntılı bir değerlendirmesi için bkz. Jasserand-Breeman (n 48) 32-55.

⁵⁵ Kindt (n 2) 36.

⁵⁶ Berle (n 30) 2.

⁵⁷ European Union Agency for Fundamental Rights (n 32) 5; Amelin and Channov (n 3) 228; Songül Atak, 'Biyometrik ve Genetik Verilerin Korunması Konusunda Avrupa Konseyi'nin Genel Yaklaşımı' (2024) 60 Türkiye Adalet Akademisi Dergisi 343, 350; Zafer İçer and Elif Dönmez, 'Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları' (2020) 15 [43] Ceza Hukuku Dergisi 421, 432.



teknolojiler, insanın fizyolojik veya davranışsal özelliklerini bilgisayar/makine tarafından okunabilir hale getirmekte ve daha fazla kullanım imkânı sunmaktadır. Kullanımın yaygınlaşması ise başta kişisel veriler olmak üzere temel haklar üzerinde yeni müdahaleler doğurur. Bireylerin otomatik olarak izlenmesine, takip edilmesine veya profillerinin çıkarılmasına olanak tanıyan bu teknolojilerin, özel hayata saygı ve kişisel verilerin korunması hakları üzerinde olası olumsuz etkileri oldukça yüksektir⁵⁸.

Kişisel verilerin korunmasına dair uluslararası mevzuata göre biyometrik veriler, hassas veya özel nitelikli kişisel veriler içerisinde sınıflandırılırken, kişisel veriler için getirilen temel ilke ve kuralların yanı sıra ek güvencelere tabidir. Özel nitelikli kişisel verilerin işlenmesi, temel ilkelere daha fazla müdahale ve ayrımcılık riski barındırdığından ayrıca sınırlamalar getirilmesi tercih edilmektedir⁵⁹. Dolayısıyla özel nitelikli kişisel verilerin elde edilmesi, saklanması ve işlenmesi söz konusu olduğunda hem temel ilke ve kurallara hem de özel ek güvencelere bakmak gerekir.

Avrupa Konseyi bünyesindeki Sözleşme 108+'nın 5. maddesi ile Avrupa Birliği bünyesinde ortaya çıkarılmış 2016/680 Sayılı Direktif'in 4. maddesine bakıldığında, kişisel verilerin işlenmesinde esas alınan temel ilke ve kurallar özetle şunlardır⁶⁰:

- Veriler açık, belirli ve meşru amaçlar için toplanır ve bu amaçlarla bağdaşmayan biçimde işlenemez.
- İşleme tabi tutulan veriler, işlenme amaçlarıyla bağlantılı olarak yeterli ve ilgili olmalı, gereksiz ve aşırı olmamalıdır.
- İşleme tabi tutulan veriler doğru ("*accurate*") olmalı ve gerektiğinde güncellenmelidir.
- Veri sahiplerinin kimliklerinin belirlenmesine izin verecek bir biçimde, bu verilerin işlenme amaçları için gerekli olandan daha uzun süre muhafaza edilmemelidir.
- İşlendikleri amaçlar göz önünde bulundurularak, hatalı verilerin gecikmeksizin silinmesi veya düzeltilmesi için, gerekli her türlü önlem alınmalıdır.
- Veriler hukuka uygun ve adil (dürüstlük kurallarına uygun) işlenmelidir.
- Veri işleme, izlenen meşru amaç bakımından orantılı olmalıdır.

⁵⁸ Article 29 Data Protection Working Party (n 33) 3-4.

⁵⁹ Julie Ringelheim, 'Processing Data on Racial or Ethnic Origin for Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?' (2007) Center for Human Rights and Global Justice Working Paper No. 13 Jean Monnet Working Paper 08/06, 28 <<https://jeanmonnetprogram.org/>> erişildi 15 Ocak 2025.

⁶⁰ Bu ilke ve kurallar ayrıca kanunilik, amaç sınırlaması, veri minimizasyonu, veri doğruluğu, veri güvenliği, şeffaflık, saklama sınırlaması, uygun güvencelerin uygulanması ve hesap verilebilirlik başlıklarıyla da formüle edilebilir.

- Veri işlemeyle elde edilecek faydayla müdahale edilecek hak ve özgürlükler arasında adil bir denge sağlanmalıdır.
- Yetkisiz veya yasadışı işlenmesi ile kazara kayıp, imha veya zararın önlenmesine ilişkin teknik ve idari tedbirlerin uygulanması da dahil olmak üzere, kişisel verilerin güvenliği sağlanmalıdır.

Biyometrik veriler için getirilen ek güvenceler bakımından ise Sözleşme 108+'nın 6. maddesine göre *“bir kişiyi benzersiz bir şekilde tanımlayan biyometrik verilerin işlenmesine, ancak Sözleşme’de öngörülen diğer güvenceleri tamamlayan uygun güvencelerin kanunda yer alması halinde izin verilir. Söz konusu güvenceler başta ayrımcılık riski olmak üzere veri sahibinin menfaatleri, hakları ve temel özgürlükleri açısından olası risklere karşı koruma sağlamalıdır”*.

2016/680 Sayılı Direktif’in 10. maddesine göre ise bir gerçek kişinin kimliğinin şüpheye yer bırakmayacak şekilde belirlenmesi amacıyla biyometrik verilerin işlenebilmesi için, işleme mutlak surette gerekli olmalı ve veri sahibinin hak ve özgürlüklerinin korunması bakımından yeterli önlemler alınmalıdır.

Biyometrik verilerin işlenmesiyle temel haklar üzerinde çeşitli riskler ortaya çıkmakta ve bu doğrultuda kişisel verilerin korunması adına temel ilkelerin yanı sıra bahsi geçen ek güvenceler öngörülmektedir. Yüz tanıma sistemlerinin kullanılmaya başlanmasıyla birlikte ise temel haklara müdahalenin arttığı söylenebilir. Nitekim yüz tanıma sistemlerinin CCTV veya polis yaka kamerası gibi mevcut gözetim araçlarına entegre edilmesiyle, biyometrik veri niteliğindeki yüz görüntülerinin toplanma ve işlenme sıklığı artarken; dijital görüntülere internet üzerinden ulaşılması örneğinde olduğu gibi verileri işlenen bireylerin iş birliği veya farkındalığı gerekmeden sürecin yürütülebilmesi temel haklar üzerindeki riski yükseltir⁶¹.

Avrupa İnsan Hakları Mahkemesi tarafından *Glukhin* kararında atıf yapılan Avrupa Konseyi bünyesinde ortaya çıkarılmış Yüz Tanıma Hakkında Kılavuz ise özellikle yüz tanıma teknolojilerinin kullanımı sırasında takip edilmesi gereken kurallar öngörmektedir. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi Danışma Komitesi tarafından 2021 yılında yayınlanan Yüz Tanıma Hakkında Kılavuz, yüz tanıma teknolojilerinden yararlanılırken temel özgürlüklerin olumsuz yönde etkilenmemesini sağlamak amacıyla referans niteliğinde bir belge olarak ortaya çıkarılmıştır.

Kılavuza göre yüz tanıma teknolojilerinin, izlenen meşru amaçla orantılı olup olmadığı ile veri sahibinin hakları üzerindeki etkisi birlikte değerlendirilmelidir.

⁶¹ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 27) 5.



Yüz tanıma teknolojisinin farklı kullanım alanları sınıflandırılarak uygun hukuki çerçeve oluşturulurken ise şu hususlar dikkate alınmalıdır⁶²:

- Kullanımın ve izlenen amacın ayrıntılı bir açıklaması
- Kullanılan algoritmanın asgari güvenilirliği ve doğruluğu (“*accuracy*”)
- Kullanılan fotoğrafların saklama süresi
- Benimsenen kıstasların denetlenebilirliği
- Sürecin izlenebilirliği
- Güvenlik önlemleri

Amaca bağlılık ilkesi bağlamında çıkarımlarda bulunan Kılavuza göre başlangıçta farklı amaçlar için kullanılan dijital görüntülerden oluşan mevcut veri tabanlarının biyometrik şablonlarını çıkarmak ve bunları biyometrik sistemlere entegre etmek için, ağır basan meşru amaçlar bulunmalı, uygulama kanunla öngörülmeli ve izlenen amaçlar için kesinlikle gerekli ve orantılı olmalıdır. İzlenebilecek örnek amaçlar arasında suçların önlenmesi, soruşturulması ve kovuşturulması ile cezaların infazı gösterilebilir⁶³.

Suçların önlenmesi, soruşturulması ve kovuşturulması ile cezaların infazı amaçlarıyla kontrollü⁶⁴ veya kontrolsüz bir ortamda kimlik tespiti yönelik yüz tanıma teknolojileriyle biyometrik veri işlenmesi, sadece bu amaçlarla sınırlı yapılmalı ve sadece yetkili kişiler tarafından gerçekleştirilmelidir. Kimlik tespiti amacıyla, hem veri tabanının (izleme listesi) oluşturulmasında hem de (canlı) yüz tanıma teknolojilerinin kontrolsüz bir ortamda kullanılmasında katı gereklilik (“*strict necessity*”) ve orantılilik gözetilmelidir⁶⁵.

C. Yüz Tanıma Sistemlerinin Ceza Adalet Sisteminde Kullanımı

Ceza adalet sisteminde yararlanılan yüz tanıma teknolojileri, doğrulamaya nazaran kimlik tespiti yöntemini kullanır. Keza belirli bir yere girmek veya hizmet almak gibi faaliyetler için tercih edilen bire bir eşleştirme değil, suçun önlenmesi veya soruşturulması amacıyla veri tabanında bulunan birçok şablonla karşılaştırma yapan bire çok eşleştirmeye sonuca ulaşmaya çalışılır. Bu sistemler görüntüleri karşılaştırarak kimlik tespiti yaparken genellikle yapay zekâ teknolojisi kullanır. Yüksek hacimlere ulaşan ve karmaşıklaşan veri havuzunda yüz görüntülerinin

⁶² ibid 7; Biyometrik verilerin işlenmesinde ölçülülük ilkesine riayet edilmesi ve veri sahipleri bakımından kişi kategorilerinin oluşturulması noktasında benzer çıkarımlar için ayrıca bakınız Neslihan Can, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması* (On İki Levha Yayıncılık 2021) 176-181.

⁶³ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 27) 9.

⁶⁴ Kontrollü ortam (“*controlled environment*”) kavramı, biyometrik sistemlerin yalnızca kişinin katılımıyla kullanılabildiği durumları kapsamaktadır. ibid 10.

⁶⁵ ibid 10.

doğru bir biçimde hızlıca eşleştirilmesi insanların kolayca üstesinden gelebileceği bir iş olmaktan çıkmakta; dolayısıyla verileri hızlıca işleyen ve isabetli sonuçlar üreten sistemlere olan ihtiyaç artmaktadır. Personel yetersizliği veya insandan kaynaklanan noksanlar da dikkate alındığında yüz tanıma sistemleri, verimliliği artırarak suçla mücadelede önemli bir araç niteliği kazanmaktadır⁶⁶.

Önleyici kolluk faaliyetleri ile soruşturmalarda parmak izi ve DNA analizi yöntemlerinin yanı sıra yüz tanıma sistemlerinden yararlanılmaya başlanmasıyla çoğunlukla şüphelilerden, sanıklardan ve hükümlülerden suçların önlenmesi ve soruşturulması amacıyla yüz görüntüleri toplanmaya başlanmıştır⁶⁷. Yüz tanıma teknolojisinin ceza adalet sistemindeki kullanımı şüpheli, sanık, mağdur veya savunmasız kişilerin tespit edilmesi biçiminde çeşitlenebilir⁶⁸.

Yüz tanıma sistemlerinin dikkate değer kullanım alanı önleyici kolluk faaliyetlerinde ortaya çıkmaktadır. Sistemin uyarıları sonucu bir risk tespit eden kolluk, olası bir tehlike veya suç önleme amacıyla durdurma, kimlik sorma ve arama gibi işlemleri tatbik edebilmektedir⁶⁹. Almanya'nın Mannheim şehrinde 2018 yılında hayata geçirilen ve yapay zekâ teknolojilerinden yararlanan sistem, tehlikeli davranışları tanımlayarak kolluk güçlerine bilgi sağlamaktadır. Bilgiyi alan kolluk ilgili görüntüleri izleyerek müdahale gerekip gerekmediğine karar vermektedir. Aynı yıl Alman Federal Polisi ("*Bundespolizei*") tarafından federal düzeyde uygulamaya konulan "*Sicherheitsbahnhof*" isimli pilot proje ise yapay zekâ temelli kameralı gözetimin yanı sıra biyometrik yüz tanımaya odaklanmaktadır⁷⁰. Macaristan'da ortaya çıkarılan bir proje kapsamında ise başkent Budapeşte ve ülke genelinde yüz tanıma özelliğine sahip otuz beş bin kamera yerleştirilerek yol güvenliği de dahil olmak üzere kamu düzeninin sağlanması amacıyla sürücülerin plakalarının ve yüz görüntülerinin yakalanarak işlenmesi planlanmaktadır⁷¹.

⁶⁶ European Data Protection Board (n 27) 6.

⁶⁷ The European Commission, *Towards the European Level Exchange of Facial Images Legal Analysis for TELEFI project* 3-4, 13 <<https://www.telefi-project.eu/telefi-project/results>> erişildi 5 Şubat 2025.

⁶⁸ Michael Veale, *Algorithms in the Criminal Justice System* (June 2019) 36 <<https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report>> erişildi 20.01.2025.

⁶⁹ İçer and Dönmez (n 57) 436.

⁷⁰ Johanna Sprenger and Dominik Brodowski, 'Predictive Policing', 'Predictive Justice', and the use of 'Artificial Intelligence' in the Administration of Criminal Justice in Germany' (2023) *Revue Internationale de Droit Pénal* 5, 16-18 <<https://www.penal.org/de/2023-2>> erişildi 11 Haziran 2025; Almanya'daki diğer benzer uygulamalar için ayrıca bakınız İçer and Dönmez (n 57) 423-424.

⁷¹ European Union Agency for Fundamental Rights (n 32) 3; Önleyici faaliyetler kapsamında kabul edilebilecek diğer bir kullanım, kayıp kişilerin bulunmasına özgülüdür. İçer and Dönmez (n 57) 438. Sınır güvenliğinin sağlanması amacıyla da yüz tanıma sistemleri geliştirilmekte ve kullanılmaktadır. Laura K. Donohue, 'Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age' (2012) 97 *Minnesota Law Review* 407, 436-437.



Ceza adalet sisteminde kimlik tespiti için biyometrik verilerin kullanılması, suç işlenmesinin önlenmesinde veya suç soruşturmalarında önemli bir rol oynayabileceği gibi birden fazla kimlik yaratma imkanını da ortadan kaldırarak terörle veya organize suçlulukla mücadele değerli bir yöntem olarak kendini göstermektedir⁷².

Terör ve organize suçluluk gibi sınır aşan suçlarla mücadele, Avrupa’da ulusal ve uluslararası mevzuatın oluşmasında önemli bir etkidir. Bu doğrultuda Avrupa Birliği bünyesinde ortaya çıkarılan çalışmalardan biri Prüm Anlaşmasıdır. Sınır ötesi suç, terörizm ve yasadışı göçle mücadele amacıyla DNA profilleri, parmak izleri ve araç kayıt verileri, anlaşmayla oluşturulan Prüm Sistemi kapsamında taraf devletler arasında paylaşılmaktadır. Avrupa Birliği’nin tüm üyelerine açık olan ve 2005 yılında sekiz devlet tarafından imzalanan Prüm Anlaşması’yla kurulan Prüm Sistemi’nin başarılı uygulaması sonucu, yüz görüntülerinin de paylaşımını içeren yeni yöntemlerin benimsenmesi değerlendirilmeye başlanmıştır⁷³.

Değerlendirme sonucu Yüz Görüntülerinin Avrupa Düzeyinde Değişimine Doğru (“Towards the European Level Exchange of Facial Images” - TELEFI) Projesi ortaya çıkarılmıştır. Avrupa Komisyonu tarafından desteklenen ve Avrupa Birliği tarafından finanse edilen Proje, suçların soruşturulması ve kovuşturulmasıyla bağlantılı olarak yüz tanımanın kurumsal, teknik ve hukuki yönlerini gözden geçirmeyi amaçlamaktadır. Bu doğrultuda Avrupa Birliği üyesi devletlerdeki suç soruşturmalarında yüz tanımanın uygulamasını araştırmaktadır⁷⁴.

Avrupa Birliği ülkelerinde tatbik edilen veya tatbik edilmesi planlanan yöntemlere bakıldığında şu uygulamalara rastlanır⁷⁵:

- Kimliği belirlenemeyen bir kişinin (şüpheli, mağdur, vb.) yüzü, fotoğraflardan oluşan bir veri tabanında aranır.
- Suç önleme amacıyla bir kişinin kamusal alandaki hareketleri izlenir. Örneğin bir kişi kamusal alanda tehlikeli gözüken bir çanta bıraktığında yüz görüntüsü veri tabanındaki şablonlarla karşılaştırılabilir.

⁷² Teröristlerin birden fazla kimlikle hareket etmesinin önüne geçmek ve suçluların, hileyle veya diğer yollardan mağdurların kimliklerini ele geçirip, dolandırıcılık ve benzeri suçları işlemelerini önlemek için kişilerin benzersiz bir şekilde tanımlanmasına yönelik yeni teknikler benimsenmeye başlamıştır. Council of Europe, *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data* (2005) para 8 <<https://rm.coe.int/16806840ba>> erişildi 16 Mart 2025.

⁷³ The European Commission, *Support to the project ‘Towards the European Level Exchange of Facial Images’* <<https://www.politico.eu/wp-content/uploads/2020/03/TELEFI-Project.pdf>> erişildi 16 Mart 2025; The European Commission, *Summary Report of the project* (n 6) 10, 16; <<https://www.telefi-project.eu/telefi-project/about-telefi-project>> erişildi 16 Mart 2025.

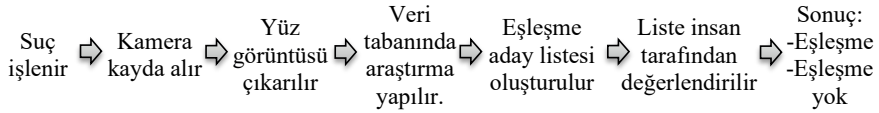
⁷⁴ The European Commission, *Support to the project* (n 73); <<https://www.telefi-project.eu/telefi-project/about-telefi-project>> erişildi 16 Mart 2025.

⁷⁵ European Data Protection Board (n 27) 9-10.

- Aranan kişilerin tespiti için kamusal alanlarda tanımlama yapılır. Örneğin canlı olarak yakalanan yüzler, hakkında yakalama kararı bulunan şüphelinin polis veri tabanındaki yüz görüntüsüyle eşleştirilmeye çalışılabilir.

Europol, Interpol ve diğer devletlerde genellikle benimsenen yüz tanıma sistemleri geriye dönük araçlardır (“*retrospective tools*”). Olay sonrası kullanım (“*post-event use*”) veya çevrimdışı kullanım (“*off-line use*”) olarak da adlandırılan bu yöntemde suç şüphesi doğuran olayla ilgili kontrolsüz yüz görüntüsü⁷⁶, olaydan sonra soruşturma sırasında incelenir. İlgili yüz görüntüsünün elde edildiği kişiyi tanımlamak amacıyla, kimliği belirli kişilerden alınan kontrollü yüz görüntülerinin⁷⁷ depolandığı veri tabanında bire çok (1:N) karşılaştırma yapılır. Karşılaştırmadan elde edilen sonuç bir insan tarafından değerlendirilir ve olası eşleşmeler için karara varılır⁷⁸.

Geriye dönük olarak kullanılan yöntemin işleyişi aşağıdaki gibidir⁷⁹:



Bir örnek üzerinden somutlaştırmak gerekirse hakkında kesinleşmiş mahkûmiyet hükmü olan kişilerden yüz görüntüleri alınır ve özel bir polis veri tabanında saklanır. Ayrıca sürücü belgesi başvuruları için toplanan yüz görüntülerinin tutulduğu veri tabanına erişim imkânı da polise verilir. Gelen bir ihbar sonucu açılan soruşturma kapsamında olay yerini gören ve yüz tanıma sistemi entegre edilmiş bir kameradan alınan video kaydından şüpheli olabilecek kişilerin yüz görüntüleri alınır. Kişilerin kimliğini tespit etmek için, polisin yüz görüntülerini sakladığı veri tabanı ile sürücü belgesi için toplanan yüz görüntülerinin depolandığı veri tabanındaki tüm yüz görüntüleriyle sistem karşılaştırma yapar. Belirli bir benzerlik oranının üstündeki eşleşmeler kullanıcıya sunulur. Kullanıcı olası eşleşmeleri değerlendirip şüphelilerin kimliğini tespit eder. Ulusal mevzuatın izin verdiği ölçüde karşılaştırma için daha fazla veri tabanından⁸⁰ da yararlanılabilir.

⁷⁶ Kontrolsüz görüntü (“*uncontrolled image*”), yüz tanıma standartlarına veya yönergelerine uygun olarak çekilmeyen görüntü olarak tanımlanır. Belirti görüntü (“*trace image*”) olarak da bilinir. Örneğin kameralı gözetimden elde edilenler, kontrolsüz görüntü niteliğindedir. The European Commission, *Summary Report of the project* (n 6) 8.

⁷⁷ Kontrollü görüntü (“*controlled image*”), yüz standartlarına veya yönergelerine uygun olarak çekilen görüntü olarak tanımlanır. Referans görüntüler (“*reference images*”) olarak da bilinir. Örneğin sürücü ehliyetinde yer alan fotoğraf, referans görüntü niteliğindedir. ibid 6.

⁷⁸ ibid 10-11, 24.

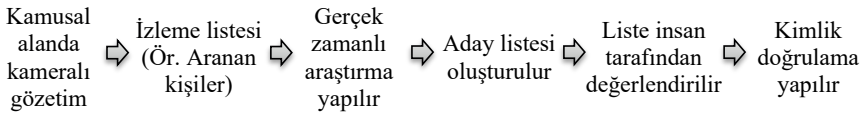
⁷⁹ ibid 24.

⁸⁰ Avrupa Birliğine üye devletlerde soruşturmalar sırasında yararlanılan yüz tanıma sistemlerinin kullandığı veri tabanlarında şüpheliler, sanıklar, hükümlüler, gözaltına alınanlar, tutuklular, aranan



Geriye dönük uygulama görece daha kontrollü müdahaleler içerse de kullanılan veri miktarının artmasıyla öngörülemez boyutlara ulaşarak, kişisel verilerin ölçsüz bir biçimde işlenmesine zemin hazırlayabilir. Amerika Birleşik Devletleri merkezli özel bir şirket olan *Clearview AI*, 60 milyardan fazla yüz görüntüsünden oluşan bilinen en büyük veri tabanını suçla mücadele ve suçların soruşturulması için kolluk kuvvetlerine ve devlet kurumlarına sunma amacıyla kurulduğunu belirtmektedir. Şirket tarafından verilen bilgiye göre yüz tanıma teknolojisi ile desteklenen platformun veri tabanı sadece kamuya açık ağ (“web”) kaynaklarından elde edilen verileri barındırmaktadır⁸¹. Şirket tarafından sağlanan bu hizmet Amerika Birleşik Devletleri, Birleşik Krallık ve Avustralya polisi tarafından kullanılmasına rağmen çeşitli sosyal medya şirketleri ve hukuk firmaları tarafından açılan toplu davalarda şirket beyanının aksi iddia edilmiştir. İddialara göre sosyal medya şirketlerinin kuralları ihlal edilmiş ve bireylerin rızası olmaksızın biyometrik bilgileri kullanılmıştır⁸². İddiaların sabit olup olmamasından bağımsız olarak, yüz tanıma sistemlerinin verimliliğini artırmak için daha fazla veriye erişme amacı, kontrollü yüz görüntülerinden çok daha fazlasını elde etme ihtiyacını doğurmaktadır. Özellikle çevrimiçi platformlara aktarılan yüz görüntülerinin toplanarak işlenmesi ise kişisel veriler üzerinde yeni tehlikeler ortaya çıkarmaktadır.

Avrupa Birliği üye devletlerinde rutin uygulamasına rastlanmayan ancak Birleşik Krallık’ta kullanılan diğer bir yöntem ise canlı yüz tanımadır. Geriye dönük araçlardan farklı olarak canlı yüz tanıma kimliği tespit edilmek istenen kişilerin bir listesi bulunur. Listede yer alan kişilerin yüz görüntüleri, elde edilmekte olan görüntülerle sürekli karşılaştırılır. Örneğin liste, hakkında yakalama kararı bulunan kişilerden oluşabilir. Caddeler, alışveriş merkezleri, toplu taşıma araçlarının durakları ve benzeri kamusal alanlara yerleştirilmiş kameralarca tespit edilen yüz görüntüleri anlık olarak haklarında yakalama kararı bulunan kişilerin yüz görüntüleriyle karşılaştırılarak olası eşleşmeler kullanıcıya sunulur. Değerlendirme sonucu eşleşme olduğuna kanaat getirilirse ilgili kişiye müdahale edilerek kimlik tespiti ve tespit amacına uygun diğer işlemler yapılır. Canlı yüz tanıma yönteminin işleyişi aşağıdaki gibidir⁸³:



kişiler, kimliği belirsiz kişiler, kayıp kişiler, kimliği belirsiz maktuller, ağır yaralıları, sığınmacılar, göçmenler ve yabancılara ait veriler bulunur. ibid 11-12.

⁸¹ <<https://www.clearview.ai/overview>> erişildi 13 Haziran 2025.

⁸² Marcus Smith and Seumas Miller, ‘The ethical application of biometric facial recognition technology’ (2022) 37 AI & SOCIETY 167, 169-170.

⁸³ The European Commission, *Summary Report of the project* (n 6) 25.

Çalışma konusu *Glukhin* kararında da irdelenen ve ceza adalet sisteminde sıklıkla kullanılan yöntem kimlik belirleme olsa da; teknolojinin yaygınlaşmasıyla birlikte yüz tanıma teknolojisi kullanılarak elde edilen bilgiler, şüpheli, sanık veya diğer kişilerin tespitinin yanı sıra ceza muhakemesine konu maddi vakıayı ispat etmek ya da sanığın cezai sorumluluğunu belirlemek amacıyla da kullanılabilir. Örneğin yüz tanıma teknolojisi kullanan polis veya kamerasından elde edilen görüntülerden ispat aracı olarak yararlanılabilir⁸⁴. Yapay zekâ teknolojisiyle birlikte kişilerin duygu durumuna dair tespitlerde de bulunabilen yazılımların çıktıları cezai sorumluluğunun belirlenmesinde dikkate alınabilir. Diğer bir örnekte ise bir otomobilin sürülmesinde insanlara yardımcı olan veya sürüşü tamamen devralabilen otonom sürüş teknolojileri, sürücünün yüz ve özellikle göz hareketlerini izleyip kayda alabilir. Yüz tanıma teknolojisiinden yararlanan bu sistemler esasen sürücünün uykulu veya yorgun olması gibi sürüşe devam etmesine uygun olmadığı durumları tespit ederek uyarı göndermek için tasarlanmıştır. Öte yandan sistemin tespiti, uyarısı ve sürücünün görüntüleri kayda alındığından, bu bilgiler olayın ispatı ve sanığın cezai sorumluluğunun belirlenmesi amacıyla ceza yargılamasında kullanılabilir⁸⁵. İkinci örnekteki kullanım doğrudan ceza adalet sistemine entegre edilmiş bir sistemden elde edilmiş olmasa da yüz tanıma sistemleri kullanılarak ulaşılan bilginin ceza adalet sisteminde kullanılmasının farklı bir örneği olarak ortaya çıkar. Ancak belirtmek gerekir ki yapay zekâ teknolojilerinden yararlanılarak ulaşılan bu delillerin ceza muhakemesindeki kullanımı, teknolojinin karmaşık yapısı da dikkate alınarak, kişisel verilerin korunması kurallarının yanı sıra adil yargılanma hakkı bağlamında özellikle çelişmeli yargılama, silahların eşitliği ve masumiyet karinesi⁸⁶ bakımından farklı bir çalışmada incelenmeye layıktır.

Veri depolama imkanlarının yanı sıra yapay zekâ teknolojisinin sağladığı imkanlarla yüz tanıma algoritmalarının verimliliği son on yıl içerisinde oldukça artmıştır. Böylece sadece kontrollü şartlar altında elde edilenler değil aynı zamanda CCTV kameralarında olduğu gibi düşük kaliteli veya farklı açılardan yakalanan görüntüler üzerinde dahi algoritmalar, insanlara kıyasla daha iyi performans göstermeye başlamıştır⁸⁷. Buna bağlı olarak terör, organize ve sınır aşan

⁸⁴ Elif Ildırar, ‘Kolluğun Vücut Kamerası Kullanımı ve Türkiye’de Uygulanabilirliği’ in Oktay Karaalp, Barkın Özyurt and Gökçen Elif Toksoy (eds), *Bilkent Üniversitesi Hukuk Fakültesi IV. Genç Hukukçu Araştırmacılar Sempozyumu 20-21 Nisan 2024 Çevrim İçi* (On İki Levha Yayıncılık 2024) 45, 55-62.

⁸⁵ Sabine Gless, ‘AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials’ (2020) 51 [2] *Georgetown Journal of International Law* 195, 202-205.

⁸⁶ Yüz tanıma sistemlerinin ceza muhakemesindeki olası diğer bir kullanımına örnek olarak şüpheli, sanık veya tanık gibi kişilerin beyanlarının doğruluğunun denetlenebilmesi gösterilmiştir. İçer and Dönmez (n 57) 438; Böyle bir kullanım masumiyet karinesinin sonuçlarından biri olan ve Anayasamızda da “hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz” biçiminde ortaya konan *nemo tenetur* ilkesi bağlamında incelenebilir.

⁸⁷ The European Commission, *Summary Report of the project* (n 6) 14.



suçluluk başta olmak üzere suçla mücadele ve etkili soruşturma amacıyla sadece Avrupa’da değil dünya genelinde yüz tanıma sistemlerinin yaygınlaşması⁸⁸ ve gelişen teknolojilerle birlikte çok yönlü ve karmaşık bir hal alması kuvvetle muhtemeldir. Kurulacak böyle bir yapı ise temel hak ve özgürlükler bakımından daha müdahaleci eylem ve işlemlere zemin hazırlamaktadır.

III. AVRUPA İNSAN HAKLARI MAHKEMESİNİN İÇTİHAT GELİŞİMİ

Mahkeme, *Glukhin* kararında Sözleşme’nin 8. maddesiyle güvence altına alınmış özel hayata saygı hakkı bağlamında, kişisel verilerin toplanması, depolanması ve işlenmesine dair çıkarımlarda bulunmaktadır.

Kararda Mahkeme kişisel veriler bakımından değerlendirme yaparken, yüz tanıma sistemlerinin müdahaleci yapısının yanı sıra kullanılan yüz görüntülerinin biyometrik veri niteliğini dikkate almıştır. Biyometrik verilerle ilgili Mahkeme’nin içtihat gelişimine bakıldığında ise parmak izi ve DNA bilgilerinin alınması ve depolanması işlemleri üzerine çeşitli kararlar verdiği görülür ki bu bağlamda sıklıkla atıf yapılan karar *S. ve Marper* davasıdır. Nitekim Mahkeme bu kararında, toplanan biyometrik verilerin depolanma şartlarıyla ilgili ilke niteliğinde kural ve çıkarımlar ortaya koymuştur. Yüz tanıma sistemlerinin mevcut teknolojilerle yaygınlaşmaya başlaması son on yılda gerçekleştiği için *Glukhin* kararı dışında bu sistemlerin ayrıca değerlendirildiği bir karar yoktur. Dolayısıyla takip eden başlıklarda kimlik tespiti amacıyla ceza muhakemesi sürecinde sıklıkla toplanan biyometrik veri niteliğindeki DNA, parmak izi ve yüz görüntülerinin saklama, depolama ve işleme koşullarına dair Mahkeme içtihadı incelenmiştir.

A. Özel Hayata Saygı Hakkı Bağlamında Kişisel Verilerin Korunması

Avrupa İnsan Hakları Sözleşmesi’nin özel ve aile hayatına hakkı başlıklı 8 § 1 maddesine göre “*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*”

⁸⁸ Özellikle Çin Halk Cumhuriyeti’ndeki yüz tanıma uygulamaları dikkat çekicidir. Birleşmiş Milletler İnsan Hakları Konseyi’nin A/HRC/41/35 numaralı 28.05.2019 tarihli “Gözetim ve İnsan Hakları” başlıklı raporuna göre, Çin Hükümeti ülke genelinde yüz tanıma teknolojisi ve gözetleme kameralarını birlikte kullanmaktayken; 16 farklı bölgedeki yirmiden fazla polis departmanı 2018’den itibaren bu tür bir teknolojiyi edinme ve kullanma arayışına girmiştir. United Nations Human Rights Council, *Surveillance and human rights Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* 5 (A/HRC/41/35, 28 May 2019) <ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35> erişildi 12 Şubat 2025; Paul Mozur, ‘One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority’ *The New York Times* (New York, 14 April 2019) <www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> erişildi 12 Şubat 2025; Amerika Birleşik Devletleri’nde Federal Soruşturma Bürosu (FBI) tarafından yürütülen işlemler için ayrıca bakınız Berle (n 30) 19-20.

Özel hayata saygı veya Anayasamızda öngörüldüğü şekliyle özel hayatın gizliliği temelde yalnız olabilmek hakkını ifade ederken⁸⁹; geniş manada mahremiyet hakkını (“*right to privacy*”)⁹⁰ ortaya çıkarır. Bu bağlamda kişilerin mahremiyeti ile ilgili her şeyin gizli kalmasını gerektirir⁹¹. Özel hayata saygı hakkının yorumlanmasıyla ortaya çıkarılan ve korunması gerekli alanlardan bir tanesi de veri mahremiyetidir⁹². Günümüz teknolojilerinin sağladığı imkanlarla özel hayatla ilgili olanlar da dahil olmak üzere neredeyse her bilginin veri biçiminde saklanabilmesi, veri mahremiyetini öncelikle korunması gerekli bir alan halinde getirmektedir. Veri mahremiyetinin sağlanması için kişilerin kendilerine ait bilginin kontrolünü ele geçirmeleri gerekir⁹³. Bu kontrol ise kişisel verilerin korunması hakkının temelini oluşturan⁹⁴ ve Avrupa İnsan Hakları Mahkemesi tarafından da atıf yapılan⁹⁵ enformasyonel self-determinasyon hakkı⁹⁶ (“*informational self-determination*” / “*informationelle selbstbestimmung*”) olarak ifade edilir.

⁸⁹ Samuel D. Warren and Louis D. Brandeis, ‘The Right to Privacy’ (1890) 4 [5] Harvard Law Review 193, 195.

⁹⁰ Mahremiyet hakkı, kişinin kendi hayatını en az müdahaleyle yaşama hakkını ifade eder. Parliamentary Assembly of the Council of Europe, *Declaration on mass communication media and Human Rights* (Resolution 428, 1970) <<https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en>> erişildi 14 Şubat 2025.

⁹¹ Muammer Ketizmen and Aslıhan Kart, ‘Kişisel Verilerin Korunması Kanunu’nun 17. Maddesi ve Yargıtay Kararları Doğrultusunda, Kişisel Verilerin Korunmasına İlişkin Suç Teşkil Eden Fiiller Açısından Uygulanacak Norm Hakkında Değerlendirme’ (2021) 1 [2] Kırıkkale Hukuk Mecmuası 256, 258; Hakkın kapsamına dair farklı görüşler için ayrıca bakınız Sultan Tahmazoğlu Üzeltürk, ‘Özel Hayatın Korunmasına İlişkin Başlıca Sorunlar’ (2008) 1 Galatasaray Üniversitesi Hukuk Fakültesi Dergisi 95, 97-102.

⁹² Ketizmen ve Kart (n 91) 259-60. Bilgi mahremiyeti (“*informational privacy*”), “*bireylerin, grupların veya kurumların kendileri hakkındaki bilgilerin ne zaman, nasıl ve ne ölçüde başkaları aracılığıyla iletileceğini kendilerinin belirleme hakkı*” olarak tanımlanmıştır. Antoinette Rouvroy and Yves Pouillet, ‘The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy’ in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 45, 69.

⁹³ Ketizmen ve Kart (n 91) 258-60.

⁹⁴ Kişisel verilerin korunması hakkı, ilgili kişinin veri üzerindeki hakimiyetini gerektirir. Murat Volkan Dülger, ‘İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması’ (2018) 5 [1] İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 71,74.

⁹⁵ *Satakunnan Markkinapörssi Oy ve Satamedia Oy v Finlandiya App no 931/13* (ECtHR, 27 Haziran 2017) para 137; *Benedik v Slovenya App no 62357/14* (ECtHR, 24 Nisan 2018) para 103.

⁹⁶ Kişisel verilerin korunmasının temelini oluşturan ve enformasyonel self-determinasyon (“*informational self-determination*” / “*informationelle selbstbestimmung*”) olarak öğretide tanımlanan hak, Alman Federal Anayasa Mahkemesi (“*Bundesverfassungsgericht*”) tarafından ortaya çıkarılmıştır. Mahkeme, 1983 yılında verdiği “Census-Nüfus Sayımı” kararında, Alman Anayasası’nın 1. ve 2. maddelerinde yer alan insan onuru ve insanın kişiliğini geliştirme hakkına dayanarak enformasyonel self-determinasyon hakkından bahsetmiştir. Kendi kaderini tayin etme biçiminde de ifade edilebilecek self-determinasyon temelinde herkes, kendisine ait verilerin kullanımı ve devri hususunda belirleyici olmalıdır. Self-determinasyon, kişilerin hareket etme ve iş birliği yapma kapasitesine dayanan özgür ve demokratik bir toplumun temel işlevsel koşuludur. Aydın Akgül, ‘Kişisel Verilerin Korunmasında



Avrupa İnsan Hakları Mahkemesi, enformasyonel self-determinasyon hakkına yaptığı atıfla dolaylı olarak gösterdiği gibi kişisel verilerin korunmasını, özel hayata saygı hakkının bir görünümü olarak benimser⁹⁷. Mahkemeye göre kişisel verilerin korunması, bireylerin Sözleşmenin 8. maddesiyle güvence altına alınan özel ve aile hayatına saygı hakkından yararlanması bakımından temel öneme sahiptir⁹⁸. Mahkeme ayrıca Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nde yer alan kişisel veri kavramına atıf yaparak, 8. maddeyle getirilen korumanın kapsamına dair yorumunu vurgularken, kişisel veriler bağlamında özel hayatın sınırlayıcı bir şekilde yorumlanmaması gerektiğini belirtmektedir⁹⁹.

Mahkemeye göre bilgiler sistematik olarak toplanıp yetkililer tarafından tutulan dosyalarda saklanırsa, bu bilgiler kamuya açık olsa dahi özel hayat bağlamında değerlendirilebilir. Bu nedenle belirli bir kişi hakkında toplanan bilgiler herhangi bir müdahaleci veya gizli yöntemle toplanmamış olsa bile, sistematik veya kalıcı bir depolama söz konusuysa 8. madde kapsamına girmektedir¹⁰⁰. Bireyin kamuya açık yerlerdeki davranışlarının, görsel verileri kaydetmeyen ekipmanlar kullanılarak izlenmesi bireyin özel hayatına bir müdahale niteliğinde görülmezken, görüntülerin kaydedilmesi ve kalıcı olacak saklanması müdahalenin varlığını gündeme getirir¹⁰¹.

B. Kişisel Verilerin Korunması Bağlamında Biyometrik Verilerin Toplanması, Saklanması ve İşlenmesi

Avrupa İnsan Hakları Mahkemesinin, kamu güvenliğinin sağlanması veya suçların önlenmesi amacıyla ya da suç soruşturması kapsamında kişilerin kamuya açık alanlardaki görüntülerinin veya seslerinin kaydedilmesiyle ve/veya bunların kullanılmasıyla ilgili kararları mevcuttur¹⁰². Ancak *Glukhin* davasına konu olay-

Yeni Bir Hak: 'Unutulma Hakkı' ve Ab Adalet Divanı'nın 'Google Kararı' (2015) 116 TBB Dergisi 11,15; Ringelheim (n 59) 25; Rouvroy and Pouillet (n 92) 45-47; Dülger (n 94) 81.

⁹⁷ Yerleşik içtihadına göre kişilerin özel hayatına ilişkin bilgiler, Sözleşmenin 8 maddesi bağlamında koruma altındadır ve örneğin bu bilgilerin saklanması özel hayata saygı hakkına müdahale oluşturur. *Leander v İsveç* App no 9248/81 (ECtHR, 26 Mart 1987) para 48; *Rotaru v Romanya* App no 28341/95 (ECtHR, 4 Mayıs 2000) para 43.

⁹⁸ *S. ve Marper v Birleşik Krallık* App nos 30562/04 ve 30566/04 (ECtHR, 4 Aralık 2008) para 103. *Satakunnan Markkinapörssi Oy ve Satamedia Oy v Finlandiya* (n 95) para 137.

⁹⁹ *Amann v İsviçre* App no 27798/95 (ECtHR, 16 Şubat 2000) para 65; *Rotaru v Romanya* (n 97) para 43; *Benedik v Slovenya* (n 95) para 102.

¹⁰⁰ *P.G. ve J.H. v Birleşik Krallık* App no 44787/98 (ECtHR, 25 Eylül 2001) para 57; Örneğin kişinin hayatı, özellikle de çalışmaları, siyasi faaliyetleri ve sabıka kaydı hakkındaki bilgiler bu kapsamda görülebilir. *Rotaru v Romanya* (n 97) paras 43-44.

¹⁰¹ *Peck v Birleşik Krallık* App no 44647/98 (ECtHR, 28 Ocak 2003) para 59; *Perry v Birleşik Krallık* App no 63737/00 (ECtHR, 17 Temmuz 2003) para 38.

¹⁰² Başvurucunun kamuya açık bir alanda yanında bulundurduğu bıçakla intihar girişiminden sonraki davranışlarının CCTV tarafından kaydedilmesi ve sonrasında CCTV uygulamasının etkililiğini

daki gibi günümüz yüz tanıma sistemleri kimlik tespiti amacıyla biyometrik veriler ve teknolojiler kullandığından, ceza muhakemesi süreciyle bağlantılı olarak DNA, parmak izi veya yüz görüntülerinin biyometrik veri niteliğinde toplanması, saklanması ve işlenmesine dair Mahkeme kararları incelenmiştir. Nitekim Mahkemenin yüz tanımayla ilgili verdiği yegâne *Glukhin* kararındaki çıkarımlar da DNA bilgileri ve parmak izi gibi diğer biyometrik verilerle ilgili ortaya çıkarılmış içtihadın üzerine inşa edilmiştir.

Sözleşmenin 8. maddesiyle güvence altına alınan özel hayata saygı hakkı bağlamında kişisel verilerin korunmasıyla ilgili içtihat gelişiminde Mahkeme, müdahalenin haklılığını değerlendirirken, izlenen meşru amaç başlığı altında “suç işlenmesinin önlenmesi” amacının takip edildiğini kabul etmektedir¹⁰³. Müdahalenin ulusal mevzuatta kanuni bir dayanağı olup olmadığı değerlendirilmesinde ise genellikle Taraf Devletlerin iç hukukundaki düzenlemelerin niteliğini, demokratik bir toplumda gerekli olma şartıyla birlikte incelemektedir. Dolayısıyla Mahkemenin ilk iki şart bakımından dikkate değer çıkarımlar yaptığı söylenemez. Bu sebeple içtihat gelişiminde, öncelikle “müdahalenin varlığı” sonrasında ise “müdahalenin demokratik bir toplumda gerekliliği” başlığı altında ortaya konan çıkarımlar, kişisel verilerin korunmasına dair ortaya çıkarılan uluslararası mevzuat dikkate alınarak değerlendirilmelidir.

1. Müdahalenin Varlığı

Kişisel verilerin kamu otoriteleri tarafından muhafaza edilmesinin özel hayata saygı gösterilmesi hakkına müdahale oluşturup oluşturmadığını değerlendirirken Mahkemenin göz önünde bulundurduğu kıstaslar arasında, verilerin gelecekteki kullanım imkanları, verinin niteliği ve saklamanın kapsamı yer almaktadır.

Mahkeme, yetkililer tarafından muhafaza edilen kişisel verilerin gelecekteki olası kullanımına ilişkin bireyde oluşan endişelerin meşru olduğunu kabul etmekte

göstermek için bu görüntülerin yayınlanmasıyla ilgili verilen ihlal kararı için bakınız *Peck v. Birleşik Krallık* (n 101) paras 53-87; Soruşturma kapsamında yakalanarak hakkında evden çıkmama adli kontrol kararı verilen başvurunun yakalandığı sırada polis tarafından çekilen fotoğrafların basına verilmesiyle ilgili olayda kanuni dayanağı bulunmayan fotoğraf çekme ve basına verme işlemleri hakkında verilen ihlal kararı için bakınız *Sciacca v. İtalya* App no 50774/99 (ECtHR, 11 Ocak 2005) paras 22-31; Teşhis işlemine katılmayı reddeden şüphelinin emniyet müdürlüğünde kapalı devre kamera sistemiyle görüntüleri gizlice kaydedilerek bu kayıtların daha sonra teşhis için kullanılmasıyla ilgili verilen ihlal kararı için bakınız *Perry v. Birleşik Krallık* (n 101) paras 30-49; Başvurucuların emniyet müdürlüğünde bulundukları süreç içerisinde seslerinin kaydedilmesiyle ilgili verilen ihlal kararı için bakınız *P.G. ve J.H. v. Birleşik Krallık* (n 100) paras 52-63; Soruşturma sırasında başvuruçuların fotoğraflarını içeren kitaplar kullanılarak delil toplanmaya çalışılmasıyla ilgili verilen açıkça dayanaktan yoksun kararı için bakınız *Lupker ve Diğerleri v. Hollanda* App no 18395/91 (ECtHR, 7 Aralık 1992); Bu ve benzer nitelikteki kararların ayrıntılı bir değerlendirmesi için ayrıca bakınız Dülger (n 94) 112-130.

¹⁰³ *S. ve Marper v. Birleşik Krallık* (n 98) para 100; *M.K. v. Fransa* App no 19522/09 (ECtHR, 18 Nisan 2013) para. 32; *Gaughran v. Birleşik Krallık* App no 45245/15 (ECtHR, 13 Şubat 2020) para 75; *P.N. v. Almanya* App no 74440/17 (ECtHR, 11 Haziran 2020) para 68.



ve buna göre verileri sınıflandırmaktadır. Bu bağlamda örneğin *Van der Velden* kararında¹⁰⁴ vurgulandığı üzere hücrel materyallerin gelecekteki olası kullanımları dikkate alınarak, sadece nesnel ve tarafsız tanımlayıcı özellik içerdiği kabul edilen parmak izinden farklı bir biçimde kategorize edilmiştir. Nitekim parmak izi bakımından değerlendirme yapan komisyon bunların saklanması müdahale olarak görmezken, hücrel materyaller açısından Mahkeme aksi sonuca varmıştır. *S. ve Marper* kararında ise DNA profillerini değerlendirirken, bireyler arasındaki genetik ilişkilerin tespit edilmesini sağlama kapasitesini, müdahalenin tespiti açısından tek başına yeterli görmüştür¹⁰⁵. Parmak izleri hususunda ise komisyonun eski görüşünden ayrılmış, kişi hakkında benzersiz bilgiler içermesi ve çok çeşitli koşullarda kişinin kesin olarak tanımlanmasına izin vermesi sebebiyle kişisel veri niteliğinde yetkili makamlarca saklanması müdahale olarak yorumlamıştır¹⁰⁶.

Gelecekteki kullanım imkanları her ne kadar sadece müdahalenin varlığı için değerlendirilse ve kişisel veriler için öngörülen temel ilke ve kurallar bakımından Mahkeme ayrıca bir çıkarım yapmasa da; bu husus amaca bağlılık ve amaçla sınırlı olma ilkelerinin bir görünümü olarak yorumlanabilir. Nitekim kişisel verilerle ilgili Avrupa Konseyi ve Avrupa Birliği bünyesinde ortaya çıkarılmış uluslararası mevzuata bakıldığında, verilerin açık, belirli ve meşru amaçlar için toplanabileceği ve bu amaçlarla bağdaşmayan biçimde işlenemeyeceği vurgulanmaktadır. Mahkeme de aslında öngörülen bu ilkelere uygun değerlendirme yapmaktadır. DNA profillerinin, parmak izi gibi nesnel nitelikte bilgiler içerdiğini kabul etmesine rağmen otomatik olarak işlenmesi sonucu kimlik tespitinin ötesine geçilmesine imkân tanıyabileceğini *S. ve Marper* kararında vurgulamıştır. Dolayısıyla elde edilen kişisel verilerin, sağlık bilgilerine ulaşmak, bireyler arasındaki olası genetik ilişkiyi belirlemek veya ırka dair çıkarımlarda bulunmak gibi ilk baştaki toplanma amacının ötesinde işlenerek yeni bilgilere erişilmesine zemin hazırlaması, amaçla sınırlı olma ilkesi açısından ciddi sakıncalar doğurur.

Gelecekteki olası kullanımla birlikte yeni bilgiler elde edilmesine dair *S. ve Marper* davasında verilen örneğe göre, DNA profillerinden etnik kökene ilişkin çıkarımlar yapılabilir. Verilen bu örnek yüz tanıma sistemleri için de dikkate alınabilir. Zira kişilerin yüz görüntüleri de ırk veya etnik değerlendirme için kullanılabilir¹⁰⁷. Böyle bir kullanım ise ırk veya etnik kökene ilişkin bilgiler içe-

¹⁰⁴ *Van der Velden v Hollanda* App no 29514/05 (ECtHR, 7 Aralık 2006).

¹⁰⁵ *S. ve Marper v Birleşik Krallık* (n 98) paras 74-76.

¹⁰⁶ *ibid* paras 84-86.

¹⁰⁷ Birleşmiş Milletler İnsan Hakları Konseyi'nin A/HRC/41/35 numaralı 28.05.2019 tarihli "Gözetim ve İnsan Hakları" başlıklı raporuna göre, güvenilir raporlar, Çin Hükûmeti'nin ülke genelinde yüz tanıma teknolojisi ve gözetleme kameralarını birlikte kullanarak, "sadece görünüşlerine göre Uygur olarak nitelendirdikleri kişileri tespit edip, arama ve inceleme için geliş ve gidişlerini kayıt altına aldığı" öne sürmektedir. United Nations Human Rights Council (n 88) 5; Çin'de uygulanan oldukça müdahaleci yüz tanıma teknolojileri için ayrıca bakınız Amelin and Channov (n 3) 226.

receğinden özel nitelikli kişisel verilerin işlenmesi için öngörülen ek güvenceleri karşılayacak nitelikte olmalıdır ve ayrımcılık gibi olumsuz diğer sonuçlar dikkate alınmalıdır.

2. Müdahalenin Demokratik Bir Toplumda Gerekliliği

Mahkeme müdahalenin kanuni dayanağının niteliğine dair ayrıntılı değerlendirmeler yapmadan bu hususu demokratik bir toplumda gerekli olma şartı içerisinde ele almasına rağmen bazı kararlarda ulusal düzenlemelere ilişkin çıkarımlar ortaya koyar. Bu bağlamda tedbirin kapsamını ve uygulanmasını düzenleyen açık ve ayrıntılı kuralların yanı sıra tedbirin süresi, verilerin ve verilerden ulaşılan bilgilerin kullanım imkanları, saklama, üçüncü kişilerin erişimi, verilerin bütünlüğünün ve gizliliklerin sağlanması hususlarında asgari güvenceler öngörülerek, kötüye kullanma ve keyfiliğin önlenmesi gerektiğini vurgulayarak¹⁰⁸ yine uluslararası mevzuatta veri koruma için getirilen temel ilke ve kuralları benimser.

Müdahalenin demokratik bir toplumda gerekliği kıstası bakımından ise Mahkeme, doğrudan Sözleşme 108 ve Sözleşme 108+ maddelerine atıf yaparak, işleme tabi tutulan verilerin işleme amaçlarıyla bağlantılı olarak yeterli ve ilgili olması, gereksiz ve aşırı olmaması kuralını kabul eder. Ayrıca özel nitelikli verilere değinerek, biyometrik veriler için getirilen ek güvencelere vurgu yapar¹⁰⁹.

Ayrıca Mahkeme *Glukhin* kararında altını çizdiği üzere özellikle terör ve örgütlü suçlulukla mücadelede, modern soruşturma ve kimlik tespiti yöntemlerinin işlevselliğini kabul ederken, bunların sınırsız kullanımına karşı çıkarak, özel hayata saygı hakkının sınırlarını bir kere daha çizerek, Mahkemeye göre ceza adaleti sisteminde modern bilimsel tekniklerin kullanımına ne pahasına olursa olsun izin verilmesi halinde eğer bu tür tekniklerin kullanımından elde edilecek fayda ile özel hayat menfaatleri dikkatli bir şekilde dengelenmezse, Sözleşmenin 8. maddesinin sağladığı koruma kabul edilemez bir şekilde zayıflar. Taraf Devletlerin genelinin ulusal mevzuatlarına da yansıyan bu anlayış ve uzlaş, bu bağlamda özel hayata yapılacak müdahalenin değerlendirilmesinde Taraf Devletlere bırakılan takdir marjını daraltır.

Demokratik bir toplumda gerekli olma kıstası bağlamında Mahkeme özellikle kişisel verilerin muhafaza altına alınmasının orantılı olup olmadığını ve birbiriyle yarışır halde olan kamu çıkarları ile özel çıkarlar arasında adil bir denge kurulup kurulmadığını değerlendirilir. Kişisel verileri saklama yetkisi veren düzenlemelerin genel ve ayırım gözetmeyen yapısı Mahkemeye göre orantısız bir müdahale oluşturur. Bu bağlamda süre sınırı olmaksızın muhafaza etme¹¹⁰, işlevsiz bir silme hakkı tanınırken yirmi beş yıl gibi uzun bir süre saklama veya nüfusun tamamına

¹⁰⁸ *S. ve Marper v Birleşik Krallık* (n 98) para 99; *Glukhin v Rusya* (n 7) para 77.

¹⁰⁹ *S. ve Marper v Birleşik Krallık* (n 98) para 103.

¹¹⁰ ibid paras 104-125.



dair bilgileri alma¹¹¹, herhangi bir sınırlandırma olmadan her suçla ilgili olarak veri toplama işlemleri¹¹² aşırı, ilgisiz veya orantısız görülmüştür.

Mahkemenin bahsi geçen çıkarımları göz önünde bulundurulduğunda, orantılılık ve adil dengenin değerlendirilmesinde bazı kıstaslar öne çıkar. Bunlar, verilerin saklama süreleri, verilerin izlenen amaca uygunluğu ve gerekliliği, verilerin imha edilme şartları, verilerin toplanmasına sebebiyet veren suçların niteliği, ilgili kişilerin adli sicili, verilerin kullanılma amacı, verilerin kötüye kullanılması ihtimali ve bu bağlamda bunlara erişebilecek kişiler biçiminde sıralanabilir. Muhafaza sürelerinin sınırsız olması veya yeterli güvence öngörülmediği için ilk baştaki toplanma amacı dışında kullanılabilme imkânı müdahaleyi orantısız hale getirirken; verilerin belirli aralıklarla denetlenerek gerekli görülmediği durumda imha edilmesi ya da sadece belirli suçlarla ve hakkında kesinleşmiş mahkûmiyet hükmü bulunan kişilerle ilgili verilerin saklanmasına izin verilmesi kamu çıkarları ile özel çıkarlar arasında adil bir denge kurulmasını sağlayabilir¹¹³. Dolayısıyla düzenlemeler ve buna bağlı olarak uygulama ne kadar genel yapıdaysa ve orantılılık ile adil dengelyi sağlamak üzere öngörülen güvenceler ne kadar azsa, müdahalenin demokratik bir toplumda gerekli olduğunu kabul etmek de o kadar güçleşir.

3. Fotoğrafların Saklanması ve Yüz Tanıma Sistemleri

Kişilerin fotoğraflarının alınıp saklanması ve yüz görüntülerinin yüz tanıma sistemleri tarafından kullanılmasına dair içtihat ise görece yeni oluşmaktadır. Nitekim Mahkemenin 2020 yılında verdiği *Gaughran* kararında vurguladığı üzere fotoğrafların ceza muhakemesi süreciyle ilgili olarak toplanması ve muhafaza edilmesi işlemleri hakkında içtihat, parmak izi ve DNA profiline ilişkin kararlara nazaran yenidir. Müdahalenin varlığını tespit ederken Mahkeme, Komisyonun eski tarihli kararlarındaki görüşünden ayrılmış ve daha koruyucu bir eğilim geliştirmiştir.

Mahkemenin, fotoğrafların saklanmasını özel hayata saygı hakkına müdahale niteliğinde kabul etmesinin temel sebebi özel hayat kavramına dair ortaya koyduğu çıkarımdır. İçtihat gelişiminde özel hayat kavramının dinamik yapısına uygun olarak kapsamını ve koruma sahasını genişletirken, diğer hakların yanı sıra kişilik/kimlik hakkı (“*right to identity*”) ve kişisel gelişim hakkı, diğer insanlarla ve dış dünyayla ilişki kurma ve geliştirme hakkının yanı sıra bireyin kendi görüntüsü üzerindeki hakkını (“*person’s right to their image*”) dahi kavramın

¹¹¹ *M.K. v Fransa* (n 103) paras 37-46.

¹¹² *Gaughran v Birleşik Krallık* (n 103) paras 87-97; *Aycaguer v Fransa* App no 8806/12 (ECtHR, 22 Haziran 2017).

¹¹³ *P.N. v Almanya* (n 103) paras 76-90; *Peruzzo ve Mertens v Almanya* App nos 7841/08 ve 57900/12 (ECtHR, 4 Haziran 2013).

içine dahil etmiştir¹¹⁴. Kişinin görüntüsü, eşsiz özelliklerini ortaya koyduğu ve onu benzerlerinden ayırdığı için kişiliğinin başlıca niteliklerinden birini oluşturur¹¹⁵. Böylece Sözleşmenin 8. maddesi, kişilerin görüntülerine dair koruma ve güvence sağlar hale gelmiştir.

Yakın tarihli kararlarda belirtildiği üzere bir kişinin fotoğrafının çekilmesi ve otomatik olarak işleme ihtimaliyle birlikte polis veri tabanında saklanması müdahalenin varlığı için yeterlidir. Otomatik olarak işleme olasılığını vurgulayarak Sözleşme 108 ve Sözleşme 108+ düzenlemelerini dikkate aldığı söylenebilir.

Müdahalenin varlığının tespitinde Mahkeme özellikle yüz tanıma ve yüz haritalama teknolojisiyle ilgili olarak bu alanda hızlı teknolojik ilerlemelerin gerçekleşebileceğini göz ardı etmemektedir. Nitekim Taraf Devletlerin bir kısmı yüz tanıma sistemlerini kullanırken, bir kısmı ise geçiş sürecindedir. Örneğin yüz tanıma sistemi kurulmuş olmasına rağmen gözetim sırasında alınan görüntüler farklı bir veri tabanında saklanıyor olabilir. Ancak veri tabanlarının birbirine entegre edilme veya fotoğrafların yüz tanıma sistemlerine yüklenme ihtimali dahi Mahkemenin müdahalenin varlığının tespitinde göz önünde bulundurduğu durumlar arasındadır. Zira bu verilerin toplanma amacı dışında ve daha müdahaleci yöntemler için kullanılma olasılığı karşısında ulusal mevzuatın yeterli güvenceleri sağlaması gerekir.

Çalışma konusu *Glukhin* kararında ise Mahkeme, yüz tanıma sistemlerini ilk defa doğrudan değerlendirmiştir¹¹⁶. Yüz tanıma teknolojisinin uygulanması bağlamında, tedbirlerin kapsamını ve uygulanmasını düzenleyen ayrıntılı kuralların yanı sıra kötüye kullanım ve keyfilik riskine karşı güçlü güvencelere sahip olmanın gerekliliğini, içtihat gelişimine uygun olarak bu sefer de yüz tanıma bağlamında bir kere daha vurgularken; özellikle canlı yüz tanıma teknolojisinin kullanımı söz konusu olduğunda güvencelere duyulan ihtiyacın daha da artacağını altını çizmiştir¹¹⁷.

Yüz tanıma sistemlerinin ve biyometrik verilerin kullanılması noktasında Mahkemenin ulusal hukuktan beklediği, yüz tanıma teknolojisinin kullanımını gerektirecek durumların niteliği, izlenen amaçlar, hedef alınabilecek kişi kategorileri veya hassas kişisel verilerin işlenmesine ilişkin çerçevenin açıkça belirlenmesi, ayrıca bu hususlara dair genel nitelikli değil sınırlayıcı bir düzenlemenin öngörülmesi ve sınırlayıcı bir yorumun benimsenmesidir. Mahkemeye göre ayrıca yetkili kişi ve mercilerin belirlenmesi, toplanan verilerin incelenmesi, kullanılma-

¹¹⁴ *P.G. ve J.H. v Birleşik Krallık* (n 100) para. 56; *Uzun v Almanya* App no 35623/05 (ECtHR, 2 Eylül 2010) para 43; *Benedik v Slovenya* (n 95) para 100; *Sciacca v İtalya* (n 102) para. 29; *S. ve Harper v Birleşik Krallık* (n 98) para 66.

¹¹⁵ *Glukhin v Rusya* (n 7) para 66.

¹¹⁶ Monika Zalnieriute, ‘*Glukhin v. Russia*. App. No. 11519/20. Judgment’ (2023) 117 [4] *American Journal of International Law* 695, 695.

¹¹⁷ *Glukhin v Rusya* (n 7) para 86.



sı ve saklanması şartlarının öngörülmesi, sürecin denetlenmesi ve ilgili kişilere kanuni çareler sunulması gibi usuli güvenceler sağlanmalıdır¹¹⁸.

Son olarak belirtmek gerekir ki terör, örgütlü ve organize suçlulukla mücadelede modern bilimsel soruşturma ve kimlik tespiti tekniklerinin önemini kabul eden Mahkemenin¹¹⁹, yüz tanıma teknolojisini ve biyometrik verilerin kullanımını bir bütün olarak reddetmesi söz konusu değildir. Aksine suçla mücadelede bu görece yeni teknolojik araç ve imkanların önemine binaen incelemesini sınırlandırmaktadır. Mahkemece yapılan değerlendirme, müdahalenin Sözleşme'nin 8. maddesi kapsamında haklı olup olmadığıdır. Verilen ihlal kararlarının büyük çoğunluğu, özel hayata saygı hakkı ile kişisel verilerin korunmasına dair ortaya çıkarılmış uluslararası mevzuatın getirdiği güvenceleri bertaraf eden genel nitelikli düzenlemeler ile sınırlayıcı bir yorum yapılmaksızın suçun önlenmesi meşru amacının lehine ancak kişisel verilerin korunması hakkının aleyhine orantısız işlemlerin uygulanması sonucudur.

IV. TÜRK HUKUKU BAĞLAMINDA DEĞERLENDİRME

Türk Hukukunda kişisel veriler, özel hayatın gizliliği kapsamında anayasal koruma altındadır. Anayasa'nın 20. maddesine 5982 sayılı Kanun'la 2010 yılında eklenen 3. fıkrası "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir*" diyerek kişisel verilerin korunmasına anayasal bir temel kazandırmıştır.

Anayasanın anılan hükmüne binaen ihdas edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun amaçlarından biri de kişisel verilerin işlenmesinde özel hayatın gizliliği ile diğer ilgili temel hak ve özgürlükleri korumaktır.

Kanun'un 4. maddesi kişisel verilerin işlenmesine dair genel ilkeler öngörür. Uluslararası veri koruma mevzuatında yer alanlara benzer nitelikte hukuka ve dürüstlük kurallarına uygunluk, veri doğruluğu, belirli ve açık amaçların izlenmesi, amaç sınırlaması, veri minimizasyonu, ölçülülük, saklama sınırlaması ilkeleri maddede öngörülmüştür.

Kanun'un 6. maddesi ise özel nitelikli kişisel verilerin işlenme şartlarını ihdas etmektedir. Uluslararası mevzuatta ve Avrupa İnsan Hakları Mahkemesinin içtihadında hassas veriler olarak da adlandırılan özel nitelikli kişisel veriler arasında yine uluslararası mevzuata uygun olarak biyometrik veriler bulunmaktadır. Biyometrik verilerin işlenmesi 6. maddede kural olarak yasaklanırken işlenebileceği istisnai hallerden bir tanesi "*kanunlarda açıkça öngörülmesi*"dir.

¹¹⁸ Mahkemenin neredeyse sadece usuli güvencelere odaklanarak, kamusal alanlarda yüz tanıma teknolojisi kullanan kitlesel gözetimi meşrulaştırdığı yönünde eleştiriler için bakınız Zalnieriute (n 116) 698-701; Mahkemenin yüz tanıma sistemlerinin keyfi kullanımına karşı sağlanması gereken güvenceleri somutlaştırmadığı ve esnek bir değerlendirme yaptığına dair ayrıca bakınız Atak (n 57) 370.

¹¹⁹ *Glukhin v Rusya* (n 7) para 84.

Kişisel Verilerin Korunması Kanunu kapsamında üzerinde durulması gereken son bir husus, 6. maddenin 4. fıkrasında yer alan “özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır” düzenlemesidir. Hükme uygun olarak Kişisel Verileri Koruma Kurulu tarafından “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili 31 Ocak 2018 tarihli ve 2018/10 sayılı karar alınmış ve Resmi Gazetede yayımlanmıştır¹²⁰. Karara göre özel nitelikli kişisel verilerin işlenmesinde sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve usul belirlenmelidir.

Kişisel Verileri Koruma Kurumu tarafından hazırlanan “Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber” içerisinde ayrıca biyometrik veri işleme ilkeleri ortaya konmuştur. Rehberde göre biyometrik verilerin işlenmesinde öncelikle Kişisel Verilerin Korunması Kanunu’nun 4. ve 6. maddesinde öngörülen ilke ve şartlara uyulmalıdır. Bunların yanı sıra temel hak ve özgürlüklerin özüne dokunulmamalı, uygulanan yöntem izlenen amaç bakımından elverişli, gerekli ve orantılı olmalı, veriler gerektiği kadar saklanmalı ve bu bağlamda bir azami süre belirlenmeli ve saklama gerekliliği ortadan kalktığında derhal silinmelidir¹²¹.

Anayasal ve kanuni düzenlemelerin yanı sıra Türkiye, Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde imzaya açılan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’ni (Sözleşme 108) aynı gün imzalamıştır. Sözleşme, 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete’de yayımlanarak iç hukuka dâhil edilmiştir¹²². Sözleşme 2018 yılında kabul edilen bir protokolle güncellenerek Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Sözleşmesi veya Sözleşme 108+ olarak adlandırılmaya başlanmıştır. Sözleşme 108+ yeterli sayıdaki devlet tarafından kabul edilerek yürürlüğe girerken, Türkiye protokolü imzalamadığı için protokolle değişen yeni haliyle değil, ilgili Resmi Gazete’de yayımlanan değişiklik öncesi haliyle bağlı kalmaya devam etmektedir¹²³.

Türkiye’nin onayladığı Sözleşme metninde özel nitelikli veriler arasında biyometrik veriler sayılmasa da verilerin işlenmesine dair kanunilik, belirli ve meşru amaçların izlenmesi, amaç sınırlaması, verilerin amaçla bağlantılı olarak yeterli ve ilgili olması, veri doğruluğu, veri güvenliği ve saklama sınırlaması gibi ilke ve kurallar öngörülmüştür. Öte yandan Kişisel Verileri Koruma Kurulu’nun ilgili

¹²⁰ <<https://www.resmigazete.gov.tr/eskiler/2018/03/20180307-7.pdf>> erişildi 6 Mart 2025.

¹²¹ Kişisel Verileri Koruma Kurumu (n 49) 9-13.

¹²² Sözleşme 108’i imzalayan ve onaylayan devletlerin listesi için bakınız <<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>> erişildi 3 Mart 2025.

¹²³ Sözleşmeyi güncelleyen protokolü imzalayan ve onaylayan devletlerin listesi için bakınız <<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>> erişildi 3 Mart 2025.



kararı ile Kişisel Verilerin Korunması Kurumunun ilgili rehberinde biyometrik verilerin de içinde bulunduğu özel nitelikli verilerin işlenmesine dair uluslararası mevzuatla uyumlu ek kurallar ve güvenceler öngörülmüştür. Dolayısıyla Avrupa İnsan Hakları Mahkemesi içtihadında da vurgulanan kişisel verilerin işlenmesinde dikkate alınması gereken ilke ve kurallar, taraf olunan Sözleşme ve ulusal mevzuat uyarınca iç hukukun bir parçasıdır ve kişisel verilerin korunması hakkına müdahale edecek düzenlemeler ile uygulamalarda bu ilke ve kuralların dikkate alınması gerekir.

A. Kimlik Tespit Amacıyla Fotoğrafların Saklanması

Türk ceza adalet sisteminde, kimlik tespiti amacıyla fotoğrafların alınarak saklanması 2559 sayılı Polis Vazife ve Salâhiyet Kanunu'nda öngörülmüştür. 5681 sayılı Kanun'un 2. maddesiyle yeniden düzenlenmiş olan 2559 sayılı Polis Vazife ve Salâhiyet Kanunu'nun "parmak izi ve fotoğrafların alınması" başlıklı 5. maddesine göre "*kişilerin fotoğrafları alınarak ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır*". Önleyici kolluk faaliyetleri ile ceza muhakemesi süreciyle bağlantılı olarak toplanarak sisteme kaydedilecek fotoğraflar şunlardır:

- Gözaltı kararı sonrası alınan fotoğraflar
- 5271 sayılı Ceza Muhakemesi Kanunu'nun 81. maddesi hükmüne göre alınan fotoğraflar
- 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un 21. maddesi hükmüne göre alınan fotoğraflar

Fotoğrafların hangi amaçla alındığı ve kullanılacağı da Polis Vazife ve Salâhiyet Kanunu'nun 5. maddesinde düzenlenmiştir. Buna göre aşağıda yer alan amaçlarla bu veriler mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir:

- Kimlik tespiti
- Suçların önlenmesi
- Yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması

Maddenin diğer fıkralarına göre tutulan bu kayıtlar gizlidir ve belirtilen amaçlar dışında kullanılamaz. Verilerin saklanma süreleri de öngörülmüştür ve ilgili fıkra göre "*fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir*". Son olarak kayıtlı verilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi de kurulmalıdır.

Polis Vazife ve Salâhiyet Kanunu’nda öngörülen bu tedbire ilişkin getirilen şart ve güvencelerin, uluslararası veri koruma mevzuatında öngörülen ve Avrupa İnsan Hakları Mahkemesi içtihadında da yer alan kişisel verilerin korunmasına ilişkin ilke ve kurallara genel olarak uygun olduğu söylenebilir.

Özel hayatın gizliliği bağlamında kişisel verilerin korunması hakkına müdahale niteliğindeki bu tedbir, Anayasa’nın 13. maddesinde de kaynağını bulan kanunla öngörülme şartını karşılamaktadır. Tedbirle izlenen meşru amaç ise Avrupa İnsan Hakları Sözleşmesinin 8 maddesi ile Anayasa’nın 20. maddesinde özel hayatın gizliliği bağlamında öngörülen suç işlenmesinin önlenmesi amacıdır.

Düzenleme gereği muhafaza edilen bu verilerin açık, belirli ve meşru amaçlar için toplandığı söylenebilir. Öte yandan kanun, belirtilen bu amaçlar dışında verilerin kullanılmasını yasaklayarak, amaçla bağdaşmayan biçimde işlenmesini de önlemektedir. Verilerin hangi kamu görevlisi tarafından hangi amaçlarla kullanıldığıнын denetlenmesine imkân tanıyan bir sistemin öngörülmesi ise amaç sınırlamasının yanında bunlara erişebilecek kişileri de sınırlandırarak, verilerin adil (dürüstlük kurallarına uygun) işlenmesine hizmet eder.

İşlemenin, izlenen meşru amaç bakımından orantılı olması gerekliliği bakımından ise düzenleme eleştirilebilir. Bu bağlamda öncelikle verilerin saklanma süresi üzerinde durulabilir. Düzenlemeye göre “*fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl*” geçtikten sonra silinmektedir. Avrupa İnsan Hakları Mahkemesi içtihadında da sıklıkla incelenen hususlardan biri olan saklama süresinin uzunluğu, tedbiri orantısız hale getirirken, kamu çıkarları ile özel çıkarlar arasındaki adil dengenin de bozulmasına sebebiyet verebilir. Kanun’un, sadece hakkında kesinleşmiş mahkûmiyet hükmü olanların değil aynı zamanda gözaltı işlemi uygulanan şüphelilerden de fotoğraf alınarak saklanmasına izin vermesi, dengeyi özel menfaatler aleyhine bozar niteliktedir. Ayrıca düzenleme, ilgili kişiler bakımından bir ayrıma gitmediği gibi isnat edilen suç açısından da farklılaştırma yapmamaktadır. Dolayısıyla verilerin toplanmasına sebebiyet veren suçların niteliği ve ilgili kişilere dair ayırım gözetmeyen genel nitelikli bu düzenleme Avrupa İnsan Hakları Mahkemesi içtihadında ortaya konan çıkarımlar bakımından sorunludur. Öte yandan kişisel verilerin korunmasıyla ilgili Türkiye’nin de taraf olduğu uluslararası metinlerde yer alan orantılılık ilkesi ve buna bağlı olarak verilerin işleme amaçları için gerekli olandan daha uzun süre muhafaza edilmemesi kuralı bakımından da eleştirilmeye layıktır¹²⁴.

Dikkate alınması gereken diğer bir husus ise ceza muhakemesi süreciyle bağlantısı olmayan hallerdir. Düzenlemeye göre “*her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan*” kişilerden de fotoğraflar alınarak aynı sisteme kaydedilecek, bu veriler kimlik

¹²⁴ Benzer çıkarımlar için bakınız Süleyman Özar, ‘Adli ve İdari Kolluk Sınırları Bakımından Fizik Kimliğin Tespiti İşleminde Kişisel Veriler’ (2023) 81 [3] Ankara Barosu Dergisi 263, 280.



tespiti, suçların önlenmesi ve maddi gerçeğin açığa çıkarılması için kullanılabilecektir. Pasaport ve özellikle sürücü belgesi için başvuruda bulunan herkesin kapsama dahil edilmesi yetişkin kişilerin büyük bir bölümünün kişisel verilerinin toplanmasına sebebiyet verir. Nüfusun tamamına dair fotoğrafların alınması söz konusu değilse de toplumun büyük bir çoğunluğunun fotoğraflarının, aynı veri tabanına dâhil edilerek suç önleme ve ceza muhakemesi süreciyle bağlantılı olarak işlenebilecek olması orantılılık bağlamında sorun yaratabilecek niteliktedir.

Eleştirisi konusu yapılan bu eksikliklerin olası olumsuz etkileri, saklanan ve işlenen verilerin biyometrik ve dolayısıyla özel nitelikli olması halinde daha da artar. Veri korumaya dair uluslararası metinlerde kabul edilen biyometrik veri tanımına göre aranan niteliklerden bir tanesi “*belirli bir teknik işleme ile ortaya çıkma*”dır¹²⁵. Düzenleme uyarınca alınan ve saklanan fotoğraflara böyle bir nitelik atfetmek mümkün gözükmemektedir. Fotoğrafların, kişilerin benzersiz veya ayırt edici özelliklerini gösterecek biçimde şablonlarının çıkarılacağı veya başka bir biçimde biyometrik veri haline getirileceğine dair herhangi bir hüküm yoktur. Kişisel Verilerin Korunması Kanunu’nun 6. maddesi ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri de özel nitelikli veriler arasında saymasına rağmen tedbir kapsamında mahkûmiyet veya güvenlik tedbiri dışında bir kararla yargılaması sonlanmış kişilerin de fotoğrafları saklanabileceğinden, muhafaza edilen bu verilerin tamamının özel nitelikli olarak kabul edilmesi ve ek güvenceleri gerektirmesi söz konusu olmayacaktır. Ancak bu fotoğraflar bir yüz tanıma sisteminde kullanılmak üzere biyometrik veri haline getirilirse daha müdahaleci olan bu yöntem için özel nitelikli veriler bağlamında yorum yapmak gerekecektir.

B. Türk Ceza Adalet Sisteminde Yüz Tanıma

Polis Vazife ve Salâhiyet Kanunu’nda öngörülen fotoğrafların alınması ve saklanması tedbirinin herhangi bir yüz tanıma sisteminin parçası olduğunu söylemek güçtür. İlgili hükmün atıf yaptığı Ceza Muhakemesi Kanunu’nun 81. maddesinin düzenlemesi ile Yargıtay kararlarına bakıldığında da, verilerin otomatik olarak işlenerek bir tanımlama yapılmadığı aksine fiziksel ortamda veya sisteme kayıtlı fotoğraflar üzerinden insanlar tarafından geleneksel yöntemler kullanılarak kimlik tespiti yapıldığı anlaşılmakta¹²⁶; aksini gösterir bir düzenleme, karar veya açıklamaya da rastlanmamaktadır.

¹²⁵ Kişisel Verileri Koruma Kurumu tarafından hazırlanan “Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber” içerisinde biyometrik veri kavramı için Genel Veri Koruma Tüzüğündeki tanıma atıf yapılması, uluslararası veri koruma mevzuatında yer alan tanımlamanın kabul edildiğini gösterir. Kişisel Verileri Koruma Kurumu (n 49) s. 4.

¹²⁶ Örneğin fotoğraflar, olaydaki failin, gözaltına alınan şüpheli ile aynı kişi olup olmadığının belirlenmesi amacıyla yapılan teşhis işlemi sırasında kullanılmaktadır. “*Teşhis işlemi gerektiğinde fotoğraf üzerinden de yapılabilecek olan ve bu yönüyle de şüphelinin imzasının alınmasının bile zorunlu olmadığı bir tanıma işlemidir.*” Yargıtay Ceza Genel Kurulu, E 2008/70, K 2008/84, T 15.04.2008 <<https://www.lexpera.com.tr>> erişildi 4 Mart 2025.

Mevcut düzenlemelere göre Türk ceza adalet sisteminde yüz tanıma sistemlerinin kullanılmadığı söylenebilir¹²⁷. Bununla birlikte 2021 yılında dönemin İçişleri Bakanının açıklamalarına göre, emniyet teşkilatı içerisinde operasyonel ve istihbari çalışma yapan Siber Suçlarla Mücadele Daire Başkanlığı ile emniyet çalışanları yüz tanıma programı geliştirmiştir¹²⁸. Ancak istihbari veya suçların önlenmesi amacıyla bahsi geçen programın test aşamasını geçip gerçek hayatta kullanımına başlanıp başlanmadığına dair bir bilgi verilmemiştir. İçişleri Bakanının 2022 yılında basına verdiği bilgiye göre ise 2021 ve 2022 yıllarında 66 terörist yüz tanıma sistemleri üzerinde yapılan analiz sonucunda yakalanmıştır¹²⁹. Fakat bu açıklamada da yöntemin kapsamı ve dayanağı düzenlemeye dair bir beyanda bulunmamıştır. Ayrıca 3713 sayılı Terörle Mücadele Kanunu’nda, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu’nda veya önleyici ve istihbari faaliyetlerin yürütülmesinde uygulanabilecek tedbirlere dair hükümler içeren 2559 sayılı Polis Vazife ve Salâhiyet Kanunu’nun ek 7. maddesinde yüz tanıma teknolojisinin kullanımına dair herhangi bir düzenleme bulunmamaktadır.

Yakın geçmişte ise uluslararası savunma elektroniği şirketi olan ASELSAN¹³⁰ tarafından geliştirilen yaka kameralarının kolluk tarafından kullanılmaya başlandığı bilgisi ortaya çıkmıştır. 2024 yılının Mart ayında yapılan habere göre ODAKAN isimli yaka kameraları jandarma tarafından kullanılmaya başlanmış, sonrasında ise Emniyet Genel Müdürlüğü’nün kullanımına sunulmuştur. Gece görüşü imkânına da sahip olan ODAKAN yaka kameraları, sesli video kaydı yapabilmekte ve yüksek çözünürlüklü fotoğraflar çekebilmektedir. Haberde “*Hem merkeze canlı yayın yapan hem de görüntüyü hafızasına kaydeden kamera sayesinde anlık taramayla aranan suçlular veya suça karışmış araç plakaları sahada görevli güvenlik güçlerinin kullandığı cihaza bildiriliyor.*” şeklinde bir açıklamayla cihazın işlevi aktarılmıştır. Yapay zekâ algoritmaları kullanabilecek biçimde tasarlanan bu cihazların yakın gelecekte yaygınlaştırılmasının ve geliştirilmiş yüz ve plaka tespit özelliklerinin kullanıma alınmasının planlandığı da haberdeki bilgiler arasında yer almıştır¹³¹. Yakın tarihlerde İçişleri Bakanı da bir açıklama yapmış ve başta büyükşehirler olmak üzere tüm Türkiye’de jandarma, polis ve trafik asayiş

¹²⁷ Türk hukukunda yüz tanıma teknolojisinin uygulamasına dayanak teşkil edecek kanuni bir düzenleme olmadığına dair benzer çıkarımlar için bakınız İçer and Dönmez (n 57) 448.

¹²⁸ <<https://www.hurriyet.com.tr/gundem/bakan-soylu-yuz-tanima-projesini-boyle-duyurdu-gecebilendaha-gormedim-41901500>> erişildi 6 Mart 2025.

¹²⁹ <<https://www.trthaber.com/haber/gundem/bakan-soylu-66-deasli-terorist-yuz-tanima-sistemiyle-yakalandi-670316.html>> erişildi 6 Mart 2025.

¹³⁰ <<https://www.aselsan.com.tr/hakkimizda>> erişildi 7 Mart 2025.

¹³¹ <<https://www.aa.com.tr/tr/bilim-teknoloji/aselsanin-yaka-kamerasi-guvenlik-guclerinin-ucuncu-gozu-oldu/3173199>> erişildi 7 Mart 2025.



ekiplerinin ASELSAN tarafından geliştirilen yüz tanımalı yaka kamerası kullanacağını söylemiştir¹³².

Yapılan açıklamalar ve basına yansıyan haberler dikkate alındığında, suç önleme ve istihbari amaçlarla kimlik tespitine yönelik olarak yüz tanıma sistemlerinin yakın gelecekte kullanılacağı ve yaygınlaşacağı anlaşılmaktadır.

Yüz tanıma sistemlerinin yakın gelecekteki kullanım ihtimaline rağmen tekrar vurgulamak gerekir ki böyle bir uygulamanın henüz kanuni bir dayanağı yoktur. Ulusal ve uluslararası veri koruma mevzuatı ile Avrupa İnsan Hakları Mahkemesi içtihadı göz önünde bulundurulduğunda Polis Vazife ve Salâhiyet Kanunu'nun 5. maddesi veya Ceza Muhakemesi Kanunu'nun 81. maddesi kapsamında bu sistemlerin kullanılması mümkün değildir. Bahsi geçen düzenlemeler ilgili kişilerden alınan fotoğraflardan biyometrik şablon çıkarılıp çıkarılmayacağını veya bunların yüz tanıma sistemlerinde kullanılıp kullanılmayacağını düzenlememektedir.

Polis Vazife ve Salâhiyet Kanunu'nun 5. maddesinde yine bir biyometrik veri olan parmak izi bakımından şartlar öngörülmüş olsa da yüz görüntülerinin ve şablonlarının elde edilmesi, saklanması ve yüz tanıma teknolojisi kullanılarak işlenmesinin, özel hayata saygı bağlamında kişinin görüntüsü üzerindeki hakkı da dikkate alınarak kendine özgü müdahaleci yapısı¹³³ göz önünde bulundurulmalı ve özel düzenleme yapılmalıdır¹³⁴.

Yüz tanıma sistemlerinin kullanımının kanuni dayanağı oluşturulurken, Polis Vazife ve Salâhiyet Kanunu'nun 5. maddesine dair bir üst başlıkta değerlendirilen, kişisel verilerin korunmasına dair temel kurallara uyulmalıdır. Öte yandan yüz tanıma sistemlerinin farklı kullanım imkanları ve müdahaleci yapısı ile biyometrik verilerin toplanması, işlenmesi ve saklanmasına dair ek güvenceler ve kurallar da dikkate alınmalıdır¹³⁵. Basına yansıyan haberler üzerinden meseleyi somutlaştırmak gerekirse, tedbirinin kapsamına dair çeşitli sorular ortaya çıkar. Yüz tanıma, suç önlemenin yanı sıra bir soruşturmayla bağlantılı olarak maddi

¹³² <<https://www.aa.com.tr/tr/politika/bakan-yerlikaya-basta-buyuksehirler-olmak-uzere-jandarma-ve-polisimizin-yuz-tanimali-yaka-kamerasi-olacak/3164725>> erişildi 7 Mart 2025.

¹³³ Diğer biyometrik verilere kıyasla yüzlerin kolayca görülebilir ve kaydedilebilir olması, müdahalenin yoğunluğunu artırır. Yaka kamerası üzerinden uygulanan kullanımlarda ise her anın kayıt altına alınması olası kötüye kullanımlara zemin hazırlar. Berle (n 30) 2, 76.

¹³⁴ Bahri Öztürk and others, *Dijital Ceza Muhakemesi Hukuku* (3rd edn, Seçkin Yayıncılık 2024) 476; İldırar (n 84) 73-78; Ayrıca yüz tanıma sistemlerinin hukuka aykırı bir biçimde uygulanması sebebiyle 5237 sayılı Türk Ceza Kanunu'nun İkinci Kitap Dokuzuncu Bölüm "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" altında düzenlenen suçların işlenebileceğine dair çıkarımlar için bakınız İçer and Dönmez (n 57) 442-443, 449.

¹³⁵ Biyometrik verilerin işlenmesinde izlenmesi gereken ilke ve kurallara dair değerlendirmeler için bakınız Aydın Akgül, 'Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı' (2015) 118 TBB Dergisi 199, 207-219; Yüz tanıma sistemleri vasıtasıyla kişisel veriler işlenirken 6698 sayılı Kanun'un 4. maddesi çerçevesinde izlenmesi gereken ilke ve şartlarla ilgili değerlendirmeler için ayrıca bakınız İçer and Dönmez (n 57) 450-455; Öztürk and others (n 134) 475-476.

gerçeğin açığa çıkarılmasında kullanılabilecek midir veya görüntüler ve eşleştirme sonucu bir delil niteliği taşıyacak mıdır? Yaka kameralarından elde edilen görüntüler ve yüz tanıma için kullanılan yüz görüntülerinin tamamı saklanacak mıdır, bunlar ne zaman silinecektir, bu verilerin izlenen amaca uygun olarak saklanma gerekliliği düzenli olarak denetlenecek midir? Elde edilen görüntüler hangi veri tabanlarındaki görüntülerle eşleştirilecek, uygulama geriye dönük mü yapılacak yoksa canlı yüz tanıma mı kullanılacaktır? Yüz tanıma için kullanılan algoritmanın asgari güvenilirliği ve doğruluğu kullanım öncesi testlerle tespit edilecek midir? Görüntülere ve eşleştirme sonuçlarına sahadaki ve merkezdeki hangi kolluk görevlileri erişebilecektir, bu sistemlere erişim ve kullanım denetlenecek midir? Tüm bu sorular ve özel hayatın gizliliği bağlamında kişisel verilerin korunmasına dair ortaya çıkmış ve çıkacak kurallar ve güvenceler dikkate alınarak hukuki temel ortaya çıkarılmalı ve gerektiğinde güncellenmelidir.

SONUÇ

Günümüzde ceza adalet sistemlerinde kullanılan yüz tanıma teknolojisi, fotoğraf veya videolardan kişilerin yüz şablonlarını ("*template*") çıkarır. Teknolojinin kullandığı yüz şablonları, kişinin benzersiz veya ayırt edici bir özelliğini ifade eder ve teknik bir inceleme sonucu kişinin tanımlanmasına, diğer bir ifadeyle kimliğinin tespit edilmesine imkân sağlar. Yüz şablonlarına atfedilen bu nitelik ve işlenme biçimi, uluslararası veri koruma mevzuatında yer alan tanımlamalara göre bunların biyometrik veri olarak sınıflandırılmasını gerektirir. Biyometrik veriler ise hem uluslararası mevzuata hem de 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre hassas veya özel nitelikli veriler arasındadır. Bu sebeple yüz tanıma sistemlerince kullanılan veriler için sadece temel ilke ve kurallar değil aynı zamanda özel nitelikli veriler için ayrıca öngörülen yasaklar ve güvenceler de devreye girer.

Kişisel verileri Sözleşmenin 8. Maddesiyle güvence altına alınan özel hayata saygı hakkı bağlamında yorumlayan Avrupa İnsan Hakları Mahkemesi, özel hayat kavramını geniş bir terim biçiminde nitelendirirken bireyin kendi görüntüsü üzerindeki hakkını ("*person's right to their image*") dahi koruduğunu kabul etmektedir.

Kişinin fotoğrafının çekilmesi ve otomatik olarak işlenme ihtimaliyle birlikte polis veri tabanında saklanmasını veya biyometrik verilerin toplanarak muhafaza edilmesini özel hayata saygı hakkına müdahale niteliğinde gören Mahkeme, yürütülen bu faaliyetlerin suçla mücadeledeki önemini göz ardı etmemektedir. Öte yandan müdahalenin demokratik bir toplumda gerekli olup olmadığını belirlerken temelde iki hususu araştırır. Bunlar kişisel verilerin toplanması, saklanması veya işlenmesinin orantılı olup olmadığı ve birbiriyle yarışır halde olan kamu çıkarları ile özel çıkarlar arasında adil bir denge kurulup kurulmadığıdır. Orantılılık ve adil denge kıstaslarının karşılanmaması sebebiyle verdiği ihlal kararlarının çoğunlukla esas sebebi ise müdahalenin ulusal mevzuattaki kanuni dayanağının



ayrım gözetmeyen genel nitelikli yapısıdır. İsnat edilen suçun niteliği veya ilgili kişi bakımından herhangi bir farklılaştırılmaya gidilmemesi, verilerin süre sınırı olmaksızın veya çok uzun süreler saklanması, ülkedeki herkesin bilgilerinin depolanması gibi uygulamalara sebebiyet veren veya bunların gerçekleşmesine zemin hazırlayan kanuni düzenlemeler ya da bunların yorumu ihlal için yeterli görülmektedir.

Orantılılık ile çıkarlar arasındaki adil dengenin sağlanması noktasında Mahkemece yapılan bu dar yorum ve gerekli güvencelerin sağlanması yönündeki beklenti, biyometrik verilerle ilgili uluslararası veri koruma mevzuatındaki çıkarımlarla uyumludur. Nitekim Sözleşme 108+'nın 6. maddesine göre biyometrik veriler işlenirken, Sözleşmede öngörülen diğer güvenceleri tamamlayan uygun ek güvencelerin kanunda yer alması gerekir. 2016/680 Sayılı Direktif'in 10. maddesine göre ise kimlik tespiti için biyometrik verilerin işlenmesi ancak işleme mutlak surette gerekli olduğunda ve veri sahibinin/ilgili kişinin hak ve özgürlüklerinin korunması bakımından yeterli önlemler alındığında mümkündür.

Türk hukuku bağlamında kişisel verilerin korunması Anayasal olarak güvence altına alınmış ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'yla kişisel verilerin işlenmesinde özel hayatın gizliliği ile diğer ilgili temel hak ve özgürlüklere getirilen korumanın kapsamı belirlenmiştir. Anayasal ve kanuni düzenlemelerin yanı sıra Türkiye, Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde imzaya açılan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni (Sözleşme 108) imzalamış ve Sözleşme 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete'de yayımlanarak iç hukuka dâhil edilmiştir. Öte yandan Kişisel Verileri Koruma Kurulu'nun ilgili kararı ile Kişisel Verilerin Korunması Kurumunun ilgili rehberinde biyometrik verilerin de içinde bulunduğu özel nitelikli verilerin işlenmesine dair uluslararası mevzuatla uyumlu ek kurallar ve güvenceler öngörülmüştür. Dolayısıyla Avrupa İnsan Hakları Mahkemesi içtihadında da vurgulanan kişisel verilerin işlenmesinde dikkate alınması gereken ilke ve kurallar, taraf olunan Sözleşme ve ulusal mevzuat uyarınca iç hukukun bir parçasıdır ve kişisel verilerin korunması hakkına müdahale edecek düzenlemeler ile uygulamalarda bu ilke ve kuralların dikkate alınması gerekir.

Kolluğun yaka kameraları üzerinden ülkemizde yakın gelecekte kullanılması planlanan yüz tanıma teknolojisi için, kaynağını ulusal ve uluslararası veri koruma mevzuatından alan ve Avrupa İnsan Hakları Mahkemesi tarafından da benimsenen temel ilke ve kurallar göz önünde bulundurulmalı ve bu bağlamda aşağıdaki hususlar gerçekleştirilmelidir:

1. **Tedbirin kanuni dayanağı olmalıdır:** Polis Vazife ve Salâhiyet Kanunu'nun 5. Maddesi, Ceza Muhakemesi Kanunu'nun 81. maddesi veya suç önleme ve istihbari amaçlarla uygulanabilecek tedbirlerin öngörüldüğü diğer kanuni düzenlemeler bu ihtiyacı karşılamadığı için ayrıca düzenleme yapılması gerekir.

2. **Yüz görüntüleri ile yüz şablonlarının toplanması için açık, belirli ve meşru amaçlar öngörülmalıdır:** Kanun'da, kimlik tespiti, suç önleme veya maddi gerçeğin açığa çıkarılması gibi hangi amaçların izleneceği açıkça ortaya konmalıdır.
3. **Elde edilen veriler, öngörülen meşru amaçlarla bağdaşmayacak bir biçimde kullanılmamalıdır:** Örneğin yüz şablonlarının sadece kimlik tespiti amacıyla kullanılabileceği kanunda öngörülmüşken, bu verilerden yola çıkılarak profillemeye veya etnik kökene dair çıkarımlar yapılmamalı ve bunlar ceza adalet sisteminde kullanılmamalıdır. Yararlanılan sisteme bu yönde güvenceler getirilmelidir.
4. **Toplanan ve işlenen veriler, yeterli ve ilgili olmalı, gereksiz ve aşırı olmamalıdır:** Kanun'da öngörülen amaç için gerekli olan veri toplanarak işlenmelidir. Dolayısıyla örneğin nüfusun büyük bir bölümünden veya tamamından kişisel verilerinin toplanmasına izin veren bir düzenleme yapılmamalıdır.
 - a. **Verileri toplanacak ve işlenecek ilgili kişiler açıkça belirlenebilir:** Örneğin sadece gözaltına alınan, hakkında tutuklama kararı verilen veya kesinleşmiş mahkûmiyet hükmü bulunan kişilerden yüz şablonu alınabileceği açıkça belirtilebilir. Farklılaştırma suç türleri bakımından da yapılabilir, bu bağlamda bir suç kataloğu öngörülebilir.
 - b. **Yüz şablonlarının eşleştirilmesinde kullanılacak veri tabanları sınırlandırılabilir:** Ülkede farklı özel ve kamusal amaçlar için yüz görüntüleri toplanıyor olabilir. Ceza adalet sisteminde yüz tanıma kullanılırken, erişilebilecek veri tabanları açıkça belirtilerek, farklı amaçlar için toplanan verilerin bulunduğu veri tabanlarına erişim sınırlandırılabilir. Kişilerin sosyal medya üzerinden paylaştıkları görüntülerin kullanılabilirliğine dair açık düzenleme yapılarak sınırlama getirilebilir.
 - c. **Verilerin doğruluğunu ve güncelliğini denetleyecek, hatalı verilerin gecikmeksizin silinmesini sağlayacak bir sistem kurulabilir.**
5. **İzlenen amaca uygun olarak verilerin saklama ve imha şartları açıkça belirtilmelidir:** Verinin yeterli ve ilgili olması ilkesiyle yakından ilişkili olan bu kurala göre özellikle hakkında kesinleşmiş bir mahkûmiyet hükmü olmayan kişiler bakımından süre sınırı olmaksızın verilerin saklanması orantısız bir müdahale oluşturduğundan, orantılılık ilkesine uygun bir süre belirlenmelidir.
 - a. **Veri türlerine göre farklı saklama süreleri belirlenebilir:** Saklanan veriden farklı bilgilere ulaşma imkânı ve saklamanın müdahaleci yapısı göz önünde bulundurularak saklama sürelerinde farklılaştırma yapılabilir. Örneğin görüntüden elde edilen yüz şablonu saklanabilirken, görüntünün daha kısa süreler içerisinde silinmesi öngörülebilir.



- b. **Alınma sebebine ve ilgili kişinin adli siciline göre saklama süreleri farklılaştırılabilir:** Gözaltına alınan kişiden elde edilen verilerin, hükümlü bir kişiden alınan verilere göre daha az saklanması öngörülebilir. Bu husus hem masumiyet karinesi hem de orantılılık ilkesiyle bağlantılıdır.
 - c. **İmha için düzenli aralıklarla inceleme gerekliliği öngörülebilir:** Verilerin saklanmaya devam edilmesinin gerekliliği düzenli aralıklarla incelenerek gerekli olmadığının anlaşılması halinde imha edileceği düzenlenebilir.
 - d. **İlgili kişiler için hukuki çareler öngörülebilir:** Saklanma şartlarının ortadan kalkması halinde imhası için yetkili mercie başvuru imkânı getirilebilir.
6. **Veri güvenliği sağlanmalıdır:** Verilerin kötüye kullanılmasını veya yetkisiz üçüncü kişilerin eline geçmesini engelleyecek güvenceler öngörülmelidir.
- a. Verilere ve işleme sonucu elde edilen çıktıya kimlerin erişebileceği açıkça düzenlenebilir.
 - b. Kişisel Verileri Koruma Kurulu tarafından “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” başlıklı kararına göre “*özel nitelikli veriler kriptografik yöntemlerle saklanmalı, verilere ve işleme sonucu elde edilen çıktıya erişebilecek kişilerin yetki kapsamı ve süresi belirlenmeli ve sistemde yapılan her bir işlem kayıt altına alınmalıdır*”. Yüz tanıma sistemlerinde biyometrik veri kullanıldığından bu güvencelerin sağlanması gerekir.
 - c. Kazara kayıp, imha ve diğer zararları önleyecek güvenlik önlemleri sağlanabilir.
7. **Yüz tanıma için kullanılan algoritmanın güvenilirliği ve doğruluğu sağlanmalıdır:** Algoritma gerçek olaylara uygulanmadan önce yeterince test edilmelidir. Erişebileceği veri türleri açıkça belirlenmelidir.
8. **Veri işlemeyle elde edilecek menfaatle, müdahale edilecek hak ve özgürlükler arasında adil bir denge ve orantılılık, hem kanuni dayanak oluşturulurken hem de uygulama sırasında gözetilmelidir.**
- a. **Kullanılan yönteme göre değerlendirme yapılmalıdır:** Geriye dönük yüz tanıma veya canlı yüz tanımadan hangisi kullanılıyorsa ona göre şartlar belirlenmelidir. Kontrolsüz bir ortamda canlı yüz tanıma yapılması oldukça müdahaleci bir yöntem olduğundan, gereklilik ve orantılılık bakımından sıkı bir inceleme yapılmalı ve katı gereklilik (“*strict necessity*”) gözetilmelidir.
 - b. **Herhangi bir sınırlandırma veya istisna olmadan herkesi kapsayan bir düzenleme ve uygulama yapılmamalıdır:** Üst başlıklarda da değinildiği üzere amaç, ilgili kişiler ve suçlar ile kullanılan veriler ve saklama şartlarına dair, gereklilik ve orantılılık temelinde sınırlamalar getirilmesi gerekir.

Tüm bu hususların yanı sıra yüz tanıma teknolojilerindeki hızlı gelişmeler sebebiyle ortaya çıkabilecek yeni müdahaleci yöntemler ve keyfilik riski ile özel hayata saygı bağlamında kişisel verilerin korunmasına dair getirilebilecek yeni kurallar göz önünde bulundurularak, yüz tanıma sistemlerinin kullanıldığı tedbirlerle dair kanuni dayanak gerektiğinde güncellenmelidir. İlgili hak ve özgürlüklerin özüne saygı gösterilerek, bunların kullanımını ciddi biçimde engelleyecek orantısız uygulamalardan kaçınılmalıdır.

KAYNAKÇA

Akgül A, ‘Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı’ (2015) 118 TBB Dergisi 199

Akgül A, ‘Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve Ab Adalet Divanı’nın ‘Google Kararı’ (2015) 116 TBB Dergisi 11

Alpaydın E, *Machine Learning* (The MIT Press 2021)

Amelin R and Channov S, ‘On the Legal Issues of Face Processing Technologie’ in Daniel A. Alexandrov, Alexander V. Boukhanovsky, Andrei V. Chugunov, Yuri Kabanov, Olessia Koltsova, Ilya Musabirov (eds), *Digital Transformation and Global Society 5th International Conference* (Springer Nature 2020) 223

Article 29 Data Protection Working Party, *Opinion 2/2012 on facial recognition in online and mobile services* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> erişildi 21 Ocak 2025

Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> erişildi 28 Ocak 2025

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> erişildi 28 Ocak 2025

Atak S, ‘Biyometrik ve Genetik Verilerin Korunması Konusunda Avrupa Konseyi’nin Genel Yaklaşımı’ (2024) 60 Türkiye Adalet Akademisi Dergisi 343

Berle I, *Face Recognition Technology Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images* (Springer Nature 2020)

Can N, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması* (On İki Levha Yayıncılık 2021)

Cole SA, *Suspect Identities A History of Fingerprinting and Criminal Identification* (Harvard University Press 2002)



Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on Facial Recognition* (2021) <<https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html>> erişildi 20 Ocak 2025

Council of Europe, *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data* (2005) para 8 <<https://rm.coe.int/16806840ba>> erişildi 16 Mart 2025

Donohue LK, ‘Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age’ (2012) 97 Minnesota Law Review 407

Dülger MV, ‘İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması’ (2018) 5 [1] İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 71

European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en> erişildi 20 Ocak 2025

European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* <<https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law#publication-tab-7>> erişildi 21 Ocak 2025

Evison MP, ‘Forensic Facial Analysis’ in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer Science Business Media 2014) 1713

Gless S, ‘AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials’ (2020) 51 [2] Georgetown Journal of International Law 195

Ildırar E, ‘Kolluğun Vücut Kamerası Kullanımı ve Türkiye’de Uygulanabilirliği’ in Oktay Karaalp, Barkın Özyurt and Gökçen Elif Toksoy (eds), *Bilkent Üniversitesi Hukuk Fakültesi IV. Genç Hukukçu Araştırmacılar Sempozyumu 20-21 Nisan 2024 Çevrim İçi* (On İki Levha Yayıncılık 2024) 45

İçer Z and Dönmez E, ‘Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları’ (2020) 15 [43] Ceza Hukuku Dergisi 421

Jasserand-Breeman C, ‘Reprocessing of biometric data for law enforcement purposes: Individuals’ safeguards caught at the Interface between the GDPR and the ‘Police’ directive?’ (PhD thesis, University of Groningen 2019) <<https://research.rug.nl/en/publications/reprocessing-of-biometric-data-for-law-enforcement-purposes-indiv>> erişildi 4 Şubat 2025

Ketizmen M and Kart A, ‘Kişisel Verilerin Korunması Kanunu’nun 17. Maddesi ve Yargıtay Kararları Doğrultusunda, Kişisel Verilerin Korunmasına İlişkin Suç Teşkil Eden Fiiller Açısından Uygulanacak Norm Hakkında Değerlendirme’ (2021) 1 [2] Kırıkkale Hukuk Mecmuası 256

Kindt EJ, *Privacy and Data Protection Issues of Biometric Applications A Comparative Legal Analysis*, (Springer 2013)

Kişisel Verileri Koruma Kurumu, *Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber* <<https://www.kvkk.gov.tr/Icerik/2030/Rehberler>> erişildi 24 Ocak 2025

Mozur P, ‘One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority’ *The New York Times* (New York, 14 April 2019) <www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> erişildi 12 Şubat 2025

National Science and Technology Council, *Biometrics History* (2006) <<https://www.hsd.org/c/view?docid=463907>> erişildi 24 Ocak 2025

Özar S, ‘Adli ve İdari Kolluk Sınırları Bakımından Fizik Kimliğin Tespiti İşleminde Kişisel Veriler’ (2023) 81 [3] Ankara Barosu Dergisi 263

Öztürk B, Tezcan D, Erdem MR, Gezer ÖS, Saygılar YF, Çalışkan EA, Alan E, Özaydın Ö, Tütüncü EE, Güzel İ, Seyhan S, Köker N and Tok MC, *Dijital Ceza Muhakemesi Hukuku* (3rd edn, Seçkin Yayıncılık 2024)

Parliamentary Assembly of the Council of Europe, *Declaration on mass communication media and Human Rights* (Resolution 428, 1970) <<https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en>> erişildi 14 Şubat 2025

Ringelheim, J, ‘Processing Data on Racial or Ethnic Origin for Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?’ (2007) Center for Human Rights and Global Justice Working Paper No. 13 Jean Monnet Working Paper 08/06, <<https://jeanmonnetprogram.org/>> erişildi 15 Ocak 2025

Rouvroy A and Poulet Y, ‘The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy’ in Serge Gutwirth, Yves Poulet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds), *Reinventing Data Protection?* (Springer 2009) 45

Smith M and Miller S, ‘The ethical application of biometric facial recognition technology’ (2022) 37 AI & SOCIETY 167

Sprenger J and Brodowski D, ‘Predictive Policing’, ‘Predictive Justice’, and the use of ‘Artificial Intelligence’ in the Administration of Criminal Justice in



Germany’ (2023) *Revue Internationale de Droit Pénal* 5 <<https://www.penal.org/de/2023-2>> erişildi 11 Haziran 2025

Şıracı S, ‘Yüz Tanıma Teknolojilerinin Kişisel Verilerin Korunması Hukuku Açısından İncelenmesi’ (2023) 5 [1] *Kişisel Verileri Koruma Dergisi* 23

Tahmazoğlu Üzeltürk S, ‘Özel Hayatın Korunmasına İlişkin Başlıca Sorunlar’ (2008) 1 *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi* 95

The European Commission, *Summary Report of the project “Towards the European Level Exchange of Facial Images”* <<https://www.telefi-project.eu/telefi-project/results>> erişildi 26 Kasım 2024

The European Commission, *Support to the project ‘Towards the European Level Exchange of Facial Images’* <<https://www.politico.eu/wp-content/uploads/2020/03/TELEFI-Project.pdf>> erişildi 16 Mart 2025

The European Commission, *Towards the European Level Exchange of Facial Images Legal Analysis for TELEFI project* <<https://www.telefi-project.eu/telefi-project/results>> erişildi 5 Şubat 2025

Tilstone WJ, ‘Scientific Basis of the Forensic Process’ in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer Science Business Media 2014) 4672

United Nations Human Rights Council, *Surveillance and human rights Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/41/35, 28 May 2019) <ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35> erişildi 12 Şubat 2025

Veale M, *Algorithms in the Criminal Justice System* (June 2019) <<https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report>> erişildi 20.01.2025

Warren SD and Brandeis LD, ‘The Right to Privacy’ (1890) 4 [5] *Harvard Law Review* 193

Weissbrodt D, ‘The Administration of Justice and Human Rights’ (2009) 1 *City University of Hong Kong Law Review* 23

Zalnieriute M, ‘Glukhin v. Russia. App. No. 11519/20. Judgment’ (2023) 117 [4] *American Journal of International Law* 695

Avrupa İnsan Hakları Mahkemesi Kararları

Amann v İsviçre App no 27798/95 (ECtHR, 16 Şubat 2000)

Aycaguer v Fransa App no 8806/12 (ECtHR, 22 Haziran 2017)

Benedik v Slovenya App no 62357/14 (ECtHR, 24 Nisan 2018)



- Delcourt v Belçika* App no 2689/65 (ECtHR, 17 January 1970)
- Gaughran v Birleşik Krallık* App no 45245/15 (ECtHR, 13 Şubat 2020)
- Glukhin v Rusya* App no 11519/20 (ECtHR, 4 Temmuz 2023)
- Leander v İsveç* App no 9248/81 (ECtHR, 26 Mart 1987)
- Lupker ve Diğerleri v Hollanda* App No 18395/91 (ECtHR, 7 Aralık 1992)
- M.K. v Fransa* App no 19522/09 (ECtHR, 18 Nisan 2013)
- P.G. ve J.H. v Birleşik Krallık* App no 44787/98 (ECtHR, 25 Eylül 2001)
- P.N. v Almanya* App no 74440/17 (ECtHR, 11 Haziran 2020)
- Peck v Birleşik Krallık* App no 44647/98 (ECtHR, 28 Ocak 2003)
- Perry v Birleşik Krallık* App no 63737/00 (ECtHR, 17 Temmuz 2003)
- Peruzzo ve Mertens v Almanya* App nos 7841/08 ve 57900/12 (ECtHR, 4 Haziran 2013)
- Rotaru v Romanya* App no 28341/95 (ECtHR, 4 Mayıs 2000)
- S. ve Marper v Birleşik Krallık* App nos 30562/04 ve 30566/04 (ECtHR, 4 Aralık 2008)
- Satakunnan Markkinapörssi Oy ve Satamedia Oy v Finlandiya* App no 931/13 (ECtHR, 27 Haziran 2017)
- Sciacca v İtalya* App no 50774/99 (ECtHR, 11 Ocak 2005)
- Uzun v Almanya* App no 35623/05 (ECtHR, 2 Eylül 2010)
- Van der Velden v Hollanda* App no 29514/05 (ECtHR, 7 Aralık 2006)

