www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt: 2, Sayı: 1

Geliş: 16.05.2020
Kabul: 29.06.2020

Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi

Göksu Hazar, Erdinç
Kişisel Verileri Koruma Kurumu, Ankara, Türkiye, goksu.erdinc@kvkk.gov.tr
ORCID: https://orcid.org/ 0000- 0002-5732-6111

ÖZ
Biyometrik veriler, özel nitelikli kişisel veri özelliğini haiz olup işlenmesi sıkı kurallara tabidir. 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda kişisel verilerin işlenme ilkeleri ve şartları hüküm altına alınmıştır. Biyometrik veriler; kişilerin ayırt edilmesini sağlayan, benzersiz, neredeyse değişmeyen biyolojik ve davranışsal özelliklerin bütünüdür. Biyometrik verilerin ifşası durumunda ortaya telafisi zor sonuçların çıkması kaçınılmazdır. Kişisel verilerin işlenme ilkeleri ve şartları bir bütün olarak değerlendirilerek biyometrik verilerin işlenmesi hususunda değerlendirme yapılmalıdır. Kişisel verilerin işlenme ilkelerinden birisi olan ölçülülük ilkesi, temel hak ve özgürlükler kapsamında önem arz eden "mahremiyet" konusunun da bir uzantısı olarak kabul edilebilir. Bu çalışmada, mahremiyet ve güvenlik kavramları ile biyometrik verilerin işlenmesine dair ulusal ve uluslararası düzenlemeler irdelenerek açık rıza ve ölçülülük kavramları ele alınmıştır.

Anahtar Sözcükler: Biyometrik Veri, Güvenlik, Kişisel Veri, Mahremiyet

Processing Biometric Data in The Scope of Adequacy Principle and Consent

ABSTRACT
Biometric data is a sensitive personal data and when processed it is subject to strict rules. Law No. 6698 on the Protection of Personal Data regulates the principles and conditions of processing personal data. Biometric data is a set of unique, almost invariant, biological and behavioral characteristics that allows individuals identifiable. The principles and conditions of processing personal data should be considered as a whole and an assessment should be made on the processing of biometric data. The principle of adequacy which is one of the principles of the processing of personal data can be accepted as a consequence of "privacy" term. Privacy plays a vital role within the scope of fundamental rights and freedoms. In this study, the concepts of privacy and security and the national and international regulations on the processing of biometric data are examined while the concepts of consent and adequacy principle are discussed.

Keywords: Biometric Data, Personal Data, Privacy, Security

Atıf Gösterme Erdinç, G. H. (2020). Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi. *Kişisel Verileri Koruma Dergisi*. *2*(1), 1-19.

GİRİŞ

Endüstri 4.0 kavramının hayatımıza girmesiyle birlikte, akıllı cihazların kullanımı yaygınlaşmış; büyük veri, yapay zekâ, veri madenciliği gibi kavramlar hayatımıza girmiştir. Teknolojinin ilerlemesiyle birlikte veri pazarı oluşmaya başlamış; bu verilerin korunması alanında duyulan ihtiyaç da bir o kadar artmıştır. Kişilere ait veriler kullanılarak çeşitli analizler yapılmakta, reklam gibi ticari kaygılar güdülerek kullanılmakta; hatta bazen Cambridge Analytica'nın yaptığı gibi manipülasyon yoluyla kişilerin kendisini yönlendirmek gibi tehlikeli faaliyetlerde kullanılmaktadır. Kişisel verilerin de önemi bu noktada ortaya çıkmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 sayılı Kanun) "*Tanımlar*" başlıklı 3 üncü maddesinin (d) bendi uyarınca kişileri tanımlayan, onları belirlenebilir kılan her türlü veri kişisel veri olarak tanımlanmaktadır. Kişisel veriler, mahremiyet kavramının da bir parçası olup özel hayatın gizliliği açısından önemli rol oynamaktadır.

Kişisel verilerin korunması hususu birçok ülke açısından önem teşkil etmekte olup bu konuda birçok düzenleme yapılmıştır. Örneğin, 28 Ocak 1981 yılında 108 Numaralı "*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*" kapsamında kişisel veriler uluslararası koruma altına alınmıştır. Mezkûr sözleşme, CETS 223 Numaralı Protokol ile 18 Mayıs 2018 tarihinde "*108+ numaralı Modernize Edilmiş Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*" olarak kabul edilerek yenilenmiştir. Benzer şekilde, Avrupa Birliği'nde ise 95/46 sayılı Direktif güncellenerek 2016/679 sayılı Genel Veri Koruma Tüzüğü (GVKT) yürürlüğe girmiştir ve bu düzenleme, kişisel verilerin korunması alanındaki temel düzenlemelerden biri olarak kabul edilmiştir.

Ülkemizde kişisel verilerin korunması hususu çeşitli mevzuatlarda kısmen düzenlenmekte olsa da bu konuda detaylı bir düzenleme bulunmamaktaydı. Kişisel veriler, öncelikle 2010 yılında Türkiye Cumhuriyeti Anayasası'nda (Anayasa) yapılan bir değişiklik ile Anayasal güvence altına alınmıştır. Bu kapsamda, "*Özel hayatın gizliliği*" başlıklı Anayasa'nın 20 nci maddesinin üçüncü fıkrası,

"*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*"

hükmünü amirdir. Bu kapsamda, kişisel verilerin ancak kanunlarda öngörülen hallerde veya kişinin açık rızası işlenebileceği belirtilmiş olup kişilerin kişisel verilerine erişme hakkı da düzenlenmiştir. Kişisel veriler Anayasal güvence altına alındıktan sonra 7 Nisan 2016 tarihinde "*6698 sayılı Kişisel Verilerin Korunması Kanunu*" Resmi Gazetede yayımlanarak 7 Ekim 2016 tarihinde yürürlüğe girmiştir.

Kişisel veriler, 6698 sayılı Kanun uyarınca özel nitelikli kişisel veriler ve (genel nitelikli) kişisel veriler olmak üzere iki kategoriye ayrılmıştır. Bu çerçevede, biyometrik veriler özel nitelikli kişisel veri olarak Kanun'un altıncı maddesinde sayılmıştır. Biyometrik veriler, kişilerin diğer kişilerden ayırt edilmesini sağlayan, kişilere has olan her türlü biyolojik ve davranışsal özelliklerin bütünü olarak tanımlanabilir (Erdinç, 2017). Biyometrik veriler, kişilerin biyometrik verilerini ömür boyu taşımaları ve bu verilerin neredeyse hiç değişmemesi dolayısıyla en önemli kişisel verilerdendir. Biyometrik verilerin hukuka aykırı olarak işlenmesi neticesinde telafisi mümkün olmayan durumlar meydana gelebilir, bundan dolayı da biyometrik veriler Kanunda sıkı koruma kurallarına tabi tutulmuştur.

Belirtmekte fayda görülmektedir ki, kişisel verilerin işlenmesinde Kanunda yer alan kişisel veri işleme şartları kadar kişisel verilerin işlenmesine ilişkin genel ilkeler de önem arz etmektedir. Bu ilkeler Kanun'un dördüncü maddesinde düzenlemiştir ve kişisel verilerin işlenmesi noktasında gerekli şartlar mevcut olsa dahi her hâl ve durumda anılan ilkeler gözetilecektir. Özellikle biyometrik verilerin işlenmesine ilişkin olarak "ölçülülük" ilkesi büyük önem arz etmektedir. Bu çalışma kapsamında, gerek mevzuatımızda yer alan biyometrik verilerin işlenmesine ilişkin temel düzenlemeler gerekse karşılaştırmalı hukuktaki ilkelerin de benimsenmesi açısından Avrupa Birliğinin Genel Veri Koruma Tüzüğü (GVKT), Avrupa İnsan Hakları Mahkemesi (AİHM) kararları ve diğer ülkelerin mevzuatlarından örnekler verilmek suretiyle biyometrik verilerin işlenmesinde mahremiyet ve güvenlik konuları ele alınarak açık rıza ve ölçülülük ilkesi karşılaştırmalı olarak incelenecektir.

BİYOMETRİK VERİ

Biyometrik Verinin Tanımı

Kimlik doğrulama üç şekilde gerçekleşebilmektedir. Bunların ilki, kişinin yalnız kendisinin bildiği şifrelerdir. Ancak şifrelerin yetkisiz kişiler tarafından ele geçirilmesi, kişinin şifreyi unutabilmesi söz konusu olabilmektedir. İkinci kimlik doğrulama yöntemi ise kişilerin akıllı kart ya da jeton gibi sahip olduklarıdır (Han, Hu, Kotagiri, 2011). Ancak bu durumda da akıllı kart ve jetonların kopyalanma, çalınma veyahut kaybolma riskleri mevcuttur (Reillo, Fernandez, Hernandez, Sandoval, 2018). Kimlik doğrulama yöntemlerinden sonuncusu ise kimlik sahibinin kendisini oluşturan biyometrik özellikleridir. Biyometri ile insana ait bir özellik ifade edilmektedir. Bu özellikler biyolojik veya davranışsal olabilir ve biyometrik veriler ait olduğu kişiye özgü olup benzersiz ve tektir. Diğer bir deyişle, kişinin kimliğini doğrudan tanımlamaya yarayan ve sadece o kişiye ait olan fizyolojik ve davranışsal verilerin bütünü biyometrik veriyi ifade eder. Biyometrik veriler, herhangi bir müdahaleye gerek olmaksızın zahmetsiz bir şekilde elde edilen ve ömür boyu değişmeden kalan verilerdir (Erdinç, 2017). Bir bireyin biyometrik verisini değiştirmesi veya unutması mümkün değildir; çünkü ona ait özellikleri bizzat kendi taşımaktadır.

Kişilerin irisi, parmak izi, DNA'sı, yüzü, avuç içi, eli, sesi, imzası, yürüyüş şekli gibi tüm özellikler biyometrinin kapsamına girmektedir. Biyometrik verilerin tespitinde önemli olan husus, o kişiye özgü, benzersiz fizyolojik ya da davranışsal özellikleri içererek bizzat kişinin kimliğinin tanımlanmasını sağlamasıdır. Öte yandan, teknolojinin gelişmesi sonucunda akıllı telefonların da hayatımıza girmesi ile siber biyometri kavramı da oluşmaya başlamıştır. Akıllı telefonlarda güvenliğin sağlanması açısından yüz, iris, parmak izi, ses tanıma gibi geleneksel yöntemlerle ilgili kişinin biyolojik/fiziksel nitelikli biyometrik verileri işlenmektedir. Buna ek olarak, kişilerin akıllı telefon kullanırken telefon üzerinde gerçekleştirdikleri parmak hareketi, klavyeye basma şekilleri, yürüyüş biçimleri gibi veriler de davranışsal biyometrik verilerini içermektedir (Snijder, 2016). Verilmiş olan bu örnekler siber biyometrinin kapsamını oluşturmaktadır.

Biyometrik veri hassas ve kritik kişisel veri özelliğini haiz olması nedeniyle, bu verilerin alınma yöntemlerinde güvenliğe dikkat edilmelidir. Biyometrik verilerin teknik olarak kendine özgü yüksek güvenlikli sisteme sahip olması hususu da ayrıca önem teşkil etmektedir. Nitekim, kişilerin biyometrik verileri alındığında birtakım sağlık verilerine de erişilebilmektedir ve bu durum da biyometrik verilerin korunmasının önemini artırmaktadır. Bir kişinin parmak izi örneğinde o kişinin Down sendromu, Turner sendromu, Klinefelter sendromu gibi kromozomsal bozukluklarının olup olmadığı tespit edilebilmektedir (Sherman, 2019). Yine bazı normal olmayan parmak izi numunelerinden ilgili kişide

göğüs kanseri, lösemi, Rubella sendromu bulunduğuna dair teşhis konulabilmektedir. Aynı şekilde, retina taramasından kişinin alkolik ya da uyuşturucu bağımlısı olduğu ortaya çıkabilir. Örneklerden de görüldüğü üzere, kişilerin medikal geçmişlerine ve yaşam biçimlerine ait bilgilere alınan biyometrik veri örneklerinden de ulaşılabilmekte; bu noktada biyometrik verilerin mahremiyeti ve kritik önemi gündeme gelmektedir (Sherman, 2019). Öte yandan, kişi için gizli olan sağlık problemlerine ilişkin bilgilerin biyometrik verilerinin ifşası sonucunda ortaya çıkması durumunda bu bilgi o kişiye karşı ayrımcılık yapılmasında, örneğin çalıştırılmamasında veya sigortalanmasının reddinde kullanılabilir (Akgül, 2015).

Biyometrik veriler çeşitli alanlarda kullanılmaktadır. Çeşitli amaçlarla yüz tanıma, parmak izinin alınması, ses tanıma, iris tanıma gibi yöntemlerle biyometrik veri alınmaktadır ve kendi aralarında güvenlik dereceleri değişkenlik göstermektedir. Yüz tanıma sisteminde, iki gözün arasındaki mesafe, elmacık kemikleri, çene hattı, burnun genişliği, ağzın şekli ve benzeri unsurlar analiz edilerek kimlik doğrulama gerçekleşmektedir. Yüz tanıma sistemleri seçilen yüz özelliklerini bir elektronik belgenin veya yüz veri tabanının saklanan görüntüsüyle karşılaştırarak dijital bir görüntü veya video karesinden kişiyi otomatik olarak tanımlayabilir veya doğrulayabilir ("Biometrics in identity", 2019). Yüz tanıma da yüksek güvenilirlik derecesine sahip biyometrik verilerden biridir; ancak yüz tanıma kullanılarak birbirine benzeyen kardeşleri, tek yumurta ikizlerini ayırt etmek mümkün olmayabilir. Yüz yapısı benzeyen insanları aynı insanmış gibi algılayarak her zaman doğru sonuç elde edilmeyebilir (Han ve ark., 2011).

İris tanıma sistemleri en yüksek güvenlikli sitemlerden biridir. İris ve retina tanıma sistemleri oldukça güvenlidir; çünkü kişilerin iki gözündeki retina yapısı bile farklıdır ve kişi öldüğünde kan damarları çok hızlı çürümeye başladığı için kişi öldükten sonra da retinası alınmak suretiyle taklit edilemez (Eye Biometrics, t.y.). İrisin ayırt edici yapısı sayesinde iris, bir insanın yaşamı boyunca sabit kalmaktadır (("Biometrics in identity", 2019). İris tanıma sistemlerinin hızlı olmasının yanında net sonuçlar da alınabildiği için hata oranı çok azdır (Eye Biometrics, t.y.).

Parmak izi de en fazla kullanılan tekniklerden biridir. Parmak izi uygulaması, özellikle mobil uygulamalarda en sık kullanılan tekniklerdendir. Aynı zamanda, en güvenilir ve doğru sonuçlar veren biyometrik verilerden biri olarak da kabul görmektedir (Erdinç, 2017). Her ne kadar parmak izlerinin yaşa bağlı olarak değişebileceğine dair kanıtlar bulunsa da bireylerin parmak sırtı yapısı yaşam boyunca aynı kalmaktadır ve bu bakımdan da kimlik belirlemede ayırt edici özelliğe sahiptir ("Biometrics in identity", 2019). Otomatik parmak izi eşleştirme sistemlerinin çoğu, minutae (ayrıntı) olarak adlandırılan sırt uçları ve sırt ayrımlarına dayanmaktadır. Bir ayrıntının tanımlanması genellikle konumuyla (x, y koordinatları) ve sırtın yönü (θ) ile yapılır. Birleşik Devletlerdeki Federal Soruşturma Bürosuna göre iki kişinin sekizden fazla aynı ayrıntıya sahip olamayacağı ifade edilmiştir (Han ve ark., 2011). Ucuz sistemlerle hızlı bir şekilde güvenilir ve verimli sonuçlar alınabildiği için parmak izi sistemleri daha çok tercih edilmektedir (Fingerprinting Criticism, t.y). Çeşitli yerlerde aktif olarak kullanılması ve teknolojinin de gelişmesi sonucunda daha ucuz ve boyut olarak daha küçük parmak izi tanıma sistemleri yapılmıştır ("Biometrics in identity", 2019).

Ses tanıma sistemi de biyometrik verilerin kullanımında söz konusu olan sistemlerdendir. Ses, davranışsal özellikli biyometrik verilerden biridir. Her bir bireyin sesinde ton, perde, ahenk farklılığı olması nedeniyle ses de biyometrik veri olarak kullanılabilir. Ses, kişilerin konuşurken ağızlarını hareket ettirme biçimleri ve ses tellerinin şekli nedeniyle eşsiz ve kişiye özgü olarak ifade edilir (Wilson, t.y.). Ses tanıma sistemlerinde konuşmayı oluşturan ses özelliklerine bakılmakta olup sadece ses ya da sesin telaffuzuna bakılmamaktadır ("Biometrics in identity", 2019). Biyometrik ses tanıma yöntemleri göç, vatandaşlık hizmetleri, ordu, uluslararası bankalar ve sağlık örgütleri, hassas bilgi korunumu, kişisel bilgi güvenliği, e-ticaret, internet bankacılığı gibi alanlarda kullanılmaktadır (Arslan ve Sağıroğlu, 2016). Ses tanıma sistemleri de yüzde birden daha az hata oranıyla çalışarak kişilerin kimliklerini belirlemektedir ("Biometrics in identity", 2019).

Teknolojinin de gelişmesiyle biyometrik verilerin işlenmesinde yapay zekânın kullanımı artmıştır. Gartner isimli şirketin araştırmasına göre, yüz tanımanın kullanımının artmasıyla birlikte 2023 yılı itibariyle 2018 yılına oranla kaybolan insan sayısının %80 oranında azalacağı belirtilmiştir ("Biometrics in identity", 2019). Akıllı aletlerle kişilere ait iki binden fazla parametre teşhis edilebilmektedir. Bunların arasında kişinin telefonun tutuş stili, dokunmatik ekran üzerine dokunurken uygulanan basınç ve parmak hareketleri, farklı çevrim içi uygulamalardaki uyarıcılara olan tepkileri gibi parametreler tutulmaktadır ("Biometrics in identity", 2019).

Türkiye'de Biyometrik Verilerin İşlenmesi İlkeleri

Biyometrik veriler, 6698 sayılı Kanun'un 6 ncı maddesi uyarınca özel nitelikli kişisel veri kategorisinde sayılmıştır. Kişisel veriler, 6698 sayılı Kanun kapsamında (genel nitelikli) kişisel veriler ve özel nitelikli kişisel veriler olmak üzere iki kategoriye ayrılmıştır. Bu ayrımın temel özelliği, özel nitelikli kişisel verilerin ifşa edilmesi halinde verinin sahibi olan ilgili kişinin zor durumda kalacak olmasıdır. Özel nitelikli kişisel veriler, öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir (Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2018). Bu nedenle, genel nitelikli kişisel verilere göre daha sıkı koruma kurallarına tabidir. Özel nitelikli kişisel verileri korumanın sıkı kurallara tabi olmasıyla birlikte, Anayasada da düzenlendiği üzere, bu koruma mutlak değildir ve tüm temel hak ve özgürlükler bakımından geçerli olduğu gibi diğer hak ve özgürlükler lehine sınırlanabilir. Yaşam hakkı, ifade özgürlüğü, haberleşme özgürlüğü, gibi birçok temel hak ve özgürlüğün kullanılması, özel nitelikli kişisel verilerin işlenmesini zorunlu hale getirmektedir (Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2018).

Biyometrik verilerin tanımı 6698 sayılı Kanunda yapılmamış olup 5490 sayılı Nüfus Hizmetleri Kanunu'nda (5490 sayılı Kanun) ve çeşitli ikincil düzenlemelerde biyometrik verinin kullanımına ilişkin hükümler bulunmaktadır. Bu çerçevede, 5490 sayılı Kanun'un "*Tanımlar*" başlıklı 3 üncü maddesinin (ff) bendinde biyometrik veri, "*elektronik sistemler aracılığı ile kimlik tespit ve kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla alınan parmak izi, damar izi ve el ayasından elde edilen kişiye özgü veriler*" olarak tanımlanmıştır. Biyometrik kavramının tanımı ise Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ'in dördüncü maddesinde yer almaktadır. Bu kapsamda, biyometrik "*bir kişinin diğer şahıslardan ayrılmasını sağlayan, bu kişiye ait ölçülebilir bir biyolojik veya davranışsal karakteristiği*" olarak tanımlanmaktadır. Yine mezkûr Tebliğ'in yirmi yedinci maddesi kimlik doğrulama konusuna ilişkindir. Bu çerçevede,

> "*Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin "bildiği" unsur olarak parola/değişken parola bilgisi gibi bileşenler, "sahip olduğu" unsur olarak tek kullanımlık parola üretim cihazı, kısa mesaj servisi ile sağlanan tek kullanımlık parola gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır. (...) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyecek yöntemler barındıracak şekilde müşteri kullanımına sunulur. Şifreleme anahtarları kimlik doğrulama için kullanılmak istendiklerinde parola, PIN (Kişisel Tanımlama Numarası) veya biyometrik bir bileşen bilgisi ile erişilebilir olmalıdır*." .

İlgili tanımlardan da anlaşıldığı üzere, Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ'de yer alan biyometrik kelimesinin tanımında da davranışsal ve biyolojik karakteristik unsurlarından bahsedilmektedir. Biyometrik verilere ilişkin değerlendirme yapılırken kişileri ayırt etmeye yarayan davranışsal ve biyolojik karakteristik özelliklerin mevcut olup olmadığı somut olay

ışığında değerlendirilmelidir. Yukarıdaki başlıkta ele alınan kişilerin kimliklerinin ayırt edilmesine ilişkin kategoriler mevzusu da Tebliğ'in yirmi yedinci maddesinde düzenlenmek suretiyle ifade edilmiştir.

Özel nitelikli kişisel veriler, 6698 sayılı Kanun'un altıncı maddesinde sayılmıştır. Bu madde kapsamında sayılan veriler dışındaki veriler özel nitelikli kişisel veri olarak kabul edilmeyecektir. Dolayısıyla, özel nitelikli kişisel veriler tahdidi yani sınırlı sayma ilkesi uyarınca sayılmaktadır. Özel nitelikli kişisel verilerin işlenme ilkesinde de ikili bir ayrım mevcuttur. Bunlardan ilki sağlık ve cinsel hayata ilişkin kişisel verilerdir. Bu verilerin işlenmesi için temel kural açık rızanın bulunması olup açık rıza bulunmadığı hallerde işlenebilmesi ancak 6698 sayılı Kanun'un altıncı maddesinin üçüncü fıkrasında sayılan hususların mevcudiyeti halinde mümkün olup kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişisel veya yetkili kurum ve kuruluşlar tarafından işlenebilmesi durumlarından herhangi biri mevcutsa, açık rıza bulunmaksızın sağlık ve cinsel hayata ilişkin veriler işlenebilecektir.

Özel nitelikli kişisel verilerin ikinci kategorisi ise sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerdir. Biyometrik veri de bu kategoride yer almaktadır. Bu kapsamda, biyometrik verilerin işlenebilmesi için ya açık rızanın bulunması ya da Kanun'un altıncı maddesinin üçüncü fıkrasında belirtildiği üzere kanunlarda açıkça öngörülmüş olması gerekmektedir. Diğer bir deyişle, biyometrik verilerin işlenebilmesi ancak diğer kanunlarda açıkça öngörülmüşse, açık rıza varsa ya da Kanun'un 28 inci maddesinde düzenlenen tam istisna hükümlerinin uygulanacak olması durumlarında söz konusu olmaktadır.

Örneğin, 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67 nci maddesinde yer alan sağlık hizmetlerinden yararlanmak amacıyla biyometrik verinin alınmasına ilişkin düzenleme, kanunlarda açıkça öngörülmesi şartına örnek teşkil etmektedir. Yine, 5490 sayılı Nüfus Hizmetleri Kanunu'nun "*Aile kütüklerinde bulunması gereken kişisel bilgiler*" başlıklı 7 nci maddesinin birinci fıkrasının (h) bendi uyarınca, aile kütüklerinde biyometrik veri bilgisi de bulunmaktadır. Anılan örneklerden de görüldüğü üzere, başka kanunlarda biyometrik verilerin işlenmesine dair hükümlerin yer alması durumunda ilgili kanunlarda yer alan hükümler uygulanacaktır.

Öte yandan, kişisel verilerin işlenmesine yönelik tam ve kısmi istisnalar 6698 sayılı Kanun kapsamında düzenlenmiştir. 6698 sayılı Kanun'un 28 inci maddesi ile "istisnalar" düzenlenmektedir. 6698 sayılı Kanun hükümlerinin bütün olarak uygulanmayacağı tam istisnalar 28 inci maddesinin (1) numaralı fıkrasında sayılmış olup; kısmen uygulanmayacağı durumlar ise (2) numaralı fıkrasında düzenlenmiştir. Bu noktada belirtmekte fayda görülmektedir ki, tam istisna durumlarında, 6698 sayılı Kanun hükümleri tamamen uygulanmayacak olsa da Anayasanın 20 inci maddesinin (3) numaralı fıkrasında düzenlenen kişisel verilerin korunmasını isteme hakkı, temel haklardan biridir ve Anayasanın 13 üncü maddesine göre; temel hak ve hürriyetler özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz. Bu bakımdan, söz konusu tam istisna durumlarında her ne kadar Kanun hükümleri uygulanmayacak olsa da kişisel verilerin işlenmesi bakımından Anayasal bir gereklilik olarak hakkın özüne dokunulmaması, demokratik toplum düzeninin gerekleri ve ölçülülük temel kriter olarak gözetilmeye devam edilecektir. Örnek olarak, 6698 sayılı Kanun'un 28 inci maddesinin birinci fıkrasının (ç) bendi uyarınca kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi durumunda biyometrik verilerin de işlenmesi söz konusu olabilecektir.

Bir başka vurgulanması gereken husus ise biyometrik verilerin işlenmesinde istisnalar ve veri işleme şartları kadar 6698 sayılı Kanun'un 4 üncü maddesinde yer alan kişisel verilerin işlenmesine ilişkin genel ilkelerin de önem arz etmesidir. Açık rızanın olması durumunda dahi kişisel veri işleme ilkeleri göz önünde bulundurulmalıdır. Özellikle belirli, açık ve meşru amaçlar için işlenme ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkeleri biyometrik verilerin işlenmesinde her zaman göz önünde bulundurulmalıdır. Öte yandan, mahremiyet ve güvenlik hususları somut olay bazında değerlendirilerek kişilerin temel hak ve özgürlükleri de göz önünde bulundurulmalıdır. Bu kapsamdaki tartışmalara detaylı olarak alt başlıklarda değinilecektir.

Konusu "*Bilgi ve İletişim Güvenliği Tedbirleri*" olan 2019/12 sayılı Cumhurbaşkanlığı Genelgesi 06 Temmuz 2019 tarihli ve 30823 sayılı Resmi Gazetede yayınlanmış olup mezkûr genelgede

> "*Bilginin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması, ciddi güvenlik risklerini beraberinde getirmektedir. Karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla aşağıdaki tedbirlerin alınması uygun görülmüştür."*

belirtilmek suretiyle genelgenin içeriği açıklanmıştır. Yine 2019/12 sayılı Cumhurbaşkanlığı Genelgesi uyarınca, "*Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır*." belirtilmek suretiyle, biyometrik veri kritik bilgi içeren veri olarak kabul edilmiş olup bu tür verilerin bulut ortamı gibi ortamlarda değil de yurt içinde güvenli bir şekilde depolanması hususu vurgulanmıştır. Bu noktada önemle belirtmek gerekir ki verilerin yurt içinde muhafazası bakımından veri bankaları büyük önem arz etmekte olup Türkiye'de yer alan veri bankalarının sayısı çoğaltılarak yurt dışından bulut hizmeti alınmasının önüne geçilmelidir. Özellikle özel nitelikli kişisel verilerin işlenmesinde bu verilerin önemine binaen herhangi bir veri ihlâli durumunda telafisi mümkün olmayan sonuçlar ortaya çıkabilecektir. Dolayısıyla, bu verilerin yurt içinde muhafaza edilmesi büyük önem taşımaktadır.

Avrupa Birliği ve Diğer Ülkelerde Biyometrik Verinin İşlenmesi İlkeleri

Avrupa Birliğinin (AB) kişisel verilere ilişkin düzenlemesi olan Genel Veri Koruma Tüzüğü'nün (GVKT) tanımlara ilişkin 4 üncü maddesinin (14) numaralı fıkrasında biyometrik veri, "*teknik bir işleme sonucu kişinin fiziksel, fizyolojik veya davranışsal özelliklerinin ortaya çıkarılarak, söz konusu gerçek kişinin yüz görüntüsü ve daktiloskopik verisi gibi ayırt edici şekilde tanımlanabilmesini sağlayan veya bunu teyit eden kişisel veriler*" biçiminde tanımlanmıştır. AB uyarınca biyometrik verilerin kişisel olduğu ve doğası gereği ilgili kişilerin hak ve özgürlüklerine özgü spesifik riskleri sunduğu vurgulanmaktadır (Snijder, 2016).

GVKT uyarınca kişisel verilerin biyometrik veri sayılabilmesi için;

- Kişinin fizyolojik, fiziksel veya davranışsal özellikleri gibi ayırt edici özellikleri teknik işleme sonucunda ortaya çıkarılmalı,
- Ortaya çıkarılan özellikler kişinin kimliğini tanımlamaya yarayan ya da kişinin kimliğini teyit eden kişisel veriler olmalıdır.

GVKT uyarınca biyometrik veri Kanunumuzda da öngörüldüğü üzere hassas nitelikli veri olarak sayılmaktadır. Nitekim GVKT'nin "*Özel nitelikli kişisel verilerin işlenmesi*" başlıklı 9 uncu maddesinin (1) numaralı fıkrası, "*Kişilerin ırk veya etnik köken, dini veya felsefi düşünceleri veya sendika üyeliğinin ifşa edildiği verilerin işlenmesi ve bir gerçek kişinin kimliğini ortaya çıkartmak amacıyla genetik veriler*

ile biyometrik verilerin, sağlık ile kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır" hükmünü amir olup biyometrik verilerin işlenmesi için açık rıza kural olarak aranmaktadır. İstisnai durumlar ise 9 uncu maddesinin (2) numaralı fıkrası ve sonrasında hüküm altına alınmıştır. Bu kapsamda, GVKT uyarınca biyometrik verilerin işlenebilmesi şartları ülkemizdeki mevzuatla benzer düzenlenmiştir. Örneğin; ilgili kişinin kendisi tarafından alenileştirilmiş olması, iş ve sosyal güvenlik hukuku alanlarında yükümlülüklerin yerine getirilmesi, hakkın tesisi için gerekli olması, ilgili kişinin hukuken rıza vermekten aciz olduğu durumlarda işleme ilgili kişinin hayati menfaati için gerekliyse ve benzeri durumlarda açık rıza aranmamaktadır (Develioğlu, 2017). Benzer düzenlemeler mevcut olmakla beraber, GVKT 9 uncu maddesinin (4) numaralı fıkrasına göre "*Üye Devletler, sınırlamalar da dahil olmak üzere genetik verilerin, biyometrik verilerin veya sağlığa ilişkin verilerin işlenmesi hakkında diğer şartlar kabul veya muhafaza edebilir.*" düzenlenmiştir.

GVKT giriş hükümlerinden (51) numaralı Resital hükmü uyarınca fotoğraflar, belirli bir teknik işlemeden geçerek o kişinin emsalsiz bir şekilde tanımlanmasını veya doğrulanmasını sağladığı takdirde biyometrik veri olarak kabul edilebilecektir. Örnek olarak, kişilerden oluşan bir fotoğrafta bu söz konusu fotoğraftaki kişilerin biyometrik verisinin bulunduğu kabul edilmemektedir. Ancak, aynı fotoğrafta teknik bir analiz sonucunda bir bireyi diğerinden benzersiz bir şekilde ayırabilirsek bu görüntüler somut olay ışığında değerlendirilerek biyometrik veri olarak nitelendirilebilir (Coraggio, 2019). GVKT'de de düzenlendiği üzere, her vesikalık fotoğrafın biyometrik veri niteliğini teşkil edeceği yorumunu yapmak doğru olmayacaktır. Kişinin kimliğinin belirlenmesi amacıyla teknik analiz gerektiren işlemler sonucu kişinin kimliğinin belirlenmesi durumu o fotoğrafın biyometrik veri niteliğini kazanmasını sağlayacaktır. İşlemenin kişinin kimliğini tespit amacı dışında gerçekleştirilmesi durumunda ilgili kişi belirli ya da belirlenebilir ise o zaman veriyi genel nitelikte olan kişisel veri olarak değerlendirmek isabetli olacaktır (Yücedağ, 2017). Örneğin, bir bankanın müşterilerinin kimliklerini ses tanımlama sistemi ile saptaması halinde, ses kaydı özel nitelikli veri (biyometrik veri) sayılacaktır; ancak müşteri memnuniyetini sağlamak ve yapılan işleme ilişkin ispat külfeti için ses kaydının tutulması durumunda bu veriler özel nitelikli veri olmayacak; genel nitelikte olan kişisel veri olacaktır (Yücedağ, 2017).

Belirtmekte fayda bulunmaktadır ki, her görüntünün, fotoğrafın biyometrik veri olarak kabul edilmesi isabetli değildir. Bir fotoğrafın veya görüntünün biyometrik veri olarak kabul edilebilmesi için somut koşullar değerlendirilmelidir. Diğer bir deyişle, bir verinin biyometrik olabilmesi için veriyi işleme amacı yani verinin teknik bir analizden geçirilerek o kişinin başka bir kişiden ayırt edilebilmesini sağlamak önem teşkil etmektedir. Diğer bir deyişle, kişinin kimliğini ortaya çıkarmak saiki ile yapılan veri işleme faaliyeti sonucu ortaya çıkan fotoğraf, görüntü gibi durumlarda bu veriler özel nitelikli kişisel veri niteliğini haiz olacaktır. Görüntüler, somut koşulların da değerlendirilmesi suretiyle biyometrik veri dışındaki diğer özel nitelikli veri veya genel nitelikte kişisel veri niteliğini haiz olabilir. Nitekim, bir kişinin fotoğrafında o kişinin kılık kıyafeti, ırkı, siyasi düşüncesi (örneğin kıyafetine bir parti amblemi takmış olabilir) gibi hususlar görülebilir. O kişinin fotoğrafında yer alan bu unsurlar sebebiyle ayrımcılığa uğraması veya zor durumda kalması söz konusu olabileceği için fotoğrafta yer alan hususlar da özel nitelikli kişisel veri olarak kabul edilecektir. Bununla birlikte, bir görüşe göre, fotoğraf ya da görüntü üzerinden kişinin etnik kökeni, dini inancı vb. makul bir kimse tarafından anlaşılabiliyorsa, bu takdirde o veriyi özel nitelikli veri kabul etmek gerekecektir (bu görüş için bkz. Yücedağ, 2017). Bu çerçevede, verinin işlenme amacı da göz önünde bulundurularak işlemenin özel nitelikli veri teşkil edip etmediği değerlendirilecektir (Yücedağ, 2017).

Benzer şekilde, kişilerin kamera görüntülerinin alınmasında da aynı görüş söz konusu olabilmektedir. Mahremiyet ve güvenlik kavramları güvenlik kameralarından alınan görüntülerin yorumlanmasında önem arz etmektedir. Öte yandan, birçok ülkede özellikle kamu güvenliği açısından kişilerin kamera görüntüsü alınırken teknik işlemeden geçerek yüz tanıma suretiyle şüphelilerin yakalanması veya tespit edilmesi söz konusudur. Güvenlik sistemleri ile istenilen kapsamda görüntü alınabilmektedir. Güvenlik sistemleri genellikle kamera, monitör, kayıt cihazı ve onları bağlayan bir kablodan oluşur. Bu tarz sistemlere kapalı devre televizyon sistemleri (KDTS) denir ("CCTV Güvenlik Kamera", t.y.).

KDTS'lerde yüz tanıma sistemi gelişmiştir ve bu sayede kişilerin biyometrik verilerine ilişkin görüntüler de elde edilebilmektedir. Kamu güvenliği, bireysel güvenlik, kamuya açık alanların izlenmesi, toplu taşıma araçlarının izlenmesi, iş yerinin gözetlenmesi gibi pek çok sebeple KDTS kameralar kurulmaktadır (Snijder, 2016). Kişilerin görüntülerinin alınmasında mahremiyet ve güvenlik ilkeleri somut olay bazında değerlendirilerek biyometrik verilerinin işlenmesi durumu analiz edilebilir. Örneğin, suçluların tespiti ya da izlenmesi minvalinde yüz tanıma analizi ile görüntünün alınması kamu güvenliğinin bir gereksinimi olup ölçülülüğü aşmayacaktır. Ancak, kişilerin bireysel güvenlik amacıyla kurdukları kamera sistemlerinde ölçülülük gözetilmelidir. Bireysel güvenlik amacıyla kurulan kameralardan alınan görüntüler sonucunda güvenlik amacı dışında yüz tanıma sistemi vasıtasıyla kişilerin analizinin yapılması ve gereğinden fazla bölgeyi içerecek şekilde görüntü alınması hukuka aykırı olacak ve ölçülülüğü aşacaktır.

İş yerlerinde görüntü alınması hususunda da ölçülülük önem arz etmektedir. Nitekim, Madde 29 Çalışma Grubuna göre iş yerlerinde KDTS izlemede aşırılığa kaçılması "yüksek riskli" profilleme olarak değerlendirilmektedir (Sellers, 2018). Bu durumda, GVKT uyarınca veri koruması etki değerlendirmesi yapılarak ölçülülük, mahremiyet, güvenlik ve yasallık gibi unsurlar değerlendirilmelidir. Avrupa İnsan Hakları Mahkemesinin (AİHM) Lopez Ribalda ve diğerlerinin (işçiler) İspanya'ya karşı açmış olduğu davada mahremiyet ilkesi ön planda tutulmuştur. Somut olayda, İspanya'da bir markette çalışan beş işçi marketteki güvenlik kameralarının bazıları hakkında bilgilendirilmemiştir. Markette gerçekleşen hırsızlık olayında gizli kameralardan elde edilen görüntülerle bu beş işçinin ürünleri çaldığı tespit edilmiş ve işçiler de hırsızlık yaptıklarını itiraf etmişlerdir. İşçiler, görünür kameralar hakkında bilgilendirildiklerini; ancak gizli kameralar hakkında ise bilgilendirilmediklerini öne sürerek dava açmışlardır. Yerel mahkeme, işverenin gizli kameralar hakkında bilgilendirmemiş olsa da işyerinin güvenliğini sağlaması amacıyla veri işlemede bulunduğu, veri işlemenin somut olayda gerekli ve ölçülü olduğu gerekçeleriyle ret kararı vermiştir (Sellers 2018). Bunun üzerine, ilgili uyuşmazlığı Lopez Ribalda ve diğerleri AİHM'e taşımıştır. Avrupa İnsan Hakları Sözleşmesinin (Sözleşme) "*Özel ve aile hayatına saygı hakkı*" başlıklı 8 inci maddesi de ailenin korunması hakkını düzenlemekte olup "*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (...)*" hükmünü amirdir. AİHM Daire, Avrupa İnsan Hakları Sözleşmesi'nin 8 inci maddesinde düzenlenen "*Özel yaşama ve aile hayatına saygı hakkı*" kapsamında her personelin özel yaşamına saygı beklentisinin bulunduğunu vurgulamıştır. Mahremiyeti ön planda tutan bu kararda AİHM Daire, İspanya mahkemelerinin işçilerin mahremiyet hakları ile işverenin işyerindeki mallarını koruma menfaati arasında bir denge kurmadığı, işverenin aldığı önlemlerin ölçülü olmadığı; personellerin özel hayatına daha az müdahale edilerek önlemler alınabileceği; kişilerin önceden bilgilendirilmemesinin yasal olmadığı gibi gerekçelere dayanarak İspanya'yı haksız bulmuştur. Böylelikle mahremiyet, şeffaflık ve ölçülülük ilkeleri doğrultusunda izlemenin hukuka uygun olacağı belirtilmiştir (Campbell, 2018). Bununla birlikte, söz konusu karara ilişkin olarak İspanya hükümeti tarafından yapılan temyiz başvurusu neticesinde AİHM Büyük Daire (Grand Chamber), Sözleşme'nin 8 inci maddesinin ihlâl edilip edilmediğini; dolayısıyla işverenin kamera ile işçilerini izleme noktasında ölçülülüğün bulunup bulunmadığı hususunu değerlendirirken temel olarak aşağıdaki ölçütlere yer vermiştir (Pjhlaw, 2020):

- İşçilerin KDTS'nin kurulduğu konusunda bilgilendirilmiş olması,
- İzleme ve müdahalenin mahremiyete olan etkisi,
- İşverenin haklı bir sebebinin bulunması. İzleme ne kadar müdahaleci olursa, haklılık gerekçesi de aynı derecede büyük olmalıdır.
- Daha az müdahaleci araçların mevcut olup olmadığı hususu.
- KDTS kanıtlarından elde verilerin işveren tarafından ne şekilde kullanıldığı
- Uygun önlemlerin bulunup bulunmadığı.

Bu çerçevede AİHM'in Lopez Ribalda ve diğerleri kararında, AİHM Büyük Daire, işyeri olan marketin kamuya açık alan olması; çalışanların görünür kameralar hakkında bilgilendirilmeleri; elde edilen verilerin kullanım süresi ve alanı; bu verilerin ifşası noktasında ne şekilde kullanıldıkları; izlemenin

boyutu ve ölçülülüğü; izlemenin hukuka uygun olması ve haklı gerekçelerle yapılıp yapılmaması; daha az müdahaleci araçların bulunup bulunmaması ve benzeri hususları da tartışarak işçilerin gizli kamera kayıtları hakkında bilgilendirilmemiş olmasının herhangi bir hak ihlâline neden olmadığına ve dolayısıyla Avrupa İnsan Hakları Sözleşmesi'nin 8 inci maddesine aykırı bir durum bulunmadığına hükmetmiştir.

Çin'de yapay zekânın kullanımının artmasıyla beraber biyometrik verilerin çeşitli yerlerde kullanımı da artmıştır. Örneğin, Pekin'de bulunan Cennet Tapınağında tuvalet kağıtlarını veren makineye yüz tanıma sistemi koyarak tuvalet kağıtlarının kullanımını sınırlandırmayı amaçlayan bir deneme gerçekleşmiştir. Bu husus da ölçülülük ilkesinin kapsamında olan orantılılık kavramının sorgulanmasına sebep olmuştur ("Biometrics in identity", 2019).

Amerika'da ise Illinois, Teksas ve Washington gibi eyaletlerde biyometrik veri yasaları bulunmaktadır. Her bir yasanın benzer özellikleri bulunmakla birlikte farklılıkları da mevcuttur. Yasaları, özel sektöre ilişkin düzenlemeler getirmektedir. En sıkı kurallara tabi yasalardan birisi olarak kabul edilen Biometric Information Privacy Act (BIPA) Illinois'da 2008 yılında yürürlüğe girmiştir. BIPA, Illinois'da mukim bireylerin biyometrik verilerinin toplanmasına ilişkin düzenlemeleri içermektedir (Krishan ve Mostafavi, 2018). BIPA, Biyometrik veriler işlenmeden önce ilgili kişilerden bilgilendirilmiş rıza alınması, biyometrik veriler sayesinde kâr edilmesinin yasaklanması, koruma yükümlülüklerinin belirlenmesi, biyometrik verilerin ihlâlinde durumlarına özgü dava hakkı tanınması gibi düzenlemeleri içermektedir. Biyometrik verinin ifşası ancak ilgili kişinin rızası, ilgili kişinin talebi üzerine finansal bir işlemin tamamlanması, Illinois yasaları, belediye düzenlemeleri veya federal yasalar tarafından istenmesi, mahkeme kararları veya geçerli bir emir üzerine söz konusu olmaktadır (Krishan ve ark., 2018). BIPA, "retina veya iris taraması, parmak izi, ses, el veya yüz geometrisi tanıması, ıslak imzalar, fotoğraflar, bilimsel testler veya görüntülemeler için kullanılan insanlara ait biyolojik numuneler, demografik veriler, dövme tarifi veya saç rengi, boy, göz rengi gibi fiziksel özelliklerin tarifi" gibi hususları biyometrik veri kapsamında düzenlemiştir (Sherman, 2019). BIPA'nın kişilere ait dövme, saç rengi, göz rengi gibi detayları da biyometrik veri kapsamında değerlendirmektedir.

Teksas Biyometrik Yasası ise dört durum dışında biyometrik verilerin ifşa edilmesini yasaklamaktadır. Bu durumlar sırasıyla kayıp veya ölü kişinin teşhis edilmesi, finansal işlemin tamamlanması, Eyalet kanunlarının izin verdiği durumlar, emniyet teşkilatının tutuklama talebi olarak ifade edilebilir (Krishan, ve ark., 2018). Washington biyometrik yasası ise biyometrik verinin tanımına ilişkin olarak detaylardan daha uzak; ama kapsamı daha geniş olarak düzenlenmiştir.

BİYOMETRİK VERİLERİN İŞLENMESİNDE AÇIK RIZA VE ÖLÇÜLÜLÜK

Ölçülülük İlkesi

Kişisel veriler, 6698 sayılı Kanun'un 4 üncü maddesi uyarınca ancak 6698 sayılı Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. Bu çerçevede, kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulması zorunludur. Öte yandan, özellikle "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi biyometrik verilerin işlenmesi noktasında kilit rol oynayan temel ilkelerin başında gelmekte olup AİHM içtihatlarında da önemi vurgulanmaktadır. AİHM S. ve Marper/Birleşik Krallık kararında, söz konusu dava, başvuranlardan alınan parmak izleri, hücre örnekleri ve DNA profilleri gibi verilerinin

haklarındaki ceza davasının birinci başvuran yönünden sona ermesine ve ikinci başvuran yönünden ise düşmesine rağmen, bir veri tabanında belirsiz bir süre boyunca saklanmasına ilişkindir ("Tematik Bilgi Notu", 2015). S. Marper /Birleşik Krallık Davasında Mahkeme,

> "*Kişisel verilerin korunması, bir kişinin Sözleşme'nin 8. maddesi kapsamında güvence altına alınan özel hayata ve aile hayatına saygı hakkını kullanması konusunda büyük öneme sahiptir. İç hukuk, kişisel verilerin bu şekilde kullanılmasının, işbu maddede yer alan güvencelere aykırılık teşkil edeceği sebebiyle, önüne geçilmesi amacıyla yeterli güvenceleri sağlamalıdır… Bu tür güvencelere olan ihtiyaç, otomatik olarak işlenen kişisel verilerin korunmasının söz konusu olduğu durumlarda, özellikle de bu verilerin polis tarafından kullanılması halinde, daha da artmaktadır. İç hukuk başta bu verilerin saklanma amaçlarına uygun ve aşırı olmamalarını ve verilerin saklanma amacının gerektirdiğinden daha uzun süre tutulmamalarına olanak tanıyan ve ilgili kişinin tespitini sağlayan bir biçimde muhafaza edilmelerini temin etmelidir…*"

belirtmek suretiyle söz konusu verilerin saklanmasının başvuranların özel hayatına ölçülülük sınırını aşan bir şekilde bir müdahale teşkil ettiğini ve bu durumun demokratik bir toplumun gerekliliği de olmadığını belirterek Sözleşme'nin 8 inci maddesinin ihlâl edildiğine karar vermiştir ("Tematik Bilgi Notu", 2015). Anılan karardan da görüleceği üzere, iç hukukta yer alan düzenlemelerin dahi ölçülü olması ve amacını aşmaması önem arz etmekte olup aksi takdirde bu durum özel hayatın gizliliğine aykırı olacaktır. İşlenen veriler amaca uygun ve amacın gerçekleşmesine yetecek ölçüde işlenmelidir. Gereğinden fazla veyahut amacı aşan verilerin işlenmesi hukuka aykırı olacaktır ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin ihlâl edilmesine yol açacaktır. Ölçülülük ilkesinden kasıt, veri işleme ile gerçekleştirilmesi hedeflenen amaç arasında makul bir dengenin kurulması; yani veri işlemenin amacı gerçekleştirecek doğrultuda yeterli olmasıdır (Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2018). Örneğin, spor salonuna başvururken kişinin felsefi görüşüne ilişkin bilgi talep edilmesi ölçülülük ilkesini aşacaktır.

Ölçülülük ilkesi, özellikle mahremiyet ve güvenlik hususlarının karşılaştırılmasında büyük rol oynamaktadır. Zira, somut olaya göre bazı durumlarda güvenlik ön plana çıkarken bazı durumlarda ise mahremiyetin öne çıktığı görülmektedir. Biyometrik veri gibi kişilere ait olan, ömür boyu değişme olasılığı az olan ve başkaları tarafından elde edilmesi halinde telafisi neredeyse imkânsız sonuçlar doğuracak verilerin işlenmesi bakımından ölçülülük ilkesi büyük önem arz etmektedir. Kişisel verilerin Anayasada düzenlenen temel hak ve özgürlükler kategorisinde olduğu hususu da değerlendirildiğinde mahremiyet kavramı kişisel verilerin işlenmesi bakımından öncelikle önem teşkil edecektir.

Güvenlik mi mahremiyet mi ön planda olmalı sorusunda öncelikli olarak ölçülülük prensibi gündeme gelecektir. Amaçsal yorum da gözetildiği takdirde ölçülülüğün gerektirdiği değerlendirme sonucunda güvenlik unsuru ağırlıklı ise güvenliğin sağlanması açısından biyometrik verilerin alınması şart ise ve başka bir alternatifi yoksa bu takdirde biyometrik verilerin işlenmesinde istisnalar söz konusu olabilecektir. Biyometrik verilerin güvenlik amaçlı işlenebilmesi için kanuni dayanakların bulunması da gerekmektedir. GVKT uyarınca da düzenlendiği üzere, teknik işlemeden geçirmek suretiyle kişilerin kimliklerinin belirlenmesi söz konusu olmaktadır ve bu suretle kişilerin kamera kayıtları biyometrik veri niteliğini haiz olarak değerlendiriliyordu. Nitekim, çeşitli ülkelerde de güvenlik amaçlı kişilerin görüntüleri ayrıntılı şekilde alınabilmektedir. Kanun veya ilgili düzenlemeler uyarınca kamu güvenliğinin gerektirdiği hallerde biyometrik verilerin hukuka uygun olarak işlenmesi söz konusu olabilmektedir. Emniyet Genel Müdürlüğü'nün 25.10.2017 tarihli 2017/7 numaralı Bakanlık Genelgesi'nde

> *"(…) Bakanlığımıza bağlı kolluk birimleri de suç ve suçlularla mücadele faaliyetleri kapsamında müdahale ettikleri olaylara ilişkin elde ettikleri görüntüleri ilgili mevzuatla düzenlenen kurallar çerçevesinde muhafaza etmek ve adli/idari mercilere iletmekle yükümlüdür*

> *(...) Bu paylaşımlar suç ve suçlularla mücadeleyi, temel hak ve özgürlükleri, özel hayatın gizliliğini ve kamu düzenini olumsuz etkileyen; (...)*"

belirtilmek suretiyle güvenlik amacıyla görüntü alınmış olsa dahi bunun mevzuat doğrultusunda işlenmesinin ve yetkili kişilerle gerektiği takdirde paylaşılmasının gerekliliği vurgulanmıştır. Emniyet Genel Müdürlüğü'nün 25.10.2017 tarihli 2017/7 numaralı Bakanlık Genelgesi'nde yer alan düzenlemelerinde ölçülülük prensibinin bir uzantısı olduğunu söylemek mümkün olacaktır. Görüntülerin alınma amacı güvenlik olup gerektiği takdirde yetkili kişilere verilmesi suretiyle alınan kayıtlardır. Bu tür görüntülerin sosyal medyadan, basın yoluyla veyahut yetkisiz kişilerle paylaşılması durumunda amacını aşacaktır dolayısıyla ölçülülük ilkesini de bertaraf etmiş olacaktır.

Kişisel Verileri Koruma Kurulu (Kurul) da spor hizmeti sunan veri sorumlularının üyelerinin giriş ve çıkışta el-avuç okutma sistemine geçilmesi, kaydı tutulan üyelere ait vesikalık fotoğraf, son ziyaret saati gibi bilgilerin herkesin görebileceği bir TV ekranında yansıtılması gibi biyometrik verileri de içeren bazı özel nitelikli kişisel verileri işlemesine ilişkin karar özetinde

> *"(...) Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinde de, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin ancak hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,*
>
> *Bu ilkelerden, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin, işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemesi gerektiği,(...)*
>
> *Öte yandan, Article 29 Working Party tarafından hazırlanan WP193 sayılı "Opinion 3/2012 on Developments in Biometric Technologies" başlıklı dokümanda, yer alan örnekte bir fitness kulübüne ya da spor salonuna sadece üyelerin girişini ve ilgili hizmetlere erişimini sağlamak için tüm müşterilerin ve personelin parmak izinin depolanarak işlenmesi, kulübe erişimi kolaylaştırma ve abonelikleri yönetme ihtiyacı ile orantısız olarak değerlendirildiği ve böyle bir uygulama yerine, basit bir kontrol listesi ya da RFID etiketlerinin kullanımı ya da biyometrik verilerin işlenmesini gerektirmeyen bir manyetik bantlı kart gibi farklı önlemler kullanılarak da aynı ihtiyaçların karşılanabileceği ifadelerine yer verildiği dikkate alındığında spor salonuna giriş için veri sorumluları tarafından uygulanan "el ve parmak izi taraması" sisteminin, hizmetten faydalanmak için zorunlu ve tek yol olarak üyelere sunulmasının, kişisel verilerin işlenmesinde ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olarak değerlendirilmediği*"

şeklinde ifade ederek ölçülülük ilkesinin her zaman gözetilmesi gerekliliğini vurgulamıştır (Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti, 2019). Kurul kararında da vurgulandığı üzere, kişisel verilerin işlenme şartları bulunsa dahi kişisel verilerin işlenmesine ilişkin genel ilkeler öncelikli olarak göz önünde bulundurulmalıdır. Diğer bir deyişle, kişisel verinin işlenirken hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun olarak işlenmesi, daha sonra açık rıza veya diğer kişisel verilerin işlenme şartları söz konusu olmalıdır. Örnek olarak, ölçülülük ilkesine aykırı bir kişisel

veri işleme faaliyetini açık rıza alınması suretiyle hukuka uygun hale getirmek mümkün değildir; ölçülülüğü aştığı takdirde o verinin hiçbir suretle işlenmemesi gerekmektedir.

6698 sayılı Kanun'da düzenlenen ölçülülük ilkesi, GVKT'deki veri minimizasyonu ilkesiyle örtüşmektedir. GVKT'nin 5(1) maddesinin c bendinde veri minimizasyonu prensibi, "yeterli, ilgili ve veri işleme amaçları doğrultusunda gerekli olduğu şekilde sınırlı olması" biçiminde tanımlanmıştır. Bu ilkeye göre, veri sorumlusunun amacına ulaşmak için gereğinden fazla veri temin etmemesi ve veri sorumlusunun amaçlarına ulaşmak için kişisel verileri işlenmesinin şart olup olmadığının değerlendirilmesi, şart olmadığı sonucuna varılırsa; yani kişisel verileri kullanmadan veya sadece bir kısmı kullanılarak hedefe ulaşması mümkün ise öncelikli olarak bu yolu tercih etmesi gerektiği ifade edilmektedir (Develioğlu, 2017). GVKT, veri minimizasyonunu tanımlarken "yeterli, alakalı ve işlendikleri amaçla bağlantılı" sıfatlarını kullanmıştır; ancak bu kavramların tanımını yapmamıştır. İngiltere Veri Komisyonunun (ICO) sayfasında ölçülülük ilkesine ilişkin birtakım örneklere ve kriterlere yer verilmiştir. ICO'ya göre, kişisel verilerin yeterli ölçüde alınıp alınmadığından emin olmak için öncelikle bu veriye neden ihtiyaç duyulduğu sorusu cevaplanmalıdır ("Principle (c): Data minimisation", t.y.). Özel nitelikli kişisel verilerde ise sadece asgari miktarda bilginin toplandığından ve saklandığından emin olmak önem teşkil etmektedir. Bununla birlikte, amaç kapsamında sahip olunması gereken veriden daha fazlası tutulmamalıdır; amaçla bağdaşmayan nitelikte veriler tutulmamalıdır. Benzer şekilde, gelecekte lazım olabileceği düşüncesiyle gereğinden fazla veriyi toplamak da ölçülülük ilkesinin ihlâl edilmesine neden olacaktır ("Principle (c): Data minimisation", t.y.). Açık kaynak verilerin işlenmesinde ise bu verilerin kamuya açık olması veriler üzerinde sınırsız tasarruf edilebileceği anlamına gelmemektedir. Tam aksine, açık kaynaktan kişileri tanımlamaya yarayan kişisel verilerin elde edilip bu verilerle yeni kayıtlar/profiller oluşturulacağı zaman, bu veriler kişileri belirlenebilir kılacağı için kişisel veri sayılacaktır ve işleme faaliyetinin gerçekleşebilmesi için yasal dayanakların olması gerekmektedir (Snijder, 2016). Dolayısıyla, ölçülülük kavramı açık kaynaklı verilerin kullanımında da söz konusu olabilmektedir.

Veri sorumluları, tutulan kişisel verilerin amaçları için uygun ve yeterli olup olmadığını kontrol etmek için işlemlerini düzenli aralıklarla gözden geçirmeli ve ihtiyaç duymadıkları verileri silmelidir. Bunlara ek olarak, tutulan veriler amacın gerçekleşmesine etki etmiyorsa veyahut ilgili kişi eksik verisinin olması dolayısıyla kişisel verisini düzeltme talebinde bulunursa tutulan verilerin yeterli olmadığı sonucuna ulaşılmaktadır ("Principle (c): Data minimisation", t.y.). Veri minimizasyonu ilkesine örnek olarak, bir iş bulma merkezi kendisine başvuranların ilgi alanları doğrultusunda onlara çeşitli iş seçenekleri sunmaktadır. Merkez, özel iş çeşitleri bakımından başvuruculara işe dair sağlık koşulları varsa bunlara ilişkin soruları da içeren genel bir anket yollayabilir; ancak ofis işi için başvuran kişiden bu tür bir bilgiyi elde etmek ilgisiz ve aşırı olacaktır ("Principle (c): Data minimisation", t.y.). Bu da veri minimizasyonu ilkesinin bir uzantısı olarak kabul edilebilecektir. Veri minimizasyonu ilkesi sadece yeterli miktarda kişisel verinin toplanması meselesi değildir; aynı zamanda bu verilere erişilmesi, daha fazla işlemeye ve/ya paylaşmaya gerek olup olmadığı, kullanılma amaçları ve saklanma sürelerini de kapsamaktadır. İşleme faaliyeti mümkün olduğunca minimize edilmelidir (Snijder, 2016).

Özetle, ölçülülük ilkesi gereği, veriler gerektiği ölçüde işlenmelidir ve amaca hizmet etmelidir. Gereğinden az veya fazla verinin toplanması durumlarında ölçülülük ilkesinin ihlâl edildiğini söylemek mümkün olacaktır. Bir kişisel veriyi işleme faaliyetinde kişisel veriyi işleyebilme şartları kadar kişisel veriyi işleme ilkeleri de önem arz etmektedir. Kişisel verilerin hukuka uygun olarak işlenebilmesi için faaliyetin kişisel veriyi işleme ilkelerinden herhangi birini ihlâl etmemesi gerekmektedir. Ölçülülük aynı zamanda mahremiyet mi güvenlik mi sorusu değerlendirilirken temel alınacak en önemli kavramlardan biridir. Güvenliğin sağlanması amacıyla özel nitelikli kişisel verilerin tutulması gerekli ve şart ise ve aksi durum Kanunda düzenlenmemişse, bu takdirde özel nitelikli kişisel verilerin tutulması hukuka uygun hâle gelecek, ölçülülük prensibini de ihlâl etmemiş olacaktır.

Açık Rıza

Açık rıza kavramı, kişisel verilerin hukuka uygun olarak işlenmesi şartları bakımından temel kural olarak mevzuatımızda düzenlenmektedir. Anayasanın özel hayatın gizliliği ve korunmasına ilişkin yirminci maddesi uyarınca, "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir (...) Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. (...)*" hükmedilmiştir. Anayasa kapsamında da belirtildiği üzere, kişilerin kişisel verilerinin korunmasını isteme hakkı temel haklardan biridir, bu hak Kanun ile düzenlenecektir veya kişinin açık rızası gerekecektir. Kanun'un 5 inci maddesinin ilk fıkrasına göre kişisel verilerin işlenmesi bakımından aranan temel şart, kişisel verisi işlenen ilgili kişilerin kendi verilerinin işlenmesine açık rıza vermesidir. Açık rıza kavramı, hem genel hem özel nitelikli kişisel verilerin işlenmesi bakımından hukuka uygunluk sebebi olarak öngörülmüştür (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.). Kişisel verilerin yurt içinde aktarılması (madde 8) ve yurt dışına aktarılması (madde 9) için de yine ilgili kişinin açık rızası şart olarak konulmuştur.

Kanun çerçevesinde açık rıza, kişinin kişisel verilerinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır; kişinin herhangi bir beyanda bulunmaması rıza gösterdiği anlamına gelmemektedir (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.). İlgili kişi açık rıza vermeden önce işlenecek kişisel verinin kapsamı, amacı ve sınırları hakkında yeterli bir biçimde bilgilendirilmeli; bu doğrultuda açık rızasını vermelidir. İlgili kişinin verdiği açık rıza veri sorumlusunun veri işleme faaliyeti bakımından kapsamı belirlemiş olacak; açık rıza verilen hususların dışında veri işlenmesi mümkün olmayacaktır. Açık rızanın şekline ilişkin olarak ise diğer mevzuat hükümleri saklı kalmak üzere herhangi bir şekle tabi değildir. Yani, açık rıza yazılı olarak alınabileceği gibi elektronik ortam ve çağrı merkezi vb. yollarla da alınabilir. Açık rızanın verildiğine ilişkin ispat yükü veri işleyene aittir (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.).

Açık rıza kavramı için 6698 sayılı Kanun üç husus aramaktadır. 6698 sayılı Kanun uyarınca, açık rızanın temel unsurları başlıca;

- Belirli bir konuya ilişkin olması,
- Rıza açıklamasının bilgilendirilmeye dayanması,
- Kişinin herhangi bir etki altında kalmaksızın özgür iradesiyle beyan açıklamasında bulunmasıdır.

Bu çerçevede, açık rızanın tanımında yer alan ilk kavram "*belirli bir konuya ilişkin olmak*"tır. Belirli bir konuya ilişkin olmak, ilgili kişinin neye rıza verdiğini bilerek kişisel verisini paylaşmaya rıza göstermesidir. Veri sorumlusu, ilgili kişiye açık rıza beyanının kapsamını ve hangi konuya ilişkin olduğunu açıkça belirtmelidir. Diğer bir deyişle ilgili kişi, hangi amaç için ve hangi kapsamda kişisel verisini paylaşacağını bilmelidir. İlgili kişinin genel bir tabir ile "*kişisel verilerimi işlemenize rıza gösteriyorum*" gibi muğlak ve açık uçlu rıza göstermesi 6698 sayılı Kanundaki açık rıza kavramı kapsamında değerlendirilemeyecek olup kanuna aykırı nitelikte olacaktır, dolayısıyla rıza geçersiz sayılacaktır (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.).

Kişinin birden çok konu için kişisel verisini paylaşması gerekiyorsa, ilgili kişi rızayı hangi verilerin ne amaçla işleneceğini bilerek bunları belirterek rızayı vermiş olması gerekmektedir. Kişi açık rıza gösterdikten sonra kişisel verisi veri kullanımından sonra üçüncü bir kişi ile paylaşılacaksa, yurt dışına aktarılacaksa ve buna benzer durumlarda ilgili kişinin rızasının tekrar alınması gerekecektir (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.).

Açık rıza kavramının tanımında yer alan ikinci unsur ise "bilgilendirme"dir. Açık rıza bir irade beyanı olup kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini ve bu rızanın sonuçlarını bilmesi gerekir (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.). Yani, bilgilendirme hangi konuya rıza gösterileceği ile birlikte bu rızanın sonuçlarına ilişkin tam bir bilgilendirmeyi kapsamalıdır.

Bu husus, 6698 sayılı Kanun'un "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı onuncu maddesinde de belirtilmektedir. 6698 sayılı Kanun'un 10 uncu maddesine göre, veri sorumluları, hangi konuya ilişkin kişisel verilerin paylaşılacağı ve rızanın sonuçları hakkında ilgili kişileri bilgilendirmekle yükümlüdür. Her ne kadar aydınlatma yükümlülüğü 6698 sayılı Kanunda kişisel verileri işleme şartlarından sayılmamış ve ayrı bir yükümlülük olarak kabul edilmiş olsa da, aydınlatma yükümlülüğü eksiksiz olarak yerine getirildiği takdirde açık rızanın tanımında yer alan bilgilendirme unsurunun da eksiksiz şekilde gerçekleştiği kabul edilebilir.

Bilgilendirme, kişi açık rızasını vermeden önce yapılmalıdır (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.). Bilgilendirme doğru bir şekilde yapılmalıdır ve kişinin vereceği açık rıza da bu bilgilendirmenin sonucunda gerçekleşmelidir. İlgili kişiden alınan açık rızanın kapsamı sadece bilgilendirildiği konuya ilişkindir. Başka bir konuda kişisel verilerinin işlenmesi gerekiyor ise ayrıca bilgilendirme yapılıp ilgili kişinin rızasının alınması gerekmektedir. Bilgilendirme yapılırken elde edilecek kişisel verilerin hangi amaçlarla kullanılacağı açıkça belirtilmeli, kişinin anlamayacağı terimler ya da yazılı bilgilendirme yapıldığında okumakta güçlük çekeceği oranda küçük puntolar kullanılmamalıdır (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.).

Açık rızanın tanımlanması için kullanılan son kavram da "*özgür iradeyle açıklanma*"dır. Özgür iradeyle açıklanma unsuru, ilgili kişilerin belirli bir konu hakkında bilgilendirildikten sonra hiçbir etki altında kalmaksızın bilinçli olarak ve kendi kararı çerçevesinde kişisel verisini paylaşmaya rıza göstermesidir. Örneğin, 6098 sayılı Türk Borçlar Kanunu'nda da tanımı yapılan iradeyi sakatlayan durumlar (cebir, aldatma, yanıltma, korkutma) var ise özgür bir iradenin varlığından söz edilemez. Rızayı sakatlayan bir durumun mevcudiyeti belirlenirken her durum ayrı ayrı değerlendirilerek rızayı etkilemenin derecesi belirlenmelidir (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.).

Tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerekir. Özellikle işçi-işveren ilişkisinde, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.).

Açık rızanın bir ürün veya hizmetin sunulmasının ya da bunlardan yararlanılmasının ön şartı olması, rızada yer alan özgür irade ile açıklanması unsurunu sakatlayacağı için hukuka aykırı olacaktır. Örneğin, bir ürünün satılması veya bir hizmetten faydalanılması için kişinin zorla kişisel verilerini paylaşmak zorunda bırakılması söz konusu olabilmektedir. Kişilere, kişisel verilerini paylaşmazlarsa o hizmetten faydalanamayacakları belirtilmek suretiyle kişilerin rıza göstermeleri için baskı olabilmektedir. Yine benzer bir şekilde, kişilerin bir hizmetten yararlanılmasının üyelik şartına bağlandığı yerlerde, üye olmak isteyen ilgili kişinin parmak izinin alınması ve işlenmesinin üyelik sözleşmesinin kurulması için zorunluluk olarak öngörülmesi hukuka aykırılık teşkil edecektir; çünkü bu şekilde alınan açık rıza özgür irade ile açık rıza verilmesi ilkesine ve ölçülülük ilkesine aykırı olacaktır (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.).

6698 sayılı Kanun'un oluşturulma sürecinde rol oynayan 95/46 EC Sayılı Avrupa Birliği Direktifi'ne göre açık rıza kavramı ülkemizdeki mevcut düzenlemeyle benzer şekilde düzenlenmiştir; ancak bu direktif kapsamında açık rıza sadece özel nitelikli kişisel verilerin işlenmesi bakımından düzenlenmiştir (Kişisel Verileri Koruma Kurumu Açık Rıza Rehberi, t.y.). Güncellenen GVKT çerçevesinde ise rıza kavramı Kanunda yer alan açık rıza kavramına benzer bir şekilde düzenlenmiştir. GVKT'nin "*Tanımlar*" başlıklı 4 üncü maddesinin (11) numaralı fıkrası uyarınca ilgili kişinin rızası "*ilgili kişinin özgürce, o konuya ilişkin yeterli bilgi sahibi olarak ve belirsizliğe mahal vermeyecek şekilde irade beyanını dile getirmesi veyahut kendisine ilişkin kişisel verinin işlenmesini kabul ettiğine ilişkin açık olumlu hareketi*" olarak tanımlanmıştır. Tanımdan da anlaşıldığı üzere, GVKT uyarınca kişinin sessiz

kalması kişisel verisinin işlenmesine izin verdiği anlamına gelmeyecektir; çünkü tanımda ilgili kişinin beyanı veya açık olumlu hareketi rızanın unsurlarından biri olarak sayılmıştır.

Biyometrik Verilerin İşlenmesinde Açık Rıza ve Ölçülülük İlkesinin Karşılaştırılması

Açık rızanın 6698 sayılı Kanunda kişisel veriyi işleme şartı olduğunu ve hizmet şartına bağlanamayacağını üst başlıklarda belirtmiştik. Her ne kadar ilgili kişi açık rıza vermiş olsa da bazı durumlarda açık rızanın sakatlanacağı söylenebilir. Bir kişisel veri işlenirken açık rıza verilmiş ancak kişisel verilerin işlenmesi ilkelerine aykırı bir işleme gerçekleşmişse bu kişisel verinin hukuka uygun olarak işlendiğini belirtmek mümkün olmayacaktır. Zira, bir kişisel verinin hukuka uygun olarak işlenebilmesi için kişisel verilerin hem genel ilkeler hem de işleme şartları çerçevesinde işlenmesi gerekmektedir. 6698 sayılı Kanun'un 4 üncü maddesinin birinci fıkrasında da hükmedildiği üzere, kişisel veriler ancak Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. Kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerinin bulunması zorunludur. Mevzuatlarda herhangi bir istisna öngörülmediği takdirde hem genel nitelikli hem özel nitelikli kişisel verilerin işlenmesinde ilkeleri ve şartları bir arada değerlendirmek gerekmektedir.

Birleşik Krallıklarda yapılan bir araştırmaya göre katılımcıların %45'i biyometrik verinin oldukça hassas nitelikte olduğunu belirterek bu tarz verilerin sıkı hukuk kurallarıyla korunması hususunda güçlü bir argüman oluşturmuştur (Freitas, Moreira, Andrade, 2017). Biyometrik verilerin işlenmesinde, açık rızanın bulunduğu hallerde dahi yasal kısıtlamalar söz konusu olabilecek; somut olay doğrultusunda ölçülülük ilkesi de gözetilecektir. Biyometrik veriler özel nitelikli veri olup kişilerin kimliğinin ayırt edilmesine ve doğrudan teşhisini sağlayan en önemli verilerden biridir. Kişinin sahip olduğu bu veri ömrü boyunca neredeyse hiç değişmeyecek olup bu verinin hukuka aykırı olarak işlenmesi halinde telafisi imkânsız sonuçlar doğabilecektir. İlgili kişi her ne kadar biyometrik verisinin işlenmesine açık rıza göstermiş olsa da bu verilerin özellikle işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması gerekmektedir. Örnek olarak, ilgili kişi bir spor salonu hizmetinden faydalanmak için parmak izinin alınmasına açık rızasını göstermiş ve spor salonu parmak izini güvenlik amacıyla da almış da olsa; bu durum ilgili kişinin kişisel verilerinin korunması hakkına yoğun bir şekilde müdahale etmektedir (Yücedağ, 2019). İşleme, ilgili kişinin rızası hukuka uygunluk sebebine dayansa da işlenen veri, işleme amacı kapsamında yeterli olanın ötesindeyse işlemenin genel ilkelere aykırılık teşkil ettiği söylenebilecektir (Yücedağ, 2019).

Ölçülülük ilkesi, kişilerin mahremiyetlerinin korunması hususu ile yakın ilişkilidir. 6698 sayılı Kanun'un henüz mevcut olmadığı zamanlarda yargı organları kişisel verilerin işlenmesine temel hak ve özgürlüklerin ihlâl edilmemesi ve ölçülülük kavramlarını irdelemekte idi. Nitekim Anayasa Mahkemesi'ne göre ölçülülük ilkesinde amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gerekliliği ifade edilmektedir (Akgül, 2015). Diğer bir deyişle ifade etmek gerekirse, kişisel verilerin toplanması ve işlenmesi sırasında kişisel verilerin korunması hakkına en az zararı verecek en uygun aracın seçilmesi ölçülülük ilkesinin bir gereğidir (Akgül, 2015).

Danıştay 11. Daire, belediye 2017/816 Esas; 2017/4906 Karar numaralı, 13 Haziran 2017 tarihli kararında personelinin mesai giriş çıkış saatlerinin tespitini sağlanmak amacıyla işçilere yüz tarama sistemi uygulaması ile ilgili başvuru hakkında, kamusal alana ilişkin olsa bile özel hayatın gizliliği bakımından bu verilerin ileride kullanılmayacağına ilişkin herhangi bir teminatın da bulunmadığı gerekçesiyle mesai giriş çıkış takibinin yüz tanıma sistemiyle yapılmasını Anayasaya aykırı bulmuştur. Danıştay'ın mezkûr kararında mesai takibinde biyometrik verilerin işlenmesinin özel hayatın gizliliğine aykırı olduğu vurgulanmakla birlikte, Danıştay'ın mahremiyet hususunu değerlendirirken ölçülülük

ilkesini de göz önünde bulundurduğunu söylemek yerinde olacaktır. Zira mahremiyet ve ölçülülük ilkesi birbiriyle ilişkili olup kişisel verilerin işlenmesinde yeterli sınırı belirlemede büyük önem teşkil etmektedir. Nitekim idare mahkemesinin kamu personelinin parmak izinin alınmasında her ne kadar mesaiye etkin bir katılım gözetilmiş olsa da hedeflenen amaç ile personelin parmak izinin alınması arasında orantısızlık bulunması gerekçesiyle özel hayatın gizliliğinin ihlâl edildiği yönündeki kararı Danıştay tarafından onanmıştır (Akgül, 2015).

SONUÇ

Biyometrik veriler, kişilerin ayırt edilebilmesini sağlayan her türlü biyolojik ve davranışsal özelliklerin bütünüdür. Biyometrik verilerin getirdiği avantajlar kadar dezavantajlar da bulunmaktadır. Biyometrik veriler kişiye ait veriler olduğu için bu verilerin şifre gibi unutulma olasılığı yoktur. Diğer taraftan, biyometrik veri sistemlerinde kişinin kimliğini tespit etme noktasında hata oranı da azdır ve bu suretle sahteciliğe karşı da yüksek derecede koruma sağlamaktadır. Ancak belirtmekte fayda görülmektedir ki biyometrik veriler ile her ne kadar kişinin kimlik doğrulaması konusunda sahtecilik ve dolandırıcılık tehlikelerinin önüne geçilmiş olsa da biyometrik yöntemlerin uygulanmasında güvenlik ve mahremiyet hususları birbirleri ile çelişmektedir. Biyometrik veriler kişilerin mahremiyeti ile alakalı olup bu verilerin ifşası durumu ilgili kişiler açısından büyük sıkıntı doğurabileceği için bu tür verilerin işlenmesi ve ifşası gibi durumlar sıkı kurallara tabidir. Nitekim 6698 sayılı Kanun'un 6 ncı maddesine göre, ilgili kişinin açık rızasının bulunmadığı durumlarda biyometrik veriler ancak kanunlarda öngörülen hallerde işlenebilecektir. Bir verinin biyometrik veri olup olmadığını anlamakta temel alınan en önemli unsurlardan biri, işleme sonucunda kişinin kimliğinin teşhis edilip edilmediği noktasıdır. Örneğin, telefon bankacılığında sistemin ilgili kişinin sesini algıladıktan sonra o kişiyi tespit edip işlem yaptırması durumunda alınan ses kaydı biyometrik veri işleme niteliğini haiz olacaktır. Diğer taraftan, bankacılık hizmetlerinde alınan ses kaydı sadece içerik bakımından kaydediliyor ise (hakaret içerip içermediği, hizmet kapsamında konuşulanların içeriğinin ispat edilmesi gibi) bu faaliyet (genel) kişisel veri işleme faaliyeti niteliğini taşıyacaktır.

Bununla birlikte KDTS sistemleri de irdelendiği takdirde, kameralardan alınan biyometrik özellikli verilerin hangi kaynaklardan alındığı öncelikli olarak irdelenmelidir; zira bu tür verilerin Facebook, Instagram gibi sosyal medya siteleri üzerinden veya basın yoluyla veyahut yetkisiz bir mecradan alınmış olması halinde bu durum hukuka aykırılık teşkil edecektir. Benzer şekilde, ilgili görüntüleri işleme amacı da önem teşkil etmektedir. Bu çerçevede, kişinin kimliğini teşhis etmek amaçlı bir veri işleme faaliyeti gerçekleştiriliyorsa söz konusu veri işleme faaliyeti biyometrik veri işleme faaliyeti olarak kabul edilecektir. Diğer taraftan, herhangi bir kimlik teşhisi elde edilmeyecek şekilde işlenen veriler ise kişisel veri niteliğini haiz olacaktır.

Kişisel verilerin işlenmesine ilişkin ilkeler, 6698 sayılı Kanun'un 4 üncü maddesinde düzenlenmiştir. Kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulması zorunludur. Bu ilkelerden işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi, özellikle biyometrik verilerin işlenmesi noktasında önem teşkil etmektedir. Anılan ilke, gerek uluslararası içtihat bakımından (AİHM kararları, GVKT, diğer ülkelerin kişisel veri mevzuatı) gerek ulusal mevzuatımızda yer alan 6698 sayılı Kanun bakımından özel hayatın gizliliği bağlamında temel olarak gözetilen ilkelerden biridir. Bu noktada belirtmekte fayda görülmektedir ki mahremiyet ve güvenlik kavramları arasında sıkı bir ilişki bulunmakta olup hangisinin önem kazanacağı belirlenirken somut olayın koşulları ve ölçülülük ilkesi önem teşkil etmektedir. Yukarıda anılan AİHM kararlarında

da belirtildiği üzere, mahremiyet hakkı ile diğer menfaatler arasında bir denge gözetilmesi ve ölçülülük hususları göz önünde bulundurulmalıdır. Ölçülülük ilkesine göre sadece gerekli olduğu kadar veri işlenmeli, gelecekte işe yarayabilir düşüncesiyle hareket edilerek veri işlenmemelidir. Veri işlemenin sınırları belirlenirken verileri işleme amacı göz önünde bulundurulmalıdır.

Kişisel verilerin işlenmesinde açık rıza bulunsa dahi, kişisel verilerin işlenmesi ilkeleri her zaman gözetilmelidir. Diğer bir deyişle, kişisel verilerin işlenmesi ilkeleri ve şartları bir bütün değerlendirilmeli; özellikle özel nitelikli verilerin işlenmesinde ölçülülük ilkesi irdelenmelidir. Biyometrik verinin 6698 sayılı Kanun'un 6 ncı maddesinde yer alan düzenleme dâhilinde işlenmesi durumunda (kanunlarda öngörülmesi veya açık rızanın bulunması) dahi, bu verilerin hukuka uygun olarak işlenebilmesi için her hâl ve koşulda 6698 sayılı Kanun'un 4 üncü maddesi gözetilmelidir. Nitekim Kurul kararlarında da belirtildiği üzere, biyometrik verilerin işlenmesinde özellikle ölçülülük ilkesi her zaman gözetilmelidir. Somut olaylara göre mahremiyet ve güvenlik arasında değerlendirme yapılmalı; makul ölçüde biyometrik veri yerine alternatif olanaklar var ise (RFID kartları gibi) bu yöntemler kullanılmalıdır. Alternatifin bulunduğu durumda yine de biyometrik verilerin işlenmesi yoluna gidilmesi Kurul tarafından ölçülülüğe aykırı olarak değerlendirilmektedir. Açık rıza hukuka uygun olarak alınmış olsa bile, kişisel verilerin işlenmesi ilkelerinden herhangi birinin ihlâli söz konusu ile işleme faaliyeti de hukuka aykırı sayılacaktır. Yukarıda da belirtildiği üzere, Danıştay kararlarında da ölçülülük ilkesi gözetilerek mesai takibi yapılması suretiyle işlenen biyometrik verilerin özel hayatın gizliliğini ihlâl ettiği hususu vurgulanmıştır. Bütün bu açıklamalar doğrultusunda, alternatifin bulunduğu durumlarda biyometrik verilerin işlenmesi, yine mesai amacıyla veya çeşitli (spor merkezi gibi) mekânlara giriş esnasında biyometrik verilerin işlenmesi ölçülülüğü aşacak olup ilgili kişinin açık rızası olsa dahi bu veri işleme faaliyeti hukuka aykırı olacaktır. Kaldı ki açık rıza unsurları da göz önünde bulundurulduğu takdirde bir işçinin işverenine açık rıza göstermesi noktasında o açık rızanın "*özgür irade*" ile verilemeyeceği aşikârdır. Benzer şekilde, mekânlar tarafından işlenecek biyometrik verilerde açık rıza verilmeden önce biyometrik verilerin işlenmesi hususu hizmet şartına bağlanmış olacak, bu noktada yine "*özgür irade*" ile açık rızanın verilmesi unsuru sağlanamayacaktır.

KAYNAKLAR

Akgül, A. (2015). Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı, *TBB Dergisi*. (118). 199-222.

Arslan, B. ve Sağıroğlu, Ş. (2016). Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme, *Politeknik Dergisi*, 19 (2). 101-114.

Biometrics in identity: Buiding inclusive futures and protecting civil liberties. (2019). Secure Identity Alliance: https://secureidentityalliance.org/publications-docman/public/156-biometrics-in-identity-building-inclusive-futures-and-protecting-civil-liberties/file adresinden 12.04.2020 tarihinde alınmıştır.

CCTV Güvenlik Kamera Kurulumu, Model ve Özellikleri Hakkında Tavsiyeler. (t.y.). Karel: https://www.karel.com.tr/blog/cctv-guvenlik-kamera-kurulumu-model-ve-ozellikleri-hakkinda-tavsiyeler adresinden 10.04.2020 tarihinde alınmıştır.

Coraggio, G. (2019). Are your customers' images biometric data under the GDPR? https://www.gamingtechlaw.com/2018/07/image-biometric-data-picture-gdpr.html adresinden 17.04.2020 tarihinde alınmıştır.

Develioğlu, H. M. (2017). *6698 Sayılı Kişisel Verilerin Korunması Kanununu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha Yayıncılık.

Erdinç, G. H. (2017). B*ilgi Güvenliği, Kişisel Verilerin Korunması ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler* (Yayımlanmış yüksek lisans tezi). İstanbul Teknik Üniversitesi Bilişim Enstitüsü.

Eye Biometrics. (t.y.). MIS Biometrics; http:// misbiometrics.wikidot.com/eye adresinden 15.04.2020 tarihinde alınmıştır.

Fingerprinting Criticism. (t.y.). Fingerprint Zone: http:// www.fingerprinting. com/fingerprinting-criticism.php. adresinden 15.04.2020 tarihinde alınmıştır.

Freitas, P. M., Moreira, T. C., & Andrade, F. (2017). Data Protection and Biometric Data: European Union Legislation. Jiang, R., Al-maadeed, S., Bouridane, A., Crookes, P. D. ve Beghdadi, A. (Ed.). *Biometric security and privacy: Opportunities & challenges in the big data era* içinde (s.413-423). İsviçre: Springer International Publishing

Han F. ve Hu J. ve Kotagiri R. (2012). Chapter 19 Biometric Authentication For Mobile Computing Applications, Li H., Toh K. A.. ve Li L. (Ed.) *Advanced Topics In Biometrics* içinde (s.461-47). Singapur: World Scientific

Kişisel Verileri Koruma Kurumu. (2018). *Kişisel Verilerin Korunmasına İlişkin Uygulama Rehberi*. Ankara: KVKK Yayınları

Kişisel Verileri Koruma Kurumu. (t.y.). Açık Rıza. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf adresinden 15.04.2020 tarihinde alınmıştır.

Krishan, R., & Mostafavi, R. (2018). Biometric Technology: Security and Privacy Concerns. *Journal of Internet Law*, 22(1), 19-23.

Pjhlaw. (2020). Lopez Ribalda and Others v Spain. https://pjhlaw.co.uk/2020/01/10/lopez-ribalda-and-others-v-spain/ adresinden 04.04.2020 tarihinde alınmıştır.

Principle (c): Data minimisation. (t.y.). Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ adresinden 16.04.2020 tarihinde alınmıştır.

Sanchez-Reillo R. ve Ortega-Fernandez I. ve Ponce-Hernandez W. ve Quiros-Sandoval, H. C. (2017). How to implement EU data protection regulation for R&D on personal data. *2017 International Carnahan Conference On Security Technology (ICCST)*. IEEE

Satapathy, S. C. ve Joshi, A. (2017). *Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1 Smart Innovation, Systems and Technologies (83))* (1st ed. 2018 ed.). Springer.

Sellers, F. (2018). The GDPR's Impact on CCTV and Workplace Surveillance. https://www.securityprivacybytes.com/2018/02/the-gdprs-impact-on-cctv-and-workplace-surveillance/ adresinden 10.04.2020 tarihinde alınmıştır.

Sherman, K. (2019). Biometrics: The Future Is In Your Hands. https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=3010&context=llr adresinden 12.04.2020 tarihinde alınmıştır.

Snijder, M. (2016). Biometrics, surveillance and privacy. https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf adresinden 29.03.2020 tarihinde alınmıştır.

Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti. (2019). Kişisel Verileri Koruma Kurumu: https://kvkk.gov.tr/Icerik/5496/2019-81-165 adresinden 12.04.2020 tarihinde alınmıştır.

Tematik Bilgi Notu – Kişisel Verilerin Korunması. (2015). T.C. Adalet Bakanlığı Basın Birimi: https://www.echr.coe.int/Documents/FS_Data_TUR.pdf adresinden 10.04.2020 tarihinde alınmıştır.

Yücedağ, N. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 75(2), 765-790.

Yücedağ, N. (2019). Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, *Kişisel Verileri Koruma Dergisi*, 1 (1), 47-63.

Wilson, T. V. (t.y.). How Stuff Works, How Biometrics Works: Voiceprints. http://science.howstuffworks.com/biometrics3.htm adresinden 28.03.2020 tarihinde alınmıştır.