

**ULUSLARARASI ALANDA BİYOMETRİK VERİ KAVRAMINA
YAKLAŞIM GÖZ ÖNÜNE ALINARAK TÜRK HUKUKUNDA
BİYOMETRİK VERİ İŞLEME ŞARTLARININ ÖLÇÜLÜLÜK İLKESİ
BAKIMINDAN SOMUTLAŞTIRILMASINA DAİR ÖNERİLER**

20.01.2020

AV. İSMAİL MERT ŞANLI

AÇIKLAMALAR

İşbu çalışmada biyometrik veri kavramı açıklanarak önemi irdelenecek, ulusal ve uluslararası boyutta meydana gelen ihlaller ve yaygın uygulamalar analiz edilerek dijitalleşen dünyada, günümüzde ve gelecekte bu ihlallerin ne gibi olumsuz sonuçlar doğurabileceği tartışılacak, bu kapsamda doğabilecek riskleri en aza indirmek için Türk Hukuku'nda yapılması gereken düzenlemelere ilişkin öneriler paylaşılacaktır. 6698 sayılı Kişisel Verilerin Korunması Kanunu¹'nda düzenlenen özel nitelikli kişisel verilerin işleme şartlarına ilişkin düzenlemenin yetersizliği ve bu güncel düzenlenmenin birçok gri nokta bırakması sorunu nedeniyle konunun özü ve meydana gelecek ihlallerin olası olumsuz sonuçlarının ciddiyeti değerlendirildiğinde ivedilikle somutlaştırılması gerektiği ortadadır. Bu doğrultuda 95/46/EC sayılı Avrupa Direktifi² ile 1998 yılından itibaren verilerin işleme şartları ve korunmasına ilişkin yasal düzenlemeye tabi Avrupa ülkelerinde biyometrik verilere dair uygulamalar ve doğan ihlallere yaklaşımı, benzeri bir yasaya tabi olmayan Çin Devleti'nin vatandaşları üzerindeki otoriter baskıyı arttıran “gözetleme”(surveillance)'ye dayalı olarak yürüttüğü politikalar neticesinde biyometrik veri alışverişini yaygınlaştırılan uygulamaları ve ihlallere yaklaşımı gibi uluslararası alanda biyometrik verinin işlenmesine ilişkin yaklaşımlar belirtilecek ve Türk Hukuku'ndaki güncel düzenlemeye getirilecek eleştirileri takiben özellikle soyut bir kavram olan amaçla ölçülülük ilkesi açısından getirilebilecek somut düzenlemelere ilişkin öneriler aktarılmaya çalışılacaktır.

İÇİNDEKİLER

1. Biyometrik Veri
2. Biyometrik Veri İhlallerinin Günümüzde ve Gelecekte Doğurabileceği Olumsuz Sonuçları
3. Ulusal Alanda Biyometrik Veri İhlalleri ve Yaygın Kullanımları
4. Uluslararası Alanda Biyometrik Veri İhlalleri ve Yaygın Kullanımları

¹ 07.04.2016 tarihli ve 29677 sayılı resmi gazetede yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu(“KVKK”).

² 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi – Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi

5. Türk Hukukunda Güncel Düzenlemeye Getirilen Eleştiriler ve Biyometrik Veri İşlenmesinde Ölçülülük İlkesinin Somutlaştırılmasına Dair Öneriler

1. BİYOMETRİK VERİ

1.1. Biyometrik Veri Kavramı

Bilgisayarlara ve güvenliğe atıfta bulunulduğunda biyometri, bir kişinin biyolojik özelliklerinin ölçülerek tanımlanmasıdır. Örneğin, kişinin kendi parmak izi veya sesi ile kendini bir bilgisayara veya binaya ya da bir yere tanıtmada kullandığı parmak izi veya ses o kullanıcının biyometri kimliği olarak kabul edilir. Biyometri, insanların fizyolojik ve davranışsal özelliklerinin ölçülmesi ve analizidir. Biyometrik veriler özellikle giriş veya hizmet alımlarında kimlik tespiti ve erişim iznini vermek veya işlemleri dijital olarak imzalamak için kullanılmaktadır. Bu uygulama herkesin benzersiz fizyolojik özelliklere sahip olduğu ve bu fizyolojik özelliklere sahip kişiler tarafından tanımlanabileceği fikrine dayanmaktadır. Nitekim tam da bu nedenden dolayı 6698 sayılı Kişisel Verilerin Korunması Kanunu madde 6³ kapsamında biyometrik veriler özel nitelikli kişisel veri olarak kabul edilmiş ve genel nitelikteki kişisel verilere göre daha ağır bir korumayı gerektirdiği kabul edilmiştir.

Biyometrik veri iki temel canlı özelliğine dayanmaktadır. Bunlar fizyolojik özellik ve farklılıklar ve davranışsal özellik ve farklılıklar olarak ikiye ayrılmıştır. Fizyolojik özellikler parmak izleri, DNA, yüz, damar ağı, iris, kulak şekli, koku olarak karşımıza çıkmaktayken davranışsal özellikler, insanların yazı yazma, yürüme biçimi veya ses ve vücut hareketleri olarak karşımıza çıkmaktadır. Bir şifre ile karşılaştırıldığında, bu sistem türü, kişiye özgü olduğundan sahte olma olasılığı daha düşük diye kabul edilmektedir. Sonuç olarak, Biyometrik veri, bireyin ölçülebilir fiziksel ve davranışsal özelliklerini tanıyarak kimlik saptamak üzere geliştirilmiş otomatik sistemler için kullanılan bir terimdir⁴.

1.2. Biyometrik Verinin Kullanım Yöntemleri

³ KVKK m.6 “(1) 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 verileri özel nitelikli kişisel veridir.”

⁴ Danıştay 15. Dairesi 2014/4562 E. sayılı kararı

Biyometri taramasının yaygın yöntemleri kişinin yüzü, eli, irisi ve retinadır. Biyometrik yüz tarayıcıları ise bir kişinin yüzünü ölçerek bir kişiyi tanımlamaktadır. Bu tanımlamayı çene, gözler (gözbebekleri arası mesafe), burun ve ağız arasındaki mesafeyi göz önüne alarak yapmaktadır. Bu tür tarayıcılar, bir kişinin resmini gerçek bir kişi ile ayırt edebilecek kadar akıllı oldukları varsayılarak kullanılmak istenen amaç doğrultusunda efektif olarak çalışabilmektedir. El avuç içi tarayıcısı, parmak izi baskı gibi avuç da kişiye özeldir. Biyometrik bir el tarayıcı, kişinin elinin avuç içi tarafından tanımlanmasını sağlamaktadır. Parmak izi tarayıcı, biyometrik bir parmak tarayıcı parmak iziyle kişiyi tanımlamaktadır. Bunlar bir kişiyi tanımlamak için güvenli bir yöntem olabilmekte bu nedenle de teknoloji geliştikçe daha çok kullanılmak istenmektedir. Retina veya iris tarayıcı, biyometrik bir retina veya iris tarayıcı, gözlerini iris veya retinayı tarayarak tanımlamaktadır. Bu tarayıcılar, diğer cihazlarla karşılaştırıldığında daha güvenli biyometrik kimlik doğrulama şekilleridir, çünkü retina veya irisi kopyalamanın bilinen bir yolu henüz yoktur. Ses tarayıcı, bir ses analiz tarayıcısı, onları tanımlamak için matematiksel olarak kişinin sesini parçalara bölerek kişinin sesine özgü olarak tanımlamayı sağlayacaktır.

2. BİYOMETRİK VERİ İHLALLERİNİN GÜNÜMÜZDE VE GELECEKTE DOĞURABİLECEĞİ OLUMSUZ SONUÇLAR

Biyometrik verilerin özü itibariyle sıkı sıkıya kişiye özgü olması, elde edilen biyometrik verilerin analizinden teknolojinin gelişmesi ile kişiye dair önemli bulguların elde edilebiliyor olması bu konuda hassas davranılması gerekliliğini ortaya koymaktadır. Şöyle ki biyometrik verilerin analiz edilerek kayıt sırasında elde edilen verilerin kayıtlı kişinin izin vermediği yollar için kullanılabilmesi mümkündür. Kişiden elde edilen biyotmerik verinin biyometrik özelliklerinin çoğunda fizyolojik ve/veya patolojik tıbbi durumlar tespit edilebilmekte, güvenlik gerekçesiyle elde edilen bir parmak izi kalıpları kromozomal hastalıklarla, iris kalıpları genetik cinsiyeti gösterebilmektedir. El damarı kalıpları vasküler hastalıkları veya çoğu davranışsal biyometri, nörolojik hastalıkları ortaya çıkarabilmektedir. Ayrıca, ikinci nesil biyometri, özellikle de davranışsal ve elektro-fizyolojik biyometri, duygu tespiti için kullanılabilir. Kimlik doğrulama için elde edilen bir biyometrik verinin tümör bulma gibi kimlik doğrulamadan daha ileri gidecek şekilde kullanılması ve bunun kişiyi toplumdan ayırıştırılmasına neden olacak olması biyometrik verinin etki alanlarının anlaşılacak öneminin

kavranmasını daha iyi sağlamaktadır. Hatta gelişen teknoloji ile kimlik tespiti veya kimlik doğrulama yapılmaksızın, bir kişinin yüzünün kalabalıkta tanımlanması ve bu tanımlanmanın kişinin haberi olmaksızın bilgisi dışında kullanılması riskler dahlindedir. Veriler ait olduğu kişi istemese de gizlice her sisteme depolanabilir. Güvenlik için kullanılan biyometrik veriler aynı zamanda hırsızları çalacağı kıymete erişmek için, kıymet sahibine zarar verme fikrine yönlendirebilir. Emtia, biyometrik bir veri ile korunuyorsa, sahibine verilen zarar geri döndürülemez ve güvenlik altındaki bulunması gerekenden daha pahalı olabilmektedir. Örneğin, 2005 yılında Malezya araba soyguncuları, arabayı çalmaya çalışırken bir Mercedes-Benz S-Serisi kullanıcısının parmak izi için parmağını kesmiştir⁵.

Bunun haricinde parolaların biyometriye kıyasla sağladığı bir avantaj, tekrar gönderilebilmesidir. Bir belirteç veya parola kaybolursa veya çalınırsa, iptal edilebilir ve daha yeni bir sürümle değiştirilebilir. Bu biyometride doğal olarak mevcut değildir. Birinin yüzü bir veri tabanından çıkarılırsa, bunlar iptal edilemez veya yeniden gönderilemez. Elektronik biyometrik tanımlayıcı çalınırsa, biyometrik bir özelliği değiştirmek neredeyse imkânsızdır. Bu nedenle de geri dönülemez zararlara yol açması mümkündür. Biyometrik verinin işleme amacıyla kişi nezdinde doğurabileceği hak mahrumiyetleri ve zararlar karşılaştırdığında bu olası kötüniyetli kullanımların geri dönülemez ve yıkıcı niteliği göz önüne alınırsa ölçülülük ilkesinin kişiden yana daha ağır bastığı kabul edilmelidir.

3. ULUSAL ANLAMDA BİYOMETRİK VERİ İHLALLERİ VE YAYGIN UYGULAMALAR

3.1. Kişisel Verilerin Korunması Kurumu'nun Spor Salonu Kararı⁶

Türkiye'deki bir spor salonun üyelerinin giriş-çıkışının takibini yapmak için üyelerinin avuç-içi verilerini kullanması Kişisel Verilerin Korunması Kurumu("Kurum") tarafından kişisel veri ihlali olarak kabul edilmiş olup Kurum ilgili spor salonuna idari para cezası uygulanmasına, biyometrik veri ile giriş-çıkış işlemleri yapılmasının ve biyometrik veri işleminin ivedilikle durdurulmasına ve bugüne kadar işlenen verilerin ivedilikle yok edilmesine karar vermiştir.

⁵ <http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>

⁶ 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti

İlgili kurul kararında ihlal ölçülülük bakımından ele alınarak “ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği, kişisel verilerin işlenmesinin ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın, aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar için ve gerektiği kadar toplanması, amacın gerektirdiği yerlerde kullanılması ve amaç için gerekli olandan uzun süre tutulmaması gerektiği” belirtilmiş ve kararda amaç doğrultusunda toplanan verinin, amaca daha az korumayı gerektiren bir yöntemle ulaşılması mümkünken olumsuz kullanımının sonuçları bakımından çok daha riskli olan biyometrik verinin kullanılmasının ölçülü olmadığı vurgulanmıştır.

3.2. Sağlık Hizmeti Sunulmasının Ön Şartı Olarak Biyometrik Veri Kullanılması

1.3.2012 tarihli ve 6283 sayılı Kanunun 1. Maddesi ile Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu⁷’nin 67. maddesinin 3. fıkrasına⁸ “biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya” ibaresi eklenerek sağlık hizmetlerinden yararlanmak isteyen kişilerin biyometrik verilerini paylaşma yükümlülüğü getirilmiş ve Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği’nin 1.6. maddesinde⁹ “ve/veya” bağlacı yerine “ve” bağlacı kullanıldığından biyometrik yöntemlerle kimlik doğrulaması uygulamada zorunlu hale getirilmiştir. Bu uygulama, izinsiz kullanımlara karşı güvenli, kamu kuruluşlarına yönelik yolsuzluk ve bunların neden olduğu zararlara karşı etkili ve sosyal güvenliği olan kişiler

⁷ 16.06.2006 tarihli ve 26200 sayılı resmi gazetede yayımlanarak yürürlüğe giren Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu (“SGK Kanunu”)

⁸ SGK Kanunu madde 67/3 “Ayrıca genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında acil haller hariç olmak üzere (acil hallerde ise acil halin sona ermesinden sonra); biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya Kurum tarafından verilen resimli sağlık kartı belgelerinden birinin gösterilmesi zorunludur.⁽¹⁾”

⁹ “(1) Sağlık kurum ve kuruluşlarınca, kişilerin müracaatı aşamasında, acil hallerde ise acil halin sona ermesinden sonra, nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya verilmiş ise Kurum sağlık kartı belgelerinden biri ile kimlik tespiti ve biyometrik yöntemlerle kimlik doğrulaması yapılması zorunludur.”

tarafından da güvenli hizmet alınmasını sağlaması amacıyla getirilmiştir. Ayrıca getirilen uygulamanın gerekçesinde sağlık hizmetlerinin elektronik ortamda güvenilir altyapılar üzerinden sağlanması ve hizmetten yararlananların kimliklerinin saptanmasında geleneksel yöntemlerin eksiklikleri nedeniyle ortaya çıkan kötüye kullanımların önlenmesinin amaçlandığı belirtilmiştir. Ancak sağlık hizmetinden faydalanmak için biyometrik veri paylaşımının zorunlu tutulması tartışmalara yol açmıştır.

Danıştay, sağlık hizmetinin sunumunda biyometrik yöntemler kullanılarak kişisel veri elde edilmesine olanak veren 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesinin 3. fıkrasını Anayasaya aykırı bularak Anayasa Mahkemesine başvurmuş ise de Anayasa Mahkemesi oyçokluğuyla itiraz başvurusunu reddetmiştir.

İlgili Anayasa Mahkemesi kararında¹⁰ 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişisel Verilerin Korunmasına Dair Avrupa Konseyi Direktifine atıf yapan Anayasa Mahkemesi biyometrik verinin kişisel bir veri olduğunu kabul etmiş ancak kararında bu direktifin 6. maddesinde özel olarak belirtilen politik düşünce, dini inanç, sağlık, cinsel yaşam veya ceza mahkumiyetlerine ilişkin veriler gibi çok hassas verilerden olduğunun söylenemeyeceğini ifade etmiştir. Hızla gelişen teknoloji ile biyometrik verilerinin kullanım alanlarının yaygınlaşmasına rağmen Anayasa Mahkemesi'nin 1981 tarihli bir sözleşmeye atıf yaparak işbu çalışmanın 2 numaralı başlığında anlatıldığı üzere biyometrik verinin kötü niyetli kullanımının olumsuz sonuçlarını değerlendirmeksizin böyle bir karar vermesi kanaatimce yerinde değildir.

Ayrıca kararda ilgili yöntemin sadece sağlık sektöründe bu hizmetten yararlanma amacıyla kullanılabilmesi ve bu amaç ve kapsam dışında kullanılması halinde Türk Ceza Kanunu¹¹'nde kişisel verilerin korunmasına ilişkin ceza hükümlerinin uygulanacak olması nedeniyle bu konuda kanuni güvence bulunması nedenleriyle yöntemin tercih edilme amacıyla ölçülü olduğu kabul edilmiştir.

Ölçülülük değerlendirmesinde her ne kadar kullanım amacının sınırlı olması ve kanuni yaptırımların öngörülerek devlet güvencesinin sağlandığından bahsedilmiş olsa da olası bir

¹⁰ Anayasa Mahkemesi 2014/180 E. 2015/30 K. numaralı, 19.03.2015 tarihli kararı

¹¹ 26.09.2016 tarihli ve 25611 sayılı resmi gazetede yayımlanarak yürürlüğe giren 5237 sayılı Türk Ceza Kanunu

ihlalin geri dönülemez sonuçlar doğuracağı ve bu ihlali gerçekleştirenlere karşı cezai yaptırımlar öngörülmüş olsa dahi biyometrik verisi ihlal edilen kişinin var olduğu süreç boyunca bu ihlalin kendisine tehdit oluşturacağı(biyometrik verinin değiştirilmez olması nedeniyle) ortadadır. Sağlık hizmetlerinden yararlanmak için biyometrik verinin paylaşılmasının zorunlu tutulmasının bu veriyi alıp depolayanın bir devlet kurumu olmasına rağmen (verinin güvencesinin devlet tarafından temin edilmesi bakımından) ölçülü olmadığını düşünmekteyim. Bu kapsamda bu uygulamanın değiştirilerek kimlik doğrulamasının kişilik haklarına daha az zarar verme ihtimali olan verilerle sağlanmasına yönelik yeni bir yöntemin kullanılması gerekmektedir.

3.3. Diğer Yaygın Uygulamalar

Ülkemizde işletmelerin ticari faaliyetleri doğrultusunda özellikle büyük fabrikalarda mavi yakalı çalışanlarının işe giriş çıkış saatlerinin takibini yapmak için çalışanlarından biyometrik verilerini aldıklarını sıklıkla görmekteyiz. Özellikle çalışan sayısı arttığında kartlı sistemle giriş çıkışların takibinin yapılamadığı ve çalışanlarca bu durumun su istimal edildiği belirtilmekte kişiyi tanımlamakta etkili yol olan parmak izi tarayıcıları veya yüz tarama sistemleri ile çalışanlarının giriş çıkışlarını takip etmektedirler. Veri sorumlusu sıfatıyla ticari işletmenin meşru menfaati ile çalışanların kendilerine sıkı sıkıya bağlı olan ve daha ağır koruma gerektiren biyometrik verilerinin işlenmesi arasında ölçülülüğün iyi irdelenerek çalışanların açık rızaları alınarak böyle bir yöntemin benimsenip benimsenemeyeceğinin değerlendirilmesi gerekmektedir.

Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun¹² kapsamında da tribünde maç seyretmek isteyen seyircilerin biyometrik verilerinin alınarak tribünde işbu kanuna aykırı davranan seyircilerin daha kolay tespit edilebilmesi amaçlanmaktadır. Yasallaşan ancak henüz fiili olarak uygulanmayan bu hüküm de birçok tartışmayı beraberinde getirmektedir. İlgili kanun her ne kadar sporda şiddet eylemlerinin önüne geçmeyi planlansa da meydana gelebilecek şiddetin kamu üzerindeki etkisi, bu şiddet eylemlerinin başka türlü önlemlerle de önüne geçilmesinin mümkün olması(uluslararası örneklerde sporda şiddet eyleminin

¹² 31.03.2011 tarihli ve 27905 sayılı resmi gazetede yayımlanarak yürürlüğe giren 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun

yaşanmadığı ülkelerde böyle bir uygulamanın olmadığı görülmekte) gibi unsurlar göz önüne alındığında ölçülü olarak değerlendirilemeyecektir.

Bunun haricinde pasaport işlemleri, cezaevi giriş çıkışlarının takibinin yapılması, emniyet tarafından kamu güvenliği açısından parmak izinin alınması gibi nedenlerle de ülkemizde yaygın olarak biyometrik veri işlenmektedir.

Vatandaşların kullandığı telefonlarda tamamen kendi tercihlerine bağlı olarak yüz tanıma sistemlerinin ve parmak izi şifrelemelerinin de yaygın olarak kullanıldığını söylemek mümkündür. Telefon kullanıcılarının biyometrik veri ile şifreleme yöntemini kullanmaları tamamen mutlak olarak kendi takdirlerindedir. Bu nedenle kanaatimce ilgili yöntem ölçülülük açısından bir değerlendirmeyi gerektirmemektedir. Kişinin seçme özgürlüğü dahilinde iradesi baskı altına alınmaksızın kendi rızasıyla biyometrik verisini paylaşmasının engellenmesi özgürlüğüne yönelik bir müdahale olacaktır. Ancak şunu belirtmek gerekir ki kullanıcı kendi rızasıyla biyometrik verisini paylaşmış olsa da bu verinin veri sorumlusu tarafından korunması ve bu kapsamda üzerine düşen yükümlülükleri yerine getirmesi ve devletlerin ilgili kurumlarının bu konuda denetim faaliyetlerini yürütmesi önem arz etmektedir.

4. ULUSLARARASI ALANDA BİYOMETRİK VERİ İHLALLERİ VE YAYGIN KULLANIMLARI

Öncelikle şunu belirtmek gerekir ihlal kavramı uluslararası boyutta farklılıklar içermekte olup her ülkenin veya topluluğun biyometrik veri kavramına yaklaşımına göre değişiklik göstermektedir. Bu kapsamda farklı ülkelerin biyometrik veri ihlali olarak değerlendirdiği olaylar açıklanacak ve biyometrik verinin yaygın kullanım alanları belirtilecektir.

4.1. İsveç Veri Koruma Kurumunun Lise Kararı¹³

İsveç'in Skelleftea kentindeki bir lise, öğrencilerinin devam durumunu takip edebilmek amacıyla 22 öğrencisinin katılımıyla 3 hafta boyunca yüz tanıma teknolojisinin testlerini yürüterek öğrencilerinin biyometrik verilerini işlemiştir. Bu kapsamda öğrencilerinin açık rızalarını aldığı öne süren okula İsveç Veri Koruma Kurumu tarafından idari para ceza yaptırımını uygulanarak ilgili yöntemin ivedilikle durdurulması için lise talimatlandırılmıştır.

¹³ https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

Kurul, alınan açık rızaları ilgili kişi ve veri sorumlusu arasındaki dengesizlik bakımından geçerli bulunmayarak ilke bir karar vermiştir. Kurumun bu kararı biyometrik veri işlenmesini daraltan bir yorumla yaklaştığını göstermektedir.

4.2. Belçikalı Çalışanların Biyometrik Verilerinin Sızdırılması¹⁴

Ülkemizde olduğu gibi Avrupa’da da çalışanların işyerine giriş çıkış takibinin yapılabilmesi amacıyla parmak izi, yüz tanıma verileri gibi biyometrik veriler yaygın olarak işlenmektedir. Çalışanlarının işyerine giriş çıkış takibini biyometrik verilerini kullanarak gerçekleştiren Adecco şirketinin güvenlik platformunu sağlayan Güney Kore merkezli Suprema şirketi nezdinde meydana gelen ihlalle Adecco şirketinde faaliyet gösteren 2000’den fazla çalışanın parmak izi ve yüz tanıma verileri çalınmıştır. Yaşanan ihlal ivedilikle Belçika Veri Koruma Kurumu’na bildirilerek ilgili verilere girişler durdurulmuş ve ihlalin nasıl doğduğu, kimler tarafından gerçekleştirildiğinin tespit edilmek için soruşturma başlatıldığı belirtilmiştir.

4.3. Çin Devletinin Biyometrik Veri Kullanımına Yaklaşımı

Çin Devleti, genel kamu güvenliğinin sağlanması veya kimlik doğrulama amaçlarıyla kişileri birbirinden ayırt etmede etkili olan biyometrik veri ile şifreleme ve ayırtlama yöntemlerini sıklıkla tercih etmektedir. Devletin bu konudaki yaygın kullanımlarının yanı sıra özel sektörde de telefon şifrelemeleri, tuvalet kağıdı hırsızlığın önlenmesi, kişisel avatar (kişiyi simgeleyen resim veya simge) oluşturulması gibi ilginç alanlarda da dahil olmak üzere çeşitli alanlarda biyometrik veriler kullanılmaktadır. Şüphesiz ki Avrupa’nın veri işlemeyi sınırlandıran politikalarının tersine vatandaşlarını gözetleme(*surveillance*) gayesiyle hareket eden Çin Devleti’nin izlediği politikalar özel sektörde biyometrik veri kullanımının artmasında büyük bir etkidir.

Uygulamada genellikle kimlik doğrulama ve güvenlik amacıyla kullanılan biyometrik veriler Çin Devleti’nde vatandaşları üzerindeki otoriter yapıyı arttırmak, onları birbirinden ayırt etmek ve biyometrik verileri ile ayrılan kişileri kolayca tespit etmek için kullanılmaktadır. Hatta Çin Devleti’nde hassas veri işlenmesi daha ileri boyuta taşınarak DNA verilerinin depolandığı ve bu verilerin gözetleme(*surveillance*) programlarında kullanıldığına dair güçlü iddialar

¹⁴ <https://www.bloomberg.com/news/articles/2019-08-21/adecco-says-data-of-belgian-unit-staff-affected-by-suprema-leak>

mevcuttur. Bu verileri yüz tanıma sistemlerinde veya yüz tanıma, sosyal kredi sistemi gibi diğer biyometrik teknolojilerde kullanılacağı belirtilmektedir. Bu kapsamda Amerika Birleşik Devletleri senatosunda Çin Devleti'ne belli alanlarda teknoloji satımının durdurulması dahi önerilmiştir.

Yukarıda Türkiye'de ve Avrupa'da telefon kullanıcılarının kendi takdirlerinde olarak yüz tanıma yöntemi ile telefonlarını şifrelediklerini ve biyometrik verilerini kendi özgür iradeleri ile paylaştıklarını belirtmişim. Türkiye'de ve Avrupa'da kullanıcının kendi iradesine bırakılan yüz tarama ile şifreleme yönteminin aksine Çin Devleti'nde 1.12.2019 tarihi itibarıyla iletişim operatörlerine getirilen yükümlülük neticesinde kullanıcıların yüz tarama kayıtlarını yaptırma zorunluluğu getirilmiştir. Getirilen yükümlülük belirtilen tarihten sonra telefon hattı alan her kullanıcının biyometrik verisi olan yüz tarama kayıtlarını paylaşması anlamına gelmektedir. Türkiye ve Avrupa'nın yaklaşımları dikkate alındığında kullanıcıların iradesine bakılmaksızın devlet gücüyle böyle bir uygulamanın getirilmesi ihlal olarak değerlendirilecekken Çin Devleti'nin bu yöntemi yaygın olarak kullanması ihlal olgusuna da yaklaşımın farklılık gösterdiğini ortaya koymaktadır.

5. TÜRK HUKUKUNDA GÜNCEL DÜZENLEMELERE GETİRİLEN ELEŞTİRİLER VE BİYOMETRİK VERİ İŞLENMESİNDE ÖLÇÜLÜLÜK İLKESİNİN SOMUTLAŞTIRILMASINA DAİR ÖNERİLER

5.1. Türk Hukukunda Biyometrik Verinin İşlenme Şartları

İşbu çalışmanın başında belirtmiş olduğum üzere biyometrik veriler Kişisel Verilerin Korunması Kanunu(daha önce KVKK olarak tanımlanmış metnin devamında "**Kanun**" olarak bahsedilecektir.) kapsamında özel nitelikli veri sınıfında tasniflenerek işlenme şartları Kanunu'nun 6. maddesinde¹⁵ düzenlenmiştir. Bu düzenlemeye göre kişisel veriler kural olarak

¹⁵ "(1)..... (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanın planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

ilgili kişinin açık rızası ile işlenebilmektedir. İstisnai olarak kanunlarda öngörülmesi halinde biyometrik veriler açık rıza olmaksızın işlenebilmektedir. İlgili maddenin 4. fıkrasında ayrıca daha yüksek derecede korumayı gerektiren hassas verilerin işlenmesi sırasında Kişisel Verileri Koruma Kurulu tarafından belirtilecek yeterli önlemlerin alınması gerektiği belirtilmiştir. Biyometrik verilerin ilgili mevzuata uygun olarak işlenmesi için ayrıca işleme fiilinin Kanun'un 4. Maddesine¹⁶ de uygun olması gerekmektedir. Burada çalışmamızın da konusunu oluşturan işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesine uygun olarak biyometrik verinin işlenmesi yükümlülüğü getirilmiştir. Ancak kanaatimce ilgili düzenleme soyut kalmakta ve dolayısıyla birçok tartışmayı da beraberinde doğurmaktadır.

5.2. Türk Hukukunda Biyometrik Verinin İşlenmesi Şartlarına Getirilen Eleştiriler

Her şeyden önce ihlallerin doğuracağı etkileri ile birlikte biyometrik veri kavramına ve kullanım gerekliliğine uluslararası alanda dahi farklı yaklaşımların olduğu göz önüne alınırsa uzmanlık gerektiren bir alan olduğu ortadadır. Güncel düzenlemede biyometrik verinin kişinin salt iradesinden çıkarılarak kanunlarda öngörülmesi halinde açık rızasız işlenebiliyor olması, ve sair kanunların bu alanda uzman kişilerce çıkarılmıyor oluşu birçok hak ihlali doğmasına neden olmaktadır. Uzmanlık gerektiren bu konuda uzman olmayan kişilerce sağlıklı bir ölçülülük değerlendirilmesinin yapılması beklenemez. Bununla birlikte biyometrik verinin kanunlarda öngörülerek işlenmesi ve sair kanunlarda öngörülen düzenlemenin ölçülülük ilkesine uygun olmaması durumunda doğacak aykırılığın nasıl giderilebileceği de henüz hukukumuzda cevaplanmamıştır.

Ölçülülük ilkesinin özünde subjektif bir değerlendirmeyi de barındırıyor olması nedeniyle biyometrik veri işlenmesinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması gerekliliği de ayrıca bir belirsizlik olarak karşımıza çıkmaktadır. Şöyle ki; bir kimlik bilgisinin işlenmesi sırasında baz alınacak ölçülülük kriterleri ile bir biyometrik verinin işlenmesi sırasında baz alınacak ölçülülük kriterlerinin bir olmayacağı açıktır. Kimlik bilgisi işlenirken veri sorumlusunun hakları daha ağır basacakken bir biyometrik veri işlenirken kişilerin hakları daha

¹⁶ MADDE 4- "(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. (2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur: a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işleme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

ön plana çıkacaktır. Bu nedenle yasal düzenlemede ölçülülük kriterinin verinin niteliği göz önüne alınarak daha somutlaştırılmaması düzenlemenin uygulanmasının veri sorumlularınca sübjektif kriterler doğrultusunda farklı yorumlanması bu eksiklikler giderilene kadar birçok ihlalin doğmasına neden olacaktır.

5.3. Biyometrik Veri İşlenmesinde Ölçülülük İlkesinin Somutlaştırılmasına Dair Öneriler

Yukarıda belirtmiş olduğum üzere güncel düzenleme beraberinde birçok soru işaretini meydana getirmektedir. Bu kapsamda öncelikle sair kanunlarda öngörülen hallerin belirlenmesinde Kişisel Verilerin Korunması Kurumu'nun aktif olarak yer alması, bu konuda çalıştayların yapılması önem arz etmektedir. Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'in 7/n maddesinde "diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" görevi Kişisel Verileri Koruma Kurumu'na getirilmiş olsa da Kurum'un yetkisinin güçlendirilerek bu görevi daha etkin icra etmesi sağlanabilir. Ayrıca Kurum'a sağlanacak açık bir görevlendirme ile ölçülülük ilkesine aykırı biyometrik veri işlemeye dair kanun maddelerine karşı Kurum tarafından iptal davası açılabilme hakkı verilebilir.

Biyometrik verinin kimlik doğrulama ve güvenlik alanlarında yaygın olarak kullanıldığı göz önüne alınırsa bu alanlarda ölçülülük kriterinin somutlaştırılması hak ihlallerinin önüne geçilmesi açısından önem arz edecektir. Örneğin çalışanların işe giriş-çıkış takiplerinin yapılabilmesi amacıyla veri sorumlularınca biyometrik veri işlenmesinde ölçülülük kriterinin bireyden yana ağır bastığının değerlendirilmesi yapılarak bu kapsamda veri sorumlusunun işe giriş çıkışların çalışanlarca suiistimal edilmesinden daha haklı bir gerekçesinin olması gerektiği kanaatimdeyim. Nitekim ilgili kişinin açık rızasının varlığı halinde dahi güncel düzenlemede işlemenin hukuka aykırı olacağı açıktır. Veri sorumluları bu uygulamada giriş-çıkışların çalışanların biyometrik verileri işlenmeksizin daha efektif, güvenli ve hızlı bir şekilde yapamayacaklarını düşünmekte, alışa gelmiş sistemi değiştirmeye yönelik düşünsel bir çalışma yapmamalarının nedenini de düzenlemenin somut olmamasıdır. Sübjektif ölçülülük değerlendirmelerinde meşru menfaatlerinin bireylerin biyometrik verisinin işlenmesi açısından haklı bir gerekçe olduğunu kabul ettikleri ve ilgili kişinin açık rızasını alarak biyometrik veri işlemlerinin ölçülülük ilkesine aykırı olmadığı dolayısıyla kanuna aykırı bir uygulama

yürütmediklerini düşünmektedirler. İşveren-işçi arasındaki açık rızanın geçerliliği ise bağımlılık unsuru açısından ayrı bir tartışma konusudur.

Vermiş olduğum örnekteki gibi belirsizliklerin önüne geçebilmek için biyometrik veri işlenmesinde ölçülülük kriterinin konu bazlı olarak sınırlandırılması, ölçülülük ilkesinin somutlaştırılmasını sağlayacaktır. Bu kapsamda kişinin menfaatini ön plana çıkaran uygulamalarda veya veri sorumlusunca korunması gereken üstün bir hakkın olduğu durumlarda ve daha da önemlisi veri güvenliğinin çifte güvence(verinin tutulduğu alana erişimin sınırlı olması ancak erişim denetiminin birden fazla kurum veya kuruluşça yapılması) altına alınması şartıyla biyometrik veri işlenmesi öngörülebilir.

Burada önerilen somutlaştırma Kanun'un sağlık verilerinin işlenmesine ilişkin düzenlediği konu bazlı sınırlandırmadır. Sağlık verilerinin işlenmesine ilişkin düzenleme her ne kadar eleştirilse de biyometrik verinin sağlık verilerinden ayrılan niteliği ve kullanım alanının daha dar olması nedeniyle böyle bir sınırlandırma ölçülülük ilkesinin daha somut değerlendirilmesine katkı sağlayacaktır. Buna ek olarak veri güvenliği için alınacak tedbirlerin özünün de ilgili düzenlemede belirtilmesi sağlıklı olacaktır.

Av. İsmail Mert ŞANLI