Eurasian Academy of Sciences
Eurasian Business & Economics Journal
2017 Volume: 1 S: 174-190
Published Online December 2017 (http://busecon.eurasianacademy.org)
http://dx.doi.org/10.17740/eas.econ.2017-insemp-14

AN ASSESSMENT OF THE DECISION OF THE 3rd CIVIL CHAMBER OF ANKARA REGIONAL COURT OF JUSTICE DATED 20th APRIL 2017 ON THE USE OF BIOMETRIC SECURITY TECHNOLOGIES IN ENTERPRISES

Zehra Binnur Avunduk*, Davut Gürses**

* Istanbul University, Ph.D. in Department of Business Administration, Research Assistant in Vocational School of Social Sciences, Istanbul, Turkey*,

Marmara University, Ph.D. in Department of Private Law; Istanbul University, Lecturer in Vocational School of Social Sciences; Attorney, QNB Finansbank Legal Affairs Manager, Istanbul, Turkey,

E-mail: avundukz@istanbul.edu.tr*, davutgurses@gmail.com**
Copyright © 2017 Zehra Binnur Avunduk, Davut Gürses. This is an open access article distributed under the Eurasian Academy of Sciences License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
The abstract of this study was presented at *International Conference on Global Competititon and Innovation Management (ICGCIM)*, held on 9-11 November, 2017 in Istanbul.

ABSTRACT

In recent years, reelingly development of technology has provided convenience to enterprises in many fields both operationally and administratively. With the penetrating of technology into the every field; enterprises has started to use biometric security technologies, which have become very popular recently to provide services from their products and even internal auditing. Biometric security technologies can be defined as systems developed to identify individuals by characterising, storing and identifying individuals' personal data. It is becoming widespread in these systems personalized biometric data such as; voice, face, fingerprint, hand geometry and eye recognition can be given as examples. Biometric security technologies are used in many fields such as mobile banking, smart products, sports clubs, call centers, entrance and exit gates of businesses,criminal investigations, hospitals and insurance companies, electronic commerce, national identity applications in order to identification with the highest possible reliability, against possible risks of the classical security systems. However, the use of these technologies may violate the personal rights and freedoms of the customers or employees. The legal aspects of these technologies which are becoming widespread nowadays in various enterprises, are important in terms of filling the related gap in the literature and guidance to the practitioners. In this context, the compliance with laws of using biometric security technologies by enterprises will be discussed and evaluated in the light of a Turkish judicial decision. The relevant judicial decisions were examined and by reason of that we determined as the most important decision could be a precedent with the our study is the decision by 3rd Civil Chamber of the Ankara Regional Court of Justice dated 20.04.2017 on the basis of 2017/388 and 2017/401numbered has been examined. As a result of the research, we have the intention of that the given decision by the court is contrary with the Law numbered 6698 on the Protection of Personal Data (LPPD). The controversial points in this case are; identification of personal data, receiving the related person's approval,stipulation the deliver of the service or the sale of product on consent.

Keywords: Turkish judicial decisions, biometric security technologies, the protection of personal data, use of technology in enterprises

JEL: K12, K15, K24, K36, L65, O14, O33

ANKARA BÖLGE ADLİYE MAHKEMESİ 3. HUKUK DAİRESİ'NİN 20 NİSAN 2017 TARİHLİ KARARI IŞIĞINDA İŞLETMELERİN BİYOMETRİK GÜVENLİK TEKNOLOJİLERİ KULLANIMININ İNCELENMESİ

ÖZET

Teknolojinin son yıllarda baş döndürücü bir şekilde gelişimi işletmelere hem operasyonel hem de yönetimsel açıdan birçok alanda kolaylık sağlamıştır. Teknolojinin her alana nüfuz etmesiyle birlikte işletmeler; ürettiği ürünlerden sunduğu hizmetlere ve hatta işletme içi denetimi sağlamak amacıyla son zamanlarda oldukça popüler hale gelen biyometrik güvenlik teknolojilerini kullanmaya başlamıştır. Biyometrik güvenlik teknolojileri, bireylerin kişisel verilerini tanımlayıp, depolayan ve kimliklendirme yaparak kişiyi tanımaya yönelik geliştirilen sistemler olarak tanımlanabilir. Bu sistemler içerisinde kullanımı yaygınlaşmakta olan; ses, yüz, parmak izi, el geometrisi, göz tanıma gibi kişiye özel biyometrik veriler örnek olarak gösterilebilir. Biyometrik güvenlik teknolojileri; mobil bankacılık, akıllı ürünler, spor kulüpleri, çağrı merkezleri, işletmelerin giriş-çıkış kapıları, kriminal incelemeler, hastane ve sigorta kuruluşları, elektronik ticaret, ulusal kimlik uygulamaları gibi birçok alanda kimlik tespiti yapmak amacıyla klasik güvenlik sistemlerinin olası risklerine karşılık, güvenilirliği en yüksek yöntem olarak kullanılmaktadır. Ancak bu teknolojilerin kullanımı, müşterilerin veya çalışanların kişisel hak ve özgürlüklerinin ihlaline neden olabilmektedir. Günümüzde çeşitli işletmelerde git gide yaygınlaşan bu teknolojilerin hukuki açıdan incelenmesi literatürdeki ilgili boşluğun doldurulması ve uygulayıcılara yol göstermesi açısından önem arz etmektedir. Bu kapsamda çalışmamızda, işletmelerin biyometrik güvenlik teknolojileri kullanımlarının hukuka uygunluğu tartışılacak olup, örnek vaka incelemesi olarak bir Türk yargı kararı ışığında değerlendirilecektir. İlgili yargı kararlarına bakıldığında, konumuzla emsal teşkil edebileceğini düşündüğümüz en önemli kararın; 20.04.2017 tarihli, Ankara Bölge Adliye Mahkemesi 3. Hukuk Dairesi'nin 2017/388 esas ve 2017/401 numaralı karar olması hasebiyle söz konusu karar incelenmiştir. Araştırmanın sonucu olarak, değerlendirdiğimiz kararın; kişisel verinin tanımlanması, ilgili kişinin rızasının alınması, hizmetin sunumu veya ürünün satışının rızanın verilmesi şartına bağlanması gibi hususlarda 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)'na aykırı olduğunu düşünmekteyiz.

Anahtar Kelimeler: Türk yargı kararları, biyometrik güvenlik teknolojileri, kişisel verilerin korunması, işletmelerde teknoloji kullanımı.

1. GİRİŞ

Son yıllarda teknolojinin hızla gelişmesi işletmelere hem operasyonel hem de yönetimsel açıdan birçok alanda kolaylık sağlamıştır. İşletmelerin, üretim sistemlerinden hizmetlerinin sunumuna kadar neredeyse her faaliyetinde teknolojinin sağladığı tüm imkânlardan faydalandığı dikkat çekmektedir. Rekabet üstünlüğü kazanmada önemli bir faktör olarak değerlendirilebilecek olan teknoloji kullanımının; işletmelerin inovasyon yeteneğini geliştirme,

faaliyetlerinde hız, esneklik, etkinlik ve verimlilik artışı gibi pek çok hususta yarar sağladığı ifade edilebilir. Teknolojideki gelişmelerle birlikte işletmeler, denetim işlevini daha etkin bir şekilde yerine getirebilmek amacıyla; yönetimsel bir süreç inovasyonu olarak değerlendirilebilecek "biyometrik güvenlik teknolojilerini" kullanmaya başlamıştır. Kullanımı her geçen gün yaygınlaşan biyometrik güvenlik teknolojileri, bireylerin kişisel verilerini tanımlayıp, depolayan ve kimliklendirme yaparak kişiyi tanımaya yönelik geliştirilen sistemler olarak tanımlanabilir. Bu sistemler içerisinde; ses, yüz, parmak izi, el geometrisi, göz tanıma gibi kişiye özel biyometrik verilerin sıkça kullanıldığı görülmektedir.

Biyometrik güvenlik teknolojileri; mobil bankacılık, akıllı ürünler, spor kulüpleri, çağrı merkezleri, işletmelerin giriş-çıkış kapıları, kriminal incelemeler, hastane ve sigorta kuruluşları, elektronik ticaret, ulusal kimlik uygulamaları gibi birçok alanda kimlik tespiti yapmak amacıyla klasik güvenlik sistemlerinin olası risklerine karşılık, güvenilirliği en yüksek yöntem olarak kullanılmaktadır. Bu teknolojilerin kullanımı birtakım yararlar sağlamakla birlikte müşterilerin veya çalışanların kişisel hak ve özgürlüklerinin ihlaline neden olabilmektedir. Bu durum ise bireyler üzerinde endişelere yol açabilmektedir.

Biyometrik güvenlik sistemlerinde kullanılan veriler, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) göre "özel nitelikli kişisel veri" kapsamında değerlendirilmekte olup, bu tür verilerin hukuki korunmadan yararlanması söz konusudur. Bu nedenle, günümüzde neredeyse her sektörde gittikçe yaygınlaşan biyometrik teknoloji kullanımının hukuki açıdan incelenmesi ihtiyacı doğmaktadır. Güncel olarak tartışılmakta olan, işletmelerin kullandığı söz konusu teknolojinin literatürdeki ilgili boşluğun doldurulması ve uygulayıcılara yol göstermesi açısından hukuki bakışla ele alınması önem arz etmektedir. Bu kapsamda çalışmamızda, öncelikle biyometrik güvenlik teknolojileriyle ilgili kavramsal bilgiler verilmekte, işletmelerin bu teknolojileri kullanımlarının hukuka uygunluğu tartışılmakta ve bir Türk yargı kararı ışığında değerlendirilmektedir.

2. KİMLİKLENDİRME ARAÇLARI

Kimliklendirme, modern toplumlarda çok yaygın kullanılan bir süreçtir (Luis-García, Alberola-López, Aghzout, Ruiz-Alzola, 2003:2539). Bireylerin kimliklerinin doğrulanmasına; bankacılık işlemlerinde, spor kulübü girişlerinde, çalışanların mesai saatlerine riayet edip etmediklerini denetlemek üzere iş yerlerinin girişlerinde, kısıtlı ve yetki gerektiren bölgelere erişimde, yurt dışına çıkış işlemleri gibi hayatın çeşitli alanlarında olası suç girişimlerinin önlenebilmesi ve kişiye özel hak ve özgürlüklerin korunabilmesi için ihtiyaç duyulmaktadır. Miller'a göre kimliklendirme türlerini üç ana grupta incelemek mümkündür (1994:22). Bunlar; kişinin bildikleri (şifre, PIN kodu vb.), sahip oldukları (akıllı kartlar, e-imza cihazı vb.) ve ayırt edici özellikleri (ses, parmak izi, el geometrisi, göz vb.)dir.

Kimlik tanımlama türlerinden birinci grupta yer alan "kişinin bildikleri" bir diğer ifadeyle "şifreler", basit karakterlerle tanımlandığında kişinin yakınları tarafından kolaylıkla tahmin

edilebilme riski söz konusu olabilmekte; büyük/küçük harf, sayı, sembol gibi çeşitli karakterlerle tanımlandığında ise hatırlanma güçlüğü yaşanabilmektedir zira bireyin elektronik cihazlarından, banka kartlarına, apartman girişinden spor kulübü girişlerine kadar hatırlamak durumunda olduğu çok sayıda şifresi bulunmaktadır. Bu şifrelerin bir yere not edilmesi hatırlama riskini ortadan kaldırmakla birlikte not edildiği defterin kaybolması durumunda başkalarının eline geçmesi veya elektronik belgenin cihazdan silinmesi gibi durumlar risk teşkil etmektedir. Bu tür riskleri önlemek amacıyla çeşitli işletmelerin kullanıcılara sunduğu şifre hatırlatma, şifre kurtarma gibi çözüm yöntemleri geliştirdiği de görülmektedir.

İkinci grubu temsil eden "kişinin sahip oldukları", geleneksel ve geçerliliğini hala yitirmeyen "nüfus cüzdanı, pasaport, ehliyet" ya da günümüzdeki "akıllı kartlar" birinci grupta olduğu gibi gene kişinin tanımlanmasını sağlayan araçlar olmakla birlikte kaybolma veya çalınma riski bulunmaktadır. Akıllı kartlar açısından olay ele alındığında, kişinin sahip olduğu akıllı kartla birlikte kendisine tanınan haklar, bu kartın başkasının eline geçmesi durumunda üçüncü şahıslar tarafından kullanılabilir. Örneğin bir iş yerinde çalışanların mesai saatlerini denetim amacıyla kullanılan personel kimlik kartlarının kaybolması ya da başkasının eline geçmesi durumunda çeşitli riskler söz konusu olabilir. Birincisi, işletme içerisindeki başka bir çalışan, kartı kaybeden çalışanın yetkinliğindeki alana giriş yapabilir ve o kişiye tanınan hakları kullanabilir ve erişim izni bulunmayan bilgi ve belgelere ulaşabilir. İkincisi, işletme dışından biri kaybolan kartı bulabilir ve bu durum işletmeye yabancı kişilerin giriş yapmasına neden olarak bir güvenlik tehdidi oluşturabilir. Üçüncü bir risk faktörü olarak da personel kimlik kartı çalışanlar arasında kolayca değiştirilerek mesai saatlerine uyulduğunu göstermek amacıyla işletmeye giriş yapmadığı halde işe zamanında gelmemiş olan çalışanın kartı sisteme okutturulabilir. Bu gibi durumlar sistemin amacına ulaşmasını engellemekte, sağlıklı bir denetimin yapılmasına olanak vermemekte ya da işletme için güvenlik tehdidi oluşturabilmektedir.

Kişilerin ayırt edici özelliklerini referans alan üçüncü kimliklendirme türü, "biyometrik teknikler" ise takip eden başlıkta daha ayrıntılı bir şekilde ele alınacaktır.

3. BİYOMETRİK GÜVENLİK TEKNOLOJİLERİ

"Biyometri" kelimesinin etimolojisi, antik Yunan literatürüne dayanmaktadır ve "Bios"-yaşam ile "metros"-ölçü kelimelerinden oluşmaktadır. Biyometri, bireylerin; fiziksel, kimyasal ya da davranışsal kişisel özelliklerine dayanan ve kimliklerini benzersiz şekilde tanımlamak için kullanılan bir teknoloji ve bilimdir (Pocovnicu, 2009: 57). Türk Dil Kurumu biyometriyi; "organizmayı ilgilendiren biyolojik özelliklerin istatistiksel yöntemlerle anlatılmasını sağlayan bilim dalı" olarak tanımlamaktadır (TDK). Uluslararası Biyometri ve Kimlik Derneği IBIA'nın tanımına göre biyometri; benzersiz fiziksel veya davranışsal özellikleri, bireyleri otomatik olarak tespit etmek için kullanılabilen bir yöntemdir. Biyometrik teknolojiler, bu özellikleri elektronik olarak yakalar, işler, ölçer ve yüksek derecede doğru bir kimlik yönetimi yeteneği yaratmak için mevcut kayıtlarla karşılaştırır (IBIA).

Biyometrik sistemler, bireye ait fiziksel (parmak izi, yüz, iris, retina, DNA, el geometrisi ve damar geometrisi vb.), kimyasal (koku, vücut ısısı) ve davranışsal (konuşma, imza, tuş vuruşu

zamanlaması vb.) özelliklerin çoğunun her bir birey için ayırt edici olduğunu, sensörler ve aygıtlar aracılığıyla bu özelliklerin doğru bir şekilde yakalanabileceğini ve bireyleri kimliklendirmek üzere otomatik karar verilmesine uygun bir biçimde temsil edilebileceklerini varsaymaktadır (Pocovnicu, 2009:57). Biyometrik teknolojiler; parmak izi, ses izi ve iris tanıma gibi fiziksel özelliklerin kullanımından yürüme ve el yazısı tanıma gibi davranışsal özelliklere kadar uzanır. Biyometrik özellikleri doğası gereği kopyalamak, taklit etmek, paylaşmak ve dağıtmak zor olduğu gibi kaybedilmesi veya unutulması da birey, fiziksel olarak var olduğu müddetçe mümkün değildir. Bu nedenle biyometrik sistemler, kurulu şifre tabanlı kimlik doğrulama sistemlerinden daha güvenilir olarak kabul edilmekte ve güvenli kimlik doğrulamanın mantıksal ve tartışmasız kaçınılmaz geleceği (Tassabehji ve Kamala, 2012:489-490) olarak addedilmektedir.

Biyometrik güvenlik teknolojilerinin sağladığı güvenilir sonuçlar ve kullanım kolaylığı açısından geleneksel yöntemlere nazaran daha üstün olduğu ifade ediliyorsa da bu yöntemin de beraberinde getirdiği birtakım dezavantajlar söz konusudur. Bazı gizlilik kuruluşları (DPC*; IPC**) iş yerinde biyometri kullanımının önemli bir çalışan gizliliği kaygısı ile sonuçlandığını ileri sürmektedir. Buna ek olarak, içtihatlar, iş yerinde biyometrik yöntemlerin uygulanmasının çalışanları sendikalaşmaya sevk etme ya da mevcut iş sözleşmelerinin yeniden müzakeresi arayışı gibi istenmeyen birtakım sonuçlara yol açabileceğini göstermektedir. Çalışanların gizlilik endişeleri, biyometrik verilerin nasıl kullanılacağının belirsizliğinden kaynaklanıyor olabilir (Carpenter, Maasberg, Hicks, Chen, 2016:735). Örneğin, bazı biyometrik veriler sadece bireyi tanımlama bilgisinden daha fazlasının elde edebilmesini mümkün kılabilir. Kişisel gizliliğe ek olarak, bir kullanıcının tıbbi durumunu ortaya çıkarmak için biyometrik verilerin kullanılabileceği endişeleri de bulunmaktadır. Bu tür bilgiler, bazı kullanıcıları istihdam etmede veya yararlı amaçlarla (örneğin, sağlık sigortası) ayrımcılık yapmak için kullanılabilecek özelliktedir (Jain ve Kumar, 2012:69). Woodward (1999) da benzer bir şekilde, biyometrik veriler alınırken bireyin sağlığı ve tıbbi geçmişi hakkında da bilgi edinilebilmesi söz konusu olabileceğini belirtmektedir. Biyometrik sistemlerin kullanımı genellikle kişisel haklara tecavüz edildiği hissiyatı oluşturabilir çünkü sensörler doğrudan ayrıcalıklı olarak kabul edilen kişiye özgü verileri yakalamak için insan vücuduyla etkileşime girer. Biyometrik özellikler, insan vücudunun ve davranışının bir parçasıdır ve bu nedenle, kayıt veya doğrulama sırasında bu bilgiyi biyometrik bir sisteme bırakmak, bazı kullanıcıların kişisel gizliliklerini tehdit edebilir (Jain ve Kumar, 2012:68). Bilimsel araştırmalar; parmak izlerinin ve parmak görüntülemenin kişiyle ilgili tıbbi bilgileri açığa vurabileceğini ileri sürmektedir. Örneğin; Down sendromu, Turner sendromu ve Klinefelter sendromu, kişide olağandışı parmak izi kalıplarına neden olan kromozomal bozukluklardır (Chen, 1988; Skoler, 1984) ayrıca cilt kanserinin bazı türleri el veya yüzdeki vasküler taramalarla tespit edilebilir (Hay, 2003:9-10). Bunlara ek olarak Jain ve Kumar (2012), biyometrik yöntemlerle kullanıcıların (çalışanların veya müşterilerin) bazı sağlık sorunlarının belirlenebileceği hakkında bir tablo hazırlamıştır. Biyometrik yöntem türlerine göre teşhis edilebilecek hastalık türleri Tablo 1.'de sunulmaktadır.

* Data Protection Commissioner
** Information and Privacy Commissioner

Tablo 1. Biyometrik Yöntemlerle İlgili Gizlilik Endişeleri

Biyometrik Yöntem	Kullanıcının Sağlığı ile İlgili Olası Göstergeler
Retina	Göz ile ilgili hastalık (ör: Diyabetik Retinopati)
DNA	Genetik hastalıklar veya spesifik hastalıklara duyarlılık, cinsiyet
Avuç izi	Konjenital kalp hastalığı ve diyabetlerde larengoskopi tahmini
Yüz	Vücut ısısı ile ilgili yüz termogramı ve ilgili tıbbi durumlar
Yürüyüş	Fiziksel engellilik

Kaynak: Jain ve Kumar, 2012:69.

Bu açıdan bakıldığında biyometrik verilerin kullanılması, bazı genetik belirteçleri veya hastalıkları taşıyan kişilerin sistematik olarak ayrımcılığa uğratılmasına sebebiyet verebilir (Carpenter vd., 2016:735). Bu noktada, çalışan veya müşterilerin verdiği özel nitelikli kişisel verilerin işletme tarafından etik kullanımına ilişkin güveni de önemli bir husus olarak addedilebilir. Kuruluşlar yalnızca sistem erişiminde biyometrik teknolojiyi kullanacaklarını iddia edebilirken, biyometrik verilerin kullanımını genişletmeye karar verdikleri takdirdeyse çalışanlar için çok az bir yasal koruma söz konusudur (Carpenter vd., 2016:736). Etik dışı davranan işletmelerin biyometrik verileri (ör.parmak izi verisi), bireylerin sabıka kaydı soruşturmaları, ırk, sınıf ve coğrafi durumuyla ilgili bilgi almak için gizlice kullanması ve elde edilen bu veri tabanıyla bireylere karşı önyargılı davranması (Cole, 2004) söz konusu olabilir. Biyometrik veri tabanının diğer veri tabanlarına bağlanarak, biyometrik özelliklerin zamanla kişileri izlemek için kullanılabilmesi teknolojik olarak mümkün olabilir (Ör:kullanıcının kredi kartı işlemlerinde nerede ve ne zaman bulunduğu bilinmektedir.) (Jain ve Kumar, 2012:69). Biyometrik veriler, diğer veri tabanlarındaki kişisel bilgilerle ilişkilendirilebilir, bu da kişisel gizliliği tehdit edici bir unsur olarak değerlendirilebilir.

Kimliklendirme kısmında ifade edilmeye çalışılan ve sair durumların dikkate alınmasıyla birlikte işletmelerin çeşitli riskleri önleyebilmek amacıyla çağımızın sunduğu ileri teknolojiden yararlanılarak tasarlanmış olan biyometrik güvenlik sistemlerinin kullanımının gittikçe yaygınlaştığı görülmektedir. Bu teknolojiler, bireyin fiziksel ya da davranışsal ayırt edici özelliklerini kullanarak her ne kadar işletmeler tarafından, yüksek düzeyde güvenlik sağlamak için geleneksel yöntemlere tercih edilse de; müşterilerin veya çalışanların "özel nitelikli kişisel veri" kapsamına giren bilgilerinin üçüncü şahısların eline geçmesi ve kötü niyetli olarak kullanılması riski söz konusudur. Bu durumda işletmelerin kendi menfaatlerini gözetirken, çalışanlar ve müşterilerinin menfaatlerini de dikkate almaları gerekliliği ortaya çıkmaktadır ve bu da biyometrik güvenlik teknolojileri kullanımının hukuki açıdan değerlendirilmesini gerekli kılmaktadır. Çalışmamızın takip eden kısmında, işletmelerin biyometrik güvenlik teknolojileri kullanımı, bir Türk yargı kararı ışığında incelenmekte olup, hukuka uygunluğu değerlendirilmektir.

4. BİYOMETRİK GÜVENLİK TEKNOLOJİLERİNİN HUKUKİ YÖNÜ

Bilgi sistemlerindeki gelişmelere bağlı olarak artan bilgi transferi, bilgi varlıkları içinde en fazla kişisel bilgilerin korunması konusunda endişeleri artırmıştır (Henkeloğlu, 2015:22). Biyometrik güvenlik teknolojilerinin kullanımının yaygınlaşmasıyla birlikte de bu teknolojilerin, hukuk karşısındaki konumunu belirleme ihtiyacı giderek önem kazanmıştır. Gerçekten bu teknolojilerin gelişimiyle birlikte temel hak ve özgürlüklere müdahale imkânı kolaylaşmış ve çoğalmış, ayrıca sistemin işleyişi için daha fazla kişisel veri kullanım ihtiyacı ortaya çıkmıştır. Tüm bu sayılanların katkısıyla da çeşitli hukuki sorunlar gündeme gelmiştir (Aksoy, 2010: 77 ve Özdemir, 2009:123).

Aşağıda sırasıyla, kişisel verilerle ilgili genel bilgiler verilerek akabinde kişisel verilerin hangi durumlarda biyometrik güvenlik teknolojilerinde kullanılabileceği konusu incelenecek, devamında da konuya ilişkin Ankara Bölge Adliye Mahkemesi 3. Hukuk Dairesi'nin 2017/388 esas, 2017/401 ve 20.04.2017 tarihli kararı incelenecektir.

4.1 Biyometrik Güvenlik Teknolojilerinde Kullanılan Verilerin Kişisel Veri Niteliğinde Olup Olmadığı Sorunu

Biyometrik güvenlik teknolojilerinin birçoğunda; parmak izi, yüz tanıma, göz tanıma (retina), DNA, el geometrisi, damar geometrisi, koku, vücut ısısı, konuşma, yürüyüş gibi veriler kullanılmaktadır (Akgül, 2015:202). Bu nedenle ilk olarak bu verilerin kişisel veri niteliğinde olup olmadığının tespit edilmesi gerekmektedir. Bu teknolojilerde kullanılan bilgilerin kişisel veri olarak kabul edilebilmesi için her şeyden önce bu bilginin kimliği belli ya da belirlenebilir bir gerçek kişiye ait olması zorunludur (Manav, 2015:97). Görüldüğü üzere bir verinin kişisel veri olarak kabul edilebilmesi için, bir kişiyi tanımlaması, onu diğerlerinden ayırması gerekmektedir (Akdağ, 2013:7). Yani veriye bakıldığında, bunun ait olduğu gerçek kişinin doğrudan ya da dolaylı olarak belirlenebilmesi gerekir. Aksi durumda, yani veriden doğrudan ya da başka yollarla ait olduğu kişiye erişim imkânı yoksa bu durumda kişisel veriden bahsetmek mümkün olmayacaktır.

Bu durumda, Türk hukuku bakımından bir verinin "kişisel veri" sayılabilmesi için iki unsurun bir arada bulunması gerektiği söylenebilir;

a) Verinin gerçek bir kişiye ilişkin olması ve
b) Bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekmektedir.

Bu unsurlardan ilkine göre, sadece gerçek kişilere ait veriler kişisel veri olarak kabul edilmektedir. Yani, tüzel kişilere ait bilgiler hiçbir koşulda kişisel veri sayılmayacaktır. Ancak, tüzel kişilere ait olup da kişisel veri niteliğinde olan bilgiler de söz konusu olabilir. Örneğin, tüzel kişinin, gerçek kişi yönetim kurulu üyesine ait kimlik bilgileri ile nüfus bilgilerinin de kişisel veri niteliğinde olduğunu unutmamak gerekir. Bu nedenle, tüzel kişilerden alınacak

verilerde toptancı bir yaklaşım yerine verinin niteliğine bakılması daha doğru sonuçlara ulaşılmasını sağlayacaktır.

Diğer unsur ise ilgili veriden kişinin kimliğine erişme imkânının bulunmasını ifade etmektedir. Yani verinin doğrudan bir gerçek kişiye ait olduğu açıksa ya da başka verilerle ya da yöntemlerle bu veriden verinin ait olduğu kişinin kimliğine erişme imkânı varsa bu veri kişisel bir veri olarak kabul edilecektir. Bu kapsamda, kişinin belirlenebilir olmasından neyin anlaşılması gerektiği önem arz etmektedir. Burada, kullanılması makul olan tüm vasıtaların kullanılması neticesinde ve belirlemeyi yapan kişinin bu konuda kararlı ve azimli olduğu varsayılarak, bu bilgiden yola çıkılarak ilgili kişinin belirlenip belirlenmeyeceği somut olayın özelliklerine göre tespit edilmelidir (Aksoy, 2010:24 ve Ayözger, 2016:12). Doktrinde bu husus orantılılık prensibi olarak şöyle ifade edilmektedir; *"Burada bir kişinin tespiti için orantısal olarak çok fazla zaman ve çaba gerekiyorsa bu durumda bu kişi belirlenebilir farz edilmemelidir. Bir kişinin kimliğinin belirlenebilir olup olmadığının tespitinde, başkaları tarafından kullanılabilecek makul yöntemler hesaba katılmalıdır."* (Korkmaz, 2016:92). Şayet makul tüm vasıtaların kullanılması ile ya da hiçbir şekilde ilgili kişi belirlenemiyorsa, bu durumda ilgili veri kişisel veri olarak kabul edilemez. Yargıtay da bir kararında kimlikleri tespit edilemeyen mağdurelerin uygunsuz fotoğraflarının çekilmesini kişisel verilerin kaydedilmesi kapsamında değerlendirmemiştir (Oğuz, 2014:20).

KVKK'nın gerekçesinde *"bireyin adı, soyadı, doğum tarihi, doğum yeri, kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerinin"* kişisel veri niteliğinde olduğu belirtilmiştir. Ayrıca yine gerekçede *"telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri ve genetik bilgilerin"* de kişisel veri olarak kabul edilmesi gerektiğine işaret edilmiştir. Örneğin, bu örneklerin bir kısmında verinin ait olduğu kişi belirli iken (adı soyadı, fotoğrafı, özgeçmişi) diğer bir kısmında ise belirlenebilir (doğum tarihi, telefon numarası, parmak izi, genetik bilgileri vb.) durumdadır.

Biyometrik güvenlik teknolojilerinin mevcut işleyişini incelediğimizde bu sistemlerin; parmak izi, yüz tanıma, göz tanıma (retina), DNA, el geometrisi, damar geometrisi, koku, vücut ısısı, konuşma, yürüyüş gibi verilerle çalıştığını görmekteyiz. Bu verileri incelediğimizde ise bunlardan yola çıkarak, bu verilerin sahibine erişme imkânının bulunduğunu söyleyebiliriz (Özdemir, 2009:124). Örneğin, parmak izinden yola çıkarak bunun kime ait olduğunun tespiti mümkündür. Yine, yüz ya da göz tanıma sistemlerinde de bu imkân fazlasıyla mevcuttur. Dolayısıyla, *-istisnai haller dışında-* bu tür sistemlerde kullanılan verilerin kişisel veri niteliğinde olduğunu söylemek mümkündür.

KVKK, kişisel veriler arasında da önem derecesine göre bir ayrım yaparak bazı kişisel verileri "özel nitelikli kişisel veri" olarak sınıflandırmış ve bu tür veriler için ayrı bir koruma rejimi oluşturmuştur. Özel nitelikli kişisel veriler, işlenmeleri halinde sahipleri hakkında ayrımcılık yapılmasına veya mağduriyete neden olma riski yüksek olan ve bu nedenle de diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gereken verilerdir (Aksoy, 2010:30). Esasında, bu tür verilerin işlenmesi kural olarak yasaktır, ancak istisnai olarak ilgilinin açık rızası ya da

kanuni bir yetki bulunması durumunda işlenebileceği kabul edilmektedir. (Şimşek, 2008:86). KVKK'da özel nitelikli kişisel veriler, sınırlı olarak belirlenmiştir. Bunlar; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir. Kanun koyucunun bu tavrı, yönetmelikle ya da yargı kararıyla bunlardan başka özel nitelikli veri oluşturulamayacağı anlamına gelmektedir. KVKK'da sayılan özel nitelikli kişisel verilerden biyometrik ve genetik verilerin, biyometrik güvenlik teknolojilerinde sıklıkla kullanıldığı bilinmektedir.

Biyometrik güvenlik teknolojilerinde işlenen verilerin "özel nitelikli kişisel veri" niteliğinde olduğunu tespit etmiş bulunuyoruz. Ancak, bu tespit tek başına bu verilerin kullanılmasına KVKK'nın uygulanmasına imkân vermemektedir. Gerçekten KVKK'nın "Kapsam" başlıklı 2. maddesine göre bu Kanun hükümleri *"kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler"* hakkında uygulanacaktır.

Dolayısıyla *"tamamen veya kısmen otomatik yollarla işlenen veriler"* ile *"herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen veriler"* Kanun kapsamında koruma altına alınmıştır. Kanun otomatik olmayan yollarla işlenen verilerden sadece bir veri kayıt sisteminin parçası olanlara uygulanacaktır. Bu anlamda kişisel verilerin bilgisayarda veya bir dosyada bulunması arasında bir fark yoktur (Korkmaz, 2016:92). Kanun'un açık düzenlemesinden ve gerekçesinden de anlaşıldığı üzere, bir veri kayıt sisteminin parçası olmayan kişisel veriler otomatik olmayan yollarla işlendiklerinde Kanun kapsamında değerlendirilmeyecektir (Korkmaz, 2016:92).

Görüldüğü üzere, kanunun uygulanması noktasında kişisel verilerin bir veri kayıt sisteminin parçası olmasının önemi büyüktür. KVKK'da veri kayıt sistemi *"kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi"* olarak tanımlanmıştır. Bu sistemler elektronik yahut fiziki ortamda oluşturulabilir. Örneğin, veri kayıt sisteminde kişisel veriler, ad, soyad veya kimlik numarası üzerinden sınıflandırılabileceği gibi adres, yaş ve cinsiyet bilgisi üzerinden de sınıflandırılabilir. Yukarıdaki tanımdan yola çıkıldığında biyometrik güvenlik sistemlerinin de birer veri kayıt sistemi olduğu söylenebilir. Zira bu sistemlerin kişisel verilerin eşleştirilmesi suretiyle çalışması mantığı nedeniyle doğası gereği kayıt esaslı çalıştığı ilk elden söylenebilir. Öte yandan, bu sistemlerin kişisel verileri işlediğini de açıklıkla söyleyebiliriz. Gerçekten KVKK'da kişisel verilerin işlenmesinin *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen"* her türlü işlemi ifade ettiği belirtilmiştir. Bu sistemlerin söz konusu fiillerin çoğunu gerçekleştirdiği düşünüldüğünde, bu sistemlerin kişisel veri işlediğini söylemek mümkündür.

Netice olarak, biyometrik güvenlik sistemlerinin ihtiyaç duyduğu verilerin özel nitelikli kişisel veri olduğunu, ayrıca bu sistemlerin veri kayıt sistemi niteliğinde olduğunu ve bu sistemlerin veriyi kullanmasının kişisel verilerin işlenmesi niteliğinde olduğunu ve bu nedenlerle de bu işlemlerin KVKK kapsamında bulunduğunu söylemek mümkündür.

4.2 Biyometrik Güvenlik Teknolojilerinde Kişisel Verilerin Kullanılması

KVKK'nın, özel nitelikli kişisel verilerin işlenmesi konusundaki ilk ve en temel kuralı, bu verilerin ilgilinin "açık rızası" olmaksızın işlenemeyeceği kuralıdır. Gerçekten, kişisel verisi işlenen gerçek kişinin, verilerinin işlenmesi konusunda açık rızası yok ise söz konusu verinin kullanılması hukuka aykırı olacaktır. Açık rıza ise, belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder. Dolayısıyla, kişisel verilerin işlenmesi için alelade bir rızadan ziyade nitelikli bir rızanın arandığını söylemek mümkündür. Bu rızanın geçerliliği herhangi bir şekil kuralına bağlanmamıştır. Rızanın hukuka uygunluk nedeni sayılabilmesi için *"şüpheye yer bırakmayacak şekilde verilmiş olması"* gerekir (Korkmaz, 2016:106). Doktrinde, içeriğe dair kuşkuların bulunması durumunda, rızanın geçersiz sayılması gerektiği de ileri sürülmektedir (Başalp, 2004:39).

Kanun koyucu bu temel ilkeden sonra bazı durumlarda, ilgili kişinin açık rızası bulunmasa bile verinin işlenebileceği istisnai durumlar belirlemiştir.

Bunlar;

a) Kanunlarda öngörülen hallerde,
b) Sağlık ve cinsel hayata ilişkin kişisel veriler, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilir.

Bu istisnalardan biri varsa, bu durumda kişisel verinin işlenmesi için ilgilinin rızası aranmaz. Ayrıca Kanunda özel nitelikli kişisel verilerin işlenmesi bakımından, Kurul tarafından belirlenen yeterli önlemlerin alınması şartı da getirilmiştir.

Ayrıca, kanun koyucu kişisel verilerin işlenmesinde bazı genel ilkelere de uyulmasını zorunlu kılmıştır. Bunlar;

a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.
c) Belirli, açık ve meşru amaçlar için işlenme.
ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Bu genel kurallara ek olarak ayrıca, özel nitelikli kişisel verilerin elde edilmesi sırasında veri sorumlusu ya da yetkilendirdiği kişinin, ilgili kişiyi; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, kişisel verisinin işlenip işlenmediğini öğrenme hakkı, kişisel verisi işlenmişse buna ilişkin bilgi talep etme hakkı olduğu, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme hakkı olduğu, yurt içinde ya da yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme hakkı, kişisel verisi eksik ya da yanlış işlenmiş ise bunların düzeltilmesini isteme hakkının olduğu, yasal şartları oluştuysa kişisel verilerinin silinmesini veya yok edilmesini isteme hakkının olduğu, kişisel verilerinin düzeltilmesi ya da silinmesi/yok edilmesi durumunda bu durumları kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini talep etme hakkı olduğu hususlarında bilgilendirmesi de gerekmektedir.

Hiç şüphe yok ki bu biyometrik güvenlik sistemlerinde kullanılacak özel nitelikli kişisel verilerin işlenmesinde de bu kurallara riayet edilmesi gerekir. İlk olarak bu verilerin işlenebilmesi için ilgili kişinin açık rızasının temin edilmesi gerekir. Bu rıza, bilgilendirmeye dayalı, belirli bir konuya ilişkin ve özgür iradeyle verilmelidir. Bilgilendirmeden ya da eksik bilgilendirme ile alınan rızalar ile ya da kişinin özgür iradesine dayanmayan ya da genel nitelikli (belirli bir konuya ilişkin olmayan) rızalar geçersiz olacaktır. Bu genel kuralın dışında, verisi işlenen gerçek kişinin hakları konusunda aydınlatılması gerekmektedir. Bunun haricinde, veri işleyen KVKK'da sayılan veri işlemeye hâkim genel kurallara da uygun davranmak zorundadır.

4.3 Konuya İlişkin Ankara Bölge Adliye Mahkemesi 3. Hukuk Dairesi'nin 20.04.2017 tarihli Kararının Değerlendirilmesi

Kişisel verilerin işlenmesi konusunda incelenecek karar Ankara Bölge Adliye Mahkemesi 3. Hukuk Dairesi'nin 2017/388 esas, 2017/401 no. ve 20.04.2017 tarihli kararıdır.

Bu karara konu olayda;

- ✓ Taraflar arasında 10 yıl süreli ve 10.500-TL üyelik bedelli bir spor merkezi kullanım sözleşmesi kurulmuş, sözleşmede *"üye, tesise üyelik kimlik kartını göstererek girer"* hükmüne yer verilmiş, buna karşın bir süre sonra davalı giriş sistemini değiştirerek, üyelere biyometrik el tanımlama (el izi ile giriş) işlemi yaparak girişi zorunlu tutmuştur.

- ✓ Üye, bu yeni giriş sisteminin sözleşmede yazmadığını, sistemin güvenli ve korunaklı olup olmadığını bilmediğini, ayrıca sistemin sertifikasız olması nedeniyle el izinin hukuka aykırı ve suç amaçlı kullanılabileceğini belirterek yeni giriş sistemini kabul etmediğini bildirmiştir.

- ✓ Bunun üzerine işyeri, tesis kurallarına uyulmadığı gerekçesiyle sözleşmeyi feshetmiştir. Bu fesih üzerine ise üye, dava açarak fesihin haksız olduğunu öne sürmüştür.

- ✓ Davalı işyeri, davacının, üyelik sözleşmesi kapsamında tesisten yararlandığını, tesisin 1995 yılından beri hizmet verdiğini, günün koşulları, güvenlik ve teknolojik gereksinimlerin zaman içinde değişim gösterdiğini, tesisin amacının tüm üyelerin güven ve huzur içinde tesisi kullanmalarını sağlamak olduğunu, sistemin biyometrik değil, geometrik el tanıma sistemi olduğunu, kişinin el izi alınmadan elin 3 boyutlu şeklinin alındığını ve koda çevrildiğini, parmak izi ve avuç içi izi alınmadığını, sözleşmenin 6. maddesinde üyelerin kurallara uymakla yükümlü olduğunu, sistemin kullanılması yönünde davacının sözlü ve yazılı olarak uyarıldığını, sözleşmenin ilgili maddesi uyarınca sözleşmenin feshedildiğini belirterek davanın reddini istemiştir.

- ✓ Yerel mahkemece, davalının spor merkezinin geçiş kontrol noktasında kurduğu geometrik el tarama sisteminin el ya da avuç izi almaksızın, kişilerin el ve parmak karakteristiklerinin üç boyutlu olarak taranması ile şekilsel durumun matematiksel olarak test edilmesi sonucu onay vermesi ya da vermemesi şeklinde gerçekleştiği, cihaz tarafından depolanan verinin HandKey II dışında bir yerde kullanılamayacağı, üyelere ait el ve parmak karakteristik taramalarının farklı yerlerde farklı amaçlarla kullanılma imkânının bulunmadığı, davalı tarafından kurulan sistemin 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun tanımladığı şekilde geniş anlamda kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verileri içerecek şekilde biyometrik kişisel veri kaydı yapmadığı tespit edilerek, taraflar arasında yapılan sözleşmenin 6 ve 8. maddeleri ile geometrik el okuma isteminin davacı tüketicinin sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kurallarına aykırı düşecek biçimde tüketici aleyhine dengesizliğe neden olmadığı, sistemi kuran davalıya külfet getirdiği, üyenin sözleşmeden kaynaklanan yükümlülüklerini ihlal etmesi halinde sözleşmenin haklı nedenle feshedilebileceği, davalının sözleşmeyi haklı olarak bakiye aidatın ödenmesi sureti ile feshettiği, davacının davasında haksız olduğu gerekçesiyle davanın reddine karar verilmiştir.

- ✓ Söz konusu karara karşı istinaf yoluna başvurulduğunda ise Bölge Adliye Mahkemesi yerel mahkemenin gerekçesine ek olarak; sözleşme hükümlerine göre davalının güvenlik tedbirleri alabileceği ayrıca Türkiye çapında 46.926, dava konusu tesiste ise 12.000 aktif üyesi olduğu belirtilen spor merkezinde davalının, spor tesisinin giriş sisteminde üye ve yakınları haricinde, sahte üyelik kartı kullananların engellenmesi ve güvenlik amacı ile değişiklik yaparak kimlik kartı uygulamasından daha gelişmiş el geometrisi okuma sistemine geçerek güvenlik tedbirleri almasında hukuka aykırılık bulunmadığı gerekçeleriyle sözleşmenin haklı nedenlerle feshedildiğine dair mahkeme kararını onamıştır.

Söz konusu yerel mahkeme kararında dikkat çekici olan kısım, mahkemenin işyeri tarafından getirilen yeni giriş sisteminin işleyişini sağlayan el taramasını kişisel veri olarak nitelendirmemesidir. Mahkeme, sistemin el ya da avuç izi alınmaksızın, el ve parmak karakteristiklerinin üç boyutlu olarak taranması, yani elin şeklinin alındığını ve bunun koda çevrilerek kullanıldığını bunun da kişisel veri niteliğinde olmadığını belirterek, işyerinin yaptığı feshin haklı olduğuna karar vermiştir. Ayrıca depolanan verinin başka bir yerde kullanılma imkânının da olmadığını belirtmiştir.

Yerel mahkemenin kararına katılmak mümkün değildir. İlk olarak şunu belirtmek gerekir ki teknik olarak, el ya da avuç izi alınmıyor olması tek başına işlenen verinin kişisel veri olmadığını ortaya koyar yeterlilikte değildir. Zira bir verinin kişisel veri olarak nitelendirilmesi için bu verinin kimliği belli ya da belirlenebilir bir gerçek kişiyle ilişkilendirilebilir olması yeterlidir. Davaya konu olayda da her ne kadar teknik anlamda avuç izi ya da el izi olarak adlandırılamayacak bir uygulama mevcutsa da sistemin temel işleyiş mantığına bakıldığında bir gerçek kişinin o işletmeye girerken başka kişilerden ayırt edilmesi amacına hizmet eden bir taramanın mevcut olduğu görülür. İlgilinin elinin şeklinin belirlenerek bunun bir koda çevrilmesi şeklinde özetlenebilecek işlemin nihai amacı her üyenin farklı olan elinin geometrik şeklinin bir anlamda şifreye dönüştürülmesidir. Dolayısıyla, söz konusu taramanın yapılması ve sisteme aktarılması neticesinde, ilgili gerçek kişinin her girişinde elini okutması sonrasında sistemin depoladığı tarama ile okutulan bu elin doğrulamasını yapması şeklinde işleyen bir süreç bulunmaktadır. Bu sistemin bir anlamda bilgi doğrulama üzerine çalıştığını söyleyebiliriz. (Akgül, 2015:203). Ve sistem bu doğrulamayı ilgili gerçek kişiyi diğerlerinden ayırt edebilecek ve teknik olarak sadece o kişiye ait bir taramayı kullanarak yapmaktadır. Bir Anayasa Mahkemesi kararında da (E.2014/180, K.2015/30, T.19.03.2015) biyometrik yöntemlerle kimlik doğrulama *"hizmet talep eden bir kullanıcının, ölçülebilir fizyolojik ve bireysel özellikler yoluyla gerçekleştirilen ve otomatik olarak doğrulanabilen kimlik denetleme yoluyla gerçek kullanıcı olup olmadığının doğrulanması"* olarak tanımlanmıştır. Bu nedenle, dava konusu olay kapsamında, sistemin işleyişi için gerekli olan tarama faaliyetiyle kişisel bir veri oluşturulduğu konusunda duraksamaya yer yoktur. Çünkü matematiksel bir koda dönüştürülmüş bu şekil, kimliği belirlenebilir bir gerçek kişiye aittir. Zira her ne kadar işyeri bu verinin başka yerlerde kullanılamayacağını ileri sürmüşse de aynen söz konusu işyerindeki sistemin yaptığı gibi söz konusu kod üzerinden ilgili gerçek kişinin kimliğine ulaşabilecek başka ya da benzer sistemler söz konusu olabilir. AİHM kararlarında da parmak izi, DNA profili ve hücre örneklerinin kişisel veri niteliğinde olduğu kabul edilmektedir (Akgül, 2015:206). Ayrıca, söz konusu taramanın ya da kodun benzer şekilde çalışan sistemlere aktarılmasında da bir engel yoktur. Yine belki bugünün teknolojik imkânlarıyla mümkün olmamasına karşın bu verinin ileride teknolojik gelişmeler sonucunda başka şekillerde kullanılması imkânı da olabilir. Bu nedenle, ilgili kişinin elinin şeklinin alınması ya da taranması suretiyle giriş yapılabilmesi için ilgili kişinin önceden bilgilendirilmesi ve açık rızasının alınması gerekmektedir (Manav, 2015:121). Dava konusu olayda ise ilgili kişinin açık rızası bulunmadığı gibi işyerinin veri işlemesine izin veren bir kanun hükmü de yoktur. Bu yönüyle esasen işyerinin böyle bir sistem değişikliğinin yapması ve uygulaması hukuken mümkün olmamalıdır. Zira bu olayda sıradan

bir sözleşme ilişkisinden ziyade, kişisel veri işlemesi söz konusudur. Ancak hem yerel mahkeme hem de bölge adliye mahkemesi, bu giriş sistemi değişikliğini sadece tüketici hukuku kapsamındaki "haksız şart" penceresinden ve genel sözleşme adaleti bakımından incelemiş ve kararını da bu çerçevede vermiştir. Bu bakımdan her iki mahkemenin kararlarının da isabetsiz olduğunu söyleyebiliriz.

Danıştay, kamu personelinin mesai takibinde biyometrik yöntemlerin kullanılmasına ilişkin olarak önüne gelen bir olayda, kişisel verilerin işlenmesinden önce toplanan kişisel verilerin ileride başka bir şekilde kullanılmayacağına ilişkin bir güvencenin mutlaka verilmiş olması gerektiğini belirtmiştir (Akgül, 2015:213) İncelediğimiz olayda ise karardan anlaşıldığı üzere, üyenin dava öncesindeki bu yönde başvurusuna karşın, işyerinin topladığı kişisel verilerin başka bir şekilde kullanılmayacağına ilişkin açık ve kesin bir taahhüdü bulunmamaktadır. İlgili karar bu yönüyle de sorunludur.

Öte taraftan, işyerinin bu tür bir uygulamayı zorunlu hale getirmesi üzerinde de durulmalıdır. Bilindiği üzere, kişisel verilerin işlenmesi konusunda verisi işlenen gerçek kişinin zorlanması mümkün değildir. Bunu "açık rıza"nın özgür iradeye dayanması ilkesinde açıkça görürüz. Öte taraftan, bu ilkenin bir diğer görünümü de *"bir ürün ya da hizmetin sunulmasının kişisel verilerinin işlenmesi için rıza verilmesi şartına bağlanamaması"*dır. Gerçekten, böyle bir durumda, rızanın özgür iradeye dayandığını söylemek mümkün değildir. Bu husus Kişisel Verileri Koruma Kurumu'nun internet sitesinde yer alan bilgilendirme dökümanlarında da açıkça ifade edilmiştir; *"Örneğin; veri sorumlusu tarafından veri sahiplerinin rızalarının elde edilmesi, bir ürün veya hizmetin sunulmasının ön şartı olarak ileri sürülmemelidir."* Dolayısıyla, işyerinin, üyenin sözleşmeye konu hizmetten faydalanmasını bu giriş şartına bağlanması da hukuken mümkün değildir. İşyeri, üyenin rıza vermemesi durumunda, bu üye özelinde eski giriş sistemini işletmeye devam etmeliydi, bunun yerine üyeyi zorlaması ve bu rızayı alamadığı durumda da sözleşmeyi feshetmesi hukuki açıdan doğru değildir. Bu nedenle de sözleşmenin feshinin de haksız sayılması gerekir, zira ortada sözleşme ilişkisini bitirecek bir haklı neden bulunmamaktadır.

Eurasian Academy of Sciences
Eurasian Business & Economics Journal
2017 Volume: 1 S: 174-190
Published Online December 2017 (http://busecon.eurasianacademy.org)
http://dx.doi.org/10.17740/eas.econ.2017-insemp-14

SONUÇ

Teknolojik yeniliklerin hızla gelişmesi, işletmelere hem operasyonel hem de yönetimsel açıdan birçok alanda kolaylık sağlamıştır. İşletmelerin, üretim süreçlerinden hizmetlerinin sunumuna kadar neredeyse her faaliyetinde teknolojinin sağladığı tüm imkânlardan faydalandığı dikkat çekmektedir. Teknolojideki gelişmelerle birlikte işletmeler, denetim işlevini daha etkin bir şekilde yerine getirebilmek amacıyla; yönetimsel bir süreç inovasyonu olarak değerlendirebileceğimiz "biyometrik güvenlik teknolojilerini" kullanmaya başlamıştır. Bu teknolojilerin kullanımı işletmelere, denetim işlevinin yerine getirilmesinde birtakım yararlar sağlamakla beraber müşterilerin veya çalışanların kişisel hak ve özgürlüklerinin ihlaline de neden olabilmektedir. Bu durum ise bireyler üzerinde endişelere yol açabilmekte ve işletmelerde kullanılan söz konusu teknolojinin hukuki olarak değerlendirilmesini gerekli kılmaktadır.

KVKK'nın yürürlüğe girmesiyle birlikte, artık kişisel veriler çok daha etkin bir şekilde koruma altına alınmıştır. Ancak, yeni sayılabilecek bu kanunun uygulanmasıyla ilgili olarak henüz yeterli içtihat oluştuğunu ve yine var olan içtihatların da henüz yeterli seviyede olduğunu söylemek güçtür. Ancak, kanunla ilgili yönetmeliklerin çıkması ve bu konudaki Kurum'un ilke kararlarının yayınlanmasıyla birlikte zamanla bu içtihatların gelişerek istikrar kazanacağı da düşünülmektedir.

Bu çalışma sonucunda, biyometrik verilerin "özel nitelikli kişisel veri" niteliğinde olduğunu ve bu nedenle de işlenmeleri için ya kanuni bir yetkinin bulunması ya da ilgili kişinin açık rızasının bulunması gerektiğini tespit etmiş bulunuyoruz. Bunun yanında söz konusu verilerin niteliği nedeniyle, Kişisel Verileri Koruma Kurulu'nun alacağı özel önlemlerin de veri işleyenler tarafından alınması gerekecektir.

Biyometrik verilerin, işletmelerin elektronik süreçlerinde kullanılmasının; güvenlik, maliyet, hız ve diğer birçok konuda avantaj sağladığı bir gerçektir. Ve bu kullanımın artarak devam edeceği de muhakkaktır. Ancak tüm bu avantajlara karşın bu verilerin kişilik hakkının bir parçası olması hasebiyle etkili bir şekilde korunması da ihtiyaç haline gelmiştir. Bu nedenle kanun koyucu bu iki farklı menfaat arasında bir denge kurmuştur. Bu verilerin kullanılması tamamen yasaklanmamış sadece hak sahibinin açık rızasına ve kanuni yetkiye bağlanmıştır. Bu nedenle, işletmeler tarafından bu sistemlerde kullanılacak verilerin elde edilmesi sırasında ilgili kişinin aydınlatılması ve rızasının açık bir şekilde alınması, ayrıca bu konuda varsa belirlenen diğer önlemlerin alınması büyük önem arz etmektedir.

Son olarak, bu çalışmada incelenen Ankara Bölge Adliye Mahkemesi 3. Hukuk Dairesi'nin 2017/388 esas, 2017/401 numara ve 20.04.2017 tarihli kararının, kişisel verinin tanımlanması, ilgili kişinin rızasının alınması, hizmetin sunumu veya ürünün satışının rızanın verilmesi şartına bağlanması gibi hususlarda 6698 sayılı Kişisel Verilerin Korunması Kanunu'na aykırı olduğunu düşünmekteyiz.

Eurasian Academy of Sciences
Eurasian Business & Economics Journal
2017 Volume: 1 S: 174-190
Published Online December 2017 (http://busecon.eurasianacademy.org)
http://dx.doi.org/10.17740/eas.econ.2017-insemp-14

KAYNAKÇA

Akdağ, H. (2013). Türk Ceza Hukuku Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi.

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

Aksoy, H.C. (2010). Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi.

Ayözger, A.Ç. (2016). Kişisel Verilerin Korunması (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil), Beta Yayınları.

Başalp, N. (2004). Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayıncılık.

Carpenter, D.; Maasberg, M.; Hicks, C.; Chen, X. (2016). A Multicultural Study of Biometric Privacy Concerns in a Fire Ground Accountability Crisis Response System, *International Journal of Information Management*, 36, 735–747.

Chen, H. (1988). *Medical Genetics Handbook*, W. H. Green, St. Louis, MO, 221-226.

Cole, S. (2004). Fingerprint Identification and the Criminal Justice System:Historical Lessons for the DNA Debate. In D. Lazer (Ed.), *DNA and the Criminal Justice System: The Technology of Justice*. Cambridge, MA: MIT Press.

DPC, Data Protection Commissioner, (Çevrimiçi) https://www.dataprotection.ie/docs/Biometrics_in_the_workplace./244.htm, 22 Ekim 2017.

Hay, R. (2004). Physical Security: A Biometric Approach. SANS Institute Reading Room.

Henkeloğlu, T. (2015). Bilgi Güvenliği ve Kişisel Verilerin Korunması, Yetkin Yayıncılık.

International Biometrics and Identity Association (IBIA), (Çevrimiçi) https://www.ibia.org/biometrics-and-identity/why-biometrics, 19 Ekim 2017.

IPC, Information and Privacy Commissioner, (Çevrimiçi) http://www.ipc.on.ca/index.asp?layid=86&fid1=87.O%E2%80%99Neil, 22 Ekim 2017.

Jain, A.K.; Kumar, A. (2012). Biometric Recognition: An Overview. E. Mordini and D. Tzovaras (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, The International Library of Ethics, Law and Technology 11, Dordrecht: Springer.

Luis-García, R.; Alberola-López, C.; Aghzout, O.; Ruiz-Alzola, J. (2003). Biometric Identification Systems, *Signal Processing*, 83, 2539 – 2557.

Kişisel Verileri Koruma Kurumu. (Çevrimiçi) http://www.kvkk.gov.tr/, 2 Kasım 2017.

Korkmaz, İ. (2016). Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, TBB Dergi, 124, 81-152.

Lexpera Mavzuat ve İçtihat Programı, https://www.lexpera.com.tr/, 1 Kasım 2017.

Manav, E. (2015). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, GÜHFD C. XIX, S.2, 95-136.

Miller, B. (1994). Vital Signs of Identity, IEEE Spectrum, 31(2), 22–30.

Oğuz, H. Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, Ulusal Hakemli Uyuşmazlık Mahkemesi Dergisi, 3. Sayı, 1-38.

Özdemir, H. (2009). Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayıncılık.

Pocovnicu,A.(2009). Biometric Security for Cell Phones, *Informatica Economică*,13(1), 57-63.

Skoler, M. (1984). Finger and Palm Prints: A Window on Your Health, *Glamour*.

Şimşek, O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayınları.

Tassabehji, R.; Kamala, M.A. (2012) Evaluating Biometrics for Online Banking: The Case for Usability, *International Journal of Information Management*, 32, 489– 494.

Türk Dil Kurumu (TDK). (Çevrimiçi) http://www.tdk.gov.tr, 18 Ekim 2017.

Woodward, J.D. (1999). Biometrics: Identifying Law & Policy Concerns, 385-405, in A. Jain, R. Bolle and S. Pankanti (eds.) *Biometrics, Personal Identification in Networked Society*, Boston, MA, Dordrecht and London: Kluwer Academic Publishers.

6698 Sayılı Kişisel Verilerin Korunması Kanunu.