Araştırma Makalesi | **Research Article** **ÇÜHAD 2022/1** | **e-ISSN:** 2822-4809

BİYOMETRİK VERİLERİN İŞLENMESİNİN YARGI KARARLARI IŞIĞINDA DEĞERLENDİRİLMESİ•

Evaluation of the Processing of Biometric Data in the Light of Judicial Decisions

Miray ÖZER DENİZ*

M. Turan ÖZER**

ÖZ

Bir kişi ile ilişki kurulabilmesini sağlayan her türlü veri, kişisel veridir. Biyometrik veriler, kanunda tanımı yapılmamakla birlikte, parmak izi, avuç içi, iris, yüz taraması gibi fizyolojik veya adım atma, kalem tutma gibi davranışsal belli bir kişi ile ilişki kurabilen verilerdir. Kişisel Verilerin Korunması Kanunu (KVKK) 6. maddesinde özel nitelikli veri olarak kabul edilmiştir. Biyometrik veriler, kişinin kimliğinin belirlenmesi imkânı veren ve kopyalanma ya da taklit edilmesine müsaade etmediğinden, gizlilik, güvenlik veya kontrol gereken yerlerin girişlerinde kullanılmaktadır. Son dönemde, çalışanların mesai saatlerine riayet etmesini ve kontrolünü sağlamak adına, teknolojinin gelişmesiyle birlikte parmak izi ile giriş sağlayan sistemlerin uygulanması yaygınlaşmıştır. Bununla birlikte, parmak izini kaydeden uygulamaların kişilik hakkını ve özel hayatın gizliliği kuralını ihlal ettiği bahsiyle uygulamaların iptaline yönelik yargıya başvurular da artmıştır. Çalışmamızda, biyometrik verilerin tanımı ve işlenme usulleri ile konuya ilişkin Anayasa Mahkemesi, Danıştay ve Kişisel Verileri Koruma Kurulu'nun verdiği kararlar değerlendirilecektir.

Anahtar Kelimeler: Kişisel Veri, Biyometrik Veri, Parmak İzi, Kişisel Verilerin İşlenmesi.

• **Gönderi**: 27.04.2022 - **Kabul**: 24.05.2022 | **Received**: 27.04.2022 - **Accepted**: 24.05.2022.

* Arş. Gör. Dr., Çukurova Üniversitesi Hukuk Fakültesi Medeni Hukuk Anabilim Dalı, Adana, Türkiye ✉ mdeniz@cu.edu.tr • ORCİD 0000-0003-2443-6290.

** LLM., Avukat ve Arabulucu, Adana Barosu, Adana, Türkiye ✉ turan@turanozer.av.tr • ORCİD 0000-0001-9715-0037.

Atıf Şekli / **Cite As**: ÖZER DENİZ, Miray, ÖZER, M. Turan (2022). Biyometrik Verilerin İşlenmesinin Yargı Kararları Işığında Değerlendirilmesi. ÇÜHAD, (1), 92-110.

İntihal / **Plagiarism**: Bu makale bir intihal engelleme yazılımı aracılığıyla denetlenmiş ve en az iki hakem incelemesinden geçmiştir. / This article has been checked via a plagiarism prevention software and reviewed by at least two referees.

ABSTRACT

Any data that enables a person to be related is personal data. Biometric data can relate to a certain person physiologically such as fingerprint, palm, iris, face scanning or behavioral such as stepping and holding a pencil. It is accepted as special quality data in Article 6 of the Personal Data Protection Law (KVKK). Biometric data is preferrable at the entrances of places where privacy, security or control is required, as it allows to identify the person and can not be copyied or imitated. Recently, with the development of technology, the application of systems that provide fingerprint access has become widespread in order to ensure that employees comply with and control working hours. In addition, applications to the judiciary for the annulment of the applications have increased with the mention that the applications that record fingerprints violate the right to privacy and the rule of privacy. In our study, the definition and processing methods of biometric data and the decisions made by the Constitutional Court, the Council of State and the Personal Data Protection Authority will be evaluated.

Keywords: Personal Data, Biometric Data, Fingerprints, The Process of Personal Data.

I. BİYOMETRİK VERİLERİN TANIMI

Kişisel veri, belirli veya belirlenebilir bir kişiye ilişkin bütün bilgileri ifade eder. Bu kapsamda, kişinin adı, doğum tarihi, iletişim bilgileri, sosyal güvenlik ya da kimlik numarası, IP adresi, fotoğrafı, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgileri, alışveriş alışkanlıkları kişisel veridir[1]. Kişisel veriler, genel ve özel olmak üzere ikiye ayrılmaktadır. Özel nitelikli kişisel veriler, KVKK m. 6'da "*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler*" olarak belirlenmiştir. Bu veriler tahdidi olarak sayılmıştır ve yorum yoluyla genişletilemezler.

Çalışmamızın esasını oluşturan biyometrik verinin tanımı KVKK'da yapılmamıştır. Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliği'ne göre, biyometrik veri *"Elektronik sistemler*

[1] Y. 12 CD. T: 19.1.2015 E. 2014/11621 K. 2015/568; Y. 12 CD. T: 12.1.2015 E. 2014/11879 K. 2015/22; Y. 12 CD. T: 12.01.2015 E. 2014/9544 K. 2015/46, Y. 12 CD. T: 10.06.2013 E. 2013/10672 K. 2013/15772, Y. 12 CD. T: 09.06.2013 E. 2013/30385 K. 2013/14157; AYM E. 2013/122 K. 2014/74; AYM E. 2014/ 149 K. 2014/151 T: 09.04.2014; AYM T: 04.12.2014 E. 2013/84 K. 2014/183; AYM T: 25.12.2014 E. 2014/74 K. 2014/201; AYM T: 19.03.2015 E. 2014/180 K. 2015/30, kazanci.com.tr, (ET: 27.04.2022).

aracılığı ile kimlik tespiti ve kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla alınan kişiye özgü verileri" ifade eder[2].

KVKK yürürlüğe girmeden önce, Danıştay bir kararında biyometrik yöntemleri, *"ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği belirtilerek, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemler"* olarak tanımlamıştır[3]. AYM ise bir kararında *"Biyometrik yöntemlerle kimlik doğrulama, hizmet talep eden bir kullanıcının, ölçülebilir fizyolojik ve bireysel özellikler yoluyla gerçekleştirilen ve otomatik olarak doğrulanabilen kimlik denetleme yoluyla gerçek kullanıcı olup olmadığının doğrulanması anlamına gelmektedir."* şeklinde tanımlanmıştır[4].

Biyometrik veri, Avrupa Birliği Veri Koruma Tüzüğü'nde (GDPR), *"Yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler"* olarak tanımlanmıştır.

Biyometrik veriler, kişiye özgü ve kişiyi ayırt edecek verilerdir. Biyometrik veriler, fizyolojik nitelikli biyometrik veriler ve davranışsal nitelikli biyometrik veriler olarak ikiye ayrılır[5]. Fizyolojik nitelikli biyometrik verilere örnek olarak el izi, avuç izi, damar şekli, kulak ve yüz şekli, ısı dağılımı verilebilir[6]. Davranışsal nitelikli biyometrik veriler ise yürüyüş şekli, parmakları kullanma şekli, araba kullanma şekli, yazı yazma ve kalem tutma şekli gibi kişiyi davranışlarını icra etme biçimine göre ayırt eden biyometrik verilerdir[7].

Çoğu biyometrik veri, kişiyi tanımlayabilmesinin yanında, kişiye ait diğer bilgilere ulaşılabilmesini sağlar. Örneğin, parmak izinden kişinin etnik kökeni ve hastalıkları gibi diğer verilere de erişilebilmektedir[8]. Dolayısıyla, biyometrik veriler, sadece kişinin parmak izi,

---

2 RG, T: 03.12.2019 ve No: 30967.

3 Danıştay 15. HD. E. 2014/4562, https://www.kvkk.gov.tr/Icerik/7047/Biyometrik-Verilerin-Islenmesinde-Dikkat-Edilmesi-Gereken-Hususlara-Iliskin-Rehber, (ET: 27.04.2022).

4 AYM T: 19.3.2015 E. 2014/108 K. 2015/30, https://www.anayasa.gov.tr/, (ET: 27.04.2022).

5 Opinion 3/2012 On Developments In Biometric Technologies, Artıcle 29 Data Protection Working Party, 00720/12/EN WP193, s. 4.

6 ERARSLAN TÜRKMEN, s. 67; AKGÜL, s. 202; ERDİNÇ, s. 3.

7 https://www.kvkk.gov.tr/Icerik/7047/Biyometrik-Verilerin-Islenmesinde-Dikkat-Edilmesi-Gereken-Hususlara-Iliskin-Rehber, s. 5, (ET: 27.04.2022).

8 JASSERAND, s. 306-308.

görüntüsü, sesi gibi verilerinin yanında sağlık ve genetik verileri hakkında bilgi sağladığı için özel nitelikli veri olarak korunmalıdır.

Biyometrik veriler, kişiye özgü olup kesin, değişmeyen ve kaybolmayan daktiloskopik verilerdir[9]. Bu nedenle, biyometrik verilerden parmak izi, avuç izi, damar izi, retina taramasına çoğunlukla yüksek güvenlik gerektiren ve mutlak suretle kişinin doğru tanımlanmasını gerektiren yerlerde başvurulmaktadır. Özel laboratuvarlar, hapishane, askeri alanlar gibi yerlerde parmak izi, avuç veya damar izi kullanılarak giriş yapılmasına rastlanmaktadır[10]. Bunun yanında, çağrı merkezleri ile yapılan telefon görüşmelerinde, kalite standartları ve muhtemel bir uyuşmazlıkta ispat amaçlı ses kaydı yapılmaktadır. Kalabalık ve değerli ürünlerin olduğu mağazalarda ya da işyerlerinde görüntü kaydı yapılmaktadır. Günlük hayatın içinde ise daha çok ses ve görüntü kaydı gibi biyometrik verilerin kullanılmasına rastlanmaktadır.

Biyometrik veriler, kimlik kontrolünü sağladığı için uluslararası alanda da kullanılmaktadır. Çoğu devlet, uluslararası alanda özellikle güvenliği sağlamak adına biyometrik fotoğraf ve parmak izini kullanmaktadır. Örneğin suç, kaçakçılık ve yasa dışı göçmenlik gibi faaliyetlerinin önüne geçilmesi amacıyla imzalanan Prüm anlaşması, taraf devletler[11] arasında vatandaşların parmak izi ve DNA verilerinin sözleşmeye taraf diğer ülkeler ile paylaşılmasına izin vermektedir[12].

Benzer amaçla, Avrupa Birliğinde "*Secure Trans European Services For Telematics Between Administrations*" (eTESTA) kurulmuştur. Bu platform, Avrupa'daki ülkeler arasında DNA ve parmak izi gibi verilerin paylaşılmasını sağlamaktadır. Böylece, üye devletin birinde işlenen suçun failinin, serbest dolaşım hakkını kullanarak diğer Avrupa Birliği içindeki üye devletlere kaçması önlenmeye çalışılmaktadır.

---

9 AKGÜL, s. 202; Ayrıca bknz. "*Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi*" ile ilgili olarak Kişisel Verileri Koruma Kurulunun 27.08.2020 tarihli ve 2020/649 sayılı karar özeti, https://www.kvkk.gov.tr/Icerik/6815/2020-649, (ET: 27.04.2022).

10 Biyometrik yöntemlerin suçlunun teşhisinde kullanılması 1870'lere kadar dayanır. İlk defa Alphonse Bertiillon tarafından kullanılmış ve kişilerin kafatası, kol ve ayak ölçülerinden yararlanılarak kimlik tespiti yapılmıştır. 1980'lerde yüz tanıma ve 90'larda ise iris tanıma özelliği ile gelişmiştir. AKGÜL, s. 200.

11 Belçika, Almanya, İspanya, Fransa, Lüksemburg, Hollanda ve Avusturya'nın imzaladığı Prüm Antlaşmasıyla, bu ülkeler suç, kaçakçılık ve yasadışı göçmenlik gibi faaliyetlerinin önüne geçilmesi için birbirleriyle DNA paylaşma konusunda işbirliği yapar. https://ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/prumtr.pdf., (ET: 27.04.2022).

12 https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/governance-and-decision-making/mopac-decisions-0/exchange-biometric-data-across-europe-prum-arrangements, (ET: 27.04.2022).

II. BİYOMETRİK VERİLERİN İŞLENMESİ

Bir verinin elde edilme aşamasından silinme ya da yok etme aşamasına kadar geçen süredeki her türlü faaliyet, işleme faaliyeti olacaktır. Zira kişisel verilerin işlenmesi, KVKK'da m. 3'te, *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması[13], devralınması, elde edilebilir hâle getirilmesi[14], sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi*" olarak tanımlanmıştır[15].

Kişisel veriler, KVKK m.5 ve m. 6 uyarınca, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Açık rıza, Kurum tarafından *"Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza."* şeklinde tanımlanmıştır[16]. Geçerli bir açık rıza için, ilgili kişinin işleme faaliyeti ve bunun sonuçları hakkında aydınlatılmış olması ve bu aydınlatma üzerine ilgili kişinin özgür ve bilinçli iradesiyle rıza göstermesi gerekir[17]. Bir başka ifadeyle geçerli bir rıza beyanını üç unsuru vardır. Bunlar, belirli bir konu ile ilgili olması, bilgilendirmeye dayanması ve özgür iradeyle açıklanmasıdır[18].

Belirli bir konuya ilişkin olma, veri sorumlusunun veri işleme amacının net bir şekilde ifade edilmesini ifade eder. Veri sorumlusunun, veri işleme amacını net ve sınırları çizilmiş olarak ilgili kişiye açıklaması gerekir[19]. Sınırları belli olmayan ve genel ifadeli bilgilendirme metinleri ve açık rıza beyanları geçersiz olacaktır. Bu kapsamda, ilgili kişinin "*Kişisel*

---

13 Aktarma işlemi, kişisel verilerin işlenmesinin bir türü olmasına rağmen Kanun'da özel olarak düzenlenmiştir. Hatta madde olarak Kanun'da yer almasının yanında, verilerin aktarılması için Kurum'un özel izninin alınması gerekmektedir. Bunun nedeni, aktarma fiiliyle kişisel verilerin çok daha geniş çapta yayılması, ilgili kişinin kontrolünden çıkması, özellikle yurtdışı aktarımlarında verilerin transfer edileceği ülkenin kişisel verileri koruma hukukunun kapsamının bilinmemesi ve buna bağlı olarak kişisel verilerin daha çok korunmaya ihtiyaç duyulması olduğu söylenebilir. ALTINOK ÇALIŞKAN, ÖZTÜRK, s. 315.

14 Bu kapsamda, arama motorlarında kişisel bilgilerin motor sağlayıcıları tarafından kullanıcılara iletilmesi de işleme faaliyetidir. https://www.kvkk.gov.tr/Icerik/6777/Kisilerin-Ad-ve-Soyadi-ile-Arama-Motorlari-Uzerinden-Yapilan-Aramalarda-Cikan-Sonuclarin-Indeksten-Cikarilmasina-Yonelik-Talepler-Hakkinda-Kamuoyu-Duyurusu, kvkk.gov.tr, (ET: 01.08.2020).

15 Kişisel Verilerin İşlenme Şartları, Kişisel Verileri Koruma Kurumu, s. 1.

16 Madde Ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, KVKK Yayınları, Ankara, Mart 2019, s. 103.

17 KAYA, s. 326; RINGELHEIM, s. 63.

18 Açık Rıza, KVKK Rehber Kitapçığı, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf, (ET: 27.04.2022).

19 BRINK, WOLFF, s. 2.

verilerimin işlenmesini kabul ediyorum." şeklindeki beyanı açık rıza olarak değerlendirilmeyecektir[20].

Bilgilendirilmeye dayanması ise veri sorumlusunun aydınlatma yükümlülüğü ile paralel olarak, ilgili kişinin veri işleme amaçları ve yöntemleri hakkında bilgilendirilmesidir. İlgili kişinin bilgilendirilmesi, KVKK m. 10 ve 11'e paralel olmalıdır. Bu kapsamda, ilgili kişi, veri sorumlusunun kimliği, verilen işlenmesi ile hedeflenen amacı[21], veri alıcılarının kimliğini[22], kendisinin verileri düzeltme ve veriler hakkında bilgi alma hakkının bulunduğu konularında bilgilendirilmelidir.

İlgili kişi, bunların yanında, verilerin korunmasına ilişkin ne tür güvenlik önlemleri alındığını, verilerin kimlerle ve ne amaçla paylaşılacağını, veri sorumlusunun kişisel verileri işleme amacıyla alakalı olup olmadığı ve vereceği rızanın hukuki sonuçları hakkında bilgi sahibi olmalıdır[23]. Bilgilendirme, yalnızca açık rızanın geçerliliği için değil kişinin düzeltilme, silme veya itiraz hakları gibi bağlantılı diğer haklarının kullanımı için de gereklidir[24]. İlgili kişinin tüm verilerinin, her türlü amaç için işlenmesine vereceği rıza, hukuka uygunluk sağlamayacaktır[25].

Açık rızanın özgür irade ile verilmesi gerekir. Bu kapsamda, kişinin iradesi hata, hile ve tehdit ile sakatlanmamalıdır. Ayrıca, uygulamada sıkça karşılaşıldığı üzere, açık rıza, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olmamalıdır. Özgür irade ile açık rızanın verilmesi hususu, özellikle işçi-işveren arasındaki ilişkilerde titizlikle değerlendirilmelidir. İşverenin, açık rıza alınmasını hizmet akdinin bir parçası olarak ileri sürmesi halinde, işçinin kişisel verilerinin işlenmesine yönelik açık rızasının özgür iradeyle vermiş olması şüpheli hale gelecektir.

---

20 Açık Rıza, s. 4.

21 *"İlgili kişinin yaptığı başvuruyu cevaplandırmayan ve internet sitesi üzerinden yayımladığı aydınlatma metni mevzuatta düzenlenen şartları taşımayan T.C. Ziraat Bankası A.Ş. hakkında"* Kişisel Verileri Koruma Kurulunun 02.05.2019 tarihli ve 2019/122 sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/5461/2019/122, (ET: 27.04.2022).

22 Özellikle kişisel verilerin yurtdışına aktarımı ve paylaşımı söz konusu olduğunda, anılan verilerin nereye, kimlere ve neden aktarılacağının özellikli olarak belirtilmesi gerekir. Aynı görüşte bknz. BRAUN, s. 25.

23 CUSTERS, VAN DER HOLF, SCHERMER, APPLEBY-ARNOLD, BROCKDORFF, s. 445; Article 29 Working Party Guidelines on consent under Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=62305, (ET: 27.04.2022).

24 BOROCZ, s. 470; AYDIN, s. 117; BU-PASHA, ALEN-SAVIKKO, MAKINEN, GUINNES, KORPISAARI, s. 320.

25 DÜLGER, s. 24; KÜZECİ, s. 241; DEVELİOĞLU. Ayrıca, Kurum kararı için bknz. https://kvkk.gov.tr/Icerik/6913/2020-404, (ET: 27.04.2022).

Kanun koyucu hem genel hem de özel nitelikli kişisel verilerin hukuka uygun olarak işlenmesinde aranan açık rıza bakımından aynı koşulları aramaktadır[26]. Öncelikle, özel nitelikli kişisel verilerin hukuka uygunluk nedenlerinin yanında genel nitelikli kişisel veriler için hukuka uygunluk nedenlerinin varlığının gerekip gerekmediği belirlenmelidir. Özel nitelikli kişisel verilerin hassasiyeti düşünüldüğünde, bu veriler için gerekli olan hukuka uygunluk nedenlerinin yanında genel nitelikli kişisel veriler için gerekli olan hukuka uygunluk nedeninin de varlığı aranmalıdır[27].

Açık rıza alındıktan sonra işleme amacının değişmesi halinde, veri sorumlusu veya ilgilisinin yeni konu sınırı ile ilgili tekrar rıza alması gerekir[28]. Aksi halde, değişen konu ile ilgili işleme yapılması hukuka aykırı olacaktır. Bunun yanında, açık rızanın verildiği konudan başka bir konu ile ilgili işleme faaliyetleri yapılması da hukuka uygun olmayacaktır. Örneğin, Kişisel Verileri Koruma Kurumu'nun önüne gelen bir olayda, ilgili kişi veri sorumlusuna belli bir amaç için kişisel verilerini işleme izni vermiş iken başka bir amaçla verilerinin işlendiğini öğrenmiştir. Kurul bu olayda, veri sorumlusunun KVKK m. 4'teki işleme ilkelerine, KVKK Geçiş Hükümlerinden 1. maddesine uygun davranmadığına karar vererek veri sorumlusu hakkında KVKK m. 18 uyarınca idari para cezası verilmesine karar vermiştir[29].

KVKK m. 6'ya göre, sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Ayrıca, bu verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır. Ayrıca, biyometrik verilerin işlenmesinde, biyometrik veri işleme şartlarının mevcudiyeti ve Kanunun 4 üncü maddesinde düzenlenen genel ilkelere riayet edilmesi önem arz etmektedir. Kanunun 6 ncı maddesinin üçüncü fıkrasına göre, sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Bu çerçevede, biyometrik veriler açık rıza yoksa kanunlarda öngörülen hallerde işlenecektir. Anılan Kanun hükmünden de anlaşılacağı üzere, başka kanunlarda biyometrik verilerin işlenmesine dair hükümlerin açıkça yer alması durumunda ilgili kanunlarda yer alan hükümler uygulanacaktır.

Biyometrik verilerin işlenmesine ilişkin kanuni düzenlemelerin birisi, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'dur. Bu Kanun'un 67. maddesinde, sağlık hizmetlerinden yararlanmak amacıyla biyometrik verinin alınmasına ilişkin düzenleme yer

---

26 Aynı şekilde bknz. BRAUN, s. 30; ERARSLAN TÜRKMEN, s. 124.

27 YÜCEDAĞ, s. 772.

28 DÜLGER, s. 24; Article 29 Working Party Guidelines on consent under Regulation 2016/679.

29 https://www.kvkk.gov.tr/Icerik/5423/2018-131, (ET: 27.04.2022).

almaktadır. Ayrıca, 5490 sayılı Nüfus Hizmetleri Kanunu'nun 7. maddesinde, aile kütüklerinde biyometrik veri bilgisinin de bulunduğu düzenleme yer almaktadır. Bunun yanında, Polis Vazife ve Salâhiyet Nizamnamesi m. 5'e göre, yetkili memurların gerekli görmesi halinde parmak izi ve fotoğraf alınabileceğini belirtmiştir. Anılan bu madde, biyometrik veri niteliğindeki parmak izi ve fotoğrafların polisler tarafından işlenmesinde kanuni dayanak oluşturmaktadır[30].

Biyometrik veriler, Covid-19 pandemi sürecinde uzaktan iletişim, öğrencilere eğitim verilmesi, iş ve sosyal amaçlı toplantı yapılması amacıyla, internet aracılığıyla iletişim sağlayan *Zoom, Teams ve House Party* gibi uygulamalarda sıkça kullanılmıştır. Uzaktan iletişim sağlayan uygulamalar, gerek kullanım şartı gerekse kullanıcı politikası olarak kullanıcıların ses ve görüntülerini kaydetmektedir. Hatta, biyometrik verilerin yanı sıra, kullanıcıların isim, elektronik posta, telefon numarası, konum bilgisi gibi diğer kişisel verilerini de işlemektedir.

Söz konusu bu uygulamalar, hayatı kolaylaştırmakla birlikte kişisel verilerin korunması noktasında soru işaretleri yaratmaktadır. Bunun birinci nedeni, uygulamalar vasıtasıyla elde edilen veriler, uygulama merkezlerinin yurtdışı olması sebebiyle, yurtdışına aktarılmaktadır. Yurtdışına aktarım ise KVKK'na göre ancak ilgili kişinin açık rızasıyla geçerlidir. Ne var ki uygulamada bu rızanın geçerliliği gerektiği gibi sağlanamamaktadır.

Ayrıca, iş hayatında bu uygulamaların kullanılmasında ise çalışanların rızalarının irade beyanlarına dayanıp dayanmadığı noktası değerlendirilmelidir. Zoom uygulaması üzerinden toplantı yapan bir şirkette çalışan kişinin, uygulamanın biyometrik verilerini işlemesine rıza göstermemesi aynı zamanda iş akdini gereği gibi ifa etmemesine de yol açacaktır. Bunun gibi, uzaktan eğitim veren eğitim kurumunda çalışan öğretmen bu uygulamaları kullanmaya rıza göstermemesi işini kaybetmesine neden olabilir. Dolayısıyla, işçi-işveren uyuşmazlıkların geçerli rıza beyanı için gerekli özgür irade koşulu, biyometrik verilerin işlenmesi noktasında da oldukça tartışmalı olmaktadır.

Kişisel Veriler Koruma Kurumu, anılan uygulamaların kullanımına ilişkin internet sitesinde bir kamuoyu duyurusu yayınlamıştır. Bu duyuruda, bu uygulama ve platformları kullanan veri sorumlularının Kurul tarafından hazırlanan *"Kişisel Veri Güvenliği Rehberi (İdari ve Teknik Tedbirler) ile Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı*

30 ATLI, s. 12.

"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" Kararı dikkate almaları gerektiğini belirtmiştir[31].

III. BİYOMETRİK VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER

Kişisel verilerin düzenlendiği her hukuk sisteminde, verilerin işlenmesine ilişkin ilkeler belirlenmiştir. Mehaz alınan 95/46/EC Yönergesinde ve Tüzükte bu ilkeler tek tek sayılmıştır. KVKK'nda ise m. 4'te *"Genel İlkeler"* başlığında Türk hukukunda kişisel verilerin işlenmesine ilişkin ilkeler düzenlenmiştir. Bu ilkeler belirlenirken çoğunlukla 108 No'lu Sözleşme ile ilkeler esas alınmıştır.

İlkeler, işleme faaliyetlerinin olabildiğince hukuka uygun, şeffaf, ilgili kişinin haklarını korumaya yönelik düzenlenmiştir. İlkelerin amacına ulaşabilmesi için bu ilkelere veri işlenme faaliyetlerinin her aşamasında riayet edilmelidir[32].

KVKK m. 4, "*Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur;*

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." şeklinde düzenlenmiştir.

İlk ilke olan hukuka ve dürüstlük kuralına uygun olma, diğer ilkelerin esasını oluşturan ve onlara kaynaklık eden bir ilkedir[33]. TMK m. 2 gibi genel hukuk normları ile konuyla ilgili olan tüm yasalara uygun olmayı amaçlamaktadır[34]. Bu ilkeye göre, işlenen tüm veriler, genel hukuk normları ve ilgili yasal düzenlemelere uygun olmalıdır[35]. Dürüstlük kuralına *(fair)* uygun olma ise veri işleme sırasında, ilgili kişinin menfaatleri de dikkate alınmasını ifade eder[36]. Örneğin, veri işleme faaliyetinin ilgili kişiye başka hiçbir seçenek olmadan sunulması, açık

31 https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu, (ET: 27.04.2022).

32 Opinion 3/2012 On Developments In Biometric Technologies, Artıcle 29 Data Protectıon Workıng Party, 00720/12/EN WP193, s. 7.

33 KÜZECİ, s. 208; DÜLGER, s. 109.

34 DÜLGER, s. 110; KÜZECİ, s. 206.

35 Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, Kişisel Verileri Koruma Kurulu, s. 4.

36 BYGRAVE, s. 263, https://doi.org/10.1093/ijlit/6.3.247, (ET: 03.11.2020); KÜZECİ, s. 206; DÜLGER, s. 111.

rızanın bir ön şart olarak ileri sürülmesi ya da işlemeye ilişkin aydınlatma yükümlülüğün hiç, gereği gibi ya da açık rıza sonrasında yerine getirilmesi dürüstlük kuralına aykırılık teşkil eder.

İkinci olarak, doğru ve güncel olma ilkesi, veri işleme faaliyetleri süresince, verilerin doğru ve güncel olmasını ifade eder. Veriler, elde edilme aşamasından başlayarak tüm aşamalarda doğru olmalıdır. Nitekim yanlış veriler, hem ilgili kişi hem de veri sorumlusunun menfaatlerini zedeleyebilir. Bunu önlemek adına, veri sorumlusunun, verileri doğru ve güncel tutmayı sağlayacak önlemler alması gerekir[37].

Üçüncü olarak, verilerin belirli, açık ve meşru amaçlar için işlenmesi gerekir. Veri işleme faaliyetinin belirli olması, veri işleme amacını açık ve kesin olarak belirlemesi anlamına gelmektedir[38]. Böylece, ilgili kişi, sınırları önceden belirlenmiş işleme faaliyetlerine rıza gösterir. Zira aksi halde, işleme faaliyetlerinin belirli olmaması, ilgili kişinin neye rıza gösterdiğinin belli olmaması ve veri sorumlusunun keyfi işlemelerine zemin hazırlar.

Ayrıca, veri işleme faaliyetlerinin meşru amaca dayanması gerekir. Kişisel verilerin işlenmesi Anayasal bir hak olarak yalnızca meşru amaçlar için işlenmelidir. Böylece, keyfi veya kanun dışı veri işlemeler önlenebilir. Örneğin, 5271 sayılı CMK'nın 80/1'e göre, "*75, 76 ve 78'inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçlan, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz*". Bu düzenleme, veri işleme amacın sınırının belli olması ilkesine uygun bir düzenlemedir[39]. Bu konuda AYM, gerçek ve tüzel kişilerin trafik bilgisinin Telekomünikasyon İletişim Başkanlığı tarafından herhangi bir gerekçe göstermeksizin elde etmesine imkân veren düzenlemeyi, meşru dayanağı olmamasından dolayı iptaline karar vermiştir[40]. Aşağıda incelenecek yargı kararlarında da meşruiyet ekseninde değerlendirilmiştir.

Dördüncü ilke, verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmasıdır. Bu kapsamda öncelikle, toplanan veri ile veri işleme amacının birbiriyle bağlantılı olmalıdır. Veri sorumlusunun, veri işleme amacına uygun veriler işlenmelidir. Örneğin, bir elektronik sisteme giriş için gerekli kimlik doğrulama verileri işlenmeli; alakası olmayan bir sağlık verisi işlenmemelidir.

---

37 Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, KVKK Yayınları, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf, s. 6.

38 Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 8.

39 Y. 17. Ceza Dairesi E. 2016/10020, K. 2016/11226.

40 AYM, T: 02.10.2014 E. 2014/149 K. 2014/15, RG, 01.01.2015, No: 29223.

Bu amaçla, verilerin elde edilme yöntemleri de değerlendirilmelidir. Örneğin, görüntü ve ses kaydı yapan cihazların işyeri içerisinde nasıl konumlandırılacağı hem veri işleme amacına uygunluk hem de dürüstlük kuralı çerçevesinde belirlenmelidir. Bir işyerinin, işçileri denetlemek amacıyla yerleştirdiği güvenlik kameralarının işyerinin kapısında ve umumi yerlerinde olması bu ilkelere uygun iken; soyunma odalarında veya tuvaletlerde olması bu ilkelere uygun olmayacaktır.

Önceden belirlenen veri işleme amacı içerisinde kalmak da söz konusu ilkenin gerekliliklerinden biridir. İşlenme amaçlarının değişmesi, hem verilen rızanın geçersizliğine hem de ilgili kişinin verilerinin korunmamasına neden olabilir. Örneğin, veri sorumlusunun yükümlülüklerini yerine getirmesi amacıyla işlenen verilerin daha sonra pazarlama ve reklam amacıyla işlenmesi, amacın dışına çıkmak olacaktır. Kişisel Verileri Koruma Kurumu, ilgili kişilerin verilerinin, veri sorumlusunun reklamının yapılması amacıyla kullanılmasını amaca aykırılık olarak değerlendirip, veri sorumlusu aleyhine idari para cezası hükmetmiştir[41].

Veri asgarileştirme *(The data minimisation principle)* ilkesi olarak da tanımlanabilecek ölçülülük ilkesine göre, veri sorumlusu, sadece işleme amacını gerçekleştirmeye yetecek kadar veri kullanmalıdır[42]. Bu kapsamda, veri işleme amacı ile ilgisi olmayan veriler işlenmemelidir. Ayrıca, amaca ulaşmayı sağlayan en az veriyi işlemelidir[43]. Örneğin, bir öğrencinin okul kaydı yapılırken anne ve babasının bilgileri alınabilir fakat ebeveynlerin parmak izinin de alınması amaç ile aykırı olacaktır. Aşağıda incelenecek Danıştay ve Anayasa Mahkemesi kararlarında olduğu gibi, kart okutma veya şifre kullanımının yeterli olduğu bir durumda, parmak izi verisi kullanılmamalıdır.

Son olarak veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. İşleme amacına ulaşıldıktan veya kanunda belirtilen süre sona erdikten sonra, veri sorumlusu artık verileri muhafaza etmemelidir[44].

41 https://www.kvkk.gov.tr/Icerik/6716/2020-58, (ET: 14.12.2020).

42 C-92/09 ve C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 Kasım 2010, parag. 89 ve 86.

43 DE HERT, PAPAKONSTANTİNOU, s. 179-194; TEKİN, s. 231; UYGUN, s. 55; SOLMAZ, s. 61–78.

44 Opinion 3/2012 On Developments In Biometric Technologies, Artıcle 29 Data Protection Working Party, 00720/12/EN WP193, s. 8.

IV. BİYOMETRİK VERİLERİN İŞLENMESİNE İLİŞKİN YARGI KARARLARI

A. İlgili Anayasa Mahkemesi Kararları

Anayasa Mahkemesinin biyometrik veriler ile ilgili olarak verdiği ilk karar, Sosyal Güvenlik Kurumu tarafından biyometrik kimlik doğrulama sisteminin zorunlu tutulmasına ilişkin kararın iptaline ilişkindir. Sağlık ve Sosyal Hizmet Emekçileri Sendikası'nın açtığı bu iptal davasında Danıştay 15. Dairesi, biyometrik kimlik doğrulama sisteminin özel hastanelere ilişkin kısmı hakkında yürütmeyi durdurma kararı vermiştir.

AYM, iptal başvurusu yapılan 5510 sayılı Kanun'un "*Sağlık Hizmetlerinden Yararlanma Şartları*" başlıklı 67. maddesini[45] *"Nitekim itiraz konusu kuralın gerekçesinde sağlık hizmetlerinin elektronik ortamda güvenilir altyapılar üzerinden sağlanması ve hizmetten yararlananların kimliklerinin saptanmasında geleneksel yöntemlerin eksiklikleri nedeniyle ortaya çıkan kötüye kullanımların önlenmesinin amaçlandığı belirtilmiştir. Dolayısıyla kuralla öngörülen yöntemin etkin bir şekilde kullanılmasının, Sosyal Güvenlik Kurumundan haksız menfaat temin edilmesini engellemeye yönelik olduğu ve kuralda kamu yararı bulunduğu açıktır. Bu bağlamda itiraz konusu kuralla özel hayatın ve kişisel verilerin korunması haklarına yönelik olarak yapılan müdahalenin, öngörülen amaçla orantılı olduğu, müdahale edilen hakların özüne dokunmadığı ve demokratik toplum düzeninin gereklerine aykırılık teşkil etmediği anlaşıldığından Anayasa'ya aykırı bir yönü yoktur."* gerekçeleriyle reddetmiştir.

Anayasa Mahkemesinin bir başka kararı 03/04/2015 tarihli Resmi Gazetede yayınlanmıştır. Bu karara konu olayda başvuru sahibi, mesai saatlerinin takibi amacıyla parmak izi kayıt sisteminin kullanılması ve bu vesileyle parmak izinin kaydedilmesinin, özel hayata saygı hakkı kapsamında kişisel verilerin ihlal edildiği iddiasında bulunmuştur. Başvurucunun devlet memuru olarak çalıştığı Belediye, parmak izi sistemi ile mesai takibine başlamıştır. Bu gerekçeyle, 13/4/2016'da tarihinde başvurucunun parmak izi sisteme kaydedilmiştir. Başvurucu, 15/4/2016 tarihinde Belediye'ye yazdığı dilekçe ile parmak izinin kaydedilmesi ve bu sistem ile mesai takibi yapılmasına itiraz etmiştir. İtiraz dilekçesinde, parmak izinin kişisel

[45] Dava konusu hüküm *"Ayrıca genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında acil haller hariç olmak üzere (acil hallerde ise acil halin sona ermesinden sonra); biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya Kurum tarafından verilen resimli sağlık kartı belgelerinden birinin gösterilmesi zorunludur."* şeklindedir.

veri olarak özel hayatın gizliliği kapsamında korunduğunu ve bu sistemin uygulanmasının kaldırılmasını talep etmiştir.

Belediye, başvurucunun dilekçesinde belirttiği talebi reddetmiştir. Bunun üzerine başvurucu, 27/6/2016'da Aydın 1. İdare Mahkemesinde başvuru konusu idari işlemin iptali talebiyle dava açmıştır. Bu davada davalı belediye, uygulanan sistemin 5393 sayılı Belediye Kanunu kapsamında belediye başkanının sevk ve idare yetkisi kapsamında çalışanların işyerine giriş ve çıkış saatlerinin takip edilmesi ve çalışanların kontrolü amacıyla diğer kurumlar tarafından da kullanıldığını; ayrıca bu sistemin özel hayata saygı hakkını ihlal etmediğini ifade etmiştir.

Başvurucu vekili cevap dilekçesinde, uygulanan sistemin parmak izini depoladığını, belediyenin bu depolanan parmak izlerinin güvenliği ve paylaşılmaması noktasında garanti veremediğini; ayrıca parmak izinin kaydedilmesi konusunda başvurucu dahil çalışanların rızasının alınmadığını ileri sürmüştür.

Neticede ise yerel mahkeme, 02.03.2017 tarihli kararında, davanın kabulü ile birlikte idari işlemin iptaline karar vermiştir. Yerel Mahkeme gerekçesinde, her ne kadar 657 sayılı Kanun'da memurların mesainin başlangıcı, devamı ve bitişine yönelik düzenleme olsa da bunların ayrıntılı olmadığını, uygulamadaki gibi temel hakların kısıtlanabilmesi için kanuni bir dayanak olması gerektiği halde, somut uyuşmazlıkta bu şekilde bir dayanak olmadığını belirtmiştir. Ayrıca, parmak izi ile mesai saati uygulamasını, özel yaşamın gizliliği kapsamında değerlendirmiştir.

Davalı Belediye, bu sistemin kart okuma sisteminden daha güvenilir olduğunu, başka kurumlar tarafından da kullanıldığını ve verilerin başka bir yerde kullanılmadığını belirterek istinaf yoluna başvurmuştur. İzmir Bölge İdare Mahkemesi 2. İdare Dava Dairesi 29.11.2017'de istinaf başvurusunu kabul ederek kesin olarak davanın reddine karar vermiştir.

Bunun üzerine başvurucu Anayasa Mahkemesi'ne bireysel başvuruda bulunmuştur. Anayasa Mahkemesi, önüne gelen olayı ilgili mevzuat ve yargı kararları açısından değerlendirdikten sonra, somut olayda başvurucunun kişisel verilerinin korunmasını isteme hakkının kabul edilebilir ve bu hakkın ihlal edilmiş olduğuna karar vermiştir.

B. İlgili Danıştay Kararı

Danıştay'ın biyometrik veriler hakkında verdiği kararlar, mesai saatlerinin kontrolünü sağlamak için parmak izi alınmasına ilişkindir[46]. Karara konu olayda, bir devlet hastanesi, çalışanların mesai saatlerine riayet edip etmediğini kontrol etmek amacıyla önce kart okutma sistemini uygulamış ancak bu yöntemin etkili olmadığı gerekçesiyle parmak izi okutma sistemine geçilmesine karar vermiştir[47]. Davacı işçi sendikasının, hastanenin parmak izi uygulamasını sonlandırması istemiyle açtığı davada yerel mahkeme, bu uygulamanın hukuka ve mevzuata aykırı olmadığı gerekçesiyle davanın reddine karar vermiştir.

Danıştay önüne gelen bu olayda[48], parmak izi tarama sistemi ile mesai takibi yapılmasının özel hayatın gizliliği ilkesi kapsamında değerlendirilmesi gerektiğini, hastanenin bu uygulamasının yasal bir dayanağı olmadığı gibi, elde edilen verilerin bir başka amaçla ve bir başka zamanda kullanılamayacağına dair bir güvence olmaması nedeniyle yerel mahkemenin kararını bozmuştur.

Yerel Mahkemenin direnmesi üzerine dava Danıştay İdari Dava Daireleri Kurulu önüne gelmiştir. Danıştay İdari Dava Daireleri Kurulu ise Danıştay 5. Dairesinin verdiği kararda olduğu gibi, parmak izi taramasının özel hayatın gizliliği kapsamında olduğunu ve işleme faaliyetinin, yasal dayanağı olmamasından dolayı temel haklar ve Anayasal ilkeler doğrultusunda, hukuka uygun olmadığına karar vermiştir.

C. İlgili Avrupa İnsan Hakları Mahkemesi Kararları

Avrupa İnsan Hakları Mahkemesi (AİHM), *S. ve Marper/Birleşik Krallık*[49] davasında, başvuruculardan S. 12 yaşında hırsızlık suçundan yargılanmış ve beraat etmiş; Marper ise darp şikâyeti üzerine tutuklanmakla birlikte, şikâyetin geri alınması üzerine beraat etmiştir. S ve Marper, soruşturma esnasında alınan parmak izlerinin silinmesini talep etmiş ancak hem yerel mahkeme hem de üst mahkeme, verilerin silinmesi talebini reddetmiştir. Zira o dönem yürürlükte olan İngiliz Kanunlarına göre veriler, sanık/şüphelinin 100 yaşına gelmesi ya da ölünceye kadar saklanması yönündeydi. Başvurucular, bu şekildeki kanuni düzenlemeye ve parmak izlerinin silinmemesi üzerine AİHM'e başvurulmuştur. AİHM, parmak izini kişisel veri

46 Danıştay İdari Dava Daireleri Kurulu E. 2014/2242 K. 2015/4991 T: 09.12.2015, lexpera.com.tr, (ET: 01.11.2019).

47 AKGÜL, s. 208.

48 Danıştay 5. Dairesi T: 10.12.2013 E. 2013/5342 K. 2013/9525.

49 S. Ve Marper / Birleşik Krallık, Başvuru no. 30562/04 ve 30566/04, https://eur-lex.europa.eu/(ET: 27.04.2022).

olarak tanımladıktan sonra, kişisel verilerin korunmasının AİHS'nin özel hayata saygı hakkını düzenleyen 8. madde kapsamında ele alınması gerektiğini belirtmiştir. Ayrıca, parmak izinin saklanması ile suç arasında orantısızlık olduğuna, parmak izi ve DNA örneğinin rastgele ve keyfi depolanmasından kaçınılması gerektiğini belirtmiştir. Sonuçta AİHM, bir suçun işlenmesinden şüphelenilen fakat mahkûm edilmeyen kişilerin parmak izlerinin muhafaza edilme süresinin belirlenmesinde Birleşik Krallık'ın takdir yetkisini aştığına karar vermiştir.

AİHM'nin önüne gelen *MK v Fransa* olayında ise MK kitap çalma suçundan iki ayrı soruşturma geçirmiş, ilk soruşturmada beraat etmiş ikincisine ise devam edilmediğinden beraat etmiş bir kişidir[50]. Başvurucu MK, soruşturma sırasında alınan parmak izinin silinmesini talep etmiş ancak bu talebi reddedilmiştir. AİHM'e yapılan başvuru üzerine mahkeme, öncelikle veri tabanının esas amacının, ciddi suçların faillerinin kimliğinin tespiti ile kovuşturmalarına, soruşturmalarına ve duruşmalara yardımcı olmak olduğunu belirtmiş; başvurucununki gibi hafif suçların, organize suç veya cinsel saldırı gibi ciddi suçlardan açıkça ayırt edilebilir olduğunu belirtmiştir. Bu nedenle Mahkeme, bir suç işlediği kesinleşmemiş masum bir kişinin parmak izinin suç ile ilişkili olarak 25 yıl süreyle veri tabanında saklanmasını demokratik ülke gerekliliği ile bağdaştırmamıştır[51].

D. İlgili Kişisel Verileri Koruma Kurumu Kararları

Kişisel Verileri Koruma Kurulu'nun da parmak izi alınmasına ilişkin çeşitli kararları mevcuttur. Kurul'un 1/12/2020 tarihli ve 2020/915 sayılı kararına konu olayda, başvurucu ilgili kişi devlet memurudur ve çalıştığı işyerinde mesai saatlerinin kontrolü amacıyla parmak izi verileri alınmaktadır. Başvurucu ilgili kişi, veri sorumlusu olan işyerinden, verilerin silinmesi ve buna ilişkin kendisine bilgi verilmesini talep etmiştir. Veri sorumlusu, verilerin silinemeyeceğini ve ilgili kişiye ait bu verilerin kendi onayı olmadan işlenemeyeceğini belirterek, ilgili kişinin başvurusunu reddetmiştir.

Başvurucu ilgili kişi, bunun üzerine Kişisel Verileri Koruma Kurum'una başvurmuştur. Kurul bu olayda, işe giriş çıkış saatlerinin, parmak izinden başka alternatif yollar ile mümkün olduğunu, işyerinin üstün güvenlik önlemlerinin alınmasını gerektirecek bir faaliyette bulunmadığını ve bu nedenlerle KVKK m. 4'te düzenlenen *"Genel İlkeler"* maddesindeki ölçülülük ilkesine aykırı olduğuna karar vermiştir. Bunun yanında, ilgili kişinin verilerinin

50 M. K. / Fransa – 19522/09 Karar,https://www.echr.coe.int/Documents/CLIN_2013_04_162_TUR.pdf, (ET: 17.02.2020).

51 KULESZA, s. 196.

silinmesi talebini ise ilgili kişinin bu işleme faaliyetine rızasının olmadığı şeklinde yorumlamıştır.

Kurulun 27/2/2020 tarihli ve 2020/167 sayılı kararına ilişkin olayda ise spor salonu hizmeti sunan veri sorumlusu, üyelerinin spor salonuna giriş çıkışlarında avuç okutma sistemini kullanmaktadır. Kurul bu olayı, ölçülülük ilkesi kapsamında ele alarak, işleme faaliyetlerinin işleme amacıyla bağlantılı olarak ölçülü olması ve amacı aşan işleme faaliyetlerinden kaçınması gerektiğinden minimum düzeyde veri işleme ilkesine (Veri minimilizasyonu) aykırı bulmuştur.

SONUÇ

Anayasa'nın 20. maddesinin üçüncü fıkrasına göre, herkes kişisel verilerinin korunmasını isteme, kişisel veriler hakkında bilgilendirilmeyi, bu verilere erişmeyi, bunların düzeltilmesini veya silinmesini talep etmeyi ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahiptir. Kişisel verilerin korunması hakkı, kişiliğin ve insan onurunun korunması ile kişinin kendi geleceğini belirleme hakkının özel bir biçimidir.

Biyometrik veriler, değişmeyen, eskimeyen ve ilgili kişiye ait pek çok bilgi sağlayabilen verilerdir. Bu verilerin, olabildiğince az ve sadece gerekli olduğu amaçlar için kullanılması gerekir. Aynı amaca, biyometrik veri olmadan ulaşılabiliyor ise diğer veriler kullanılmalıdır zira bu verilerin işlenmesi için gerekli ve yeterli teknolojik önlemler alınmadan verilerin işlenmesi, geri dönülemeyecek sorunlara neden olabilecektir.

Bu noktada, öncelikle biyometrik verilerin işlenmesi için açık rızanın varlığı mutlaka bulunmalıdır ancak burada da verilen rıza beyanının özgür iradeye dayandığını söylemek oldukça güçtür[52]. Özellikle, yargı kararlarında olduğu gibi veri sorumlusunun bir kamu kurumu olması halinde çalışanların verilerinin işlenmesine özgür iradeleriyle rıza gösterdiği söylenemeyecektir.

Yargı kararlarında yer aldığı gibi biyometrik veri olmaksızın kimlik kontrolünün sağlanabileceği hallerde parmak izine başvurulması ölçülülük ilkesine (veri minimizasyonu ilkesi) uymamaktadır. Bu sebeple, kanaatimizce, AYM'nin SGK başvurusu üzerine verdiği bu karar kişisel verilerin korunmasına ilişkin ölçülülük ilkesine uygun düşmemektedir. Bununla birlikte, Anayasa Mahkemesinin, 03/04/2015 tarihli Resmî Gazetede yayınlanan kararı, parmak

[52] Bu konuda, parmak izi vermediğinden pasaport başvurusu reddedilen kişinin Avrupa Adalet Divanı'na yaptığı başvuru sonucunda Divan, pasaport başvurusunda bulunan vatandaşlardan parmak izi alınmasında, vatandaşın rızasının özgür iradesiyle verilmediğini belirtmiştir. Case C-291/12 Schwartz v Stadt Bochum, http://curia.europa.eu/juris/liste.jsf?num=C-291/12.

izinin işlenmesine ilişkin bir açık kanuni dayanak olmadığı ve bu noktada müdahalenin kanunilik şartını sağlamadığı, ilgili kişinin açık rızasının alınmadığı gibi işlemeye ilişkin genel ilkelere de riayet edilmediği bahsiyle işleme faaliyetleri ihlal olarak kabul edilmiştir.

Bunun yanında, Danıştay Daireleri Kurulu'nun kararı yerindedir. Zira bu karar kişisel verilerin işlenmesine ilişkin ilkelere özellikle veri minimizasyonu ilkesine uygundur. Zira ilkelere göre veri işleme için belirlenen amaç doğrultusunda asgari miktarda veri toplanması gerekir. Kart okutma veya imza alma yoluyla belirli amaca ulaşılabilecek iken parmak izi elde edilmesi ilkelere uygun değildir. Kişisel Verileri Koruma Kurumu da önüne gelen şikâyetleri, ölçülülük ilkesi ekseninde değerlendirmektedir.

Uygulamadaki sıkça karşılaşılan sorun, veri sorumlularının genellikle, ilgili kişilerden bir kerede açık rıza almak adına tüm verilerin işlenmesine yönelik rıza almasıdır. Bu da hem rıza beyanlarının geçerli olmamasına hem de keyfi veri işlemeye yol açmaktadır. Bu sorunun aşılması için öncelikle veri sorumlularının veri işleme amaçlarının sınırlarını önceden net olarak belirlemesi gerekir. Daha sonra, bu amaçlara ulaşılmak için gereken veriler belirlenmeli ve sadece bu gereken veriler işlenmelidir. Veri işleme amacına daha az veri ile ulaşılabilecek iken gerekmeyen veriler de işlenmektedir. Bu ise kişinin kendi geleceğini belirleme hakkını ihlal etmektedir.

KAYNAKÇA

AKGÜL, A. (2015). Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı. Türkiye Barolar Birliği Dergisi, 118, 199-222.

ALTINOK ÇALIŞKAN, E/ÖZTÜRK, B. (2018). Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu. Fasikül Hukuk Dergisi, 10 (100), 277-336.

ATLI, T. (2019). Kişisel Verilerin Önleyici, Koruyucu Ve İstihbari Faaliyetler Amacıyla İşlenmesi. Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, 2(1), 1-19.

AYDIN, S. E. (2015). AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu. İstanbul.

BOROCZ, I. (2016). Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. European Data Protection Law Review, 3(2), 467-480.

BRAUN, A. C. (2018). Kişisel Verilerin İşlenmesinde Rıza. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 15 (1), 13-35.

BRINK, S., WOLFF, H. A. (2018). BeckOK Datenschutzrecht, Online Kommentare.

BU-PASHA, S., ALEN-SAVIKKO, A. MAKINEN, J., GUINNES, R., KORPISAARI, P. (2016). EU Law Perspectives On Location Data Privacy In Smartphones and Informed Consent for Transparency. European Data Protection Law Review 6(1), 312 -323.

BYGRAVE, L. A. (1998). Data Protection Pursuant To The Right To Privacy In Human Rights Treaties. International Journal of Law and Information Technology, 6(3), 247-284.

CUSTERS, B. / VAN DER HOLF, S. /SCHERMER, B. /APPLEBY-ARNOLD, S. /BROCKDORFF, N. (2013). Informed Consent in Social Media Use- The Gap Between User Expectations and EU Personal Data Protection Law. Scripted, 10 (4), 437-457.

DE HERT, P., PAPAKONSTANTİNOU, V. (2016). The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?. Computer Law & Security Review, 32, 179-194.

DEVELİOĞLU, H. M. (2017). 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku. İstanbul.

DÜLGER, M. V. (2019). Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi. İstanbul

ERARSLAN TÜRKMEN, S. (2019). Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller. İstanbul.

ERDİNÇ, G. H. (2021). Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi. Kişisel Verileri Koruma Kurumu Dergisi. 2 (1), 1-19.

JASSERAND, C. (2016). Legal Nature of Biometric Data Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data. European Data Protection Law Review, 2 (3), 297-311.

KAYA, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, LXIX, (1-2), 317-334.

KULESZA, J. (2018). Europol Regulation, US and Data Protection, Data Protection and Privacy: The Internet of Bodies, Ed: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul de Hert. 189–202.

KÜZECİ, E. (2018). Kişisel Verilerin Korunması. Ankara.

RINGELHEIM, J. (2006). Processing Data On Racial Or Ethnic Origin For Antidiscrimination Policies: How To Reconcile The Promotion Of Equality With The Right To Privacy?". Center For Human Rights And Global Justice Workİng Paper, New York.

SOLMAZ, E. (2018). Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunmasına Katkısı. İdare Hukuku ve İlimleri Dergisi, 18 (1), 61–78.

TEKİN, N. (2014). Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi. Uyuşmazlık Mahkemesi Dergisi, 4, 222-262.

UYGUN, M. (2010). Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması. Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Avrupa Birliği Hukuku Bilim Dalı Yayımlanmamış Yüksek Lisans Tezi, Ankara.

YÜCEDAĞ, N. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, LXXV (2), 765-789.