www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt:6 Sayı:2

Geliş:4.11.2024
Kabul:20.12.2024

Türkiye'de Biyometrik Veri Güvenliği: Kişisel Verilerin Korunması Kanunu Çerçevesinde Etik Bir Değerlendirme

Melike, ÇİÇEK
Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Doktora Öğrencisi
Hazine ve Maliye Bakanlığı, Gelir Uzmanı.
melkeglmz@hotmail.com
ORCID ID: 0009-0009-0412-2113

ÖZ

Bu çalışma, Türkiye'de biyometrik verilerin korunmasına yönelik yasal düzenlemeler çerçevesinde ortaya çıkan güvenlik ve etik sorunları analiz etmeyi amaçlamaktadır. Biyometrik veriler, kimlik doğrulama ve güvenlik sağlama işlevi nedeniyle önemli bir role sahiptir. Ancak bu veriler, geri dönülemez nitelikte olmaları sebebiyle kişilerin mahremiyetini tehdit eden riskleri de beraberinde getirmektedir. Çalışmada, Kişisel Verilerin Korunması Kanunu'nun (KVKK) biyometrik verilerin güvenliğini sağlama konusundaki yeterliliği ve eksiklikleri ele alınmıştır. Literatür taraması ve nitel analiz yöntemleri kullanılarak KVKK'nın biyometrik veri koruma kapsamı değerlendirilmiş ve veri güvenliği açısından bazı eksiklikler tespit edilmiştir. Bulgular, biyometrik verilerin korunmasında şeffaflık ve bireylerin rızasının alınmasının kritik bir öneme sahip olduğunu ortaya koymaktadır. Bu kapsamda, gelişen dijital tehditlere uyum sağlayabilecek veri koruma politikalarının benimsenmesi ve alternatif teknolojilerin kullanımının teşvik edilmesi önerilmektedir. Ayrıca, Türkiye'de biyometrik veri koruma politikalarının dijital tehditlere uyum sağlaması gerektiği vurgulanmıştır.

Anahtar Kelimeler: *Biyometrik Veri, Etik, Kişisel Verilerin Korunması Kanunu (KVKK), Dijital Kimlik, Yasal Düzenlemeler.*

Biometric Data Security In Türkiye: An Ethical Evaluation Within The Framework Of The Personal Data Protection Law

ABSTRACT

This study aims to analyze the security and ethical issues that arise within the framework of legal regulations regarding the protection of biometric data in Turkey. Biometric data has an important role due to its identity verification and security function. However, these data also bring risks that threaten the privacy of individuals due to their irreversible nature. The study addresses the adequacy and deficiencies of the Personal Data Protection Law (KVKK) in ensuring the security of biometric data. Using literature review and qualitative analysis methods, the scope of KVKK's biometric data protection was evaluated and some deficiencies in terms of data security were identified. The findings reveal that transparency and obtaining individuals' consent are of critical importance in the protection of biometric data. In this context, it is recommended that data protection policies that can adapt to evolving digital threats be adopted and the use of alternative technologies be encouraged. In addition, it was emphasized that biometric data protection policies in Turkey should adapt to digital threats.

Key Words: *Biometric Data, Ethics, Personal Data Protection Law (PDPL), Digital İdentity, Legal Regulations*

Atıf Gösterme Çiçek, M., (2024). Türkiye'de Biyometrik Veri Güvenliği: Kişisel Verilerin Korunması Kanunu Çerçevesinde Etik Bir Değerlendirme, *Kişisel Verileri Koruma Dergisi* 6(2),54-76.

GİRİŞ

Günümüzde bilgi ve iletişim teknolojilerindeki ilerlemeler sayesinde dijital teknolojiler, kimlik doğrulama ve güvenlik alanlarında biyometrik verilerin kullanımını giderek yaygınlaştırmıştır. Yüz tanıma, parmak izi, retina tarama ve DNA analizi gibi kişiye özgü benzersiz biyometrik özellikleri içeren veriler, kişilerin kimliklerini doğrulamak ve güvenliği sağlamak amacıyla kullanılmaktadır. Ancak biyometrik veriler, içerdiği hassas bilgiler nedeniyle geri dönülemez bir yapıya sahiptir ve bu durum, biyometrik verilerin korunmasını kritik bir konu haline getirmektedir. Türkiye, bu kapsamda 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK) ile yasal bir düzenleme oluşturmuştur. KVKK biyometrik verilerin toplanması ve korunması süreçlerinde uyulması gereken kuralları hüküm altına almıştır.

Biyometrik veriler hızla dijitalleşen dünyada güvenliğin sağlanması ve kimlik doğrulama süreçlerinin verimliliği açısından büyük önem taşımakla birlikte kişisel mahremiyetin korunması konusunda ciddi riskler de barındırmaktadır. Kişilerin retina ve parmak izi gibi geri döndürülemez özelliklerine dayanan bu veriler yalnızca güvenlik alanında değil etik boyutuyla da endişelere yol açmaktadır. Bu çalışmada biyometrik verilerin Türkiye'de korunması hususunda KVKK'nın sunduğu yasal çerçeve bağlamında ortaya çıkan etik sorunlar ele alınmıştır. Özellikle biyometrik verilerin toplanması sırasında karşılaşılan etik sorunlar çalışmanın odak noktasını oluşturmaktadır. Ayrıca Türkiye'de biyometrik verilerin korunması aşamasında karşılaşılan zorluklar ve bu verilerin gelecekte daha güvenli bir şekilde yönetilmesine ilişkin çözüm önerileri de değerlendirilmektedir. Bu bağlamda çalışma Türkiye'de biyometrik veri güvenliğinin mevcut durumu hakkında bir değerlendirme sunarken KVKK'nın bu alandaki etkisini ve geliştirilmesi gereken yönlerini de ele almayı amaçlamaktadır. Böylece biyometrik veri güvenliği kapsamında etik sorunların giderilmesine katkı sağlayabilecek bir bakış açısı sunulması hedeflenmektedir.

Çalışmanın gerekçesi Türkiye'de biyometrik veri güvenliğinin mevcut yasal düzenlemeler çerçevesinde koruma sağlayıp sağlamadığını incelemek ve bu düzenlemelerin bireylerin mahremiyet haklarını koruma konusundaki etkinliğini değerlendirmektir. Çalışma biyometrik verilerin kullanımı sırasında karşılaşılabilecek etik sorunları ve bu sorunların çözümüne yönelik önerileri kapsamlı bir şekilde ele almayı amaçlamaktadır. Bu konu hem dijital alanda güvenliğin sağlanması hem de kişilerin temel haklarının korunması açısından kritik bir önem taşımaktadır. Bu kapsamda dijital teknolojilerin hızla gelişmesiyle birlikte biyometrik veri kullanımı yaygınlaşırken bu alandaki yasal ve etik düzenlemelerin de gelişen teknolojilere uyum sağlayarak geliştirilmesi gerekmektedir. Çalışma kapsamında KVKK'nın biyometrik veri güvenliği için yeterli olup olmadığı biyometrik veri kullanımında karşılaşılan etik sorunlar ve Türkiye'de biyometrik veri güvenliğini artırmaya yönelik hangi çalışmaların yapılabileceği sorularına yanıt aranmaktadır. Çalışmanın biyometrik verilerin güvenli ve etik kullanımına katkı sağlayacak öneriler sunması ve bu alandaki gelecekteki düzenlemelere yol göstermesi amaçlanmaktadır.

Çalışmada Türkiye'de biyometrik veri güvenliği KVKK çerçevesinde ele alınırken etik ve yasal boyutları değerlendirmek amacıyla kapsamlı bir literatür taraması ve nitel araştırma yöntemleri benimsenmiştir. Çalışmanın sınırlılıkları ise biyometrik veri güvenliğinin pratikteki uygulamalarına dair sınırlı erişim bulunmasından kaynaklanmaktadır. Çalışma mevcut yasa metinleri ve literatür incelemelerine dayanmaktadır; saha verisi ya da kurum içi uygulamalara yer verilmemiştir. Öte yandan biyometrik veri teknolojilerinde yaşanan hızlı gelişmeler nedeniyle mevcut yasal düzenlemelerin gelecekte ne ölçüde yeterli kalacağı belirsizdir ve bu durum çalışmanın kapsamını daraltmaktadır. Çalışmanın sonuçları gelecekte bu alanda yapılacak daha kapsamlı ve ampirik çalışmalara ihtiyaç duyulacağını göstermektedir.

1. BİYOMETRİK VERİLERİN TANIMI VE KAVRAMSAL ÇERÇEVESİ

Kimlik bir kişiyi tanımlayan biyolojik ve karakteristik özellikler ile davranış biçimleri olarak ifade edilebilir. Kimlik sosyal bilimlerde kişilerin kendilerini ve çevrelerini algılama süreçleri olarak

tanımlanmaktadır (Kavut, 2020, s.989). Tarihsel süreç içerisinde teknolojide yaşanan gelişmeler ve günümüzde gelinen aşamada dijitalleşme sayesinde dijital kimlikler gündeme gelmiştir. Dijital kimlikler online alanda yapılan her işlemi kapsamaktadır. Bu itibarla dijital kimlik öznenin dijital olma hali olup dış alanda açıklanmak üzere bilgisayar sistemleri tarafından kullanılan kişi ile ilgili özelliklerdir (Kavut, 2020, s.991). Dünya Ekonomik Formuna göre dijital kimlik etik olarak da ele alınması gereken bir husustur (World Economic Forum, 2018).

Genel olarak değerlendirildiğinde elektronik bir kimlik olan dijital kimlikler biyometrik veri, dijital imza ve kimlik doğruluma sistemleri olarak açıklanabilir. Bu sistemler sayesinde her türlü işlemde kişisel verilerin güvenli bir şekilde yönetilmesi amaçlanmaktadır. Kişisel veri belirli ya da belirlenebilir nitelikteki bir kişiye ait olan her türlü bilgi olarak tanımlanmaktadır. Bu kapsamda kişisel veriden söz edebilmek için verinin kişiye ait olması ve belirli ya da belirlenebilir olması da gerekmektedir (Küzeci, 2010, s.9). Dijital kimlik sistemlerinin temel bileşenleri kimlik bilgileri; Kimlik doğruluma sistemleri, kimlik yönetim sistemleri, güvenlik protokolleri ve şifreleme, yasal ve düzenleyici mekanizmalardır (World Bank, 2021). Kimlik bilgileri; Kişinin adı, doğum tarihi ve doğum yeri gibi kişinin kendine özgü özelliklerini oluşturmakta olup bu bilgiler kişinin dijital kimlik oluşturma aşamasındaki ilk aşamadır. Kimlik doğruluma mekanizmaları; parmak izi, yüz tanıma, iris tanıma gibi biyometrik verilerin kullanıldığı iki faktörlü kimlik doğrulama yöntemleridir. Kimlik yönetim sistemleri ise dijital kimliklerin oluşturulması, saklanması ve kullanılması süreçlerini ifade etmektedir. Güvenlik protokolleri ve şifreleme, dijital kimlik sistemlerinin güvenliğini sağlamak adına kullanılan şifreleme tekniklerini ve güvenlik protokollerini içermektedir. Yasal ve düzenleyici mekanizmalar ise dijital kimliklerin kullanımı, veri koruma ve güvenlik ile ilgili düzenlemeleri ifade etmektedir (World Bank, 2021).

Grekçe'de yaşam anlamına gelen bios ve ölçü anlamına gelen metron kelimesini temel alan biyometrik veriler; biyolojik ve davranışsal özellikleri içeren kişiye özel, genelde ömür boyu aynı kalan güvenilirlik düzeyi yüksek veri bütünlüğü olarak ifade edilebilir (Bulut, 2020, s.114). Biyometrik veriler kimlik doğrulama aşamasında üç şekilde uygulanmaktadır. Birincisi kullanıcının belirlediği ve sadece kendisinin bildiği şifrelerdir. Ancak şifrelerin deşifre olması durumu söz konusu olmaktadır. İkinci kimlik doğrulama yöntemi dijital kart vb. ögelerin kullanılmasıdır. Ancak bu yöntemde de kartların veya kullanılan ögelerin çalınması, kopyalanması söz konusu olmaktadır. Üçüncü yöntem ise kullanıcının kendisine ait biyometrik verileridir (Erdinç,2020, s.3).

Biyometrik veriler, kişilerin fiziksel ve davranışsal özelliklerine göre tanımlama ve kimlik doğrulama amacıyla kullanılan öznel verilerdir. Biyometrik veriler; parmak izi, yüz tanıma, retina ve iris taraması, ses tanıma gibi özellikleri de kapsamaktadır. Bu verilerin geri alınamaz ve benzersiz olması onları diğer kişisel verilerden ayıran en temel özelliklerden biridir. Örneğin, şifre veya kimlik numarası gibi bilgiler değiştirilebilirken biyometrik veriler değiştirilemez niteliktedir. Bu nedenle biyometrik verilerin kötüye kullanılması durumunda ilgili kişiler için ciddi güvenlik ve mahremiyet sorunları ortaya çıkabilir (Khine, Mi, Shihad,2021, s. 6730). Bu itibarla kimlik doğrulama ve tanımlama sırasında daha güvenilir yöntemlere ihtiyaç duyması ile biyometrik veriler ortaya çıkmıştır. Bu veriler, kişinin benzersiz olan biyolojik ve davranışsal özelliklerini kapsamaktadır. Bu doğrultuda biyometrik veriler kişinin kimlik doğrulamasında güvenlik amacıyla kullanılan verilerdir (Jain, Flynn, Ross, 2011).

Tarihe bakıldığında biyometrik verilerin kullanımı oldukça eski dönemlere dayanmaktadır. Örneğin, M.Ö. 500'lü yıllarda Babil'de kil tabletlerde parmak izi kullanıldığı bilinmektedir. Modern dönemde ise 19. yüzyılda Sir William Herschel kişilerin kimlik doğrulamasında parmak izinden yararlanan ilk kişi olmuştur. Biyometrik kimlik doğrulamanın ilk belgelenmiş örneğini bu oluşturmaktadır (Berry, Stoney,2001, s.25-26). 20.yüzyıl başlarına gelindiğinde Fransız polis Alphonse Bertillon suçluların kimliklerini belirlemek amacıyla vücut ölçümlerini içeren bir sistem geliştirmiştir. 'Bertillonage' adı verilen bu sistem ile biyometrik veri suçluları belirlemek için kullanılmaya başlanmıştır (Jain, Ross, Prabhakar, 2004, s.4).

Biyometrik veri kullanımının dijitalleşmesi ve yaygınlaşması genel olarak 20. yüzyılın ikinci yarısından itibaren bilgi ve iletişim teknolojilerinde yaşanan gelişmelere bağlı olarak gelişme göstermiştir. 1960'lardan itibaren Amerikan İstihbarat Birimlerinden biri olan FBI parmak izi tanıma sistemlerini otomatik hale getirerek, 1970'li yıllarda otomatik parmak izi tanıma sistem olan AFIS'i oluşturmuştur (Prabhakar, Pankati, Jain, 2003, s.40). 1980'li ve 1990'lı yıllar boyunca da yüz tanıma, iris tanıma, ses tanıma ve DNA analizi gibi birçok biyometrik veriye ilişkin gelişmeler yaşanmıştır.

Biyometrik veri türleri fizyolojik biyometrik veriler ve davranışsal biyometrik veriler olarak iki ana kategoriye ayrılmaktadır. Fizyolojik biyometrik veriler, bireyin fiziksel yapısına dayanan ve genellikle yaşam boyu değişmeyen özelliklerinden oluşmaktadır. Bu veriler şunlardır. (Jain ve ark.,2004,s.4;Erdinç,2021,s.3;Özer Deniz,Özer,2022,s.94; Yalçın,Yıldırım,2023,s.184-191):

- Parmak İzi: Her kişinin parmak izleri benzersizdir ve kimlik doğrulamada en çok kullanılan biyometrik veridir.

- Yüz Tanıma: Yüzün geometrik yapısı, uzaklık ve oranlar gibi özellikler analiz edilerek kimlik tespiti yapılmaktadır.

- İris ve Retina Taraması: Gözün iris ve retina yapıları, karmaşık ve benzersiz desenlere sahip olduğundan güvenilir biyometrik veriler olarak kullanılmaktadır.

- El ve Avuç İçi Geometrisi: Elin ve avuç içinin şekli, boyutu ve damar yapısı gibi özellikler kullanılarak kimlik doğrulama yapılmaktadır.

-Kulak Yapısı: Kulakların şekli ve yapısı, kişiye özgü özellikler içerir ve kimlik tespitinde kullanılabilmektedir.

Davranışsal biyometrik veriler ise kişilerin belirli bir görevi yerine getirirken sergilediği davranışsal özelliklere dayanır. Bu veriler, zamanla değişebilse de genellikle kişiye özgü kalıplar içermektedir. Başlıca davranışsal biyometrik veri türleri ise şunlardır (Gümüş, Ata, Balık, 2018, s.349-359; Yalçın, Yıldırım, 2023, s.184-191):

- Ses Tanıma: Kişinin ses tonu, frekansı ve konuşma tarzı analiz edilerek kimlik doğrulama yapılmaktadır.

- İmza Hareketleri: İmza atma sırasında uygulanan basınç, hız ve yön gibi dinamik özellikler değerlendirilmektedir.

- Klavye Vuruş Hareketleri: Klavye kullanırken tuşlara basma süresi ve aralıkları gibi özellikler analiz edilmektedir.

-Yürüyüş Analizi: Kişinin yürüme şekli, adım uzunluğu ve ritmi gibi özellikler incelenmektedir.

Biyometrik veriler bireylerin kimliklerinin doğrulanması ve izlenmesi bağlamında çeşitli teknolojik yöntemlerle farklı sektörlerde etkili biçimde uygulanmaktadır. Biyometrik veriler havaalanları, fabrikalar, okul kampüsleri, hastaneler, yurtlar gibi birçok yerde kullanılmaya başlanmıştır (Akçay, Çetinkaya,2011,385). Parmak izi, avuç içi, el geometrisi ve el damar örüntüleri gibi fiziksel biyometrik özellikler; sınır kontrolü, suçlu tanıma ve kimlik kartları gibi uygulamalarda sıkça kullanılmaktadır. Özellikle parmak izi teknolojisi, adli bilişimde suçluların kimliklerinin tespiti ve olay yeri analizlerinde büyük önem taşımaktadır. Yüz tanıma teknolojisi, pasaport doğrulama süreçlerinden kayıp çocukların tanınmasına kadar geniş bir kullanım alanına sahiptir. İris, retina ve göz akı gibi gözle ilgili biyometrik unsurlar, erişim kontrolü ve bilgisayar oturum açma işlemleri gibi güvenlik odaklı uygulamalarda yaygın şekilde kullanılmaktadır. Ayrıca ses tanıma ve tuşa basma

örüntüleri, özellikle e-ticaret ve akıllı telefonlarda kimlik doğrulama için kritik bir araç haline gelmiştir. Erişim kontrolü ve görüntülenme sistemlerinde biyometrik veriler, kalabalık izleme ve suçlu takibi gibi alanlarda güvenliği artırırken video izleme ve biyometrik tabanlı e-banka hizmetleri, bireylerin finansal güvenliklerini sağlamada kritik bir rol oynamaktadır (Yalçın, Yıldırım, 2023, s.183).

Genel olarak biyometrik veri sistemleri basit olarak şu şekilde çalışmaktadır: Sistem ilk olarak kişinin biyometrik özelliğini algılayarak dijital bir şablon oluşturmaktadır. Oluşturulan bu şablon veri tabanında muhafaza edilmektedir. Daha sonra kimlik doğrulama sırasında alınan yeni biyometrik veri, kayıtlı şablonla karşılaştırılmakta ve eşleşme sağlanırsa kimlik doğrulama başarılı kabul edilmektedir. Bu yöntem, özellikle mobil cihazlarda uzaktan erişim, kişisel veri gizliliği ve erişim güvenliğini artırmak amacıyla kullanılmaktadır (Arslan, Sağıroğlu, 2016, s.102). Öte yandan biyometrik yöntemler kullanım amaçlarına göre şu üç temel şekilde de uygulanmaktadır. Birinci yöntem, bire-çok (1:N) karşılaştırma olarak bilinmektedir ve genellikle tanıma (identification) ya da algılama (recognition) amacıyla kullanılmaktadır. Bu yöntemde, sisteme giriş yapmaya çalışan kullanıcının bilgileri, sistemde daha önce kayıtlı olan tüm kullanıcı bilgileriyle karşılaştırılır ve eşleşme sağlanması durumunda giriş onayı verilmektedir. İkinci yöntem, bire-bir (1:1) karşılaştırmadır ve doğrulama (verification) işlemi için kullanılmaktadır. Bu yöntemde, kullanıcının sisteme sunduğu biyometrik veriye ek olarak, kimlik numarası gibi ikinci bir veri daha alınmaktadır. Bu veri, sistemde kayıtlı bilgilerle eşleştirilmekte ve sadece eşleşme sağlanırsa giriş onayı verilmektedir. Bire-çok yönteminin dezavantajı, büyük veri tabanlarında kıyaslama yapılacak kayıt sayısının artmasıyla sistemin yavaşlatılmasıdır. Buna karşılık bire-bir yöntemde, ikinci verinin unutulması veya kaybedilmesi gibi riskler bulunmaktadır. Üçüncü yöntem ise sınıflandırma (classification) yöntemidir ve büyük veri tabanlarındaki biyometrik verilerin benzer özelliklerine göre gruplandırılmasını sağlamaktadır. (Yalçın,Gürbüz,2015,s.401;Jain ve ark.,2004, s.4-5; Gelb,Clark,2013,s.8-9).Yüz tanıma teknolojisi, kimlik doğrulama yöntemleri arasında en yaygın kullanılanlardan biridir. Bu teknoloji yüzün temel özelliklerini analiz eden 'yüz ölçümü' ve 'öz yüz (eigenface)' yöntemleriyle analiz yapmaktadır. Yüz ölçümünde, gözler arası mesafe veya burun ağız mesafesi gibi fiziksel ölçümler kaydedilirken öz yüz yöntemi yüzün aydınlatma farklılıklarıyla oluşturulan desenlere dayanmaktadır.

Biyometrik veri sistemleri fiziksel temas gerektirmeden bireylerin hızlı ve gizli bir şekilde doğrulanmasını sağlarken özellikle hükümet, ticaret ve güvenlik sektörlerinde geniş kullanım alanı bulunmaktadır. Devlet ve ceza sektöründe, suçluları tespit etme, kayıp çocukları bulma ve aşırılık yanlılarını izleme gibi gözetim uygulamalarında kullanılmaktadır. Ticari sektörde, müşteri profilleme ve ödeme güvenliğini artırma amacıyla tercih edilmektedir. Güvenlik sektöründe ise sınır kontrol noktalarından mobil cihazların kilidini açmaya kadar birçok alanda kimlik doğrulama süreçlerini daha güvenilir ve verimli hale getirmektedir. Bu teknolojiler, hız ve doğruluk sağlarken, insan kaynaklı hataları ve ön yargıları azaltarak güvenlik standartlarını yükseltmektedir (Galterio, Shavit, Hayajneh, 2018,3-4).Bu kapsamda Tablo 1 de çeşitli biyometrik verilere yönelik kullanılabilirlik elverişliliğine yönelik karşılaştırmalı bir değerlendirme sunulmuştur.

Tablo 1

Çeşitli Biyometrik Verilerin Karşılaştırılması

Biyometrik Veriler	Parmak İzi	Yüz	El Geometrisi	İris	Ses
Evrenselliğe Yönelik Engeller	Aşınmış izler; el veya parmak engeli	Yok	El engeli	Görme engeli	Konuşma engeli

Ayırt Edicilik	Yüksek	Düşük	Orta	Yüksek	Düşük
Kalıcılık	Yüksek	Orta	Orta	Yüksek	Düşük
Toplanabilirlik	Orta	Yüksek	Yüksek	Orta	Orta
Performans	Yüksek	Düşük	Orta	Yüksek	Düşük
Kabul Edilebilirlik	Orta	Yüksek	Orta	Düşük	Yüksek
Dolandırıcılığa Karşı Potansiyel	Düşük	Yüksek	Orta	Düşük	Yüksek

Kaynak: (Prabhakar ve ark.,2003, s.36)

Tablo 1'den anlaşılacağı gibi biyometrik verilerin farklı yönleri kapsamında yapılan değerlendirmede her bir verinin güçlü ve zayıf yönleri ele alınmıştır. Parmak izi biyometrisi yüksek ayırt edici ve kalıcılık ile ön planda iken el veya ayak engeli gibi evrenselliğe karşı engellerle karşı karşıya kalabilir. Yüz biyometrisi toplama kolaylığı ile kabul edilebilirlik açısından yüksek performans içermesine rağmen ayırt edilebilirlik açısından orta düzeydedir. El geometrisi hem toplanabilirlik hem de kabul edilebilirlik açısından orta düzey performansa sahipken el engeli gibi evrenselliğe karşı engellerle karşılaşabilir. İris biyometrisi yüksek ayırt edicilik, kalıcılık, performans ile öne çıkarken görme engeli gibi evrenselliğe karşı engellerle karşılaşabilir. Ses biyometrisi yüksek ayırt edicilik ve toplama kolaylığı sunmasına karşın düşük ayırt edicilik, kalıcılık ile performans göstermekle birlikte konuşma engeli gibi evrenselliğe karşı engellerle karşı karşıya kalabilir. Dolandırıcılığa karşı potansiyel ise parmak izi ve iris biyometrisinde düşükken, yüz ve ses biyometrisinde yüksek bir oran sunmaktadır. Bu değerlendirme biyometrik verilerin seçiminde kullanım amacına göre farklı ögelerin dikkate alınması gerektiğini ortaya koymaktadır.

Biyometrik kimlik doğrulama sistemlerinin performansı genellikle FAR (False Acceptance Rate) ve FRR (False Rejection Rate) gibi ölçütlerle değerlendirilmektedir. FAR, yetkisiz bir kişinin yanlışlıkla sistem tarafından yetkili olarak tanınma oranını ifade ederken FRR, yetkili bir kullanıcının hatalı bir şekilde reddedilme oranını belirtmektedir. Bu iki öge arasındaki denge, çoğu biyometrik sistemin etkinliğini belirlemekte ve en ideal performans, FAR ve FRR oranlarının kesiştiği noktada elde edilmektedir. FAR oranını düşürmek, sistemin saklanan örüntüyle daha az benzer olan girişleri eşleştirmesini sağlayarak hatalı kabul durumlarını azaltmayı hedeflemektedir. Ancak biyometrik verilerin doğası gereği bazı bireylerin verilerinin birbirine benzeyebileceği düşünüldüğünde, bu hassas ayarlamalar mahremiyet riski potansiyelini de taşımaktadır. Bu nedenle biyometrik sistemlerde güvenilirlik ile mahremiyet arasında ince bir denge kurulması gereklidir (Paşaoğlu, Adje, Demirtaş, 2019, s.38).

Biyometrik güvenlik sistemleri, kullanıcıların benzersiz fiziksel veya davranışsal özellikleri kullanılarak kimlik doğrulama sağlamaktadır ancak bu sistemlerin bazı zayıf noktaları da bulunmaktadır. Örneğin, parmak izi tanıma sistemleri, parmak üzerindeki kesikler, kir veya nem gibi çevresel faktörlerden etkilenerek doğruluk oranını düşürebilmektedir. Aynı şekilde yüz tanıma sistemleri, aydınlatma koşulları, yüz ifadeleri veya yaşlanma gibi değişkenlerden olumsuz

etkilenebilmektedir. Öte yandan biyometrik verilerin saklanması ve iletilmesi sırasında güvenlik açıkları da oluşabilmektedir. Bu verilerin ele geçirilmesi durumunda kullanıcıların kimlik bilgilerinin kötüye kullanılması riski ortaya çıkmaktadır (Alkan, 2020, s .146).

Biyometrik güvenlik sistemlerinin zayıf noktaları genel olarak sistem tasarımı, veri depolama, doğrulama süreçleri ve veri gizliliği ile alakalıdır. Örneğin, biyometrik veriler ele geçirildiğinde bu verilerin değiştirilmesi veya geri alınması mümkün değildir çünkü parmak izi veya iris gibi veriler kişiye özgüdür ve yenilenemez. Sistemlerde kullanılan veritabanlarının güvenliği kritik öneme sahiptir zira bir saldırgan bu veritabanına erişim sağladığında kimlik sahtekarlığı yapma olasılığı artmaktadır. Öte yandan biyometrik cihazlar sahte parmak izleri veya maskeler gibi fiziksel saldırılara karşı savunmasız olabilmektedir. Bazı cihazlar çevresel faktörlerden (örneğin, nem veya ışık) etkilenerek doğru sonuçlar veremeyebilir. Sistemlerdeki algoritmaların doğruluk oranı düşük olduğunda yanlış eşleşme veya sahte kabul oranları ciddi sonuçlara yol açabilme potansiyeline sahiptir. Biyometrik verilerin gizliliği ve bu verilerin nasıl kullanıldığı konusunda etik ve yasal sorunlar da önemli bir zayıflık olarak öne çıkmaktadır. Bu nedenle biyometrik sistemlerin tasarımında ve uygulanmasında bu zayıf noktaların dikkate alınması ve gerekli önlemlerin alınması büyük önem taşımaktadır.

2.BİYOMETRİK VERİ KULLANIMININ ETİK SORUNLARI

Etik, kişilerin davranışlarını ahlaki bakış açıları kapsamında değerlendirip neyin doğru, neyin yanlış olduğunu belirlemeye çalışan bir felsefe disiplinidir. Bu itibarla etik kavramı insan ilişkilerini etkileyen değerleri, ahlaki bakımdan iyi ya da kötü olduğunu doğru ya da yanlış davranışların niteliğini ve temelini araştıran, özetle insan davranışlarını ahlaki açıdan değerlendiren bir felsefe disiplinidir Etik aynı zamanda belirli bir meslek, iş kolu ya da sanat dalında uyulması gereken profesyonel ilkeler, standartlar ve kuralları da ifade etmektedir. Dolayısıyla her meslek, iş kolu ve sanat dalında etik ilke ve kuralların varlığından bahsedilebilmektedir (Esmer, Özdaşlı, 2023, s.398).

Etik kavramı günümüzde sıkça ahlak kavramı ile karıştırılan bir kavramdır. TDK etik kelimesini "*çeşitli meslek kolları arasında tarafların uyması veya kaçınması gereken davranışlar bütünü*" şeklinde tanımlarken ahlak kelimesini "*bir toplum içinde kişilerin uymak zorunda oldukları davranış biçimleri ve kuralları*" şeklinde tanımlamıştır. Bu iki kavram yakın olarak algılanabilir ancak etik kavramı, sonuçları başka insanları etkileyebilecek eylemler ve bu eylemlere ilişkin düşüncelerle ilgilenirken; ahlak kavramı, toplum içerisindeki bir dizi kurallar kümesi olarak tanımlanmaktadır (Uğurlu, 2020, s.69).

Etik, kişilerin eylemlerini yönlendiren temel değerler ve ilkeler bütünü olarak çağımızın hızla gelişen teknolojik ilerlemeleri karşısında yeniden yorumlanmaktadır. Bu nedenle biyometrik veriler gibi hassas ve bireysel özelliklere dayanan teknolojiler için etik sorumluluk ile haklar arasındaki dengenin dikkatlice değerlendirilmesi gerekmektedir. Etik çerçevesinde bireyin mahremiyeti ve güvenliği gibi kavramlar, biyometrik verilerin kullanımıyla ilgili tartışmaların temelini oluşturmaktadır. Bu kapsamda biyometrik veri kullanımında etik sorunların nasıl şekillendiğini daha ayrıntılı olarak ele almak gerekmektedir.

Biyometrik verilerin kullanımı yaygınlaşmakla birlikte bu verilerin kötüye kullanım riski de her geçen gün artmaktadır. Biyometrik veriler kişilere ait hassas bilgileri içermektedir. Bu kapsamda verilerin toplanması ve güvenli bir şekilde saklanması önemli bir mahremiyet ve güvenlik endişesini de gündeme getirmektedir. Yüz tanıma sistemleri, büyük şehirlerde güvenlik amacıyla kullanılmakta iken parmak izi ve iris taraması gibi biyometrik doğrulama yöntemleri sağlık sektöründe hasta bilgilerinin korunmasında önemli rol oynamaktadır. Öte yandan bu verilerin merkezi veri tabanlarında saklanması, olası veri ihlalleri ile saldırılar sonucunda kişilerin kimliklerinin tehlikeye atılmasına yol açabilme potansiyeline sahiptir. Bu itibarla biyometrik verilerin ele geçirilmesi durumunda, kişilerin kimliklerinin geri döndürülemez bir şekilde ifşa olma riski ortaya çıkmaktadır (Vujković, Ravšelj, Umek, Aristovnik, 2022, s. 293).Öte yandan biyometrik verilerin korunması ve bu verilerin etik sınırlar içinde kullanılması durumunda ortaya çıkabilecek sorunlar da bulunmaktadır. Biyometrik

verilerin olağan olarak sürekli izlenme ve takip etme uygulamaları ile ilişkili olma hali mahremiyet ihlalleri ile sonuçlanabilir potansiyelleri ortaya çıkarmaktadır. Biyometrik verilerin kötü kullanımı ya da yetkisiz erişimlere maruz kalması ciddi sonuçları da beraberinde getirebilmektedir. Öte yandan biyometrik verilerin toplanması ve işlenmesi sırasında ilgili kişilerin rızasının da alınması durumu verilerin korunması anlamında kritik öneme sahiptir. Çünkü biyometrik verilerin izinsiz kullanımı bireylerin mahremiyet hakları kapsamında ciddi ihlalleri yaratabilme potansiyeline sahiptir (NIST,2020). Bu itibarla kişilerin fiziksel ve davranışsal özellik bilgisini içeren verilerin toplanması, saklanması ve kullanılması birçok mahremiyet ve güvenlik sorununa yol açmaktadır.

Bu sorunlardan en önemlisi veri ihlalleri ve kimlik hırsızlığıdır. Biyometrik veriler, kişilerin kimlik doğrulaması ve güvenlik amaçlı kullanıldığından bu verilere yetkisiz kişilerce ulaşılması, verilerin geri alınamaz şekilde kaybedilmesine ve sahte kimlik oluşturması gibi ciddi güvenlik sorunlarına yol açmaktadır (Gelb ve ark., 2013, s.15). Biyometrik verilere yönelik bir diğer önemli sorun özellikle yüz tanıma teknolojilerinin izinsiz kullanımının kişilerin sürekli izlenmesi ve gözetlenmesi riskini ortaya çıkarmasıdır. Bu durum da kişilerin mahremiyet haklarını ihlal edip onların özgürlüklerini kısıtlamaktadır (European Digital Rights, 2020). Biyometrik verilerin toplanmasına yönelik bireylerin bilgilendirilmiş onay verme durumunda da bazı sorunlar ortaya çıkabilmektedir. Bireyler hangi verilerinin toplandığı, ne için kullanılacağı ve bu bilgilerin kimler ile paylaşılacağı konularında yeterince bilgilendirilmemesi durumlarında kendilerine karşı mahremiyet ihlalleri oluşturabilmektedir (World Bank,2018). Bu husus da bazı güvenlik sorunlarına neden olmaktadır. Biyometrik verilere yönelik yetkisiz erişime maruz kalan bilgiler sonucunda ilgili kişilerin yaşamsal haklarına varabilecek bazı ciddi sorunlar oluşabilmektedir (NIST,2020). Ayrıca biyometrik veri sistemleri, sosyal adaletsizliklere de neden olabilmektedir. Örneğin, bazı biyometrik özellikler bazı etnik gruplar veya yaş gruplarında daha az belirgin olup onların dışlanmalarına da neden olabilme potansiyeline sahiptir (Pereira, 2021, s. 2566; İlter Güven, 2023, s.12-13). Öte yandan biyometrik verilerin yanlış kullanımı da kişilerin mahremiyet haklarına yönelik ciddi tehdit oluşturmaktadır (Jain ve ark.,2004, s.13).

Biyometrik veriler, kişilere özgü ve genellikle değiştirilemez özellikleri içerdiğinden, yanlış kullanıldığında ciddi etik ihlallere neden olabilir. Parmak izi, yüz tanıma, retina ve iris taraması, ses tanıma, yürüyüş analizi, DNA verileri gibi biyometrik veriler bu ihlallerin başlıca kaynaklarıdır. Örneğin, parmak izi verilerinin yetkisiz paylaşımı, sahte parmak izleriyle sistemlerin kandırılması veya işverenlerin çalışanlarını izlemek için bu verileri zorunlu tutması, ciddi mahremiyet ihlallerine sebep olabilir (Özer Deniz,Özer,2022,s.99).Benzer şekilde yüz tanıma teknolojisinin kitlesel gözetim amacıyla kullanılması, algoritmik önyargılar nedeniyle ayrımcılık yapılması veya kişinin bilgisi dışında yüz tanıma verilerinin toplanması, etik açıdan tartışmalıdır (İlter Güven,2023,s.12-13).Retina ve iris taramaları da hassas biyometrik verilerdir ve bu verilerin kötü niyetli kişiler tarafından taklit edilmesi ya da zorla alınması, kişilerin güvenliğini tehlikeye atabilir. Ses tanıma teknolojisi de derin sahtecilik (deepfake) gibi manipülasyonlarla kötüye kullanılabilir ve bireylerin rızası olmadan iletişimlerinin izlenmesi gibi mahremiyet ihlalleri yaratabilir (Yalçın, Yıldırım, 2023, s.198). Yürüyüş analizi gibi teknolojiler, bireylerin izlenmesini kolaylaştırarak mahremiyeti ortadan kaldırabilir. Ayrıca, DNA verilerinin rıza dışı saklanması, genetik ayrımcılık veya aile bağlarıyla ilgili gizlilik ihlallerine yol açabilir (İlter Güven, 2023, s.12-13). Bu tür ihlallerin önüne geçebilmek için bazı temel ilkelere dikkat edilmesi gerekmektedir. Biyometrik verilerin toplanması öncesinde kişilerden açık ve bilgilendirilmiş onam alınması, yalnızca gerekli verilerin toplanmasını sağlayacak veri minimizasyonu politikalarının benimsenmesi ve verilerin güvenli bir şekilde şifrelenerek depolanması büyük önem taşımaktadır. Ayrıca, verilerin nasıl ve neden toplandığını açıklayan şeffaflık ilkesi ile sıkı yasal düzenlemeler (örneğin, GDPR ve KVKK) bu alanda yaşanabilecek sorunların önüne geçebilme potansiyeline sahiptir. Ancak biyometrik veri kullanımının her zaman bireysel haklara saygılı bir şekilde ve etik ilkeler çerçevesinde yönetilmesi gerektiği unutulmamalıdır.

3. BİYOMETRİK VERİLERE YÖNELİK YASAL DÜZENLEMELER

Her alanda olduğu gibi, dijital kimlikler kamu ve özel sektör uygulamalarında geniş bir kullanım alanına sahiptir. Dijital kimlik sistemleri hem kamu hizmetlerinde hem de özel sektörde bireylerin işlemlerini hızlandırmak, şeffaflığı artırmak ve güven oluşturmak amacıyla kullanılmaktadır (World Bank, 2019). Bu sistemler, hizmet kalitesini yükseltirken bürokratik süreçleri azaltır, maliyetleri düşürür ve aynı zamanda güvenlik ile şeffaflığı sağlar. Dijital kimliklerin kullanımı sayesinde bireyler, çeşitli hizmetlere daha kolay erişim sağlayabilirken kriz durumlarında da hızlı ve etkili müdahaleler mümkün hale gelmektedir (Financial Inclusion Global Initiative, 2021).

Hem kamu hem de özel sektörde kimlik doğrulama süreçlerinde biyometrik verilerin kullanımına sıkça başvurulmaktadır. Bu veriler; e-Devlet, finansal hizmetler, sağlık, eğitim ve sosyal yardım gibi birçok farklı alanda kimlik tanıma amacıyla kullanılmaktadır. Ancak, biyometrik verilerin bu alanlardaki kullanımı çeşitli riskleri de beraberinde getirmektedir. Bu nedenle biyometrik verilerin toplanması ve kullanımı sırasında şeffaflık, hesap verilebilirlik ve adalet ilkelerine uygun hareket edilmesi gerekmektedir. Ayrıca bu verilere yönelik güçlü güvenlik önlemleri ve politikaların uygulanması büyük önem taşımaktadır. Bu bağlamda, küresel ölçekte veri güvenliğini sağlamaya yönelik birçok yasal düzenleme yayımlanmıştır ve bu düzenlemeler, kamu ve özel sektör tarafından dikkate alınmalıdır.

- Avrupa Genel Veri Koruma Tüzüğü (GDPR): Avrupa Birliği'nin 2016 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü, biyometrik verilerin korunması konusunda katı bir düzenlemeyi kapsamaktadır. Tüzük Avrupa Birliği hukukunda tüm Avrupa Birliği ve Avrupa Ekonomik Alanı içerisinde yer alan her kişi için koruma ve güvenlik sağlayan hükümleri içermektedir. GDPR, biyometrik verilerin toplanması ve işlenmesi hakkında ilgili kişilerden açık rıza getirilmesini koşullandırmaktadır. Ayrıca tüzük veri ihlallerine karşı ciddi yaptırımları da hüküm altına almıştır (European Union, 2016).

-Amerika Birleşik Devletleri'nde Uygulanan Kaliforniya Tüketicilerin Kişisel Verilerini Koruma Yasası (CCPA) ABD'nin Kaliforniya eyaletinde yürürlülüktedir. Tüketicilere hangi kişisel verilerin toplandığını bilme ve bu verilere yönelik red hakkı vermektedir (California Legislative Information,2018).

- Amerika Birleşik Devletleri'nde Uygulanan Biyometrik Bilgi Gizliliği Yasası (BIPA), ABD'nin Ilinois Eyaleti'nde uygulanmaktadır. Biyometrik verilerin toplanması, saklanması ve kullanılması hakkında ciddi katı düzenlemeleri içermekle birlikte ihlal durumunda ilgili kişilere dava açma hakkı da tanınmaktadır (BIPA,2008).

-Singapur'da uygulanan kişisel verilerin korunmasına ilişkin kanun (PDPA) ise ülkede vatandaşlara yönelik kişisel verilerin korunmasını düzenleyen yasal düzenlemedir. Kişilere verilerin erişimi ve düzeltme hakkı vermekte olup ihlal durumunda ciddi yaptırımı öngören düzenlemedir (Personal Data Protection Commission Singapore, 2014).

- Ulusal ve Uluslararası Düzenlenmeler: Birçok ülke biyometrik veri koruma konusunda çeşitli düzenlemeleri uygulamaktadır. Her ülke kendi ulusal düzenlemeleri doğrultusunda vatandaşlarına yönelik veri koruma politikalarını içeren yasal düzenlemeleri hüküm altına almıştır. Uluslararası platformda ise biyometrik veri korunmasına ilişkin uluslararası standartlar bulunmaktadır. Bu standartlar biyometrik verilerin güvenli ve etik olarak toplanması ve kullanmasını sağlamaktadır. ISO/IEC 24745 standardı biyometrik veri koruma ile mahremiyet yönetimi için uluslararası alanda kabul görmüş bir standarttır. Söz konusu belgede biyometrik verilerin saklanması ve kullanılması sırasındaki gizlilik için uygun yönetim ve öneriler ele alınmıştır. Bu itibarla belgede; biyometrik sistem uygulama modellerine ilişkin tehditler ve bunlara karşı önlem analizi, biyometrik temel veri ile kimlik doğruluma verisi arasındaki güvenli eşleştirmeye ilişkin uygulamalar, verilerin saklanması ve karşılaştırılmasına yönelik uygulama alternatifler ile biyometrik verilerin kullanılması sırasında kişilerin mahremiyetinin korunmasına ilişkin rehberlik uygulamaları da bulunmaktadır. (ISO,2022).

4. TÜRKİYE'DE BİYOMETRİK VERİLERİN YASAL STATÜSÜ

Türkiye, dijital kimlik ile biyometrik veri kullanımını arttırarak kamu hizmetlerinde verimliliği ve güvenliğini sağlamayı amaçlayan projeleri yaygınlaştırmaktadır. Ülkede 2017 yılından itibaren her Türk vatandaşına verilen ve benzersiz bir kimlik kartı (T.C. kimlik kartı) imkanı veren dijital kimlik sistemi uygulanmaya başlamıştır (Çiçek, 2024, s.275). T.C. kimlik kartları kimlik doğrulama, dijital imza atma ile çeşitli kamu hizmetlerine erişim amacıyla kullanılmaktadır. T.C. kimlik kartları çipli olup biyometrik veriler ile kişisel özelliklere ilişkin bilgileri içermektedir (T.C. İçişleri Bakanlığı,2024). Türkiye'de biyometrik veriler elektronik pasaportlarda kullanılmaktadır.2010 yılından beri tüm pasaportlarda biyometrik veriler yer almaya başlamıştır. Bu itibarla kullanıcıların parmak izi ve yüz tanıma gibi biyometrik verileri pasaportlarda kullanılmaya başlanmıştır. Öte yandan kullanılan dijital kimlik sistemi, vatandaşların devlet hizmetlerine çevrimiçi olarak erişim imkanı tanırken; vergi beyanı, sağlık hizmetleri, sosyal güvenlik işlemleri ve diğer birçok kamu hizmeti ile özel sektör alanlarında hizmet sunmak ve hizmet almak için kullanılmaktadır.

Türkiye'de dijital kimlik ve biyometrik veri kullanımında yüksek standartlara sahip veri koruma kanunlarını uygulamaktadır. 2010 yılındaki anayasa değişikliği ile kişisel verilerin korunması anayasal güvence altına alınmıştır. Öte yandan 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK) ile kişisel verilerin korunması ve kişilerin mahremiyetinin sağlanması için önemli bir düzenleme yapılmıştır (Kişisel Verileri Koruma Kurumu (KVKK) ,2024). Söz konusu kanunun üçüncü maddesinde kişisel veri, kişileri tanımlayan ve belirlenebilir kılan her türlü veri olarak açıklanmış ve kişisel verilerin mahremiyet kavramının bir parçası olmasından dolayı özel hayatın gizliliği açısından önemli olduğu da belirtilmiştir. Kanun kapsamında kişisel veriler özel ve genel olarak iki şekilde sınıflandırılmıştır. Bu kapsamda biyometrik veriler özel nitelikli kişisel veriler olarak tanımlanmıştır. (Alkan, Menteş, İnceefe ,2020, s.23). KVKK'da biyometrik verilerin kesin bir açıklaması yapılmamış olsa da Nüfus Hizmetleri Kanunu'nda biyometrik veri; elektronik sistemler aracılığıyla kimlik tespit etme ve kimlik doğrulama işlemleri için kullanılan parmak izi, damar izi ve el ayasından elde edilen kişiye özel bilgiler olarak tanımlanmıştır (Nüfus ve Vatandaşlık İşlemleri Genel Müdürlüğü,2024).

Kişisel Verileri Koruma Kurumu tarafından yayımlanan '*Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber'*de, biyometrik verilerin işlenmesinde dikkat edilmesi gereken ilkeler aşağıdaki şekilde sıralanmıştır (Kişisel Verileri Koruma Kurumu (KVKK) ,2024):

- Temel hak ve özgürlüklerin özüne dokunulmaması,

- Başvurulan yöntemin işleme amacına ulaşabilmesi açısından elverişli olması, veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması,

- Biyometrik veri işleme yönteminin ulaşılmak istenen amaç açısından gerekli olması,

- Veri işleme ile ulaşılmak istenilen amaç ve aracın arasında orantı olması,

-Gerektiği süre kadar tutulması, gereklilik ortadan kalktıktan sonra söz konusu verilerin derhal imha edilmesi,

- Açık rızanın gerekmesi durumunda ilgili kişilerin açık rızalarının alınması gerekmektedir.

Bahse konu rehberde biyometrik verilerin korunması açısından iki temel husus ön plana çıkmaktadır. Bunlardan birincisi teknik tedbirlerdir. Teknik tedbirler kapsamında biyometrik veriler bulut sistemlerinde ancak güncel teknolojiye uygun kriptografik yöntemler ile orijinal biyometrik özelliğini yeniden elde edilmesine imkan veremeyecek şekilde saklanması gerektiği belirtilmiştir. İdari tedbirler kapsamında ise biyometrik veriyi kullanamayan veya kullanmak istemeyen kişiler için alternatif çözümler geliştirilme şeklinde bir yönlendirme yapılmıştır Ayrıca yetkili kişilerin erişim mekanizması sürekli kontrol edilmeli ve belgelendirilmelidir. Biyometrik veri kullanımından sorumlu

kamu personeli bilgilendirilmeli, güvenlik zafiyetleri ile tehditleri için resmi raporlama prosedürleri düzenlenmelidir. Öte yandan veri ihlali durumlarında uygulanması gereken acil durum prosedürü oluşturulmalı ve tüm ilgililere iletilmelidir (Kişisel Verileri Koruma Kurumu (KVKK) ,2024).

Öte yandan Kişisel Verileri Koruma Kurulu Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ve 22. maddesi uyarınca özel nitelikli kişisel verilerin işlenmesine ilişkin veri sorumlularının alması gereken yeterli önlemleri belirlemek üzere 31 Ocak 2018 tarihinde oy birliği ile 2018/10 sayılı kararı almıştır. Bu karar, özel nitelikli kişisel verilerin korunmasını sağlamak için veri sorumlularının uygulaması gereken teknik ve idari tedbirlerin çerçevesini çizmektedir. Karar doğrultusunda veri sorumlularının özel nitelikli veriler için ayrı bir güvenlik politikası oluşturması, çalışanlara yönelik özel eğitimler düzenlenmesi, gizlilik sözleşmelerinin imzalanması ve erişim yetkilerinin net bir şekilde tanımlanması gibi önlemleri içeren sistematik bir yaklaşım benimsemeleri gerektiği ifade edilmiştir. Ayrıca verilerin güvenliğini sağlamak için fiziksel ve elektronik ortamlarda şifreleme, işlem kayıtlarının loglanması, güvenlik güncellemelerinin takip edilmesi ve uzaktan erişimlerde iki aşamalı kimlik doğrulamanın uygulanması gibi tedbirlerin alınması zorunluluğu vurgulanmıştır. Bu karar, özel nitelikli kişisel verilerin güvenliğini artırmak ve veri sorumlularının yükümlülüklerini netleştirmek adına önemli bir adım olarak değerlendirilmekte ve veri işleme süreçlerinde güvenlik standartlarının yükseltilmesine katkı sağlamaktadır (KVKK 2018/10 K., ,2024).

Kurulun 2022/662 sayılı kararında ise bir işletmenin, müşterilerinin hizmet binasına girişlerinde el geometrisi bilgilerini işlemeye yönelik uygulamasını ele almıştır. Şikayet kapsamında, ilgili kişinin açık rızası olmaksızın el geometrisi bilgisinin kaydedildiği ve kullanıldığı iddia edilmiştir. Veri sorumlusunun savunmasında, el geometrisi bilgilerinin biyometrik veri olmadığını, sadece fiziksel ölçümlerle tanımlandığını ve kimlik doğrulama sürecinin şifre ile desteklendiği belirtilmiştir. Ancak Kurul, el geometrisinin biyometrik veri kapsamında değerlendirilmesi gerektiğine karar vermiştir. Kurulun değerlendirmesinde el geometrisi verisinin, otomatik kimlik doğrulama teknikleriyle işlendiği ve özel nitelikli kişisel veri niteliği taşıdığı tespit edilmiştir. Bu nedenle, veri sorumlusunun, kişisel veri güvenliği yükümlülüklerini ihlal ettiği sonucuna varılmıştır. Kurul, veri sorumlusuna idari para cezası uygulanmasına, biyometrik veri işlemenin durdurulmasına ve mevcut verilerin imha edilmesine karar vermiştir. Ayrıca silme işlemleri ve üçüncü taraflara yönelik bildirim süreçlerinin belgelenerek kurula raporlanması gerektiği vurgulanmıştır. Bu karar, özel nitelikli kişisel veri işlemenin, veri güvenliği ve hukuki dayanaklara bağlı olarak sıkı bir şekilde denetlenmesi gerektiğini bir kez daha ortaya koymuştur (KVKK 2022/662 K., ,2024).

5.KİŞİSEL VERİLERİN KORUNMASI KANUNU (KVKK) İLE AB GENEL VERİ KORUMA TÜZÜĞÜNÜN (GDPR) KARŞILAŞTIRILMASI

Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK) ve AB Genel Veri Koruma Tüzüğü (GDPR) kişilerin verilerine yönelik haklarını koruma amacını temel almaktadır. 2016 yılında kabul edilen Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin korunması konusunda AB'nin en kapsamlı ve güncel düzenlemesidir. GDPR, bilişim teknolojilerinin günümüzdeki kadar gelişmediği bir dönemde yürürlüğe giren 95/46/EC sayılı direktifin yerini almıştır. Söz konusu direktif, AB ülkeleri arasında veri koruma hukukunda beklenen yeknesaklığı sağlayamamış ve bilişim teknolojilerindeki ilerlemelerle uyumlu bir yapıya ihtiyaç duyulmasına yol açmıştır. Bu gereklilik doğrultusunda hazırlanan GDPR, Mayıs 2016'da kabul edilmiştir (Dülger, 2019, s.71). Tüzüğün en dikkat çekici özelliği, Avrupa Birliği'nde kişisel verilerin korunması hukukunu yeknesak bir yapıya kavuşturma çabasıdır. Bu itibarla, GDPR hem tamamen yeni düzenlemeler getirmiş hem de önceki düzenlemeleri daha detaylı ve somut bir şekilde yeniden ele almıştır. Tüzüğün bu ayrıntılı yaklaşımı, AB ülkeleri arasında uyum sağlamayı ve bireylerin veri koruma haklarını daha etkin olarak güvence altına almayı hedeflemektedir.

Kişisel veri işleme eylemlerini yöneten hukuki ilkeler, her işleme faaliyetine temel rehberlik eden önemli bir kurallar bütününü oluşturmaktadır. Bu ilkeler, bireylerin haklarını korumak ve kişisel verilerin sorumlu ve etik şekilde işlenmesi için bir çerçeve sunmak amacıyla hem GDPR hem de

KVKK'da düzenlenmiştir. GDPR ve KVKK'da belirtilen hukuki ilkeler Tablo 2 de kısaca açıklanmıştır.

Tablo 2

GDPR ve KVKK'da Belirtilen Hukuki İlkeler

Hukuki İlke	**Açıklama**	**Dayanak**
Hukuka Uygunluk	İşleme faaliyetleri, en az bir yasal dayanağa sahip olmalıdır.	GDPR Madde 5(1)(a), KVKK Madde 4(2)(a)
Adillik	Bu ilke, ilgili kişinin işleme faaliyetlerinden haberdar olmasını ve bu faaliyetlere dair olumlu beklentilere sahip olmasını içerir. İşlemenin, ilgili kişileri olumsuz etkilediği durumlarda adil olmadığı kabul edilir.	GDPR Madde 5(1)(a), KVKK Madde 4(2)(a)
Şeffaflık	İşleme faaliyetleri, ilgili kişilerin bilgilendirilmesi yoluyla açık ve şeffaf bir şekilde yürütülmelidir.	GDPR Madde 5(1)(a); KVKK'da doğrudan yer almasa da bu ilke otoritenin rehberlerinde ve kararlarında görülmektedir.
Hesap Verebilirlik	Veri sorumluları, GDPR ve KVKK'ya uyum sağladıklarını kanıtlamak ve bu uyumu göstermekle yükümlüdür.	GDPR Madde 5(2); KVKK'da doğrudan yer almasa da otoritenin rehberlerinde ve ikincil düzenlemelerde bu ilkeye vurgu yapılmaktadır.
Amaçla Sınırlılık	Veri sorumluları, işlenen kişisel verileri yalnızca belirlenen meşru amaçlarla kullanmalıdır.	GDPR Madde 5(1)(b), KVKK Madde 4(2)(c)
Veri Minimizasyonu	Veri sorumluları, belirlenen amaç için gerekli olan en az ve ilgili kişisel veriyi işlemelidir.	GDPR Madde 5(1)(c), KVKK Madde 4(2)(ç)
Doğruluk	Veri sorumluları, işlenen kişisel verilerin doğruluğunu ve güncelliğini sağlamakla yükümlüdür.	GDPR Madde 5(1)(d), KVKK Madde 4(2)(f)

Depolama Süresi ile Sınırlılık	Kişisel veriler, yalnızca işleme amaçları için gerekli olan süre boyunca saklanmalıdır.	GDPR Madde 5(1)(e), KVKK Madde 4(2)(d)
Bütünlük ve Gizlilik	Veri sorumluları, kişisel verilerin teknik ve operasyonel olarak güvenliğini ve bütünlüğünü sağlamak için gerekli önlemleri almalıdır.	GDPR Madde 5(1)(f); KVKK'da doğrudan yer almasa da KVKK Madde 12 kapsamındaki yükümlülüklerle bu ilke desteklenmektedir.

Not : (Evren,2023,s.41-42) çalışmasından yararlanılarak geliştirilmiştir.

Tablo 2'den de anlaşılacağı üzere GDPR ve KVKK arasında, sayılan ilkeler açısından genel bir benzerlik bulunsa da bazı ilkeler KVKK'da doğrudan ifade edilmemiştir. Şeffaflık ve hesap verebilirlik ilkeleri, KVKK'da doğrudan hukuki ilkeler başlığı altında yer almasa da çeşitli rehberlerde ve otorite kararlarında bu ilkelere atıflar yapılmaktadır. KVKK'daki şeffaflık ilkesi, adillik ilkesinin bir parçası olarak değerlendirilebilirken hesap verebilirlik ise veri sorumlularının KVKK'ya uyum sağlama yükümlülükleri aracılığıyla uygulamada yer bulmaktadır. Ayrıca GDPR, ilkeleri açıklayıcı bir şekilde ele alırken KVKK, ilkeleri doğrudan liste halinde sunmaktadır. Ancak, KVKK otoritesinin yayımladığı rehberlerde bu ilkeler daha detaylı şekilde ele alınmıştır. Sonuç olarak, GDPR ve KVKK'daki hukuki ilkeler genel anlamda uyumlu bir yapı göstermektedir. GDPR'da yer alan bir ilke, aynı şekilde KVKK'da yorumlanarak uygulanabilir. Bu doğrultuda GDPR, KVKK'ya göre daha kapsamlı ve geniş bir düzenleme içermekte olup KVKK GDPR'yi esas alarak oluşturulmuştur. Öte yandan aşağıda yer alan Tablo 3'te karşılaştırmalı olarak KVKK ve GDPR arasındaki farklar açıklanmıştır.

Tablo 3

KVKK ve GDPR'nin Karşılaştırmalı Analizi

KVKK (Kişisel Verilerin Korunması Kanunu)	**GDPR (General Data Protection Regulation - Genel Veri Koruma Tüzüğü)**
Türkiye'de kişisel verilerin toplanması, saklanması ve paylaşılması aşamalarında ilgili kişilerin haklarını korumaya ilişkindir. (Madde-1) Türkiye sınırları içinde faaliyet gösteren kurum ve kuruluşlar ile veri sorumlularına uygulanmaktadır.	Avrupa Birliği'ne üye ülkelerde geçerli olan, AB vatandaşlarının verilerinin işlenmesi ile ilgilenen her kuruluşu kapsamaktadır. AB dışında olsa bile AB vatandaşlarına hizmet sunan ya da onların verilerini işleyen her kuruluş GDPR kurallarına tabi olmaktadır. (Madde-3)
Verilerin hukuka ve dürüstlük kurallarına uygun olarak toplanması, doğru ve güncel olması, belirli ve meşru amaçlar için işlenmesi gibi ilkelere dayanmaktadır. (Madde-4) Öte yandan ilgili kişilerin açık rızası olmadan kişisel verilerin işlenmesi yasaktır. (Madde-5)	GDPR, veri minimizasyonu, şeffaflık, veri doğruluğu, depolama sınırlamaları gibi daha geniş kapsamlı ilkelere dayanmaktadır. GDPR, veri sahiplerine genişletilmiş haklar sunarak veri sorumlularının daha fazla sorumluluk almasını sağlar. (Madde-5)

Kişisel verilerin toplanması için ilgili kişinin açık rızası zorunludur. Ancak belirli durumlarda (kanunlarda açıkça öngörülmesi, kamu sağlığının korunması vb.) ilgili kişinin rızası olmadan da veri işleme mümkün kılınmaktadır. (Madde-5 ve Madde-6)	GDPR, veri toplamak için altı yasal dayanak sunar: açık rıza, sözleşmenin ifası, yasal yükümlülük, hayati çıkarlar, kamu görevinin yerine getirilmesi ve meşru menfaat. (Madde-6) Bu argümanlar KVKK'dan daha geniş bir çerçeve sunar.
İlgili kişilere, veri toplama faaliyetleri hakkında bilgi edinme, yanlış veya eksik verilerin düzeltilmesini talep etme, verilerin silinmesini isteme gibi haklar tanır.(Madde-7,Madde-10,Madde-11) Ayrıca, ilgili kişinin verilerini kimlerle paylaşıldığını öğrenme hakkı da bulunur.(Madde-10,Madde-11)	GDPR, veri sahiplerine daha geniş haklar tanır. Veri taşınabilirliği, otomatik karar verme ve profil oluşturma süreçlerine karşı çıkma gibi haklara da sahiptir.(Madde-12 ve Madde 23 arası)
Veri sorumlularının kişisel verilerin güvenliğini sağlamak için gerekli teknik ve idari önlemleri alması gerekmektedir. Veri ihlallerini önlemek için kurumların uygun güvenlik önlemleri alması zorunludur.(Madde-12)	GDPR, veri ihlalleri konusunda sıkı düzenlemeler getirir. İhlal durumunda, en geç 72 saat içinde veri koruma otoritesine bildirim zorunluluğu vardır.(Madde-33)
Kanuna aykırı veri işleme faaliyetleri için idari para cezaları öngörülmüştür. Cezalar, veri sorumlularının yükümlülüklerini ihlal etmeleri durumunda uygulanmaktadır ve ceza miktarı ihlalin ciddiyetine göre değişmektedir.(Madde-17,Madde-18)	GDPR, veri ihlallerine yönelik çok daha ağır yaptırımlar öngörmektedir. İhlal durumuna göre, yıllık cironun %4'üne veya 20 milyon avro kadar para cezası uygulanabilir.(Madde-83) GDPR yaptırımları, uluslararası kuruluşlar için caydırıcı niteliktedir.
KVKK kapsamında açıkça belirtilmiş bir "unutulma hakkı" yoktur ancak ilgili kişinin verilerin silinmesini veya yok edilmesini talep etme hakkı vardır.(Madde-7)	GDPR, unutulma hakkını açıkça tanımlar ve veri sahiplerinin, verilerinin silinmesini talep etme hakkını garanti eder. Bu hak, özellikle bireyin verilerinin gereksiz hale geldiği veya veri sahibinin rızasını geri çektiği durumlarda önemlidir.(Madde-17)
KVKK, veri koruma görevlisi atama zorunluluğu getirmez.(KVKK ve ikincil mevzuatı bir veri koruma görevlisi atanmasına ilişkin düzenleme içermemektedir.)	GDPR, kamu kurumları ve büyük ölçekli veri işleyen şirketler için veri koruma görevlisi atama zorunluluğu getirir. Bu görevlinin, veri koruma politikalarının uygulanmasını sağlamak ve veri güvenliğiyle ilgili denetimlerde bulunmak gibi sorumlulukları vardır.(Madde-37)

KVKK,bireylerin otomatik veri işleme süreçlerine itiraz hakkını düzenlemektedir ancak kapsam ve detaylar açısından GDPR'ye göre daha sınırlıdır. KVKK'da kişilere yalnızca **olumsuz sonuç doğuran** otomatik veri işleme süreçlerine itiraz etme hakkı tanınmaktadır. Örneğin, bir kişinin kredi başvurusunun otomatik değerlendirme sonucunda reddedilmesi durumunda birey, bu işleme karşı çıkabilir. Ancak KVKK'da profil oluşturma veya insan müdahalesi talep etme gibi haklar açıkça düzenlenmemiştir. Bu durum, KVKK'nın itiraz hakkını yalnızca olumsuz etkilere bağlı olarak sınırlandırdığını göstermektedir.(Madde-11/1-g)	GDPR'nın bireylerin otomatik veri işleme süreçlerine itiraz hükmü daha geniş bir koruma sunar. GDPR otomatik işlemeye dayalı kararların, bireyin haklarını, özgürlüklerini veya meşru menfaatlerini etkileyen durumlarda bireylerin bu kararlara itiraz etme hakkını tanır. Ayrıca GDPR, bireylere otomatik işlem süreçlerinde **insan müdahalesi talep etme** ve bu süreçlerin mantığını anlama hakkını da verir. Profil oluşturma gibi işlemler GDPR kapsamında açıkça düzenlenmiş olup herhangi bir olumsuz sonucun doğması şartı aranmaz. Bu nedenle GDPR, bireysel hakların korunması açısından daha kapsamlı bir düzenleme sunmaktadır.(Madde-22)

Kaynak: (Kişisel Verileri Koruma Kurumu (KVKK), 2016; European Union, 2016)

Tablo 3'ten de anlaşılacağı üzere GDPR daha kapsamlı bir düzenlemedir. GPDR sadece Avrupa Birliği ülkeleri için değil AB vatandaşlarına hizmet sunan tüm kuruluşlar için geçerli olmaktadır. GDPR'nin uluslararası açıdan daha geniş ölçekte olması, veri koruma standartlarını daha yüksek bir seviyeye taşımaktadır. Öte yandan KVKK Türkiye sınırları içerisinde geçerli olup GDPR'ye göre daha sınırlı bir koruma çerçevesi sunmaktadır. Tablo da ayrıca ilgili kişinin hakları, veri toplama, veri güvenliği, unutulma hakkı ve yaptırımlar hakkında iki düzenleme arasındaki farklar değerlendirilmektedir. GDPR ilgili kişilere ilişkin daha fazla hak sunup daha fazla yaptırımlar ön görürken, KVKK veri güvenliği sağlama açısından daha sınırlıdır. Tabloda yer alan karşılaştırmalı değerlendirme de Türkiye'de veri güvenliği sağlama adına GDPR referans alınarak daha iyi iyileştirmeler yapılabileceği gösterilmektedir.

Öte yandan GDPR ve KVKK karşılaştırıldığında, veri işleme süreçlerini yöneten temel ilkeler açısından genel bir uyum olduğu görülmektedir. Ancak bu uyum, KVKK'nın yapısal özelliklerinden çok Kişisel Verileri Koruma Kurumu'nun proaktif yaklaşımlarına dayanmaktadır. KVKK, temel ilkelerde GDPR ile örtüşse de hukuki dayanakların belirlenmesi ve ilgili kişilerin haklarının detaylandırılması konularında yeterince kapsamlı değildir. Özellikle, KVKK'da meşru menfaat ve kamu yararına işleme gibi hukuki dayanaklara ilişkin eksiklikler, ilgili kişiler ve işleyenler arasındaki hak ve menfaat dengesini sağlama konusunda zorluklar yaratmaktadır. Ayrıca, ilgili kişilerin işleme itiraz hakkı, işleme kısıtlama hakkı ve veri taşınabilirliği hakkı gibi hakların sınırlı olması, kişisel veri üzerindeki bireysel kontrolü zayıflatmaktadır. Bu eksikliklere rağmen KVKK'nın temel yapısı, bütüncül bir yaklaşım ve düzenleyici çabalarla GDPR ile daha uyumlu hale getirilebilir. Bu durum, KVKK'nın gelişime açık bir yasal çerçeve sunduğunu göstermektedir (Evrim, 2023, s.60-61).

6. KVKK KAPSAMINDA BİYOMETRİK VERİ GÜVENLİĞİ VE ETİK SORUNLARIN ANALİZİ

Etik, insan davranışlarına ilişkin eylemlerin doğru-yanlış, iyi-kötü gibi değerlere dayanarak incelenmesi ve bireyin hayatını şekillendiren ahlaki temelleri tartışan bir disiplindir. Bu doğrultuda hem teorik hem de uygulamalı yaklaşımlar ön plana çıkmaktadır. Uygulamalı etik, 20. yüzyılın sonlarında teknolojik gelişmelerin getirdiği güncel sorunlara çözüm üretme amacıyla ortaya çıkmış ve biyoetik, robot etiği, medya etiği gibi çeşitli alt dallara ayrılmıştır. Özellikle yapay zeka ve teknolojinin hızla ilerlemesi, etik açıdan yeni sorunları ortaya çıkarmıştır (Öztürk Dilek, 2019, s.48) Bu teknolojilerin toplumsal etkileri üzerine yapılan akademik çalışmalar, etik ihlallerin boyutlarını ve çözüm önerilerini tartışmaktadır. Yapay zeka sistemlerinin karar alma süreçlerinde şeffaflık eksikliği, önemli bir etik sorun olarak karşımıza çıkmaktadır (Yeşilkaya, 2022, s.951; Topakkaya, 2019, s.96) Özellikle derin öğrenme algoritmalarının karmaşık yapısı, alınan kararların nasıl ve neden verildiğinin

anlaşılmasını zorlaştırmaktadır. Bu durum, hesap verebilirlik ve güvenilirlik konularında endişelere yol açmaktadır.

Büyük veri analitiği ve yapay zeka uygulamalarında karşılaşılan bir diğer önemli etik mesele, algoritmik önyargılar ve ayrımcılıktır. Mahremiyetin korunması da büyük veri ve yapay zeka uygulamalarında kritik bir etik konudur. Kişisel verilerin toplanması, depolanması ve işlenmesi süreçlerinde bireylerin gizlilik haklarının ihlali riski bulunmaktadır. Yapay zeka ile ilişkili etik zorluklar arasında öne çıkan temel meselelerden biri gizlilik ve veri koruma konusundaki endişelerdir. Ancak bu iki kavramın aynı anlama gelmediğini belirtmek önemlidir. Gizlilik, bireylerin özel bilgilerinin korunması ile alakalı iken veri koruma bu gizliliği sağlamak için kullanılan mekanizmalardır. Yapay zeka etiği bağlamında, gizlilik endişeleri çoğunlukla bilgi gizliliği ekseninde şekillenmektedir. Bununla birlikte, yapay zekanın hızlı gelişimi, mahremiyet ve gözetim konularını etik tartışmaların merkezine yerleştirmiştir. Özellikle yapay zeka tabanlı sistemlerin bireylerin ve toplumların birçok alanda sürekli olarak izlenmesine olanak tanıması, mahremiyetin aşınmasına yol açmaktadır. Bu durum, kişilerin özel alanlarının giderek daha fazla ihlal edilmesine ve yaygın gözetim uygulamalarının yapay zeka aracılığıyla daha da artmasına neden olmaktadır. Aşırı gözetimin yapay zeka destekli gelecekte daha belirgin hale gelmesi, mahremiyetin sonu olarak yorumlanırken, bu durumun aynı zamanda etik açıdan ciddi kaygılar doğurduğu ifade edilmektedir (Yeşilkaya, 2022, s.956).

Büyük veri ve yapay zeka teknolojileri, veri işleme kapasitesi ve karar alma süreçlerinde insan yaşamını etkileyebilecek bir potansiyele sahipken, aynı zamanda bireysel haklar, mahremiyet ve adalet gibi etik soruları gündeme getirmektedir. Bu itibarla, bireylerin fiziksel ve davranışsal özelliklerini temel alarak çalışan biyometrik veri teknolojileri hem büyük veri hem de yapay zeka uygulamalarıyla doğrudan alakalıdır. Ancak biyometrik veriler, doğası gereği daha hassas ve kişiye özel olduğu için, bu alanda etik kaygılar daha da önemli bir hal almaktadır. Bu nedenle biyometrik veri etiğinin kendine özgü zorluklarını ele almak önem arz etmektedir. Biyometrik verilerin kullanımıyla ilgili etik ihlaller, çeşitli aktörler tarafından farklı nedenlerle gerçekleştirilebilmektedir. Kurumlar, bireyler, devletler ve teknoloji şirketleri bu ihlallerin temel sorumluları olarak ele alınabilir. Örnek vermek gerekirse ticari kazanç elde etmek isteyen bazı şirketler, kişilerin açık rızası olmadan biyometrik verileri toplayabilmekte ve pazarlama gibi amaçlarla kullanabilmektedir. Bunun yanı sıra güvenlik veya kamu düzenini sağlama argümanı ile devletler, vatandaşların biyometrik verilerini izleme ve gözetim için kullanabilmektedir. Bu durum da etik açıdan bireylerin mahremiyet haklarının ihlali olarak değerlendirilmektedir (Yıldırım, Yalçın, 2023, s.511).

Bireyler açısından bakıldığında, biyometrik verilerin kötü niyetle kullanımı dolandırıcılık ve kimlik hırsızlığı gibi suçlarla sonuçlanabilmektedir. Çalışanların, kurum içi veri tabanlarından yetkisiz erişim sağlayarak verileri dışarı sızdırması da bu ihlaller arasında gösterilebilir (Küzeci, 2018, s.487). Teknoloji şirketleri ise rekabet avantajı sağlama veya ürün geliştirme amacıyla kullanıcıların rızası olmadan biyometrik verileri toplayabilmektedir. Bu durum, etik ilkelere uygun olmayan bir Ar-Ge sürecine yol açabilmektedir (Yıldırım, Yalçın, 2023, s.512).

Etik ihlallerin nedenleri arasında farkındalık eksikliği, düzenlemelerin yetersizliği ve denetim eksikliği önemli yer tutmaktadır. Özellikle, yasal boşlukların olması ve biyometrik verilerin korunmasına yönelik ulusal politikaların henüz yeterince gelişmemiş olması, bu tür ihlalleri de kolaylaştırmaktadır. Öte yandan biyometrik sistemlerin hızlı ve etkili olması nedeniyle, şirketler maliyet ve zaman tasarrufu sağlama amacıyla zaman zaman etik kaygıları da göz ardı edebilmektedir. Bu doğrultuda, biyometrik veri kullanımına ilişkin etik ihlaller, bireylerin mahremiyet haklarını tehdit etmekte ve güven kaybına yol açmaktadır. Bu ihlallerin önüne geçmek için güçlü yasal düzenlemeler, farkındalık artırıcı eğitimler ve denetim mekanizmalarının geliştirilmesi gerekmektedir.

Biyometrik verilerin işlenmesi, kişilerin temel hak ve özgürlüklerinin korunması kapsamında anayasal bir hak olarak güvence altına alınmıştır. Bu nedenle, biyometrik verilerin işlenmesinde ölçülülük ilkesi ve açık rıza kavramları büyük önem taşımaktadır. Ölçülülük ilkesi, verilerin

işlenmesinde amaca uygunluk, gereklilik ve orantılılık kriterlerinin gözetilmesini ifade ederken, açık rıza ise bireyin bilgilendirilmiş ve özgür iradesiyle verdiği onayı ifade etmektedir (Erdinç, 2020, s.11). Bu doğrultuda kişisel veri güvenliği ile biyometrik güvenlik arasında doğrudan bir ilişki bulunmaktadır. Biyometrik verilerin güvenliğinin sağlanması, genel kişisel veri güvenliği politikalarının bir parçası olup bu verilerin korunması için hem teknik hem de hukuki önlemlerin alınması gerekmektedir.

Öte yandan kişisel verilerin güvenliğini sağlamak için öncelikle güçlü şifreleme yöntemleri kullanılmalı ve iki faktörlü kimlik doğrulama mekanizmaları uygulanmalıdır. Ayrıca güvenlik yazılımlarının güncel tutulması ve düzenli olarak sistem taramaları yapılması da önemlidir. Bireylerin, kişisel verilerini paylaşmadan önce aydınlatma metinlerini dikkatlice okumaları ve gerekli durumlarda açık rıza vermeleri gerekmektedir. Bu sayede, verilerin hukuka uygun olarak işlenmesi ve korunması sağlanabilecektir (Altıntaş, Barkuş, 2023, s.51).

Türkiye'de yürürlükte olan Kişisel Verilerin Korunması Kanunu (KVKK), bireylerin kişisel bilgilerinin korunmasını ve gizlilik haklarının sağlanmasını güvence altına alan bir yasal düzenleme olarak öne çıkmaktadır. Bu kanun, biyometrik veriler (parmak izi, yüz tanıma, retina taraması gibi) gibi kişiye özgü özellikleri "özel nitelikli kişisel veriler" kategorisine dahil etmektedir. Biyometrik veriler, kişilerin fiziksel veya davranışsal özelliklerinden yola çıkarak oluşturulan, kişileri diğerlerinden ayıran veriler olarak tanımlanmakta olup bu verilerin benzersiz yapısı, kimlik doğrulama süreçlerinde güvenliği artırırken aynı zamanda ciddi etik ve güvenlik risklerini de beraberinde getirmektedir. Türkiye'de KVKK çerçevesinde biyometrik veri güvenliği ve etik sorunların ele alınması, veri işleme süreçlerinin hem yasal hem de etik açıdan incelenmesini gerekli kılmaktadır (Başkaya, Karacan, 2022, s. 482).

KVKK, biyometrik verilerin işlenmesinde yüksek koruma standartları gerektiren bir çerçeve sunmaktadır. Kanunun 6. maddesi, biyometrik verileri "özel nitelikli kişisel veriler" olarak tanımlayarak işlenme koşullarını diğer verilere kıyasla daha katı kurallarla sınırlandırır. Bu bağlamda biyometrik veriler ancak kanun tarafından belirlenen özel koşullar çerçevesinde ya da ilgili kişinin açık rızası alınarak işlenebilir. Ayrıca biyometrik verilerin güvenliğinin sağlanması, veri sorumluları için yasal bir zorunluluktur. KVKK'nın Haklar ve Yükümlülükler başlıklı bölümünün 12'nci maddesinde veri güvenliğine ilişkin hükümler bulunmaktadır. Bahse konu maddenin birinci fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu hüküm altına alınmıştır. Öte yandan dördüncü fıkra da ise veri sorumluları ile veri işleyen kişilerin, öğrendikleri kişisel verileri Kanun hükümlerine göre aykırı olarak başkalarına açıklayamayacakları ve işleme amacı dışında kullanamayacakları belirtilmiştir (Kişisel Verileri Koruma Kanunu,2016.).Bu nedenle, biyometrik veri güvenliğine yönelik teknik ve idari tedbirlerin eksiksiz uygulanması önemlidir. Bu tedbirler arasında veri şifreleme, erişim kontrol mekanizmaları ve biyometrik verilerin anonim hale getirilerek kullanılması gibi işlemler yer alır. Örneğin, yüz tanıma verilerinin anonimleştirilmesi veya sadece gerekli olan verilerin işlenmesi, biyometrik veri güvenliğini artıran yaygın yöntemlerdendir (Tanışık, Bal, 2024, s. 269).

Biyometrik veri güvenliği, yalnızca teknik güvenlik önlemleri ile sınırlı kalmayıp aynı zamanda etik açıdan da önemli sorunları gündeme getirmektedir (Akkurt, 2020, s.21). Biyometrik verilerin toplanması, KVKK'da belirtilen özel durumlar haricinde ancak kişinin açık rızasının alınmasıyla mümkün kılınmaktadır. Ancak biyometrik verilerin toplanması sürecinde, kişilerin mahremiyet haklarını ihlal etme riski gibi ciddi etik sorunlar bulunmaktadır. Biyometrik veriler, kişilerin kimlikleriyle doğrudan ilişkilendirilebildiğinden mahremiyetin ihlali ve sürekli gözetim altında olma hissi gibi ciddi etik endişelere yol açabilmektedir. Özellikle kamusal alanlarda yaygın olarak kullanılan yüz tanıma sistemleri, bireylerin günlük yaşamlarını sürekli bir izlenme durumu altında hissetmelerine neden olabilir. Bu durum, bireylerin mahremiyet haklarının ihlal edilmesi riski yaratmakta ve bireysel özgürlükler üzerinde baskı oluşturabilmektedir. Bu bağlamda bireylerin yüz

tanıma sistemlerine veya diğer biyometrik sistemlere maruz bırakılmadan önce rızalarının alınması, etik açıdan temel bir gereklilik olarak öne çıkar. Örneğin, kamuya açık alanlarda yüz tanıma teknolojilerinin kullanımı, bireylerin izinsiz şekilde takip edilmesine yol açabilir. Kişinin rızası olmaksızın izlenmesi gibi durumlar, KVKK'nın mahremiyet haklarını koruma amacına ne kadar hizmet ettiğini sorgulatmaktadır. Ayrıca bu sürecin şeffaflığı çoğu zaman yetersiz kalmaktadır. Bilgilendirilmiş onanımın sağlanamaması, kişilerin verilerinin nasıl kullanılacağı konusunda kararlarını sınırlandırmakta ve bu durumda ciddi etik bir sorun oluşturmaktadır. Kişilere yönelik bilgilendirilmiş onam sürecindeki bu eksikliklerin giderilmesi, KVKK'nın veri koruma etkinliğinin daha etkin hale gelmesi için önemlidir.

Biyometrik verilerin kullanımında karşılaşılan etik sorunlar, kişilerin bilgiye erişim hakları ve şeffaflık taleplerini de ortaya çıkarmaktadır. Kişilerin, kendileri hakkında toplanan biyometrik verilerin nasıl ve ne amaçla kullanıldığını bilme hakları, veri işleme süreçlerinin etik sorumluluklarla uyumlu olması gerekmektedir. Kurumlar, biyometrik verilerin işlenme amacını ve süresini belirtmeli ayrıca ilgili kişilere verileri üzerinde kontrol imkanı da sunmalıdır. KVKK, bu bağlamda kişilere, verilerinin işlenmesine yönelik bilgi edinme, düzeltme ve silme hakkı tanımaktadır (Akkurt, 2020, s. 25).

Biyometrik veriler, kötü niyetli kişilerin veya grupların hedefi haline geldiğinde, kimlik doğrulama ve güvenlik süreçlerinde ciddi güvenlik açıkları yaratabilir. Örneğin, parmak izi verilerinin sızdırılması, kimlik hırsızlığı riskini artırabilir ve bu verilerin yeniden üretilmesi veya değiştirilmesi neredeyse imkansız olduğu için geri dönüşü olmayan bir kimlik kaybına neden olabilir. Veri ihlalleri durumunda biyometrik verilerin telafisi mümkün olmadığından, bu verilere yönelik güvenlik önlemlerinin etkin bir şekilde uygulanması ve güncellenmesi gerekmektedir. KVKK'nın biyometrik veriler için öngördüğü güvenlik tedbirleri, bu tür yetkisiz erişim risklerini azaltmaya yöneliktir ve biyometrik verilerin işlenmesi sırasında yüksek güvenlik standartlarının benimsenmesini şart koşar**.**

Biyometrik veri sistemleri, adalet ve ayrımcılık konularında da önemli etik sorunlar doğurmaktadır. Biyometrik verilerden özellikle yüz tanıma algoritmalarının bazı etnik gruplar üzerinde daha düşük doğruluk oranlarına sahip olması gibi önyargı sorunları, toplumsal eşitsizlikleri körükleyebilmektedir (İlter Güven, 2022, s.12-13). KVKK doğrudan bu önyargılara değinmese de yapay zeka sistemlerinin etik açıdan denetlenmesi gerekliliğini vurgulamaktadır. Türkiye'de biyometrik veri uygulamalarında önyargısız algoritmaların kullanılması, etik açıdan büyük bir önem taşımaktadır. Bu nedenle, biyometrik veri işleme süreçlerinde eşitlik ve ayrımcılık karşıtı prensiplerin gözetilmesi, etik açıdan temel bir gereklilik olarak kabul edilmektedir.

Biyometrik veri güvenliğinde karşılaşılan önemli bir sorunda dijitalleşmede gerçekleşen sürekli gelişim sürecidir. Dijital güvenlik tehditlerinin hızla evrildiği günümüz şartlarında biyometrik verilerin güvenliği, veri sızıntılarına veya saldırıları ile karşı karşıya kalabilir. Bu kapsamda veri güvenliğini sağlayan alt yapıların sürekli güncellenmesi gerekmektedir. Öte yandan biyometrik verilerin korunması adına biyometrik kimlik doğrulama ve şifreleme gibi daha spesifik yöntemlerin kullanılması gerekmektedir (Diri, 2022, s. 50).

Biyometrik veri güvenliği açısından modern çözümler arasında federe öğrenme gibi yeni teknolojiler ön plana çıkmaktadır. Bu yöntem verilerin merkezi olan depolama alanlarına alınmadan kullanılmasına imkan vermektedir. Bu durum kişisel verilerin mahremiyetin üst düzeyde korunmasına imkan vermektedir. Federe öğrenme, veri toplanmasını yerel cihazlar üzerinden yaparak, kişilerin biyometrik verilerini büyük veri içinde güvenli bir şekilde kullanılmasını sağlamaktadır (Başkaya, Karacan, 2022, s. 483) .

Türkiye'de yürürlükte olan KVKK, biyometrik verilerin işlenmesi sürecinde güvenlik, şeffaflık ve etik ilkelere uyulmasını şart koşarak bireylerin mahremiyet haklarının korunmasını sağlamayı hedeflemektedir. Öte yandan Türk Ceza Kanunu'nda 132.-140. Maddeler özel hayatın gizliliğinin ihlali, Türk Medeni Kanunu kişiliğin korunması gibi bölümlerde pozitif hukuk açısından

özel kişisel verilerin korunmasına yönelik menfaat dengesi kurulmaya çalışılsa da biyometrik veri gibi hassas verilerin hukuksal düzenlemeleri açısından türdeşlik bulunmamaktadır. Ayrıca hassas kişisel verilerin kendisini oluşturan unsurlar yönünden objektif bir tanımı yapılmamakta olup bu durum hassas veri tanımı kapsamında ciddi uygulama zorlukları ve çelişkiler yaratacak potansiyel durumlar ortaya çıkarmaktadır (Bulut, 2020, s.119-122).

Biyometrik veri güvenliği ve etik sorunlar, teknolojinin hızla ilerlemesiyle giderek daha karmaşık bir hale gelmektedir. Bu bağlamda, biyometrik verilerin yalnızca yasal düzenlemelere uygun olarak değil, aynı zamanda etik ilkelere de bağlı kalınarak işlenmesi büyük önem taşır. Veri sorumlularının, biyometrik verilerin güvenliğini sağlarken etik sorumluluklarını da gözetmeleri, bireylerin haklarının korunması açısından kritik bir gereklilik olarak kabul edilmektedir. KVKK biyometrik verilerin güvenliği konusunda önemli hükümler içermesine karşı etik sorunlar açısından tam anlamı ile yeterli bir düzenleme sağlamamaktadır. Biyometrik veri toplama sürecinde şeffaflık, hesap verilebilirlik ve tarafsızlık gibi etik ilkelerin daha güçlü bir şekilde ele alınması, Türkiye'de biyometrik veri güvenliğinin arttırılmasına katkı sağlayacaktır (Güdek, 2023, s.249.). Teknolojinin hızlı gelişmesi ve biyometrik verilerin kullanım alanlarını genişletmesi, KVKK'nın daha sıkı denetim ve güncelleme ihtiyacını ortaya çıkarmaktadır. Biyometrik verilerin korunması, sadece hukuki değil, aynı zamanda etik sorumluluk gerektiren bir alan olduğundan veri güvenliğinin sağlanması, bireylerin mahremiyet haklarının korunması ve etik ihlallerin önlenmesi için hem kanuni düzenlemelerin hem de teknolojik yeniliklerin sürekli olarak takip edilmesi gerekliliğini ortaya koymaktadır (Tanışık, Bal, 2024, s. 270).

SONUÇ

Türkiye'de teknolojinin hızla gelişmesi, dijital kimlik ve biyometrik veri kullanımını her alanda yaygınlaştırmaktadır. Bu bağlamda, biyometrik verilerin güvenli ve etik standartlara uygun olarak işlenmesi, bireylerin mahremiyet haklarının korunmasında kritik bir rol oynar. Etik çerçevede, kişilerin açık rızasıyla veri toplanması, bu verilerin yine etik ilkelere göre işlenmesi ve saklanması gereklidir. Türkiye'de biyometrik veri güvenliğinin sağlanmasında Kişisel Verilerin Korunması Kanunu (KVKK) temel bir işlev üstlenmektedir. Ancak bu kanun kapsamında biyometrik veriler "özel nitelikli kişisel veri" olarak sınıflandırılsa da güvenlik ve etik sorunlarına dair kapsamlı düzenlemeler sınırlıdır.

Bu çalışmada, biyometrik veri toplama süreçlerinde karşılaşılan mahremiyet ihlalleri, bilgilendirilmiş onam eksiklikleri ve algoritmalardaki önyargılar gibi etik sorunlar analiz edilmiştir. Türkiye'de bu sorunlara yönelik daha şeffaf, hesap verebilir ve birey haklarını koruyucu bir yaklaşım benimsenmesi gerektiği vurgulanmıştır. KVKK'nın sağladığı yasal çerçevenin yanı sıra, veri koruma uygulamalarının pratikte nasıl işlediğini inceleyen denetim ve uyum mekanizmalarının güçlendirilmesi gerektiği öne çıkarılmıştır. Ayrıca, Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) gibi uluslararası standartlardan alınabilecek dersler doğrultusunda Türkiye'deki düzenlemelerin daha kapsayıcı hale getirilmesi önerilmektedir.

Sonuç olarak, biyometrik verilerin etik kullanımı ve güvenliğinin sağlanması için yalnızca yasal düzenlemeler yeterli olmayıp aynı zamanda toplum bilincinin artırılması ve bilgilendirilmiş onam süreçlerinin güçlendirilmesi gerekmektedir. Veri işleyen kuruluşların sorumluluklarının artırılması, bireylerin mahremiyetine saygı duyan etik ilkelerle uyumlu bir veri koruma kültürünün oluşmasına katkı sağlayacaktır. Bu kapsamda, Türkiye'de biyometrik veri güvenliğini daha etkin kılmak için çeşitli öneriler sunulmuştur.

Önerilerin ilki, yasal çerçevenin genişletilmesine yöneliktir. KVKK'nın biyometrik veri işleme süreçlerine dair düzenlemeleri daha ayrıntılı hale getirilerek özellikle yapay zeka destekli biyometrik sistemlere yönelik özel düzenlemeler sağlanmalıdır. İkinci öneri, bilgilendirilmiş onam süreçlerinin güçlendirilmesi üzerinedir. Bu bağlamda biyometrik verilerin toplanması ve kullanılması süreçlerinde bireylerin kapsamlı bir şekilde bilgilendirilmesi sağlanmalı, verilerin saklama süresi ve işlenme

amaçları net bir şekilde açıklanmalıdır. Ayrıca, kişilerin verdikleri onamı kolayca geri alabilmeleri sağlanmalıdır.

Üçüncü öneri, etik rehberlerin hazırlanmasıdır. Biyometrik verilerin kullanımında etik ilkelere bağlı kalmayı hedefleyen bir rehber oluşturulmalı, mahremiyetin korunması, önyargıların önlenmesi ve toplumsal eşitliğin sağlanması gibi konulara vurgu yapılmalıdır. Dördüncü olarak, biyometrik veri işleyen kurumların KVKK'ye uygun şekilde düzenli olarak denetlenmesi ve ihlaller karşısında hızlı müdahale mekanizmalarının kurulması gereklidir; bu süreçte KVKK'nın yaptırım gücü artırılmalıdır.

Beşinci öneri, biyometrik veri kullanımına yönelik halkın farkındalığını artıracak geniş çaplı bilgilendirme kampanyalarının düzenlenmesidir. Bu kampanyalar, biyometrik verilerin nasıl işlendiği, bireylerin hakları ve KVKK çerçevesindeki hakları konusunda bilgi sağlamalıdır. Böylece bireyler, mahremiyetleri üzerinde daha fazla kontrol sahibi olabilir ve bilinçli kararlar alabilir. Altıncı olarak, biyometrik veri toplama süreçlerinde tarafsızlığı sağlayacak algoritmalar geliştirilmelidir; böylece yüz tanıma gibi alanlarda etnik ve sosyal gruplar üzerinde daha eşit sonuçlar elde edilebilir.

Son olarak, biyometrik veri teknolojilerinin hızla gelişmesine paralel olarak yasal düzenlemelerin de güncellenmesidir. Bu kapsamda, teknolojik gelişmeleri yasal çerçeveye uyarlayacak daha esnek düzenlemeler yapılmalı ve biyometrik veri güvenliğini sağlamak için sürekli güncellenen yasal çerçeveler oluşturulmalıdır. Bu öneriler, Türkiye'de biyometrik veri güvenliğini artırmayı ve bireylerin mahremiyet haklarını korumayı amaçlayan hem kısa hem de uzun vadeli adımlardır. Böylelikle biyometrik verilerin güvenli ve etik bir çerçevede toplanması sağlanarak toplumsal güvenin de pekişmesine katkıda bulunulacaktır.

KAYNAKLAR

Altıntaş, S.,Barkuş, F.(2023). Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması. Ejovoc (Electronic Journal of Vocational Colleges), 13(1), 46-69. https://doi.org/10.17339/ejovoc.1311027

Alkan M., Menteş T.,İnceefe M.A.(2020).Kişisel Verileri Koruma Kitabı. Nobel Yayınları, Ankara.

Akçay,M.,Çetinkaya,H.H.(2011).Kampüslerde Uygulanan Yeni Biyometrik Sistemler,Akademik Bilişim Konferansı Bildirileri .İnönü Üniversitesi, Malatya

Akkurt, S. S.(2020). Kişisel Veri Kavramının Hukukî Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış. Kişisel Verileri Koruma Dergisi, 2(1), 20-32.

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

Başkaya, F., Karacan, H.(2022). Yapay Zeka Tabanlı Sistemlerin Kişisel Veri Mahremiyeti Üzerine Etkisi: Sohbet Robotları Üzerine İnceleme. Bilişim Teknolojileri Dergisi, 15(4), 481-490. https://doi.org/10.17671/gazibtd.1053803

Berry, J., Stoney, D. A.(2001). The history and development of fingerprinting. Advances in Fingerprint Technology, 2, 13-52. https://link.springer.com/referenceworkentry/10.1007/978-0-387-73003-5_181

Bulut, M.(2020). Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler. Ankara Barosu Dergisi, 78(3), 99-150. https://doi.org/10.30915/abd.811902

California Legislative Information.(2018). California Consumer Privacy Act (CCPA). Erişim tarihi 10/07/2024. https://cppa.ca.gov/regulations/pdf/cppa_act.pdf

Çiçek, Melike . Kamu Yönetiminde Kimlik ve Mahremiyet: Biyometrik Veri Kullanımının Etik ve Yönetişimsel Boyutları ve Ülke İncelemeleri. Kamu Yönetimi Çalışmaları, Livre de Lyon , ed. Bekir Parlak, Kadir Caner Doğan, Lyon, 2024 , ss.263-283.

Diri, N.,Yalçınkaya, B.(2022). Blokzincir Uygulamalarında Kişisel Veri Problemi: Depolama Riskleri ve Öneriler. Bilgi Yönetim Dergisi, 5(1), 47-67. https://doi.org/10.33721/by.1000702

Dülger, M. V.(2019). Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması. Yaşar Hukuk Dergisi, 1(2), 71-174.

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

Esmer Y.,Özdaşlı K.,(2023). Bilimsel araştırmalarda etik: Kavramlar ve ilkeler. Yükseköğretim ve Bilim Dergisi/Journal of Higher Education and Science, 13(3), 397-409. https://doi.org/10.5961/higheredusci.1291201

European Union.(2016). General Data Protection Regulation (GDPR).Erişim tarihi 03/09/2024 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

European Digital Rights.(2020). Facial recognition and the right to privacy in Europe. Erişim tarihi 28/08/2024 https://edri.org/our-work/facial-recognition/

Evren, A. G.(2023). Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects. Kişisel Verileri Koruma Dergisi, 5(2), 39-64.

Financial Inclusion Global Initiative.(2021). Digital ID to Enhance Financial Inclusion. Erişim tarihi 12/07/2024.

https://documents1.worldbank.org/curated/en/099650005162214653/pdf/P16477001277440f10b8080dc6f51daf2dc.pdf

Galterio, M. G., Shavit, S. A.,Hayajneh, T.(2018). A review of facial biometrics security for smart devices.Computers,7(3), 37.

Gelb, A., Clark, J.(2013). Identification for Development: The Biometrics Revolution. Center for Global Development. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2226594

Güdek, B.(2023). Kamu Sektöründe Etik Yönetime İlişkin Politikaların Uygulanması: KVKK ve Veri Etiği. Politik Ekonomik Kuram, 7(2), 237-251. https://doi.org/10.30586/pek.1325605

Gümüş, F., Ata, O.,Balık, H. H.(2018). Davranışsal Biyometrinin 5 Yılı: Kimlik Doğrulama ve Anomali Tespit Uygulamaları. Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 30(1), 345-364.

İlter Güven, İ.(2023). Biyometrik teknolojilerin yarattığı etik tartışmalar bağlamında güncel sanat örnekleri. Journal of Arts, 6(1), 9-18.

Illinois General Assembly.(2008). Biometric Information Privacy Act (BIPA). Erişim tarihi 09/07/2024.

https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

ISO.(2022). ISO/IEC 24745:2022. Erişim tarihi 29/07/2024. https://www.iso.org/standard/75302.html#lifecycle

Jain, A. K., Flynn, P.,Ross, A. A.(Eds.).(2011). Handbook of Biometrics. Springer. https://link.springer.com/book/10.1007/978-0-387-71041-9

Jain, A. K., Ross, A., Prabhakar, S.(2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.https://ieeexplore.ieee.org/abstract/document/1262027

Kavut, S.(2020). Kimliğin Dönüşümü: Dijital Kimlikler. Selçuk İletişim, 13(2), 987-1008. https://doi.org/10.18094/josc.691445

Khine, P. K., Mi, J., Shahid, R.(2021). A comparative analysis of co-production in public services. Sustainability, 13(12). https://doi.org/10.3390/su13126730

Kişisel Verileri Koruma Kurumu (KVKK).(2016). Kişisel Verilerin Korunması Kanunu. Türkiye Cumhuriyeti Resmi Gazete.Erişim tarihi 27/07/2024. https://kvkk.gov.tr

Kişisel Verileri Koruma Kurumu (KVKK).(2024). Biyometrik verilerin işlenmesinde dikkat edilmesi gereken hususlar rehberi. Erişim tarihi 27/07/2024. https://kvkk.gov.tr

Küzeci, E.(2018). Sağlık Bilişim Teknolojileri ve Yeni Hukuksal Sorunlar. İnönü Üniversitesi Hukuk Fakültesi Dergisi, 9(1), 477-506. https://doi.org/10.21492/inuhfd.410571

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

National Institute of Standards and Technology(NIST).(2020).Biometrics. Erişim tarihi 27/07/2024.https://www.nist.gov/programs-projects/biometrics

Özer Deniz, M.,Özer, M. T.(2022). Biyometrik Verilerin İşlenmesinin Yargı Kararları Işığında Değerlendirilmesi.Çukurova Üniversitesi Hukuk Araştırmaları Dergisi(1), 92-110.

Öztürk Dilek, G.(2019). Yapay Zekanın Etik Gerçekliği. Ankara Uluslararası Sosyal Bilimler Dergisi, 2(4), 47-59.

Paşaoğlu, C., Adje, K. H., Demirtaş, O.(2019). A review on privacy preserving biometric authentication methods. Kişisel Verileri Koruma Dergisi, 1(1), 34-46.

Pereira, D.(2021). Public administration and values oriented to sustainability: A systematic approach to the literature. Sustainability, 13(5), 2566. https://doi.org/10.3390/su13052566

Prabhakar, S., Pankanti, S., Jain, A. K.(2003). Biometric recognition: Security and privacy concerns. IEEE Security & Privacy, 1(2), 33–42. https://doi.org/10.1109/MSECP.2003.1193298

Personal Data Protection Commission Singapore .(2014). Erişim tarihi 02/08/2024.

https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act

Tanışık, S., Bal, S.(2024). Dijital Mahremiyet ve Kurumsal Sorumluluk: Kişisel Verilerin Korunmasında İletişim Teknolojilerinin Kamusal Rolü. Yeni Medya Dergisi, 16, 269-280. https://doi.org/10.55609/yenimedya.1424182

T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü.(2024). T.C. Kimlik Kartı.Erişim tarihi 25/07/2024 https://www.nvi.gov.tr/tc-kimlik-karti

Topakkaya, Eyibaş, A. Y.(2019). Yapay Zeka ve Etik İlişkisi.Felsefe Dünyası(70), 81-99.

Uğurlu, H.(2020). Bilimsel araştırmalarda etik. Ahi Evran Akademi Sosyal Bilimler Dergisi, 1(1), 67-78.

Vujković, P., Ravšelj, D., Umek, L.,& Aristovnik, A.(2022). Bibliometric analysis of smart public governance research: Smart city and smart government in comparative perspective. Social Sciences, 11(7), 293. https://doi.org/10.3390/socsci11070293

World Bank.(2019). Identification for Development (ID4D) Global Dataset. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

World Bank.(2021). ID4D Global Dataset 2021: Volume 2 - Digital Identification Progress & Gaps. Erişim tarihi21/07/2024https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099020824141510923/p176341192f2c50e11bc5619be95c4fb2ed

World Economic Forum.(2018). Identity in a Digital World: A New Chapter in the Social Contract. Erişim tarihi 25/07/2024https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Yalçın,N.Yıldırım T.(2023).Biyometrik Güvenlik.Bilişim Teknolojileri Güvenliği, ed.Nursel Yalçın,Hüseyin Çakır,Nobel Yayınevi,Ankara,ss.179-207.

Yalçın, N.,Gürbüz, F.(2015). Biyometrik Güvenlik Sistemlerinin İncelenmesi. Duzce University Journal of Science and Technology, 3(2), 398-413.

YıldırımT.Yalçın N.(2023). Kişisel Verilerin Güvenliği. Bilişim Teknolojileri Güvenliği, ed.Nursel Yalçın,Hüseyin Çakır,Nobel Yayınevi,Ankara,ss.499-527.