www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt:5 Sayı:1

Geliş:04.05.2023
Kabul:23.06.2023

Yüz Tanıma Teknolojilerinin Kişisel Verilerin Korunması Hukuku Açısından İncelenmesi

Sertel ŞIRACI
Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü Öğretim Görevlisi
Beşiktaş, İstanbul, Türkiye
sertel.siraci@sch-legal.com
ORCID: https://orcid.org/0000-0002-1560-5446

ÖZ
Bireylerin yüz şekli üzerinden tespit edilen veriler 6698 Sayılı Kişisel Verileri Koruma Kanunu m.6 hükmüne göre özel nitelikli kişisel veridir. Biyometrik yöntemlerle kişisel verilerin işlenmesi kişilerin temel hak ve özgürlüklerinin korunması kapsamında Anayasal hak olarak güvence altına alınmıştır. Kanun hükümleri kapsamında ortaya konulan hukuksal koruma sınırları çerçevesinde koruma altında olduğuna şüphe yoktur. Bir yanda teknolojinin sağladığı büyük kolaylıklar varken diğer yanda temel ve özgülüklerin ihlali ihtimali vardır. Geçmişte sinema filmlerine konu olup içselleştirdiğimiz kullanımlar, bugün gerçek hayatta uygulamaya geçirilmiştir. Yüz tanıma teknolojisinin kullanım oranına paralel olarak temel hak ve özgürlüklere bilinçli veya bilinçsiz müdahale de artmaktadır. Bu çalışmada yüz tanıma teknolojisi, kişisel verilerin korunması hukukunun temel ilkeleri açısından ele alınırken uygulama örnekleri, kurgusal ihtimaller, mevzuat ve kararlar kapsamında konu değerlendirilecektir.
Anahtar Sözcükler: Anahtar Sözcükler: Kişisel Veri, Özel Nitelikli Kişisel Veri, Biyometrik Veri, Yüz Tanıma, Açık Rıza

Examination Of Face Recognition Technologies From The Perspective Of Personal Data Protection Law

ABSTRACT
The data determined through the face shape of individuals are sensitive personal data according to the Article 6 of the Personal Data Protection Law No. 6698. The processing of personal data by biometric methods is guaranteed as a constitutional right within the scope of the protection of fundamental rights and freedoms of individuals. There is no doubt that it is under protection within the framework of the legal protection limits set forth under the provisions of the law. On the one hand, there are great conveniences provided by technology, on the other hand, there is the possibility of violation of fundamentals and specificities. The uses that we have internalized by being the subject of movies in the past are now put into practice in real life. In parallel with the rate of use of facial recognition technology, conscious or unconscious interference with fundamental rights and freedoms is increasing. In this study, facial recognition technology will be discussed in terms of the basic principles of personal data protection law, while the subject will be evaluated within the scope of examples, fictional possibilities, legislation and decisions.
Keywords: Personal Data, Sensitive Personal Data, Biometric Data, Face Recognition, Explicit Consent

Atıf Gösterme Şıracı, S., (2023). Yüz Tanıma Teknolojilerinin Kişisel Verilerin Korunması Hukuku Açısından İncelenmesi, *Kişisel Verileri Koruma Dergisi.* 5(1), 23-46. DOI:

GİRİŞ

Bilgi teknolojilerinin hızlı gelişmesinin kişisel veriler üzerindeki en büyük yansıması, her türlü bilgi yanı sıra kişilere ait verilere de kolay ve hızlı erişim imkânı ile kişilerin sürekli siber takip ve gözetim altında oldukları yönündeki çekincelerdir. Kişisel verilerinin işlenmesi bireyin doğumu ile başlayıp, ölümüne kadar devam edebilen uzun bir süreci kapsamaktadır. Bu bağlamda bireyin ilk karşılaştığı veri sorumlusu da devlettir. İlk ve en büyük veri işleme sorumlusu olan devlet tüzel kişiliği, kamu hizmetlerinin yürütülmesi ve yurttaşlara ulaştırılması, kamu sağlığı ve kamu güvenliğinin temin edilmesi ve korunması için devamlı surette bireyleri takip eder ve kişisel verilerini kaydeder. Doğal olarak da gerek devlet tüzel kişiliği, gerekse ticari tüzel kişilikler - şirketler, kişisel verilerin kaydedilmesi ve bireylerin siber takibinde bilgisayar ve görüntü kayıt teknolojilerindeki gelişmelerden en ileri şekilde faydalanırlar. Özellikle bilgisayar teknolojilerindeki çok ileri seviyedeki değişim ve gelişmeler sayesinde istenilen bilgiye saniyeler içinde erişim sağlamak mümkün hale gelmiştir. Her türlü bilgi gibi, kişisel verilere de erişimin bu kadar kolay ve hızlı olduğu günümüzde, kişisel verilerin korunması da bir zorunluluk hale gelmiştir.

İnsanın kim olduğu, nereden gelip nereye gittiği, fiziksel özellikleri her zaman diğer insanların merak konusu olmuştur. Bu merak sadece bireyler için değil, genel olarak toplumlar ve devletler için de geçerlidir. Bu bağlamda en ilkel kabile toplumlarında dahi, kabile nüfusuna dahil olan insanların kimliğini tanımaya yönelik olarak gerekli bilgilerin kaydedildiğini görmek mümkündür. Özellikle devletler, bireylerden vergi toplama ve kamusal hizmet sunma gibi faaliyetlerin doğru yürütülmesi için bireylerin kayıt altına alınmasına ihtiyaç duymuşlardır.

Her zaman kesin ve doğru sonuçlar vermediği yönünde tartışma ve eleştiriler de olmakla birlikte özellikle suç faillerinin tespitini sağlayabilmek için parmak izi emniyet görevlilerince 20. yüzyılda sıkça kullanılmıştır. Gelişen teknolojik uygulamalar ve bilgisayar sistemleri nedeniyle gerek güvenlik alanında gerekse ticari alanda parmak izi ile tanımla yeterli görülmemiş, yüz tanıma, iris ve göz retinası veya el geometri taramaları da biyometrik uygulamalar arasına girmiştir. Örneğin optik alandaki gelişmelerle yüksek çözünürlüklü kameraların yaygınlaşması, çekilen fotoğrafların çözünürlüğünün yükselmesi ile yüz tanıma teknolojilerinde bir sıçrama olmuştur.

Diğer taraftan da biyometrik uygulamalarda önemli bir yer tutan parmak izine göre kişilerin tanımlanması da geliştirilerek, özellikle parmak izi veri tabanı genişletilerek, parmak izinin kontrol edilmesinde bilgisayar teknolojilerinin de yerini alması ile dakikalar içinde parmak izi sahibinin kimliği tespit edilebilir hale gelmiştir. Zira parmak izinin kullanılması suretiyle kimliğin tespit edilmesinde parmak izi örneği ve bu örneğin karşılaştırılacağı kimlikleri tespit edilmiş parmak izi veri tabanı olmak üzere iki unsur söz konusudur. Parmak izi veri tabanında yapılan karşılaştırma ve eşleştirme, bilgisayar teknoloji ve yazımlarının olmadığı yıllarda, elde edilen veriler görevli kişilerce manuel olarak parmak izi veri tabanında karşılaştırılmakta ve eşleşme aranmakta iken, bu konuda bilgisayar uygulama ve yazılımlarının ortaya çıkması ile, veri tabanındaki arama ve eşleştirme bilgisayar tarafından otomatik olarak yapılmaktadır. Bu durum da karşılaştırma ve eşleştirmenin manuel olarak günler sürebildiği durumdan, dakikalar içinde sonuç alınabildiği hale evrilmesine yol açmıştır. Şu an hiç şüphesiz otomatik yöntemler çok daha yoğun kullanılmaktadır.

Biyometrik yöntemlerin görüldüğü yerlerin geniş ve çeşitli olduğuna şüphe yoktur. Bu uygulamalar genellikle genel kamu güvenliği, kamu sağlığını koruma amaçlı kullanıldığı gibi, bireysel güvenlik tedbirlerini sağlama amaçlı da kullanılabilmektedir. Güvenlik tedbirlerinin en üst seviyede olduğu hava limanlarına giriş ve çıkış işlemleri, ceza infaz kurumlarına girişlerde (özellikle ülkemizdeki tüm ceza infaz kurumlarına avukat ve ziyaretçi girişlerinde göz retinası taraması yapılarak kişi sisteme tanıtılmakta, ziyaretçi kuruma her girişinde göz retinası üzerinden sistem veri tabanındaki eşleşme sonrası onay alınarak girişe izin verilmektedir) internet bankacılığı ve cep şube bankacılığında müşteri

kimliğinin tanımlanmasında, kredi kartı uygulamaları, çalışan takibi, cep telefonları ve kapı sistemlerinde de kullanılmaktadırlar. Özellikle akıllı telefonlarda biyometrik verinin kullanılabiliyor olması ve bu sistemin sürekli ilgili kişinin elinin altında olması sebebiyle kullanım alanı gittikçe artmaktadır. Her geçen yılda, biyometrik uygulamalar üzerine çalışma yürüten şirketlerin sayısının artması ile, ticari rekabetten dolayı bu alanda yüksek pazar payına sahip olmak isteyen firmalar, bu uygulamaların çeşitliğini artırdığı gibi hızlı bir şekilde gelişmesine ve yaygınlaşmasına yol açmışlardır.

BİYOMETRİK VERİ VE YÜZ TANIMA

Genel Tanım

Biyometri, insanları birbirinden ayırt edebilecek fiziksel ve davranışsal özellikleri inceleyen bilim dalıdır (Dede ve Sazlı, 2010). Biyometri kelimesi, latincede hayat anlamına gelen "Bios" ve ölçü anlamına gelen "Metron" kelimelerinin birleşmesinden meydana gelmiştir (Derya, 2011). Kişilerin biyometrik verileri doğuştan kazanılan fiziksel özellikleri ve sonradan kazanılan davranışsal özellikleri olarak iki türü olduğu kabul edilmektedir. Biyometrik uygulamalarda kişileri tanımaya ve diğer bireylerden ayırmaya yarayan ölçülebilir fiziksel özellikleri, yüz şekli, retina, iris, parmak izi, avuç izi, damar izi ve dna profili şeklinde ortaya çıkarken, davranışsal özellikler ise ses, yürüyüş şekli, imza, vücut kokusu, bir nesne veya aygıtı kullanma şekli olarak tespit edilmiştir. Kişinin boyu ve kilosu ise biyometrik veri olarak kabul edilmemektedir. Zira olasılığının düşük olması ile birlikte, kişinin boy uzunluğu veya kilosu birebir başka bir kişi ile aynı olabilmektedir. Bir kişinin fiziksel veya davranışsal özelliklerinin yüzde yüz olarak bir başka bir bireye benzemesinin imkansız olduğu düşünüldüğünde insanları tanımak, tanımlamak ve kimliğini belirlemek için biyometrik veriler dışında da çok fazla aracın olduğu görülecektir. Bu araçlar; özellik, işaret, gösterge, kimlik tanıtıcı, anahtar, tanımlayıcı şeklindeki terimlerle ifade edilmektedir (Jain, Ross, Nandakumar). Akıllı telefon kullanıcılarının kullanım esnasındaki dokunma hareketi, sürükleme yolu gibi verilerin de biyometrik veri olarak değerlendirilebileceği anlaşılmıştır (Snijder, 2016). Kişisel Verileri Koruma Kurumuna göre bir kişisel verinin biyometrik niteliği haiz olabilmesi için ilgili kişinin ayırt edici biyometrik özellikleri ortaya çıkartılmalı ve bu özellikleri ile kimliği tanımlanmalı veya doğrulanmalıdır (Kişisel Verileri Koruma Kurumu, 2021).

Kişi Tanıma ve Doğrulama Sistemleri

Kişisel veri güvenliğini sağlamak ve korumak amaçlı kullanılan kişi tanıma ve kimlik doğrulama işlemi, bilgi, aidiyet ve biyometrik orjinli olmak üzere üç farklı şekilde incelenmektedir. Bilgiye dayanan kimlik tanımlamasında, kullanıcıların ve söz konusu sistemi yönetenlerin kimlik doğrulaması yapabilmesi için bireyin kullanıcı adı, şifre, parola, pin kodu gibi daha önceden verilmiş ve teslim edilmiş özel verilere sahip olması gerekir (Berber ve Lostar, 2006). Kişilere özgü bu tür bilgiler veri güvenliği sistem yöneticileri tarafından sağlanan bir veri tabanında saklanır, sisteme giriş yapmak isteyen kullanıcılar gerekli verileri sisteme girdiklerinde veri tabanında yer alan veriler ile yapılan karşılaştırma ve kontrol sonucu birbirleri ile eşleşmesi halinde kişinin kimliği doğrulanmış olur ve kişinin sisteme erişim yapması sağlanır. Aidiyete dayanan kimlik tespitinde ise kişilerin kendileri ile eşleşen daha önceden belirlenmiş, kişiye ait verileri de içeren bir nesneye ile kimliklerini doğrularlar. Bu nesneler genelde manyetik kart, rozet veya anahtardır (Şamlı, 2009). Son olarak da ayrıntılı olarak inceleneceği üzere biyometrik verilerimize dayanan tanıma ve doğrulama sistemleridir. Kimlik tespiti, güvenlik sağlama, müşteri memnuniyeti, finans sistemine kolay katılım ve nüfus hareketlerinin yönetilmesi gibi kullanım alanları mevcuttur (Secure Identity Alliance, 2009).

Yüz Tanıma Yöntemi

Yüz tanıma, insan yüzünü tespit edip tanımlamaya yarayan, gelişmiş, çok hızlı büyüyen bir biyometrik teknolojidir. Gelişmiş kameralarla kaydedilen görüntülerle elde edilen bireyin yüzüne ait yüzün ölçümünden ibaret olan matematiksel veriler, geniş veri tabanı ile karşılaştırılarak uygun eşleşme aranmakta, eşleşme sağlandığı durumda, veri sahibinin kimliği tespit edilmiş olmaktadır. Yüz tanıma sistemleri ya da yüz tarama teknolojisi; elde ettiği insan yüzü görüntüsü üzerinde çeşitli noktaları inceler ve elde edilen verilerden bilgisayar yazılımları aracılığı ile bir şablon oluşturur. Elde edilen kalıp da veri tabanındaki biyometrik şablonlar ile karşılaştırılarak bir eşleşme aranır.

Günümüzde artık akıllı cep telefonları, ekran kilidi olarak pin kodu yerine parmak izi veya yüz tarama uygulamasını tercih etmektedir. Bu tür güvenlik ve kimlik doğrulama sistemlerinin kullanılmasının kişiye özgü olması, kopyalanamaması nedeniyle de ele geçirilemediğinden klasik yöntemlere göre daha güvenli olduğu söylenebilir (Sağıroğlu ve Özkaya, 2006). Dünyada özellikle kolluk kuvvetleri tarafından gün geçtikçe yüz tanıma teknolojilerinde artış görülmektedir. Çünkü bu yöntem ile çok geniş bir alanda aynı anda onlarca kişinin fizyolojik ve davranışsal görüntüsü üzerinden aranan şahıslar bulurken yapay zeka destekli sistemlerle önleyici tedbirler alınabilmektedir.

İşyerlerinde çalışanların işe giriş ve çıkışlarında çalışanların hem kimlik kartını taşıma zorunluluğundan kurtarmak hem de kimlik kartının, kartı sahibi dışında başkaları tarafından okutulması gibi kötü niyetli uygulamaların önüne geçilme gerekçesiyle yüz tanıma sistemleri kullanılmaktadır. Parmak izi okumada bireyin parmaklarından birisi veya birkaçını optik okuyucuya temas etmesi gerekmekte iken, yüz tanımada sistem görüntü kaydeden cihazlar sayesinde otomatik olarak çalışmakta olduğundan biyolojik veri kaydedilmesi otomatik olarak gerçekleşir. Ancak buna rağmen yüz tanıma sistemleri parmak izi okuma sistemlerine göre daha masraflı olduğundan bahisle parmak izi okuma sistemleri tercih edilmektedir. Buna karşılık Covid-19 salgını sonrası aynı parmak izi okuyucu sistemine dokunmak istenmemesi sebebiyle yüz tanımaya doğru bir yönelme olmuştur.

Yüz Tanıma Verilerinin Otomatik Olarak İşlenmesi

Yüz tanıma verilerinin otomatik olarak işlenmesi; bilgisayar, kamera, telefon gibi tanımlama özelliğine sahip cihazların yazılım desteği ile insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyetidir. 6698 Sayılı **Kişisel Veri**lerin Korunması Kanunu (Kanun) kapsamında otomatik işleme konusunda açık bir düzenleme bulunmamakla birlikte kişisel verilerin işlenmesi tanımında kişisel verilerin tamamen veya kısmen otomatik olan yollarla işlenmesinden bahsetmektedir. Yine konumuz ile bağlantılı olarak ilgilinin kişinin haklarının sayıldığı Kanun'un 11. Maddesinin g fıkrasında "münhasıran otomatik sistemler vasıtasıyla analiz edilme" kavramı zikredilmektedir.

Kimlik tanımlaması yapan yüz tanıma sistemleri için teknoloji geliştiricileri tarafından genellikle bu sistemlerde ham kişisel veri tutulmadığı sadece bir algoritmaya dayanan sayısal bir veri tutulduğu ve bu sebeple de söz konusu faaliyetlerin kişisel verilerin korunması hukuku alanında olmadığı ifade edilmektedir. Öncelikle uygulamalarla ilk kayıt esnasında ve daha sonra doğrulama ve tanımlama adımlarında kişisel veri işlenmek zorunda olduğu için sisteme bir bütün olarak bakıldığında bu faaliyet kişisel verilerin korunması hukukunun inceleme alanında kalmaktadır. Diğer yandan saklanan sayısal verinin de kaynağı yine ilk tespitte kayıt edilen kişinin fizyolojik veya davranışsal özelliklerinden elde edilen şablon bir biyometrik veridir. Bu sayısal verinin hiçbir zaman ilgili kişinin biyometrik verisine sistemde yüklü algoritma olmadan geri dönüştürülemeyecek olması ancak bir güvenlik tedbiri olabilir. 2022/662 sayılı Kurul kararına konu olan olayda veri sorumlusu ilgili kişi abonelerden otomatik olarak alınan geometrik verinin bir matematiksel hesaplama olduğu, el geometrisinin herkes de aynı olmayacağı için bir biyometrik veri olmadığı, elin bütün noktalarının taranmadığı kısıtlı bir alanındaki noktaların tarandığı dolayısı ile özel nitelikli bir kişisel veri olmadığı yönünde savunma yapılmıştır.

Kurul, el geometrisi verisinin ilgili kişiye ait ölçülebilir fizyolojik bir özellik olması, eldeki 31.000 noktadan el geometrisinin toplanması, bu yöntemle otomatik şekilde kimlik denetleme ile işlendiğinin anlaşıldığından idari yaptırım kararı vermiştir. İlgili kişiyi bizatihi bu mevcut biyometrik veriyi işleyen veri sorumlusundan da korumaya ihtiyacımız vardır. Biyometrik veritabanı üçüncü şahısların eline geçtiğinde işe yaramayacak olabilir fakat halihazırda sistem sahibi veri sorumlusunun bu biyometrik veri sistemini başka amaçlarla kullanmayacağının da garantisi yoktur. Örneğin Kanun yürürlüğe girmeden önce pek çok işyerinde yüz tanıma sistemleri kullanılmaktaydı. Kanun'un yürürlüğü tarihinden sonra bu sistemlerin kullanımı durduruldu fakat bu sistemlerin yeniden aynı şekilde kurularak tekrar kullanılıp kullanılmayacağını bilme imkanımız yoktur.

YÜZ TANIMA BİYOMETRİK UYGULAMALARIYLA ELDE EDİLEN KİŞİSEL VERİLERİN HUKUKİ ANALİZİ VE BU VERİLERİN İŞLENMESİNDEKİ GENEL İLKE VE KURALLAR

Hukuki Niteliği ve Kapsamına Dair Örnekler

Kişisel veri, kişiye özgü ve özel olup, kişiyi tanıma veya tanımlamada kullanılabilen bilgidir. İşyerinde kullanılan yüz tanıma sistemleri de işçinin yüzünün görüntüsü ile kimlik bilgileri doğrudan eşleştirildiği için gerçek kişiye ilişkin belirli bir kişisel veridir (Küzeci E. ve Kılıç Ş, 2019).

Kişisel verilerin işlenmesi kişinin doğumu ile başlayıp ölünceye kadar devam eden uzun bir zaman dilimini kapsamaktadır. İnsan yaşarken ve toplum içerisinde sosyalleşirken aslında sürekli olarak biyometrik verilerini bilinçli veya bilinçsiz olarak kısmen veya tamamen açıklar ve başka kişilerle paylaşır. Özellikle günümüzde kamusal alanlarda MOBESE kameraları ile, işyerlerinde de güvenlik kameraları ile sürekli şekilde kesintisiz olarak görüntü ve ses kaydı yapıldığına dikkat edilirse, kameraların merceklerine ve optik okuyuculara giren insanların görüntü ve fiziksel özellikleri, yürüyüş şekli, ses kaydı gibi biyometrik verileri işlenmektedir. Özellikle biyometrik veriler, kişinin yaşaması ve canlı olmasından doğan kişiye özgü bilgiler olduğundan bahisle kişinin ölümü ile biyometrik verilerin işlenmesi de son bulacaktır. Kurul, mirasçılar tarafından kişisel verilerin talep edilmesi ile ilgili verdiği 2020/507 sayılı kararında kişisel veri hukukunda, kişisel verilerin gerçek kişilere ait olduğu ve ölümle birlikte kişiliğin de sona erdiği bu sebeple Kanun'un uygulama alanından çıktığını ve bundan sonraki taleplerin ölünün sağlık verilerine erişim konusunun düzenlendiği Kişisel Sağlık Verileri Hakkında Yönetmeliğin, 11 inci maddesi kapsamında yerine getirilmesi gerektiğini karara bağlamıştır. Konumuz özelinde ilgili kişinin ölümü ile birlikte biyometrik verilerin Kanun anlamında işlenmesinin de sona erdiğinin kabulü gerekecektir.

Biyometrik uygulamalar, kişilerin ölçülebilir fizyolojik ve davranışsal niteliklerini tespit etme yolu ile yapılan ve otomatik şekilde doğrulanabilen kimlik tanıma ve doğrulama yöntemlerini ifade eder (Cüneyd Er, 2007). Bu uygulamalardan bazıları; kişinin kimliğin, kim olduğunun tespitini sağlayan iris, retina, parmak izi, yüz şekli, el veya damar geometrisi, DNA, yürüyüş tanıma şeklinde kendini gösterir. Nitekim Avrupa İnsan Hakları Mahkemesinin S. ve Marper / Birleşik Krallık kararında; devlet kurumlarının elde ettiği ve sakladığı parmak izi, DNA profili ve hücre örnekleri kayıtlarının, belirlenmiş ya da belirlenebilecek kişilerle ilgili olduklarından biyometrik kişisel veri olduğunu kabul etmiştir. Bu açıdan, biyometrik uygulamalar yolu ile kişinin fiziksel veya davranışsal özelliklerinden yola çıkılarak kimlik tespiti yapılabileceğinden, bu yöntemlerle kişinin kim olduğunun tespit edilmesini sağlayan kişiye özgü verilerini ifade eder (Akgül A., Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması). Bu tespitin sonucu olarak, kişinin biyometrik verilerinin de, genel olarak Anayasanın 20. maddesi ve özel olarak da 6698 Sayılı Kişisel Verileri Koruma Kanunu ile güvence altına alınan kişisel verilerin korunması hakkı açısından, haksız, ölçüsüz ve hukuka aykırı müdahale veya saldırıya karşı en geniş çerçevede korunması ve kişisel verilerin korunması hakkına ilişkin usul ve ilkelere tabi olmasıdır.

Kişisel Verileri Koruma Kanununun özel nitelikli kişisel verileri tanımlayan m. 6 f.1. hükmü uyarınca biyometrik özel nitelikli kişisel veridir. Özel nitelikli verilerin bireylerin özel hayatlarıyla bağlantılı olduğundan, hassas doğaları sebebiyle daha yüksek düzeyde korunması gerektiği düşünülür. Bu bağlamda, biyometrik teknolojilerle toplanan kişisel verilerin işlenmesine dair kurallar ve ilkelerin de katı düzenlemelerle yönetilmesi bir gerekliliktir.

Yüz tanıma sistemlerinin en çok kullanıldığı alan güvenlik ile ilgili tedbirlerdir. Yetişkin bir kişinin yaşamı boyunca bu verileri değiştiremeyecek olmasındaki hassasiyetin bir diğer sebebi gelecekte biyometrik verinin kullanım alanının genişleyecek olmasıdır. Biyometrik veri kayıt cihazlarının gösterdiği gelişim, bilgisayarların veri işleme ve başka veri tabanları ile eşleştirme kapasitesinin artması gibi teknolojik gelişmeler bugün aklımıza gelmeyen fakat gelecekte ilgili kişilerin aleyhine olabilecek kullanımları artıracaktır. Örneğin güvenlik için alınan iris kaydı ile ilgili kişinin yatkın olduğu sağlık problemlerinin tespit edilmesi ve ticari olarak kullanılması, damar izinin aynı zamanda kalp ve damar hastalıkları hakkında bilgi vermesi, düzenli kayıt ettiği videolardaki yüz hareketlerinden ruh sağlığı hakkında bilgi sahibi olunması gibi alternatif özel nitelikli kişisel veriler türetilebilecektir. Yapay zekalı sistemlerde biyometrik tanımlama kullanımı gittikçe artmaktadır, bu yazılımların ilgili kişileri ırk, cinsiyet, din gibi ayrımcılık yaratacak amaçlarla kullanılmasından endişe edilmektedir (*EPDP, 2021*). Elbette ilk tespitlerde amaç bu değildir fakat son çare olarak kullanılmak istenmesinin sebebinin anlaşılması için bu ihtimaller üzerinde düşünülmelidir.

Biyometrik veri işleme amacı olmaksızın, biyometrik veriye temel olabilecek bir verinin işlenmesi faaliyeti özel nitelikli kişisel veri işleme olarak kabul edilmeyecektir. GVKT Recital bölümünün 51. maddesinin 3. paragrafına göre fotoğraflar belirli bir teknik yöntemle kimlik doğrulaması veya tanımlaması yapılmadıkça özel nitelikli kişisel veri işleme faaliyeti olarak değerlendirilmemelidir. Sosyal medyada arkadaşlarımız ile çekilen fotoğraflarınızın paylaşılması genel bir veri işleme faaliyetiyken, bu fotoğraflardaki kişilerin yüzleri seçilerek gerçek kişiyle ilişkilendirilecek şekilde etiketlenmesi ve sosyal medya hesabımızdaki arkadaşlarımıza ait fotoğraflara uygulanması halinde bir biyometrik veri işleme faaliyeti gerçekleştirilmiş olacaktır. Bu sebeple artık bu tür uygulamalarda, ilgili kişiler için tanımlama yoluyla etiketlemeye izin verme özelliği eklenmiştir.

Yine yüz tanımaya benzer şekilde işleme amacına göre yorum yapılmasına örnek de ses kayıt sistemleridir. Bir bankanın telefonda kimlik tespiti için müşterisinin ses kayıtlarını kullanması halinde özel nitelikli kişisel veri işlediği kabul edilirken, aynı ses kayıtları verilen talimatın ispatı için tutulması halinde genel nitelikli kişisel verilerin işlenmesi olarak kabul edilecektir (Yücedağ, 2017). Ses ile ilgili bir başka örneği kişinin konuşmasının dökümünün yapılması veya konuştuğu konunun anlaşılıp kendisine otomatik yanıt verilmesi ile bu işlemleri yaparken kişinin sesinden kimliğinin tanımlanarak işlem yapılması arasındaki fark olarak da sunabiliriz. Kişinin konuşmasının makinelerin anlayacağı sayısal bir dile dönüştürülmesine bağlı olarak sonuç üretilmesinde kişiyi tanımlama amacı olmadığı için biyometrik veri işleme olarak kabul edilmeyecektir.

Reklamcılık sektörü mümkün mertebe doğrudan müşterilerine tanıtım materyallerini ulaştırmak için gayret göstermektedir. Özellikle açık veya kapalı alanlardaki ekranlarda o sırada ekrana bakan veya bakma ihtimali olan kişilere doğrudan reklam yapmak oldukça kıymetlidir. Bunun için yüz tanıma teknolojisinin sunduğu nimetler oldukça cezbedicidir. Teknoloji kullanılırken bu ekranların önünde geçen kişilerin daha önce elde olan kimliği ile eşleştirme yapılması hatta kimlik ile eşleşmede de daha sonrası için yüzlerinin biyometrik şablonunun kayıt edilmesi halinde doğrudan özel nitelikli kişisel veri işleme faaliyeti gündeme gelecektir. Nitekim Avrupa Konseyi'nin 2021 yılında yayınlandığı yüz tanıma sistemleriyle ilgili rehberde özel kuruluşların alışveriş merkezleri gibi kalabalık ve kontrolsüz ortamlarda pazarlama amacıyla veya özel güvenlik amacıyla kişileri tespit etmek için yüz tanıma teknolojilerini kullanmaması gerektiği vurgulanmıştır (Avrupa Konseyi, 2021). Bununla birlikte aynı sistem kişileri tekil olarak hedeflemeden ve tekil bir biyometrik şablon oluşturmadan o an mağazada

olan kişilerin ortak özelliklerine göre örneğin cinsiyet gibi fiziksel bir özellik üzerinden gösterilecek reklama karar verilmesi halinde özel nitelikli kişisel veri işlemeden bahsedilmeyecektir.

Bir otel yönetiminin yüksek konuk memnuniyeti amacıyla otelin çeşitli noktalarına konukların yüzlerinden duygu durumunu takip eden özel bir sistemin konulduğunu varsayalım. Bu sistem şayet konukların kimlikleriyle eşleştirilip mutsuz konuğa ekstra ikramlar yapılması üzerine kurulmuşsa yine özel nitelikli kişisel verilerin işlenmesi için gerekli şartları yerine getirmelidir. Fakat otelin amacı herhangi bir ilgili kişiye ait biyometrik veri şablonu oluşturmadan, konukların tekil olarak duygusal durumdan çok bütün konukların ortalama sadece mutlu/mutsuz durumunu veya restoran bölümündeki yemek öğünlerindeki memnuniyeti kimlik tespiti yapmadan, anonim olarak takip etmekse yine bir özel nitelikli kişisel veri işlediği varsayılmayacaktır.

Günümüzdeki diğer bir tartışma da akıllı telefon uygulamalarının yüz tanıma sistemini kullanmasıyla ilgilidir. Örneğin Apple tarafından üretilen Iphone marka telefonlarda çalışan uygulamalar etkinleştirme için Face ID ismi verilen yüz tanıma sistemini kullanmaktadırlar. Apple web sitesinde bu uygulamanın yüz tanıma verilerini buluta yüklemediği, cihazda şifreli olarak saklandığı, özel bir anahtar ile kullanılabildiği, kullanıcının dilediği zaman silebildiği, doğrulama yapan uygulamalar ile sadece doğrulamanın başarılı olduğu bilgisinin paylaşıldığı, uygulamaların yüz tanıma verilerine erişemediği yazmaktadır (Apple, Face ID ve Gizlilik). Kanaatimizce ilgili kişinin yüz tanıma verisi yine kullanıcıya ait bir cihazda ve kullanıcının hakimiyet alanında çıkmadığı ve uygulamalarla sadece yüz tanıma onay bilgisi evet/hayır olarak paylaşıldığı için şahsi bir veri işleme söz konusu olup, bir üçüncü şahıs tarafından veri işleme faaliyeti yoktur. Bununla birlikte ilgili cihaz üreticisi şirketin yüz tanıma verilerinin yetkisiz üçüncü şahısların eline geçmemesi için geri dönüştürülemez şekilde şifrelemelidir (W29 - 192, 2012).

Akıllı telefonlardaki bu uygulamayı bir adım daha ileri götürüp örneğin basit bir kapı geçiş sistemi için kurgulayabiliriz. İlgili kişinin akıllı telefonuna indirilen bir uygulama ve uygulamanın karşılığı olan bir istemci otomatik kapıya bağlanmış olsun. İlgili kişi kapının önüne geldiğinde akıllı telefondaki uygulamayı aktif ederek yüz tanıma sistemi ile yüzünü okutması halinde Face ID uygulamaya onay bilgisi veriyor, onay bilgisini olan akıllı telefonda uygulama da istemciye onay bilgisi gönderiyor ve kapı açılıyor. Bu kurgudaki diğer bütün siber güvenlik çekincelerini bir kenara bırakıp sadece yüz tanıma verisinin işlenmesi açısından olaya bakıldığında veri işleme faaliyeti yine ilgili kişi tarafından tamamen kendisi ile ilgili yapılmakta, ilgili kişi dış dünya ile özel nitelikli olmayan kişiler verilerini paylaşmaktadır. Bu durumda genel bir veri işleme faaliyetine dönüşen kurgu Kanun kapsamı dışına tam anlamıyla çıkmamaktadır.

Avrupa Birliği Mevzuatında Biyometrik Verilerin İşlenmesi

Avrupa Birliğinde kişisel verilerin korunmasının temel taşını Genel Veri Koruma Tüzüğü (GVKT) oluşturmaktadır. GVKT tanımlara ilişkin 4.maddesinin 14.fıkrasında biyometrik veri, işlemin teknik yöntemlerle gerçekleşmesi, kişinin tekil, ayırt edici özelliklerinin meydana çıkartılması, yüz tanıması gibi bu ayırt edici özellikleri ile kimlik doğrulamasının yapılması biçiminde tanımlanmıştır. GVKT 29. Madde için oluşturulan Çalışma Grubu (Working Party 29-W29) ise Tüzükteki bu tanımı biraz daha ayrıntı ekleyerek; "k*işiye özgü ve ölçülebilir olan tekrarlanabilir eylemlerini, belirli bir derecede olasılık içerse bile teknik olarak ölçmek için kullanılan şablonları ifade etmektedir*" tanımı yapılmıştır. Tanımlardan anlaşılacağı üzere biyometrik veri ilgili kişiyi tanımlayan eşsiz bir bağlantıdır.

Avrupa Birliği mevzuatında biyometrik uygulamalar ile elde edilen kişisel veriler, özel nitelikli veri olarak kabul edilmiş ve bu verilerin işlenmesi, kullanılması ve paylaşımı hususunda, genel kişisel verilere oranlara daha korumacı bir yaklaşım ortaya konulmuştur. GVKT 9. Maddede özel nitelikli kişisel verilerin dolaysıyla biyometrik verilerin işlenme ilkeleri düzenlenmiştir. Düzenlemeye göre,

biyometrik verilerin işlenebileceği haller sayılarak, bu haller dışındaki alanlarda biyometrik verilerin işlenmesi yasaklanmış ve özel nitelikli kişisel verilerin işlenmesinin önüne geçilmiştir. GVKT 9. Madde biyometrik veri işleme ile ilgili yasağı düzenlemektedir.

GVKT'ye göre veri işleme için veri sahibinden alınan rızanın geçerliliğinin Avrupa Birliği mevzuatı ya da ulusal mevzuat uyarınca yasaklanmamış olduğu hallerde, kişinin veri işlemeye dair açık rızasının olması halinde biyometrik veriler işlenebilir. Kanun herhangi bir nitelik ayrımı yapmaksızın her türlü kişisel veri için açık rıza düzenlemesi getirmişken GVKT özel nitelikli kişisel veriler için açık rıza düzenlemesine yer vermiştir (Çekin, 2016). Bir veri işleme faaliyetinin GVKT kapsamında biyometrik veri işleme olarak kabul edilebilmesi için 9. madde gereği "bir gerçek kişiyi tanımlamak amacıyla" hareket edilmesi gerekmektedir. Yine GVKT 4. maddedeki tanıma göre bir faaliyeti biyometrik veri işleme olarak kabul edebilmemiz için ilgili veri gerçek kişiye ait fiziksel, duygusal veya davranışsal verilerden oluşmalı, teknik bir işleme faaliyetinin sonucu ortaya çıkmalı ve gerçek kişiyi tanımlamak için kullanılmalıdır.

AB'ye üye ülkeler GVKT'de yer alan düzenlemeler çerçevesinde, tüzük hükümlerine aykırı olmamak şartı ile, genetik, sağlık veya biyometrik verilerin işlenmesine ilişkin olarak başkaca yeni yasal kurallar koyabilir. Biyometrik kişisel verilerin işlenmesi ve kullanılmasında bulunması gereken usul ve esasların ana çerçevesi GVKT hükümleri ile ortaya koyulurken, AB ye üye ülkeler ancak bu ana ilkelere aykırı olmamak kaydı ve şartı ile bu hususta düzenleme yapabilmektedirler. GVKT düzenlemelerinin genel hatlarının dışına çıkacak şekilde yasal düzenleme yapılmasına izin verilmemektedir. Ayrıca yapılacak düzenleme ve uygulamaların Avrupa İnsan Hakları Sözleşmesinde yer alan temek hak ve özgürlükleri uygun olması ve temel haklara müdahale niteliğinde olmaması da zorunludur. Bu noktada biyometrik uygulamaların kitle gözetiminde kullanılmasına dair çekinceler bulunmaktadır. Özellikle bu uygulamaların uzaktan çalışabilmesi, başkaca uygulama ve sistemlerle entegrasyonu risk teşkil edebilmektedir. Kamu politikaları doğrultusunda kriminal süreçlerde kullanılmak üzere geliştirilmiş olsa dahi, temel haklara müdahaleyi önlemek üzere GVKT'nin 35. maddesinde yer alan veri koruma etki değerlendirmesi yapılması gerekebilir.

Türk Hukukunda Biyometrik Verilerin İşlenmesi

6698 Sayılı Kişisel Verileri Koruma Kanunun 3. maddesinin (e) fıkrası kişisel verilerin işlenmesi tanımlamıştır. Biyometrik veri işleme ise, biyometrik uygulamalarla elde edilen özel nitelikli verilerin kaydedilmesi, tasnifi, depo edilmesi, kullanılması, başka şahıslarla paylaşılması, ilan edilmesi ve ortadan kaldırılmasını da içine alan işlemler bütünüdür (Kılınç, 2012).

Kişisel Verileri Koruma Kurulu, 2019/81, 2019/165 ve 2020/167 sayılı kararlarında Kanun'da biyometrik veri tanımına yer verilmediği tespitini yaptıktan sonra GVKT'de yer alan tanıma yer vermiştir. 6698 Sayılı KVKK 6.maddesinin 1.fıkrasında biyometrik veri, özel nitelikli kişisel verilerin arasında sayıldıktan sonra 2, 3, ve 4. fıkralarda bu özel nitelikli kişisel verilerin işlenmesi için aranan özel şartlar belirtilmiştir.

Ülkemizde biyometrik veri işlenmesine cevaz veren mevzuatlar bulunmaktadır. Bu haliyle kamunun özel sektörden daha avantajlı olduğunu söylemek yanlış olmaz. Nitekim özel sektörün biyometrik veriyi işleyebilmesi için genellikle açık rızaya başvurması gerekmektedir ki bu yöntem uygulama açısından kolay değildir.

5490 sayılı Nüfus Hizmetleri Kanunu'nda biyometrik verinin kullanımına ilişkin hükümler bulunmaktadır. Kanun'un "Tanımlar" başlıklı 3 üncü maddesinin (ff) bendinde biyometrik veri, ilgili kişinin kimliğinin tespit edilmesi için kullanılan kişiye özel fizyolojik özellikler örnek verilerek tanımlanmıştır.

Yine bir başka tanımlama Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğin dördüncü maddesinde kişinin ölçülebilir ayırt edici özelliklerine atıfta bulunularak bir tanım yapılmıştır. Her ne kadar biyometrik veri tanımı yapılmasa da 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 67'nci maddesinde kimlik doğrulama için biyometrik veri kullanılabileceği belirtilmiştir.

Kanuna Göre Biyometrik Kişisel Verilerin İşlenme Şartları

Kanun, kişisel verilerin genel olarak işlenme usul ve şartlarını da düzenlemiştir. Bu usul ve şartlar şüphesiz biyometrik kişisel verilerin işlenmesi için de geçerlidir. Biyometrik kişisel verilerin kaydedilmesinin hukuka aykırı olmaması, temel ve hak ve özgürlüklere müdahale niteliği taşıyarak kişilerin zararına neden olmaması için söz konusu kanunun 6. maddesinde ifade edilen şartlardan birinin mutlaka bulunması gerekir.

Özel Nitelikli Kişisel Veri İşlenmesinin Kanunlarda Düzenlenmesi

Anayasal hukuk sistemimizin esaslı unsurlarından birisi de temel hak ve özgürlüklerin ancak kanunlarla sınırlandırılabilmesidir. Böylece yürütmenin yasamanın çizdiği sınırlarından çıkarak yönetmelik, tüzük, genelge, tebliğ gibi ikinci mevzuatlarla temel hak ve özgürlüklere müdahale eden düzenlemelerinin önüne geçilmektedir (Kızılyel, 2014). Kişilere ait kişisel verilerin işlenmesi ile ilgili olarak yasalarda herhangi bir zorunluluk ve yükümlülük olması halinde, ancak bu yasal şartlara ve amaca uygun olarak kişisel verilerin kaydedilmesi gerekliliği bu ilke kapsamındadır. İşyerlerinde çalışanların işe başlamasında kimlik ve adres bilgilerinin sosyal güvenlik kurumlarına bildirilmesi işverenler açısından yasal bir zorunluluk olup, aksi halde işverenin idari para cezası yaptırımı ile karşılaşması söz konusudur. Bu bağlamda, işe başlama sırasında işverenin işçinin kimlik ve adres bilgilerini alması yasadan kaynaklanan bir yükümlülükten doğmaktadır. Ancak bu durumda işveren sadece çalışanın genel kimlik bilgilerini işleme ve kaydetme yetkisine haiz olup, çalışana ait özel nitelikli olan biyometrik verileri işlemesi mümkün değildir. İşveren çalışanın kimlik fotokopisini talep edebilecek iken, parmak izi, iris veya retina tarama izi, dna profili verilerine ihtiyacı olmayacağından bahisle, bu tür biyometrik verileri çalışanından talep edemeyecektir. Yine suç şüphesi ile kolluk kuvvetleri tarafından göz altına alınan şahsın kimlik bilgilerinin kaydedilmesinde yasadan kaynaklanan bir görevin ifası ve yetkinin kullanılması söz konusu olduğundan bahisle kişisel verilerin işlenmesinde, parmak izinin alınması veya fotoğrafının çekilmesinde şüphelinin rızası aranmayacaktır. Bu durumda şüpheli, kimlik bilgilerini kolluk görevlilerine doğru olarak beyan etmek zorundadır.
Danıştay, memurların mesai takip sistemi için biyometrik veri kullanılmasıyla ilgili 2017/816 sayılı kararında mesai takibinin biyometrik veri ile yapılabilmesi için kanuni düzenlemenin olmadığına gerekçesinde yer vermiştir. Anayasa Mahkemesi de 2018/11988 sayılı bireysel başvuruda yine aynı doğrultuda devlet memurlarının mesai durumunun kontrolü amacıyla özel nitelikli kişisel verilerin işlenmesine ilişkin açık bir düzenlemenin olmadığı üzerinde durulmuştur.

Islak imza ile kolaylık sebebiyle gittikçe yaygınlaşan tablet üzerine imza atma şeklinde özetlenebilecek iş modelinde atılan imza biyometrik veridir (Berber, 2019). Kurul, biyometrik imza ilgili olarak görüş talebi üzerine verdiği 2020/649 sayılı kararında biyometrik imzanın içerdiği benzersiz teknik özellikler sebebiyle özel nitelikli kişisel veri kapsamında olduğunu belirtmiş ve ardından bu verinin işlenmesinin kanunlarda açıkça öngörülmesi veya açık rıza ile işlenebileceği genel kuralını hatırlatmıştır. İlgili kararda kanunlarda öngörülme şartının geniş yorumlanmaması ve dayanılan hükümlerin şüpheye yer bırakmayacak kadar açık olması gerektiği vurgulanmıştır. 6098 sayılı Borçlar Kanunu'nun 15 nci maddesinde yer alan imza ile ilgili hükmün klasik ıslak imza ve elektronik imzayı kapsadığı, biyometrik imzayı bu kapsama dahil edilemeyeceği dolayısıyla dayanak maddenin kanunlarda öngörülme şartına karşılık gelmediği tespiti yapılmıştır.

Danıştay 8. Dairesi 2012/10385 esas ve 13.4.2016 tarihli kararında kanunlarda özel düzenleme gerekliliğine dikkat çekmiştir. Milli Eğitim Bakanlığı Özel Eğitim Kurumları Yönetmeliğinin "*Günlük çalışma saatleri ve devam devamsızlık takibi*" başlıklı 25. maddesinde ders devam takibinin Bakanlıkça belirlenecek usul ve esaslara göre yapılacağı ve engelli birey ve eğitim personelinin kimlik doğrulama sistemine tanıtılmalarının ise rehberlik araştırma merkezlerince yapılacağı belirlenmiştir. Bu yönetmelik sonrasında özel eğitim ve rehabilitasyon merkezinde kimlik doğrulama sisteminin avuç içi damar izi yöntemiyle yapılması hususunda 5.6.2014 tarihli Genelge yayımlanmıştır. Danıştay gerekçesinde uygulamanın sınırlarını, kişisel verinin nasıl depolanıp, kullanılacağını tespit eden, usul ve esaslarını gösteren bir kanuni düzenleme olmaması nedeniyle ilgili yönetmelik hükümlerinin iptaline karar vermiştir.

Biyometrik verilerin işlenmesinin kanunlarla düzenlenmesinin de bir usulü olduğuna da dikkat çekmekte fayda vardır. Biyometrik verinin özel niteliği dikkate alındığında bir kanunda maddesinde amaç ve sınırları gibi temel ilkeleri içeren bir çerçeve belirlemeden biyometrik veri ile doğrulama yapılabilir gibi genel bir ifade yeterli olmamalıdır (Akgün, 2015). Henüz daha Kişisel Verilerin Koruması Kanunu yasalaşmamışken ortaya çıkan "avuç içi" tarama ile sağlık hizmeti verilmesi ile ilgili verilen kararlar bu tartışma için güzel bir örnektir. Danıştay Onbeşinci Dairesi, 2014/1150 esas sayı ile önüne gelen davada 5510 sayılı kanunnun 67. maddesinin 3. fıkrasında yer alan "... *biyometrik yöntemlerle kimlik doğrulanması yapılması ve/veya*.." ibaresinin, toplanma ve işlenmenin kapsamı, koruma için alınacak tedbirlere ilişkin usul ve esasların belirtilmeden, bu temel ilkeleri konulmadan, çerçevesi çizilmeden bir kısa hükmün belirlenmesinin Anayasa aykırı olduğundan bahisle ibarenin iptali için Anayasa Mahkemesine başvurmuştur. Anayasa Mahkemesi 19.03.2015 tarih ve 2015/30 sayılı kararında ilgili düzenlemenin sahteciliğin veya kötüye kullanmanın önlenmesi için biyometrik veri kullanımın gerekli olduğu, kamunun ekonomik çıkarları açısından öngörülen amaçla ölçülü olduğu, sadece sağlık sektöründe hizmet alım amacıyla kullanılabileceği, Türk Ceza Kanunundaki ilgili hükümlerin tedbirler için yeterli olduğu gerekçeleriyle Anayasa'ya aykırı olmadığına ve itirazın reddine hükmedilmiştir. Genel Sağlık Sigortası Uygulamaları Yönetmeliği, 18.4.2014 gün ve 28976 sayılı Resmi Gazete'de yayımlanarak yürürlüğe sokulmuştur. Yönetmeliğin "kimlik tespiti" başlıklı 26. maddesinin 1. fıkrasında hasta kimlik doğrulaması ile ilgili klasik yolların arasına "ve biyometrik yöntemlerle kimlik doğrulamasını yapar" ifadesi eklenmesi üzerine Türk Tabipler Birliği tarafından Danıştay 15. Dairesinin 2014/4689 E. sayı ile hükmün iptali için dava açılmıştır. Bu defa Danıştay Anayasa Mahkemesi tarafından verilen yukarıdaki karara atıf yaparak yönetmelik düzenlemesinin Kanun maddesine paralel olduğu ve kamu yararı ve hizmetin gereklerine uygun olduğu için talebi reddetmiştir. Kanun ile yönetmelik arasındaki fark kanunda "ve/veya" yazarken yönetmelikte "ve" olarak düzenlenmiştir ve bu uygulama zorunlu hale getirilmiştir.

Yukarıdaki "avuç içi" ile ilgili verilen karardan daha bir yıl önce Anayasa Mahkemesi'nin verdiği 9/4/2014 tarih ve 2013/122 esas sayılı karar çelişkili de görünmektedir (Akgün, 2015). Danıştay Dava Daireleri Kurulu tarafından Elektronik Haberleşme Kanunu'nun 51. maddesindeki "*Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir*" hükmü ile düzenleme yapma yetkisinin bütünüyle yürütme organına bırakıldığı, temel ilkeleri koyulmadan, çerçeve çizilmeden bir alanı düzenleme yetkisinin yürütme organına bırakılmasının, Anayasanın 13. ve 20. maddesine aykırı olduğu gerekçesiyle itiraz yoluna başvurulmuştur. Konuyu inceleyen Anayasa Mahkemesi, kanun maddesini iptal etmiştir.

İlgili kararlar verildiğinde Kanun henüz tasarı halinde olup yasalaşmamıştır. Bugün için KVKK özel nitelikli kişisel verilerin işlenmesi ile ilgili usul ve esasları düzenlemiştir ve Kurul'un da yayımladığı rehber, ilke kararı ve özet kararlar uygulamaya yol gösterici niteliktedir. Fakat yine de görüldüğü üzere gittikçe kullanımı yaygınlaşan biyometrik veriye özel bir düzenleme söz konusu değildir.

Örneğin 6222 Sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un Seyirden Yasaklama başlıklı 18. maddesinin 8. Fıkrasına 2019'da yapılan değişiklikle "*kolluk birimlerince biyometrik*

yöntemler de kullanılabilir" hükmüne yer verilmiştir. 6114 Ölçme, Seçme ve Yerleştirme Merkezi Hizmetleri Hakkında Kanun'un Sınav Güvenliği başlıklı 9. maddesinin 6. fıkrasında, ÖSYM Başkanlığının aday ve görevlileri için biyometrik yöntemlerle kimlik doğrulaması yapılabileceği ve elde edilen verilerin sınav hizmetlerinde kullanılmak üzere saklanabileceği düzenlenmiştir. Daha önce de açıklandığı gibi temel bir hak ve özgürlüğe müdahalenin nedeni, gerekliliği, son çare olması için alternatif yöntemleri, uygulamanın hangi yöntem ile gerçekleştirileceği düzenleme amacına özel olarak bütün yönleriyle kanun metnin yer almalıdır.

Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine İlişkin Yönetmeliğin 6. maddesinin 2. fıkrasında "*uzaktan kimlik tespiti sürecinde, kişinin uzaktan kimlik tespitinin yapılması amacıyla özel nitelikli kişisel verilerden sadece biyometrik verisi kullanılabilir ve kişinin buna dair açık rızası elektronik ortamda kayıt altına alınır"* hükmündeki biyometrik veri kullanmaya cevaz veren yöntem bir yönetmelik maddesi olarak düzenlenmiştir. Bunun açık rızaya bağlanmış olması biyometrik veri işleme sürecinin yönetmelikle düzenlenebileceği anlamına gelmemelidir. Açık rıza bir hukuka uygunluk sebebi ve bir idari tedbir olmakla birlikte alınan her açık rıza, ölçülülük ve veri minimizasyonu ilkesi karşısında biyometrik veri işlenmesini meşrulaştırmayacaktır. Bu sebeple yine kanun ile düzenlenmelidir. Şu haliyle yönetmelik metninde açık rıza verilmemesi imkanın olup olmadığı, açık rıza verilmemesi halinde alınacak aksiyonun ne olduğu, açık rızanın geri alınması halinde ilgili kimlik tespitinin akıbeti ve bu kimlik onayı saklanırken ilgili kişinin onay bilgisi ile birlikte biyometrik verisinin de saklanıp saklanmayacağı gibi ilk akla gelen soruların cevabı yoktur. Bu soruların cevabının henüz daha biyometrik verinin tanımının yapılmadığı Kişisel Verilerin Korunması Kanununda veya Kurum tarafından düzenlenen ikinci mevzuat veya rehberlerde cevabının da olması imkan dahilinde değildir. Örneğin Kurul, 2019/165 ve 2020/167 sayılı "Spor Salonu" kararlarında açık rıza alınmış olsa dahi biyometrik veri işlenemeyeceğini kararlarında geçirmiştir. Veri sorumlularının Kurul'un bu yaklaşımından haberdar olması için ve bu kararlarında neden böyle bir ifadenin yer aldığını anlamaları için uzman olmaları gerekmektedir. Elbette biyometrik verileri düzenleyen özel hükümler her zaman uygulama alanı bulacaktır fakat bu düşünce ile temel çerçevenin yer almadığı kanun maddelerinin düzenlenmesi, temel hak ve özgürlük kapsamındaki biyometrik verinin yönetmeliklerle düzenlenmesinin önü açılmış olacaktır.

Nitekim dayanak Kanun olan At Yarışları Kanununda herhangi bir düzenleme olmamasına rağmen At Yarışları Yönetmeliği'nin Atların Koşulara Kaydı başlıklı 29. maddesinde "*Yarış Müessesesi kayıt yapanın kimlik tespiti için biyometrik kimlik doğrulama yöntemlerini (parmak izi tanıma, yüz tanıma, avuç içi damar tanıma ve benzeri) kullanabilir. Biyometrik kimlik tanıma yönteminin kullanılması halinde ayrıca kişilerin imzasının alınmasına gerek yoktur.*" hükmüne yer verilmiştir. Kanuni dayanağı olmayan ilgili işlemin alternatifinin imza olduğu da bizatihi hükmün içerisinde yer almakta olup, biyometrik kimlik doğrulama varsa imza alınmasına gerek yoktur yazılmıştır. Dahası ilgili yönetmelik, Kanun'un yürürlükte tarihinden sonra 23/6/2018'de düzenlenmiştir. Kanaatimizce yönetmeliğe eklenen bu hüküm kanunlarda düzenlenme şartını karşılayacak nitelikte değildir ve benzer yönetmelik düzenlemelerine karşı idareler nezdinde derhal farkındalık yaratılmalıdır.

Burada alternatif bir çözüm önerisi olarak da gittikçe kullanımı artan, gelecekte ne tür kullanımların olacağını bilmediğimiz, veri sorumlularının nasıl davranmasının gerektiğinden emin olamadığı biyometrik verilerin işlenmesini düzenleyen bir kanun da düşünülebilir. Nitekim Amerika Birleşik Devletleri'nde New York, California, Washington, Illinois ve Texas eyaletlerinde biyometrik veriler için sıkı denilebilecek özel kanunlarla konu düzenlenmiştir.

Özel kanun düzenlemesinin de sürekli gelişen teknolojiden geri kalacağı gerçeği karşısında genel ilkelerin belirlendiği bir temel kanun daha yerinde olacaktır. Buna ek olarak AB GVKT m. 35 ve 36'da öngörüldüğü gibi etki değerleme raporu çalışmasının da KVKK'ya dahil edilmesi yine önemli bir çözüm olacaktır.

İlgili Kişinin Açık Rızası

Bu şart, veri sorumlusu tarafından ilgili kişinin doğru şekilde bilgilendirilen ilgili kişinin, özgür iradesi kısıtlanmadan belirli bir amaçla ilgili vermiş olduğu açık rızadır. Kişisel verilerin işlenmesinde yasanın 4.maddesine aykırılık, bireyin temel hak ve özgürlüklerine, özel hayatının gizliliği ve kişilik haklarına müdahale halleri ancak ilgili kişinin kurallara uygun açık rızasının olması halinde ortadan kalkacaktır.

Biyometrik veri işleme gibi teknik bir hususta sade, anlaşılır, ilgili kişiye sonuçları hakkında bilgi veren bir aydınlatma yapmak hiç şüphesiz oldukça zordur. Fakat işlenen verinin ilgili kişinin ömrü boyunca değiştiremeyecek olması ve gelecekte ortaya çıkabilecek yeni teknolojiler de düşünüldüğünde genel kişisel verilere nazaran daha nitelikli bir aydınlatmanın yapılması gerekmektedir. Aydınlatma kurallarına aykırı bir bilgilendirme ile alınan, genel sözleşmenin içerisine sıkıştırılmış, bütün verilerin işlenmesine rıza veren, ilgili hizmetin alınması için ön şart olan bir açık rıza beyanları geçerli kabul edilemeyecektir (Kişisel Verileri Koruma Kurumu, Açık Rıza Rehberi).

Aydınlatma Tebliğinin 5. maddesinin (b) fıkrasına göre; aydınlatma, açık rıza alınmadan önce ve açık rızadan ayrı olarak yapılmalıdır. Biyometrik veri işleme için aydınlatma zamanı öncelikle ilk biyometrik veri kaydı esnasında yapılabilir. Devamında da biyometrik verinin işlendiği kimlik tespiti ve doğrulama alanlarında katmanlı aydınlatma ile yöntemiyle rızanın yorgunluğunun da önüne geçilmiş olacaktır.

Özgür iradeye dayalı açık rıza açıklama şartı biyometrik veri işlemelerinde en sık tartışılan hususlardan birisidir. Nitekim özellikle işçi-işveren ilişkisinde ölçülülük temel ilkesi ile sürekli yan yana gelmektedir ve çoğu zaman birbirine karışmaktadır. Aşağıda ölçülülük ilkesi ele alındıktan sonra daha ayrıntılı olarak bu iki kavram ele alınacaktır.

Özgür iradeye dayalı açık rıza açıklanması, ilgili kişi kurallara uygun bir aydınlatmanın ardından kararını etkileyen hiçbir tesirin altında kalmaksızın kişisel verisinin işlenmesine rıza göstermesidir. Taraflar eşit değilse özgür iradenin değerlendirilmesi gerekir. İşveren tarafından işçiden alınan açık rıza kapsamında mesai takibi için biyometrik veri kullanılması durumunda, işçiden açık rıza alınırken reddetme imkanının sunulmamış olması ya da rıza göstermemesi halinde iş kaybı gibi bir olumsuzluk yaşanacağının hissettirilmesi halinde özgür iradeye dayalı bir açık rızadan söz edilemeyecektir (Kişisel Verileri Koruma Kurumu, Açık Rıza Rehberi). Kanunlarda öngörülmese de ölçülülük ilkesine uyumlu bir biyometrik veri işleme faaliyetinin ancak açık rıza ile gerçekleştirilebilecektir. Bu hususta her ne kadar çalışanların özgür iradesiyle güvenlik sebebiyle gereklilik hali karşı karşıya gelse de bu güvenliğin tesis edilmesinden sorumlu olan kişiler aynı zamanda biyometrik verisi işlenen çalışanlar olduğu için gayet bilinçli bir şekilde bu açık rızalarını vermektedirler.

Açık rızaya dayanılan hallerde veri sorumlusu, veri sahibi ilgili kişiye biyometrik uygulama yerine bir alternatif sunmalıdır. Aksi durumda açık rızanın hizmet şartına bağlanması söz konusu olacaktır. Kişisel Verileri Koruma Kurulu, 12/08/2021 tarihli ve 2021/799 sayılı Kararında bir sınavın güvenilirliğini ve güvenliğini sağlamak üzere herhangi bir alternatif sunulmaksızın veri sahibi ilgili kişilerden parmak tarama kayıtları alınmasını, rızanın kanunda sayılan unsurları barındırmadığı gerekçesiyle veri güvenliğine ilişkin yükümlülüklerin ihlali olarak değerlendirmiştir.

Kişisel Verileri Koruma Kurulu, 20/05/2020 tarihli ve 2020/404 sayılı Kararında işçi-işveren ilişkisinde biyometrik uygulamaların kullanımını ele almış, işverenin biyometrik uygulama kullanımına açık rıza vermeyen çalışanlarla ilgili bir liste tutmasını, bu kişilerin ikna edilmesi için başkaca çalışanlardan yardım talep etmesini ve biyometrik uygulama kullanımına açık rıza vermeyen çalışanların özlük kayıtlarının işveren tarafından eksik özlük kaydı olarak kabul edilmesini hukuka aykırı bulmuştur.

Müşteri ilişkilerinde her ne kadar taraflar eşit konumda gibi görünseler de işletmelerin kurgularının veya çalışanlarının yeterli zaman ayırmaması sebebiyle çoğu zaman biyometrik veri işlemelerine baskı altında dikkatsizce veya mecburen onay verdiği de görülmektedir. Burada işletmeler ekonomik menfaatleri gereği özellikle kimlik doğrulama için kart geçiş sistemlerini yerine biyometrik sistemleri tercih etmemektedirler. Müşterilere sunulan hizmet sözleşmesinin bir maddesinde bu konuya değinmekte hatta biyometrik veri için rıza verilmemesi halinde hizmet verilemeyeceği dahi düzenlenmektedir. Kurul, 2020/167 numaralı kararında bir hizmetin sunumunun, açık rıza verme ön şartına bağlanmaması gerektiği tespit edildikten sonra avuç içi izinin alınmasına onay verilmesinin sözleşmenin kurulması için zorunlu bir şart olarak üyelik sözleşmesinde yer verildiği ve bu şarta uyulmaması halinde spor salonuna fesih hakkı tanınmış olduğundan açık rızaların özgür irade ile verilmediği sonucuna ulaşılmıştır.

İngiltere Gelir ve Gümrük Dairesi (HMRC) yardım hattında müşterin kimliklerini tespit etmek amacıyla Sesli Kimlik sistemi (Voice ID system) kullanmaktadır. Ses doğrulama sistemi kullanılması sonucu, yaklaşık 7 milyon müşterinin biyometrik verilerinin yasadışı bir şekilde işlendiği tespit edilmiştir. Birleşik Krallık Veri Koruma Otoritesi (ICO) yaptığı incelemede, HMRC'nin müşterilerinin biyometrik verilerinin nasıl işleneceği hakkında yeterli bilgi vermediğini ve kimlik doğrulama için alternatif bir yöntem sunmadığını tespit etmiştir. ICO, HMRC'ye ve HMRC adına biyometrik verileri işleyenlere, açık rızası olmayan müştere ait kayıtları (5 milyondan fazla kayıt) silinmesine karar vermiştir (ICO, 2018).

Biyometrik veriler internette kullanıcıların kendilerinin paylaştığı içeriklerden de üretilebilir. Sosyal paylaşım ağlarına eklenen videolardan ses tanıma veya fotoğraflardan görüntü tanıma yapılabilir. Kullanıcıların kendi rızalarıyla alenileştirdiği bu içeriklerden biyometrik veri şablonları çıkarılabilir ardından da gerçek kişi kimlikleriyle eşleştirilmiş milyonlarca insanın veritabanı oluşturulabilir. Bu bahsettiğimiz hususu gerçekleştiren girişim Clearview AI hakkında Fransız Veri Koruma Otoritesi inceleme başlatmış ve Fransız vatandaşlarının verilerinin silinmesi şirkete süre vermiştir (CNIL, 2021). Aynı şekilde İngiltere Veri Koruma otoritesi de şirketin faaliyetlerini incelemeye aldı ve 17 milyon GBP para cezası verdimiştir (ICO, 2021). Facebook, Youtube, Google ve Twitter şirkete yazı gönderip, faaliyetlerini sonlandırmasını istedi fakat dünyanın en büyük yüz tanıma veritabanı olarak kendisini tanıtan şirketin en büyük müşterilerinin devletler olduğu düşünüldüğünde çalışmalarını tam olarak sonlandıracakları şüphelidir. Nitekim şirketin ürününü Ukrayna, Rusya ile aralarındaki savaşta gerek ölenlerin tespiti gerekse asker sivil ayrımı için kullanıldığına dair haberler de basında yer almıştır (Reuters, 2022).

Açık rıza açısından yüz tanıma sistemlerinde dikkat çekilmesi gereken bir konuda yüz okumak için yerleştirilmiş cihazlar ilgili kişiler tarafından kolaylıkla fark edilememektedir. Fark edilecek seviye bir uyarı olsa da bu defa kimlik tespiti için yerleştirilmiş yüz okuyucuların taramasına maruz kalmak istemeyen ilgili kişiler için alternatif oluşturulması gerekmektedir. Bütün hukuka uygunluk şartlarını taşıyan bir yüz tanıma sistemi kimlik eşleştirmesi yapmak için görüş alanına giren bütün yüzleri okuyup önceden kayıtlı veritabanı ile eşleştirmeye çalışacaktır. Bu sebeple görüş alanına açık rıza alınmamış kişilerin girmesinin engellenmesi gerekmektedir (EDPB, 2020).

KVKK DOĞRULTUSUNDA BİYOMETRİK KİŞİSEL VERİLERİN İŞLENMESİNDE GENEL İLKELER

Hukuka ve Dürüstlük Kurallarına Uygun Olma

Bu ilke, bireylerin kişisel verilerinin işlenmesinde, veri sorumlusunun Anayasa ve diğer yasalarla ortaya konulan tüm kural, düzenleme ve şartların gereğini yerine getirmeyi, ayrıca verilerin kaydı yapılırken veri sahibi ilgili kişinin çıkarlarını ve hakkaniyete uygun taleplerini de dikkate almak, veri sahibinin

zararına hareket etmemek anlamına gelmektedir. Hukuk kuralları denince, evrensel hukuk ilkelerini de içine alacak şekilde geniş anlamda yorumlamak gereklidir. Yani veri sorumlusu sadece 6698 sayılı KVKK kanunu değil, kişisel verilerin işlenmesini düzenleyen tüm genel hukuk kurallarını ve Anayasayı da dikkate almak zorundadır. Dürüstlük, veri sahibi ilgili kişinin hak ve menfaatlerini kısmen veya tamamen ortadan kaldıracak nitelikte haksızlık oluşturacak hareketlerde bulunmamak, kişisel verilerin işlenmesinin veri sahibinin makul beklentilerinin karşılanması ve açıklanan amacın dışına çıkılmaması suretiyle yapılmasıdır.

Kişisel verilerin yasalara uyumlu bir şekilde ele alınması, Kanun'da belirtilen diğer ilkelerin temel dayanağını oluşturmaktadır. Veri sorumluları, verileri işlerken "adil bir tutum sergileme" yükümlülüğüne sahip olmaları amaçlanan bir düzenlemeye tabidirler (Küzeci, 2010; Çekin, 2020).

Doğru ve Güncel Olma

Bu ilke ile hem veri sorumlusuna hem de veri sahibine dürüst davranma sorumluluğu yüklenmektedir. İşlenen verinin doğru ve güncel olması, veri sahibi ilgilisinin bilgi verdiği konuda gerçeğe uygun beyanda bulunması veri sorumlusunu yanıltmaması anlamına gelmektedir. Beyan edilen verilerin doğru ve güncel olması ilkesi, bireylerin daha önce kaydedilmiş kişisel verileri düzeltme hakkı ile de doğrudan bağlantılıdır. Kişisel verinin işlenmesi sırasında, veri sahibi ilgili kişinin beyanının kayda doğru olarak geçilmesi ve gerektiği zamanlarda verinin sahibinin bilgi ve rızası doğrultusunda güncellenmesi bu ilke kapsamındadır.

Veri sorumluları, ilgili kişinin açık rızasını aldıktan sonra, beyanına istinaden, verileri doğru ve güncel tutmak hususunda kendilerinden beklenen seviyede bir özen göstermeleri beklenir. (Bainbridge, 2000, Çekin, 2020). Aksi takdirde, ilgili kişinin temel hak ve özgürlüklerine, özellikle ekonomik çıkarlarına ve manevi bütünlüğüne zarar verme riski doğurabilir. (Develioğlu, 2017).

Belirli, Açık ve Meşru Amaçlar İçin İşlenme

KVKK m. 4 f. 2 (c) bendine yer alan bu ilke, veri sorumlusunun kişisel veriyi işleme amacını belirli olacak şekilde net ve anlaşılabilir nitelikte ortaya koymasını bu amacın makul ve kabul edilebilir olması anlamına gelmektedir. Veri işleme faaliyetinin amacı işleme faaliyetinin esas sebebi olduğu için özel bir önem arz etmektedir (WP29 203, 2013). Biyometrik veriler açısından belirli, açık ve meşru amaç genel olarak güvenlik tedbirleri için gerekli olması olarak kabul edilebilir. İlgili kişiye, sistemin mantığına dair bilgiler verilmeli, biyometrik veri işleme faaliyetinin ilgili kişi açısından ne derece önem taşıdığını ve amaçlanan sonuçları içermelidir (Çekin, 2016).

Biyometrik veri işlemenin karmaşıklığı ortadadır, bütün ayrıntılarıyla ilgili kişiye belirli ve açık bir bilgilendirme yapmak kolay değildir, hatta belirliliği oradan da kaldırabilecek yaklaşım haline de gelebilir. Fakat biyometrik veri işleme ile ilgili gerekliliğin belirli ve açık şekilde ortaya konması gerekmektedir. Biyometrik verinin ilk işlenmesi kişinin biyometrik verisinin kayıt edildiği andır. Bu ilk toplamadan sonra gerçekleşen her türlü işleme amacı, ilk işleme amacına uygun olmalıdır ve uygunluk değerlendirilmesi toplama amacına göre yapılacaktır (Yücedağ, 2019).

Aydınlatma Tebliğinde her ne kadar kişisel verilerin sayılmasına dair bir hüküm olmasa da Kanunun ruhu gereği en azından kategorik bazda bildirilmesinin ve hukuki sebeplerle bir eşleştirme yapılmasının beklendiğini örneğin 08/10/2020 Tarihli ve 2020/765 sayılı kararından anlamaktayız. Bu bağlamda biyometrik veri gibi özel nitelikli kişisel verilerin açık rıza ile işlenmesi halinde bunun da aydınlatma metnin de ayrıca gösterilmesi faydalı olacaktır. Zira açık rıza alma aşamasında aydınlatma ve açık rızanın ayrı olması da Kurul'un rehberlerinde yer alan diğer bir beklentidir.

Kanun düzenlemesi veri sorumlularına belirli görev ve yükümlülükler yüklediği gibi, kişisel veri sahiplerinin haklarını da 11. maddede hüküm altına almıştır. Buna göre veri sahibi veri sorumlusuna başvuru yaparak bu madde kapsamında bilgi talebinde bulunabilmektedir. Bu haklardan amaca uygun kullanım, eksik veya yanlış işleme hakkında sorular, silme veya yok etme talebi, otomatik sistemler ile analiz edilmesi sonucu aleyhe çıkan sonuçlara itiraz etme veri sorumlusu için en kritik talepler olacaktır. Hollanda Veri Koruma Otoritesi (DPA) bir şirketteki çalışanların işe giriş çıkış saatlerinin denetlenmesi amacıyla toplanan parmak izi verisinin hukuka aykırı olarak işlendiğine karar vermiştir. Kuruma göre, şirketin biyometrik veri işleme faaliyetinde GVKT'deki açık rıza dışındaki veri işleme şartları mevcut değildir. Açık rıza konusunda ise işveren ve çalışan arasındaki iş ilişkisi göz önüne alındığında, çalışanların özgürce rıza veremeyeceği dolasıyla onların açık rızasının geçerli sayılmayacağı belirtilmiştir. Nitekim çalışanlar açık ve belirli şekilde aydınlatılmadıkları için bu rızayı verirken bir çalışmak için bir zorunluluk olduğunu düşündükleri ortaya çıkmıştır (DPA, 2020).

İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Ölçülülük ilkesi, araç ve amaç ilişkisidir. Amaca ulaşmak için seçilen aracın denetlenmesidir. Kamu Hukuku açısından kanun koyucunun belirlediği veya idare tarafından kullanılan aracın, ulaşılmak istenen amaç için elverişlilik, gereklilik, amaç ile araç arasında orantılılık sorunuyla ilgilidir. Temel haklara müdahalelerde yalnızca ulaşılmak istenen amaca bir katkı sağlayan ve en az yükümlülük getiren araçlar kullanılarak, sınırlamadaki orantılılık korunmalıdır (Metin, 2017). Amaçla bağlantılı ve sınırlı bir faaliyet için işlenen verilerin hedeflenen amaca ulaşma için yeterli, elverişli, gerekli ve uygun olmasını, söz konusu amaç için gerekli olmayan, ilgisiz ve gereksiz kişisel verilerin kaydedilmesinden kaçınmak olarak kabul etmek gereklidir. Hukuka uygun bir amaç için kayıt edilen iris görüntüsü, sağlık sorunlarının tespiti için kullanılmamalıdır.

Kişiye özgü ve özel nitelikte olan biyometrik kişisel veriler hakkında gerek 6698 Sayılı Kanunda ve diğer kanunlarda, gerekse alt yönetmeliklerde yer alan hukuksal koruma, veri işlemenin sıkı kurallara tabi olması nedeniyle geniş ve etkili olmakla birlikte, bu hukuksal koruma sürekli ve mutlak değildir. Mutlak olmama, başka Anayasal hak veya özgürlükler ile çatıştığında ve karşı karşıya geldiğinde sınırlandırılabilir veya tamamen ortadan kaldırılabilir anlamına gelmektedir. (Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu ve Uygulaması Rehberi, 2017)

Bireylerin kişisel verilerinin işlenmesi, özel hayatın gizliliği ve dokunulmazlığı kapsamında değerlendirilerek, temel hak ve özgürlüklerin korunmasının esas, kısıtlanmasının ise istisna olduğu da dikkate alındığında belirlenen amaca kişisel verilerin işlenmesi haricinde ulaşılabiliyorsa, bu yöntemler tercih edilmelidir. Veri işleme faaliyeti gerekliliksе bu durumda da kişisel verilerin korunması hedeflenen temel hak ve özgürlüklere hiç veya daha az müdahale eden yolun tercih edilmesi doğru olacaktır (Çekin, 2018). Temel hak ve özgürlüğün korunması açısından en elverişli ve uygun aracın kabul edilmesi ölçülülük ilkesinin zorunlu şartı olarak ortaya çıkmaktadır (Şimşek, O. 2008). Kişisel veriler işlenirken belirlenen makul amaca ulaşmaya yetecek düzeyde ve en az sayıda verinin işlenmesi esastır.

Yasal olarak sıkı şartlara bağlanmış olan veri işlemenin, amaçla uyumlu, sınırlı ve ölçülü olması gerekir. Bu nedenle, veri işleme sırasında var olmayan veya gerçekleşmemiş olan, gelecekte kişisel verinin faydalı olabileceği ihtimali ile belirsiz ve muğlak şekilde veri işlenmesinin kabul edilmesi mümkün değildir (Jay/Hamilton, 2003). Yine işlenen ve saklanan biyometrik veriler doğru olmalıdır ve geçerli, kabul edilen gayelere ulaşmaya yeterli seviyede ve gerektiği kadar kaydedilmelidir. Belirlenen ve hedeflenen makul amacın gerektirdiğinden daha fazla biyometrik verinin işlenmesi veya saklanması, veri işlemenin yasal şartlarından olan ölçülülük, iyi niyet ve dürüstlük ilkelerine aykırılık oluşturacaktır.

Biyometrik kişisel verilerin işlenmesinde en çok ihlal edilen ve göz ardı edilen ilke ölçülülüktür. Zira veri sorumlularının veri işleme eylemi sadece bir kez icra edilen nitelikte bir eylem olmayıp, zaman

içerisinde uzunca bir süre devam eder mahiyettedir. Hal böyle olunca, veri sorumluları veri işlemenin başında veri sahibinin açık rızasını aldıktan sonra, veri işlemede zaman zaman keyfi ve ölçüsüz davranabilmektedirler. Bu bağlamda veri sorumluları bazen hedeflenen makul amacı aşan seviyede yersiz, gereksiz ve fazladan kişisel veri işleyerek hak ihlallerine ve kişisel zararlara yol açabilmektedir. Anayasa Mahkemesinin kararlarında görüldüğü üzere ölçülülük ilkesi; amaç ve araç arasında hakkaniyete uygun bir dengedir. Ölçülülük, veri işlemenin amaca ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranda olmasını ve sınırlayıcı önlemin zorunlu olmasını içeren bir ilkedir. (Anayasa Mahkemesi 26.12.2013, E:2013/67, K:2013/164, 27.3.2014 T. 28954 sayılı R.G.) Bu ilke, idarenin sınırlayıcı kararı ile karşı karşıya gelen, çatışan temel hak ve özgürlükler arasında denge kurmayı sağlamaktadır (Oğurlu, Y., 2002).

Biyometrik verilerin, işlenme amacına uygun şekilde ölçülü ve kişilerin mağduriyetime sebep olmayacak şekilde bireysel haklar ve beklenen fayda dengesi gözetilerek işlenmesi gerekir. Örneğin bir okulda öğrencilerin giriş çıkışlarını kolaylıkla yapabilmesi için parmak izi yönteminin kullanılması ölçülülük ilkesine aykırıdır (Develioğlu, 2017).

Teknolojinin takip kolaylığını artırması sonucu yaygın şekilde işçi ve memurların mesai takibinin biyometrik veri ile yapılmaktadır. İşçi ve işveren arasındaki en temel maddi ilişki ücret ile ilgilidir. İşçi aylık belirli bir zamanını işverene özgülerken, işveren de bu zaman karşılığında işçiye bir ödeme yapmaktadır. İşverenin mesai takibini biyometrik veri ile yapmasındaki temel motivasyon da bu ödediği ücretin karşılığını mesai takibi ile almak istemesinde yatmaktadır. Bu temel ilişkide işverenin ekonomik çıkarları karşısına işçinin temel ve özgürlükleri konduğunda hiç şüphesiz işçinin temel hakları daha ağır gelmektedir. Anayasa Mahkemesi, Söke Belediyesi'nin çalışanlar için parmak izi ile mesai takibi yapmak için kurduğu sisteme dahil olmak istemeyen çalışanın itirazı, idare mahkeme tarafından kamunun mesai takibi açısından yüksek menfaati olduğu gerekçesiyle reddedilmiştir. Konuyu inceleyen Anayasa Mahkemesi biyometrik verinin ancak açık rıza veya kanunlarda öngörülen hallerde işlenebileceğini ifade ettikten sonra kamu kurum ve kuruluşlarının mesai takibinin özel nitelikli kişisel veri işleyerek takip edilebileceğine için kanuni bir düzenleme olmadığını tespit ederek başvuruya konu müdahalenin kanunilik şartını sağlamadığına karar verilmiştir (Anayasa Mahkemesi 10.3.2022, Başvuru Numarası: 2018/11988 , 19.4.2022 T. 31814 sayılı R.G.).

Danıştay, personelin mesai takibinde biyometrik sistemlerin kullanılması ile kurumlar tarafından amaçlanan kamu yararı arasında orantılılık ve ölçülülük bulunmadığından ve bu kullanımın sınırlarının, usul ve esaslarının da belirli olmaması nedeniyle hukuka aykırılık tespiti yapmıştır (Danıştay 12. D., 2010; Danıştay 5. D., 2013; Akgül , 2013).

Kurul'un vermiş olduğu "spor salonu" kararlarında açık rıza alınsa dahi biyometrik veri işlenemeyeceği, açık rızanın gerekenden daha fazla veri işlenmesini meşrulaştırmayacağını karara bağlamıştır. Kanunlarda öngörülmedikçe biyometrik veri işlemenin imkansız olduğu akla gelmektedir. Kurul bu kararlarındaki yaklaşımına 2021'de yayımlandığı biyometrik veri işleme rehberinde açıklık getirmiştir. Kurul'a göre ilgili amaca ulaşmak için biyometrik veri işlemekten başka bir alternatif varsa biyometrik verinin işlenmesinin bir gereklilik olmadığı anlaşılacağından ve veri minimizasyonu ilkesine de aykırı olduğundan biyometrik veri işlenmemelidir. Spor salonları üye giriş-çıkışlarında kart gibi bir alternatif varken biyometrik veri işlenmesini ölçülülük temel ilkesine uygun bulmadığı için açık rıza ile işlenmesinin faaliyeti hukuka uygun hale getirmediği sonucuna varılmaktadır. Önce ölçülülük ilkesine uyum sağlanması ardından mevzuata uygun açık rızanın varlığı aranmaktadır.

Gizli devlet sırrı niteliği taşıyan askeri alanda herhangi bir silah üretim tesisine girişte biyometrik uygulamalarla kimlik tespiti yapılması ölçülü bulunabilir. 24 saat içerisinde işlenmesi gereken çiğ sütün işlem steril alanların korunması, kamu sağlığı için süt tanklarına yabancı madde eklenmesinin engellenmesi, bu alanlara tam korumalı özel elbise ile girilmesinden dolayı kartlı geçiş sisteminde bizatihi kartın kirletici olmasından dolayı uygun olmaması sebebiyle yüz tanıma sistemi kullanılmasının denge testinden geçebileceği söylenebilir. Bir işletmenin hassas verilerinin tutulduğu veri merkezine giriş-çıkış kontrolünün diğer yöntemlerin yetersiz kalması sebebiyle biyometrik veri işleyen sistemlerle yapılabilir (WP29, 2017/2, s.18-19). Tehlikeli virüslerle ilgili araştırma yapan bir şirketteki laboratuvara

sadece yetkili ve güvenilir araştırmacıların girdiğinden emin olmak geçişlerde için biyometrik veri kullanılabileceğine dair bir örnek de Kurum rehberinde yer almaktadır (Kişisel Verileri Koruma Kurumu Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber İlke Kararı, 2021). Bir bankanın veri merkezine giriş çıkışlarda, buraya girmesi gereken çalışanlardan açık rıza alarak biyometrik geçiş sistemlerinin güvenlik amacıyla kullanılması kabul edilebilirken, bu sistemin çalışanların mesai takibi için kullanılması ölçülülük ilkesine uygun düşmeyecektir. Bu seçimleri yaparken çalışanların haklarına en az zarar verecek yöntemin seçilmesi gerekmektedir (Akgül, 2015). Nitekim Anayasa Mahkemesi ölçülülük ilkesi için temel hal ve özgürlüklere getirilecek sınırlamalarda seçilen yöntemin son çare olması, ilgili müdahale ile alınan tedbirin temel haklara en az müdahale eden yöntem olup olmadığının da kontrol edilmesi gerektiğini belirtmiştir (Anayasa Mahkemesi, 2018).

Görüldüğü üzere biyometrik veriler açısından ölçülülük ilkesinin unsurlarından olan gereklilik, amaca uygunluk ve elverişlilikten daha çok ön plana çıkmaktadır. Gereklilik unsurunun tartışıldığı örneklerde kişinin tanımlanmasının bir gereklilik olması ve bunun alternatifinin de biyometrik veri kadar olmaması ve riskin de alınmayacak olmasından dolayı uygulanabilir olduğu kabul edilmektedir. Yukarıda örnekleri verilen istisnai durumlara izin veren bir düzenleme Kanun'da yer almadığı için ancak açık rıza ile bu faaliyetler gerçekleştirilebileceğine değinilmiştir fakat bir veri merkezinde çalışan işverenden alınacak açık rızanın, her ne kadar üstün bir gereklilik hali olsa da, özgür irade açısından klasik işçi-işveren eşitsizliği üzerinden bir tartışmaya yol açabileceği de bir gerçektir. Kanunda sağlık verilerinin işlenmesinde getirilen açıklık biyometrik veri için de getirilebilir. Böylece rehberde de örnek olarak verilen istisnai durumlar için açık rıza almanın yaratabileceği sorunlara da yol açmadan uygulama alanı bulunabilecektir. Örneğin Fransız Veri Koruma Kanunun 8. maddesinde ve Hollanda Veri Koruma Kanunun 29. maddesinde gereklilik halinde biyometrik veri işlemenin yapılabileceğini düzenlemiştir. Hollanda Veri Koruma Otoritesi yetkilileri bir süpermarketin hırsızlık ile mücadele için yüz tanıma sistemleri kurması üzerine yapılan açıklamada kanında geçen gereklilik çıtasının oldukça yüksek olduğunun altını çizmek için biyometrik veri kullanmanın ancak bir nükleer tesis güvenliğini sağlamak için bir gereklilik olduğunun kabul edilebileceğini beyan etmişlerdir (DPA, 2020).

Yine de bir gerçek kişi bütün temel ilke ve veri işleme şartlarının yerine getirildiği bir yüz tanımaya dayalı veri işleme faaliyetine izin veremez mi? Devlet otoritesi, salt alternatifi olduğu için veya gerekli olmadığı için vatandaşının iradesine aşırı bir korumacı yaklaşım ile müdahale edebilir mi? Konaklama sektörü misafir memnuniyetinin sadakati artırdığı için buna ticari olarak yatırım yapmaya hazırdır. Örneğin müşteriye misafir olarak hitap edilen, konforun ön planda olduğu turizm sektöründe ilgili kişilerden alınan açık rıza ile yüz tanıma sisteminin nimetlerden faydalanıldığı bir örnek kurguyu ele alalım. Otelin yüz tanıma sisteminin kullanıldığı ayrı kapısından geçiş yapan misafirin işlemleri otomatik olarak hazırlamakta böylece klasik resepsiyon ziyareti saniyelere düşmektedir sadece girişte yüz tanımaya izin verdiklerinin sistem tarafından anlaşılması için bir yaka kartı teslim edilmektedir. Bütün çalışanlar kullandıkları gözlük sayesinde misafirleri tanımakta ve anlık olarak misafirin muhtemel talepleri kendilerine iletilmektedir nitekim sistem misafirin memnuniyet durumunu yüz mimiklerini takip ederek ölçmektedir. Restoran bölümüne giriş yaptığında her zamanki tercihlerine göre servis yapılmaktadır. Bu kurgunun teknolojik alt yapısı günümüzde mevcuttur bir kısmı da halihazır da uygulanmaktadır. Fakat ilgili kişiler veri koruma otoritelerinin konuya yaklaşımına göre bu servislerden istifade edeceklerdir. Kanaatimizce aceleye getirmeden, pazarlama unsurları kullanılmadan riskin anlatılarak yeterli aydınlatmanın yapıldığı, toplanan verilerin sadece amaçlar için kullanıldığının denetlendiği ve tek tek sürelerin belirlenerek kısa sürede imha edildiği, tasarımda mahremiyet ilkelerine göre geliştirilen ve güvenli bir etki analiz raporu sahibi otellerden ilgili kişilerin bu çok özel hizmeti açık rıza ile alabilmelerinin önünde bir engel olmamalıdır. Bu özel hizmet için açık rızanın ön şartı olduğu iddiası gündeme gelebilir fakat misafirler bu uygulama olmadan da temel hizmeti alabildikleri için sorun olmayacaktır. Nitekim sadakat kart uygulaması kararında Kurul indirimden faydalanmadan da alışveriş yapılabildiği için alınan açık rızanın hizmetin ön şartı olmadığına karar vermiştir (Kurul, 2019).

İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

Kişisel verilerin veri sorumlusu tarafından elde edilmesi ve işlenmesi akabinde, bu verilerin ne kadar saklanacağı sorunu ortaya çıkmaktadır. Kişisel verilerin saklanması, veri sahibinin menfaatlerinin korunması adına, veri sorumlusunun insiyatifine bırakılmamıştır. KVKK m. 4 f. (d) bendine göre veri sorumluları veri işlenme amacına dair yasalarda verilerin saklanması ve korunması için düzenlenmiş bir zaman aralığı var ise bu sürenin dolduğu tarihe kadar kişilere ait verileri saklayacaktır. Ancak yasalarda veri saklama ile ilgili bir süre belirlenmemişse de verilerin kaydedilmesindeki amacın gerçekleşmesi için yeterli, gerekli ve makul süre kadar saklayacaklardır. Kişilere ait veriler, kanunlarda düzenlenmiş sürenin dolması ya da beklenen amacın gerçekleşmesi sonrasında gelecekte kullanma ihtimaline dayanılarak saklanamazlar. Bu ilke kişisel verilerin saklanmasında zaman ve amaç sınırını belirleyerek, veri sorumlusunun verileri saklamasında keyfi davranmasını yasaklamaktadır. İlgili kanunda düzenlenen sürenin dolması ya da veri saklama amacının gerçekleşmesi sonrasında, veri işleyenin elinde bulundurduğu kişisel verileri yok etme ve silme yükümlülüğü ortaya çıkmakta olup, veri sorumlusu tarafından bu yükümlülüğün yerine getirilmemesi de hukuki ve cezai sorumluluk gerektirecektir.

Biyometrik verilerin muhafaza edilmesi için gerekli olan zaman belirlenmesinde biyometrik verinin işlenme amacı belirleyicidir. Kişisel verilerin muhafaza edilme süresinin bitimi, kişisel verilerin kaydedilme amacının sona ermesi, artık kişisel veri işlenmesinden kişisel veya kamusal bir fayda sağlanamayacak olması halinde söz konusu olacaktır. Biyometrik veriler, yine hedeflenen amaca da uygun olarak, güncel ve ilgili kanunda yer alan usullere uygun şekilde muhafaza edilmelidir. Bu konuda Kişisel Verileri Koruma Kurulu'nun 30.01.2018 tarihinde yayımladığı özel nitelikli kişisel verilerin işlenmesinde alınması gereken tedbirlerle ilgili kararı yol göstericidir. İşlenme amacı ortadan kalkan biyometrik veri gecikmeksizin/derhal imha edilmelidir (Kişisel Verileri Koruma Kurumu, 2021). Örneğin bir hastanenin veri merkezine giriş-çıkışın sadece bilgi işlem personeli tarafından yapılması gerektiği için ilgili personelden alınan biyometrik veri, personelin bu veri merkezine girmesini gerektirmeyen başka bir göreve atanması veya işten ayrılması halinde derhal yok edilmelidir.

Biyometrik verilen açısından şayet kanuna dayalı bir işleme faaliyeti varsa muhafaza süresi de bu kanundan hareketle belirlenebilecektir. Şayet açık rıza ile bir veri işleme faaliyeti varsa muhafaza süresi bu açık rızaya dayalı amacın ortadan kalması ile veya ilgilinin kişinin açık rızasını geri almasıyla muhafaza süresi dolmuş olacaktır. Muhafaza süresinin uzatılması veri sorumlusunun da riskinin artması anlamına gelecektir (Dülger, 2020). Biyometrik veriler açısından ise risk çok daha yüksektir ve muhafaza devam sürdükçe veri sorumlusu açısından risk ve maliyet demektir.

Anonimleştirme, özel veya genel kişisel veri ayrımı olmaksızın başka verilerle eşleştirilse dahi hiçbir surette bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Biyometrik veriler tekil olarak ilgili kişiyi tanımlamaktadır. Oluşturulan biyometrik veri şablonu bizatihi koruma altına alınan kişisel verinin kendisidir. Bu sebeple de anonimleştirmenin uygulama alanı olmayacağı kanaatindeyiz.

Biyometrik Veri Güvenliğinin Sağlanması ve Tasarımdan İtibaren Mahremiyet

Diğer kişisel verilerde olduğu gibi biyometrik uygulamalar ile elde edilen verilerin de güvenliğinin sağlanması veri sorumlusunun yükümlülüğü altındadır. Veri sorumlusunun veri güvenliğinin sağlanması ve korunmasına dair yükümlülüğü Kanunun 12. maddesinde kişisel verilerin hukuka aykırı olarak işlenmesinin, erişilmesinin önüne geçilmesi ve muhafazasının sağlanması için alınması teknik ve idari önlemlerin alınması bir zorunluluk olarak bütün siber güvenlik tedbirlerini kapsayacak şekilde düzenlenmiştir. Nitekim bilişim ve teknoloji alanındaki tehditler her an gelişim gösterdiği için Kanunda ayrıntılı bir düzenleme yapılmaması isabetli olmuştur.

Kanunu'nun 6. maddesinin 4. fıkrasında, Kurul tarafından belirlenecek olan yeterli önlemlerin alınması yükümlülüğü belirlenmiştir. Kurul teknik bir standart belirlemek için Kişisel Veri Güvenliği Rehberini yayınlamıştır ve içeriğinde veri sorumluları için genel olarak alınacak tedbirlere yer verilmiştir. Kurul ayrıca Kanunun 6. maddesi kapsamında 31/01/2018 tarihinde özel nitelikli kişisel verilerin korunması için alınabilecek tedbirlerle ilgili rehber niteliğinde bir karar yayımlamıştır. Bu kararda özel nitelikli kişisel veriler için ayrı bir politika ve prosedür hazırlanması, çalışanlar ile ilgili tedbirlerin alınması, kişisel verilerin işlendiği dijital ve fiziki ortamlarla ilgili alınması gereken tedbirler, aktarım ile ilgili alınacak tedbirlere yer verilmiştir. Yine Kurul tarafından 16/09/2021 tarihinde Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber ve İlke Kararı yayımlanmıştır. Biyometrik veri işlenmesinde dikkat edilmesi gereken hususlar maddeler halinde sayılırken, alınması gereken güvenlik tedbirlerine de yer verilmiştir. 2019/12 sayılı Cumhurbaşkanlığı Genelgesi'nde, biyometrik veriler kritik bilgi kapsamında tanımlanmış ve veriler yurtiçinde saklanacağı belirtilmiştir. Dolayısıyla yüz tanıma verileri de yurt dışına transfer edilmemelidir. Bu bağlamda yurtiçindeki bulut bilişim servislerinin sayısı ve niteliği artırılarak vatandaşlarımızın çok hassas verileri olan biyometrik verilerinin yurtiçinde kalması sağlanmalıdır (Erinç, 2020).

Veri sorumlusunun her türlü hukuka aykırı girişimi engellemesi mümkün değildir, bu siber güvenlik dünyasında %100 güvenlik olmaz şeklinde de ifade edilmektedir. Bunun bilincinde olan kanun koyucu burada gerekli önlemlerin alınması şeklinde bir özen sorumluluğu yüklemiştir. Her türlü gerekli tedbirin alınmasına rağmen bir ihlal meydana gelmişse veri sorumlusu gerekli özeni gösterdiğini ispatlaması halinde artık bu sorumluluktan kurtulabilmelidir. (Çekin, 2016) Kişisel Verileri Koruma Kurulunun 09.10.2020 tarih ve 2020/787 sayılı sağlık sektöründe faaliyet gösteren bir şirketin ihlal bildirimi hakkında verdiği kararda veri sorumlusunun üzerine düşen yükümlülükleri yerine getirmesi sebebiyle işlem yapılmasına gerek görülmemiştir. Yine de yüz tanıma verilerinin hassasiyeti düşünüldüğünde bu çıta oldukça yüksek olacaktır.

Kurul, 2020/167 numaralı kararında spor salonu girişinde avuç içi tarama sistemiyle kimlik doğrulaması yapılması ile ilgili kararında minimum düzeyde bilgi talep etme (veri minimizasyonu) ilkesine atıfta bulunulmuştur. Kanun da bu ilke ile ilgili doğrudan bir hüküm yoktur, GVKT de ise m. 25 f.1'de özellikle asgari miktarda kişisel veri işlenmesi için gerekli önlemlerin alınması, tasarımda ve varsayılan olarak veri koruma yöntemlerinin ilk aşamasında uygulanması gerektiği düzenlemiştir (Çekin, 2016). Biyometrik veriler ile ilgili gelecekteki kullanım alanlarından duyulan endişeler sebebiyle veri minimizasyonunun önemi büyüktür. Mevzuatımızda şimdilik doğrudan hüküm bulunmasa da Kurul'un verdiği kararlarda sıklıkla anılan bir ilkedir.

Bir verinin kişisel veri olarak kabul edilebilmesi için belirli veya belirlenebilir şekilde gerçek kişiyle ilişkilendirilebilmesi gerektiği tanımı ortaya konulmuştu. Doğrudan biyometrik veriye bakarak ilgili kişi tespit edilemez fakat bu biyometrik verinin karşılığı olan sayısal değerin gerçek kişilerle eşleştirildiği bir veritabanı olması sebebiyle belirlenebilirlik söz konusudur. Diğer yandan kimlik eşleştirilmesinin yapılmadan sadece "evet/hayır" sonucu üreten sistemler de mevcuttur. Bu sistemlerde ilk kayıt yapılırken de ilgili kişinin kimlik bilgisi alınmaz sadece biyometrik verisi kayıt edilmeden, geri dönüştürülemeyecek şekilde o an matematiksel bir karşılığa olan şablona dönüştürülür ve anonim olarak bu bilgi saklanır. Örneğin bir kapı geçiş sisteminde yüz tanıma sistemi sadece evet/hayır sonucu üreterek kapının açılması sağlanır. Fakat kapıdan geçen kişinin kim olduğu bilinmez. Bu yöntemde de ilk şablon oluşturma esnasında yine bir biyometrik veri işleme süreci vardır ve açık rıza gerektirecektir. Fakat kimlik eşleştirmesi yapılmadığı için bu saklanan anonim verilerden ilgili kişilere ulaşamayacaktır. Diğer temel ilkelerin varlığı halinde veri minimizasyonu ilkesi açısından da tercih edilebilecek bir iyi uygulama olacaktır.

Nitekim bu risk temelli yaklaşım ile biyometrik veri işleyen veri sorumlusu kendi risklerini kendisi belirleyecektir, en azından faaliyetinin sonuçları hakkında fikir sahibi olacaktır. Sadece etki değerleme

çalışmasının mevzuatımıza dahil edilmesi yetmeyecektir, yaptırımların da eş zamanlı olarak daha caydırıcı hale getirilmesi de gerekecektir. Etki değerleme raporu sonucunda bulduğu risklere rağmen faaliyetini sürdüren veri sorumlusu bir ihale sebebiyet verdiğinde sonuçlarına katlanması gerekecektir veya bu tedbirleri alabilecek gücü yoksa bu faaliyete hiç başlamamayı seçecektir.

Yine biyometrik veriler açısından değinilmesi gereken diğer iki kavram GVKT m. 23'te kapsamında tasarımdan itibaren mahremiyet ve varsayılan olarak mahremiyet uygulamalarıdır. Buna göre mahremiyet, henüz bir geliştirmenin ilk aşamasında temel bir unsur olarak esas alınmaktadır (Çekin, 2016). Özellikle teknoloji geliştiricilerinin ileride bir ihlalin konusu olabilecek bir teknolojik kullanımının önüne geçilirken aslında ilgili geliştirmenin genel ilkelere uygun olarak yapılması sağlanarak ilgili kişilerin temel hak ve özgürlüklerine müdahalenin önüne geçilirken geliştirici de gelecekte ürünü sebebiyle yaşayacağı maddi kayıpları engellemektedir. Bu uygulama bir yandan geliştiricilere mevzuatların belirsizliğinden korkarak geliştirme yapmaktan vazgeçmek yerine belirliliğin getirdiği cesaretle geliştirme yapmayı sürdüreceklerdir. Ülkemizde sürekli teknolojinin gelişmesi için teşvikler artırılmaktadır, teknoloji geliştirme bölgelerin özel istisnalar tanınmaktadır, bu teşviklerin aslında hiç kullanılamayacak bir yazılım veya donamım için harcanmasındaki kamu zararına ek olarak bu geliştirmeyi kullanan veri sorumlularının yaşayabileceği sorunlara da dikkat etmek gerekecektir. Bunların yaşanmaması için mevzuatımızda tasarımdan itibaren ve varsayılan olarak mahremiyete dikkat çeken düzenlemeler yapılmasının getireceği yükümlülükler girişimcilerin gerekli tedbirleri almasını sağlayacaktır.

Temel olarak veri koruma etki analizi ve tasarımdan itibaren mahremiyet ve varsayılan olarak mahremiyet uygulamaları birer güvenlik tedbiridir. Yeni ve gelişmekte yüz tanıma sistemleri açısından veri koruma etki analizi uygulama alanı bulacaktır. Sorumluluk ilkesi gereğince veri sorumlusu riskler gerçekleşmeden önce bu riskleri öngörüp gerekli tedbirleri alması beklenmektedir. Bu yöntem ile riskler ortadan kaldırılmasa da üzerinde düşünülmüş hatta rapora dönüştürülmüş analiz sonuçlarına göre tedbir alınması riskleri en aza indirecektir. GVKT m.35 f.3, özel nitelikli kişiler verilerin geniş çapta işlenmesi halinde etki analizi yapılmasını öngörmektedir. Yazılı olarak sunulacak olan raporda kullanılan bilişim sistemi, çalışma prensibi, kişisel verilerin niteliği, işleme amaçları, süreci ve süresi, etkilenmesi muhtemel kişi gruplarına yer verilecektir. Bu işleme faaliyetindeki meşru menfaatin ne olduğu, bu kullanılan yöntemin ölçülülük kapsamında neden gerekli olduğu, risklerin somutlaştırılarak tehlike ihtimalinin derecesi ve bu risklere karşı alınan tedbirlerin neler olduğuna değinilmelidir (Çekin, 2016,). Yüz tanıma sistemlerinin geniş çapta işlenmesi özel sektör açısından ölçülü olmayacağı için uygulaması hukuka aykırı olacaktır fakat kolluk kuvvetleri açısından gittikçe artan bir kullanım alanı vardır ve Avrupa Birliği uygulamasında etki analizi çalışmasının yapılması öngörülmektedir (EDPB, 2022).

Kurul tarafından yayımlanan Yapay Zeka ve Biyometrik Veri Rehberlerinde kullanım amaçlarının, gerekliliklerinin belgelendirilmesi, risklerinin belirlenmesi, geliştirme aşamasında dikkate alınacak hususlar ve hatta yapay zeka rehberinde mahremiyet etki değerlendirmesine doğrudan yer vermiştir. Rehberlerde GVKT'deki ilkelerden hareketle projelerin başlangıcından itibaren dikkat edilmesi gereken hususlar risk temelli bir bakış açısıyla düzenlendiği görülmektedir.

SONUÇ

Biyometrik veri ile ilgili teknolojiler sürekli gelişim içerisinde olacaktır. Bu konuda kaleme alınan her makalede tarih itibariyle yeni gelişmelerin olduğu göze çarpmaktadır. Teknoloji gelişmeye devam etse de kişisel verilerin korunması ile ilgili temel ilkeler uzun süre değişmeyecektir. Biyometrik veriler, kişilere ait olup da kişiye özgü ölçülebilir fiziksel ve davranışsal bilgilerdir. Bu açından da kişiye ait ve kişiye özgü olması nedeniyle de 6698 Sayılı Kişisel Verileri Korunması Kanunu m.3/d hükmü uyarınca biyometrik veriler de kişisel veridir. Kanunun 6/1maddesi uyarınca biyometrik kişisel veriler, özel nitelikte olup, genel kişisel verilere göre daha sıkı teknik ve idari tedbir alınmalıdır. Fakat doğrudan

Kanun'da biyometrik veri tanımının olmaması bir eksiklik olarak göze çarpmaktadır. Bununla birlikte biyometrik veri ile ilgili özellikle ölçülülük konusunu netleştirmek için özel bir madde eklenmesi de düşünülebilir. Risk temelli yaklaşımın bir sonucu olarak daha tasarımdan itibaren mahremiyet kurallarının dikkat alınması için mevzuat düzenlemelerinin yapılmasında fayda vardır. Biyometrik uygulamaların özellikle kimlik doğrulama ve tespitinin çok önem arz ettiği alanlarda, kesinlik, doğruluk ve hızlı sonuç alma amaçları ile kullanıldığı görülmektedir. Özellikle kamu uygulamalarında oldukça geniş ve yoğun yaşam alanlarında yüz tanıma ile tespit yaptığı uzaktan anlaşılamamaktadır. İstisna hükümlerdeki işleme faaliyetleri bir yana bu tür kullanım ihtimalleri bilinçli ilgili kişilerde gittikçe artan bir şüphe yaratmaktadır.

Kişinin yüz, damar, parmak, retina ve iris izi gibi doğuştan elde edilen ve değişmesi neredeyse imkansız olan fiziksel özelliklerin kullanılarak ortaya çıkan biyometrik uygulamalar yolu ile, kişinin kimliğinin en doğru, kesin ve hızlı bir şekilde doğrulanabilmektedir. Ancak burada bireylerin fiziksel niteliklerini kullanmak suretiyle uygulanan biyometrik yöntemlerde makul amaç ile orantılı ve ölçülü şekilde davranılması, özelde ilgili kişinin bireysel faydası veya genelde kamusal faydanın söz konusu olmadığı durumlarda, kimlik kartı ile kimlik doğrulama gibi eski klasik yöntemlerin uygulanması suretiyle, bireylerin özel nitelikte olan biyometrik verilerinin ve özelliklerinin veri tabanına girilmemesi ve işlenmemesi daha uygun olup, temel hak ve özgürlükleri korunması adına daha isabetli bir yol olacaktır. Her ne kadar biyometrik kişisel veriler yaşam hakkı gibi asla müdahale edilemez ve sınırlandırılamaz nitelikte mutlak olmasa da doğrudan kişinin özel hayatını ve birey olma niteliğini ifade ettiği için keyfi, ölçüsüz, gereksiz biyometrik uygulamalar ile müdahale edilmesine hukuk düzeni izin vermemektedir. Biyometrik kişisel verilerin yasalardan kaynaklanan zorunlu ve kamu sağlığı, kamu güvenliğinin sağlanması ve korunması gibi gerekli hallerde ilgili kişinin rızası dışında veya diğer hallerde açık rıza ile işlenmesinden sonra, verilerin saklanması ve kontrol edilmesi açısından kişilerin zarara uğramaması, özel hayatlarına müdahale edilmemesinin temin edilmesi yükümlülüğü tamamen veri sorumlularının üzerindedir. Bu bağlamda en büyük veri sorumlusu olan devlet tüzel kişiliğine ve ticari nitelikli tüzel kişiliklerine bu konuda büyük görev düşmektedir. Veri sorumluları kişisel verilerin korunması hukuku kurallarına ne kadar yüksek seviyede uygun davranırlarsa, o oranda hak ihlali görülme ve kişisel - kamusal zarara uğrama ihtimali azalacaktır.

KAYNAKLAR

Apple Inc. Face ID ve Gizlilik. https://www.apple.com/tr/legal/privacy/data/tr/face-id/ adresinden 22.04.2023 tarihinde erişilmiştir.

Akgül, A. (2014). Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması. İstanbul:Beta Yayınları.

Akgül, A. (2013). Danıştay Kararları Işığında Kişisel Sağlık Verilerinin Korunması. Danıştay Dergisi, S:133, s.21-45.

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

Arslan, B., Sağıroğlu, Ş. (2016). Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme. Politeknik Dergisi, C.19, No.2, s. 101-114.

Article 29 Data Protection Working Party. (2003). Working document on biometrics, WP80, Brussels.https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf adresinden alınmıştır.

Article 29 Data Protection Working Party. (2012). Opinion 02/2012 on facial recognition in online and mobile services, WP 192, Brussels. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf adresinden alınmıştır.

Article 29 Data Protection Working Party, Opinion on Data Processing at Work, 2017, https://ec.europa.eu/newsroom/document.cfm?doc_id=45631 adresinden alınmıştır.

Avrupa Konseyi. (2021). Guidelines on facial recognition Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 adresinden alınmıştır.

Başalp, N. (2004). Kişisel Verilerin Korunması ve Saklanması. Ankara:Yetkin Yayınları.

Berber, L., Lostar, M. (2006). Bilişimde Biyometrik Yöntemler. Ankara:Yetkin Yayınları.

Berber, L. (2019). İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü yayınları https://itlaw.bilgi.edu.tr/media/document/2019/08/biyometrik-imza.pdf adresinden alınmıştır.

Commission Nationale de l'Informatique et des Libertés (CNIL). (2021). Decision of the Executive Committee of the Commission Nationale de l'Informatique et des Libertés n° MEDP-2021-002 of 6th December 2021 to make public the order n°MED-2021-134 of 26th November 2021, issued to CLEARVIEW AI. https://www.cnil.fr/sites/default/files/atoms/files/decision_ndeg_medp-2021-002.pdf adresinden erişilmiştir.

Çekin, M.S. (2020). Avrupa Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku. İstanbul: Oniki levha yayınevi

Çekin, M.S. (2016). 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi. İÜHFM, C.74, S.2.

Develioğlu, H.M. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü. İstanbul: Oniki Levha yayınevi.

Dutch Data Protection Authority (DPA). (2020). Dutch DPA issues formal warning to supermarket for use of facial recognition technology, https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-issues-formal-warning-supermarket-use-facial-recognition-technology adresinen erişilmiştir.

Dutch Data Protection Authority (DPA) (2020), Company fined for processing employees' fingerprint data https://autoriteitpersoonsgegevens.nl/en/news/company-fined-processing-employees'-fingerprint-data erişilmiştir.

Er, C. (2007). Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı: Parmak İzi, Göz ve DNA Tarama Gibi Teknolojik Kimlik Denetleme Usullerinin Hukuki Statüsü. Ankara: Yetkin Yayınları

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

Erkan, D. (2011). Parmak İle Yüz Arasındaki İlişki Analizi, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara.

European Data Protection Board. (2020). Guidelines 3/2019 on processing of personal data through video devices, version 2, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf adresinden erişilmiştir.

European Data Protection Board. (2021), EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

European Data Protection Board. (2022). Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf adresinden erişilmiştir.

Dede, G., Sazlı, M. H. (2010). Biyometrik Sistemlerin Örüntü Tanıma Perspektifinden İncelenmesi ve Ses Tanıma Modülü Similasyonu, EEBM Ulusal Kongresi.

Information Commissioner's Office (ICO). (2021). ICO issues provisional view to fine Clearview AI Inc over £17 million, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/ adresinden erişilmiştir.

Information Commissioner's Office (ICO). (2018). Enforcement Notice, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf adresinden erişilmiştir.

Jain, A. K., Arun A. R. ve Nandakumar, K. (2011). Introduction to Biometrics. New York:Springer Siecense Business Media.

Jay, R., Hamilton, A. (2003). Data Protection Law and Practice: London: Sweet&Maxwell.

Kılınç, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. AÜHFD, sayı 3, s. 1133.

Kızılyel, S. (2014). Temel Hak ve Özgürlüklerin Kısıtlanmasında Kamu Güvenliği Ölçütü. İstnabul:Beta Yayınları.

Küzeci, E. (2010). Kişisel Verilerin Korunması. Ankara: Turhan Kitabevi.

Küzeci, E. ve Kılıç, Ş. (2019). 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler. İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, cilt. 16, sayı. 63, s.947-992.

Kişisel Verileri Koruma Kurulu. (2021). Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber İlke Kararı.

Kişisel Verileri Koruma Kurulu. (2019). Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında 25/03/2019 tarihli ve 2019/82 sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/5463/-Bir-market-zincirinin-sadakat-kart-uygulamasina-iliskin-ihbar-ve-sikayetler-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-25-03-2019-tarihli-ve-2019-82-sayili-Karari adresinden 16.03.2023 tarihinde erişilmiştir.

Kişisel Verileri Koruma Kurulu. (2020). Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi ile ilgili karar özeti. https://www.kvkk.gov.tr/Icerik/6815/2020-649 adresinden 16.03.2023 tarihinde erişilmiştir.

Kişisel Verileri Koruma Kurulu. 27/02/2020 tarihli ve 2020/167 sayılı Karar Özeti, https://kvkk.gov.tr/Icerik/6738/2020-167 adresinden 16.03.2023 tarihinde erişilmiştir.

Kişisel Verileri Koruma Kurulu. "el geometrisi" konulu 07/07/2022 tarihli ve 2022/662 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/7399/2022-662 adresinden 16.03.2023 tarihinde erişilmiştir.

Kişisel Verileri Koruma Kurulu. "ölenin sağlık verisi" konulu 30/06/2020 tarihli ve 2020/507 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/6926/2020-507 adresinden 12.03.2023 tarihinde erişilmiştir.

Kişisel Verileri Koruma Kurumu. (2018). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi.
Metin, Y. (2017). Temel Hakların Sınırlandırılması ve Ölçülülük. SDÜHFD, Cilt:7, Sayı: 1

Oğurlu Y., Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi, Seçkin Yayınevi, Ankara 2002.

Sağıroğlu, Ş., Özkaya, N. (2006). Açık Anahtar Altyapısı ve Biyometrik Teknikler, I. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.

Reuters (2022), Exclusive: Ukraine has started using Clearview AI's facial recognition during war, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

Secure Identity Alliance. (2019). Biometrics in identity: Buiding inclusive futures and protecting civil liberties. https://secureidentityalliance.org/publications-docman/public/156-biometrics-in-identity-building- inclusive-futures-and-protecting-civil-liberties/file adresinden 19.03.2023 tarihinde erişilmiştir.

Sevimli, A. (2006). İşçinin Özel Yaşamına Müdahalenin Sınırları, Doktora Tezi, İstanbul Üniversitesi, İstanbul
Snijder, Max. Biometrics, surveillance and privacy, 2016, https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf adresinden 01.05.2022 tarihinde erişilmiştir.

Şamlı, R., Yüksel, M. E. (2009). Biyometrik Güvenlik Sistemleri, Akademik Bilişim'09- XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi.

Şimşek, O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması, Ankara: Beta Yayınevi

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