T.C.
ÜSKÜDAR ÜNİVERSİTESİ
BAĞIMLILIK VE ADLİ BİLİMLERİ ENSTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN PARMAK İZİ DELİLİ

Burak SUCAKLI

YÜKSEK LİSANS TEZİ

Tez Danışmanı
Prof. Dr. Sevil ATASOY

İSTANBUL-2023

T.C.
ÜSKÜDAR ÜNİVERSİTESİ
BAĞIMLILIK VE ADLİ BİLİMLERİ ENSTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN PARMAK İZİ DELİLİ

Burak SUCAKLI

YÜKSEK LİSANS TEZİ

Tez Danışmanı
Prof. Dr. Sevil ATASOY

İSTANBUL-2023

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Kişisel Verilerin Korunması Açısından Parmak İzi Delili” adlı çalışmanın, tarafımdan bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını, intihal yapmadığımı ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yaparak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

Tarih

Burak Sucaklı

İmza

TEŞEKKÜR

Tez danışmanlığımı üstlenerek beni onurlandıran ve öğrencisi olmaktan gurur duyduğum kıymetli hocam Prof. Dr. Sevil ATASOY'a bana kattıkları ve destekleri için sonsuz teşekkürlerimi sunarım.

Kişisel verilerin korunması konusunu içselleştirmesi ve uluslararası uygulamalara hakimiyeti ile beni bu çalışmaya başlamakta yüreklendiren meslektaşım Av. Sibel ÖRER'e, lisans eğitimimden bu yana hocalığı ve ağabeyliği ile yanımda duran Dr. Nuri Aziz MİDYAT'a, bana huzurlu bir çalışma ortamı yaratan meslektaşlarım Av. Gonca ÖNDEMİR KÜÇÜK'e ve Av. Cansu GÖKHAN KESEN'e çok teşekkür ederim.

Yaşamımın her alanında varlıkları ile bana destek olan anneme ve babama da minnettarım.

Son olarak, elbette bu çalışmanın bir diğer mimarı, meslektaşım, arkadaşım, eşim Av. Tuğba SUCAKLI'ya ve her çalışmada bana susayan Deniz kızıma da teşekkürü bir borç bilirim.

Şişli 2023

Av. Burak SUCAKLI

İÇİNDEKİLER

YEMİN METNİ ……. i
TEŞEKKÜR ……. ii
ŞEKİLLER TABLOSU ……. iv
ÖZET ……. v
ABSTRACT ……. vi
GİRİŞ ……. 1

BİRİNCİ BÖLÜM
PARMAK İZİNE İLİŞKİN GENEL BİLGİLER

1.1. Geçmişten Günümüze Parmak İzi ……. 3
1.2. Parmak İzinin Sınıflandırılması ……. 5
1.3. Parmak İzinin Özellikleri ……. 7
1.4. Parmak İzi Eşleştirilmesinde Kullanılan Özellikler ……. 8
1.5. Parmak İzi Tipleri ……. 10

İKİNCİ BÖLÜM
KİŞİSEL VERİ KAVRAMININ DOĞUŞU VE KAPSAMI

5.1. Kişisel Verilerin Korunması İhtiyacının Doğuşu ……. 11
5.2. Kişisel Veri Tanımı Ve Tanımın Kapsamı ……. 13
5.2.1. Kişisel Verinin Tanımı ……. 13
5.2.2. Özel Nitelikli Kişisel Veri ……. 14
5.2.3. Kişisel Veri Kavramının Kapsamı ……. 15

ÜÇÜNCÜ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN KAYNAKLARI

3.1. Uluslararası Kaynaklar ……. 18
3.1.1. Oecd ……. 18
3.1.2. Birleşmiş Milletler Düzenlemeleri ……. 19
3.1.3. Avrupa Konseyi Düzenlemeleri ……. 20
3.1.4. Avrupa İnsan Hakları Sözleşmesi ……. 20
3.1.5. Avrupa Birliği Düzenlemeleri ……. 22
3.2. Ulusal Kaynaklar ……. 22
3.2.1. Türkiye Cumhuriyeti Anayasası ……. 22
3.2.2. 6698 Sayılı Kişisel Verilerin Korunması Kanunu ……. 23

DÖRDÜNCÜ BÖLÜM

6698 SAYILI KANUNDA YER ALAN TEMEL KAVRAMLAR

4.1. Kişisel Verilerin İşlenmesi ……... 23

4.2. İlgili Kişi ……... 24

4.3. Veri Sorumlusu ……... 24

4.4. Veri İşleyen ……... 25

4.5. Açık Rıza ……... 25

4.6. Kişisel Verilerin Silinmesi, Yok Edilmesi Ve Anonim Hale Getirilmesi ……... 27

4.6.1. Kişisel Verilerin Silinmesi ……... 27

4.6.2. Kişisel Verilerin Yok Edilmesi ……... 29

4.6.3. Kişisel Verilerin Anonim Hale Getirilmesi ……... 32

BEŞİNCİ BÖLÜM

KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR VE TEMEL İLKELER

5.1. Kişisel Verilerin İşlenmesinde Temel İlkeler ……... 33

5.2. Kişisel Verilerin İşlenme Şartları ……... 37

5.2.1. Özel Nitelikli Olmayan Verilerin İşleme Şartları ……... 38

5.2.2. Özel Nitelikli Verilerin İşleme Şartları ……... 46

ALTINCI BÖLÜM

PARMAK İZİNİN KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR VE TEMEL İLKELER BAKIMINDAN DEĞERLENDİRİLMESİ

6.1. 6698 Sayılı Kanun'un İstisnaları Bakımından Değerlendirme …….…… 48

6.2. 2559 Sayılı Polis Vazife Ve Salahiyet Kanun'u Gereğince Toplanan Parmak İzi Verisinin Kişisel Verilerin Korunması Temel İlkelerine Aykırılığı Sorunu ……. 50

6.2.1. Amaç İlkesi Bakımından Değerlendirme …….. 52

6.2.2. Ölçülülük İlkesi Bakımından Değerlendirme ……... 53

6.3. İmha Politikaları Açısından Değerlendirme …… 54

6.4. Parmak İzi Delilinin Yeni Bilimsel Gelişmeler Işığında Biyometrik Verilerin Korunmasına İlişkin Usullerden Genetik ve Biyolojik Delillerin Korunmasına Yönelik Usullere Geçirilmesine Yönelik Gereklilikler ……. 56

6.5. Parmak İzi Delilinin Toplanmasına Yönelik Amacın Dışında Kullanılması Yönünden Değerlendirme ……... 57

SONUÇ ……... 60

KAYNAKÇA ……... 62

ÖZGEÇMİŞ……63

ŞEKİLLER TABLOSU

Şekil 1: Henry'nin oluşturmuş olduğu parmak izi sınıflandırma sistemi (Neil Yager, 2004). 4
Şekil 2: Ülkemizde parmak izi ile çözülen ilk vakanın mukayese tablosu (AKDENİZ, 2021) 5
Şekil 3: Parmak İzlerinin Sınıflandırılması (Doğukan Ölmez, 2021). 6
Şekil 4: Parmak izlerinde bulunan özellikler (Cantürk, 2019). 8
Şekil 5: Parmak izindeki karakteristik noktalar (Gül, 2014) 8

ÖZET

(SUCAKLI, Burak, Yüksek Lisans, İstanbul, 2023)

Kişisel Verilerin Korunması Açısından Parmak İzi Delili

Bu çalışma ile parmak izi verisinin idari merciler ve özellikle kolluk tarafından işlenmesi, kaydedilmesi ve kullanılmasının Kişisel Veri Hukuku yönüyle değerlendirilmesi yapılmıştır.

Çalışmada öncelikle bir delil olarak parmak izi verisi ele alınmış, güncel teknolojiler ışığında parmak izi delili değerlendirilmeye çalışılmıştır.

Diğer yandan kişisel verinin korunması gerekliliğinin doğuşu, kişisel verinin korunmasına yönelik uluslararası gelişmeler ve ulusal normlar değerlendirilmiştir.

Ayrıca parmak izi verisinin, Kişisel Verilerin Korunması Hukuku açısından değerlendirilmesine yönelik olarak AİHM kararları incelenmiş, Türkiye'nin üye olduğu uluslararası kuruluşlar nezdinde bağlayıcı olan ve olmayan normlar incelenmiştir.

Bu incelemelerin yapılmasındaki amaç, parmak izi delilinin soruşturma öncesi ve soruşturma sonrası kullanımına yönelik olarak Kişisel Verilerin Korunması Hukukuna uygunluğunun sorgulanması, Kişisel verilerin korunmasına yönelik milli güvenliğe ve kamu düzenine ilişkin istisnaların doğru bir şekilde değerlendirilmesini sağlamaktır.

Gelinen noktada; özellikle soruşturma öncesi parmak izi delilinin kullanımının Kişisel Verilerin Korunmasına yönelik ulusal ve uluslararası normlara aykırılık teşkil edebildiği, Türkiye'nin taraf olduğu uluslararası sözleşme ve Mahkeme kararlarına aykırılıklar içerebildiği görülmüştür.

Bu doğrultuda; var olan mevzuat hükümlerinde düzenlemeler yapılması gerektiği, kullanımın Kişisel Veri Hukukuna uygun olduğu noktalarda dahi normların daha açık ve sınırsız kullanım biçimine dönüşmemesini sağlayacak önlemler alınması gerektiği anlaşılmaktadır.

Anahtar Kelimeler: Parmak İzi, Kişisel Veri, Hukuk, Anayasa

ABSTRACT

(SUCAKLI, Burak, Master, Istanbul, 2023)

Fıngerprınt Evıdence In Terms Of Protectıon Of Personal Data

This study evaluates the processing, recording and use of fingerprint data by administrative authorities and especially by law enforcement agencies in terms of Personal Data Law.

In the study, first of all, fingerprint data is discussed as an evidence and fingerprint evidence is tried to be evaluated in the light of current technologies.

On the other hand, the emergence of the necessity to protect personal data, international developments and national norms regarding the protection of personal data were evaluated.

In addition, the decisions of the ECtHR have been examined for the evaluation of fingerprint data in terms of Personal Data Protection Law, and the binding and non-binding norms before the international organizations of which Turkey is a member have been examined.

The purpose of these examinations is to question the compliance of fingerprint evidence with the Law on the Protection of Personal Data for the use of fingerprint evidence before and after the investigation, and to ensure that the exceptions related to national security and public order for the protection of personal data are evaluated correctly.

At this point, it has been observed that the use of fingerprint evidence, especially before the investigation, may be contrary to national and international norms regarding the Protection of Personal Data, and may be contrary to international conventions and Court decisions to which Turkey is a party.

In this direction, measures should be taken to ensure that the norms do not turn into a more open and unlimited form of use, even at points where the existing legislation provisions should be amended and the use is in accordance with the Personal Data Law.

Keywords: Fingerprint, Personal Data, Law, Constitutio

GİRİŞ

Hukukun her alanında normların sağladığı menfaatlerin çatıştığı alanlar görmek mümkündür. Nitekim çatışan menfaatlerin taraflarından birinin idare olması halinde ise bu çatışma durumunun değerlendirilmesi daha fazla önem arz eder.

Nitekim devlet otoritelerinin kamu düzeni ve genel güvenlik ihtiyaçları ile kişilerin kendilerine sıkı sıkıya bağlı hakları birçok noktada çatışır. Kişisel Verilerin ve hatta özellikle Özel Nitelikli Kişisel Verilerin kullanımına yönelik de aynı husus geçerlidir.

Bir yandan otoritenin kamu düzeni ve genel güvenlik ihtiyaçları devredeyken diğer yandan kişilerin özel nitelikteki verilerinin kullanılmasına yönelik sınırsız yetkilerle donatılması çatışmanın ana kaynağını oluşturur.

Çağdaş hukuk sistemlerinde kural olarak geçerlilik kazanmış ceza ve ceza muhakemesi hukukundan son çare olarak yararlanılması; bir suç işlendiği dair şüphe üzerine adli yetkilerin doğması; ve kişinin işlediği iddia olunan suçun muhakemesi kapsamında, suçluluğu veya suçsuzluğunun ispatlanmasıdır. Bu itibarla ceza ve ceza muhakemesi sürecinin amacı, olaya ve olayın unsurlarına yönelik delil elde edilmesi olup; suç işlenmesinden öncesiyle kural olarak ilgilenmez. Suç öncesi alanda bu anlamda idare yetki sahibidir.

Suçların meydana gelmeden engellemek zarar oluştuktan sonra faili cezalandırmaktan kuşkusuz daha önemlidir.

Uygulamaya bakıldığında, suç önlemeye yönelik yönelik klasik yöntemlerin özellikle suç amaçlı kurulmuş geniş çaplı yapıların önüne geçmekte yetersiz kaldığı görülmektedir. Dolayısıyla klasik yöntemlerin yanı sıra teknolojik gelişmelere paralel olarak pek çok yeni yöntemden yararlanılmakta; fakat bunun yanında aslında ceza ve ceza muhakemesinde uygulanan yöntemlere yani suç sonrası yöntemlere, daha sık ve daha erken biçimde başvurulmaktadır. Bu durumun doğal bir sonucu olarak, suç sonrası alan ile suç öncesi alanın arasında uygulanan yöntemlerin, birbirlerinin alanlarına girdiği görülmektedir.

Bununla birlikte bahse konu ayrım, Ceza Ve Ceza Muhakemesi Hukukunun temel hak ve özgürlüklerle doğrudan ve yakın ilişkisi gözetildiğinde, çok kalın ve ayırıcı olmak zorundadır.

Nitekim bu çalışma ile birlikte parmak izi gibi kişinin özel nitelikli olarak kabul edilen verisinin, gelişen teknolojik gelişmeler ışığında artık sadece parmak izi verisini kapsamadığı, parmak izi ile DNA verisine dahi ulaşılabilen bir gelişme içinde olduğumuzu göz önüne alarak bu veriler özelinde soruşturma öncesi ve sonrasına ilişkin ayrımların nasıl değerlendirilmesi gerektiği, konunun AİHM kararları ile Türk Hukukundaki yeri incelenmeye çalışılmış ve bunun sonuçları ortaya konulmaya gayret edilmiştir.

BİRİNCİ BÖLÜM

PARMAK İZİNE İLİŞKİN GENEL BİLGİLER

1.1. Geçmişten Günümüze Parmak İzi

Parmak izi insanın ana rahmindeyken oluşan ve insan vücudunda kişiye özel olan özelliklerden biridir. Parmak izinin varlığı çok uzun yıllar önce bulunmasına rağmen parmak izlerinin rutin olarak kullanılması hemen hemen 100 yıllık bir tarihe sahiptir (Criminalistic). Parmak izinin ilk kullanımı Babiller'e kadar dayanmaktadır. M.Ö. 1300'lerde ticari anlaşmalarda iki tarafında onaylamasını simgeleyen işaret olarak parmak izlerinin kullanıldığı fark edilmiştir (Akbulut, 2023).

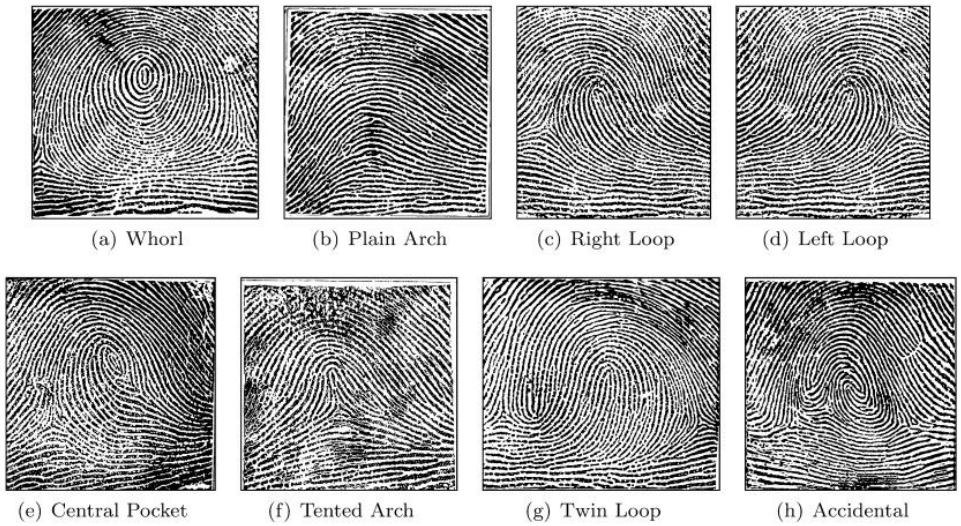
Adli Bilimler yönünde bakıldığında ise resmi olarak parmak izlerinin kullanımı 1800'lü yıllara dayanmaktadır. Her insanın parmak izinin farklı olduğu o yıllarda anlaşılmaya başlanmıştır. Bu konu hakkında ilk güvenilir kanıt ise kayıt Sir William Herschell'e aittir. Herschell 1858'de Doğu Hindistan Şirketinde bir çalışandı. Bazı materyaller yapmak üzere bölgesel bir sözleşme imzaladığı esnada, daha konveksiyonel bir imza kullanımı için insanların avuç izlerini almaya karar verdi. Herschel, yaptığı çalışmalarla kısa bir zaman sonra parmak izlerinin kişisel tanımlamadaki potansiyelini tespit etti ve bu konu üzerine başlangıçta vermiş olduğu karardan sonra yıllarca bir hobi olarak çalıştı. Bir kişiden almış olduğu parmak izinin otuz iki yıl sonra aynı kaldığını not ettikten sonra Herschell, parmak izlerinin değişmezliğini keşfetti.

Parmak izinin kullanımı hakkındaki ilk bilimsel yayın ise aynı yıllarda Henry Faulds tarafından yazılmıştır. 1800'lerin sonunda Sir Francis Galton parmak izi tanımlamaya yönelik ilk ciddi çalışmaları yapmaya başlamıştır. Bu yaptığı çalışma parmak izi sınıflandırılmasını içeren ilk çalışma olarak da kayıtlara geçmektedir. Onun yapmış olduğu sınıflandırma, parmak izlerini birçok parmak izinin arasından özel bir parmak izini bulabilmeyi kolaylaştırmak amacıyla oluşturulmuş bir dizinleme işlemiydi. 3 adet basit parmak izi sınıfı oluşturmuştu: ark (arsch), loop ve helezon (whorl). Galton'un diğer büyük katkısı ise parmak izlerinin benzemezliği ile ilgili çalışmasıydı. Buna ek olarak, benzemezlik, görünür bir kişisel tanımlama yöntemi olabilmesi için parmak izlerinin bir diğer gerekliliğiydi. Bu çalışmadan yıllar sonra Edward Henry,

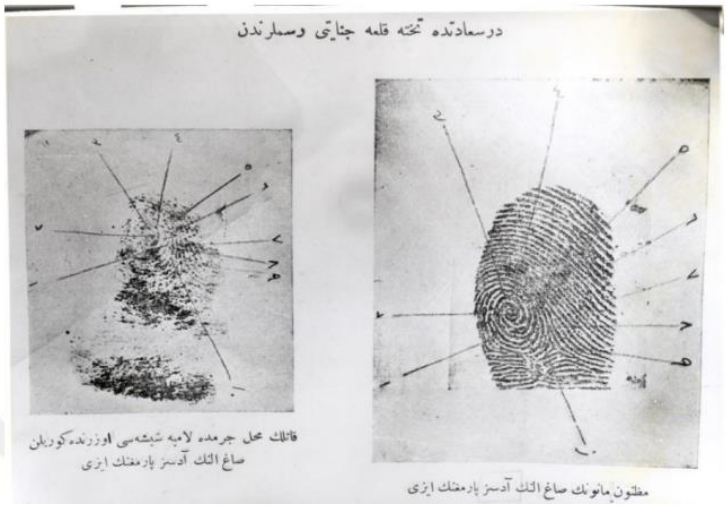
Galton'un parmak izi çalışmalarını geliştirerek devam etti. Henry, Galton'a ek olarak parmak izlerini 3 ana ve 3 ara sınıfa tekrardan ayırdı. Ayrıca parmak izleri üzerinde core ve delta noktalarını tanımladı ve sınıflandırmada bunları kullandı. Henry'nin oluşturduğu bu sistem modern sınıflandırma sisteminin temelini oluşturmaktadır. (Neil Yager, 2004)

Şekil 1: Henry'nin oluşturmuş olduğu parmak izi sınıflandırma sistemi (Neil Yager, 2004).

Ülkemizde hâlihazırda kullanılan Henry-Galton sistemi, 1910 yılında Yusuf Cemil Bey tarafından Türkiye' getirilmiştir. Günümüzde parmak izi kimlik tespitinde en yaygın olarak kullanılan fiziksel özelliklerden biridir (Kolay, 2021). Parmak izi, kimlik



doğrulamada, adli olaylarda ve güvenlik amacı ile çok yaygın bir şekilde kullanılmaktadır.



Şekil 2: Ülkemizde parmak izi ile çözülen ilk vakanın mukayese tablosu (AKDENİZ, 2021)

Günümüzde parmak izi kimlik tespitinde en yaygın olarak kullanılan fiziksel özelliklerden biridir. Parmak izi, kimlik doğrulamada, adli olaylarda ve güvenlik amacı ile çok yaygın bir şekilde kullanılmaktadır.

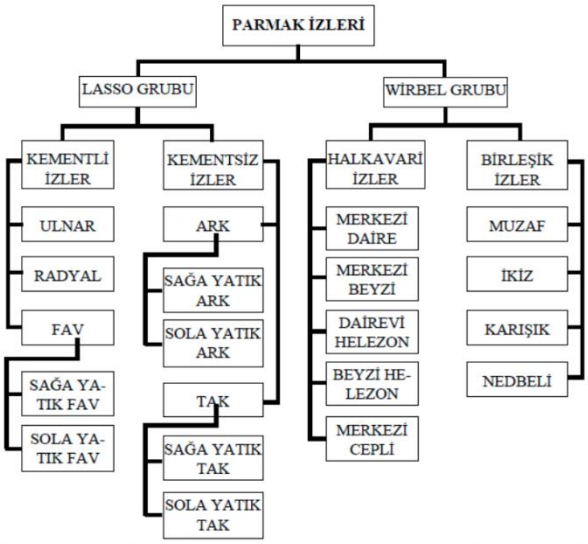
1.2. Parmak İzinin Sınıflandırılması

Parmak izleri temel olarak bazı özelliklere sahiptir. Bunlar, benzemezlik, değişmezlik ve sınıflandırılabilirliktir. Dünyadaki hiçbir insanın parmak izi birbiriyle aynı değildir. Bu özellik parmak izlerinin benzemezlik özelliğinin bir sonucudur. İnsan hayata geldiği andan öldüğü ana kadar aynı parmak izini taşımaktadır. Parmağın büyümesi ile parmak izinin boyutları büyüyebilir fakat karakteristik özelliğinden hiçbir şey kaybetmez. Çok büyük bir yangın, aside batırma, büyük kesikler parmak izinin yapısını bozabilmektedir.

Tasnif edilebilir özelliği ise özel bir formülasyon sistemiyle parmak izlerinin şekillerine bakılarak gruplara ayrılmasıdır. Bu gruplar kendi içerisinde çeşitli harf ve rakamlar ile kodlanabilmektedir. Bu gruplar kendi içerisinde harf ve rakamlar ile kodlanmaktadır. Formülize edilen unsurlar bir tasnif sistemi ile sıralamaya sokulmaktadır. 10 parmak, tek parmak, çift el parmak olarak formülize sistemleri bulunmaktadır. Gelişen teknoloji ile bu sınıflandırma sistemi yerini dijital sisteme bırakmıştır. Dijital sistemde verileri arşive kaydederek, olay yerinden elde edilen bir

parmak izi arşivde taratılıp veri tabanında karşılığının bulunması prensibine dayanmaktadır (Doğukan Ölmez, 2021).

Şekil 3: Parmak İzlerinin Sınıflandırılması (Doğukan Ölmez, 2021).



Parmak izlerinin sahip olduğu sınıflandırılabilme özelliği sayesinde, olay yerinden alınan izlerin ve arşivde bulunan izlerin karşılaştırılması tüm izlerle değil de yukarıdaki şekilde gösterilen gruplardan içine girdiği grupla karşılaştırılacağından kolaylaşmaktadır. Olay yerinden elde edilen bir izden tanımlama yapmak için ek olarak herhangi bir bilgisayar sistemine- yazılımına ihtiyaç duyulmayabilir, hatta uzman sadece on parmak kartını kullanmaya ve uzmanlığına da güvenebilir.

Parmak izleri, incelenmek için herhangi bir laboratuvara ihtiyaç duymazlar ve herhangi bir zarar meydana geldiğinde uzun bir süre sabit olarak kalabilirler (Komarinski, 2004). Bu özellikler, adli bilimler açısından bakıldığında, parmak izlerinin birincil delil olarak neden tercih edildiğinin en büyük göstergelerindendir.

1.3. Parmak İzinin Özellikleri

Dünyada şu ana kadar hiç kimsenin birbirine benzemediğini belirttiğimiz parmak izlerinin belli özellikleri bulunmaktadır. Bu özelliklerinden dolayı da en güvenilir

delillerden sayılmaktadır ve çözülen olaylarda en çok pay sahibi olan delillerden biri şüphesiz parmak izidir (Kolay, 2021).

1.3.1. Tasnif Edilebilme Özelliği

Parmak izinin tasnif edilebilme özelliği, belirli özelliklerine göre belirli gruplara bölünerek sınıflandırılabiliyor olmasıdır. Bu özelliğin artısı ise parmak izinin arşivlenmesi ve kodlanmasının kolaylaştırılmasıdır (Richard Saferstein, 2021).

1.3.2. Benzemezlik Özelliği

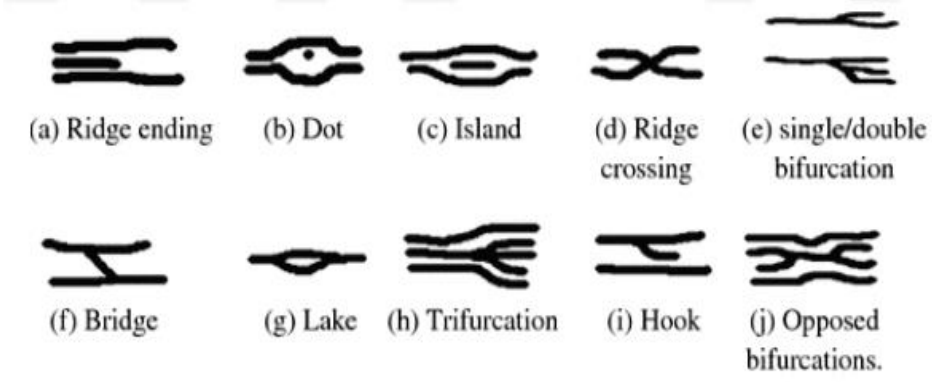
Parmak izleri ilk bakışta görünüş olarak birbirine benzese de bazı özellikleri kendi içerisinde sınıflandırılabilmesi ve kişiye özgü olabilmesini sağlamaktadır. Bu özelliklerin başında çatal, hat sonu, hat başı gibi özellikler gelmektedir. Değişkenlik göstermekle beraber dünya literatüründe kabul görmüş olan genel kurula göre, her iki parmak izinin eşleştirilebilmesi için en az on altı özelliğin iki izde de ortak olarak bulunması gerekmektedir (E. Hülya Yükseloğlu, 2008).

1.3.3. Değişmezlik Özelliği

Parmak izleri dış etkenlerle tahrip olmadıkça, kişinin büyümesi ve gelişmesiyle değişime uğramazlar ve oluştuğu zamandan yok olduğu zamana kadar değişmeden kalabilirler.

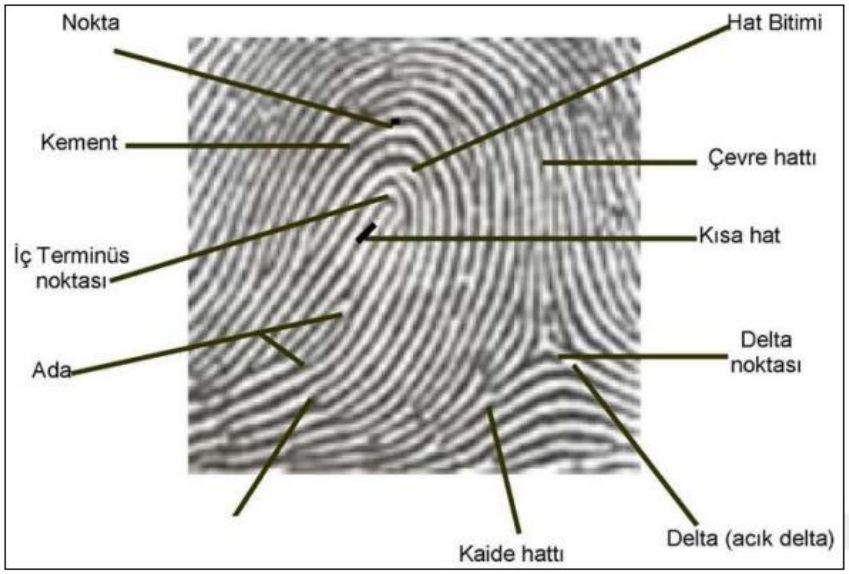
1.4. Parmak İzi Eşleştirmesinde Kullanılan Özellikler

Parmak izleri olay yerinden uygun bir biçimde alındıktan sonra, uzman tarafından AFIS sistemi kullanılarak mukayese edilir ve eşleştirilir. Uzman, parmak izinde olması gereken özellikleri her iki parmak izinde arar ve bu özellikleri konumu, sayısı vb. özelliklere göre eşleştirir. Bu özellikler temel olarak çatal, ada, müstakil hatlar,



kanca, kement olarak karşımıza çıkar (Cantürk, 2019). Bu özellikler şekilsel olarak aşağıdaki gibidir:

Şekil 4: Parmak izlerinde bulunan özellikler (Cantürk, 2019).



Şekil 5: Parmak izindeki karakteristik noktalar (Gül, 2014)

Açık delta: Parmak izini çevreleyen çevre hattı ile kaide hattının birbirinden ayrılmasıyla meydana gelen şekle denir.

Kapalı delta: Parmak izini üstten çevreleyen çevre hattı ile alttan çevreleyen kaide hattının izin merkezine yakın yerdeki birleşmesine denir.

Delta ağzı: Birbirine paralel iki papil (çevre hattı ile kaide hattı) hattının birbirinden uzaklaştığı yere denir.

Delta noktası: Kapalı deltalarda çevre hattı ile taban hattının (kaide hattı) birleştiği yere denir.

Kement: Papil hatları parmağın bir tarafından girip merkezde dönüş yaptıktan sonra aynı yönde çıkması ile meydana gelen şekle kement denir.

Yarım daire: Birbirine paralel iki papil hattının dönüş yapmaya başladığı nokta ile dönüşün bittiği nokta arasında kalan yaya denir.

Düz hat: Kementli izin merkezinde oluşan iç kementin ve yarım dairenin içine giren, ucu müstakil papillere denir.

İç terminüs noktası: Parmak izinin papil sayımlarına esas olacak en içteki noktasıdır. Merkez şekillerine göre farklılıklar gösterirler.

Nokta: Bir veya en fazla iki porun birleşmesinden oluşan şekildir.

Kesik Çizgiler: Papil hattının devam ederken aynı kalınlıkta kesilip aynı kalınlıkta devam etmesi durumudur. Bu durumda papil bozulmadan devam etmiş sayılır.

Ada: Bir papilin yoluna devan ederken ikiye ayrılıp bir süre sonra tekrar birleşmesiyle oluşan şekle denir.

Köprü: Paralel iki papilin, kısa bir papil hattıyla birleşmesi sonucu oluşan şekle denir.

Kanca: Bir papilin yan tarafından kanca görünümü veren küçük bir papil çıkıntısının oluşturduğu şekle denir (Gül, 2014).

1.5. Parmak İzi Tipleri

1.5.1. Görünür Parmak İzleri

Görünür parmak izleri isminden de anlaşılacağı gibi, olay mahallinde çıplak gözle direk olarak -herhangi bir ışık kaynağı veya yöntem kullanmaksızın- görülebilen parmak izleridir. Bu parmak izleri gerçekleşen olayın niteliğine göre kanlı, yapışkan yüzeye dokunma sonucu oluşmuş veya eski pencerelerde bulunan camı tutan macun üzerinde bulunabilir (Richard Saferstein, 2021).

1.5.2. Görünmez (Latent) Parmak İzleri

Görünmez parmak izleri olay yerlerinde en sık karşılaşılan parmak izleridir. Tahmin edileceği üzere parmak izleri dokunulan her yüzeye yukarıda anılan kimyasal özellikleri sayesinde bulaştığından, her yerde olabilirler. Ancak çıplak gözle görülemediklerinden, görünmez parmak izleri olarak adlandırılırlar. Bu tip izlerin bulunması olay yeri inceleme uzmanının olayın niteliğine göre parmak izlerinin bulunacağı yüzeyleri ışık kaynağı kullanarak ve gerekli yöntemleri kullanarak keşfetmesi ve görünür hale getirilmesiyle tespit edilirler (Richard Saferstein, 2021).

1.5.3. Kabartma (3 boyutlu) Parmak İzleri

Kabartma parmak izleri, olay yerinde bulunabilecek (macun gibi) kıvamlı maddelere dokunulması sonucu, parmaklarımızda bulunan ve parmak izi desenimizi oluşturan ve aslında anıldığı gibi parmak yüzeylerinde sürtünmeyi artırarak tutunmamızı sağlamak amaçlı evrimleşmiş kıvrımların, bu kıvamlı yüzeye tutunması sonucu kıvamlı yüzeyde orijinal kabartma desenini aktarmasıyla oluşan izlerdir. Bu tip yüzeylerde oluşan parmak izleri aynı zamanda görünür parmak izlerine de örnektir. Eski tip pencere camında bulunan macunlar, henüz donmamış bir beton gibi maddelere dokunulması sonucunda meydana gelirler (Richard Saferstein, 2021).

İKİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMININ DOĞUŞU VE KAPSAMI

2.1. Kişisel Verilerin Ve Korunması İhtiyacının Doğuşu

Tarihin bilinen ilk dönemlerinden bu yana insanlar, merak duygusu ile bilmeyi istemiştir. Toplumların ilk dönemlerinde insanların yaşayışları, kabile, koloni gibi küçük çaplı yaşam alanlarına dayanmaktadır. Hatta aynı odada, aynı çadırda bir yaşam mevcuttur. Böyle bir yaşam içerisinde yaşayanların birbirleri hakkında bilmedikleri pek bir şeyin kalmayacağı da aşikardır.

Ancak toplumların yaşam biçimleri değiştikçe, özellikle dünyada teknolojinin de gelişimiyle birlikte sanayi toplumları oluştukça, öncelikle otorite olan devletin ve akabinde işverenin, kar amacı güden işletmenin vs., her bir bireyi gözetim altında tutma isteği gelişmiştir. O zaman; kişisel verilerin korunması hukukunun oluşmasında temelde üç etkinin bulunduğu söylenebilir;

a. çeşitli örgütlerce kişisel verilere duyulan ihtiyaç,

b. teknolojik ilerlemeler ve

c. gözetim teknolojilerindeki gelişmeler nedeniyle duyulan kaygı. (Küzeci, 2018)

"Modernleşme" olarak da adlandırılabilecek bu süreç "aralarında eşgüdüm sağlanmış çok sayıda görevin hizmetindeki tek bir merkezden gelen bilgiyle harekete geçen ve o merkezce yönetilen bir makine" olarak tanımlanabilecek modern devleti ortaya çıkarmıştır (Poggi, 2019).

Merkezi yönetimi sağlayabilmek için hüküm sürdüğü alanın en ücra köşelerine kadar uzanmış bürokratik kollarıyla bu karmaşık mekanizma, ilk ortaya çıktığı günden beri yurttaşlara ilişkin bilgilere gereksinim duyar (Küzeci, 2018).

Bu gereksinim, modernleşmenin bir gereği olduğu gibi devletin yönetim tekelinin, yönetim stratejileri ve planlamalarının gerçekleştirilmesinin de bir gereğidir. Zira toplumsal yaşama düzenine ilişkin kuralların belirlenmesi, bu kurallara uyulmamasının yaptırımlarının belirlenmesi ve uygulanması, vergilendirme, verginin toplanması, ticari ilişkiler, diplomatik ilişkiler, askeri ilişkilerin düzenlenmesi, bilgiye olan ihtiyacı beraberinde getirmektedir. Bu ihtiyaç doğrultusunda kişisel veriler toplanır, kaydedilir ve devlet bürokrasisi oluşturulur.

Öncesinde bu denli basit bir yapıda olan kişisel veri işleme faaliyetleri, bilgisayarların ve veri bankalarının ortaya çıkışı ile birlikte önemli bir değişim göstermiş, akabinde internetin ortaya çıkması ve yaygınlaşmasıyla ise büyük dönüşümünü gerçekleştirmiştir.

Bu dönemde "veri" her şeyin merkezine konmuştur. Zira daha önce de veri toplama yoluyla kişiler ayrıştırılabilmekteyse de bilgisayarın gelişmesi ile birlikte çok sayıda verinin kaydedilmesi sağlanabilmiş, daha da önemlisi bu veriler, birbirleri ile ilişkilendirilebilir hale gelmiştir. Bilgisayarların son 30 yılda gelişimi ile birlikte, nicelik olarak tahmin edilmesi mümkün olmayacak kadar verinin bir arada tutulduğu veri bankaları da oluşmaya başlamıştır. Bu kadar çok veri içinde bilgiye ihtiyaç duyan açısından kullanışlı verinin bulunulabilir olması açısından da "veri madenciliği" yolu geliştirilmiştir.

Bilgisayar kullanımının bahse konu son dönemde yaygınlaşması ile birlikte veriye ulaşma çok daha kolay bir hal almış, dolayısıyla kişisel verinin korunması ihtiyacı da artmıştır.

İnternetin ortaya çıkması ve yaygınlaşması ile birlikte ise veri sahibinden bilinçli olarak veri toplamanın yanı sıra bilinçsiz veri toplama faaliyetleri de gelişmiştir. Diğer bir deyişle, internet sitelerini kullanan kullanıcılar, örneğin üye olmak yoluyla kişisel verilerini kendi rızaları ile toplayıcıya sunarken, internette herhangi bir sayfayı gezerken IP adresi takibi, çerez kullanımı gibi yollarla kullanıcının haberi dahi olmadan kişisel verileri elde edilebilmektedir. Öyle ki, bilgisayar kullanımı sırasında kullandığımız farenin tüm hareketleri ile kişisel eğilimlerimiz ortaya çıkarılmakta, kullanıcıya ait bir profil oluşumu sağlanabilmektedir (Özdilek, 2008).

Görüldüğü üzere, modernleşme ile başlayan otoritenin gözetim isteği doğrultusunda veri toplama faaliyeti, günümüzde sadece otoritenin değil bilişim teknolojilerini kullanan tüm yapıların, kolayca kullanılabilir bir faaliyet alanına dönüşmüştür.

Diğer yandan teknolojik gelişmeler, bir verinin sağladığı bilgiye yönelik olarak da çeşitliliğin artmasını sağlamıştır. Örneğin kişinin DNA verisi günümüzde veri sahibinden başlayarak çok daha fazla kişinin kişisel verilerine ulaşmayı olanaklı hale getirmektedir.

Dolayısıyla bu denli büyük teknolojik gelişmelerin altında bireyin kişilik haklarının, özel hayatın korunmasına yönelik haklarının ezilmemesi adına kişisel verilerin korunmasına yönelik düzenlemeler doğmuştur.

2.2. Kişisel Veri Tanımı Ve Tanımın Kapsamı

2.2.1. Kişisel Verinin Tanımı

Kişisel veri kavramı, geçmiş dönem uluslararası düzenlemelerden günümüze kadar benzer tanımlar üzerinden gelişme göstermiştir.

Avrupa Birliği tarafından 95/46/EC sayılı yönergenin yerini almış olan ve 25 Mayıs 2018 tarihinden itibaren yürürlüğe girerek tam etkilerini doğurmaya başlayan Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) amaçları doğrultusunda geçerli saydığı kişisel veri ve veri sahibi tanımı 4. maddesinde hüküm altına almıştır. Buna göre; *"'kişisel veri' tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir ('veri sahibi'); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum*

verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir."

Uluslararası düzenlemeler ışığında gelişen 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bu Kanun ile ilgili Yönetmeliklerde bulunan tanım da aynı doğrultuda oluşmuştur; *"Kişisel veri; kimliği belirli yada belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder"*. Buradan hareketle; kişisel verinin varlığından bahsedebilmek için bir verinin olması, bu verinin belirli bir kişiye ait olmayan bir bilgi içermesi halinde dahi kişiyi belirli ya da belirlenebilir kılması, verinin gerçek bir kişiye ait olması gerektiği anlaşılmaktadır.

2.2.2. Özel Nitelikli Kişisel Veri

Uluslararası düzenlemelerden başlamak üzere direkt olarak kişinin temel hak ve özgürlüklerini etkileyen ve bu nedenle kötüye kullanma halinde kişide yaratacak mağduriyetin çok daha ağır olacağı düşüncesi ile ve Kişisel Verilerin Korunması Kanunu'nun gerekçesinden anlaşılacağı üzere ayrımcılığa mahal vermemek adına bazı verilerin özel nitelikli veri olarak değerlendirilmesi öngörülmüştür. Nitekim Kişisel Verilerin Korunması Kanunu'nun 6. Maddesinin birinci fıkrası özel nitelikli kişisel verileri sınırlı sayılı olarak hüküm altına almıştır; *"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."*

Özel nitelikli kişisel veri ayrımı, kişisel verinin işlenme amacına yönelik olarak da değerlendirilmelidir. Zira madde lafzına istinaden özel nitelikli kişisel veri gibi görünmemekle birlikte, tıbbi bir diyet programı hazırlamak amacıyla elde edilen boy ve kilo bilgisi sağlık verisi oluşturacağından özel nitelikli kişisel veri olarak değerlendirilecektir.

Diğer yandan çalışma konumuz olan parmak izi de madde metninde ortaya konmuş biyometrik veri kategorisine girmektedir. Ancak, bu hususta da günümüz teknolojilerinin getirdiği ve parmak izinin de biyometrik verinin çok ötesinde, genetik veriye yaklaşan bir veri olduğu kabul edilmelidir. Parmak izi delilinin günümüz

teknolojileri ile gelişimine ilişkin yukarıda yapılan açıklamalar ışığında, artık parmak izi delilinden DNA verisi elde edilebildiği düşünüldüğünde, biyometrik delilin aksine Ceza Muhakemesi Kanununda özel olarak korunan genetik veriler gibi korunma ihtiyacı olduğu aşikardır.

2.2.3. Kişisel Veri Kavramının Kapsamı

6698 sayılı Kişisel Verilerin Korunması Kanununun 3. maddesinde tanımlanan kişisel veri kavramı, Kanun gerekçesinde daha ayrıntılı olarak açıklanmaya çalışılmıştır; *"Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Yalnızca ad, soyad, doğum tarihi ve doğum yeri gibi kişinin kesin teşhisini sağlayan bilgiler değil, kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Bu durum, kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar."*

Madde gerekçesi ile kişisel veri tanımı, daha geniş kapsamlı olarak ele alınmış gibi görünse de çok geniş ve sınırlı sayıda sayılması mümkün olmayan bir kavram olması nedeniyle ayrıntılı açıklamaya muhtaçtır. Bu doğrultuda, kişisel veri kavramını daha iyi anlamak adına 6698 sayılı Kişisel Verilerin Korunması Kanununun 3. maddesinde mevcut tanımı, yapısı içinde incelemek faydalı olacaktır.

2.2.3.1. Bir Verinin Bulunması Gereklidir

6698 sayılı Kanun anlamında veri, bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli, belli bir kimsenin kimliği, etnik kökeni, fiziksel özellikleri, sağlık, eğitim, istihdam durumu, cinsel yaşamı, aile hayatı, başkaları ile yaptığı haberleşmeler, ikamet adresi, kredi kartı, kişisel düşünce ve inançları, dernek ve sendika üyelikleri, alışveriş alışkanlıkları gibi hususları da kapsayan ve ancak sınırlı sayıda sayılamayacak dijital olan yada olmayan her türlü bilgiyi kapsar.

Burada bahsedilen verinin, gizli olması ya da gizli kalması gereken bir veri olması gerekmez. Hatta bu veri, kişisel veri içeren bir belgenin hazırlayıcısına dahi ait olabilir. Önemli olan, eldeki veri ya da veriler doğrultusunda kişinin belirli ya da belirlenebilir olmasıdır.

2.2.3.2. Verinin, Kimliği Belirli ya da Belirlenebilir Hale Getirmesi

Bir verinin, ilgilisinin kimliğini belirlemesi ya da belirlenebilir hale getirmesi halinde bu veriler kişisel veri olarak değerlendirilir. Kişinin kimliğini belirlemeye yönelik akla gelen ilk veri isim, soyisim gibi verilerdir. Bu veriler ile başkaca bir veriye ya da veriyi anlamlandıracak bir altyapıya ihtiyaç duyulmaksızın kişi belirlenebilir olmaktadır.

Ancak direkt olarak kişinin kimliğini belirli kılan bu tür veriler dışında başkaca veri ya da veri grupları ile birlikte değerlendirildiğinde kişiyi belirlenebilir hale getiren veriler de kişisel veri olarak değerlendirilmektedir. Örneğin kişinin kimlik numarası tek başına kişinin kimliğini belirlenebilir hale getirmez. Ancak kimlik numarasının bir sisteme girilmesi ile kişinin kimliği belirlenebilir hale gelir. Yine hiçbir isim, kimlik numarası, yaş, fiziki özellik olmaksızın sadece bir doktorun görev yaptığı bir ilçede *"doktor bey/hanım"* tabiri dahi dolaylı olarak kişinin kimliğini belirlenebilir hale getirir.

Bu anlamda belirlenebilir olma, sadece bir kişi tarafından belirlenebilir olmayı yeterli kılar. Bunun için kişisel veriye sahip herkes için belirlenebilir olma beklenmemekte, bir kişi ya da grup yada kesim tarafından belirlenebilir olmak yeterlidir. Yukarıda verilen örnekte olduğu gibi sadece bir doktorun görev yaptığı bir ilçede *"doktor bey/hanım"* tabiri sadece o ilçede yaşayanlar tarafından belirlenebilir olmasına karşın kişisel veri olarak kabul edilir.

Belirlenebilir olmayı, kişinin kimliğinin tam anlamıyla ortaya çıkarılması olarak da değerlendirmemek gerekir. Zira, kişiye özel davranış şekilleri belirlenmesini sağlamaya yönelik olarak kişiyi diğer kişilerden ayrıştırmaya yarayacak her türlü veri de kişisel veridir. Bu bağlamda kimlik verisini açıkça ortaya koymamakla birlikte kişiyi diğer kişilerden ayrıştıran IP adresleri, bir web sitesinin ziyaret edilmesi ile kişinin o web

sitesindeki çalışma ve gezinme alışkanlıklarının sistematik şekilde elde edilmesi de kişisel veri olarak değerlendirilmektedir.

Verinin kişiyi belirlenebilir hale getirmesi, görüldüğü üzere çok çeşitli şekillerde olabileceği gibi teknolojik gelişmeler doğrultusunda da sınırsız bir şekilde uygulanabilir olduğu düşünülmektedir. Ancak burada Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) verinin kişiyi belirlenebilir hale getirmesine yönelik olarak "makul olasılık" ilkesini benimsemektedir. Buna göre kişisel veri sahibinin birden çok verinin bir araya getirilmesi yolu ile belirlenebilmesi makul şartlarda mümkün ise burada kişisel verinin varlığından bahsedilebilecektir. "Makul olasılık" her bir uygulamanın kendi şartları içinde değerlendirilmeli ve her uygulamanın kendi şartları içinde makul sayılabilecek olasılıklar göz önünde bulundurulmalıdır.

2.2.3.3. Verilerin Kişiyle ya da Kişiye Bağlı Nesnelere İlişkin Olması

İsim, soyisim, kimlik numarası gibi kişinin kimliğini tam olarak ortaya koyan veriler incelendiğinde, bu veriler doğrultusunda kişisel verinin tanımında belirtildiği gibi belirli ya da belirlenebilir olma halinin kolaylıkla tespit edildiği görülecektir. Veri ile kişi arasındaki bu bağ, genel olarak veri ile kişinin arasındaki açık kişisel ilgisinden kaynaklanır. Bu da verinin kişisel veri olarak değerlendirmesini sağlar.

Bunun yanında eldeki verinin kişi ile ilgisi olmamakla birlikte nesnelere ilişkin olması halinde dahi kişisel verinin varlığından söz edilebilir. Zira veri, her ne kadar nesnelere ilişkin olsa da nesnenin belirli ya da belirlenebilir bir kişi ile bağının mevcut olması halinde bu kez nesne ile kişi arasındaki bağ, eldeki verinin kişisel veri olarak değerlendirilmesini sağlamaktadır. Örneğin araç plakası verisi nesneye ilişkin olmakla birlikte plaka sahibini belirli ya da belirlenebilir kıldığından dolayı araç plakası da kişisel veri olarak değerlendirilecektir.

Burada nesneler üzerinden elde edilen verilerin kapsamının ölçüsüzce genişletilmemesi gerekir. Buna ilişkin olarak da Avrupa Veri Koruma Kurulu'nun kriteri, bilginin kişinin kimliğine, karakterine veya davranışlarına gönderme yapıyorsa ya da bilginin, kişinin nasıl bir ayrıma tabi tutulacağına yönelik belirlemede kullanılıyorsa, bilginin kişiye ilişkin olduğu yönündedir. Nesneye yönelik verinin bu kapsamda değerlendirilmesi gerekmektedir.

2.2.3.4. Verinin Gerçek Kişiye Ait Olması

Gerek Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) gerek ulusal mevzuatlar doğrultusunda kişisel veri, sadece gerçek kişilere ilişkindir. Tüzel kişilere ilişkin unvan, fiziki ve dijital adres, telefon numarası gibi veriler kişisel veri olarak kabul edilemez.

Ancak tüzel kişiliğe ait olmakla birlikte kişisel verinin tanımında yer alan kişiyi belirli ya da belirlenebilir hale getirmeye uygun verilerin kişisel veri olarak kabulü gerekir. Yani tüzel kişiliğe ilişkin bir bilgi, tüzel kişiliğe ait olmaktan çıkıp yine gerçek bir kişi ile ilişkilendirildiğinde kişisel veri olarak kabul edilebilecektir.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN KAYNAKLARI

3.1. Uluslararası Kaynaklar

3.1.1. OECD

OECD, İktisadi İş Birliği ve Gelişme Teşkilatı, ikinci dünya savaşı sonrasında Avrupalı ülkelerin her alanda yaşadığı olumsuzlukların sonuçlarının bertaraf edilmesi ve üye devletlerin ekonomik istikrarının sağlanması, sanayileşmenin teşviki, işsizliğin azaltılması, yönetimlerin demokratikleşmesi ve insan haklarına bağlı yapılar oluşturulması amacıyla, Türkiye'nin de içerisinde yer aldığı 19 ülkenin katılımıyla 1961 yılında kurulmuştur.

Teşkilatın kişisel veriler yönünden çalışmaları, uluslararası bankacılık ve sigortacılık faaliyetlerinin yürütülmesinde, sektörel sıkıntıların giderilmesi açısından başlamıştır. Bu çalışmaların ilk meyvesi ise 1980 yılında Teşkilat tarafından kabul edilen ve üye ülkelerin iç hukuklarına uyarlanması tavsiye edilen "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler"dir.

Sekiz ana ilkeden oluşan Rehber İlkeler gereğince veri, hukukun temel ilkeleri ışığında dürüstlük kuralına uygun olarak veri sahibinin rızası ile toplanmalı, veriler en geç toplanma anında belirli bir amaç doğrultusunda kullanılması ve amaca uygun olmalıdır. Veriler rıza dışı paylaşıma konu edilmemeli, yetkisiz erişime karşı azami bir

koruma sağlanmalı ve veriyi saklayanın veri sahibine karşı sorumlu olduğu kabul edilmelidir.

2013 yılında ana ilkeler yeni birtakım düzenlemelerle güncellenmiştir. Güncellenmiş hali ile dahi tavsiye niteliğinde kalması olumsuz bir yan olarak değerlendirilse de kendisinden sonra gelen düzenlemelere ışık tutması yönünden önemli bir çalışmadır.

3.1.2. Birleşmiş Milletler Düzenlemeleri

BM kuruluş tüzüğü incelendiğinde, kuruluş taahhütlerinin dünya barışını sürdürmek, toplumlar için sosyal hakların ve özgürlüklerin arttırılması ve uluslararası iş birliğinin sağlanması olduğu görülmektedir.

Bununla birlikte insan haklarını ilgilendiren çalışmalarda yürütülmüş ve bu husus örgüt tüzüğünün dört ana amacından biri olarak kabul edilmiştir. Buna istinaden 1948 tarihinde örgütün ilk uluslararası düzenlemelerinden olan "Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi" düzenlenmiştir. Bu bildiri insan hakları açısından kendinden sonra düzenlenen tüm metinlerin ana referans kaynağı olmuş, sahip olduğu ilkeler kendinden sonraki metinlerde geliştirilerek düzenleme altına alınmıştır.

Birleşmiş milletlerin doğrudan kişisel verilere ilişkin en önemli düzenlemesi ise 1990 tarihinde genel kurul tarafından kabul edilen Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber ilkelerdir. Bağlayıcı olmamakla birlikte tüm devletler açısından iç hukuk düzenlemelerinin gerçekleştirilmesini sağlamak adına yol gösterici niteliktedir. Bu ilkeler genel itibari ile kamu ve özel sektör açısından düzenlemeler içermesi sebebiyle kapsamı da oldukça geniştir. Yine rehber ilkelerin önemli bir özelliği de konuya ilişkin düzenlemelere uyulup uyulmadığına noktasında bir denetim mekanizmasının da kurulmasını ön görmesidir.

Kişisel verilere ilişkin olarak da rehber içeriğinde dokuz prensip belirlenmiştir. Bunlar: hukukilik ilkesi doğruluk ilkesi, amacın belirli olması ilkesi, ilgilinin verilere erişiminin sağlanması ilkesi, ayrımcılığı önleme ilkesi, denetim ve yaptırım ilkesi, güvenlik ilkesi, istisna düzenleme ilkesi ve sınır ötesi veri akışı ilkesidir.

3.1.3. Avrupa Konseyi Düzenlemeleri

Avrupa Konseyi'nin kuruluş tüzüğünde belirtilmiş olan amaçları özetle hukukun üstünlüğü, insan hakları ve çoğulcu demokrasi ilkelerini korumak ve güçlendirmek, ayrımcılık, yabancı düşmanlığı, ırkçılık gibi sorunlara çözüm aramak, Avrupa çok kültürlülüğün oluşması ve gelişmesini sağlamak olarak sıralanmıştır. Bu amaç kapsamında Avrupa konseyi üye devletler arasında hukuki bir denklik yaratmayı amaçlamış ve mütekabiliyet esaslı hukuk birliğine zemin oluşturmuştur.

Kişisel verilerin korunması hususunda ise Konseyi'nin yaptığı düzenlemeler sırayla İnsan Hakları Avrupa Sözleşmesi, 108 Nolu Sözleşme, 181 Sayılı Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar Ve Sınır Aşan Veri Akışına İlişkin Protokol Ve Bakanlar Komitesi Tavsiye Kararlarıdır.

3.1.3.1. Avrupa İnsan Hakları Sözleşmesi

Avrupa insan hakları Sözleşmesi Türkiye'nin de dahil olduğu Avrupa konseyine üye devletler tarafından 4 Kasım 1950 tarihinde imzalanmıştır. Türkiye Cumhuriyeti tarafından da 10 Mart 1954 tarih ve 6366 sayılı onay kanunu ile iç hukukta da geçerlilik kazanmıştır.

Avrupa insan hakları sözleşmesinin kişisel verilerin korunması hakkını doğrudan koruyan tek düzenlemesi sekizinci maddesidir. Bu nedenle Avrupa insan hakları Mahkemesi de kişisel verilerin korunmasına ilişkin önüne gelen uyuşmazlıkları bu madde özelinde ele almaktadır. Madde metni şu şekildedir;

Madde 8 Özel Ve Aile Hayatına Saygı Hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın

veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

Avrupa insan hakları sözleşmesinin bu maddesi henüz Türkiye'de kişisel verilerin korunmasına ilişkin bir hukuki düzenleme yokken dahi Türkiye cumhuriyeti Anayasası'nın temel hak ve özgürlüklere ilişkin milletlerarası sözleşmelerde kanunların farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası anlaşma hükümlerini esas alan düzenlemesi nedeniyle kişisel verilerin korunması düzleminde bağlayıcı bir nitelik kazanmıştır.

3.1.3.2. 108 Nolu Sözleşme

Avrupa konseyi 1970 li yılların başlarından itibaren kişisel verilerin korunması ile ilgili çalışmalarını başlatmıştır. Bu çalışmalar ışığında Avrupa Konseyi Bakanlar Komitesi kişisel verilerin daha etkin bir şekilde korunmasının sağlanması amacıyla öncelikle Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar ve hemen akabinde Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar kabul etmiştir. Bu iki karar 108 nolu sözleşmenin de bir nevi çıkış yolu olarak görülmektedir.

Bu kez 1981 tarihinde 108 nolu sözleşme olarak da anılan ve kişisel verilerin korunmasını ilişkin düzenlemeler içeren ilk uluslararası belge niteliğindeki kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme kabul edilmiştir. Bu sözleşme sözleşmeyi imzalayan devletler özelinde ve kişisel verilerin korunması hususunda hukuki olarak bağlayıcı ilk devletler arası metin olarak tarihte yerini almıştır.

Türkiye ise sözleşmeyi imzalayan ilk devletler arasında yer almışsa da 2016 yılına kadar sözleşmeyi iç hukuka dahil edecek düzenlemeleri gerçekleştirmemiştir.

3.1.4. Avrupa Birliği Düzenlemeleri

Kişisel verilerin korunmasının başlangıcının gerçekleştirildiği yer olarak nitelendirilebilecek Avrupa'da, bu alanda hem Avrupa Birliği (AB), hem de ulusal hukuk sistemleri düzeyinde oldukça kapsamlı bir mevzuat bulunmaktadır. Almanya'nın Hessen eyaletinde ilk yasal düzenlemenin yapıldığı zamandan bu yana bölgede kişisel verilerin korunması hukuku yayılmış, gelişmiş ve olgunlaşmıştır. Konuya ilişkin devam eden sorunlara çözüm bulma arayışı ise halen sürmektedir.

Konumuz bakımından Avrupa Birliği bünyesnde oluşturulan en önemli düzenleme, Avrupa Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli 2016/680 sayılı, kişisel verilerin yetkili merciler tarafından suç işlenmesinin önlenmesi, işlenen suçların tespiti, araştırılması, kovuşturulması ve ceza mahkumiyetlerinin infazına ilişkin direktifidir.

2016/680 sayılı Direktif'in düzenlediği alanın nispeten yeni olması, GDPR'a ilişkin tartışmaların gölgesinde kalmasına neden olmuştur. GDPR daha ziyade özel hukuk ilişkilerine ilişkin iken, 2016/680 sayılı Direktif, özellikle üye devletlerin ve kolluk güçlerinin veri işlemelerine ilişkin düzenlemeler içermektedir.

Bu Direktif'in, kişisel verilerin korunması hakkı ile suçların önlenmesi ve aydınlatılmasındaki menfaat arasında bir denge kuracağı, kolluk güçleri arasındaki işbirliğini kuvvetlendireceği belirtilmektedir.

3.2. Ulusal Kaynaklar

3.2.1. Türkiye Cumhuriyeti Anayasası

Bugün yürürlükte olan 1982 tarihli Türkiye Cumhuriyeti Anayasası, 1980 yılında yapılan askeri darbenin ardından kurulan Kurucu Meclis tarafından anti-demokratik bir ortamda hazırlanmış ve 9 Kasım 1982'de yürürlüğe girmiştir.

Yukarıda bahse geçen Avrupa konseyi 108 nolu sözleşmesinin imza tarihi 1982'den önce olmasına karşın Türkiye Cumhuriyeti Anayasası'nın ilk halinde kişisel veriler noktasında bir düzenleme bulunmamaktadır. Kişisel verilerin korunması ibaresi ile kendisine yer bulduğu dönem ise ancak 2010 yılında olacaktır. 2010 yılında yapılan

Anayasa değişikliği ile kişisel verilerin korunması hakkı doğrudan Anayasanın 20. Maddesine ekleme yapmak suretiyle anayasa içinde kendine yer bulmuştur.

3.2.2. Kişisel Verilerin Korunması Kanunu

Her ne kadar 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ile kişisel verilere ilişkin kapsamlı bir koruma gerçekleştirilmişse de bu tarihten önce kişisel verilerin hiçbir koruma altında olmadığını söylemekte mümkün değildir. Zira kişilik haklarını koruyan Medeni Kanun, ticari ve bankacılık özelinde sırların korunmasına yönelik hükümleri ile Türk Ticaret Kanunu ya da iş yaşantısı içerisindeki veri akışını düzenleme altına alan İş Kanunu sınırlı da olsa bir koruma sağlamaya çalışmıştır.

Ancak elbette 6698 sayılı yasa ile gerek imzamız bulunan uluslararası sözleşmelerle uyumlu bir kişisel veri yasasının oluşması gerek kişisel verilerin korunması hukuku açısından ilk düzenlemelerden günümüze her daim altı çizilmiş amaç unsurunun öne çıkartılması son derece önemlidir.

DÖRDÜNCÜ BÖLÜM

6698 SAYILI KANUNDA YER ALAN TEMEL KAVRAMLAR

4.1. Kişisel Verilerin İşlenmesi

Kişisel Verilerin Korunması Kanunu'nun "Tanımlar" başlıklı 3. maddesinde kişisel verilerin işlenmesi; *Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem* olarak ifade edilmektedir.

Kanunda mevcut tanımda belirtilen otomatik işleme; bilgisayar, telefon, saat vb. işlemci sahibi cihazlar tarafından yerine getirilen, yazılım veya donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyetidir.

Yukarıda belirtildiği gibi, kişisel veriler otomatik işlemeye tabi tutulmasalar da, "veri kayıt sistemi" aracılığıyla işlendiklerinde de Kanun hükümlerine tabi olacaklardır. Kanunda veri kayıt sistemi, "kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi"ni ifade etmektedir. Bu sistemler elektronik yahut fiziki ortamda oluşturulabilir. Buna göre, örneğin veri kayıt sisteminde kişisel veriler, ad, soyad veya kimlik numarası üzerinden sınıflandırılabileceği gibi, kredi borcunu ödemeyenlere ilişkin oluşturulacak sınıflandırma da bu kapsamda değerlendirilebilecektir. Kanun, otomatik olmayan yollarla veri işlenmesini tamamen Kanun kapsamı dışında tutmamaktadır. Yani, otomatik olmayan yolla veri işleme eğer veri kayıt sisteminin parçası ise, bu durumda veri işleme faaliyeti Kanun kapsamında kabul edilecektir.

4.2. İlgili Kişi

Kanun tarafından yalnızca gerçek kişilerin verilerinin korunması öngörüldüğünden "ilgili kişi" tabiri ile kişisel verisi işlenen gerçek kişinin anlaşılması gerekir.

Kanunda yer alan kişisel verinin tanımı gereği, tüzel kişiye ait bir verinin herhangi bir gerçek kişiyi belirlemesi ya da belirlenebilir kılması halinde, bu veriler Kanun kapsamında koruma altındadır. Ancak burada korunan menfaat tüzel kişiye değil, düzenlemenin temellendirdiği öncelik gereği belirlenen ya da belirlenebilecek gerçek kişiye ait olacaktır.

Örneğin; bir elektronik ticaret sitesinin müşterilerine ilişkin işlenen kişisel veriler bakımından ilgili kişi, müşteridir.

4.3.Veri Sorumlusu

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Örneğin; bir şirket bünyesinde yer alan birimlerin tüzel kişiliği bulunmadığından, bu birimlerin veri sorumlusu olması mümkün değildir. Bununla birlikte, bir şirketler topluluğunu oluşturan her bir şirket tüzel kişiliğe sahip olduğundan, bu şirketlerin her biri ayrı ayrı veri sorumlusudur. Burada veri sorumlusundan kastedilen bizzahati tüzel kişiliğin kendisidir.

4.4. Veri İşleyen

Veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiler olarak tanımlanmaktadır. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen, veri sorumlusu organizasyonu dışında çalışan gerçek ve tüzel kişilerdir. Başka bir ifade ile veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişidir.

Örneğin; bir şirketin verilerini saklamak amacıyla hizmet satın aldığı bulut sağlayıcıları veri işleyendir.

Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu hem de veri işleyen olabilir. Örneğin, bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.

4.5. Açık Rıza

Kanunun 3. maddesinde açık rıza; "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlanmıştır. Kanun çerçevesinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır. Açık rıza açıklamasının bir diğer önemi de veri işleyene gerçekleştireceği fiil konusunda yol göstermesidir. Kişi açık rıza açıklaması ile aslında veri sorumlusuna kendi hukuksal değerine ilişkin verdiği kararı bildirmiş olmaktadır. Açık rıza açıklaması, ilgili kişinin, işlenmesine izin verdiği verinin sınırlarını, kapsamını ve gerçekleştirilme biçimini de belirlemesini sağlayacaktır. Açık rızanın bu anlamda, rıza veren kişinin "olumlu irade beyanı"nı içermesi gerekmektedir. Diğer mevzuattaki düzenlemeler saklı kalmak üzere, açık rızanın yazılı şekilde alınmasına gerek yoktur. Açık rızanın elektronik ortam ve çağrı merkezi vb. yollarla alınması da mümkündür. Burada ispat yükümlülüğü veri sorumlusuna aittir.

Kanunun 3. maddesinde yer verilen açık rıza tanımı kapsamında, açık rızanın belirli bir konuya ilişkin olması, rızanın bilgilendirmeye dayanması ve özgür iradeyle açıklanması olmak üzere üç unsuru bulunmaktadır.

Açık Rızanın Belirli Bir Konuya İlişkin Olması: Veri işlemek üzere verilen açık rızanın geçerli olması için açık rızanın belirli bir konuya ilişkin ve o konu ile sınırlı olması gerekir. Veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerekmektedir. Buna göre, ilgili kişinin genel bir irade açıklaması ile "kişisel verilerimin işlenmesini kabul ediyorum" şeklinde açık uçlu ve belirsiz rızası tek başına Kanun bağlamında "açık rıza" olarak kabul edilemez. Eğer birden çok kategoriye ilişkin verinin işlenmesine dair açık rıza beyanında bulunulacaksa, açık rızanın hangi verilerin ve ne amaçlarla işleneceği gibi, işlemenin farklı noktaları açısından da verilmiş olması gerekir

Rızanın Bilgilendirmeye Dayanması: Açık rıza bir irade beyanı olup, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerekir. Kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerekir. Bilgilendirme, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmelidir. Bilgilendirmenin mutlaka verinin işlemesinden önce yapılması gerekir.

Bilgilendirme yapılırken elde edilecek kişisel verilerin hangi amaçlarla kullanılacağı açıkça belirtilmeli, kişinin anlamayacağı terimler ya da yazılı bilgilendirme yapıldığında okumakta güçlük çekeceği oranda küçük puntolar kullanılmamalıdır. Örneğin; genel işlem şartı oluşturan ve küçük puntolarla hazırlanmış abonelik sözleşmeleri içeriğine saklanmış açık rıza beyanlarının hukuka uygun olmayacağını belirtmek gerekir.

Rızanın Özgür İradeyle Açıklanması: Kişinin irade beyanı olan rıza, kişinin yaptığı davranışın bilincinde ve kendi kararı olması halinde geçerlilik kazanacaktır. Kişinin iradesini sakatlayacak her türlü fiil, kişisel verilerin işlenmesi için verdiği açık rızayı da sakatlayacaktır.

Tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerekir. Özellikle işçi-işveren ilişkisinde, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından

muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez.

Öte yandan, açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir.

Örneğin; bankanın kredi vereceği müşterisine yönelik bilgileri pazarlama faaliyeti amacıyla paylaşılmasına yönelik rıza beyanı, rıza verilmemesi halinde bankacılık hizmetinden faydalanılamayacağı sonucunu doğuracağından rızayı sakatlamaktadır.

4.6.Kişisel Verilerin Silinmesi, Yok Edilmesi Ve Anonim Hale Getirilmesi

Kanun'un 7. maddesi, kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesini, yok edilmesini veya anonim hâle getirilmesini düzenlemektedir.

Nitekim; 28.10.2017 tarihli Resmi Gazetede yayınlanan ve 01.01.2018 tarihinde yürürlüğe giren "Kişisel Verilerin Silinmesi, Yok Edilmesi Ve Anonim Hale Getirilmesi Hakkında Yönetmelik" ile de buna ilişkin hükümler daha net olarak ortaya konmuştur.

4.6.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel Verileri Koruma Kurumu tarafından hazırlanan rehber doğrultusunda kişisel verilerin silinmesi işleminde izlenmesi gereken süreç şu şekildedir:

● *Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.*

● *Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.*

● *İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.*

● *İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.*

Yine aynı rehber, silme işlemine ilişkin yöntemleri de ortaya koymaktadır;

Hizmet Olarak Uygulama Türü Bulut Çözümleri (Ofice 365, Salesforce, Dropbox gibi): Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

Kağıt Ortamında Bulunan Kişisel Veriler: Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

Merkezi Sunucuda Yer Alan Ofis Dosyaları: Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

Taşınabilir Medyada Bulunan Kişisel Veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

Veri Tabanları: Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

4.6.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin yok edilmesinin silinmesinden farkı, kişisel verilerin silinmesi halinde objektif olarak yani özel bir uğraş gerektirmeksizin kişisel veriye kimsenin erişememesi sağlanırken yok edilmesi halinde bilişim ve veri kurtarma yolları da dahil hiçbir şekilde veriye ulaşılmasının mümkün olmamasıdır.

Bunun nasıl yapılacağı da yine Kişisel Verileri Koruma Kurumu tarafından hazırlanan rehberde belirtilmiştir;

Yerel Sistemler: Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.

i) De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

ii) Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.

iii) Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

Çevresel Sistemler: Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

i) Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

ii) Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

iii) Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

iv) Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

v) Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

vi) Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

vii) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir

viii) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok

etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

Kağıt ve Mikrofiş Ortamları: Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

Bulut Ortamı: Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

Yukarıdaki ortamlara ek olarak; arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması, gerekir.

4.6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Dolayısıyla anonim hale getirme işlemi ile kişisel verinin, "kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi" tanımında yer alan "belirli yada belirlenebilir" olma özelliği kaybolmaktadır.

Örneğin; bir kurumun gerçekleştirmiş olduğu sınava yönelik hazırlanan tabloda, kişi isimleri, kimlik numaraları silinerek sadece sınava girenlerin ikamet ettikleri il ve aldıkları not bilgilerinin tutulması, "belirli ya da belirlenebilir" olma özelliği taşıyan verilerin anonimleştirilmesi olup, geriye kalan veriler ile iller bazında alınan notların değerlendirmesi veya istatistiği tutulabilecektir.

Anonim hale getirmeye yönelik olarak uygulanabilecek bazı yöntemler ve uygulanma şekillerine ilişkin olarak Kişisel Verileri Koruma Kurumu tarafından ayrıntılı olarak hazırlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Ve Anonim Hale Getirilmesi Rehberinden yararlanılabilir.

BEŞİNCİ BÖLÜM

KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR VE TEMEL İLKELER

5.1. Kişisel Verilerin İşlenmesinde Temel İlkeler

Kişisel verilerin işlenmesine ilişkin temel ilkeler, 108 sayılı Avrupa Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine, 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifine ve Avrupa Birliği Genel Veri Koruma Tüzüğü'ne (GDPR) paralel olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde "Genel İlkeler" başlığı altında düzenlenmiştir;

Genel ilkeler

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 işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kanunun açıkça emredici kuralla uyulmasını zorunlu kıldığı ilkeler, her bir veri işlemesi için ayrı ayrı değerlendirilmek ve uygulanmak zorundadır.

a. Hukuka Ve Dürüstlük Kurallarına Uygun Olma: Tüm ilkelerin ana kaynağını oluşturan bu ilke, öncelikle genel ve evrensel tüm hukuk kurallarına uygun

olmayı ve elbette Kişisel Verilerin Korunması Hukukuna ilişkin tüm mevzuat hükümlerine uygun davranılması gerekliliğini ortaya koymaktadır. Bunun yanında Türk Medeni Kanununda da kendisine yer bulan temel dürüstlük kuralına uyumlu olma ve objektif olarak kişiden beklenebilecek makul davranışın sergilenmesi beklenmektedir. Kişiden beklenecek makul davranış ise aslında diğer ilkeler içinde kendine yer bulmaktadır.

b. Doğru Ve Gerektiğinde Güncel Olma: Veri sorumlularınca işlenen kişisel verilerin doğru olması, gerek ilgili kişi gerekse veri işleyen bakımından oldukça önemli olup verilerin doğruluğu hususunda veri sorumlusuna bir sorumluluk yüklenmektedir. Ayrıca verilerin güncelliğinin sağlanması bakımından veri sahibi ile birlikte hareket etmesi beklenmektedir.

Burada veri ilgili kişiden ya da ilgili kişinin bilgisi dahilinde endirekt olarak alınıyorsa, verinin doğru bir şekilde verilmesinde ilgili kişi sorumlu olacaktır. Verinin doğru verilmesine karşın veri sorumlusu tarafından isteyerek ya da istemeyerek hatalı bir şekilde işlenmesi halinde ise veri sorumlusu sorumlu olacaktır. Yine ilgilisinin hatalı kayıtların düzeltilmesine ilişkin talebine karşın gerekli düzeltmeyi yapmayan veri sorumlusu sorumlu olacaktır.

Verilerin güncel olup olmadığının sürekli olarak denetimi, pek tabi sadece veri sorumlusunun üzerine bırakılacak bir sorumluluk olamaz. Ancak verilerin güncel ve doğru olmasına yönelik sorumluluk Kanun ile veri sorumlusu üzerine yüklenmiş olup veri sorumlusunun da bu kapsamda makul sayılabilecek önlemleri alması, sürekli olmasada belirli aralıklarla denetim sağlaması ve en önemlisi ilgilisinin hatalı kişisel verilere ilişkin talepleri mutlak suretle gecikmeksizin değerlendirilmelidir.

c. Belirli, Açık Ve Meşru Amaçlar İçin İşlenme: Uygulayıcılar açısından oldukça önem arz eden bu ilke ile veri sorumlusunun veri işleme amacının belirli, açık ve meşru olması gerekliliğini ortaya koymaktadır. Uygulama sürecinde hangi verilerin hangi amaçlarla işlendiği ve işleneceği hususları değerlendirilirken amacın belirli, açık ve meşru olması hususu öncelikle değerlendirilecek hususlardandır.

Zira veri sorumlusu belirli, açık ve hukuken de zemini olan meşru bir amaca yönelik veri işlerken, veri sahibini de aydınlatma metinlerinde ve açık rıza beyanlarında

bu amaca yönelik veri işlendiğine ilişkin bilgilendirecektir. Veri sorumlusu daha sonraki bir dönemde aynı veriyi işlenmesi aşamasında planlanan amacından başka bir amaç için kullanma eğilimine girdiğinde bu kez bahse konu bilgilendirmeler de eksik kalacak ve yeni amaca yönelik veri işleme eylemi genel ilkelere ve dolayısıyla Kanun'a aykırılık teşkil edecektir.

Burada meşru amacın, bir sonraki ilke olan sınırlı ve ölçülü olma ilkesi ile de bağlantılı olduğunu belirtmekte fayda vardır. Zira, kişisel verinin işlenmesindeki meşru amacın belirlenmesinde, işlenen kişisel verinin, veri sorumlusunun yaptığı iş veya sunduğu hizmet ile bağlantısı olması ve amacı gerçekleştirmekle de sınırlı kalması gerekecektir. Örneğin, bir internet sitesi üzerinden cep telefonu satan veri sorumlusunun, alıcının konum bilgisini işlemesinde meşru bir amaçtan söz edilemezken, yine bir internet sitesi üzerinden araç kiralama hizmeti verilmesi halinde veri sorumlusunun, hizmeti alıcının konum bilgisini işlemesinde meşru bir amacın varlığından bahsedilebilecektir.

Yine aynı örnek üzerinden hareket edecek olursak bu ilke özelinde önemli olan bir nokta da meşbu bir amaç için işlenen verinin, yine bu amaç uğruna kullanılması gerekliliğidir. Zira verinin kullanımı, veri toplama aşamasında hedeflenen amacın dışında bir amaç için gerçekleştiğinde bir internet sitesi üzerinden araç kiralama hizmeti verilmesi halinde veri sorumlusunun, hizmeti alıcının konum bilgisini işlemesinde meşru bir amacın varlığından söz edilebilecekken daha sonraki bir aşamada bahse konu konum bilgilerini, hizmet alıcının seyahat deneyimlerini belirlemede kullanması genel ilkelere ve dolayısıyla Kanun'a aykırılık teşkil edecektir.

d. İşlendikleri Amaçla Bağlantılı, Sınırlı Ve Ölçülü Olma: Veri sorumlularının kişisel verileri toplamadan önce amaçlarıyla bağlantılı olarak verilerin mutlaka kullanıp kullanmaması gerektiğini araştırması, söz konusu kişisel verilerden amacına ulaşmak için yeterli miktarını toplaması ve işlemesi, gereğinden fazla veri toplamaması ve işlememesi gerektiği kuralını ifade etmektedir. Bu çerçevede, belirlenen amacı gerçekleştirmeye elverişli olmayan kişisel verilerin işlenmemesi gerektiği ifade edilmektedir. Ayrıca kişisel verilerin sonradan ortaya çıkması muhtemel ihtiyaçların karşılanması amacıyla işlenebilmesi için, işlemeye ilk kez başlanıyormuş gibi, Kanunun 5. maddesinde yer alan işlenme şartlarından birinin gerçekleşmesi gerekmektedir.

Bu ilke de uygulayıcılar açısından önem arz etmektedir. Her uygulayıcı öncelikle veri sorumlusunun yaptığı iş veya hizmete ilişkin amacı değerlendirmeli, akabinde bu amaca ulaşmak için gerekli, ilgili, yeterli ve bu amacı aşmayan verilerin işlenmesini sağlamaya yönelik uygulamalar gerçekleştirmelidir.

Örneğin; bir şirketin muhasebe departmanı tarafından sadece müşterilerine fatura göndermek amacıyla işlenen elektronik posta adresi kullanılmak suretiyle, amaç ile bağlantılı ve sınırlı olmayan reklam içerikli elektronik postaların müşteriye gönderilmesi bu ilkeye aykırılık teşkil edecektir. Bunun yanında aynı amaca yönelik olarak muhasebe departmanına müşterinin isim, soyisim, kimlik numarası ve elektronik posta adresi verileri yeterli olabilecekken ölçüsüzce ve lazım olabileceğinden bahisle evlenmeden önceki soyisim, kan grubu gibi verilerin işlenmesi de bu ilkeye ve dolayısıyla Kanun'a aykırılık teşkil edecektir.

e. İlgili Mevzuatta Öngörülen Veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme: Kişisel verilerin "amaçla sınırlılık ilkesi" nin bir gereği olarak işlendikleri amaç için gerekli olan süreye uygun olarak muhafaza edilmesi gerekir. Bu konuda, veri sorumlusu, idari ve teknik tedbirleri almakla yükümlüdür. Kişisel Verilerin Korunması Kanunun 12. maddesinde de belirtildiği gibi veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Bununla ilgili olarak veri sorumlusu, kişisel veri saklama ve imha politikası ve esaslarını oluşturmak, saklama süreleri ve muhafazada uygulamaya alınacak teknik ve idari tedbirleri belirlemek ve kişisel verilerin bu esaslara uygun olarak muhafazasını sağlamakla yükümlüdür.

Kişisel verilerin saklanması için amaçla sınırlılık ilkesi uyarınca veri sorumlusu tarafından belirlenen saklama sürelerinin yanı sıra, veri sorumlusunun tabi olduğu ilgili mevzuat kapsamında da belirlenmiş saklama süreleri mevcuttur. Buna göre; veri sorumluları, ilgili kişisel veriler için mevzuatta öngörülmüş bir süre varsa bu süreye riayet edecek; eğer böyle bir süre öngörülmemişse verileri ancak işlendikleri amaç için gerekli

olan süre kadar saklayabilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep bulunmaması halinde, o veri silinecek, yok edilecek ya da anonim hale getirilecektir. İleride tekrar kullanılabileceği düşünülerek ya da herhangi bir başka gerekçe ile kişisel verilerin muhafaza edilmesi yoluna gidilemeyecektir.

Örneğin; araç kiralama hizmeti veren veri sorumlusu, hizmete ilişkin düzenlemiş olduğu faturayı, fatura düzenlenen kişi artık müşterisi olmasa da mali yükümlülükler gereği faturada mevcut kişisel veriler ile birlikte ilgili Kanunda belirtilen sürelerde saklamak zorundadır. Ancak aynı veri sorumlusu araç ve müşteri güvenliği amacıyla ilgili kişinin aracı kullandığı sürece işlediği anlık konum bilgisini/verisini, aracın ilgili kişi olan müşteri tarafından iadesi ile birlikte silmesi, yok etmesi ya da anonim hale getirmesi gerekecektir.

Ayrıca veri sorumlusu, Kişisel Verilerin Korunması Kanununun 16. maddesi uyarınca sicile kayıt için başvuru yaparken kişisel verilerin işlenme amacı için gerekli azami süreyi Veri Sorumluları Sicili Hakkında Yönetmeliğin 9. maddesini göz önünde bulundurarak tespit etmek ve bu süreyi bildirmek zorundadır.

5.2. Kişisel Verilerin İşlenme Şartları

Mutlak suretle kişisel verilerin işlenmesine ilişkin temel ilkelerle birlikte değerlendirilmesi gereken kişisel verilerin işlenme şartları, Kişisel Verilerin Korunması Kanunu'nun 5. ve 6. maddeleri ile özel nitelikli olan kişisel verilerin işlenmesi ve özel nitelikli olmayan kişisel verilerin işlenmesi ayrımına tabi tutularak ele alınmıştır. Bu yolla kişisel verilerin işlenmesinin hukuka uygun sayılabilmesi için gerekli şartlar belirtilmiştir. Bu şartlar, madde metninde sınırlı olarak sayılmış ve yorum ya da kıyas yoluyla genişletilmesi kabul edilmemektedir.

Burada önemle üzerinde durulması gereken konu, kişisel verilerin işlenmesi konusunda kişisel verilerin işlenmesine ilişkin temel ilkeler unutulmamalıdır. Zira Kanuni şartlara haiz olmakla birlikte temel ilkelere aykırılık teşkil edecek kişisel veri işleme eylemi hukuka aykırı olacaktır.

5.2.1. Özel Nitelikli Olmayan Kişisel Verilerin İşleme Şartları

Kişisel Verilerin Korunması Kanunu'nun 5. maddesi, ilk fıkrası ile kişisel verilerin işlenmesine yönelik olarak ana şartın "açık rıza" olduğunu ortaya koymuş ve ikinci fıkra ile de bu ana şartın istisnalarını yani açık rıza aranmaksızın kişisel verilerin işlenmesine ilişkin şartların neler olduğunu belirtmiştir. Buna göre; kişisel verilerin hukuka uygun olarak işlenmesi için maddenin ikinci fıkrasında bulunan şartlardan en az birinin gerçekleşmesi gerekir;

Kişisel verilerin işlenme şartları

MADDE 5- (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Burada, daha önce de belirtmiş olduğumuz gibi kişisel veri işleme faaliyetinin, kişisel veri işlenmesindeki temel ilkelere uygun olarak işlenmesi gerektiği ve maddede

sayılan şartlardan birinin veya birkaçının varlığı halinde dahi maddede sayılan amacın dışına çıkılarak veri işlemesi yapılmaması gerekliliğini tekrar hatırlatmak isterim.

Aksi bir durum, veri işlemenin madde metninde var olan bir şarta istinaden yapılıyor olmasına karşın, bunun saptanmamış olması nedeniyle hukuka aykırı bir veri işleme sonucunu doğurur ki bu da cezai yaptırıma tabidir.

Bu nedenle öncelikle kişisel veri tespit edilmeli, kişisel verinin işlenmesine ilişkin madde metninde var olan şartlardan hangi ya da hangilerinin var olduğu saptanmalı ve verinin işlenme amacının bununla sınırlı olmak kaydı ile varlığı korunmalıdır.

Örneğin; bir işveren, işçinin isim, soyisim, kimlik numarası, telefon numarası ve banka hesap numarasını kanunen zorunlu olduğu işlemleri yapma ve belgeleri hazırlama, ilgili kurumlara bildirme, sözleşme kurma ve sözleşmeyi devam ettirme, işçiye hak edişlerini ödeme, vergi ve sigorta yükümlülüklerini yerine getirme ve olası bir uyuşmazlık halinde mahkemeye sunma sebepleri ile işlemektedir. Bu sebepler teker teker incelendiğinde; kanunen zorunlu olduğu işlemleri yapma ve belgeleri hazırlama, ilgili kurumlara bildirme sebepleri 2. fıkranın a bendinde belirtilen şartları, sözleşme kurma ve sözleşmeyi devam ettirme, işçiye hak edişlerini ödeme sebebi 2. fıkranın c bendinde belirtilen şartları, vergi ve sigorta yükümlülüklerini yerine getirme sebebi 2. fıkranın ç bendinde belirtilen şartları, olası bir uyuşmazlık halinde mahkemeye sunma sebebi 2. fıkranın e bendinde belirtilen şartları sağladığı görülmektedir. İşçi işten ayrılmış, çıkartılmış yada herhangi bir sebeple iş akdi son bulmuşsa işveren, aynı kişisel verileri 2. fıkranın c bendinde belirtilen şart dahilinde işleyememekle birlikte madde metninde sayılı diğer nedenlerin bir yada bir kaçının varlığını devam ettirmesi halinde o şartlarla sınırlı kalmak kaydı ile işlemeye devam edecektir.

Bu aşamada madde metninde sayılı şartları kısaca incelemenin yararlı olacağını düşünüyorum.

5.2.1.1. İlgili Kişinin Açık Rızası

Kişisel Verilerin Korunması Kanunu'nun 3. maddesinde açık rıza; *"Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"*yı ifade etmektedir.

Kişisel Verileri Koruma Kurumu, veri sorumlusu tarafından veri işleme faaliyetinin gerçekleştirilmesinde öncelikle madde metninde yer alan diğer veri işleme şartlarından birine dayanılıp dayanılamayacağının değerlendirilmesi gerektiğini, bunlardan hiçbirisi yoksa ilgili kişinin açık rızasının alınması yoluna gidilmesi gerektiğini ortaya koymuştur.

Bu bağlamda, madde metninde yer alan şartlardan bir ya da birkaçının var olmadığı hallerde açık rızaya ihtiyaç duyulmalıdır. Burada önemle belirtmek isterim ki, başkaca bir veri işleme şartının mevcut olmadığı her durumda rıza beyanı alınmak suretiyle hukuka uygun bir veri işlemesi yapıldığından bahsedilemez. Zira kişisel verilerin işlenmesine ilişkin temel ilkelere her zaman uyumlu olmak mutlaktır.

Açık rıza alınması aşaması da önem arzetmektedir. Zira, açık rıza alınırken gerekli ve yeterli bilgilendirme yapılmalı, ilgili kişinin özgür irade beyanını sakatlayacak türde fiillerden kaçınılmalı ve açık rıza beyanından geri dönülmesine ilişkin yollar açık tutularak bu yollara ilişkin ilgili kişiye bilgilendirme yapılmalıdır.

Örneğin; elektronik ürün satışı hizmeti sunan bir e ticaret firması, her ne kadar müşterisinin iletişim bilgilerini, maddenin 2. fıkrasında mevcut şartlardan biri nedeniyle işlemekteyse de bu iletişim bilgilerini aynı zamanda pazarlama ve reklam faaliyetleri için de kullanmak istemesi halinde ilgili kişinin açık rızasını alması gerekecektir.

Unutulmamalıdır ki; hukuka uygun bir şekilde açık rıza alındığına ve bu açık rızadan dönülmediğine ilişkin ispat yükü veri sorumlusundadır.

5.2.1.2. Kanunlarda Açıkça Öngörülmesi

Kimi durumlarda veri sorumlusu, kanunların açık hükümleri ile kişisel veri işleme faaliyeti gerçekleştirmeye mecbur tutulmuştur. Bu durumlarda veri sorumlusu açık rıza aranmaksızın veri işlemekle yükümlüdür.

Örneğin; işverenin kanundan kaynaklanan özlük dosyası düzenleme yükümlülüğü, işverenin kanundan kaynaklanan işiçin işe giriş bildirgesini düzenleyerek kuruma beyan etme yükümlülüğü gibi.

Veri sorumlusu, kanunlarda açıkça öngörülmesi haline dayanarak işlediği verilere ilişkin, ilgilisinin kişisel verilerinin silinmesine veya işlenmesine rıza göstermemesine ilişkin taleplerini dikkate almayacaktır.

5.2.1.3. Fiili İmkânsızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan Veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisinin Ya Da Bir Başkasının Hayatı Veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması

Madde içerinde mevcut bu şarta ilişkin akla ilk gelen durum her ne kadar tıbbi müdahale gerektirecek haller ve bu hallerde şuurun açık olmaması hali gelse de kişinin sağlık verileri özel nitelikli kişisel verilerden olduğundan bu şart özelinde sağlık nedenleri düşünülmemelidir.

Bu şartın varlığından söz edilebilmesi için fiili imkansızlık ve rızaya hukuki geçerlilik tanınamaması hallerinin, kişinin yada üçüncü kişinin hayatı veya beden bütünlüğünün korunmasının zorunluluğuna dayanması gerekecektir.

Örneğin; dağda mahsur kalan bir kişinin konumunun belirlenmesi için cep telefonu sinyali verisinin işlenmesi, hayat ve beden bütünlüğü için zorunluluğu ve rıza alınması için fiili imkânsızlık halini ortaya koymaktadır.

5.2.1.4. Bir Sözleşmenin Kurulması Veya İfasıyla Doğrudan Doğruya İlgili Olması Kaydıyla, Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması

Sözleşme, iki ya da daha çok kişinin aralarında hukuki bir bağ yaratmak, bu bağı değiştirmek ya da ortadan kaldırmak amacıyla, karşılıklı ve birbirine uygun iradelerini beyan ederek yaptıkları hukuki işlemlerdir.

Bu bağlamda bir sözleşmenin kurulabilmesi ve gereklerinin yerine getirilmesi, kişisel veri işlenmesi zorunluluk haline getirecektir. İşte burada, sözleşme taraflarına ait olmak ve sözleşmenin kurulması ile ifasıyla doğrudan doğruya ilgili olmak kaydıyla kişisel veri işlenmesi hali Kanunda kendisine yer bulmuştur. Ancak bir sözleşmenin varlığı, kesinlikle her türlü verinin işlenmesine ilişkin şartın varlığını göstermez. Burada önemle incelenmesi gereken husus, işlenen kişisel verinin, sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilişki içinde olmasıdır. Sözleşmenin konusuna bakıldığında, sözleşme konusu ve ifası ile sınırlı verileri bu kategoride değerlendirmek gerekir. Örneğin; sözleşme kurulması amacıyla gerekli olan elektronik posta adresi, e faturanın tebliği amacıyla gerekli iken pazarlama amacıyla kullanılması, sözleşmenin ifası için gerekli değildir. Bu halde verinin mutlaka sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması aranmalıdır.

Burada sözleşmenin yazılı ya da sözlü olması arasında bir farklılık olmamakla birlikte kişisel verilerin hukuka uygun işlenmesi ve bunun ispatı noktasında sorumluluğunun veri işleyen veri sorumlusunda olduğu düşünüldüğünde, veri işlenmesini gerektirir sözleşmelerin yazılı yapılmasında fayda vardır.

Örneğin; bir emlakçının, her ikisiyle de arasında bulunan simsarlık sözleşmesi gereği, ev sahibi ve kiracı arasında imzalanan sözleşme kapsamında tarafların isim, soyisim, kimlik numarası, banka hesap numaraları, adres, imza gibi kişisel verilerini işlemesi simsarlık sözleşmesinin kurulması için gerekli olduğu gibi bu sözleşmenin ifası için de gereklidir. Bu bağlamda bu verilerin işlenmesi de hukuka uygundur.

Bu konuya ilişkin olarak hatalı uygulamalara yol açan açık rıza alınması konusuna da değinmekte fayda görüyorum. Kanunun bu bendi özelinde bahsedilen konu, veri işleme faaliyeti gerçekleşmeksizin sözleşmesel yükümlülükler yerine getirilemiyorsa

veri işlemenin hukuka uygun olacağıdır. Ancak, veri işleme konusunda sözleşme içeriğine bir hüküm koymak suretiyle bu veri işlemeyi sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili hale getiremeyeceğimiz gibi sözleşme içindeki hüküm vasıtasıyla açık rıza gereken hallerde açık rıza alınmasından da kurtulunamaz. Özellikle genel işlem şartı içeren sözleşmelerde gördüğümüz bu hallerde, açık rıza şartı gereken veri işlemeleri için sözleşme hükümleri içine saklanmış beyanlarla bu şartın gerçekleştirilmesi mümkün değildir. Çoğunlukla tüketicilerle yapılan ve genel işlem şartı içeren bu sözleşmelerin içeriği, bu tür hükümlerden arındırılmalı ve Kanun'un öngördüğü şartlar uygulanmalıdır.

5.2.1.5. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Açık rıza aranmaksızın veri işlenmesine ilişkin şartları incelediğimiz bu bölümün 2. Maddesinde Kişisel Verilerin Korunması Kanunu'nun 5. Maddesinin 2. Fıkrasının "a" bendinde "Kanunda açıkça öngörülmesi" şartını incelemiştik.

Hukuki yükümlülüğün yerine getirilmesi için zorunlu olma şartı "Kanunda açıkça öngörülme" şartından farklı olarak Kanunlar dışındaki tüm hukuki düzenlemeler ile resmi makamlarca verilmiş olan kararlara ilişkin yerine getirilmesi zorunlu yükümlülükleri düzenlemektedir.

Örneğin; Cumhurbaşkanlığı Kararnameleri, Yönetmelikler, Tebliğler, Mahkeme kararları bu bağlamdadır.

Burada dikkat edilmesi gereken nokta zorunluluktur. Veri işleyen, verilerin işlenmesi bakımından gerçekten zorunluluk hali içindeyse bu kapsamda değerlendirilmelidir.

5.2.1.6. İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

İlgili kişinin, kendisine ait kişisel verileri yine ve ancak kendisi tarafından herkesçe ulaşılabilir hale getirmesi halinde bu verilerin işlenmesi, ancak herkesçe ulaşılabilir hale getirme amacıyla sınırlı kalmak kaydı ile işlenebilir.

Örneğin; bir avukatın ya da bir doktorun, kendisine ilişkin bilgi sahibi olunması ve kendisine ulaşılabilmesi amacıyla kişisel verilerini internet adresinde paylaşması halinde veri sahibinin kendisi tarafından verinin alenileştirildiğinden bahsedilebilir.

Bu örnek üzerinden dikkat edilmesi gereken hususlardan biri, kişisel veriyi yine veri sahibinin kendisinin alenileştirmiş olmasıdır. Zira aynı avukatın ya da doktorun kendisi ile birlikte aynı yerde çalışan diğer kişilere ilişkin bilgileri de internet sitesinde paylaşması halinde, paylaşan kişi açısından bu kişilerin paylaşılan verilerine ilişkin bir işleme şartına ihtiyaç duyulacaktır. Bir diğer husus ise kendisine ilişkin bilgi sahibi olunması ve kendisine ulaşılabilmesi amacıyla alenileştirilen kişisel verilerin ancak bu amaçlarla işlenmesi hukuka uygun olacaktır. Bu amaca yönelik kişisel verilerini alenileştiren bir avukatın bilgilerinin, hukuk kitapları satan bir şirket tarafından pazarlamaya yönelik mesaj gönderilmesi amacıyla işlenmesi, alenileştirmeye rağmen hukuka aykırı olacaktır.

5.2.1.7. Bir Hakkın Tesisi, Kullanılması Veya Korunması İçin Veri İşlemenin Zorunlu Olması

Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması halinde ilgili kişinin kişisel verilerinin işlenmesi mümkündür. Örneğin, bir şirketin kendi çalışanı tarafından açılması muhtemel bir davada ispat yükünden dolayı bazı verileri dava zamanaşımı sürelerinin sonuna kadar saklaması, sözleşme sona erdikten sonra, olası yasal takiplere karşı zamanaşımı süresinin sonuna kadar fatura, sözleşme, kefaletname gibi belgelerin bu amaçlar için saklanması bu kapsamda değerlendirilecektir.

5.2.1.8. İlgili Kişinin Temel Hak Ve Hürriyetlerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması

Kanun'un ilgili bendine istinaden ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydı ile veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda, kişisel verilerinin işlenmesi mümkündür.

Kanun'un lafzından da anlaşılacağı üzere bu şarta dayalı olarak veri işlenebilmesi için veri sorumlusunun meşru bir menfaati olmalı ve ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi gerekmektedir.

Burada "meşru olma" kavramından ne anlamak gerektiği çok önemlidir. Veri sorumlusunun, ilgili kişinin temel hak ve özgürlüğü ile yarışabilecek, yeterli düzeyde etkin, belirli ve halihazırda mevcut olan bir menfaatlerinin meşru olduğu kabul edilebilir. Ayrıca veri sorumlusunun gerçekleştirdiği güncel aktivitelerle ilişkili ve ona yakın gelecekte fayda sağlayacak bir işlem olması gerekmektedir.

Bu şarta dayanabilmek için öncelikle değerlendirilmesi gereken nokta veri sorumlusunun yukarıda açıklanan şekilde bir meşru menfaatinin var olup olmadığının tespiti gereklidir. Bu tespitin yapılmasının ardından meşru bir menfaatin var olduğu yönünde bir sonuca varıldığı takdirde, ilgili kişinin temel hak ve özgürlükleri ile veri sorumlusunun meşru menfaati bir terazide ele alınmalıdır. Nitekim ilgili kişinin temel hak ve özgürlükleri, veri sorumlusunun daha az öneme sahip menfaatinden daha üstün gelebilecektir. İşte bu noktada verilerin işlenmesine ya da işlenmemesine, yarışan menfaatler dengesine göre karar verilmelidir.

Örneğin; bir şirket sahibinin, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağılımında esas alınmak üzere çalışanların kişisel verilerinin işlenmesi şirket sahibinin meşru menfaati kapsamına alınmıştır.

Başka bir örnekle; otomobil filosu kiralayan şirketlerin, pazarlama amacı gütmeksizin tüm araç kullanıcılarına meteoroloji verilerine göre yoğun dolu yağışı beklenen zamanlarda mesaj göndermek amacıyla veri işlemesi, hem müşterisinin hem şirket araçlarının güvenliği açısından meşru bir menfaat olarak sayılabilecektir.

Bu şarta bağlı olarak uygulayıcıların önemle dikkat etmesi gereken husus, diğer tüm veri işleme şartlarının uygulanamadığı hallerde bir can simidi gibi meşru menfaat şartına sarılınılmamalıdır. Meşru menfaat şartı, veri işlenmesi bakımından başvurulacak son çare olmadığı gibi her şeyi kapsamına dâhil edebilecek ve tüm kişisel verilerin işlenmesine ilişkin faaliyetleri kanuni hale getirecek bir düzenleme de değildir. Zira yarışan menfaatler değerlendirmesinde her zaman veri sorumlusunun menfaatlerinin öne çıkacağı sonucu doğru olmayacaktır. Bu nedenle bu tür yaklaşımlarla veri işlemeyi hukuka uygun hale getiremeyiz.

5.2.2. Özel Nitelikli Kişisel Verilerin İşleme Şartları

Özel nitelikli kişisel veriler, öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir. Bu nedenle diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerekmektedir. Bu nedenle uluslararası düzenlemeler ışığında ancak çok daha katı bir şekilde Kanun, bu verilere özel bir önem atfetmekte ve bu verilerle ilgili farklı bir düzenlemeler getirmektedir.

Kanun metninden de anlaşılacağı üzere özel nitelikli kişisel veriler, sınırlı sayma yoluyla belirlenmiştir ve bunların kıyas yoluyla genişletilmesi mümkün değildir.

Daha sıkı bir koruma altına alınmış olması nedeniyle özel nitelikli kişisel verilerin işlenmesinin mutlak yasak olarak kabul edilmemesi gerekir. Zira yaşam hakkı, ifade özgürlüğü, haberleşme özgürlüğü gibi birçok temel hak ve özgürlüğün kullanılması, özel nitelikli kişisel verilerin işlenmesini zorunlu kılmaktadır.

Kişisel Verilerin Korunması Kanunu'nun 6. maddesi, özel nitelikli verilerin neler olduğunu ortaya koyarak özel nitelikli kişisel verilerin hukuka uygun olarak işlenmesi için aranan şartları içermektedir;

Özel nitelikli kişisel verilerin işlenme şartları

MADDE 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.

(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 finansmanının 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.

5.2.2.1. Sağlık Ve Cinsel Hayat Dışındaki Özel Nitelikli Kişisel Veriler

Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler ancak ilgili kişinin açık rızasının bulunması ya da kanunda öngörülen hallerde işlenebilir. Bu iki hal dışında bu nitelikteki verilerin işlenmesine yönelik hukuki bir sebep mevcut değildir.

Örneğin; Toplu İş Sözleşmesi Kanunu ve İş Kanunu çerçevesinde çalışanların sendika üyeliği bilgisi, veri sorumlusu işveren tarafından kanunda öngörülmesi şartı nedeniyle amaç ve gerekçe sınırlamasına tabi olmaksızın işlenecektir.

5.2.2.2. Sağlık Ve Cinsel Hayata İlişkin Özel Nitelikli Kişisel Veriler

Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler bakımından Kanun'un öngördüğü ilk şart ve kısıtlama bu verileri işleyebilecekler bakımındandır. Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. Bunun dışındaki kişi, kurum ve kuruluşlar tarafından her ne şartta olursa olsun sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veri işlenemeyecektir.

Burada "sır saklama yükümlülüğü altında bulunan kişiler" tabirinden öncelikle hekimler ve sağlık çalışanları anlaşılsa da avukatlar, noterler, mali müşavirler, bankalar gibi kişi, kurum ve kuruluşlar da sır saklama yükümlülüğü altında bulunanlardan sayılabilir.

Kanunda belirtilen "yetkili kurum ve kuruluşlar" tabirinden ise yine Sağlık Bakanlığı tarafından verilmiş ruhsat dahilinde çalışan kurum ve kuruluşlardır.

Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlara ilişkin şartın varlığı halinde ise Kanun'un aradığı diğer şart işleme amacına yöneliktir. Buna göre Kanun metninde sınırlı şekilde sayılan işleme amaçları; kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimidir.

Bu bağlamda, Sağlık Bakanlığına bağlı kurum ve kuruluşlarca bu amaçlara yönelik çalışmalarda veri işlenebilmektedir.

ALTINCI BÖLÜM

PARMAK İZİNİN KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ŞARTLAR VE TEMEL İLKELER BAKIMINDAN DEĞERLENDİRİLMESİ

6.1. 6698 Sayılı Kanun'un İstisnaları Bakımından Değerlendirme

6698 Sayılı Kanun'un 28. Maddesi, işbu Kanunu tamamen devre dışında bırakan bir takım istisnai halleri hüküm altına almıştır;

İstisnalar

MADDE 28- (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

Asıl itibariyle Ceza Adaleti Direktifi ile ortaya konmuş olan bu istisnalar, uluslararası düzenlemeler de genel hatları ile uyumludur.

Böylesine istisnai hallerin yaratılmasındaki ana amaç, kolluk ve adli makamların yetkilerini geniş tutabilmek, suçların önlenmesi veya suçun aydınlatılmasının kamu düzeni ve ülkeler güvenliği açısından önceliği, milli güvenlik, kamu düzeni, ekonomik güvenlik gibi hususlarda etkin bir çalışma yürütülmesini sağlamaktır.

Bu bağlamda örneğin alelade bir şirkete ilişkin uygulanabilir nitelikte olan koruma hükümlerinin, devletlerin ulusal güvenlikleri açısından da uygulanması zorunlu hükümler olarak değerlendirmek mümkün değildir.

Ancak, her ne kadar devletlerin kamu düzeni, kamu güvenliği, ekonomik güvenlik gibi ihtiyaçlarının giderilmesine yönelik istisnalar yaratılması bir gereklilikse de kişisel verilerin korunmasına ilişkin temel ilkeler yine de değerlendirme dışında bırakılmamalıdır. Zira temel ilkeler dediğimiz hususlar istisnaları da kapsar niteliktedir.

Çünkü istisnalar, Bir takım yetkileri genişletilmesini amaçlarken diğer yandan her ne şartta olursa olsun insan haklarına saygıyı da bir kenara itemez.

Bu bağlamda, yerel düzenlememiz olan ve yukarıda yer verilen 28. Madde özelinde temel ilkelerin değerlendirilmesi gerekmektedir. Temel ilkeler noktasında özellikle belirli açık ve meşru amaçlar için işlenme ile işlendikleri amaçla bağlantılı, sınırlı ve Ölçülü olma ilkelerinin istisnalar bakımından özellikle değerlendirilmesi gerektiği kanaatindeyiz.

Madde metni, bu kanun hükümlerinin kesinlikle uygulanmayacağı haller olarak istisnaları belirtmektedir. Ancak her şartta ve her uygulamasında devletin de Anayasa ile bağlı olduğu, Anayasa hükümleri gereği insan haklarına bağlı ve bir hukuk devleti olması ilkesine binayen hukuka ve dürüstlük kurallarına uygun olma ilkesine uymak zorundadır.

Bu doğrultuda devletin adli veya idari bir süreçte kişilerin parmak izi verilerini toplaması bazı durumlarda istisnai bir nitelik taşıyor olsa da kişisel verilerin korunmasına ilişkin belirttiğimiz ilkelere uyumlu hareket edilmesi zorunludur.

Sonuç olarak devletin tüm birimleri, istisnai hükümler çerçevesinde parmak izi verisi toplarken de, veriyi toplama amacıyla bağlı, sınırlı, ölçülü olmak zorundadır. Bu nedenle devletin kişisel veri işleme faaliyetleri açısından kamu düzeni, kamu güvenliği, ekonomik güvenlik gibi gerekçelerle bazı istisnaları sahip olması kabul edilebilir olmakla birlikte 28. Maddenin, 6698 Sayılı Kanun'un, istisnai hallerde hiçbir hükmü ile uygulanmayacağını ortaya koymak, Ölçülü olmadığı gibi devletin istisna elde etmekteki amacını da oldukça aşar niteliktedir.

6.2. 2559 Sayılı Polis Vazife ve Salahiyet Kanunu Gereğince Toplanan Parmak İzi Verisinin Kişisel Verilerin Korunması Temel İlkelerine Aykırılığı Sorunu

2559 Sayılı Polis Vazife ve Salahiyet Kanunu'nun 5. Maddesi, parmak izi ve fotoğrafların kayda alınması hususunu hüküm altına almıştır;

Parmak izi ve fotoğrafların kayda alınması

Madde 5- (Değişik: 2/6/2007-5681/2 md.)

Polis;

a) Gönüllü,

b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan,

c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen,

ç) Türk vatandaşlığına başvuruda bulunan,

d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı,

e) Gözaltına alınan,

kişilerin parmak izini alır.

Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez.

Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilinceye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir.

5271 sayılı Ceza Muhakemesi Kanununun 81 inci maddesi ile 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunun 21 inci maddesi hükümlerine göre alınan parmak izleri de bu sisteme kaydedilir.

(a) bendi hariç birinci fıkra ile dördüncü fıkra kapsamına giren kişilerin ayrıca fotoğrafları alınarak, ikinci fıkrada belirlenen esaslara uygun olarak parmak izi ile birlikte sisteme kaydedilir.

Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya

çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir.

Kolluk birimleri, kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir.

Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur.

Sistemde yer alan kayıtlar gizlidir; altıncı ve yedinci fıkralarda belirlenen amaçlar dışında kullanılamaz.

Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir.

Parmak izi ile fotoğrafların sistemde kaydedilmesi ve saklanması ile bu kayıtlardan yararlanmaya ilişkin diğer esas ve usûller, İçişleri Bakanlığı tarafından Adalet Bakanlığının görüşü alınarak çıkarılacak yönetmelikle düzenlenir.

Bu Kanun'un parmak izi verisinin toplanmasına yönelik uygulaması; Kişisel Verilerin Korunmasına Yönelik İlkeler bağlamında amaç ve ölçülük ilkesi açısından değerlendirilecektir.

6.2.1. Amaç İlkesi Bakımından Değerlendirme

Madde lafzi incelendiğinde öncelikli olarak parmak izi alınabilecek kimselerden bahsedilmiştir. Burada kolla verilen yetki ve kişiler değerlendirildiğinde bir takım parmak izi verisi toplama işleminin idari nitelikte olduğu, bir takım parmak izi birisi toplama işleminin ise adli nitelikte olduğu anlaşılmaktadır.

Maddenin ikinci fıkrası bu verilerin kişinin kimlik verileri ile birlikte ne zaman ve kim tarafından alındığı da belirtilmek suretiyle buna özgü bir sisteme kaydedileceği belirtilmiştir. Ancak fıkra sonunda parmak izinin hangi sebeple alındığının sisteme kaydedilmeyeceği belirtilmiştir.

Kanun gerekçesi incelendiğinde, Kanun Koyucunun parmak izinin işlenmesine yönelik amacın sisteme işlenmemesi hususunda ki iradesinin bilinçli olduğu görülmektedir. Gerekçeden anlaşılan, amacın sisteme işlenmemesi yoluyla fişleme olarak tabir edilen olguların Gerçekleşmeyeceğine yönünde bir ön fikir oluştuğudur.

Ancak madde metninde gönüllü olarak parmak izi veren kişilerin de aynı sisteme eklendi görülecektir. Bu bağlamda gerekçenin de çok doğru bir ön fikir yaratmadığı ve kişisel verilerin korunması noktasında temel ilkelere uygun olmadığı anlaşılmaktadır. Zira sistem içerisinde parmak izi verisi olan kişilere yönelik ön yargının daha baskın olacağı aşikardır. Gönüllü olarak parmak izi vermiş kişilerin de bu açıdan gereksiz ve hukuka aykırı bir ayrımcılığa tabi tutulacağı düşünülebilir. Kişinin parmak izi verisine sistem üzerinden ulaşan kolluğun, kişinin parmak izi verisine hangi sebeple sisteme işlenmiş olduğunu görmesi, amaca uygun işleme ve bu ilkenin devamı niteliğindeki amaca uygun kullanma ilkelerinin de doğru bir şekilde hayata geçirilmesine sağlayabilecektir.

6.2.2. Ölçülülük İlkesi Bakımından Değerlendirme

Kişisel verilerin korunmasına ilişkin önemli bir diğer ilke olan ölçülülük ilkesi, kişisel verinin ihtiyaç duyulacak düzeyde ve sürede saklanmasını öngörmektedir.

Diğer yandan ceza adalet sistemi açısından da unutulma hakkı, hükümlülüğü bir ömür boyu etiket haline getirilerek topluma kazandırma çalışmalarının sekteye uğratılmaması bakımından ölçülülük ilkesi önem arz etmektedir.

Hatta bu öneme binayen adli sicil kayıtlarında mevcut hüküm kayıtlarının dahi belirli şartların oluşması ve belirli sürelerin geçmesi ile birlikte silinmesi buna örnek olarak gösterilebilir.

Bu bağlamda madde metni incelendiğinde sisteme kayıtlı olan parmak izi ve fotoğraf verilerinin veri sahibi kişinin ölümünden itibaren on yıl ve herhalde kayıt tarihinden itibaren 80 yıl geçtikten sonra sistemden silineceğine ilişkin fıkrası ölçülülük ilkesine açıkça aykırılık teşkil etmektedir.

Üstelik burada, kolunun adli işlemler yönüyle parmak izi verisi kaydetmesi halinde adli işlemin kişi lehine ve kişiye herhangi bir sorumluluk yüklenmeyecek şekilde sonlanması halinde dahi, verinin derhal silinmesine yönelik bir hüküm mevcut değildir.

Avrupa İnsan Hakları Mahkemesi'nin 04.12.2008 tarih ve 30562/04 sayılı "S. Ve Marper/Birleşik Krallık" kararı da bu konuda verilmiş önemli bir karardır.

Bahse konu kararda; S.'nin işlemeye teşebbüs ettiği hırsızlık suçu nedeniyle yürütülen soruşturmada parmak izi örneği alınmış ve S. beraat etmiştir. Marper hakkında yürütülen soruşturma ise taciz nedenine dayanmakta olup onunda DNA ve parmak izi örneği alınmıştır. Akabinde tarafların uzlaşması sonucunda soruşturma kapatılmıştır. Buna karşın toplanan veriler, Birleşik Krallık mevzuatı gereği kişinin beraat etmesi veya herhangi bir nedenle yargılamanın sona ermesi hallerinde dahi verilerin süresiz ve sistematik olarak saklanacağına yönelik hükümleri gereğince tutulmaya devam edilmesi üzerine yapılan başvuruyu incelemektedir.

Avrupa İnsan Hakları Mahkemesi bu konuda vermiş olduğu kararında, verilerin süresiz olarak tutulmasında yarışan kamu menfaati ve başvurucuların menfaatini tartmış, verilerin belirtilen şekilde tutulmasının, beraat eden ya da soruşturması kişi lehine sonlananlar açısından masumiyet karinesine aykırılık teşkil edeceği gibi, süresiz bir işleminin de Ölçülü olamayacağını belirtmiştir.

Bu karar üzerinden yerel normumuz değerlendirildiğinde de; 80 yıllık bir veri kayıt süresinin insan ömrü açısından değerlendirildiğinde süresiz kayıt niteliği taşıdığı ve diğer yandan kolluğun, süreç lehine biten kişilere ilişkin verileri buna rağmen tutmasının hukuka aykırı olduğu aşikardır.

6.3. İmha Politikaları Açısından Değerlendirme

Parmak izi verisi, yukarıda alıntılanan 2559 Sayılı yasanın yanı sıra adli ve idari işlemler yönünden birçok Kanun ve Yönetmelik ile toplanabilir hale getirilmiştir.

Bahse konu verilerin, ölçüsüz toplanmasına ilişkin bilgilerimizi tekrarla bu verilerin imha edilmesi noktasında da gerek norm eksikliği açısından gerek var olan normların uygulanabilirliği açısından sorunlar mevcuttur.

Öncelikle, var olan normlar adli işlemler yönünden başta 5271 Sayılı Ceza Muhakemesi Kanunu olmak üzere bu Kanunu dayanak alan Yönetmeliklerden oluşmaktadır.

Açıkça norm bulunan Yönetmeliğe "Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğinin Tespiti Hakkında Yönetmelik" örnek olarak gösterilebilir. Yönetmeliğin 16. Maddesi, parmak izi vs. kişisel verilere yönelik olarak, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde elde edilen verilerin, Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle derhâl yok edileceği ve bu hususun tutanağa geçirileceği hüküm altına alınmıştır.

Diğer yandan norm içeriyor gibi görünmekle birlikte, sadece verilerin silineceği yönünde hükümler içeren ve hiçbir hüküm içermeyen düzenlemeler mevcuttur.

Bu düzenlemelerin, Kişisel Verilerin Korunması Kanunu özelinde yukarıda detayları ile açıklanan Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi usullerinin hiçbirini kapsamadığı görülmektedir.

Bir kere, dijitalleşen dünyada UYAP sistemi gibi Avrupa da takdirle izlenen bir yargı ağına sahip ülkemizde, kişisel verilerin silinmesi ve yok edilmesinin sadece Cumhuriyet Savcıları görevine ve gözetimine verilmesi uygulanabilir değildir. Diğer yandan kişisel veri içeren fiziki evrakların imhasına yönelik ise Cumhuriyet Savcılarına imha sürelerinin takibi ve imha prosedürlerinin işletilmesi görevlerinin yüklenmesi, konunun işlevsizleştirilmesine yol aşmaktadır.

Sonuç olarak imha politikalarının şeffaf olmaması ve uygulayıcıları açısından sorunlar olduğu aşikardır. Bu halde yapılacak olanın, parmak izi ve diğer kişisel verilerin imhasına yönelik protokollerin Bakanlıklar düzeyinde hazırlanması, gerekirse Kanun veya Yönetmeliklerle yayınlanması, sadece imhaya yönelik ayrı birimlerin oluşturulması ve bu sistemin dijital veri sistemleri açısından da uygulanabilir olması adına bu birimlerin teknik altyapısının da kuruluş aşamasında oluşturulması gerekmektedir.

6.4. Parmak İzi Delilinin Yeni Bilimsel Gelişmeler Işığında Biyometrik Verilerin Korunmasına İlişkin Usullerden Genetik ve Biyolojik Delillerin Korunmasına Yönelik Usullere Geçirilmesine Yönelik Gereklilikler

Suç önleme ve suçun aydınlatılması noktasında parmak izi delili, en önemli deliller arasında yer almaktadır. Bu denli öneme sahip bir delile ilişkin de her geçen gün yeni araştırma ve geliştirme çalışmaları yayınlanmaktadır.

Bu çalışmalar ışığında, Parmak izlerinin DNA molekülü içerdikleri kanıtlanmıştır. Ancak olay yerinde bulunması olası izlerin farklı özellikler gösterebildikleri de bilinmektedir. Dokunma ile gerçekleşen her transferde olduğu gibi temasın şiddeti, süresi, izi bırakan bireyin özellikleri, izin bulunduğu ortamın olay yeri olarak nitelenip delilin laboratuvara ulaştırılmasına kadar geçen süre, bırakılan hücrelerin dolayısı ile de DNA'nın miktarını ve kalitesini belirleyebilmektedir.

Bu açıdan DNA verisine ulaşmak zorlaşmaktaysa da kullanılabilir parmak izi delillerinden ortalama %38 inde DNA verisine de ulaşılabildiği anlaşılmaktadır.

Parmak izi delilinden DNA verisi elde edilmesinin, parmak izini bir DNA verisi haline getirdiğini söylemek elbette mümkün değildir. Parmak izi delili, niteliği gereği biyometrik veri olarak değerlendirilmek zorundadır.

Diğer yandan; DNA verisine ulaşılması demek, verinin artık biyometrik veri olmasının yanı sıra, buradan elde edilmesi muhtemel DNA verisi ile veri sahibinin kendisinin dışında yakınlarına yönelik olarak da veri üretilebileceği anlamına gelir ki bu durum suçların aydınlatılmasında son derece verimli olmakla birlikte verinin korunmasına yönelik de o denli önemsenmesi gereken bir durumdur.

Günümüz Ceza ve Adalet sistemi, parmak izini olması gerektiği üzere biyometrik delil olarak değerlendirmektedir. Ancak, Ceza Muhakemesi Kanunu, biyometrik delile yönelik olarak, genetik ve biyolojik delile nazaran daha az koruma sağlar niteliktedir.

Oysa ki; yukarıda yapılan açıklamalarımız ışığında parmak izi delilinin de, kendisinden biyolojik delil elde edilebildiği düşünüldüğünde Genetik ve Biyolojik Delil kategorisindeki deliller gibi koruma altına alınması ve Kişisel Verilerin Korunmasına

yönelik olarak da özel nitelikli kişisel veri olarak değerlendirmeye alınması gerekmektedir.

6.5. Parmak İzi Delilinin Toplanmasına Yönelik Amacının Dışında Kullanılması Yönünden Değerlendirme

Kişilerin parmak izi verilerinin alınmasını kolaylaştıran teknolojilerin gelişmesiyle birlikte bu hususta çalışan sistemlerin her alanda kullanımı da kolaylaşmıştır. Bu yönüyle parmak izi verisini okuyan sistemler işyerlerinde dahi kullanılır olmaya ve mesai takibi gibi verinin değeri ile son derece ölçüsüz uygulamalara dahi konu olmuştur. Nitekim hem idari hem adli Yüksek Mahkeme kararları ile bu tür uygulamaların ölçüsüz olduğu ve hukuka aykırılık teşkil ettiği artık yerleşik karar haline gelmiştir.

Diğer yandan idari makamlarca da parmak izi verisi toplandığı görülmektedir. 5510 sayılı Kanun ve Genel Sağlık Sigortası Uygulamaları Yönetmeliğinin dayanak olduğu Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliğinin Birinci Bölüm altıncı kısmında Kimlik tespiti başlığı altında biyometrik yöntemlerle kimlik doğrulaması yapılabileceğini belirtmektedir;

1.6 - Kimlik tespiti

(1) Sağlık (Değişik ibare:RG-25/8/2022-31934 Mükerrer) (94) hizmeti sunucularınca, 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. Kimlik tespiti, biyometrik kayıt işlemi veya biyometrik kimlik doğrulama işlemini usulüne uygun yapmayan ve bu nedenle bir başka kişiye sağlık hizmeti sunulması nedeniyle Kurumun zarara uğramasına sebebiyet veren sağlık hizmeti sunucularından ödenen tutar geri alınır.

(2) 2828 sayılı Sosyal Hizmetler Kanunu kapsamında sağlanan yardımlardan ücretsiz faydalananların, sağlık(Değişik ibare:RG-25/8/2022- 31934 Mükerrer) (94) hizmeti sunucularına birinci fıkrada belirtilen belgeleri ibraz edememeleri halinde 2828 sayılı

Kanun kapsamında bulunduklarını gösterir belgeye göre gerekli işlemler yürütülecek sonrasında söz konusu belgelerin ibrazı ilgili Kurumdan istenecektir.

(3) Kapsamdaki kişilerin kendi adına bir başkasının sağlık hizmeti almasını veya Kurumdan haksız bir menfaat temin etmesinis ağlaması yasaktır. Bu fiilleri işleyenlerden Kurumun uğradığı zararın iki katı kanunî faiziyle birlikte müştereken ve müteselsilen tahsiledilir ve ilgililer hakkında 5237 sayılı Türk Ceza Kanunu hükümleri doğrultusunda suç duyurusunda bulunulur.

Madde metninden de anlaşılacağı üzere parmak izi yada avuç içi izi verisinin toplanma amacının, sağlık hizmetlerinin verilmesinde usulsüzlüğü önlemek olduğu belirtilmektedir. Burada veri işleme amacı da sağlık hizmeti alan ile parmak izi verisi eşleşen kişilere hizmet verilmesi olarak ortaya çıkmaktadır.

Ancak bu verilerin toplanma amacı, tebliğ ile de açıkça ortaya konulmuşken, kolluk ve soruşturma makamlarınca bu veriler üzerinden araştırma yapılmaya çalışıldığı da görülmektedir.

Yukarıda daha ayrıntılı olarak açıklandığı üzere, bu verilerin soruşturma makamlarına açık hale getirdiği düşünülen norm, 6698 Sayılı Kanun'un 28. Maddesinde kendine yer bulan istisnalardır.

Suçun aydınlatılmasını, her türlü haktan yüksek ve kamu düzeni, milli güvenlik ve ekonomik güvelik gibi özel uygulama alanları içinde değerlendirmek elbette tek başına mümkün değildir. Ancak soruşturma makamlarının bu sistemlerde var olan verilere ulaşmak adına yazışmalar yapması halinde, bu verilerin veriliş amacına aykırı bir şekilde verilerin paylaşıldığı, veri aktarımı denilen bu paylaşımların da 6698 Sayılı Kanun'un 28. Maddesine dayandırılarak verilerin soruşturma makamlarına gönderildiği görülmektedir.

Yukarıda açıklandığı üzere artık biyolojik delil olarak dahi kullanılması mümkün hale gelen parmak izi verisinin, veri sahibi tarafından sadece sağlık hizmetlerine ulaşmak adına verildiği ve sisteme işlendiği, hatta veri sahibinin bu noktada iradesinin dahi zorunlu bırakılma nedeniyle olmadığı bir aşamada, amaç dışında verilerin kullanılması ve aktarılması açıkça hukuka aykırıdır.

Bu yönüyle kişisel verilerin ve hatta özel nitelikli kişisel verilerin toplanması, aktarılması, silinmesi, yok edilmesi ve anonim hale getirilmesi hususlarında ayrı birimlerin oluşturulması ve sistemlerin kurulmasının önemi bir kez daha anlaşılabilmektedir.

SONUÇ

Kişisel verilerin korunmasına yönelik dünyadaki gelişmelerin, milletlerarası sözleşmeler ve uluslararası birlik kararları yoluyla ülkemize de sirayeti sonucunda Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir.

Bununla birlikte Kanunun içeriğinde mevcut temel ilke niteliğindeki birçok hüküm de kendisinden önce var olan normlarla çelişik hale gelmiş yada Kişisel Verilerin Korunmasına yönelik temel düşünceye aykırı hale gelmiştir.

Bu doğrultuda yapmış olduğumuz çalışma ile öncelikle parmak izi delili incelenmiş, özel nitelikli kişisel veri kategorisinde olmakla birlikte Ceza Muhakemesi anlamında özel olarak koruma sağlanmamış olan parmak izi verisinin, güncel teknolojik gelişmeler ışığında bir DNA verisi haline gelebilirliği karşısında toplanması, saklanması ve imhasına yönelik özel bir korumaya ihtiyaç duyduğu değerlendirilmiştir.

Parmak izi verisinin kolluk tarafından toplanmasına ilişkin ise soruşturma öncesi ve soruşturma sonrası ayrımının mevcut olmamasının gerek Anayasal anlamda gerek Kişisel verilerin Korunmasına yönelik temel mantığa aykırı olduğu, ülkemizde mevcut normların da bu ayrım üzerinde durmadığı tespit edilmiştir.

Diğer yandan, kolluğun veri toplamasına ilişkin hükümleri düzenleyen normların, Ceza Hukukunun ve Kişisel verilerin Korunması Hukukunun bazı temel ilkelerine de aykırı düştüğü görülmüştür. Zira, gönüllü olarak parmak izi verenlerin masumiyet karinesinde yararlanamadıkları, soruşturma öncesi elde edilen parmak izi verisinin amaca uygunluk ve ölçülülük ilkeleri değerlendirilmeksizin toplandığı belirlenmiştir. Dolayısıyla soruşturma öncesi toplanan verilerin toplama amacı yayınlanmalı, amaca uygun kullanılmalı, gönüllülere ilişkin veri toplama amacının yayınlanmaması ilkesinden vazgeçilmelidir.

Diğer yandan kişisel verilerin özellikle soruşturma ve kovuşturma alanlarında toplanması ve imhasına giden yolda bir takım normların mevcut olduğu ancak bu normların uygulanabilir olmadığı, bu bağlamda verilerin imhasına yönelik olarak ayrı birimlerin kurulması ve teknolojik gelişmelerden yararlanılması gerektiği anlaşılmıştır.

Kişisel Verilerin Korunmasına ilişkin ulusal normlar, uluslararası normlara paralel olarak ülke güvenliğini ve kamu düzenini önceleyecek şekilde düzenlenmiş, Kişisel Veri kavramına yönelik istisnalar belirlenmiştir. Buna karşın ulusal normlarımız Anayasa'dan başlayarak değerlendirildiğinde, "milli güvenlik", "kamu güvenliği", "suçun aydınlatılması", "suçun önlenmesi" kavramlarının sıklıkla kullanıldığı, ancak bu kavramların kanun gerekçelerinde ve Doktrinde kesin hatlarla birbirinden ayrılmadığı, hangi eylemin "milli güvenlik" hangi eylemin "kamu güvenliği" kavramı içinde yer alabileceği belirlenmediği görülmüştür. Bu durumun da verilerin toplama amacının, ölçülülüğünün değerlendirilmesini olanaksız kıldığı anlaşılmıştır. Zira kolluk, soruşturma makamları, yargılama makamları kendi çalışma alanlarını tam anlamıyla Kişisel Verilerin Korunması Kanunu istisnaları içinde görmekte ancak temel ilkelere her halükarda uyulması gerektiği unutulmaktadır.

Tüm bu hususlar, özellikle kolluğun veri toplamasına ilişkin kuralları ortaya koyan normlarda, tüm kuralların detaylandırılmaksızın Kanun'lar ile düzenlenmeye çalışılması, Kanun metninin tekrarı niteliğindeki detaylandırılmamış Yönetmeliklerin uygulama alanında yoruma açık bırakılması gibi sebepleri de üzerinde barındırmaktadır.

Kişisel Verilerin Korunması Hukuku açısından çok açık bir temel değerlendirme yapılacak olursa; kişisel veri toplamak, kaydetmek, saklamak yasak değildir, sadece temel ilkelere uygun davranılması beklenmektedir. Parmak izi verisinin toplanması noktasında da bu çalışmanın amacı, verilerin toplanmasının engellenmesi yada maddi vakıaların ortaya çıkmasına yardımcı olacak bir delili kanunsuz hale getirmek değil, tam aksine böylesine değerli bir verinin hukuka uygun olarak kullanılmasını sağlamaktır. Nitekim önemli olan Hukuk Devleti ilkesine bağlı kalmaktır.

Buna istinaden bir Hukuk Devleti olarak AİHM kararları da öncelikli olarak değerlendirilmek suretiyle süresizlik sonucunu doğuran uzun süreli veri saklama hükümlerinden vazgeçilmeli, kişisel veri hukuku açısından temel ilkeler olan amaca bağlı kullanım, ölçülü saklama ve belirli sürelerde imha ilkelerine uygun normlar yaratılmalıdır.

KAYNAKÇA

Akbulut, P. D. (2023, 08 05). https://www.uralakbulut.com.tr/wp-content/uploads/2012/12/parmakizi.pdf adresinden alındı

AKDENİZ, C. (2021). Polis Mecmuası (1913-1928) Yazılarına Göre Osmanlı Devleti'nde Polis Teşkilatı. S. 364-401.

Bayram, Z. (2009) Yüksek Lisans Tezi, Kolluğun, Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi, İstanbul

Beyli, C. (2006) Bilgi Toplumunda Kişisel Veriler- Kişisel Verilerin Korunması Kanun Tasarısı Üzerine Eleştiriler, İstanbul

Boga, G. (2021) Yüksek Lisans Tezi, Ceza Muhakemesinde Kişisel Verilerin Korunması, Konya

Can, N. (2020) Yüksek Lisans Tezi, Kolluk Ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması, İstanbul

Cantürk, S. (2019). Doktora Tezi. *Robustness Of Fingerprint Verification, Algorithms Against Synthetic Deformations*.

Doğukan Ölmez, E. Ç. (2021, 12 2). Adli Vakaların Çözümlenmesi ve Güvenlik Amacıyla Parmak İzinin Alınmasının Önemi. *Adli Bilimler ve Suç Araştırmaları Dergisi* , s. 29-45.

Dülger, Murat Volkan (2004) Bilişim Suçları, Seçkin, Ankara

Dülger, Murat Volkan (2019) Kişisel Verilerin Korunması Hukuku, 2. Baskı, Hukuk Akademisi, İstanbul

E. Hülya Yükseloğlu, Ş. Ö. (2008). Olay Yeri İncelemesi ve Türkiye'deki Uygulamalar. *Polis Bilimleri Dergisi,* 61-80.

Gemalmaz, Mehmet Semih (2007) Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş, 6. Baskı, Legal.

Gül, F. (2014). Yüksek Lisans Tezi. *Ninhidrinin Schiff Bazı Oluşturma Özelliğinden Faydalanarak Parmak İz Tayininde Kullanılması*. Konya.

Journal of Medical Sciences 2020, 1(5) 46-58

Kızılarslan, Hakan (2007) Ceza Muhakemesi, Adli Tıp, Adli Bilimlerde Vücudun Muayenesi ve Örnek Alma, Kızılarslan Serisi I, Ankara

Kızılırmak, B. (2018) Yüksek Lisans Tezi, Önleyici Amaçla Elde EDİLEN Verilerin Ceza Muhakemesinde Kullanılabilirliği, İstanbul

Kütük, D. (2022) Yüksek Lisans Tezi, Kişisel Verilerin Korunması Hakkı ve İstisnalar, İstanbul

Kolay, F. (2021). Doktora Tezi. *dli Soruşturmalarda Olay Yeri İncelemesinde Elde Edilen Meyve ve Sebzeler Üzerindeki Parmak İzinin Tespiti ve Zamana Bağlı Değişimi*. Ankara, Türkiye.

Komarinski, P. (2004). *Automated Fıngerprınt Identıfıcatıon System (AFIS).* Academic Press.

Küzeci, E. (2018). *Kişisel Verilerin Korunması.* Turhan Kitabevi Yayınları.

LYON, David (1997) Elektronik Göz, Gözetim Toplumunun Yükselişi, çev. Dilek HATTATOĞLU, Sarmal, İstanbul

Neil Yager, A. A. (2004). Fingerprint Classification: A Review. Pattern Anal Applic. s. 77-93. doi:https://doi.org/10.1007/s10044-004-0204-7

Özdilek, A. O. (2008). *İnternet ve Hukuk.* Papatya Yayıncılık.

Poggi, G. (2019). *Modern Devletin Gelişimi Sosyolojik Bir Yaklaşım.* İstanbul Bilgi Üniversitesi Yayınları.

Richard Saferstein, T. R. (2021). *Criminalistic An Introduction to Forensic Science.* New York: Pearson.

İnternet Siteleri

- www.mevzuat.gov.tr
- https://www2.tbmm.gov.tr/d23/1/1-0576.pdf
- https://kararlarbilgibankasi.anayasa.gov.tr/
- https://www.coe.int/en/web/conventions/home
- https://eur-lex.europa.eu/homepage.html
- https://edps.europa.eu/_en
- https://curia.europa.eu/jcms/jcms/j_6/en/
- https://www.oecd.org/

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

AD: Burak

SOYAD: Sucaklı

EĞİTİM

- **İstanbul Haydarpaşa Lisesi**
- **İstanbul Üniversitesi Hukuk Fakültesi**
- **Üsküdar Üniversitesi, Adli Bilimler (Yüksek Lisans)**

YETKİNLİKLER

- Microsoft Office (Word, Excel, Powerpoint)