



İŞÇİYE AİT KİŞİSEL VERİLERİN KORUNMASI

YİĞİT EFE LİMONCUOĞLU

Yüksek Lisans Tezi

Lisansüstü Eğitim Enstitüsü

İzmir Ekonomi Üniversitesi

İzmir

2022

İŐÇİYE AİT KİŐİSEL VERİLERİN KORUNMASI

YİĐİT EFE LİMONCUOĐLU

İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü

Özel Hukuk Anabilim Dalı'na

Yüksek Lisans Tezi

olarak sunulmuştur.

İzmir

2022

ÖZET

İŞÇİYE AİT KİŞİSEL VERİLERİN KORUNMASI

Limoncuođlu, Yiđit Efe

Özel Hukuk Yüksek Lisans Programı

Tez Danışmanı: Doç. Dr. Siyami Alp Limoncuođlu

Ocak, 2022

Teknolojik gelişmelerin ilerlemesiyle kişilerin verilerinin işlenmeye tabi tutulması yaygınlaşmakta ve bu durum iş ilişkisine de yansımaktadır. İşverenler, yeni oluşturulan sistemlerle işçilerin kişisel verilerini işlemekte ve işçilerin özel hayatlarının gizliliğine müdahalede bulunmaktadır. İşverenlerin işçiyi gözetme borcu kapsamında işçilerin kişisel verilerini koruma yükümlülüđü bulunmaktadır. Aynı zamanda işverenlerin işçilerin kişisel verilerini işlemeleri hususunda yerine getirmeleri gereken kanuni düzenlemeler, işçinin üstün yararı, işleme faaliyetinin sözleşmenin ifası için gerekli olması gibi haklı menfaatleri bulunmaktadır. İşverenin haklı menfaati ile işçinin özel hayatın gizliliđi arasındaki dengenin hakkaniyetli biçimde kurulması önemlidir. Kişisel Verilerin Korunması Kanunu uyarınca düzenlenen ilkelere ve belirlenen usullere riayet edilmeksizin işçilerin kişisel verilerinin işlenmesi hukuka aykırılık teşkil etmektedir. İşyerlerinde uygulanan kamera ile gözetleme, araç takip sistemi, yüz, parmak izi, retina tarama gibi biyometrik sistemler Kanun'da belirlenen esas ve usullere uygun yürütülmediğinden işçilere ait

kişisel verilerin hukuka aykırı olarak elde edildiği gibi, bu veriler gerekçe gösterilerek işçilere yaptırımlar uygulanmaktadır. Bu durumu önleyebilmek adına, iş ilişkisi içerisinde ve dışında işçilerin kişisel verilerinin işlenmesi faaliyetlerinin hukuka uygun olup olmadığının tespiti yapılmalıdır. Bu çalışmanın konusunu, iş ilişkisi henüz başlamadan, iş ilişkisi esnasında ve iş ilişkisi bittikten sonra işçilerin kişisel verilerinin ne tür işleme faaliyetlerinin konusu olduğu, işçilere ait kişisel verilerin nasıl korunması gerektiği ve işçilerin kişisel verilerinin ihlal edilmesi halinde işçilerin sahip olduğu hak ve talepler ile işverenlerin karşılaşacağı yaptırımlar oluşturmaktadır. Bu bağlamda öncelikle kişisel veri kavramı tanımlanmış, veri koruma hukukuna dair ulusal ve uluslararası kaynaklar incelenmiş, genel anlamda kişilerin verilerinin korunması hususu açıklanmış ve bahsedilen hususlar işveren-işçi arasındaki iş ilişkisi çerçevesinde değerlendirilmiştir.

Anahtar Kelimeler: Kişisel veri, iş ilişkisi, kişisel verilerin işlenmesi, kişisel verilerin korunması

ABSTRACT

PROTECTION OF PERSONAL DATA RELATED TO WORKER

Limoncuođlu, Yiđit Efe

Master's Program in Private Law

Advisor: Assoc. Prof. Dr. Siyami Alp Limoncuođlu

January, 2022

With the technological developments advancing, the processing of the personal datas becomes widespread and this situation reflects on labour relationships. Employers are interfering workers' right of privacy by processing their personal datas. Employers also have to protect workers' datas according to the obligation to look after workers. Concurrently, employers may have fair interests in spect of processing workers' personal data such as; fulfilling a legal obligation, workers' best interest, the activity of processing personal data being required for carrying out a contract. It's important to tread a fine line between employers' fair interests and workers' right of privacy. Practices in workplace are processing and acquiring personal datas illegally by not following the basis and procedures regulated by the Act. In addition, based on these illegally acquired datas, employers are imposing sanctions on workers. In order to prevent this situation, the activities of processing worker's personal data must be determined whether they abide by the law or not. This study analyzes which data processing activities are conducted before establishing, throughout and after the labour

relationship ends, how worker's data should be protected, which rights workers have and which sanctions will be imposed on employers if workers' personal data have been violated. In this regard; primarily the concept of personal data was defined; national and international resources regarding data protection law were examined; protection of personal data were explained in general manner; and all mentioned matters were evaluated within the scope of labour relationship.

Keywords: Personal data, labour relationship, processing personal data, protection of personal data



Çok kıymetli avukat, yazar ve düşün adamı merhum İbrahim Önder
LİMONCUOĞLU'na İthafen



TEŐEKKÜR

Yüksek lisans eğitimin boyunca fikir ve nasihatleriyle yardımlarını asla esirgememiş olan danışmanın Sayın Doç. Dr. Siyami Alp LİMONCUOĞLU'na, lisansüstü eğitimime önayak olan ve her alanda sınırsız destek sağlayan Banu LİMONCUOĞLU'na, avukatlık stajı ve mesleđi ile yüksek lisans eğitimi bir arada yürütememe imkân sağlayan ve bu nedenle çalışmamı hazırlamamda bana çok büyük yardımları dokunan Av. Sabit Emre LİMONCUOĞLU'na, çalışmanın hazırlanma sürecinde bana destek olan, kontrollerimi yapmamda ve imla yanlışlarını düzeltmemde bana yardımcı olan çok sevgili Ceren Perihan GÖNÜL'e, manevi destekleriyle sürecin sorunsuz geçmesini sağlayan arkadaşlarıma ve lisansüstü eğitimim başta olmak üzere hayatımın her döneminde maddi ve manevi anlamda yanımda olan aileme en içten teşekkürlerimi sunarım.

İÇİNDEKİLER TABLOSU

ÖZET.....	iii
ABSTRACT.....	v
İTHAF.....	vii
TEŞEKKÜR.....	viii
İÇİNDEKİLER TABLOSU.....	ix
KISALTMALAR LİSTESİ.....	xii
BÖLÜM 1: GİRİŞ.....	1
BÖLÜM 2: KİŞİSEL VERİ.....	5
2.1 Kişisel Verinin Tanımı.....	5
2.2 Kişisel Verilerin Unsurları.....	6
2.2.1 Bilgi unsuru.....	6
2.2.2 Kişi Unsuru.....	8
2.2.3 Kişinin Belirli veya Belirlenebilir Olma Unsuru.....	11
2.3 Kişisel Verinin Hukuki Niteliği.....	12
2.3.1 Mülkiyet Hakkı ile İlişkisi.....	13
2.3.2 Fikri Mülkiyet Hakkı ile İlişkisi.....	15
2.3.3 Kişilik Hakkı ile İlişkisi.....	17
2.3.4 Kişisel Verilerin Hukuki Niteliğine İlişkin Değerlendirme.....	19
2.4 Kişisel Verilerin İşlenmesi.....	21
2.5 Hassas (Özel Nitelikli) Veri Kavramı.....	22
BÖLÜM 3: KİŞİSEL VERİLERİN KORUNMASI HAKKININ HUKUKİ DAYANAKLARI.....	28
3.1 Kişisel Verilerin Korunması Hakkında Uluslararası Kaynaklar.....	28
3.1.1 Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Rehber İlkeleri.....	29
3.1.2 Uluslararası Çalışma Örgütü (ILO) İşçilerin Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu.....	33
3.1.3 Avrupa Konseyi'nin 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi.....	36

3.1.4 95/46/EC Bireylerin Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Açısından Korunması Hakkında Direktif.....	40
3.1.5 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR).....	44
3.2 Kişisel Verilerin Korunması Hakkında Ulusal Kaynaklar.....	54
3.2.1 1982 Anayasası.....	55
3.2.2 5237 Sayılı Türk Ceza Kanunu.....	58
3.2.3 4857 Sayılı İş Kanunu.....	59
3.2.4 İş Sağlığı ve Güvenliği Mevzuatı.....	61
BÖLÜM 4: KİŞİSEL VERİLERİN KORUNMASI KANUNU.....	63
4.1 6698 Sayılı Kişisel Verilerin Korunması Kanunu.....	63
4.2 6698 Sayılı Kanun'un Kapsamı.....	65
4.3 KVKK'ya Özgü Terimlere Dair Tanımlar.....	68
4.4 Temel İlkeler.....	69
4.5 Normal Nitelikli Verilerin İşlenmesi.....	71
4.6 Özel Nitelikli Verilerin İşlenmesi.....	75
4.7 Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi.....	78
4.8 Üçüncü Kişilere Veri Aktarımı.....	81
4.9 Veri Sorumlusunun Yükümlülükleri.....	83
4.9.1 Veri Sorumlusunun Aydınlatma Yükümlülüğü.....	83
4.9.2 Veri Güvenliğine İlişkin Yükümlülükler.....	84
4.9.3 Veri Sorumluları Sicili'ne Kayıt Yükümlülüğü.....	87
4.9.4 Kişisel Veri Envanteri.....	88
4.10 İlgili Kişinin Hakları.....	89
BÖLÜM 5: İŞÇİLERİN KİŞİSEL VERİLERİNİN KORUNMASI.....	92
5.1 Kişisel Verilerin İşlenmesinin İşverenin Gözetme Borcu İle İlişkisi.....	93
5.2 İşçi Adaylarının İş Sözleşmesinin Kurulmasından Önce Kişisel Verilerinin Korunması.....	94
5.2.1 Kişisel Duruma İlişkin Sorular.....	97
5.2.2 Eğitime İlişkin Sorular.....	98
5.2.3 Sağlığa İlişkin Sorular.....	99
5.2.4 Engellilik Durumuna İlişkin Sorular.....	100

5.2.5 Hamileliğe İlişkin Sorular	100
5.2.6 Hükümlülüğe İlişkin Sorular.....	101
5.2.7 İnanışa, Sendika Üyeliğine ve Siyasi Düşüncelere İlişkin Sorular.....	102
5.3 İşçilerin İş Sözleşmesi Süresince Kişisel Verilerinin Korunması.....	104
5.3.1 İşçinin Giriş-Çıkışlarının Denetlenmesi	104
5.3.2 İşçilerin Elektronik Ortamda İzlenmesi ve Gözetlenmesi.....	107
5.3.3 İşçinin İletişiminin Gözetlenmesi.....	110
5.4 İş Sözleşmesi Sona Erdiğinde İşçilerin Kişisel Verilerinin Korunması	115
5.5 İşçilere Ait Kişisel Verilerin Hukuka Aykırı İşlenmesinin Yaptırımları.....	116
BÖLÜM 6: SONUÇ.....	122
KAYNAKÇA.....	127

KISALTMALAR LİSTESİ

AB : Avrupa Birliđi

ABAD : Avrupa Birliđi Adalet Divanı

Bkz. : Bakınız

CNIL : Fransa Ulusal Veri Koruma Komisyonu (Commission nationale de l'informatique et des libertés)

Direktif : 95/46/EC Bireylerin Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Açısından Korunması Hakkında Direktif

EDPB : Avrupa Veri Koruma Kurulu (European Data Protection Board)

GDPR : Avrupa Birliđi Genel Veri Koruma Tüzüğü (General Data Protection Regulation)

ILO : Uluslararası Çalışma Örgütü (International Labour Organization)

Kurum : Kişisel Verileri Koruma Kurumu

Kurul : Kişisel Verileri Koruma Kurulu

KVKK : Kişisel Verilerin Korunması Kanunu

KVSYAY: Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik

m. : Madde

OECD: Ekonomik İşbirliđi ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development)

SGK : Sosyal Güvenlik Kurumu

Sözleşme : 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

STİSK : Sendikalar ve Toplu İş Sözleşmesi Kanunu

TBB : Türkiye Barolar Birliđi

TBK : Türk Borçlar Kanunu

TCK : Türk Ceza Kanunu

TDB : Türk Diş Hekimleri Birliđi

TEB : Türk Eczacılar Birliđi

TESK : Türkiye Esnaf ve Sanatkarları Konfederasyonu

TMMOB : Türk Mühendis ve Mimar Odaları Birliđi

TMK : Türk Medeni Kanunu

TOBB : Türkiye Odalar ve Borsalar Birliđi

TODAİE : Türkiye Orta Dođu Amme İdaresi Enstitüsü

TTB : Türk Tabipleri Birliđi

TÜRMOB : Türkiye Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler Odaları Birliđi

Tüzük : Avrupa Birliđi Genel Veri Koruma Tüzüğü

TVHB : Türk Veteriner Hekimleri Birliđi

TZOB : Türkiye Ziraat Odaları Birliđi

VERBİS : Veri Sorumluları Sicil Bilgi Sistemi

BÖLÜM 1: GİRİŞ

21. yüzyılla birlikte gelişen teknoloji, beraberinde teknolojiye ilişkin yeni kavramları getirmiştir. Kişisel veriler de işbu kavramlardan bir tanesidir. Kişisel veriler, şahıslara ait gerek fiziki gerekse internet yani sanal ortamdaki bilgilerini ifade etmektedir. Bu bilgiler şahsın ismine ve görüntüsüne ilişkin bilgileri, mesleki bilgileri, sağlık ve düşüncelerine ilişkin bilgiler olabileceği gibi; kişinin söz konusu internet sitesini ne kadar ziyaret ettiği, kişinin arama motorlarında en çok hangi tekstil ürünü arattığı, internette beğendiği fotoğrafların en yaygın hangi ürüne ilişkin olduğu gibi bilgiler de kişisel veri statüsündedir. Dolayısıyla kişisel veriler, şahısların sosyal medya platformları üzerinde paylaştıklarından çok daha geniş bir veri grubunu oluşturmaktadır.

Şahısların kişisel verileri çeşitli firmalarca ekonomik amaçlarla toplanmakta, saklanmakta ve aktarılmaktadır. Herkesçe kullanılan Google, Amazon, Facebook gibi uygulamalar, kar marjlarını artırabilmek adına sitelerini ziyaret eden şahısların bilgilerine erişmekte ve kişilere daha yatkın ve isabetli hizmet sunabilmek adına bu bilgileri işleyerek kişilerin karşısına ilgilerini daha fazla çekebilecek arama sonuçları, ürünler, yazılar, başlıklar çıkarmaktadır. Hatta, bahsettiğimiz bu amaçlarla üçüncü kişilerle veri alım-satımı bile gerçekleştirebilmektedir. Bu faaliyetler şahsın kişisel verilerinin işlenmesini ifade eder. Kişilere ait bu verilerin işleme faaliyetinden dolayı kimi zaman veri sahibi şahıslarca istenmeyen sonuçlar ortaya çıkmaktadır. Örneğin, kişinin bir internet sitesinde başka bir kişiyle tartıştığını gösteren bir videonun, aynı kişinin bir firmada tezgahlar pozisyonunda iş başvurusunda bulunması sonucu söz konusu videoyu gören işveren tarafından işe alınmaması durumları yaşanabilir. Bu tür durumlarda kişilerin kişisel verilerinin korunması hakları ihlal edilmektedir. Zaten halihazırda ekonomik olarak firmalardan zayıf konumda bulunan şahısların verilerinin ihlal edilmesi ile mağdur duruma düşürülmesine karşı şahıslara kişisel verilerinin korunması kapsamında belirli haklar tanınmıştır. Bu haklar da veri koruma hukukunun konusunu oluşturmaktadır.

Kişisel verilerin korunması hakkı Anayasamız tarafından korunan temel hak ve özgürlüklerden biri olup, çoğu zaman diğer haklarla ilişkilendirilmektedir. Özel yaşamın gizliliği, haberleşme hürriyeti, mahremiyet, düşünce ve kanaat özgürlüğü, din ve vicdan özgürlüğü bu haklardan birkaçıdır. Hakların bazı durumlarda şahsa ait aynı

şeyi koruduğu olsa da; bu haklar birbirlerinden farklıdır. Kişiler arasında gizli olan bir haberleşme faaliyetinin üçüncü şahıslarca açığa çıkarılması, kişilerin hem Anayasa'nın 22. maddesinde düzenlenen haberleşme hürriyetinin, hem de 20/3. maddesinde düzenlenen kişisel verilerin korunması hakkının ihlali sonucunu doğurmaktadır. Aynı şekilde, iş başvurusunda adaya hangi siyasi partiye oy verdiğinin sorulması, adayın hem kişisel verilerinin korunması hakkına hem de Anayasa'nın 25. maddesinde düzenlenen düşünce ve kanaat özgürlüğüne aykırılık teşkil etmektedir. Bu durumda aday işçide, soruyu cevaplamaması halinde işe alınmayacağı korkusu oluşacağından aday işçinin düşüncelerini açıklamaya zorlanması söz konusudur. Aynı şekilde işverenin, aday işçinin hangi siyasi partiye oy verdiği bilgisine erişmekte herhangi bir hukuka uygunluk sebebi bulunmadığından ve söz konusu durumda işçinin rızası da olmadığından aday işçinin kişisel verilerinin korunması hakkının ihlal edildiği söylenebilir. Ancak kişilerin belirli bir işyerine dini simgeleri ile birlikte gelememeleri işçilerin anayasal hakları olan din ve vicdan özgürlüğü haklarına müdahale teşkil ederken, veri koruma hukuku açısından herhangi bir sonuç doğurmamaktadır. Görüldüğü üzere, kişilerin verileri üzerinde yapılan bir işlem, kişisel verilerin korunması hakkı ile birlikte verilerin türüne göre düşünce ve kanaat özgürlüğü veya haberleşme hürriyeti gibi temel hak ve hürriyetlere müdahale teşkil ederken, özel hayatın gizliliği veya haberleşme hürriyeti haklarına aykırı her işlem kişisel verilerin korunması hakkına da aykırılık teşkil etmemektedir. Dolayısıyla bu hakların koruma kapsamının çakıştığı durumlar bulunsa da; hakların özü bakımından farklılıkları bulunmaktadır. Zira, Anayasada farklı maddeler veya fıkralarla düzenlemeleri de bu hususu destekler niteliktedir.

Kişisel verilerin korunmasına ilişkin hukukumuzda 2016 yılına kadara herhangi bir mevzuat bulunmamaktaydı. İç hukukta kişisel verilere ilişkin diğer kanunlarda hükümler bulunmakla birlikte, Türkiye'nin tarafı olduğu uluslararası örgütlerin kişisel verilerin korunmasına ilişkin düzenlemeleri mevcuttur. Türkiye'nin tarafı bulunduğu örgütler tarafından hazırlanan bu uluslararası sözleşmelerin herhangi bir bağlayıcılığı bulunmadığından uygulamada yetersiz kalmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 2016 yılında yürürlüğe girmesiyle veri sahibinin hakları ve veri sorumlusu ve işleyenlerin yükümlülükleri açıkça düzenlenmiş, ilgili kişilerin kişisel verilerinin işlenmesine ilişkin esas ve usuller belirlenmiş, Kişisel Verileri Koruma Kurulu oluşturularak, kişisel verilerin korunması hususunda görüş

sunan ve gerektiğinde adli süreç başlatabilme veya idari boyutta ceza yaptırımını gerçekleştirme yetkisi bulunan bir denetim mekanizması oluşturulmuştur.

Veri koruma hukukunda veri sorumlusunun bulunduğu ülkenin mevzuatına riayet edilmesi yeterli değildir. Günümüzde veri dolaşımı çoğunlukla ülkeler arası gerçekleştiğinden veri aktarımı yapılan üçüncü kişinin bulunduğu ülkenin mevzuatının da yeterli korumaya sahip olduğundan emin olunmalıdır. Nitekim, Avrupa Birliği'nde an itibariyle yürürlükte olan Avrupa Genel Veri Koruma Tüzüğü uyarınca Avrupa Birliği üyesi olmayan Türkiye üçüncü ülke statüsünde olup, Tüzük kapsamında yeterli koruma sağlaması gerekmektedir. Veri koruma hususunda yapılan ihlallerde üçüncü ülke statüsünde bulunan ülkelerdeki veri sorumlularına da yaptırım uygulanmaktadır. Bu nedenle özellikle sınır ötesi veri aktarımı gerçekleştiren veri sorumlularının yalnızca kendi ülkelerindeki değil, veri aktarımı yapacakları ülkelerin de mevzuatlarına uygun davranmaları gerekmektedir.

İşçi ve işveren ilişkisi de kişisel verilerin işlenmesinin yoğun biçimde gerçekleştiği bir ilişkidir. İşçinin kişisel verilerinin korunması, işverene gözetim borcu kapsamında yüklenilmiş bir yükümlülüktür. İşçilerin kişisel verileri işlenirken, işçilerin özel hayatlarının gizliliği ile işverenin veri işlemedeki menfaati arasındaki dengenin sağlanması gerekmektedir. Önceki paragraflarda bahsedildiği gibi tıpkı bu ilişkide de bir zayıf taraf, bir de güçlü taraf bulunmaktadır. İşçi, ekonomik açıdan işverenden daha zayıf konumda olduğundan tereddütlü hususlarda işçi lehine yorum ilkesi gereği işçinin özel hayatının gizliliğinin muhafazası gerekmektedir. Ancak bu ilke mutlak olmayıp işverenin meşru menfaatinin de göz ardı edilmemesi gerekmektedir.

Uygulamada çoğunlukla işçilerin kişisel verilerinin hukuka aykırı yollarla elde edilmesi sonucu işçilerin iş akitlerine son verilmesi ile karşılaşmaktadır. Bu husus, işçiye iş hukuku bakımından haksız fesih hükümleri gereğince tazminat gibi belirli haklar sağlamakla beraber; işçinin veri koruma hukuku bakımından da işverene başvurarak kişisel verilerinin silinmesini talep etme, uğradığı zararın tazminini isteme ve Kişisel Verileri Koruma Kurul'una şikâyet yoluyla başvurma gibi hakları bulunmaktadır.

İşçinin kişisel verilerinin korunması iş sözleşmesiyle birlikte başlamamakta ve iş sözleşmesinin bitimiyle de bitmemektedir. İş sözleşmesi henüz kurulmamışken iş başvuruları esnasında aday işçilerin kişisel verileri işleme faaliyetine tabi tutulmaktadır. Aynı şekilde işçinin işten ayrılmasından sonra işverenler çeşitli nedenlerle işçilerin kişisel verilerini muhafaza etmektedir.

Çalışmanın ilk bölümünde, kişisel verilerin işlenmesi hususunda bilgi verilecektir. Kişisel verilerin tanımı, unsurları ve hukuki niteliği belirlenecek; akabinde kişisel verilerin işlenmesi faaliyetlerinden bahsedilecektir. Kişisel verilerin işlenmesi konusunda ayırım yapılarak, hem normal nitelikli kişisel verilerin işlenmesi hem de özel nitelikli kişisel verilerin işlenmesi açıklanacaktır. İkinci bölümde ulusal ve uluslararası boyutta veri koruma hukukundan bahsedilecektir. Kişisel verilerin korunması hakkında uluslararası kaynaklar incelenecek; benzerlikleri, farkları ve yürürlükte olan güncel düzenlemeye kadar gerçekleşen değişimler tespit edilecektir. Ulusal kaynaklar kısmında kişisel verilerin korunmasına ilişkin KVKK dışında başka hangi kanunlarda ne tür düzenlemelerin bulunduğu hakkın bilgi verilecek. Üçüncü bölümde Kişisel Verilerin Korunması Kanunu hükümleri irdelenecek ve genel anlamda bütün kişilerin özel nitelikli ve normal nitelikli tüm verilerinin nasıl korunması gerektiği, işlenmesinin hangi ilkelere tabi olduğu, yurtiçine ve yurtdışına aktarımının nasıl gerçekleşeceği, ilgili kişi veri sahiplerinin hakları ile veri sorumluları ve veri işleyenlerin yükümlülüklerinin neler olduğu açıklanacaktır. Son bölümde ise işçilerin kişisel verilerin korunması hususu değerlendirilecektir. Bu değerlendirme iş ilişkisi kurulmadan önce işçilerin kişisel verilerinin korunması, iş ilişkisi süresince işçilerin kişisel verilerinin korunması ve iş ilişkisi bittikten sonra işçilerin kişisel verilerinin korunması olmak üzere üç ayrı başlık altında yapılacaktır. Son olarak işçilerin kişisel verilerinin hukuka aykırı işlenmesinin hukuki yaptırımlarından ve bu durumda işçilerin ileri sürebileceği hak ve taleplerden bahsedilecektir. Sonuç bölümünde ise bütün bulgular değerlendirilerek işçiye ait kişisel verilerin korunmasının yeterli olup olmadığı tespit edilecektir.

BÖLÜM 2: KİŞİSEL VERİ

2.1 Kişisel Verinin Tanımı

Kişisel Veri kavramı, literatür, mevzuat ve içtihatlarca birden çok kez tanımlanmaya çalışılmış bir kavramdır. Bu kavram ilk olarak karşımıza 1980 senesinde Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)'nün Kişisel Verilerin Korunması ve Sınır Ötesi Akımların Korunması Rehberi'nde “*tanımlanmış veya tanımlanabilir bir kişi ile ilgili herhangi bir bilgi*” şeklinde karşımıza çıkmaktadır¹. 6698 sayılı Kişisel Verilerin Korunması Kanunu²'nun (KVKK) tanımlar alt başlıklı 3. maddesinde “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır. 108 sayılı Sözleşme olarak da bilinen Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Avrupa Konseyi Sözleşmesi³'nin tanımlar bölümünde de aynı tanım yer almıştır⁴. Keza, Anayasa Mahkemesi'nin 06.03.2013 tarihli 2010/40 Esas, 2012/8 Karar sayılı ve 04.12.2014 tarihli 2013/84 Esas, 2014/183 Karar sayılı kararlarında da kişisel verinin kimliği belirli veya belirlenebilir bir kişiye ait bir bilgi olması⁵ şartı aranmıştır. Ulusal ve uluslararası mevzuatta yakın tanımlamalara sahip olan kişisel veri kavramının en kapsamlı tanımının, “*kişisel verilerin doğrudan ya da dolaylı olarak gerçek bir kişiyle ilgili olabilecek ve onu tanımlanabilir kılan herhangi bir bilgi*”⁶ olduğunu söyleyebiliriz.

¹ Yardımcı, A. (2019). *İş Yaşamında Kişisel Verilerin Korunması: Malatya Büyükşehir Belediyesi Ve İlçe Belediyelerinde Çalışan Personelin Kişisel Verilerinin Korunmasına Yönelik Algı Örneği*. Yüksek Lisans Tezi, Fırat Üniversitesi.

² 6698 sayılı Kişisel Verilerin Korunması Kanunu, *T.C. Resmi Gazete*, Sayı: 29677, 7 Nisan 2016 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

³ 6705 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar Ve Sınıraşan Veri Akışına İlişkin Protokolün Onaylanmasının Uygun Bulduğuna Dair Kanun, *T.C. Resmi Gazete*, Sayı: 29703, 5 Mayıs 2016 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

⁴ Dursun, Y. (2019). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Korunması*. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, s. 4.

⁵ Toprak, B. (2018). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Işığında İşçinin Kişisel Verilerinin Korunması*, Yüksek Lisans Tezi, Ankara Yıldırım Beyazıt Üniversitesi, s. 4.

⁶ Yardımcı, A., (2019), s. 12.

2.2 Kişisel Verilerin Unsurları

Literatürde kişisel verilerin unsurlarının üç adet olduğu kabul edilmiştir. Bir kişisel veriden bahsedilebilmesi için (1) ortada bir bilgi olmalı, (2) bu bilgi bir kişiye ait olmalı ve son olarak (3) bahsi geçen bu kişi belli veya belirlenebilir olmalıdır.

2.2.1 Bilgi unsuru

Bu unsurda karşımıza üç kavram çıkmaktadır. Veri, bilgi ve enformasyon. Üçü de birbirinden farklı kavramlar olup, anlam olarak bir hayli benzerlik gösterdiklerinden çoğu zaman karıştırılabilmekte ve birbirleri yerine kullanılabilir. Bilginin, insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat ve benzeri şekillerde birden fazla tanımı mevcuttur. Fakat konumuz ile bağlantılı ve en faydalı tanımı, kurallardan yararlanarak kişinin veriye yönelttiği anlam olabilir⁷. Bu tanımdan yola çıkarak anlam yüklenebilen veri parçalarının bilgileri oluşturduğunu söyleyebiliriz. Zira internet, çok yüksek miktarda verinin dolaştığı uçsuz bucaksız bir kara delik niteliğinde olup, içerisinde anlamlı veya anlamsız birden çok veri barındırmaktadır. Bu verilerinden anlam yüklenebilenler bilgi vasfını sağlayabilecektir.

Fransızca kökenli olan ve haberleşme anlamına gelen enformasyon kelimesi ise filtrelenmesi ve işlem geçirmesi sonucu kullanılabilen veriler⁸ olarak tanımlanmıştır. Görüldüğü üzere enformasyonun tanımı, bir önceki paragrafta kullanmış olduğumuz bilgi tanımı ile oldukça benzerlik göstermektedir. Bu kavramların ayrımı şu şekilde yapılabilir; enformasyonun yapıtaşı veriler olup, bilginin yapıtaşını ise enformasyonun oluşturması, aralarında hiyerarşik olarak bir alt-üst ilişkisinin bulunması ve önceki paragrafta bahsettiğimiz üzere, anlamlı verilerin bilgiyi oluşturmasıdır⁹.

Mevzuatta “*her türlü bilgi*” ibaresi ile kişisel verilerin kapsamı oldukça geniş tutulmuştur. Bu “*her türlü bilgi*” ifadesi kişilere ait nesnel ve öznel bilgileri de kapsayacaktır. Bu halde bilgilerin kimlere göre ve hangi kriterlere göre doğru olduğu

⁷ Türk Dil Kurumu. (2021). *Bilgi* [Çevrimiçi], Erişim adresi: <https://sozluk.gov.tr/>. (Erişim Tarihi: 19.03.2021)

⁸ Yardımcı, A., (2019), s. 15.

⁹ Elbir, N. (2020), *Kişiliğinin Korunması Bağlamında İşçiyeye Ait Kişisel Verilerin Korunması*, Doktora Tezi, Ankara Üniversitesi, s. 39.

veya olmadığı şeklinde muğlak bir durum ortaya çıkacaktır. Diğer bir deyişle kişilerin verilerinin doğruluğunun işbu verilerin korunmasında bir kriter olarak alınıp alınmayacağı sorusu söz konusudur. Mevcut uluslararası mevzuat olan Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) uyarınca kurulan Avrupa Veri Koruma Kurulu'ndan önce yürürlükte olan Avrupa Birliği Konseyi'nin 29. Madde Çalışma Grubu (Article 29 Data Protection Working Party) ilkeleri uyarınca bir bilgi gerçeğe aykırı nitelikte olsa dahi kişisel verilerin korunmasına tabidir¹⁰.

Bir örnekle desteklemek gerekcek olursa, ünlü bir kişinin hakkında gazetelerde yayınlanan olumsuz nitelikte ve gerçeğe bağdaşmayan bir bilginin kişisel verilerin korunması ilkeleri uyarınca koruma kapsamı altına alınıp, işbu verinin işletilmesinin ve aktarılmasının kısıtlanması icap edecektir. Zira işbu veri her ne kadar doğru olmasa da kişinin gerek maddi gerekse manevi bütünlüğüne ve diğer kişilik haklarına zarar verebileceğinden gerçekten de bu tür verilerin korunması gerektiğinden söz edebiliriz.

Kanımızca kişisel verilerin kapsamının “her türlü bilgi” şeklinde geniş ve ucunun açık tutulması, koruma kapsamı hususunda bir eksiklik yaşanmaması için önemlidir. Kapsam altına alınan bilgilerin liste halinde yazılması, yazılmayan bilgilerin kapsam dışı tutulacağı sonucunu doğuracağından; bu şekilde geniş bir tanım yapılması hem bu problemin önüne geçmiştir hem de ileride ortaya çıkabilecek yeni bilgi türlerini de gözeterek koruma kapsamına alınmasına ön ayak olacaktır.

Bununla birlikte, Avrupa İnsan Hakları Mahkemesi tarafından kişisel veri olarak kabul edilen bazı bilgiler mevcuttur. Bunlar;

- a) cinsiyet, medeni hal, doğum yeri, etnik kimlik ve diğer hassas bilgiler hakkında zorunlu bilgilerin toplandığı resmi nüfus sayımları;
- b) parmak izleri, görüntüler, hücre örnekleri, DNA profilleri;
- c) tıbbi verilerin ve diğer tıbbi kayıtların toplanması ve saklanması;
- d) finansal ve ticari bilgiler;
- e) telefon görüşmeleri;

¹⁰ Aksoy, H. C. (2010) *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, İnci Bası. Ankara: Çakmak Yayınevi s. 14-15.

- f) idari ve kişisel amaçlar için kurulan sağlık, sosyal ve finansal veri tabanları gibi kişisel tanımlama sistemi;
- g) kamuya açık caddelerde görüntü yakalayan kameralar;
- h) hapishanelerde tutuklu veya mahkumları izleyen gözetim sistemleri şeklinde sıralanabilir¹¹.

2.2.2 Kişi Unsuru

Başlangıçta yapılan kişisel veri tanımında yola çıkarak, kişisel verinin kimliği belirli veya belirlenebilir bir kişiye ait olma zorunluluğundan bahsedilmiştir. İşbu kişinin kimliğinin belirli yahut belirlenebilir olması hususu ayrı bir başlık altında incelenecek olup, bu kısımda söz konusu kişinin özelliklerine değinilmelidir.

Kişisel verilerin hangi kişilere ait olması gerektiği hususunda literatürde geçen en tartışmalı konulardan biri şüphesizdir ki bu verilerin gerçek kişilere mi, tüzel kişilere mi ait olması gerektiği hususudur. Bu sorunun mutlak bir cevabı olmayıp, cevabın düzenlemeden düzenlemeye göre değiştiğini söylemek yanlış olmayacaktır.

Nitekim, kişisel verilerin korunması hakkında en yetkin sayılabilecek iki düzenleme olan 95/46/EC sayılı Avrupa Birliği Konseyi Direktif'i ve onun yerini almış bulunan Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) yalnızca gerçek kişilerin kişisel verilerini koruma kapsamı altına almıştır. Buna karşın 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Avrupa Parlamentosu ve Konsey Direktifi'nin kapsam bölümünde hem gerçek kişilerin hem de tüzel kişilerin söz konusu sektörde bulunan kişisel bilgilerini koruma kapsamına almıştır¹².

Bu düzenlemeler uluslararası sözleşmeler olup, temel hak ve özgürlüklerin en azından asgari düzeyde korunması amacını taşır. Bir başka deyişle, işbu uluslararası sözleşmelerde yazılı kurallar olması gereken en alt seviye korumayı teşkil etmektedir. Dolayısıyla bu sözleşmeler, daha geniş çerçevede koruma sağlayan bir iç hukuk düzenlemesinin uygulanmasının önüne geçmeyecektir. Zira bahsi geçen sözleşmelerde de kapsamın genişletilmesini kısıtlayıcı hükümler bulunmamaktadır. Gerçekten de, Avrupa Birliği'ne üye ülkeler olan Avusturya, Danimarka, İtalya ve

¹¹ Yardımcı, A., (2019), s. 12-13.

¹² Aksoy, H. C., (2010), s. 18.

Lüksemburg ülkelerinin iç hukuklarında kişisel verilerin gerçek yahut tüzel kişi gözetmeksizin korunduğu görülmektedir. Avrupa Birliği dışında İzlanda, Norveç ve İsviçre ülkeleri de bu tarz koruma biçimini benimsemiştir¹³. Buna karşın Fransa, GDPR'nin yürürlüğe girmesiyle güncellediği mevzuatında aksi kararlaştırılmadıkça GDPR'deki tanımların geçerli olacağını düzenleyerek, kişisel verilerin tanımını gerçek kişileri kapsayacak şekilde yapmıştır. Aynı şekilde İngiltere 2018'de yürürlüğe geçirdiği “*Veri Koruma Tüzüğü*”nde kişisel verilerin tanımını “*kimliği belirli veya belirlenebilir yaşayan kişilere ilişkin her türlü bilgi*” şeklinde düzenleyerek sadece gerçek kişilerin kapsama altına alındığını açıkça belirtmiştir. Belçika ise daha doğrudan bir yol tercih edip, iç hukukundaki kişisel verilerin korunması hakkındaki ana düzenlemesini “*Kişisel Verilerin Korunması Bakımından Gerçek Kişilerin Korunması Hakkında Kanun*” olarak adlandırarak tüzel kişileri tümüyle kapsam dışı bırakmıştır¹⁴.

Mevzuatımızda bu konu hakkında bir bütünlük sağlanmamış olup, sektörel farklılık görülmektedir. Kişisel Verilerin Korunması Kanunu'nun tanımlar kısmı 3. maddesinde gerçek kişi kavramı kullanılmıştır. Türkiye'de kişisel verilerin korunmasından sorumlu kurum olarak nitelendirilen Kişisel Verileri Koruma Kurumu (Kurum)'nun internet sitesinde yaptığı açıklamada Kişisel Verilerin Korunması Kanunu'nun süjesinin yani koruduğu “*ilgili kişinin*” gerçek kişiler olduğu belirtilmiştir.¹⁵ Fakat elektronik haberleşme sektörüne baktığımız zaman, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik¹⁶'te kişisel veri tanımının hem gerçek hem de tüzel kişileri kapsayacak şekilde yapılmış olduğunu görürüz¹⁷.

Bu düzenlemelerin amacına baktığımız zaman, düzenlemelerin sektörlerine göre gerçek veya tüzel kişilerin kişisel verilerini korumalarının isabetli olduğunu söyleyebiliriz. Zira tarafları gerçek ve tüzel kişi olan bir etkileşimde, bu etkileşimde zayıf olacak tarafın, yani kişisel verisinin korunmasına ihtiyaç olan tarafın gerçek kişi

¹³ Aksoy, H. C., (2010), s. 19.

¹⁴ Elbir, N., (2020), s. 42.

¹⁵ Kişisel Verileri Koruma Kurumu. *İlgili Kişi Kimdir?* [Çevrimiçi]. Erişim adresi: <https://kvkk.gov.tr/Icerik/2034/Ilgili-Kisi-Kimdir> (Erişim Tarihi: 20.05.2021).

¹⁶ Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, *T.C. Resmî Gazete*, Sayı: 31324, 4 Aralık 2020 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

¹⁷ Beytar, E. (2018) *İşçinin Kişiliğinin Ve Kişisel Verilerinin Korunması*. İnci Bası. İstanbul: On İki Levha Yayıncılık, s. 52.

olduğu açıktır. Zira bankaya kredi çekmek amacıyla giden bir müşteri ile banka arasındaki etkileşimde kişisel verilerinin korunması ihtiyacı taşıyan taraf şüphesiz ki müşteri olan gerçek kişi olacaktır. Fakat iki tarafın da tüzel kişi olduğu etkileşimlerde kişisel verilerin eşit derecede korunması icap edecektir. Dolayısıyla temel düzenlemenin gerçek kişileri kapsam altına alması, tüzel kişilerin verilerinin güvenliğinin tehlikede olduğu durumlarda özel kanunlara eklenecek hükümlerle tüzel kişilerin verilerinin kişisel veri sayılması düşüncemize göre idealdir.

Kişi unsuru ile ilgili bir diğer önemli tartışma ise kişinin sağ olup olmamasının önemidir. Türk Medeni Kanunu¹⁸'nin 28. Maddesi uyarınca kişinin hak ehliyeti sağ doğmak koşuluyla ana rahmine düşüldükten itibaren başlar. “Infans Conceptus¹⁹” adı verilen bu hukuk kuralının söz konusu ceninin kişisel verilerini ilgilendiren durumlarda uygulanıp uygulanmayacağı tartışmalıdır. Konuyla ilgili herhangi ulusal veya uluslararası hukuk normuna rastlanamamış olup, bağlantılı Fransız Yargıtay kararları mevcuttur. Fransız Yargıtay kararlarına göre doğmamış cenine ait sağlık verileri, cenin sağlıklı bir şekilde doğmuşçasına kişisel veriler kapsamında koruma altında olacaktır. Buna göre, doğmamış çocukların tıbbi verilerinin, ergin olmayan bir kişinin tıbbi verileriyle aynı korumaya tabi olacağı sonucuna ulaşılmaktadır²⁰.

Bir diğer tartışma ise kişiliğin bitişinin kişisel veri tanımına etki edip etmeyeceği hususudur. Kısacası, ölü kişilerin verileri kişisel veri kapsamı altında korunabilir mi? 95/46/EC sayılı AB Konseyi Direktifi'nin kişisel verilerin tanımını gerçek kişilerle sınırladığı belirtilmiştir.. Dolayısıyla kişinin ölümüyle de kişilik bittiği için bu esnadan sonra kişiye ait verilerin kişisel veri korumasına tabi olmayacağını söylenebilir. Nitekim, Avrupa Birliği Konseyi'nin 29 Madde Çalışma Grubu'nun 4/2007 sayılı görüşü de bu kanaattedir²¹. Ancak önceki paragraflarda bahsettiğimiz üzere işbu düzenlemeler mutlak olmayıp aksi üye devletlerce kararlaştırılabilir. Kanada hukukunda kişinin verilerinin, ölümünden 20 sene sonra kişisel veri teşkil etmeyeceği hakkında hüküm mevcuttur²². Ölü kişinin kişisel verisi ile yaşayan

¹⁸ 4721 sayılı Türk Medeni Kanunu, *T.C. Resmi Gazete*, Sayı: 24607, 8 Aralık 2001 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

¹⁹ Dictionnaire juridique de Serge Braudo. Infans Conceptus definition. Erişim Adresi: <https://www.dictionnaire-juridique.com/definition/infans-conceptus.php> (Erişim Tarihi: 10.01.2022).

²⁰ Elbir, N., (2020), s. 43

²¹ Elbir, N., (2020), s. 44.

²² “Under the Canadian federal Privacy Act, which governs the personal datahandling practices of federal institutions, information about a person who has been dead for more than 20 years is no longer considered “personal information” when applying certain sections of the Act.”, International

akrabasının kişisel verisinin bağlantılı olduğu durumlarda kişinin kişisel verilerini koruyan düzenlemeler bulunmaktadır²³. Zira genetik bir hastalık söz konusu olduğunda, ölü şahsın sağlık verisinin korunmaması çocuklarının sağlık verisinin korunmayacağı sonucunu doğuracağından, ölü şahsın işbu sağlık verisinin kişisel veri kapsamında korunması isabetlidir. Bir başka örnek ise Fransa'daki Bilişim, Dosyalar ve Özgürlükler Hakkında Kanun uyarınca kişilerin yaşadıkları müddetçe, ölümlerinden sonra kişisel verilerinin saklanması, aktarılması veya silinmesine ilişkin talimatları verebileceği şeklindeki düzenlemedir²⁴. Görülmektedir ki, kişisel veriler kişinin ölümüyle kişisel veri özelliğini kaybetmektedir. Lakin bu kuralın aksine düzenleme getirmek mümkündür.

2.2.3 Kişinin Belirli veya Belirlenebilir Olma Unsuru

Avrupa Birliği Konseyi'nin 29 Madde Çalışma Grubu, "belirli" olmayı, bir kısım insan arasında ayırt edilebilir olmak ve "belirlenebilir" olmayı bir kısım insan içerisinde ayırt edilebilir olmamasına rağmen, bir takım ekstra çabayla ayırt edilebilir olmak şeklinde kabaca tanımlamıştır²⁵. Bunu kısaca özetlemek gerekirse, bir ofis ortamında belirli bir isme sahip tek şahıs mevcutsa, o şahsın ismi bilinerek şahıs tam olarak ayırt edilebildiğinden, şahsın isminin bilinmesi ile artık o şahıs "belirli" olacaktır. Lakin yine aynı ofis ortamında bir başka isme sahip birden fazla şahıs mevcutsa, isim bilinerek istenilen şahıs ayırt edilemeyecektir. Zira birden fazla aynı isimde şahıs mevcuttur. Ancak şahsın isim bilgisinin yanına örnek olarak soy isim, saç rengi ya da boy uzunluğu gibi verilerin eklenmesiyle şahıs tam olarak ayırt edilebilecektir. Dolayısıyla sadece isim bilgisiyle tam olarak ayırt edilemeyen şahıs, şu durumda kimliği "belirlenebilir" konumdadır.

Kişisel Verileri Koruma Kurumu'nun belirli ya da belirlenebilir olma tanımı, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o

Committee of the Red Cross. (2002). *The Missing: Action To Resolve The Problem Of People Unaccounted For As A Result Of Armed Conflict Or Internal Violence And To Assist Their Families, The Legal Protection Of Personal Data & Human Remains* [Çevrimiçi]. Erişim adresi: <https://www.icrc.org/en/doc/resources/documents/misc/5callj.htm> (Erişim Tarihi: 20.05.2021).

²³ Aksoy, H. C., (2010), s. 21.

²⁴ Elbir, N., (2020), s. 44.

²⁵ Elbir, N., (2020), s. 45

kişinin tanımlanabilir hale getirilmesi şeklindedir²⁶. Eğer bir veri kişinin kimliğinin tespitini mümkün hale getiriyorsa kişisel veridir ve artık kişisel veri kapsamında koruma altındadır. Bu durum oldukça muğlak gözükmemekte olup, kime göre belirlenebilir, neye göre belirlenebilir olma konusunda tartışma yaratmaktadır. Örnek olarak; bir bireyin sarışın olması, dünya üzerindeki sarışın bireylerin başka bilgilerinin de bilinmesi halinde bireyi ayırt edilebilir hale getirebilmektedir; ancak belirlenebilir sayılmaz. Zira 95/46/EC sayılı Direktif'in 26. Maddesi gereği kimliği tespit edecek şahsın "makul vasıtalar kullanması" şartı aranmıştır²⁷. Dolayısıyla, dünya üzerinde bir bireyin kimliğini tespit etmek için sadece sarışınlığından yola çıkmak makul olmadığından, kişinin sarışın olması kişiyi belirlenebilir yapmamaktadır. O halde sarışın olmak mevcut örnekte kişisel veri vasfını taşımaz. Böylece kişisel veri kavramının sınırları belirlenmeye çalışılmış olup, kavrama çok geniş anlamlar yüklenilmesinin önüne geçilmiştir.

2.3 Kişisel Verinin Hukuki Niteliği

Kişisel verilerin birden fazla hak ile ilişkilendirilmesi mümkündür. Bu verilerin internet şirketleri tarafından çerezler vasıtasıyla toplandığını ve yüklü miktar para karşılığında reklam şirketleri gibi tüzel kişiliklere satıldığı düşünüldüğünde kişisel verilerin mülkiyet hakkı içerisinde değerlendirilmesi pek olası gözükecektir. Aynı şekilde insanların düşüncelerini dile getirdikleri sosyal medya platformlarındaki yorum ve eleştiri benzeri yazıların kaynak gösterilmeden kullanılması durumunda fikri mülkiyet hakkının ihlalinden söz edilmesi yanlış bir sonuç doğurmayacaktır. Bir başka örnekte, bir kafe ortamında magazin tarafından eşcinsel olduğu belgelenen bir ünlüye ilişkin eşcinsel olduğu bilgisini içeren bir haber, pekâlâ özel hayatın gizliliğine aykırılık ile ilişkilendirilebilecektir. Kişisel verilerin hukuki niteliği ile ilgili somut bir sınır çizilememesinin asıl sebebi, Avrupa Birliği ve Türk mevzuatlarında hakkın niteliği konusunda açık bir düzenleme bulunmamasıdır²⁸. Lakin genel çerçeveye bakıldığında, Anglosakson ekolünde ekonomik bakış açısı olan mülkiyet ya da fikri

²⁶ Kişisel Verileri Koruma Kurumu. *6698 Sayılı Kanun'da Yer Alan Temel Kavramlar* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar> (Erişim Tarihi: 20.05.2021).

²⁷ Aksoy, H. C., (2010), s. 24.

²⁸ Han, I. A. (2020) *Veri Sahibinin Kişisel Veri Üzerindeki Hakkının Hukuki Niteliği Işığında Kişisel Verinin Ticarileşmesi*. Genç Hukukçu Araştırmacılar Sempozyumu. İstanbul: On İki Levha Yayıncılık, s. 517.

mülkiyet hakkı kapsamı altında, Kıta Avrupası ekolünde ise temel hak ve özgürlükçü bir bakış açısı ile kişilik hakkı kapsamı altında değerlendirildiğini görmekteyiz²⁹.

Öğretide kişisel verilerin korunması hakkı üç ana hak kapsamında değerlendirilmiş olup, bunlar; kişilik hakkı, mülkiyet hakkı ve fikri mülkiyet hakkıdır. Çalışmanın bu kısmında bu haklar genel olarak açıklanmaya çalışılıp, kişisel verilerin korunması hakkı ile ilişkisi üzerinde durulacak ve hangisinin kişisel verilerin korunması hakkının hukuki niteliğini oluşturduğu tespit edilecektir.

2.3.1 Mülkiyet Hakkı ile İlişkisi

Gelişen teknoloji ile birlikte kişisel verilere paha biçmek mümkün hale gelmiştir. Büyük kitleler tarafından kullanılan ve tabi oldukları pazarların liderleri olan Apple, Facebook, Google, Amazon gibi şirketlerin kişilerin veriler üzerinden yüklü miktarda para kazandıkları genel geçer bir bilgidir. Dolayısıyla kişisel veriler eşya hukuku uyarınca bir eşya gibi satılmaya, kiralanmaya, kullanılmaya veya saklanmaya başlanmıştır.

Mülkiyet hakkı görüşü uyarınca kişisel verilerin malikinin ilgili kişi, yani veri sahibi olduğu kabul edilmektedir³⁰. Bu bağlamda söz konusu ilgili kişi kendi kişisel verilerinin üzerinde 3 yetkiye sahip olacaktır; kişisel verilerini kullanma, kişisel verilerinin semerelerinden yararlanma ve kişisel verilerini tasarruf etme. Bu görüşü ortaya çıkaran şey ise en büyük serbest piyasa ekonomisine sahip ülkelerden biri olan ABD'nin kişisel verilere bir ekonomik değer verebilmiş olmasıdır³¹. Böylece kişisel verilerin kendi piyasası oluşmuştur. Ayrıca bu görüşü ortaya çıkaran bir başka hususun da kişisel verilerin kişilik hakkıymışçasına korunmasının oldukça geniş kapsamlı bir koruma sağlamasından ötürü görüşün kaynağı olan ABD ekonomisinin bundan kötü etkilenmesi sonucunun doğacağı ihtimalidir³². Bu görüş gereğince internet sitelerinde kişinin verilerinin işleme, aktarma ve benzeri işlemlere tabi tutulacağı haber verilerek ve kişiden buna onay vermesi istenerek, işbu onay alındıktan sonra mülkiyet hakkıyla birlikte gelen kullanma yetkisi süresiz biçimde veri işleyiciye bahsedilecektir. Dahası,

²⁹ Akkurt, S. S. (2020) *Kişisel Veri Kavramının Hukukî Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış*, *Kişisel Verileri Koruma Dergisi*, C. 2(1), s. 21.

³⁰ Aksoy, H. C., (2010), s. 57.

³¹ Elbir, N., (2020), s. 47.

³² Akkurt, S., (2020), S. s. 22.

kişisel verilerini para karşılığında satan bir şahsın artık kendine ait verilerin üzerinde hiçbir tasarruf yetkisinin bulunmaması gibi bir durumla karşılanacaktır³³.

İşbu görüşün eleştirilmesindeki en büyük etmenin bu olduğunu söyleyebiliriz. Zira kişinin kendi inancı, politik düşünceleri, cinsel tercihleri, yaşı ve diğer fiziksel özelliklerine ilişkin verilerin bir başkasının mutlak kontrolünde olması ve kişinin bunlardan feragat etmesi gibi bir durum imkân dahilinde değildir, olmaması da gerekir.

Kaldı ki, mülkiyet hakkı görüşünün kabulü halinde, veri işleyenlerin sorumluluğu bir hayli azalmış olacağından, veriyi işleme tabi tutarken gerekli özenin gösterilmemesi gibi durumlarla karşılaşılması kuvvetle muhtemeldir³⁴. Bu durumda hukuki ilişkide hali hazırda zayıf konumda bulunan veri sahibi ilgili kişinin aleyhine bir sonuç oluşacağından hakkaniyet açısından istenmeyen bir sonuç doğacaktır. Gerçekten de doktrinde tarafların eşit olmamasından kaynaklı bu tarz sorunların çıkacağı öngörülmüştür³⁵.

Özetle mülkiyet hakkı görüşü, pazar açısından bolca avantaj yaratırken, veri sahiplerini korumakta yetersiz kalmaktadır. Bu nedenle Avrupa Birliği ve Türk mevzuatlarında bu görüşün benimsenmediği görülmektedir. Türk hukukunda kişisel verilerin, Türk Medeni Kanunu kaynaklı eşyalara özgü el atmanın önlenmesi, istihkak gibi davaların konusunu oluşturmasının isabetli olmayacağı görüşü mevcuttur³⁶. Ayrıca, Fransız hukukunda da işe yararlık ve sahiplenme olanağının imkansızlığından mütevellit mülkiyet hakkı kapsamına alınamayacağı benimsenmiştir³⁷.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde, "*unutulma hakkı*", "*veri taşıma hakkı*" ve "*eski hale iade*" kurumlarının mülkiyet hakkı görüşünü destekler nitelikte olduğu bazılarınca iddia edilse de; mülkiyet hakkı görüşünün aksine, verileri kişinin hakimiyetinden ayrılmasından sonra dahi korumaya devam etmesi ve verinin kimde olduğu önemsenmeden işbu hakların veri sahibine verilmiş olması

³³ Elbir, N., (2020), s. 48.

³⁴ Elbir, N., (2020), s. 48.

³⁵ "*Gerçekten pazarlıkta taraflar eşit olmadığından, örneğin birey bir devlet kurumunda çalışmak için başvuruda bulunduğu verileri üzerindeki mülkiyet hakkından gönüllü olarak vazgeçmesi doğaldır. Özel sektör açısından da durum pek farklı değildir. Kişisel bilgilerin alınıp satılan bir mal gibi değerlendirildiği bir ortamda, bireyler zarar görür. Bu durumdan yarar sağlayanlar ise şirketler olacaktır. Bir başka ifadeyle, ekonomik yaklaşım ile bireylerin verileri üzerindeki denetimi yeniden kazanabilmeleri olanaklı değildir. Böylesine bir yaklaşım, daha az varlıklı olan kesimin aleyhine olur.*" Küzeci, E. (2010). *Kişisel Verilerin Korunması*, Doktora Tezi, Ankara Üniversitesi, s. 70.

³⁶ Akkurt, S. S., (2020), s. 23-24.

³⁷ Elbir, N., (2020) s. 48.

gerekçeleriyle Avrupa Birliği Genel Veri Koruma Tüzüğü'nün mülkiyet hakkı görüşünü savunmadığını rahatlıkla söyleyebiliriz³⁸.

Kanımızca mülkiyet hakkı görüşü hukuki anlamda isabetli bir sonuç doğurmayıp, kişisel verilerin korunması hakkının özünüyle bağdaşmamaktadır. Zira kişisel verilerin korunması hakkının süjesi veri sahibi olup, kişisel verilerin “eşya” niteliğinde olduğunun kabulü ile veri sahibinin aleyhine sonuçlar doğacaktır. Halbuki kişisel verilerin korunması hakkı ile amaçlanan zayıf konumdaki veri sahibinin kişisel verilerinin, güçlü konumdaki tüzel kişilere karşı olabildiğince korunmasıdır. Mülkiyet hakkı görüşü tam tersine tüzel kişiliklere avantajlar sağlayan bir görüş olduğundan ve herhangi bir kişisel verinin bir eşyaymışçasına tasarruf edildikten sonra söz konusu kişisel veriyi koruma imkanının bitmesinden yahut oldukça zorlaşmasından mütevellit hakkı temsil etmekte yetersiz kalmaktadır. Bu nedenle makul bir görüş değildir.

2.3.2 Fikri Mülkiyet Hakkı ile İlişkisi

Fikri mülkiyet hakkı görüşü, verinin internet üzerinde patentlenebilir olmasından ya da patentlenebilir bir yöntemle üretilmesinden dolayı, patent hakkının sağladığı korumadan yararlanması görüşünü ifade etmektedir³⁹. Üzerine düşünüldüğünde, amaçsal olarak iki hakkın temelinde de (hem kişisel verilerin korunması hakkı, hem de fikri mülkiyet hakkı) kişiye ait olan bilginin korunması ve dağılımının kontrol altına alınması mevcuttur⁴⁰.

Kişisel verilerin korunması hakkıyla fikri mülkiyet hakkının ilişkilendirilmesindeki bir başka sebep ise kişisel verilerin veri sahibinin veri üzerinde sahip olduğu haklar ile, fikri mülkiyette eser sahibinin eser üzerinde sahip olduğu hakların benzerliğidir. Nitekim, fikri mülkiyet hakkının getirdiği imkanlardan olan “*eseri umuma arz yetkisi*” ve “*eserde değişiklik yapılmasını yasaklama yetkisi*”, veri sahibinin kendisine ait verilerinin ne şartlarda saklanacağı, işleneceği veya paylaşılacağı hakkında söz sahibi olması ile benzer nitelikte görülmektedir. Örnek olarak eserde değişiklik yapılmasını yasaklama yetkisi, eser; eser sahibinden başka bir kişinin hakimiyeti altında bulursa dahi, eser sahibinin izni olmaksızın eserin değişikliğe uğratılamayacağını ifade eder. Bu kurum mevzuatımızdaki, veri sahibinin

³⁸ Han, I. A., (2020), s. 522-523.

³⁹ Han, I. A., (2020), s. 530.

⁴⁰ Aksoy, H. C., (2010), s. 60.

açık rızası olmaksızın verilerinin üçüncü kişiler tarafından işlenmesinin ve aktarılmasının yasaklanması durumuyla oldukça benzerlik göstermektedir⁴¹.

Bu görüşe karşı eleştirilerin ortak noktası, hakların konularının farklı olması hususunda birleşmektedir. Zira fikri mülkiyet hakkının konusu olan şey bireyin emek ve zaman harçayarak yarattığı ürün iken, kişisel verilerin korunması hakkında böyle bir tanımlama aranmamaktadır. Önceki bölümlerde bahsedildiği üzere, kişisel verilerin korunması hakkının konusu, ilgili kişiye ait yahut ilgili kişiyle ilişkilendirilebilen her türlü anlamlı bilgidir ki, bunlara kişinin düşüncelerinin veya ifadelerinin dahil edilebileceği gibi kişinin fiziksel özellikleri, yaşı, cinsiyeti, ırk ve dini de dahil edilebilir⁴². Sadece bu husustan yola çıkılarak kişisel verilerin korunması hakkının, fikri mülkiyet hakkından çok daha geniş kapsamlı olduğunu ve fikri mülkiyet hakkının kişisel verilerin korunması hakkını nitelendirmesinde yetersiz kaldığı sonucuna ulaşılabılır.

Bir başka eleştiri ise hakların amacına ilişkindir. Fikri mülkiyet hakkı, hak sahibini umuma karşı ekonomik amaçlarla korurken, veri sahibinin korunmasında böyle bir kaygı güdülmemiştir. Fikri mülkiyet sahibi şahıs eserini oluşturduğunda, eserin umuma açılmasıyla üçüncü kişilere getirilen sınırlamalarla, eser sahibinin bu eserin semeresinden tam anlamıyla yararlanması amaçlanmaktadır. Bir başka deyişle, eser sahibinin eserini yaratırken gösterdiği emek korunmalıdır. Böylece eser sahipleri eser yaratmaya teşvik edilmiş olur. Lakin veri sahibinin kişisel verisi üzerinde bir emeği bulunmamaktadır. Dolayısıyla kişisel veri oluşturmaya teşvik gibi bir durum söz konusu da değildir⁴³.

Bu durum kısa bir örnek ile özetlenirse daha iyi anlaşılabilir. Bir eser sahibinin eserinin kendi rızası dışında bir internet sitesinde korsan olarak paylaşılması durumunda, birden fazla şahıs o esere para vermeden ulaşabileceğinden, eser sahibinin maddi kaybı doğmaktadır. Bu noktada, eser sahibinin telif hakkı gündeme gelerek eser sahibinin; eser kaçak olarak paylaşılmasaydı elde edeceği kazanç korunacaktır. Lakin bir kimsenin, dini, dili, ırkı, cinsel tercihlerinin bir sitede açıklanması durumunda bu verilerin ortadan kaldırılması için kişinin maddi kayba uğramış olması

⁴¹ Aksoy, H. C., (2010), s. 61.

⁴² Elbir, N., (2020), s. 49.

⁴³ Aksoy, H. C., (2010), s. 66-67.

aranmayacağından, veri sahibi kişisel verilerin korunması hakkı dolayısıyla bu verilerin ortadan kaldırılmasını yahut anonimleştirilmesini talep edebilecektir.

Son olarak, fikri mülkiyet hakkının ihlali halinde ortaya çıkacak olan zararın, kişisel verilerin korunması hakkının ihlali durumunda oluşacak zarardan çok daha somut ve tahmin edilebilir olduğunun kabulü gerekmektedir. Dolayısıyla iki hak arasında sonuç bakımından da farklılıklar mevcuttur⁴⁴.

Bu doğrultuda kişisel verilerin hukuki niteliği bakımından fikri mülkiyet hakkı görüşünün, mülkiyet hakkı görüşüne nazaran daha sağlam zemine bastığı görüşüne⁴⁵ katılmaktayız. Ancak kişisel verilerin hukuki niteliğini oluşturmakta yetersiz kaldığı görüşündeyiz. Zira hakların konuları, amaçları ve sonuçları benzer gözükse de birbirinden bir hayli uzaktır. Fikri mülkiyet hakkının ekonomik koruma temelli olmasının kişisel verilerin korunması hakkının özülle bağdaşmaması sebebiyle işbu görüş isabetli değildir. Bu nedendendir ki, görüş doktrin genelinde kabul görmemiştir.

2.3.3 Kişilik Hakkı ile İlişkisi

Kişilik hakları, 16. yüzyılda ortaya çıkan (ya da fark edilmeye başlanan), kişilerin tam ve sağ olarak doğmasından başka şart aranmaksızın kişilere atanan, başlangıçta kişileri devlete karşı korumayı amaçlamış olup, sonradan kişilerin diğer kişilere karşı da ileri sürebilme imkanının ortaya çıktığı haklardır⁴⁶. Bu doğrultuda işbu hakların ölümle de sona ereceğini söyleyebiliriz. Aynı şekilde kişilik hakları, şahsa mutlak surette bağlı haklar olduğundan, başkalarına devredilemez, vazgeçilemez veya zamanaşımına uğrayamazlar. Bir maddi değere sahip olmamalarına rağmen, hakların ihlali durumunda maddi veya manevi olarak tazmin edilebilme durumu söz konusudur⁴⁷.

Kıta Avrupası hukukunda, OECD gibi uluslararası örgütlerin düzenlemelerinde ve hatta 6698 sayılı Kanunu'muzun Genel Gereğesinde kişisel verilerin korunması hakkının bir temel hak olduğu vurgulanmıştır.

⁴⁴ Aksoy, H. C., (2010), s. 67.

⁴⁵ Han, I. A., (2020), s. 530-531.

⁴⁶ Aksoy, H. C., (2010), s. 38.

⁴⁷ Aksoy, H. C., (2010), s. 43-44.

Bir diğerk benzerlik ise, söz konusu haktan feragat edilip edilemeyeceđi hususudur. Zira insan hakları kiřiye sıkı sıkıya bađlı haklar olduđundan, bu hakların devredilmesi yahut bu haklardan vazgeçilmesi kabul görmemektedir. Halbuki mülkiyet hakkı ile iliřikeyi tartıřtıđımız bölümde bahsedildiđi üzere, kiřiisel verilerin korunması hakkında feragat edilmesi, veri üstündeki haklardan da feragat edilebilmesi ve verinin adeta bir eřiaymıřçasına bir başkasına devredilmesi durumuna yol açacaktır. İřbu durumda verinin kiřiye ait olmasına rađmen veri üzerinde tasarruf yapabilme yetkisi bulunmadıđından kiřiisel verilerin korunması kavramıyla amaçlananın tam tersinin gerçekleşeceđi söylenebilir. Zaten halihazırda kiřiisel verilerin korunması hakkının bir insan hakkı gibi devredilemeyeceđini ve iřbu haktan feragat edilemeyeceđi görüřü hakimdir⁴⁸.

Kiřiisel verilerin korunması hakkı ile kiřilik hakkı, mahremiyet ve özel hayatın gizliliđi kavramları üzerinden iliřkilendirilmiřtir. En çok eleřtiri de özel hayatın gizliliđi kavramından ayrıldıđı noktaya getirilmiřtir. Özel hayatın gizliliđi ile, adının da ađıkça ifade ettiđi üzere kiřinin özel hayatındaki gizli olan hususların korunması amaçlanmış olup, kamuda veya aleni herhangi bir ortamda yařanan hadiseler ve bu hadiseler sonucu oluřturulan veriler bu koruma kapsamında deđildir⁴⁹. Ancak önceki bölümlerde de ađıklandıđı üzere, kiřiisel verilerin korunması hakkının konusunu oluřturan kiřiisel verilerin üç adet unsuru bulunmakta olup, “gizlilik” bu unsurlardan biri deđildir. Dolayısıyla gizli olmayan bir verinin de bu koruma kapsamında olduđunun kabulü gerekecektir.

95/46/EC sayılı Avrupa Birliđi Konseyi Direktifi'nin amaç bařlıklı maddesinde “özellikle” mahremiyet hakkı olmak üzere, temel hak ve özgürlüklerin korunması amaç olarak belirlenmiřtir. Dolayısıyla mahremiyet hakkının kiřiisel verilerin korunmasıyla korunması amaçlanan haklardan biri olduđunu ve korunması amaçlanan başkaca haklar ve kavramların da bulunduđunu söyleyebiliriz. Zira sadece mahremiyetin korunması amaçlanmış olsaydı, kiřiye ait gizli bir verinin ifřa olmasıyla

⁴⁸ Gürsel, İ. (2016), *İřçinin Kiřiisel Verilerinin Korunması Hakkı*, Doktora Tezi, Dokuz Eylül Üniversitesi, s. 53.

⁴⁹ Veliođlu, A. (2020). *Sosyal Medya Özelinde İřçinin Kiřiisel Verilerinin Korunması*. Yüksek Lisans Tezi, İstanbul Üniversitesi, s. 19.

kişinin mahremiyeti zedelenmiş olacaktı ve o noktadan sonra kişisel verinin korunması söz konusu olamayacaktı⁵⁰.

Aleni ortamda yaşanan bir hadisede kişinin mahremiyetine herhangi bir zarar gelmeyecek olmasına rağmen, işbu hadise sonrası toplanan veriler kişiye zarar verecek şekilde kişinin aleyhine kullanılabilir. Bu durumda mahremiyet konusunda herhangi bir ihlal olmamasına rağmen kişisel verilerin korunmasının gerçekleştirilemediğini görülmektedir⁵¹. İşbu durum da kişisel verilerin korunmasının özel hayatın gizliliği veya mahremiyet kavramlarından ayrıldığını göstermektedir.

2.3.4 Kişisel Verilerin Hukuki Niteliğine İlişkin Değerlendirme

Kişisel verilerin korunması hakkının hukuki niteliğinin tespit edilmesi, hukuki niteliğinin ne olduğuna göre hakkın korunması için ne gibi uygulamaların kimler tarafından gerçekleştirileceği konuları bakımından önem taşımaktadır. Zira Amerikan hukukundaki gibi niteliğinin mülkiyet hakkı ve fikri mülkiyet hakkı olduğu kabul edilirse, kişisel veriler ticari bir niteliğe sahip olacağından, serbest ekonominin hâkim olduğu tüm yerlerde ekstra regülasyonlara gerek olmaksızın yalnızca eşya, ticaret ve fikri sınai haklar hukukuyla hakkın korunması sağlanabilecektir. Ancak kişilik hakkı olduğu kabul edilirse, hakkın sınırlarının ve korunmasının devlet tarafından gerçekleştirilmesi söz konusu olacaktır⁵².

Kişisel verilerin günümüzde büyük bir ticarete konu olduğu ve kişilere ait verilerin çokça şirketler tarafından internet üzerinden elde edilip bunun yine birçok şirkete satılarak kar edilmesi sebebiyle büyük bir pazara sahip olduğu gerçeği yadsınamaz. İşte tam olarak da bu nedenle kişisel verilerin korunmasının sıkı bir denetime sahip olması gerekmektedir. Zira hukuki ilişki olarak düşünüldüğünde iki taraftan zayıf olanın, çoğunluğunu Google, Facebook, Twitter ve Amazon gibi hizmetlerinin çok büyük kitlelerce kullanıldığı şirketlerin oluşturduğu veri işleyen değil, internete türlü amaçlarla girmiş ve kişisel verilerini bu şirketlerin kullanımına ekspozite etmiş veri sahibi olduğu görülecektir. Hukuk sistemlerinin çoğunda benimsenmiş olan ve hakkaniyet gereği uygulanması icap eden ilke zayıf olanın

⁵⁰ Aksoy, H. C., (2010), s. 63.

⁵¹ Aksoy, H. C., (2010), s. 63.

⁵² Velioğlu, A., (2020), s. 20.

korunması ilkesidir. Bu nedenle zayıf konumda olan veri sahibinin mağdur olmaması için verilerini işleyen gerçek ya da tüzel kişiliklerin sıkı denetlenmesi gerekmektedir.

Her ne kadar, 95/46/EC sayılı Avrupa Birliği Konseyi Direktifi'nin ve işbu Direktif'ten esinlenen Avrupa Birliği Genel Veri Koruma Tüzüğü'nün emredici hukuk kuralları düzenlemediğinden bahisle veri sahiplerine verilerin ticari olarak işletilebilmesi imkânı tanınmış olsa da; mülkiyet veya fikri mülkiyet hakkının benimsenmesi söz konusu değildir. Çünkü mülkiyet ve fikri mülkiyet görüşü veri sahibi ile veri işleyen arasındaki dengeyi bozarak veriyi ticari anlamda metalaştırmaktadır⁵³. Bu durumda da hakkaniyete ve hakkın özüne aykırı bir sonuç doğması kaçınılmazdır.

Bu doğrultuda yukarıda bahsedilmiş olunan amaca en iyi hizmet eden görüş olarak kişilik hakkı görüşü karşımıza çıkmaktadır. Kişilik hakkı görüşü kişisel verilerin korunması hakkını, özel hayatın gizliliği hakkı ve mahremiyet kavramı gibi insan hakları gibi nitelendirmekte olup, bu kapsamda kişisel verilerin korunması hakkının da insan haklarının sahip olduğu geniş ve sıkı korunmadan faydalanması sonucunu doğuracaktır. Nitekim Süzek, tüm bireylerin ve doğal olarak işçilerin kişisel verilerinin korunmasının kişilik hakkı kapsamında olduğu ve bu doğrultuda kişisel verileri üzerinde hukuken korunma hakkı bulunduğu görüşünü benimsemektedir⁵⁴. Süzek'in görüşüne katılmaktayız.

Kişisel verilerin korunması hakkı, kişilik hakkı kapsamında özel hayatın gizliliği ile “gizlilik” konularında ayrışsa bile, önceden bahsettiğimiz üzere kişisel verilerin korunması hakkının korumayı amaçladığı temel hak ve özgürlüklerden yalnızca bir tanesi özel hayatın gizliliği olup, işbu haklar sınırlı sayıda değildir. Alman Anayasa Mahkemesi, 1983 kararında “*enformasyonel self-determinasyon hakkı*” adı altında kişisel verilerin hangilerinin, kimler tarafından ve nasıl işlenebileceğinin veri sahibi kişiye ait olduğunu belirtmiştir. Bu ifade aynı kararda insan onuru ve kişinin maddi ve manevi varlığını geliştirme hakkıyla iç içe yorumlanmıştır⁵⁵. Bu yorumla beraber, hakkın kişilik hakkıyla daha çok özdeşleştiği görülmektedir.

⁵³ Aksoy, H. C., (2010), s. 69.

⁵⁴ Süzek, S. (2021) *İş Hukuku*. 21inci Bası. İstanbul: Beta Basım Yayım. s. 418.

⁵⁵ Aksoy, H. C., (2010), s. 71.

Özet olarak, kişisel verilerin korunması hakkının hukuki niteliğinin fikri mülkiyet yahut mülkiyet hakkı olduğu görüşü kabul gördüğü takdirde veri işleyen ve veri sorumlusunun, kişilik hakkı olduğu görüşü kabul gördüğü takdirde ise veri sahibi şahsın lehine bir sonuç doğacaktır. Görüşümüz, hakkın özünün kişilik hakları ve temek hak ve özgürlüklerle daha çok bağdaştığı, ayrıca hukuki ilişkide zayıfın korunması prensibi gerekçeleriyle kişisel verilerin korunması hakkının hukuki niteliğinin kişilik hakkı olduğu yönündedir.

2.4 Kişisel Verilerin İşlenmesi

Kişisel verilerin korunmasına ilişkin mevzuatta “kişisel verilerin işlenmesi” kavramı çokça karşımıza çıkmaktadır. Bu nedenle bu kavramın açıklanması yararlı olacaktır. Kişisel verilerin işlenmesinin tanımı, KVKK’nın tanımlar başlıklı 3. Maddesinde ve Kişisel Verileri Koruma Kurumu’nun internet sitesinde şu şekilde yapılmıştır:

“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.”

Ayrıca verilerin silinmesinin, anonim hale getirilmesinin ve yok edilmesinin de işlemenin kapsamına girdiği belirtilmiştir⁵⁶. Kişisel verilerin işlenmesi faaliyetlerinin kanun maddesinde sayılan işlemler ve yöntemlerle sınırlı olmadığı, tanımdaki koşulların sağlanması halinde her türlü işlemin kişisel verilerin işlenmesini oluşturacağına ilişkin baskın görüş mevcuttur⁵⁷.

95/46/EC sayılı Avrupa Birliği Konseyi Direktifi’nde de veri işleme mevzuatımızdakine benzer bir tanıma sahip olup, silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletlemeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma

⁵⁶ Kişisel Verileri Koruma Kurumu. *Kişisel Verilerin İşlenmesi* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/2048/Kisisel-Verilerin-Islenmesi> (Erişim Tarihi: 06.11.2021).

⁵⁷ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkara, E. (2021). *İş Hukuku Dersleri*. 34üncü Bası. İstanbul: Beta Basım Yayım. s. 404.

gibi faaliyetlerin tümü veri işlemenin kapsamına alınmıştır. Verilerin hangi ortamda işlenmesi gerektiği belirtilmediğinden, Direktif uyarınca verilerin herhangi bir ortamda işlenmesi yeterlidir. Ayrıca 3. maddede geçen “*otomatik olmayan yollarla, tamamen veya kısmen otomatik olan yollarla*” şeklindeki ibareyle verilerin nasıl işlendiğinin önem taşımadığını söyleyebiliriz⁵⁸.

Türkiye’nin de taraf bulunduğu Avrupa Konseyi’nin 108 sayılı Sözleşmesi’nde de benzer tanım bulunmakta olup, farklılık olarak verilerin işlenmesinin “*tamamen ya da kısmen otomatik yollarla yapılması halinde*” veri işleme kapsamına alınabileceğini hükmetmiştir. Ancak Sözleşme, üye devletlerin işbu sözleşmeyi otomatik olmayan yollarla işlenen verilere de uygulayacağını bildirebileceğini öngörmüştür. Nitekim, Türkiye 2016 senesinde Sözleşme’ye taraf olurken sözleşmeyi “*otomatik olmayan yollarla işlenen kişisel verilere de uygulayacağını*” bildirmiştir⁵⁹.

Avrupa Birliği’nde yürürlükte olan Avrupa Veri Koruma Tüzüğü’nde de veri işleme otomatik yollarla olup olmaması fark etmeksizin, verilerle yapılan faaliyetlerin tümünün kişisel verilerin işlenmesi olacağı öngörülmüş olup, toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarılma veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha işlemleri sayılmıştır⁶⁰. Belirtmek gerekir ki kişisel verilerin işlenmesi yalnızca bu işlemlerle sınırlı değildir. Tüzük’te de işleme faaliyetleri sınırlı sayıda tutulmamıştır.

Bütün bu bilgilerden, kişisel verilerin işlenmesinin veriyle yapılan her türlü işlem olduğu söylenebilir. Bu verilerin hangi ortamda işlendiği ve ne şekilde işlendiği de önem taşımamaktadır. Verilerin ele geçmesinden sonra zayi olmasına kadar yapılan bütün işlemler kişisel verilerin işlenmesini oluşturmaktadır⁶¹.

2.5 Hassas (Özel Nitelikli) Veri Kavramı

Hassas kişisel veriler, mevzuatımızda özel nitelikli veriler olarak tabir edilmekte olup, KVKK’nın 6. maddesinin gerekçesinde, lafzından da anlaşılacağı üzere, niteliği olarak özel koruma gerektiren ve üçüncü kişiler tarafından öğrenilmeleri

⁵⁸ Toprak, B., (2018), s. 16.

⁵⁹ Elbir, N., (2020), s. 68

⁶⁰ Avcı, Y. (2019). *Kişisel Verilerin Korunması*, Yüksek Lisans Tezi, Selçuk Üniversitesi, s. 49-50.

⁶¹ Süzek, S., (2021), s. 419.

durumunda kişinin mağdur durumuna düşebilme ihtimalini haiz veriler olarak açıklanmıştır⁶². Nitekim öğretide, özel nitelikli veri tanımının ayrımcılığa vurgu yapması üzerinde durulmuş ve bu tür verilerin, açığa çıkarılması halinde veri sahibi ilgili kişinin aleyhine sonuç doğurabilecek ya da ayrımcılığa uğramasına neden olabilecek veriler olduğu belirtilmiştir⁶³. Dolayısıyla işbu özel nitelikte olan veriler, diğer verilerden daha sıkı bir korumaya tabidirler. KVKK'nın tasarısının esin kaynağı olan Direktif'in 8. Maddesinin 1. fıkrasında hassas veriler; ırksal ve etnik köken, siyasi görüşler, dini ve felsefi inançlar, sendika üyeliği, sağlık durumu ve cinsel yaşama ilişkin veriler olarak belirlenmiştir⁶⁴. Mevzuatımız ile direktif arasında birkaç farklılık mevcuttur. Her ne kadar KVKK'nın özel nitelikli verilerinin belirtildiği 6. maddesinde Direktif'ten farklı olarak din ve inançların yanında mezhebin de kapsam altına alındığı görülse de⁶⁵; din ve inançların geniş yorumlanması gerekmekte olup, bu şekilde yorumlandığında mezhebin de uluslararası kaynaklarda hassas veriler arasına alındığı görülecektir. Ek olarak “kılık, kıyafetiyle ilgili veriler” ve “genetik veriler”in de kapsam altına alındığını görüyoruz. İzlanda⁶⁶ ve Portekiz⁶⁷ ülkelerinin de Avrupa Birliği üyesi olup Direktif'e ek olarak hassas verilerin kapsamını “genetik verileri” de ekleyerek genişlettiği görülmektedir. Avrupa Birliğinde an itibariyle yürürlükte olan Avrupa Birliği Genel Veri Koruma Tüzüğü'nde de genetik veriler hassas veri kapsamına alınmıştır.

⁶² Kişisel Verileri Koruma Kurumu. (2019). *Madde Ve Gerekeşi İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü*. Ankara: KVKK Yayınları, s. 21.; Gürsel, İ., (2016), s. 111.

⁶³ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 403.

⁶⁴ “Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”, EUR-Lex. (1995). *Document 31995L0046* [Çevrimiçi]. Erişim adresi: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046> (Erişim Tarihi: 03.11.2021)., Beytar, E., (2018), s. 148.; Yardımcı, A., (2019), s. 19.; Toprak, B., (2018), s. 7.

⁶⁵ Beytar, E., (2018), s. 148.

⁶⁶ “Sensitive data: a. Data on origin, skin colour, race, political opinions, religious beliefs and other life philosophies. b. Data on whether a man has been suspected of, indicted for, prosecuted for or convicted of a punishable offence. c. Health data, including genetic data and data on use of alcohol, medical drugs and narcotics. d. Data concerning sex life (and sexual behaviour). e. Data on trade-union membership.”, Council Of Europe, (2000). *The Data Protection Act - Act On The Protection Of Privacy As Regards The Processing Of Personal Data, No. 77/2000* [Çevrimiçi]. Erişim adresi: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af22f> (Erişim Tarihi: 03.11.2021).; Toprak, B., (2018), s.8

⁶⁷ “The processing of personal data revealing philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data, shall be prohibited.”, Council Of Europe, (1995). *Assembleia Da República [Portuguese Parliament] Act 67/98 Of 26 October* [Çevrimiçi]. Erişim adresi: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af2ea> (Erişim Tarihi: 03.11.2021)., Toprak, B., (2018), s.8

Hassas verilerin bahsettiğimiz kanunlarda belirtilen şekilde ve sınırlı sayıda yani “*numerus clausus*” olmaması gerektiğine ilişkin verilerin gruplandırılması gerektiğine dair bağlamsal görüş ve amacına bağlı olarak kapsamının değiştirilmesi gerektiğine dair amaçsal görüş şeklinde iki görüş mevcuttur. Bağlamsal görüş kişisel verilerin kullanım amaçları, işlenmeleri, alıcıları, ne koşullarda işlendikleri kriterleri göz önünde bulundurularak kişisel verilerin belli gruplara ayrılması ve bu kriterlere göre belli bir grubun hassas veri olamayacağını savunmaktadırlar. Bu görüş çoğu sektöre düzenlemeler yapılma gerekliliği sebebiyle zor ve maliyetli olacağı gerekçesiyle eleştirilmektedir. Diğer bir görüş olan amaçsal görüş ise hassas verinin hangi amaçla işleneceğine göre belirlenmesini savunmaktadır. Buna göre hassas bir kişisel verinin işleme amacı o veriyi ekspozite etmek ise bu kişisel veri hassas kişisel veri kategorisinde olmalıdır. Ancak bu görüş de, mevzu bahis verinin hassas veri olup olmadığının tespiti konusunda eleştirilere maruz kalmıştır⁶⁸.

Bu noktada amaçsal görüşe katılmaktayız. Örnekle izah etmek gerekirse, kişinin adresinin çoğu zaman umuma açık ortamlarda paylaşıldığı düşünüldüğünde hassas veri niteliğinde olmadığı; ancak bir ceza davasının duruşma zaptında, dinlenen şikayetçinin adresinin aynı celsede dinlenen sanığın gözleri önünde yazılmasının, kişinin adres bilgisinin o ihtimal bakımından hassas veri niteliğinde olduğunun kabulü gerekmektedir. Zira sanığın şikayetçisinin adresini öğrenmesi riskli bir durum olup, şikayetçi kişinin tehditlerle karşılaşmasına, şikayetini cebir ile geri çekmesine yol açma, şikayetçi kişiyi mağdur duruma getirebilme ihtimallerine sahiptir. Bu durumda verinin hassas nitelikte olduğu tartışmasız olup; adresinin sanığın görebileceği bir yere yazılması, şikayetçi şahsın açık rızasına bağlı olmalıdır. Ancak KVKK'nın 28. maddesi uyarınca kovuşturma aşamasında işlenen kişisel veriler KVKK kapsamına girmemektedir. Buna karşın kişisel verilerin korunması hakkı anayasal bir hak olduğundan ve anayasa tarafından güvence altına alındığından, ayrıca Türkiye'nin taraf olduğu uluslararası sözleşmelerde de düzenlendiğinden kanımızca bu hususun KVKK kapsamında olmaması, veri ihlali olmadığı anlamına gelmemektedir.

Hassas verilere ilişkin 2006 yılında İngiltere'de yapılan bir araştırmada kişilerin hassas verilerden ne anladığı sorulmuş olup, anket sonucunda kişilerin hassas veri olarak nitelendirdiği en yüksek oranlı veri türü olarak “*finansal veriler*”

⁶⁸ Beytar, E., (2019), s. 55-56.; Aksoy, H. C., (2010), s. 33-34.

belirlenmiştir. İlginç kısmı ise finansal verilerin, o dönem Avrupa Konseyi'nde yürürlükte olan 95/46/EC sayılı Direktif'e ve ülkelerin kendi mevzuatlarına göre hassas veri kategorisine girmemesidir. Bu husus da kanun koyucu ile bireylerin kişisel veri algılamasının farklı olduğu ortaya koymaktadır⁶⁹.

Hassas verilere ilişkin bir başka problemlili husus ise, tespit edilmelerinde karşılaşılan güçlüklerdir. Normal şartlar altında hassas veri olarak kabul edilmeyen, genel nitelikli verilerden olan veriler (örneğin bireylere ait fotoğraflar), kişilerin ırk, din, cinsiyet, sağlık verilerini içerebilmekte olup (örneğin kişinin fotoğraflarında tekerlekli sandalyede olması, veya dini bir kıyafet giymiş olması), bu durumda söz konusu genel nitelikte olması gereken verinin niteliğini tespit etmekte sorunlarla karşılaşmaktadır. İşbu güçlükler örnek olarak Naomi Campbell v. MGN⁷⁰ davası verilebilir. Naomi Campbell'ın fotoğraflarının onun ten rengini açığa çıkardığından dolayı hassas veri olarak nitelendirilip nitelendirilemeyeceği hususunda Mahkeme'nin değerlendirme yapma zorunluluğu vuku bulmuştur. Mahkeme, Naomi Campbell'ın tanınmış bir siyahi manken olduğu gerçeğinden yola çıkarak, fotoğraflarının onun mesleğinin ve yaşam tarzının bir parçası olduğunu, bu nedenle hassas veri olarak sayılmaması gerektiğine kanaat getirmiştir⁷¹. Görüldüğü üzere hassas veriler tanımlarında olduğu kadar belirli ve sabit olmayıp, tespitlerinde duruma göre yorum yapılması gerekmektedir.

Bu çalışmanın süjesi 4857 sayılı İş Kanunu⁷² uyarınca tanımlanmış ve kapsam altına alınmış işçiler olduğundan işçiler açısından da kişisel verilerin neleri kapsadığının ve hangi verilerin hassas veriler olduğunun tespitinin yapılması gerekmektedir. İşçilerin işverenleri tarafından kaydolarak tutulan ve çoğunlukla iş hukuku davalarında da delil olarak mahkemeye sunulan özlük dosyaları mevcut olup, işbu dosyalar işçilerin iş hayatındaki ve bazen iş hayatı dışındaki bilgileri kapsamaktadır. Bu dosyalarda, işçilerin sağlık raporları ve içerisinde sağlığına ait veriler, TC kimlik numaraları, adresleri, kan grupları, hastalık geçmişleri, cinsiyetleri,

⁶⁹ Kaya, C. (2011) *Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 69(1-2), s. 320-321.

⁷⁰ House Of Lords, *Opinions Of The Lords Of Appeal For Judgment In The Cause, 06.05.2004, Campbell (Appellant) v. MGN Limited (Respondents)* [Çevrimiçi], Erişim Adresi: <https://publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm> (Erişim Tarihi: 09.01.2022)

⁷¹ Kaya, C., (2011), s. 322.

⁷² 4857 sayılı İş Kanunu, *T.C. Resmi Gazete*, Sayı: 25134, 10 Haziran 2003 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

yaşları, medeni durumları, ırkları ve dinleri; işçilerin yıllık izin istemi belgeleri, mesleki bilgileri, disiplin cezaları, eğitim durumları, sendikal ve siyasi bilgileri; hatta işçilerin varsa yakınlarına ilişkin bilgiler ve benzerleri bulunmakta olup, bu bilgilerin hepsi kişisel veri olarak nitelendirilmekte ve korumaya tabi olmaktadır⁷³.

Hassas veya özel nitelikli verilerin kişisel verilerin korunması kapsamında daha sıkı bir denetime tabi tutulduğundan bahsedilmiştir. Kural olarak KVKK'nın ilgili hükmü olan 6. Maddesinin 2. Fıkrası özel nitelikli verilerin ilgili kişinin açık rızası olmaksızın işlenmesinin yasak olduğu belirtilmiştir. Bu hükümde bahsi geçen ilgili kişiden veri sahibi gerçek kişi anlaşılması gerektiği bu çalışmanın "*Kişi Unsuru*" başlıklı bölümü altında irdelenmiştir. Ancak özel nitelikli verilerdeki açık rıza şartının aranmadığı olasılıklar da mevcut olup, KVKK'nın ilgili maddesinde düzenlenmiştir. Mevzuatımızda hassas nitelikte veriler de sağlık ve cinsiyetle alakalı olanlar ile diğerleri olarak ikiye ayrılmıştır. Başka kanunda düzenlenen haller mevcutsa, sağlık ve cinsiyetle alakalı olmayan verilerin açık rızaya tabi olmaksızın işlenebileceği düzenlenmiştir. Ancak sağlık ve cinsiyetle alakalı verilerin belirli durumlarda kanunlardaki özel düzenlemelere gerek olmaksızın açık rıza olmadan da işlenebileceği öngörülmüştür. Bu sebepler kanunda; kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi olarak belirlenmiştir⁷⁴. Bu kapsamdaki verilerin hangi kişiler tarafından işleneceği de önem taşımaktadır. Kanuna göre işbu veriler ancak sır saklama yükümlülüğü altında olan kişiler veya yetkili kurum ve kuruluşlar tarafından, yukarıda bahsettiğimiz durumlarda işlenebilecektir. Dolayısıyla bu durum, özel tüzel kişilerin işbu sebeplerle açık rıza olmaksızın veri işleme sonucunu doğurmayacaktır.

Açık rızanın tanımı konusunda bir belirsizlik mevcut olup, işbu husus ne KVKK'da ne de gerekçesinde açıklanmamıştır. Açık rızanın yazılı olması şartı aranmamış olup, yazılı olması halinde ispat kolaylığı sağlayacaktır⁷⁵. GDPR'de ise bu konuda açık rızanın net olarak unsurlarının belirlendiği 4. Maddesinin 11. Alt bendi bulunmaktadır. Hükme göre açık rıza özgür iradeyle verilmiş, ilgili kişinin isteklerini

⁷³ Beytar, E., (2018), s. 148.

⁷⁴ Deniz, M. Ö. (2021) *İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması Ve Bundan Doğan Sorumluluk*. Türkiye Adalet Akademisi Dergisi, C. (45), s. 363.

⁷⁵ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 405.

kesin olarak gösterir, konuya özel nitelikte olmalı, ayrıca verisi hakkında açık rıza verecek şahsın doğru biçimde bilgilendirilmiş olması gerekmektedir⁷⁶. Ancak işbu unsurların tümünün varlığı halinde açık rızadan söz edilebilir.

Hassas verilerin işlenmesi hususu, ilgili şahsın açık rızasının alınmasıyla bitmemektedir. Zira hassas veriyi işleyecek olan veri sorumlusunun hassas veri işlenirken uyması gereken belirli kriterler mevcuttur. Kanun'un 6. maddesinin 4. fıkrasında özel nitelikte verilerin işlenmesinde Kurul tarafından belirlenecek yeterli önlemlerin alınması şart koşulmuştur. Kişisel Verileri Koruma Kurulu, 31.01.2018 tarihli Resmî Gazete'de 2018/10 sayılı karar ile "*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*"i yayınlamıştır⁷⁷. Bu önlemler özel nitelikli verilerin muhafaza edilirken, işlenirken veya aktarılırken güvenliğin sağlanmasını amaçlamakta olup, hem fiziksel ortamda hem de elektronik ortamda kişisel verilerin muhafaza edilirken nelere dikkat edilmesi gerektiği, aktarılırken ne şekillerde aktarılmasının güvenli olacağı, veri işleyenlerin periyodik eğitimlere tabi tutulması gerektiği ve bütün bunların özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedüre göre yapılması gerektiği belirlenmiştir⁷⁸.

Yukarıdaki bilgiler ışığında, çalıştırdığı işçiye ait işyeri şahsi dosyası düzenleyen bir işverenin, işçinin özel nitelikli ve genel nitelikli pek çok kişisel verisini muhafaza ettiğinden dolayı verileri işlerken, aktarırken veya muhafaza ederken dikkat etmesi gereken birden çok husus olduğunu görmekteyiz. İşyeri şahsi dosyasında bulunan işçiye ait çoğu kişisel veri hassas nitelikte olup, işbu veriler toplanırken, başka firmalarla paylaşılırken, aktarılırken, hatta silinirken işçilerin açık rızasına ihtiyaç duyulmasına rağmen uygulamada işçiler bu tarz işlemlerden bağımsız ve habersiz tutulmaktadır. Bu durum da işçilerin kişisel verilerinin korunması haklarının ihlaline yol açmaktadır.

⁷⁶ Selek, O. (2019) *Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması*. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 21(2), s. 922.

⁷⁷ Deniz, M. Ö., (2021), s. 363.

⁷⁸ Kişisel Verileri Koruma Kurumu. (2018). "*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*" ile ilgili *Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli Ve 2018/10 Sayılı Kararı* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/4110/2018-10> (Erişim Tarihi: 06.11.2021).

BÖLÜM 3: KİŞİSEL VERİLERİN KORUNMASI HAKKININ HUKUKİ DAYANAKLARI

3.1 Kişisel Verilerin Korunması Hakkında Uluslararası Kaynaklar

Kişisel verilerin korunması hakkı uluslararası düzenlemelerde fazlaca kaynakta karşımıza çıkmaktadır. Uluslararası kaynakların çoğunda spesifik olarak kişisel verilerin korunması hakkı geçmese de özel yaşamın gizliliği ve mahremiyet hakları adı altında kişilerin verilerinin korunduğunu görmekteyiz. Özel yaşamın gizliliği ve mahremiyet haklarının korunmasına yönelik ilk düzenlemelerin Birleşmiş Milletler Evrensel İnsan Hakları Bildirgesi ve Avrupa İnsan Hakları Sözleşmesi olduğunu söyleyebiliriz⁷⁹. Ancak spesifik olarak “*Kişisel Verilerin Korunması*” kavramının uluslararası düzenlemelere konu olması İkinci Dünya savaşını takiben kurulan Ekonomik İş birliği ve Kalkınma Örgütü (OECD) sayesinde gerçekleşmiştir. Bunun akabinde 108 sayılı Avrupa Konseyi Sözleşmesi hazırlanmış ve devletlerin mevzuatlarına girmeyi başarmıştır. 90’lı yıllarda internetin ortaya çıkması, 181 sayılı Avrupa Konseyi Ek Protokolü’nün hayat bulmasına yol açmıştır. Daha sonra kişisel verilerin korunması kavramı yaygınlaşarak başka örgütlerin çalışma alanlarının da konusu olmaya başlamıştır. ILO’nun tavsiye kararı niteliğindeki İşçilerin Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu, işçilerin kişisel verilerinin ve özel hayatlarının gizliliklerinin korunmasına ilişkin önemli bir düzenlemedir.

Nihayet, günümüzde birçok ülkenin kişisel verilerin korunması mevzuatının temelini oluşturan ve ülkemizdeki Kişisel Verilerin Korunması Kanunu’nun alıntılıandığı, Avrupa Birliği’nde an itibariyle geçerli Avrupa Birliği Genel Veri Koruma Tüzüğü’nün bir önceki versiyonu şeklinde nitelendirebilecek 95/46/EC sayılı Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi yürürlüğe girmiştir ve kişisel verilerin korunması mevzuatları son halini almaya başlamıştır. 6698 sayılı Kanunumuz tasarısı işbu Direktif’ten esinlenerek hazırlanmış olup, düzenlemeleri oldukça benzerlik göstermektedir. Günümüzde ise 2016 yılında düzenlenip Avrupa Birliği’ne üye devletlerde 2018 yılı itibariyle yürürlüğe girmiş olan GDPR mevcuttur. Kişisel verilerin korunması hususunda gelinmiş en son nokta olmakla beraber, Türkiye’nin üçüncü devlet

⁷⁹ Toprak, B., (2018), s. 22.

konumunda olduđu bir düzenlemedir. Ancak üçüncü devletlerin de yükümlülükleri bulunmaktadır. Dolayısıyla Türkiye’deki veri işleyenlerin taraf olunmasa bile dikkat etmesi gereken hususlar vardır. Bahsetmiş olduğumuz kişisel verilerin korunmasına ilişkin uluslararası düzenlemeler, çalışmamıza dayanak teşkil edeceğinden ve Türkiye’nin taraf olduđu uluslararası düzenlemelerde mevcut olduğundan, işbu düzenlemelerin benzerliklerini ve farklılıklarını açıklamak isteriz.

3.1.1 Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Rehber İlkeleri

Aslen İkinci Dünya Savaşı sonrası 1961 yılında Batı devletlerinin ekonomilerini desteklemek için OECC örgütü yerine kurulan örgüt⁸⁰, 1978 yılında kurduđu çalışma grubu sayesinde 1980 yılında “*Özel Yaşamın Gizliliğinin ve Kişisel Verilerin Sınır Ötesi Dolaşımının Korunmasına İlişkin Rehber İlkeler*” adı altın kişisel verilerin korunmasına ilişkin dünyada ilk düzenlemeyi oluşturmuşlardır. Bu düzenlemeler bağlayıcı olmayıp, yalnızca tavsiye niteliğindedir⁸¹.

OECD gibi dünya ekonomisiyle ilgili çalışmalar yapan bir örgütün kişisel verilere ilişkin ilkeler yayınlamasının arkasındaki amaç akıllarda soru oluşturmaktadır. Bunun sebebi verilerin ülkeler arası dolaşımının kontrol edilemeyecek derece büyük ve yaygın hale gelmesi, bu nedenle verileri işlenen kişilerin mağdur olmaması amacıyla kişilerin verilerin korunmasıdır. Zira o dönemde OECD örgütüne üye devletler ile diğer devletler arasından mevzuat farklılıkları bulunmaktaydı ve mevzuattaki bu farklılıkların veri dolaşımının önüne geçeceği, bu nedenle bankacılık gibi önemli sektörlerin sekteye uğrayacağı endişesiyle kişisel verilerin sınır ötesi dolaşımının korunmasına ilişkin ilkeler hazırlanmıştır. Dedğimiz üzere, OECD’nin bu düzenlemesindeki amacı verilerin ülkeler arasındaki dolaşımında bir denge kurmaktır⁸². Reed ve Angel, OECD’nin, örgütün kuruluş amacı da düşünüldüğünde gizlilikten çok, ülkeler arası ekonomik ilişkilerinin güçlendirilmesi ve bu süreçte bir aksaklıkla karşılaşılmasında amacını taşıdığını söylemektedir⁸³. Bu durumda, kişisel verilerin ekonomik değerinin kaygısı güdüldüğünden hukuki nitelik başlığı altında belirttiğimiz gibi hukuki niteliğinin mülkiyet hakkı gibi yorumlandığını görmekteyiz.

⁸⁰ Yardımcı, A., (2019), s. 24.

⁸¹ Elbir, N., (2020), s. 69.; Toprak, B., (2018), s. 23.

⁸² Özkan, O. (2020). *Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, Ankara Üniversitesi, s. 46.

⁸³ Reed, C. ve Angel, J. (2004) *Computer Law*. 5nci Bası. ABD: Oxford University Press, s. 423.

OECD'nin Rehber İlkelerinde sekiz adet ilkeden bahsedildiğini görmekteyiz. İşbu ilkeler, 7. maddede düzenlenen veri toplamada sınırlı olunması ilkesi, 8. maddede düzenlenen veri kalitesi ilkesi, 9. maddede düzenlenen amacın belirli olması ilkesi, 10. maddede düzenlenen veri kullanmada sınırlı olunması ilkesi, 11. maddede düzenlenen veri güvenliği ilkesi, 12. maddede düzenlenen açıklık ilkesi, 13. maddede düzenlenen bireysel katılım ilkesi ve 14. maddede düzenlenen hesap verebilirlik ilkesidir⁸⁴.

Veri toplamada sınırlılık ilkesi ile amaçlanan, kişilerin verilerinin toplanmasındaki keyfilik unsurunu ortadan kaldırmaktır. İlke uyarınca veriler, yalnızca yasada geçen amaçlarla ve yasada geçen şekillerle toplanabilecektir. Veri sahibinin bilgilendirilmesinin de gerekli olduğu düzenlenmiştir.

Veri kalitesi ilkesi, verilerin kullanım amaçlarına uygun ve güncel olmasını icap eder. Zira kişisel verilerin kullanım amaçlarının gerektirdiğinden uzun süre kullanılması ve güncelliğini yitirmesi kişisel verilerin korunması hakkını ihlal etmekte olup, işbu husus KVKK'da da olmak üzere birçok ülkenin kişisel verilerin korunması mevzuatında aranan şartlardan biridir.

Amacın belirli olması ilkesi, kişisel verilerin toplanması esnasında toplanma amacının belirli olması anlamına gelmektedir. Nitekim, kişisel veriler toplanma amaçlarının dışında kullanılamaz, toplandıktan sonra oluşan bir amaç değişikliği durumunda derhal veri sahibine bildirimde bulunulmalıdır.

Sınırlı kullanım ilkesi de bir önceki ilkeyle ilişkili olarak, verilerin toplanma amaçları dışında kullanımlarını yasaklamaktadır. Bu ilkenin istisnaları olarak veri sahibinin onayı ve diğer kanunlarda öngörülen haller verilebilir⁸⁵.

Veriler gerek kısmen veya tam otomatik gerekse otomatik olmayan ortamlarda toplanmakta olup, işbu ortamlarda verilen kaybedilmesi, yok edilmesi, çalınması, açığa çıkarılması gibi istenmeyen durumlarla karşılaşabilmektedir. Verilerin güvenliği ilkesi verilerin işbu durumların gerçekleşmesinin önüne geçilmesi amacıyla güvenlik önlemleri alınmasının gerekliliğini düzenlemektedir⁸⁶. Kişisel Verileri Koruma Kurumu'nun 31.01.2018 tarihli Resmî Gazete'de 2018/10 sayılı karar ile "*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken*

⁸⁴ Elbir, N., (2020), s. 70.; Özkan, O., (2020), s. 47.; Toprak, B., (2018), s. 23.

⁸⁵ Yardımcı, A., (2019), s. 26.

⁸⁶ Yardımcı, A., (2019), s. 26.

Yeterli Önlemler” işbu ilkeyle paralel düşünebiliriz. Yeterli önlemler kararı uyarınca verilerin işlendiği, saklandığı ve erişildiği ortamların fiziksel ortam ve elektronik ortam olmasına göre alınan önlemler değişilecek olup işbu önlemler açıkça belirtilmiştir. Bu önlemlerin OECD’den farkı, önlemlerin adından da anlaşılacağı üzere özel nitelikli verilerin işlenmesinde uygulanacak olmasıdır. Ancak OECD örgütünün rehber ilkelerinde genel nitelikli ve özel nitelikli veri ayrımı yer almamaktadır. Bu nedenle verilerin güvenliği ilkesinin her nitelikteki veri için geçerli olacağını söyleyebiliriz.

12. maddede düzenlenen açıklık ilkesi, şeffaflık olarak da bilinen (uluslararası literatürde transparency) kişisel verileri işleme tabi tutulan veri sahibi kişiye, verilerini işleyen kurum ve kuruluşlara erişebilme ve onlar hakkında bilgi sahibi olma imkânı tanımaktadır. Yani, ilgili kişi verilerine kimlerin erişim sağladığı, verilerini işlediğini ve verilerinin ne tür işlemlere tabi tutulduğunu açıklık ilkesi gereğince takip edebilecektir. Amaç olarak bireysel katılım ve hesap verilebilirlik ilkelerine oldukça benzemektedir. Bireysel katılım ilkesi ise kabaca kişinin verilerinin işlenmesinde söz sahibi olmasını ifade eder. İlkeye göre üçüncü şahısların veri sahibinin verilerine erişebilmesi veri sahibinin izni şartına bağlanmıştır. Ek olarak veri sahibi, veri sorumlusuna başvurup işbu ilke uyarınca kendisi hakkında verilerin bulunup, bulunup bulunmadığının bilgisini alabilme ve verileri hakkında makul süre içerisinde anlaşılabilir biçimde bilgi alabilme hakkını haizdir. Bu talepli başvurusunun söz konusu veri sorumlusu tarafından reddi durumunda ilgili kişi olan veri sahibine bir itiraz hakkı, itirazının haklı bulunması halinde ise veri sorumlusunda bulunan mevcut verilerinin silinmesini, değiştirilmesini veya anonimleştirilmesini isteme hakkı verilmelidir⁸⁷.

Son olarak hesap verilebilirlik ilkesi, veri sorumlusunun işbu ilkelere uymaması halinde sorumluluk taşınmasını ifade etmektedir. OECD bu ilkenin gereği olarak, bir mahremiyet yönetim programı uygulanmasını ve bu mahremiyet programının veri sahibinin tüm verilerini kapsamasını tavsiye etmektedir. Mahremiyet yönetim programı, talep halinde yetkili otoritelere sunulabilmelidir. Herhangi bir güvenlik ihlali durumunda ise yetkili otoriteler, ilgili diğer kurumlar ve etkilenmesi durumunda veri süjesi ilgili kişinin de bilgilendirilmesi gerekmektedir. Belirtmekte

⁸⁷ Yardımcı, A., (2019), s. 26.

fayda görüyoruz ki, hesap verilebilirlik ilkesi için henüz ortada bir güvenlik ihlali bulunmazken mevcut olan bir mahremiyet yönetim programı olmalıdır. İşbu ilke diğer mevzuatlara da konu olmakla beraber, OECD'nin hesap verilebilirlik ilkesi düzenlemesi yalnızca tavsiye niteliğinde kaldığı ve sorumlu olanların muğlak olması sebebiyle eleştirilmektedir⁸⁸.

OECD'nin rehber ilkeleri 2013 yılında revize edilmiş olup; yukarıda bahsetmiş olduğumuz mahremiyet yönetim programı, revizyon sonrası rehber ilkelerden olan hesap verilebilirlik ilkesi başlığı altına eklenmiştir. Getirilen bir başka yenilik, veri güvenliği ilkesi başlığının altında, verilerin ihlali durumlarında ilgili kişinin bilgilendirilmesi düzenlemesidir⁸⁹. İşbu düzenleme 2016 yılında hazırlanan Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 33. Maddesinde de bulunmaktadır. GDPR, bir veri ihlali durumunda ilgili kişiye bildirim 72 saat içerisinde yapılmasını zorunlu kılmaktadır⁹⁰. Görüldüğü üzere kişisel verilerin korunması konusunda ilk düzenleme sayılan OECD Rehber İlkeleri, kendinden sonraki mevzuatların da şekillenmesine yardımcı olmuştur.

Son olarak, 2013 revizyonuyla gizliliğin sağlanmasına yönelik otoriteler kavramı eklenmiştir. İşbu kavram Rehber İlkelerin önceki metninde bulunmayan bir kavram olup, üye devletlerin karar verme mekanizmalarını oluşturan objektif kurumlar yaratmasını, bu kurumların verilerin ve özel hayatın gizliliğini sağlamasını ve bu kurumların devamlılığının sağlanmasını ifade etmektedir⁹¹.

OECD rehber ilkelerinin taraf devletlerine sağladığı bir başka avantaj ise, kendi mevzuatlarında yeterli korumayı gerçekleştirilmeyen üçüncü devletlere sınır ötesi veri aktarımını durdurma yetkisi vermesidir⁹². Fakat işbu ilkeler, herhangi bir bağlayıcılığı bulunmayan tavsiye niteliğindeki düzenlemeler olduğundan verilen yetkinin uygulanabilirliği muallaktır. Zira üye devletler bu düzenlemelerin hepsinin aksi yönünde hükümler düzenleyebilmektedirler.

⁸⁸ Kaya, M. B. (2021) *Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi*, İstanbul Hukuk Mecmuası, C. 78(4), s. 1867.

⁸⁹ Elbir, N., (2020), s. 70.

⁹⁰ General Data Protection Regulation. (2018). *Art. 33 GDPR – Notification Of A Personal Data Breach To The Supervisory Authority* [Çevrimiçi]. Erişim adresi: <https://gdpr-info.eu/art-33-gdpr/> (Erişim Tarihi: 11.11.2021).

⁹¹ Elbir, N., (2020), s. 70.

⁹² Aksoy, H. C., (2010), s. 99.; Toprak, B., (2018), s. 24.

Yukarıda bahsettiğimiz bilgiler ışığında, OECD tarafından hazırlanan Verilerin Sınır Ötesi Dolaşımına İlişkin Rehber İlkeleri'nin KVKK da dahil olmak üzere birçok mevzuata önayak olduğunu görmekteyiz. Bu açıdan, 1980'de hazırlanmış olmasına karşın, gelişen teknolojiye karşı eskimediyini ve ilerisi düşünülerek kaleme alınmış bir düzenleme olduğu pekâlâ söylenebilir. Ayrıca üç kıtanın bir araya gelmesini sağlayan bir örgüt nezdinde hazırlandığından farklı kültür anlayışlarının ortak bir ürünü olarak değer kazanmaktadır⁹³.

3.1.2 Uluslararası Çalışma Örgütü (ILO) İşçilerin Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu

Uluslararası Çalışma Örgütü'nün 1996 yılında kabul ettiği "*İşçilerin Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu*", hem ILO'nun Türkiye'nin üyesi olduğu bir örgüt olduğundan hem de araştırma konusu ile yakından ilgisi bulunduğundan ötürü önemli bir düzenlemedir.

Uluslararası Çalışma Örgütü'nün 1995 yılındaki 267. Yönetim Kurulu Toplantısı'nda alınan karar sonucu bu tarihten 1 yıl sonra 1996 "*İşçilerin Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu*"nun metni hazırlanmıştır⁹⁴. İşbu metindeki düzenlemeler işçilerin kişisel verilerinin korunması ve özel hayatlarının gizliliği açısından yöntemler geliştirilmesine, işçilerinin verilerinin bilgisayar ortamında tutulmasının önüne geçilmek adına bilgisayar kayıtlarının en aza indirgenmesine, işçilere kişisel verilerine göre ayrımcılık yapılmamasına, işçilere ait verilerin üçüncü kişilerle paylaşımının önüne geçilmesine, işçilerin cinsiyeti, ırkı, dini gibi özel nitelikli verilerine ilişkin soru sorulmamasına ve sağlık hususunda yalnızca gerektiğinde soru sorulmasına ilişkindir⁹⁵.

Uygulama Kodu'nun kapsam maddesine baktığımızda, veri sahibi işçilerin kamu sektöründen veya özel sektörden olmasının ayrımının yapılmadığını görmekteyiz. Aynı zamanda tıpkı OECD Rehber ilkelerinde ve KVKK'da düzenlendiği üzere verilerin kısmen veya tamamen otomatik yollarla işlenmesiyle el

⁹³ Toprak, B., (2018), s. 24.

⁹⁴ Kaplan, E. T. (1997) *İş Hukukunda Kişilik Haklarının Özellikle Bilgisayarda Toplanan Bilgilere Karşı Korunması*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, C. 52(1), s. 382-383.; Manav, E. (2015) *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 19(2), s. 102.; Dursun, Y., (2019), s. 19.; Elbir, N., (2020), s. 88.

⁹⁵ Manav, E., (2015), s. 103.; Dursun, Y., (2019), s. 20.

ile işlenmesinin bir farkı bulunmamaktadır. Her iki türlü de, Uygulama Kodu'nun kapsamına girmektedir. Uygulama Kodu'nun düzenlemeleri bağlayıcı nitelikte olmayıp, sadece tavsiye niteliğindedir. Uluslararası Çalışma Örgütü'nün diğer düzenlemeleri bağlayıcı olmasına rağmen, Uygulama Kodu'nun hükümleri tavsiye kararları olup, bu sebeple ILO'ya üye olan ülkelerin mevzuatlarında da farklılıklar görülmektedir. Bu özelliğiyle OECD'nin rehber ilkelerine benzemektedir⁹⁶.

Uygulama Kodu'nun düzenlediği ilkeler bakımından da OECD'nin Rehber İlkelerine benzediğini ve düzenlemelerinin işbu rehber ilkelerden bazılarını içerdiğini görmektediriz. Kodu'n "Genel İlkeler" başlıklı 5. Maddesi uyarınca işçilerin kişisel verileri yalnızca toplanma amaçları doğrultusunda, hukuka uygun ve adil bir şekilde ve sadece iş ile alakalı sebeplerle işlenebilir. Eğer veri sorumlusu, işçiden toplamış olduğu kişisel veriyi başka bir amaçla kullanmak veya işlemek isterse, yeni amacın toplanma amacıyla çakışmadığını ve amacın değişmesinin yanlış yorumlamalara yol açmayacağını temin etmesi gerekmektedir. Bir diğer ilke, işçilerin otomatik sistemlerin güvenliğini sağlamak üzere teknik ve organizasyonel önlemler kapsamında toplanan verilerinin işçinin davranışlarını kontrol amacıyla kullanılmayacağını belirtmektedir. Bu ilke, bu amaçla toplanan verilerin işçinin iş akdinin feshi veya disiplin cezası yaptırımlarına neden oluşturmayacağı⁹⁷ şeklinde yorumlansa da kanımızca böyle bir durum mevcut değildir. Amaç olarak baktığımızda "*işçilerin davranışlarını kontrol amacıyla*" ifadesinin, toplanan verilerle işçilere baskı oluşturmanın önüne geçilmesi amacına hizmet ettiği açıktır. Lakin bir işçinin kişisel verilerin toplanırken tespit edilen bir sözleşmeye aykırılık, kabahat veya suç tarzı durumlarda gereğinin yapılması işçiye baskı uygulanması amacını taşımayacaktır. Dolayısıyla, bir işçinin otomatik sistemlerin güvenliğini sağlamak üzere teknik ve organizasyonel önlemler kapsamında verilerinin toplanması durumunda; söz konusu işçinin işe girerken iş sözleşmesinin esaslı noktalarından biri için gerekenleri taşımadığının ve buna rağmen taşıdığını iddia ettiğinin tespit edilmesi ve bunun akabinde işçinin iş akdine son verilmesi, işçinin kişisel verilerinin korunması hakkını ihlal etmeyecektir.

Bir diğer hüküm, işçilerin performanslarının değerlendirilmesinde işçilerin elektronik ortamdaki görüntülerinin tek kriter olamayacağını öngörmektedir. Yargıtay

⁹⁶ Elbir, N., (2020), s. 88-89.

⁹⁷ Elbir, N., (2020), s. 89.

kararları ışığında performans değerlendirme sisteminde hukuken olması gereken kriterlere baktığımızda; performans değerlendirmenin objektif olması, kriterlerinin somut ve ölçülebilir olması, kriterlerin ve değerlendirmenin yapılacağına bilgisinin önceden işçiye verilmesi, tespit edilen performans düşüklüğünün sürekli olması ve işyerinde olumsuzluğa yol açması ve sonuçların işçiye bildirilerek işçiye performansını arttırması için makul süre verilmesi gerektiğini görüyoruz⁹⁸. Fakat bu kriterler arasında elektronik gözetlemenin performans ölçmede tek kriter olamayacağına ilişkin bir kriter bulunmamaktadır. Dolayısıyla Türkiye, ILO'nun tavsiye kararındaki işbu ilkeyi mevzuatlarında ve içtihatlarında benimsememiştir.

Genel ilkeler kısmınının 10. alt bendinde, işçilerin toplanan kişisel verilerinin kullanımının ayrımcılığa yol açmaması gerektiği ifade edilmiştir⁹⁹. Nitekim, ILO'nun kuruluş amaçlarından biri de çalışma hayatında ayrımcılığın yok edilmesidir. Ek olarak birçok ülkenin iş hukuku mevzuatlarında da olduğu üzere, 4857 sayılı Kanun'un "eşit davranma ilkesi" başlığı altındaki beşinci maddesinde de işçilere din, dil, ırk, cinsiyet, inanç ve benzeri özelliklerine göre ayırım yapılamayacağı düzenlenmiştir. Spesifik olarak kişisel verilerin işlenmesi hususuyla ilişkili bir düzenleme olmasa da kişisel verilerin işlenmesinden doğan ayrımcılığın da bu madde kapsamına girdiğini söyleyebiliriz. Uygulama Kodu'nun 5.10 maddesinin ihlali, İş Kanunu'nun 5. maddesinin de ihlali sonucunu doğuracaktır.

Uygulama Kodu'nun 6. maddesi işçilere ait kişisel verilerin toplanmasındaki usulü, 8. maddesi işbu verilerin saklanması usulünü ve 10. maddesi de verilerin üçüncü kişilerle paylaşımının ne şekilde mümkün olabileceğini düzenlemektedir. Verilerin saklanması, kural olarak makul süreli ve verilerin güncelliği kontrol edilerek mümkün olmakla beraber, 8. maddenin 5. alt bendinde belli durumlarda verilerin uzun süreli saklanması mümkün hale gelmiştir. İşbu durumlar, uzun süreli saklamaya dayanak teşkil edecek bir yasal düzenlemenin bulunması, işçinin belirli bir süre olası bir iş için adaylar arasında yer almak istemesi veya mevcut veya bitmiş bir iş ilişkisine ilişkin bir dava veya başka bir hukuki süreç bulunması durumlarıdır¹⁰⁰. Uygulamada,

⁹⁸ Yargıtay 22. HD. E.2018/14692, K.2018/24703, T.19.11.2018, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

⁹⁹ International Labour Organization. (2001). *Protection Of Workers' Personal Data* [Çevrimiçi]. Erişim adresi: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107727.pdf (Erişim Tarihi: 13.11.2021).

¹⁰⁰ Elbir, N., (2020), s. 89-90.

işçi ile işverenlerin karşılıklı oldukları davalarda mahkemelerin işverenlerden işçiye ait özlük dosyalarının getirilmesini istediklerini görmekteyiz. Bu durumda işverenlerin, işçilere ait özlük dosyalarını bulundurmaları işçilerin kişisel verilerin korunması haklarının ihlalini teşkil etmeyecektir. Ancak işçinin işten ayrılmasını takip eden 10. senenin sonunda, bütün alacaklar ve talepler zamanaşımına uğramış olacağından ve işverenin işçiye ait kişisel verilerin bulunduğu özlük dosyasını saklamakta artık bir hukuki yararı bulunmayacağından; veri sorumlusu işverenin özlük dosyalarını bu süreyi aşacak şekilde saklamalarının işçilerin kişisel verilerin korunması haklarını ihlal ettiği kabul edilmelidir.

Uluslararası Çalışma Örgütü tarafından hazırlanan “*İşçilerin Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu*” nitelik olarak OECD’nin Rehber İlkeleriyle benzerlik taşımaktadır. Her iki düzenleme de nitelik olarak bağlayıcı olmadığından hem OECD hem de ILO üyesi olan devletlerin mevzuatlarında farklılıklar bulunmaktadır. Farklılıkları olarak düzenlemelerin yaratılış amacı örnek verilebilir. Zira Uluslararası Çalışma Örgütü, iş yaşamında özgürlük, eşitlik, güvenlik ve saygınlık koşullarında insana yakışır ve üretken çalışma koşullarından oluşan uluslararası çalışma standartlarını oluşturmayı hedeflediğinden¹⁰¹, mevcut düzenlemenin amacı da budur. Lakin OECD’nin Rehber İlkeleri düzenlemesindeki amaç ise gelişen teknolojiyle beraber yaygınlaşan sınır ötesi veri aktarımının ülkelerin ekonomileri üzerindeki etkilerini kontrol altına almaktır. Düzenlemelerdeki ilkeler de benzerlik göstermektedir.

3.1.3 Avrupa Konseyi'nin 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Avrupa Konseyi tarafından 29 Ocak 1981 tarihinde hazırlanan 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, aynı tarihte Türkiye tarafından da imzalanmıştır¹⁰². Avrupa Konseyi’ne üye olmamasına rağmen Türkiye’nin işbu sözleşmeyi imzalayabilmesi, sözleşmenin 23 maddesinin birinci fıkrası uyarınca, Avrupa Konseyi Bakanlar Komitesi’nin Avrupa Konseyi’ne üye olmayan herhangi bir devleti işbu sözleşmeye katılmaya davet

¹⁰¹ Sengenberger, W. (2014) *Uluslararası Çalışma Örgütü*. İnci Bası. Berlin: Friedrich-Ebert-Stiftung, s. 27.

¹⁰² Aksoy, H. C., (2010), s. 5.; Yardımcı, A., (2019), s. 30.; Toprak, B. s. 28.; Özkan, O., (2020), s. 47-48.; Avcı, Y., (2019), s. 22.; Velioglu, A., (2020), s. 39.

etme yetkisi sayesinde gerçekleşmiştir¹⁰³. Ayrıca, bu sözleşmeye ek niteliğinde olan “181 sayılı Kişisel Verilerin Otomatik İşleme Tabii Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol” 2001 senesinde Türkiye dahil bir çok devlet tarafından imzalanmıştır¹⁰⁴. Ancak, Türkiye’nin işbu düzenlemelerin ikisini imzalayan ilk ülkelerden biri olmasının yanında, aynı düzenlemeleri onaylayarak iç hukukuna dahil etmesi 17 Mart 2016 tarihini bulmuştur¹⁰⁵.

Bu ulusal düzenlemeyi diğerlerinden ayıran en önemli özellik, kişisel verilerin korunmasına ilişkin düzenlemeler arasından bağlayıcı olan ilk düzenleme olmasıdır. Üstelik bağlayıcılık kapsamı, Avrupa Konseyi ile sınırlı kalmamaktadır. Mevcut sözleşmeyi Avrupa Konseyi’ne üye olmayan ülkeler de imzalayabildiğinden sözleşmenin uluslararası bağlamda bir bağlayıcılığı bulunmaktadır. Bağlayıcı olmasına karşın, etki gücünün fazla olmaması nedeniyle eleştirilmektedir¹⁰⁶.

Sözleşme, kapsam ve amaç hususlarında önceki düzenlemelerden farklılık göstermektedir. Bahsedildiği üzere, OECD Rehber ilkeleri kapsam bakımından gerçek kişilerin kişisel verilerini kapsam altına almakta olup, Uygulama Kodu’nun kapsamı işçilerle sınırlıdır. 108 sayılı Sözleşme’nin de kapsam başlıklı maddesinden, işbu düzenlemenin gerçek kişilerin verilerine ilişkin uygulanacağı anlamı çıkarılmaktadır. Ancak niteliği gereği Sözleşme, kişisel verilerin korunmasına ilişkin asgari şartları düzenlediğinden dolayı; Sözleşme’ye taraf olan ülkelerin Sözleşme’yi onaylayıp iç hukuklarına geçirirken tüzel kişilerin verilerini de kapsam altına almalarının önünde bir engel bulunmamaktadır¹⁰⁷.

Ek olarak, kapsam bakımı süje açısından olduğu gibi, yöntem açısından da önem barındırmaktadır. Nitekim, başlığında da anlaşılacağı üzere Sözleşme yalnızca kişisel verilerin otomatik olarak işlenmesi durumunda uygulanacaktır. Ancak az önce bahsettiğimiz üzere, kişisel verilerin hangi yollarla işleme tabii tutulacağına kapsamını genişletmek de mümkündür. Asgari şartlar kişisel verilerin otomatik olarak işleme tabii tutulması halinde belirlenmiş olup, taraf devletler bu Sözleşme’nin kısmen otomatik

¹⁰³ Elbir, N., (2020), s. 74.

¹⁰⁴ Velioğlu, A., (2020), s. 23.; Yardımcı, A., (2019), s. 30.

¹⁰⁵ Yardımcı, A., (2019), s. 30.

¹⁰⁶ Özkan, O., (2020), s. 48.

¹⁰⁷ Yardımcı, A., (2019), s. 31.; Toprak, B., (2018), s. 29.

ya da elle işleme tabi tutulması durumlarında da uygulanacağını öngörebilirler. Sözleşme'nin 3. Maddesinin 2. alt bendinde devletlerin bu durumları da Sözleşme kapsamına alacağını bildirmeleri öngörülmüştür¹⁰⁸.

Amaç olarak işbu Sözleşme OECD Rehber İlkelerinden çok Uygulama Kodu ile benzerlik taşımaktadır. Zira Sözleşme'nin amacı, amaç başlıklı maddesinde:

“Her bir tarafın ülkesinde, uyruğu ve ikamet yeri ne olursa olsun her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır.”

olarak düzenlenmiş olup, OECD Rehber İlkeleri'nde olduğu gibi ticari bir amaç bu düzenlemede görülmemektedir. Ayrıca ILO'nun düzenlemesinde olduğu gibi sadece işçilerle de sınırlı kalmamaktadır. Tüm gerçek kişilerin temel hak ve özgürlüklerini ve özel hayattaki saygınlıklarının korunmasını amaçlamaktadır.

Sözleşme uyarınca düzenlenen ilkelerin çoğu, önceki düzenlemelerde bahsettiğimiz ilkelerle benzerlik göstermektedir. Örnek göstermek adına; Sözleşme'nin 5. maddesinde aynı zamanda Rehber İlkelerde de yer verilen “*veri niteliğinin kaliteli olması*” ilkesi, 7. maddesinde yine Rehber İlkelerden aşına olduğumuz “*veri güvenliği*” ilkesi ve 8. maddesinde ise Rehber İlkelerden “*hesap verebilirlik ilkesi*” ile oldukça benzer olan “*bilgi alma, verilere ulaşma, verilerin silinmesini veya düzeltilmesini talep etme hakkı*” düzenlenmiştir¹⁰⁹. Verilerin kalitesi ilkesinde verilerin güncel ve doğru olma şartına ek olarak, OECD Rehber İlkelerinden “*veri sınırlılığı ilkesi*” uyarınca hukuki yollarla elde edilmiş olma ve meşru amaçlarla kullanılma şartları mevcuttur.

Sözleşme'nin 6. maddesi “*hassas nitelikli veriler*”den bahsetmiş olup, işbu verilerin devletlerce yeterli önlem alınmaması durumunda otomatik yollarla işlenemeyeceğini öngörmektedir¹¹⁰. Bu düzenlemenin bir benzerini KVKK'nın 6. Maddesinde ve akabinde Kurul tarafından yayınlanan Yeterli Önlemlerde

¹⁰⁸ Elbir, N., (2020), s. 74.; Özkan, O., (2020), s. 49.

¹⁰⁹ Özkan, O., (2020), s. 49-50.

¹¹⁰ Özkan, O., (2020), s. 50.; Toprak, B., (2018), s. 30.;

gözlemlemekteyiz. Kapsamı sınırlı sayıda belirlenmiş olan özel nitelikli veriler, 2018 yılında gelen güncelleme ile daha geniş bir kapsama sahip olmuştur¹¹¹.

Sözleşme, taraf ülkeleri birbirlerine yardım etme yükümlülüğü altına sokmakta olup, işbu hükümlerin amacı Sözleşme'nin kolayca uygulanmasını sağlamak ve etkinliğini artırmaktır¹¹². Ancak bağlayıcılığı gibi, bu yardımlaşmaya ilişkin hükümler de taraf devletlerin iç hukuktaki düzenlemelerinin farklılıkları gerekçesiyle¹¹³ pek etkili olmamıştır.

Sözleşme 18 Mayıs 2018 yılında “*Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Modernize Edilmiş Sözleşme*” veya “*Sözleşme 108+*” adları altında güncelleştirilmiştir ve GDPR gibi Avrupa Birliğinde an itibariyle yürürlükte olan mevzuatlarla uyarlanmıştır. Türkiye Sözleşme'nin güncel haline taraf değildir. Modernizasyon ile getirilen yeniliklere örnek olarak, şeffaflık ilkesi, verilerin orantılı ve asgari düzeyde işlenmesi ilkesi, hesap verilebilirlik ilkesi ve gizlilik ilkeleri verilebilir¹¹⁴.

2001 yılında devletlerce imza altına alınan Ek Protokol, Sözleşme'ye ülkelerin denetleyici kurumlar oluşturma zorunluluğu getiren hükümler eklemiştir. İşbu denetleyici makamlar, Protokol'ün birinci maddesi uyarınca Sözleşme'nin uygulanışını denetleyen bağımsız makamlar olup, Sözleşme dolayısıyla iç hukuka eklenen hükümlere aykırılık durumlarında bunu yargının önüne getirebilme ve şahısların kişisel verilerin korunmasına ilişkin taleplerini ve şikayetlerini dinleme yetkilerini haizdir.¹¹⁵ Niteliğine bakıldığı zaman her ne kadar Kişisel Verileri Koruma Kurumu da bu bağlamda denetleyici bir makam olarak sayılsa da, 181 sayılı Ek Protokol'de bahsi geçen nitelikte bir denetleyici makam değildir. Zira protokol de geçen bağımsızlık unsuru Kişisel Verileri Koruma Kurumu'nda bulunmamaktadır. Kişisel Verileri Koruma Kurumu Adalet Bakanlığı'na bağlı bir kurum olup, 9 adet üyesinin 5'i TBMM içerisinde ve 4'ü Cumhurbaşkanı tarafından (değişiklikten önce

¹¹¹ Elbir, N., (2020), s. 75.

¹¹² Elbir, N., (2020), s. 75.

¹¹³ Toprak, B., (2018), s. 30.

¹¹⁴ Velioğlu, A., (2020), s. 23-24.

¹¹⁵ Kişisel Verilerin Korunması Platformu. (2016) *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol)* [Çevrimiçi]. Erişim adresi: <https://www.kisiselverilerin korunmasi.org/mevzuat/kisisel-verilerin-otomatik-isleme-tabi-tutulmasi-karsisinda-bireylerin-korunmasi-sozlesmesine-ek-denetleyici-makamlar-ve-sinirasan-veri-akisina-iliskin-protokol-181-sayili-ek-protokol/> (Erişim Tarihi: 18.11.2021).

iki üye Bakanlar Kurulu tarafından seçilmekteydi.) seçilmektedir¹¹⁶. Bu bağlamda 181 sayılı Ek Protokol'ün ihlalinden bahsedilebilir.

Protokol'ün ikinci maddesi ise, Sözleşme'ye taraf devletlerin yetki alanında bulunan birinden, Sözleşme'nin tarafı olmayan bir devletin yetki alanına sınır ötesi olarak veri aktarımında uyulması gereken prosedürden bahsetmektedir. İşbu maddeye göre, bu durum ancak veri aktarımı yapılacak ülkenin veya yetki alanında bulunan kuruluşun, yeterli seviyede korumayı sağladığını garanti etmesi koşulu sağlandığında gerçekleşebilmektedir¹¹⁷. İşbu yeterli düzeyde koruma kavramı birden fazla düzenlemede karşımıza çıkmakta olup, bu kavram Avrupa Birliği Adalet Divanı'nın (ABAD) 2015 tarihli Maximillian Schrems hakkındaki kararında Avrupa Birliği hukukundaki temel hak ve özgürlüklere ilişkin güvencelerle en azından eşdeğer bir koruma düzeyi olarak yorumlanmıştır¹¹⁸.

108 sayılı Sözleşme ve Eki 181 sayılı Protokol, kişisel verilerin korunması hususunda bağlayıcılığı bulunan ilk düzenleme olması ve Türkiye'nin de işbu düzenlemeye taraf olması yönünden önemlidir. İçerdiği ilkeler bakımından OECD Rehber İlkeleri'yle benzerlik gösterse de amaç bakımından bir benzerlik taşımamaktadır.

3.1.4 95/46/EC Bireylerin Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Açısından Korunması Hakkında Direktif

Esasen OECD Rehber İlkeleri ile 108 sayılı Sözleşme arasındaki farklılıkların giderilmesi hedefiyle düzenlenen¹¹⁹ 95/46/EC sayılı Direktif, gerek ülkemizde geçerli kişisel verilerin korunması mevzuatının tasarısı hazırlanırken esinlenen gerekse Avrupa Birliği'nde yürürlükte olan GDPR'nin temelini oluşturan önemli bir düzenlemedir. Direktif'in başlangıç kısmının 3. paragrafında görüleceği üzere, 1. paragrafta ve Direktif'in amacının düzenlendiği 1. maddesindeki nedenlerin yanında; Direktif'in aynı zamanda malların ve sermayelerin ülkeler arası serbestçe aktarılıp

¹¹⁶ Kişisel Verileri Koruma Kurumu. *Kişisel Verileri Koruma Kurulu'nun Yapısı ve Görevleri* [Çevrimiçi]. Erişim adresi: <https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0%20KORUMA%20KURULU%E2%80%99NUN%20YAPISI%20VE%20G%C3%96REVLER%C4%B0> 0.pdf (Erişim Tarihi: 18.11.2021).

¹¹⁷ Yardımcı, A., (2019), s. 32-33.

¹¹⁸ Elbir, N., (2020), s. 83.

¹¹⁹ Toprak, B., (2018), s. 31.

dolaşabilmesi de amaçlanmıştır¹²⁰. Bu durum başlı başına OECD Rehber İlkelerinin amacı ile 108 sayılı Sözleşme'nin amacının bir düzenlemede buluşturulduğunu göstermektedir. Ancak sınır ötesi veri dolaşımı hususu Direktif bakımından bir hayli önemlidir ki; Direktif'te Üye Devletler'in birbirleriyle olan veri dolaşımının engellenmeyeceği spesifik olarak vurgulanmış ve öngörülmüştür¹²¹.

Yönergeler, Avrupa Birliğinin İşleyişi Hakkında Anlaşma uyarınca üye devletler için çerçeve niteliğindedir. Bu da demek oluyor ki, yönergeyle amaçlanana ulaşıldıktan sonra düzenlemelerin yöntemi ve şekli üye ülkeler arasında değişiklik gösterebilmektedir. ILO Uygulama Kodu'nda olduğu gibi, 95/46/EC sayılı Direktif de asgari koruma öngörmekte olup, Direktif'in hükümleri yerine daha geniş kapsamlı koruma sağlayan hükümlerin öngörülmesi ve uygulanmasının önünde bir engel bulunmamaktadır. Diğer bir deyişle, Direktif'in bağlayıcı olma özelliği yalnızca asgari düzey korumaya kadar geçerlidir¹²².

Direktif'in kapsamına baktığımızda süje bakımından tıpkı 108 sayılı Sözleşme'de olduğu gibi gerçek kişilerin kapsam altına alındığını ve kişisel verilerin işleme biçimi bakımından ise otomatik olan, kısmen otomatik olan ya da otomatik olmayan yollarla işlenen verilerin ayrımının yapılmadan her türlüünün kapsam altına alındığı görülmektedir. Kapsam ile ilgili diğer düzenlemelerden farklı olarak bir istisna mevcut olup, topluluk hukuku, ulusal güvenlik, ceza hukuku, kamu güvenliği ve savunmaya ilişkin faaliyetlerden ile gerçek kişilerin tamamen ev içi ve kişisel faaliyetlerinden doğan kişisel verilerin kapsam içine alınmayacağı öngörülmüştür¹²³.

Direktif ile kişisel verilerin korunmasına ilişkin olarak 29. Madde Çalışma Grubu ve 31. Madde Komitesi adında iki yeni organ getirilmiştir. 29. Madde Çalışma Grubu, üyelerini, her bir Üye Devletin kişisel verilerin korunmasına ilişkin denetleyici makamından birinin oluşturduğu, görevinin ise kişisel verilerin korunması hususunda ve Direktif uygulanırken ortaya çıkan soruların cevaplandırılmasıyla Üye Devletlerin aldığı önlemleri tekdüzeleştirilmek ve bu karşılaşılan sorunlara ilişkin görüş bildirmek olduğu bir organdır. Ek olarak Üye Devletlerin koruma düzeylerini tespit etmek ve Komisyon'a bildirmek, yıllık raporlar hazırlamak gibi önemli görevleri de

¹²⁰ Elbir, N., (2020), s. 76.

¹²¹ Özkan, O., (2020), s. 53-54.

¹²² Avcı, Y., (2019), s. 25.

¹²³ Elbir, N., (2020), s. 77.

bulunmaktadır¹²⁴. GDPR'nin 2018 yılında yürürlüğe girmesiyle mülga edilen Direktif'le beraber bertaraf olan 29. Madde Çalışma Grubu, yerini Avrupa Veri Koruma Kurulu'na (European Data Protection Board - EDPB) bırakmıştır¹²⁵.

31. Madde Komitesi ise 29. Madde Çalışma Grubundan farklı olarak yalnızca görüş veren bir organ değildir. İşbu organ Üye Devletlerin temsilcilerinden oluşmakla birlikte, aynı zamanda önemli kararların alındığı ve düzenlemelerin imzalandığı bir komitedir¹²⁶.

Direktif'in düzenlediği ilkelerin çoğu daha önce bahsettiğimiz düzenlemelerle karşımıza çıkmış olup, 6. maddesinde düzenlenen “*veri kalitesi*” ilkesinin unsurları verilerin adil ve hukuka uygun olarak işlenmesi, işleme amacının belirli ve açık olması, toplanma amacıyla bağlantılı ve sınırlı olması, verilerin doğru ve güncel olması ve verilerin toplanma amacının gerektirdiği süreden fazla saklanmaması olarak belirlenmiştir¹²⁷. Bu ilkenin yer aldığı diğer düzenlemelere bakıldığında, ilkenin kapsamının ve unsurlarının arttığı görülecektir. Zira Rehber İlkelerden itibaren öngörülmekte olan bu ilkede ilk olarak amaca uygun olarak kullanılma ve güncel olma şartı aranmıştır. Sonrasında, 108 sayılı Sözleşme'de düzenlenen versiyonunda, verilerin güncel olmasının yanında doğru olması ve hukuka uygun olarak elde edilmiş olması şartı getirilmiştir. En sonunda Direktif'te verinin saklanma süresinin toplanma amacının gerektirdiği süreyi geçmemesi şartı getirilerek, ilke son halini almıştır.

7. maddede verilerin işlenmesinde meşruiyet kriterleri düzenlenmiştir. Bu düzenlemeye göre kişilerin verileri taraf olunan sözleşme gereğince isteniyorsa ya da işlenmesi gerekiyorsa, ilgili kişinin rızası durumunda, veri sorumlusunun bir yasal yükümlülüğü yerine getiriyor olması durumunda, ilgili kişinin hayati çıkarlarının korunması durumunda, verilerin açıldığı şahıs ya da şahıslar ile denetleyicinin takip ettiği meşru menfaatlerin gerekli olması durumunda ve kamu yararı durumunda kişisel verilerin işlenmesi meşru kılınmıştır¹²⁸. Ek olarak yine aynı maddede veri

¹²⁴ Özkan, O., (2020), s. 55.

¹²⁵ Avcı, Y., (2019), s. 26.

¹²⁶ Elbir, N., (2020), s. 77.

¹²⁷ Özkan, O., (2020), s. 55.

¹²⁸ Yardımcı, A., (2019), s. 37.

sahibinin temel hak ve özgürlüklerinin ihlal edilmemesi, kişisel verilerin işlenmesinin meşru olması hususunda şart olarak koşulmuştur¹²⁹.

29 Madde Çalışma Grubu'nun 2/2017 sayılı İşyerinde Veri İşlenmesi Hakkında Görüş (2/2017 sayılı Görüş), araştırmamız açısından oldukça önemli bir belgedir. Bu görüş ile beraber işçilere ait kişisel verilerin, işçilerin öncelikli olarak bilgilendirilmiş olmaları şartıyla, verileri işlemenin gerekli olması şartıyla ve bir önceki paragrafta bahsetmiş olduğumuz meşru menfaat kavramının işçilerin özel hayatlarının gizliliği hakkından daha ağır basmaması şartıyla veri işlemede söz konusu veri sorumlusunun meşru menfaatten söz edilebileceği belirtilmiştir.¹³⁰ Ne var ki, işbu görüş uyarınca meşru menfaat mevcut olsa dahi, işlemenin gerekli ve orantılı olup olmadığının ve temel hak ve özgürlüklere asgari müdahalede bulunulup bulunulmadığının değerlendirilmesinin yapılması gerekmektedir¹³¹.

Direktif'in hassas verilerin işlenmesine ilişkin 8. Maddesinde, hassas verilerin sağlık durumuna ve cinsel yaşama, sendika üyeliğine, dini ve felsefi inançlara, siyasi görüşlere, ırk ve etnik kökene ilişkin veriler olduğu belirtilmiş ve bu tür verilerin işlenmesi yasaklanmıştır. Bu yasağın uygulanmayacağı istisnai haller ise ikinci bentte düzenlenmiştir. İlgili veri sahibinin açık rızası durumunda, işlemenin denetleyicinin yükümlülüklerini ve özel haklarını yerine getirme amacı için gerekli olması durumunda, veri sahibinin rıza vermesinin imkansızlığı halinde diğer bir kişinin veya veri sahibinin hayati menfaatlerinin korunması için gerekli olması durumunda, işlemenin uygun bir koruma teminatı veren kar amacı gütmeyen kuruluş tarafından yapılması halinde üçüncü kişilere aktarımın yapılmayacağı ve işlemenin yalnızca amaçlarıyla bağlantılı olarak düzenli iletişimde oldukları kişileri veya kuruluş mensuplarını ilgilendirmesi durumunda hassas verilerin işlenmesi meşru kılınmıştır.¹³² Unutmamakta fayda vardır ki, işbu istisnai durumların varlığı yalnızca hassas verilerin

¹²⁹ Toprak, B., (2018), s. 32.

¹³⁰ Uncular, S. (2020) *Teknolojinin Etkisiyle Dönüşen İş İlişkisinde Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme*. Çalışma ve Toplum Ekonomi ve Hukuk Dergisi, C. 66(3), s. 1679.

¹³¹ Uncular, S., (2020), s. 1681.

¹³² 95/46/EC sayılı Direktif Çevirisi. *95/46/EC Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi* [Çevrimiçi]. Erişim adresi: <https://kisiselveri.com/9546ec-turkce> (Erişim Tarihi: 20.11.2021).

işlenmesi yasağını kaldırmakta olup, diğer ilkelerin sağladığı korumalar sürmektedir¹³³.

Direktif'in 25. Maddesinde, tıpkı OECD'nin Rehber İlkelerinde olduğu gibi verilerin sınır ötesi aktarımında bulunması gereken durumlardan ve hangi koşullarda verilerin sınır ötesi aktarımının gerçekleştirilebileceği düzenlenmiştir ve Rehber İlkeler'deki düzenlemeye benzer olarak, üye devletler ile yeterli seviyede koruma sağlayan ülkeler arasında veri aktarımı yapılabileceği öngörülmüştür¹³⁴.

İşbu düzenleme 2018 yılına kadar yürürlükte kalmış olup, 2018 yılında Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) yürürlüğe girmesiyle beraber mülga olmuştur. Gerek 29. Madde Çalışma Grubunun yapmış olduğu diğer çalışmalar (Kişisel Verilerin İşlenmesinde Bireylerin Korunması Hakkında Görüş, İşyerinde Elektronik İletişimin İzlenmesi Hakkında Görüş, İş İlişkisinde Kişisel Verilerin İşlenmesi Hakkında Görüşü, İşyerinde Veri İşlenmesi Hakkında Görüş, vb...)¹³⁵, gerekse kendinden önceki düzenlemeleri tek noktada birleştirerek bir yeknesaklık oluşturması bakımından oldukça önemli bir düzenlemedir.

3.1.5 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Avrupa Birliği genelinde yürürlükte olan kişisel verilerin korunması mevzuatı, 14.04.2016 tarihinde Avrupa Parlamentosu tarafından kabul edilip ancak 25.05.2018 tarihinde yürürlüğe girmiş olan ve yürürlüğe girmesiyle kendisinden önceki düzenleme olan 95/46/EC sayılı Direktif'i mülga eden Avrupa Birliği Genel Veri Koruma Tüzüğü'dür¹³⁶.

Direktif gibi, kişisel verilerin korunması hususunun veri koruma düzenlemeleri arasında en isabetli ve kapsamlı biçimde işleyen bir düzenlemenin yerine neden yeni bir düzenleme getirildiği sorusu akılları meşgul etmektedir. Bunun nedeninden GDPR'nin giriş kısmında bahsedilmiş olup, işbu yeni düzenlemenin gerekçesi olarak gelişen teknoloji ve küreselleşme ile beraber kişisel verilerin korunmasında yeni tehlikelerin oluşması, veri işlemenin ve veri aktarımının oldukça yaygınlaşması,

¹³³ Kaya, C., (2011), s. 323.

¹³⁴ Toprak, B., (2018), s. 33.

¹³⁵ Velioğlu, A., (2020), s. 46.

¹³⁶ Toprak, B., (2018), s. 33.

kolaylaşması ve hızlanması hususları gösterilmiştir¹³⁷. Bu gerekçeler her ne kadar doğru olsa da, tüm nedenleri oluşturmamaktadır. Bir önceki düzenleme olan Direktif'in, her ne kadar başarılı olsa da hedefi olan "kişisel verilerin korunması düzenlemelerinde yeknesaklık durumu"nu oluşturmakta yetersiz kaldığını görmekteyiz. Zira bazı Üye Devletler'in, belirli hükümleri bütün hatlarıyla uygulamayıp yetersiz şekilde uygulaması, bazı hükümleri ise Direktif'te düzenlenenden daha sıkı ve yüksek denetimle uygulaması söz konusu olduğundan bu durum karışıklıklara neden olmuş ve ülkelerin birbirleriyle olan veri akışının, düzenleme farklılıklarından dolayı kesilme tehlikesi doğmuştur. Hakikaten de Direktif uyarınca Üye Devlet olan devletlerin iç düzenlemelerinde içerik ve yorum bakımından farklılıkların olduğu tespit edilmiştir. Bu farklılıklarla birlikte devletlerin sınır ötesi veri dolaşımında aksaklık olması ve buna bağlı olarak devletlerin ekonomilerinin zarar görmesi kaçınılmaz olacaktır¹³⁸. İşte Tüzük'ün getirilmesindeki gerçek sebep, yukarıda açıkladığımız üzere Direktif'in hedefleyip gerçekleştiremediği devletlerin düzenlemelerinde birlik oluşturup, veri akışının sorunsuz gerçekleştirilmesidir. Bununla beraber, değişen teknolojiyle eklenen kavramlara ilişkin düzenlemeler yapılarak kişisel verilerin karşılaşılabileceği yeni tehlikeler de bertaraf edilmiştir.

Direktif'in başaramadığı "*düzenlemelerde tekdüzelik*" durumunu GDPR'nin başarıp başaramadığı, eğer başardıysa nasıl başardığı soruları da dikkat çekmektedir. İşbu soruların cevabı ile GDPR düzenlemesinin neden Tüzük şeklinde çıkarıldığına cevabı aynı hükümde gizlidir. Avrupa Birliği'nin İşleyişi Hakkında Anlaşma'nın 288/2 maddesi, tüzüklerin genel uygulama alanına sahip olduğu, üye devletler açısından direkt olarak uygulanacağı ve üye devletler arasında bağlayıcılık teşkil ettiği hükümlerini amirdir¹³⁹. Halbuki, bir önceki düzenleme, yine aynı maddenin 3. alt bendi uyarınca yönerge şeklinde kabul edildiğinden, tarafları yalnızca sonuç bakımından bağlamakta ve şekil ve yöntem bakımından taraflar üzerinde bağlayıcılığının bulunmamasıydı¹⁴⁰. Bu da demek oluyor ki, Direktif'teki "*çerçeve nitelik*"ten vazgeçilmiştir ve Tüzük, yürürlük tarihi itibarıyla herhangi bir değişiklik yapılmaksızın direkt olarak Üye Devletler'in mevzuatlarına dahil edilmiştir. Bu kapsamda GDPR'nin Avrupa Birliği'ne üye devletlere herhangi bir değişiklik yapma imkanı vermemesi dolayısıyla,

¹³⁷ Toprak, B., (2018), s. 34.

¹³⁸ Özkan, O., (2020), s. 59.

¹³⁹ Avcı, Y., (2019), s. 28.; Özkan, O., (2020), s. 61.

¹⁴⁰ Özkan, O., (2020), s. 61.

95/46/EC sayılı Direktif'ten beri amaçlanan düzenlemeler birliğine ulaşıldığı tespitinde bulunmak doğru olacaktır.

Ek olarak, GDPR ile gündeme gelen “*one-stop shop*” ilkesi de yeknesaklığa katkı sağlayan hususlardan bir tanesidir. İlke gereğince Tüzük'e aykırılık durumunda aykırılığı yapan taraf tek otoriteyle muhatap olacaktır. Buna göre ihlalin sonuçları ihlalin yapıldığı ülke içerisinde gerçekleşiyorsa o ülkede yetkili veri koruma otoritesi söz sahibi olurken, ihlal olayının taraflarının birden fazla ülke olması ya da ihlali birden fazla ülkeyi ilgilendirmesi durumlarında söz sahibi olan otorite Avrupa Veri Koruma Kurulu olacaktır¹⁴¹. Kurul'un görevlerinin ve yetkilerinin düzenlendiği Tüzük'ün 70. maddesi uyarınca Kurul uyuşmazlıklar hakkında tavsiye mahiyetinde görüşler vermenin yanı sıra bağlayıcı kararlar alma yetkisine de sahiptir¹⁴². Bu durumda, ülke içi bir ihlalde farklı uygulamalar olsa dahi ülke içi ile sınırlı olacağından sınır ötesi veri dolaşımı etkilenmeyecek, ülkeler arası bir ihlalde farklı ve keyfi uygulamaların olmamasını sağlamak adına Kurul yetkili olacağından sınır ötesi veri dolaşımının sekteye uğraması tekrardan engellenmiş olacak ve sonuç olarak uygulama birliği sağlanmış olacaktır. Bu haliyle 29. Madde Çalışma Grubu'nun yetkisinin sorunlara tavsiye niteliğinde görüş bildirmeye sınırlı olmasından ötürü Kurul'a göre pasif kaldığını ve bu nedenle Direktif'in yeknesaklığı oluşturmakta GDPR'ye nazaran başarısız olduğunu söyleyebiliriz.

Bir önceki paragrafta Avrupa Veri Koruma Kurulu'nun bir önceki düzenleme uyarınca toplanan 29. Madde Çalışma Grubu'nun yerine geçtiğini söylenmiştir. Fakat 29. Madde Çalışma Grubu'nun sona ermesi, Grup tarafından sağlanan çalışmalar ve görüşlerin de geçerliliğini yitirmesi anlamına gelmemektedir. Grup tarafından hazırlanan 16 adet metnin GDPR ile ilişkili sayılıp söz konusu düzenleme bakımından da uygulanacağı hususu, Kurul'un ilk toplantısında karara bağlanmıştır¹⁴³. Dolayısıyla 29. Madde Çalışma Grubu'nun aktifliğini yitirmesine rağmen, kişisel verilerin korunmasına yönelik kavramların tanımlanması ve sorunların çözümüne ilişkin görüşleri hala kabul görmekte ve kullanılmaktadır.

Tüzük'ün kapsamının düzenlendiği 3. maddesi Tüzük'ün, Avrupa Birliği sınırları içerisinde bulunan veya faaliyetlerini Avrupa Birliği sınırları içerisinde

¹⁴¹ Velioğlu, A., (2020), s. 48

¹⁴² Velioğlu, A., (2020), s. 49.

¹⁴³ Elbir, N., (2020), s. 81.

yürüten işletmelerin kişisel verileri işleminde uygulanacağını düzenlemekte olup, ek olarak (1) ivazlı veya ivazsız bir ürün ya da hizmet teklifiyle bağlantılı, (2) ilgili kişilerin davranışlarını gözlemlemeyle bağlantılı olmak kaydıyla; Avrupa Birliği sınırları içerisinde bulunmayan bir kuruluşun Avrupa Birliği sınırları içerisinde bulunan kişilerin kişisel verilerini işlemesi durumunda da uygulanacağı belirtilmiştir¹⁴⁴. Bu bağlamda GDPR'nin uygulanabilmesi için veri süjesinin AB vatandaşı olması şartının aranmadığını söyleyebiliriz¹⁴⁵. Kapsamının bu denli geniş tutulması Avrupa Birliği dışında bulunan veri sorumlusu işletmeleri de endişelendiren bir durum olmuştur. Zira sosyal medyayı oluşturan büyük şirketlerin çoğu Amerika Birleşik Devletleri menşeli olmalarına rağmen, GDPR'nin yürürlüğe girmesiyle politikalarını ve sözleşmelerini değiştirmek durumunda kalmıştır. Fransa'nın Ulusal Veri Koruma Komisyonu'nun (CNIL) 21 Ocak 2019 tarihinde kişisel verilerin korunması hakkının ve Tüzük hükümlerinin ihlali gerekçesiyle Google aleyhine 50 milyon Euro idari para cezası hükmetmesi de bu değişikliklere önyak olmuş durumlardan bir tanesidir¹⁴⁶. Söz konusu uyuşmazlıkta CNIL, Google'ın kişisel verileri işlerken şeffaflık ve bilgilendirme ilkelerine aykırı davrandığını, kişilerin yeteri kadar bilgilendirilmediğini ve istenilen bilgilere ilgili kişiler tarafından ulaşılmasının zor olduğunu, ayrıca kişilerin rızaları alınırken hangi işlemler için alındığının belli olmadığını ve rızaların çoğu aşamada ilgili kişi tarafından verilmeyip otomatik olarak alındığını tespit etmiştir¹⁴⁷. Görüldüğü üzere Veri Koruma Tüzüğü, kapsam bakımından Avrupa Birliği'nin dışına çıkmakta ve üye olmayan devletleri de ilgilendirmektedir. Türkiye de Tüzük uyarınca üye olmayan üçüncü devlet statüsünde olup, bu durum Türkiye aleyhine ihlal ve para cezası kararları verilmesine engel değildir.

GDPR ile birlikte kişisel verilerin korunması hakkına yenilikler getirilmiştir. Yenilik olarak sayılabilecek ve detaylı olarak işlenmiş hususlardan birisi de “rıza” kavramıdır. Rıza, Tüzük'ün 7. maddesinde:

¹⁴⁴ Çekin, M. S. (2019) *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*. 2nci Bası. İstanbul: On İki Levha Yayınları, s. 36.

¹⁴⁵ Özkan, O., (2020), s. 63.

¹⁴⁶ Avcı, Y., (2019), s. 29.

¹⁴⁷ EDPB. (2019). *The CNIL's Restricted Committee Imposes A Financial Penalty Of 50 Million Euros Against Google Llc* [Çevrimiçi]. Erişim adresi: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (Erişim Tarihi: 22.11.2021).

“Kişisel verilerin işlenmesinin kabul edildiğini bir beyan ya da açık onaylayıcı bir eylemle ortaya koyan.”

şeklinde tanımlanmıştır. Aynı zamanda çalışmamızın önceki bölümünde GDPR uyarınca rıza da olması gereken özgür irade ile verilme, konuya özel verilme, ilgili kişinin bilgilendirilmiş olması ve kesin olması kriterlerinden bahsedilmiştir. Bir başka önemli detay ise, Tüzük’ün 7/1 maddesi ile rızanın varlığını ispat yükümlülüğü veri sorumlusuna yüklenmiştir¹⁴⁸. Zira aksi takdirde bir kişinin hiç vermediği bir rızayı ispatlama olanağı bulunmamakla birlikte, böyle bir düzenleme hayatın olağan akışına aykırı olacaktır.

Tüzük’ün 7. Maddesi rıza konusundaki koşulları düzenlemektedir. Rıza birden fazla konu hakkında ve yazılı biçimde verilecekse, rıza talebi açık ve sade bir dille, konuların açıkça ve kolayca ayırt edilebildiği bir şekilde sunulmalıdır.¹⁴⁹ Bu kriterlere uymayan rıza talebi sonucunda edinilmiş rıza meşru olmayacaktır. Ek olarak verilen rıza her zaman geri çekilebilir. Ancak rızanın geri çekilmesi anına kadar kişisel verilere ilişkin yapılan işlemler rızanın varlığından dolayı hukuka uygun olduğundan; rızanın sonradan geri çekilmesi, bu işlemlerin hukuka uygunluk durumunu bertaraf etmeyecektir. Ayrıca rızanın geri alınması işleminin rızanın verilmesi işlemi kadar kolay olması gerektiği düzenlenmiştir¹⁵⁰.

7. maddede düzenlenen rızaya ilişkin son koşul, rızanın özgür biçimde verilip verilmediğinin değerlendirilmesi konusuyula ilgilidir. Bir sözleşmenin ifası amacıyla kişisel verilerin işlenmesi için rıza istendiğinde; gerçekten de söz konusu sözleşmenin ifa edilebilmesi için işlenmek istenen kişisel verilerin işlenmesinin gerekli olup olmadığı, gerekli olması durumunda ise rızanın işbu gerekli kısım için istenip istenmediği hususlarına dikkat edilmesi gerekmektedir. Bu düzenlemenin amaçlanan, sözleşmenin taraflarının eşit olmaması durumunda zayıf olan tarafın kişisel verilerinin korunmasıdır¹⁵¹.

Rıza aynı zamanda Tüzük’ün 6. ve 9. maddelerinde kişilerin verilerinin işlenmesinde hukuka uygunluk sebeplerinden biri olarak öngülmüştür. Tüzük’ün 6. Maddesi genel nitelikli verilerin işlenmesine ilişkin bir düzenleme olup, düzenlenen 6

¹⁴⁸ Selek, O., (2019), s. 921.

¹⁴⁹ GDPR m.7/2

¹⁵⁰ GDPR m.7/3

¹⁵¹ Selek, O., (2019), s. 921.

adet hukuka uygunluk sebeplerinden en az birinin bulunması halinde işleme faaliyeti hukuka uygun sayılacaktır. İşbu maddeye göre hukuka uygunluk sebeplerinden biri olarak belirlenen rıza, genel bir rızadır. Lakin, Tüzük'ün hassas verilerin işlenmesine ilişkin maddesi olan 9. Maddede hukuka uygunluk sebebi olarak belirlenen rıza, “açık rıza”dır. Açık rıza ile rıza arasındaki farklar, değişik düzenlemelerde tespit edilmeye çalışılmış olup, Direktif uyarınca “opt out” yöntemi kabul edilmiştir. Bu yöntemle göre, ilgili kişi kişisel verilerinin işlenmesine sessiz kalıyorsa veya itiraz etmiyorsa ortada zımni kabul niteliğinde bulunan bir rızadan bahsedilebilecektir. Ancak hassas veriler, spesifik olarak açık rıza aradığından bu yöntem geçerli olmayacaktır. Tüzük'te ise rızanın “beyan veya açık onaylayıcı eylemle” yapılması öngörüldüğünden “opt out” yöntemi GDPR bakımından hiçbir şekilde kabul görmemektedir¹⁵². Dolayısıyla GDPR her ne kadar hassas verilerin işlenmesine yönelik açık rıza arasa da Tüzük rızanın genel olarak zaten açık bir şekilde yapılmasını tanımladığından bütün veri işleme durumlarında hukuka uygunluk sebebi olarak aranan rızanın açık bir şekilde olması gerektiğini söylemek yanlış olmayacaktır.

Rıza konusu ile ilgili son olarak, çocuklara ilişkin kişisel verilerin işlenmesine dair bir düzenleme olan 8. maddeye göre; 16 yaşının üzerindeki çocukların kişisel verilerinin işlenmesi bizzat kendilerinin rıza vermesi durumunda gerçekleşebilecektir. Çocuğun 16 yaşından küçük olması halinde ise çocuğa ait kişisel verilerin işlenebilmesi adına çocuğun üzerinde velayet hakkı bulunan kişinin rızasının bulunması şart koşulmuştur. Maddede öngörülen yaş sınırı devletlerce aşağı çekilebilmekte olup, alt sınır olarak 13 yaş öngörülmüştür¹⁵³. Bu yaş sınırı, çocuklara ait kişisel verilerin veri sorumluları tarafından işlenmesi durumunda çocuğun kendi rızasının alındığı durumlara ilişkindir. Verisi işlenecek ilgili kişi çocuk 13 yaşının altındaysa her türlü velayet hakkı sahibinin rızası gerekecektir¹⁵⁴. Belirtmekte fayda görüyoruz ki; genel nitelikli verilerin işlenmesinde aranan diğer hukuka uygunluk sebepleri olan Tüzük'ün 6/1-b,c,d,e ve f alt bentlerinin varlığı durumlarında ek olarak çocuğun ya da duruma göre çocuk üzerinde velayet hakkı sahibi olanın rızası aranmamaktadır.

¹⁵² Selek, O., (2019), s. 933.

¹⁵³ GDPR m.8/1

¹⁵⁴ Özkan, O., (2020), s. 65.

Tüzük uyarınca düzenlenen veri sahibinin haklarından birisi de 13. ve 14. maddelerde düzenlenen bilgilendirilme hakkıdır. Genel olarak, veri sahibinin verilerin üzerindeki kontrolünü sağlamak adına verilerinin toplanma ve işleme aşamaları hakkında bilgilendirilmiş olması icap etmektedir. 13. maddede kişisel verilerin veri sahibinden toplanması durumunda veri sorumlusunun veri sahibine sağlaması gereken bilgiler düzenlenmekte ve 14. maddede kişisel verilerin veri sahibinden toplanmaması durumunda veri sorumlusunun veri sahibine sağlaması gereken bilgiler düzenlenmektedir. İşbu bilgilendirme yükümlülüğü veri sorumlusu tarafından re'sen yerine getirilmelidir, yani bilgilerin veri sorumlusu tarafından sağlanması için veri sahibinin herhangi bir başvuruda ya da talepte bulunmasına gerek yoktur. Veri sahibinin bilgilendirme yükümlülüğünün istisnası olan durumlar da düzenlenmiştir. Buna göre, eğer verisi doğrudan kendisinden alınan veri sahibi ilgili kişi, veri sorumlusunun bilgilendirmekle yükümlü olduğu 13. maddede düzenlenen tüm bilgilere halihazırda sahipse, işbu bilgilendirme yükümlülüğü uygulanmayacaktır¹⁵⁵. Ancak veri sorumlusu veri sahibinin verisini doğrudan kendisinden edinmediyse, 14. Madde uyarınca düzenlenen haller olan (1) veri sahibinin halihazırda tüm bilgilere sahip olması, (2) GDPR'nin 89. Maddesinde belirlenen koşullara ve güvencelere tabi olarak kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar başta olmak üzere söz konusu bilgilerin sağlanmasının imkânsız olması veya ölçüsüz bir çaba gerektirmesi, (3) elde etme veya açıklamanın kontrolörün tabi olduğu ve veri sahibinin meşru menfaatlerinin korunması amacıyla uygun tedbirler sağlanan Birlik veya üye devlet hukukunda açık bir şekilde ortaya konması, (4) kişisel verilerin yasal bir gizlilik yükümlülüğü de dahil olmak üzere Birlik ya da üye devlet hukuku ile düzenlenen bir mesleki gizlilik yükümlülüğüne tabi olarak gizli kalmasının gerekmesi durumlarının en az birinin gerçekleşmesi halinde veri sorumlusunun bildirim yükümlülüğünden söz edilemeyecektir.

Tıpkı 181 sayılı Ek Protokol'ün öngördüğü ve akabinde Direktif'te de düzenlenen bağımsız veri koruma otoriteleri kurulmasına hüküm gibi, Tüzük uyarınca da işbu “*veri koruma otoriteleri*” adı verilen denetim mekanizmalarının oluşturulması öngörülmüştür. Fakat Tüzük, diğer düzenlemelerden farklı olarak söz konusu veri koruma otoritesinin bağımsızlık özelliğine spesifik olarak değinmekte ve denetim

¹⁵⁵ Tolun, Y. (2020). *Kişisel Verilerin KVKK Ve GDPR Kapsamında Korunması*. Yüksek Lisans Tezi, Kırıkkale Üniversitesi, s. 78-81.

mekanizmasında tamamen bağımsızlık aramaktadır. Tüzük, tamamen bağımsız konusunda kriterleri belirlemiş olup, düşüncemize göre en önemli kriter; oluşturulan veri koruma otoritesine kendi üyelerini seçme hakkının tanınmasıdır¹⁵⁶. Sırf bu kriterden bile anlaşılacağı üzere; ülkemizde olan ve veri koruma otoritesi olarak görev yapan Kişisel Verileri Koruma Kurulu, GDPR uyarınca oluşturulması öngörölmüş bağımsız bir veri koruma otoritesi değildir. İşbu veri koruma otoritelerin kişisel verilerin korunması hususunda tavsiye vermek, idari düzenlemelere izin vermek, kurum ve kuruluşları teftiş etmek, uyarıda bulunmak, kınamak ve kişisel verilerin korunmasına ilişkin çıkan uyuşmazlıkları yargı önüne taşımak gibi yetkileri mevcuttur¹⁵⁷.

Veri sahibi ilgili kişiler, Tüzük'ün 15. maddesinde düzenlenen erişim hakkı uyarınca uyarınca her zaman veri sorumlularına başvurup kişisel verilerinin işlenip işlenmediği sorabilmekte, işleniyorsa işlenme sürecine ilişkin bilgilere erişmeyi talep edebilmektedir¹⁵⁸. İşbu hak, OECD Rehber ilkelerinden bireysel katılım hakkıyla aynı temele sahiptir. Aynı zamanda ilgili kişiye, veri sorumlusunda bulunan kendine ait verilerin doğru olmadığı durumda işbu verilerin düzeltilmesini talep etme, eksik olduğu takdirde ise bu verilerin tamamlanmasını talep etme hakkı verilmiştir.¹⁵⁹ Bu hükme benzer mahiyette bir düzenlemeyi 108 sayılı Sözleşme'nin 8. maddesinde görmekteyiz.

Tüzük ile birlikte gelen iki yeni hak olduğunu görmekteyiz. Bunlardan ilki 17. Maddede düzenlenen “*unutulma hakkı(right to be forgotten)*”dır. Temeli, kişilerin maddi ve manevi varlıklarını geliştirebilmeleri düşüncesine dayanan¹⁶⁰ unutulma hakkı; kişilerin verilerinin internet üzerinden silinerek kişisel verilerin korunmasını amaçlamaktadır. İşbu konunun Tüzük'ten önce bahsi geçtiği yer ABAD'ın 13 Mayıs 2014 tarihli “*Google Inc. v. Spain*” kararıdır. Karara konu olay, M. Gonzalez adlı şahsın sosyal güvenlik borçları dolayısıyla evinin satılmasına ilişkin La Vanguardia adlı yayın kuruluşu tarafından ilan verilmesi ve işbu ilanın Google arama motoru vasıtasıyla herkesçe görünebilmesi sonucunda ilgili kişi M. Gonzalez'in kişisel verilerinin korunması hakkının ihlal edildiği gerekçesiyle konunun yargı önüne

¹⁵⁶ Elbir, N., (2020), s. 85.

¹⁵⁷ Elbir, N., (2020), s. 85.

¹⁵⁸ Elbir, N., (2020), s. 81.

¹⁵⁹ GDPR m.16.

¹⁶⁰ Elbir, N., (2020), s. 102.

getirilmesinden ibarettir. En sonunda Ulusal Mahkeme tarafından uyuşmazlığın ABAD'a taşınması sonucunda ABAD, Google'ın bir arama motoru olması nedeniyle ve kişisel verileri arayıp bulma, otomatik olarak işleme faaliyetlerinin veri işleme faaliyeti olması gerekçesiyle Google şirketinin veri sorumlusu olduğu, veri sahibi ilgili kişilerin ekspozite edilen kişisel verilerin adıyla ilişkilendirilmesini istememe hakkı bulunduğu, bu hakkın veri sorumlusunun iktisadi yararına veya kamu yararına baskın kaldığı durumlarda veri sahiplerinin kendine ait verilerin internet üzerinden silinmelerini, değiştirilmelerini, düzeltilmelerini, kaldırılmalarını, erişiminin engellenmesini talep edebileceğini ifade eden bir hüküm kurmuştur.¹⁶¹ İşbu karar takiben halen faal olan 29. Madde Çalışma Grubu bu kararın yorumlanmasına ilişkin ve karara konu ilke hakkındaki görüşler bildirmiştir. Buna göre silinmesi yahut unutulması talep edilen kişisel verinin doğru ya da yanlış olması bir önem arz etmemektedir. Bu bilginin tutulmasının gerekli olmaması ya da veri sahibinin, veri sorumlusunun veri sahibi ilgili kişiye ait kişisel verileri nezdinde barındırmasından rahatsızlık duyması bile verilerin silinmesi için yeterli sebep oluşturacaktır¹⁶².

Unutulma hakkının düzenlendiği Tüzük'ün 17. Maddesi, unutulma hakkının talep edildiği veri sorumlusuna; ilgili kişinin kişisel verilerinin kamuya açılmış olması halinde silinmesinin yanında, mevcut teknoloji ve uygulama maliyeti göz önünde bulundurularak makul olması durumunda verilerin aktarıldığı diğer veri sorumlularını da bilgilendirme zorunluluğu getirmiştir¹⁶³. Bu durumla amaçlanan, günümüzde verilerin ne kadar hızlı dolaştığının bilinmemesiyle birlikte bu durum karşısında unutulma hakkına sahip ilgili kişinin mağdur duruma düşmemesinin sağlanmasıdır¹⁶⁴. Tabii ki bunun ne ölçüde gerçekleştiği halen muallaktır. Zira bazı görüşlere göre kişisel verilerin internet ortamından tamamen yok edilmesi imkânsız bir uğraştır. Konuyla ilgili olarak, bir kere internet ortamına düşmüş bir materyalin, sonsuza dek

¹⁶¹ Akkurt, S. S. (2016) *17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı"*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 65(4), s. 2609-2610.; Elbir, N., (2020), s. 103-104.

¹⁶² Yörük, O. D. (2019). *AB 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi, s. 79.

¹⁶³ Özkan, O., (2020), s. 68.; Elbir, N., (2020), s. 107., Avcı, Y., (2019), s. 32., Yörük, O. D., (2019), s. 80.

¹⁶⁴ Özkan, O., (2020), s. 68.

internet ortamında kalacağına ilişkin oldukça yaygın bir söz mevcuttur¹⁶⁵. Bir diğer düşünce ise unutulmak istenen kişinin başta hatırlanmaması gerektiğidir¹⁶⁶.

Unutulma hakkı sınırsız ve mutlak bir hak olmayıp, GDPR uyarınca düzenlenen gerekli görünen hallerde kısıtlanabileceği düzenlenmiştir. Zira ilgili kişi veri sahibinin kişisel verilerinin korunması hakkıyla, veri sorumlularının ifade özgürlüğü, haberleşme özgürlüğü, basın özgürlüğü gibi hakları karşı karşıya gelebilmekte olup, ortada bir menfaat çatışması durumu söz konusu olabilmektedir. Böyle bir durumda iki hak arasında denge kurulup, bir hakkın diğerine baskın olması da göz önünde bulundurularak kısıtlanması gerekecektir¹⁶⁷. Tüzük'e göre unutulma hakkının sınırlanabileceği durumlar; (1) ifade özgürlüğü ve bilgi edinme hakkının kullanıldığı, (2) bir yasal yükümlülüğün veya kamu yararının söz konusu verinin saklanması veya işlenmesini gerektirdiği, (3) hassas verilerin işlenmesine dair kriterlerin bulunması kaydıyla, kamu sağlığının gerektirdiği, (4) söz konusu verilerin unutulma hakkı kapsamında silinmesinin verileri işleme amacına ulaşılmasını imkansız hale getirmesi veya oldukça zorlaştırması durumunda, kamu yararına arşivleme amaçlarının, bilimsel veya tarihi araştırma amaçlarının ya da istatistiki amaçların gerektirdiği ve (5) yasal bir hakkın kurulması, kullanılması veya savunulması için gerekli olan durumlardır¹⁶⁸. Unutulma hakkına böyle bir sınırlama getirilerek, kendinden daha üstün ve baskın olan üçüncü kişilerin hakları ve kamu yararı ile unutulma hakkı arasında makul bir denge kurulmuştur.

Son olarak bahsedilmesi gereken husus, yine GDPR ile kişisel verilerin korunması hukuka katılmış “*veri taşınabilirliği hakkı*”dır. Bu hak, veri sahibinin bir veri sorumlusuna kendinin sağlamış olduğu kişisel verileri, kendi amaçlarıyla kullanmak için yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkını ve bu verilerin, önceden bulunduğu veri sorumlusu engellemeksizin başka bir veri sorumlusuna aktarabilme hakkını ifade etmektedir. Tüzük'te kişilerin bu hakka sahip olması için iki koşul öngörülmüştür; biri, veri sorumlusuna sağlanan verilerin rızaya dayalı sağlanmış olması durumudur, diğeri ise veri sorumlusuna sağlanan verilerin bir sözleşmenin ifası için gerekli olması

¹⁶⁵ Tolun, Y., (2020), s. 83.

¹⁶⁶ Kulevska, S. (2013, Haziran 24) The Future of Your Past: A Right to be Forgotten Online?, [Blog yazısı]. Erişim adresi: https://www.lumendatabase.org/blog_entries/521

¹⁶⁷ Özkan, O., (2020), s. 69-70.

¹⁶⁸ Yörük, O. D., (2020), s. 80.

durumudur¹⁶⁹. Ek olarak, işbu hakkın kullanımının unutulma hakkına halel getirmeyeceği, aynı zamanda kamu yararının gerektirdiği veya veri sorumlusunun yasal bir yükümlülüğü yerine getirdiği durumlarda bu hakkın uygulanmayacağı düzenlenmiştir. Dolayısıyla tıpkı unutulma hakkı gibi veri taşınabilirliği hakkının da mutlak ve sınırsız bir hak olmadığı bu düzenlemeden anlaşılmaktadır.¹⁷⁰

Hakkı kapsamı yönünden incelendiğimizde, “*kişisel verilerin ilgili kişi veri sahibi tarafından veri sorumlusuna sağlanmış olması*” kriteri arandığından, veri sorumlusu tarafından oluşturulan ilgili kişiye ait verilerin kapsam dışı kaldığı görülmektedir¹⁷¹. Ayrıca otomatik olmayan yollarla işlenen veriler de veri taşınabilirliği hakkının kapsamı altında değildir¹⁷².

Yukarıdaki bilgiler ışığında, Avrupa Birliği Genel Veri Koruma Tüzüğü kişisel verilerin korunması hakkına ilişkin düzenlemeler bakımından gelinen son noktadır. Kişisel verilerin korunması hakkının kapsamını genişletmiş ve yeni kavramlar oluşturmuştur. Tüzük olması sayesinde, kendinden önceki Direktif’in amaçlayıp başaramadığı bağlayıcılık ve düzenleme birliği hususlarında başarılı olmuştur. Hatta yürürlükte bulunduğu Avrupa Birliği sınırlarını aşmış, üye olmayan devletlerin ve üçüncü kişilerin üzerinde de etki sahibi olmuştur. Ülkemiz de bu üçüncü ülke statüsünde bulunan ülkelerden biri olup; mevzuatımızla Tüzük karşılaştırıldığında Tüzük’ün daha geniş kapsamlı bir koruma sağladığı görülmekle beraber, uluslararası bir uyumsuzluk durumunda Türkiye’nin ya da Türkiye’de bulunan bir veri sorumlusu işletmenin idari anlamda yaptırımla karşılaşma tehlikesi bulunmaktadır. Bu nedenle, mevzuatımızın 2016 yılında 95/46/EC Direktif’i baz alınarak hazırladığı da göz önünde bulundurularak güncellenmesi ve Direktif’ten sonra GDPR ile veri koruma hukukuna katılan hak ve kavramların da mevzuatımıza dahil edilmesi gerekmektedir.

3.2 Kişisel Verilerin Korunması Hakkında Ulusal Kaynaklar

2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’ndan önce, Türk hukukunda, kişisel verilerin korunmasına ilişkin herhangi bir veri koruma düzenlemesi bulunmamaktaydı. Tıpkı 1980 öncesi uluslararası

¹⁶⁹ Avcı, Y., (2019), s. 32.

¹⁷⁰ Tolun, Y., (2020), s. 86.

¹⁷¹ Tolun, Y., (2020), s. 87.

¹⁷² Özkan, O., (2020), s. 74.; Tolun, Y., (2020), s. 87.

düzenlemelerde olduğu gibi konu, özel hayatın gizliliği, kişilik hakkı ve mahremiyet hakkı kapsamı altında inceleniyordu. Türkiye'nin de ilk imzalayan ülkelerden bir olduğu 108 sayılı Sözleşme ile beraber kişisel verilerin korunması hakkı gündeme gelmiştir. Fakat Türkiye'de bulunan yasal düzenlemeler Sözleşme'nin şartlarını karşılamamaktaydı ve Sözleşme'nin gerektirdiği kurumların ülkemizde bulunmamaktaydı. Bu nedenle Sözleşme iç hukukta yürürlüğe geçirilememiş olup, kişisel verilerin korunmasına ilişkin söz konusu düzenleme Türkiye'de 2016 yılına kadar uygulanmamıştır. T.C. Anayasası'nda 2010 yılında değişikliğe gidilmiş olup, Anayasanın 20. maddesine 'Herkesin, kendisiyle ilgili kişisel bilgilerin korunmasını talep etme hakkı vardır.' ibaresi eklenerek, Türkiye'de ilk defa kişisel verilere yönelik hukuki bir koruma sağlanmıştır. Akabinde yapılan çalışmalarda 95/46/EC Direktif'inden esinlenerek Kişisel Verilerin Korunması Kanunu tasarısı hazırlanmıştır. Ancak 2000 yılından itibaren hazırlık çalışmaları yapılan tasarı ancak 2016 yılından KVKK adı altında kanunlaşabilmiştir.

Kişisel verilerin korunmasına yönelik hükümler diğer kanunlarda da görülmektedir. Türk Ceza Kanunu¹⁷³, nun 135. Maddesiyle kişisel verilerin hukuka aykırı olarak kaydedilmesi suç olarak öngörülmüş ve yasaklanmıştır. Kapsam olarak oldukça dar gözüktüğü de kişisel verilerin korunması hakkı açısından yapılan ilk düzenlemelerden biri olduğu dolayısıyla oldukça önemlidir. 4857 sayılı İş Kanunu ile işverenlere işçilerin bilgilerinin saklandığı özlük dosyaları hazırlama ve saklama yükümlülüğü getirilmiştir. Aynı şekilde İş Sağlığı ve Güvenliği Kanunu¹⁷⁴, nda da sağlık muayenesi yapılan işçilerin sağlıklarına ilişkin hassas verilerinin özel hayatın gizliliği kapsamında gizli tutulmasının hükmedildiğini görmekteyiz.

3.2.1 1982 Anayasası

Kişisel verilerin korunması hakkı esasen bireyin temel hak ve özgürlüklerinden biri olduğu için kaynağını Anayasa'dan almaktadır. 2010 yılında gelen değişiklik öncesi kişisel verilerin korunması hakkı, Anayasa'nın 20. maddesiyle düzenlenen özel hayatın gizliliği hakkı kapsamı altında incelenmekteydi. Anayasa'nın 17. Maddesinde düzenlenen bireyin maddi ve manevi varlığını serbestçe geliştirebilme hakkı da kişisel

¹⁷³ 5237 sayılı Türk Ceza Kanunu, *T.C. Resmi Gazete*, Sayı: 25611, 12 Ekim 2004 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

¹⁷⁴ 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, *T.C. Resmi Gazete*, Sayı: 28339, 30 Haziran 2012 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

verilerin korunması hakkıyla ilişkilendirilebilir. Zira bu çalışmada genel olarak bahsedildiği üzere, kişisel verilerin korunması hakkının ve bu haktan doğan diğer hakların temelini, insan onuru ve insanın maddi ve manevi varlığını geliştirme hakkı olduğu yorumlanmıştır. Aynı şekilde 21. Madde ile düzenlenen konut dokunulmazlığı hakkıyla da kişisel verilerin korunmasının sağlanacağını söylemek yanlış olmayacaktır. 24. maddede düzenlenen din ve vicdan hürriyeti uyarınca kimse dini inanç ve kanaatlerini açıklamaya zorlanamaz. Aynı mahiyette 25. Maddede düzenlenen düşünce ve kanaat hürriyeti uyarınca da kimse düşünce ve kanaatlerini açıklamaya zorlanamaz¹⁷⁵. Kişilerin özel nitelikli verilerinden olan dini inançlar ve düşüncelerin üçüncü kişilerle paylaşımının rızaya bağlı olduğunu, rızanın bulunmadığı takdirde işbu verilerin aktarımının yapılamayacağını işbu hükümden de anlayabiliriz.

Nitekim, 2010 yılındaki değişiklikten önce Anayasa Mahkemesi'nin önüne gelen, Türkiye İstatistik Kanunu¹⁷⁶'nun 8. ve 54/2-b maddesinin Anayasa'ya aykırı olduğundan bahisle yapılan başvuru; Anayasa Mahkemesi'nce değerlendirilmiş ve Türkiye İstatistik Kanunu'nun:

“İstatistiki birimler, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür.”

hükmünü amir olan 8. maddesinde ve istenilen verilerin verilmemesi veya eksikliklerin tamamlanmaması halinde idari para cezası öngören 54. maddenin 2. fıkrasının (b) bendinde Anayasa'ya aykırılık bulunmuş olup, söz konusu maddeler iptal edilmiştir. Anayasa Mahkemesi değerlendirmesinde, söz konusu maddelerin Anayasa'nın özel hayatın gizliliğini düzenleyen 20. maddesine ve düşünce ve kanaat özgürlüğünü düzenleyen 25. maddesine aykırılık teşkil ettiğini belirtmiştir¹⁷⁷. Bu husustan da anlaşılacağı üzere kişisel verilerin korunması hakkı Anayasa'da düzenlenen bir temel hak ve özgürlük olmadan önce bir önceki paragrafta belirttiğimiz haklar genelinde incelenmekteydi.

¹⁷⁵ Dursun, Y., (2019), s. 11.

¹⁷⁶ 5429 sayılı Türkiye İstatistik Kanunu, T.C. Resmi Gazete, Sayı: 25997, 18 Kasım 2005 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

¹⁷⁷ Resmi Gazete. (2008). *AYM. 2006/167 E., 2008/86 K. Ve 20.03.2008 Tarihli İptal Kararı* [Çevrimiçi]. Erişim adresi: <https://www.resmigazete.gov.tr/eskiler/2008/06/20080625-8.htm> (Erişim Tarihi: 27.11.2021).; Elbir, N. s. 115.

05.07.2010 tarihli ve 5982 sayılı Anayasa'nın Bazı Hükümlerinde Değişiklik Yapılması Hakkında Kanun uyarınca Anayasa'nın özel hayatın gizliliğini düzenleyen 20. maddesine üçüncü bir fıkra eklenmiş olup, fıkra uyarınca bireylere kişisel verilerinin korunmasını isteme hakkı verilmiştir. Hükmün devamında bu hakkın kapsamı, kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme olarak belirlenmiştir. Kişisel verilerin işlenmesi rızaya tabi tutulmuştur ve işlemeye dair usulün kanunla düzenleneceği hükmedilmiştir. İşbu hükümdeki “*isteme*” ibaresi öğretide eleştirilmektedir. Zira lafzi olarak bakıldığında, kişinin talep etmemesi halinde kişiye ait kişisel verilerin korunmayacağı anlamı çıkarılmaktadır. Aktif olarak vatandaşlarının kişisel verilerini koruma konusunda devletlere herhangi bir pozitif yükümlülük yüklenmeyecektir. Bu haliyle hüküm, kişisel verilerin korunması hakkı temel hak ve özgürlük olarak düzenlenmemişçesine, yalnızca talep edildiğinde hakkın bireysel düzeyde korunacağı anlamı oluşturmaktadır. Anayasa'da kişisel verilerin korunmasına ilişkin maddenin bu şekilde kaleme alınması korumanın eksik ve yetersiz olduğu kanaati oluşturmaktadır. Uncular, bu ibareyle birlikte veri sahiplerinin kişisel verilerinin korunması konusunda devlete bir pozitif yükümlülüğün yüklenmediği görüşündedir¹⁷⁸. Görüşümüz, Velioğlu'nun da izah ettiği üzere işbu hükümle beraber bireylere kişisel verilerin korunmasını hakkının tahsis edildiği yönünde olup¹⁷⁹, maddede geçen “*isteme*” ibaresi hukuka uygunluk sebebi olan ilgili kişinin rızasını kastetmektedir. Bu durumda kişisel verileri isteği dışında işlenen kişilerin yetkili mercilere başvurması ve bireylerin kişisel verilerinin korunması bir anayasal güvence olarak verilmiştir.

Eleştirilen bir diğer husus ise, maddede kişisel verilerin kapsamının dar tutulmuş olmasıdır¹⁸⁰. Uluslararası düzenlemelerle kıyaslandığında, veri koruma ilkelerinden bahsedilmediğini, veri sorumlusunun yükümlülüklerinin ve ilgili kişi veri sahibinin haklarının hepsinin düzenlenmediğini görmekteyiz. İşbu hususlar 20. maddenin 3. fıkrasının devamında kanuna bırakılmış olup, bu ilkelerin Anayasa'da geçmemesi işbu hakkın kapsamının dar olacağını veya anayasal hak olmadığı anlamına gelmemektedir. Kaldı ki, Kanun'da yer almayan bir hak veya Kanun ile uluslararası düzenlemelerin kesiştiği bir husus söz konusu olsa bile; kişisel verilerin

¹⁷⁸ Velioğlu, A., (2020), s. 54

¹⁷⁹ Velioğlu, A., (2020), s. 54.

¹⁸⁰ Velioğlu, A., (2020), s. 54-55.

korunması bir temel hak ve özgürlüktür. Anayasa'nın 90. maddesinin 5. fıkrası uyarınca taraf olunan kişisel verilerin korunmasına ilişkin uluslararası düzenlemeler de kanun hükmünde olmakla birlikte, kanunlarla çatıştığı halde normlar hiyerarşisine göre uluslararası düzenlemelerin uygulanması esastır. Bu hükmün tek istisnası ulusal düzenlemelerimizin temel hak ve özgürlükler konusunda daha geniş kapsamlı bir koruma sağlaması durumudur ki, ulusal ve uluslararası veri koruma mevzuatlarına bakıldığında böyle bir durum maalesef söz konusu değildir.

3.2.2 5237 Sayılı Türk Ceza Kanunu

Kişisel verilerin korunması konusunda Türk Ceza Kanunu'nun düzenlemesi oldukça önemlidir. Özel hayat ve hayatın gizli alanına karşı suçlar başlığı altında düzenlenen TCK'nın 135. maddesi uyarınca kişisel verilerin hukuka aykırı olarak kaydedilmesi suç olarak düzenlenmiştir¹⁸¹.

Kanundaki bahsettiğimiz hükümler, “kişisel veriler” kavramını mevzuatımıza ilk defa getiren düzenlemelerdir. Bu husus da kişisel veri kavramının sınırlarının bilinmemesinden dolayı hangi durumların TCK m. 135 uyarınca suç teşkil edileceği bilinmemekteydi. Kanun'un gerekçesinde kişisel veri kavramı 108 sayılı Sözleşme'ye atıfta bulunarak açıklanmaya çalışılmıştır. Gerekçe, veri sahibinin rızası ve kanunun verilerin kaydedilmesini öngördüğü durumlarda işbu fiilin suç teşkil etmeyeceğini belirtmiştir¹⁸². İşbu hususlar, henüz KVKK'nın tasarısı bile gündemde değilken düzenlenmiştir.

İlgili kanun hükmünün ikinci fıkrasında suça konu kişisel verinin:

“Kişilerin siyasi, felsefi veya dinî görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması.”

durumunu ağırlaştırıcı hal olarak düzenlemiştir¹⁸³. Bu düzenleme ile TCK'da da özel nitelikli ve genel nitelikli veri ayrımının yapıldığını ve özel nitelikli verilerin genel nitelikli verilere nazaran daha geniş bir koruma kapsamında olduğunu görmekteyiz.

¹⁸¹ Yardımcı, A., (2019), s. 45.

¹⁸² Özkan, O., (2020), s. 80.

¹⁸³ Toprak, B., (2018), s. 44.

İşbu maddeyi takiben, kişilerin yasa dışı yollarla ele geçirilmesi ve aktarılması TCK'nın 136. maddesinde, kişisel verilerin kanunun öngördüğü süreler geçtikten sonra silinmemesi TCK'nın 138. maddesinde suç olarak düzenlenmiştir¹⁸⁴. Bu hükümlerle de KVKK uyarınca düzenlenen veri aktarma yasağı ve veri sorumlularına yüklenmiş verileri silme, yok etme ve anonimleştirme yükümlülüğünün ihlalleri durumunda müeyyideler öngörülmüştür. Bunun yanında, tam olarak kişisel verilerle ilişkili olmasa da; kişiler arasındaki konuşmaların yasadışı dinlenmesi ve kayda alınması TCK m. 133 ile, özel hayatın gizliliğinin ihlali TCK m. 134 ile ve haberleşme özgürlüğünün ihlali TCK m. 132 ile suç olarak sayılmaktadır¹⁸⁵.

3.2.3 4857 Sayılı İş Kanunu

Kişisel verilerin korunması hususu hakkında 4857 sayılı İş Kanunu içerisinde de hükümler bulunmaktadır. Bu hükümlerden en önemlisi, çalışmamızın çeşitli yerlerinde bahsettiğimiz işverenlerin veri sorumlusu olmaya zorunlu bırakan ve Sicil'e kaydolmasını zorunlu kılan 75. maddedir. İşbu madde işverenlere işçileri hakkında özlük dosyası hazırlama ve işbu dosyaları saklama yükümlülüğü altına sokmaktadır.¹⁸⁶ Dolayısıyla Kanun işverenlere işçilere ait verileri bir yerde muhafaza etmesini emrederek işçilerin kişisel verilerini işlenmesini öngörmektedir. Kanunda öngörülen saklama yükümlülüğünün otomatik olmayan veya kısmen ya da tamamen otomatik olan ortamlarda gerçekleştirilmesi konusunda bir ayırım yapılmamıştır¹⁸⁷. Tabii ki de, işveren tarafından işlenebilecek kişisel verilerin de bir sınırı bulunmaktadır. Zira, KVKK'nın 4. maddesinde düzenlenen genel ilkeler kapsamında işverenlerin işçilere ait kişisel verileri yalnızca iş ile alakalı amaçlarla işlemesi hukuka aykırı olacaktır. Yine aynı nedenlerle, işçilerin iş ile alakalı olmayan verilerinin işlenmesi, işlenmesi için gerekliliğin bulunmaması durumunda işçilerin kişisel verilerinin işlenmesi, işçinin güncel ve doğru olmayan verilerinin işlenmesi de hukuka aykırı olup, yapıldığı halde işçinin kişisel verilerinin korunması hakkının ihlali sonucunu doğuracaktır¹⁸⁸.

Maddenin devamında talep halinde yetkili memur ve mercilere işçilere ait verilerin aktarılması zorunluluğu getirilmiş olup, verilerin aktarılması KVKK m. 3

¹⁸⁴ Toprak, B., (2018), s. 44-45.; Velioglu, A., (2020), s. 66.

¹⁸⁵ Dursun, Y., (2019), s. 16.

¹⁸⁶ Süzek, S., (2021), s. 418-419.

¹⁸⁷ Velioglu, A., (2020), s. 63.

¹⁸⁸ Manav, E., (2015), s. 107.

uyarınca işleme faaliyetleri kapsamında sayılmaktadır. İşyerine teftiş amacıyla gelen müfettişlerin işçilerin işyeri özlük dosyalarını görmeyi talep etmeleri ya da mahkemelerin işyerlerine müzekkere yazıp, işçilerin özlük dosyalarının getirilmesini istemeleri bu kapsamda değerlendirilir.

Maddenin son fıkrasında kanun koyucu, işverenleri işçilere ait kişisel verileri hukuka uygun ve dürüstlük kuralı çerçevesinde kullanmakla ve işçilere ait gizli kalması gereken kişisel verileri açıklamamakla yükümlü kılmıştır. Bu hüküm ile KVKK m. 12’de “*veri sorumlularının veri güvenliğine ilişkin yükümlülükleri*” başlığı altında düzenlenen sır saklama yükümlülüğü ile bağlantılıdır¹⁸⁹.

Kişisel verilerin korunması kapsamında sayılabilecek bir başka madde ise İş Kanunu’nun 28. maddesidir. Söz konusu madde uyarınca işveren işinden ayrılan işçiye işçinin hangi çeşit olduğunu ve ne kadar süre çalıştığını belirtir bir belge verir. İşçiye ait bilgiler içerdiğinden bu belgenin işçinin kişisel verisi olduğu kabul edilmelidir.¹⁹⁰ İşçinin, işbu belgenin zamanında verilmemesinden veya içerdiği bilgilerin doğru olmamasından kaynaklı bir zararı oluşursa bu zarar ilgili maddenin ikinci fıkrası uyarınca işverenden talep edilebilmektedir. Bu düzenlemeyle de KVKK’nın 11. maddesinde düzenlenen ilgili kişi veri sahibinin zararını talep edebilme hakkının İş Kanunu kapsamında koruma altına alındığını görmekteyiz.

İşverenlerin bu yükümlülükleri riayet etmemesi durumunda İş Kanunu tarafından da yaptırımlar öngörülmüştür. İş Kanunu’nun 104. maddesi işçilerin özlük dosyalarında gizli olarak tutulması gereken kişisel verilerin işveren tarafından hukuka aykırı biçimde herhangi bir işleme tabi tutulması durumunda işverenlere idari para cezası öngörmüştür. Ayrıca, işverenler tarafından işçilerin kişisel verilerinin korunması hakkının ihlali bazı durumlarda 25. maddenin 2. fıkrası uyarınca iş akdinin işçi tarafından feshedilmesi için haklı neden oluşturabilmektedir.

¹⁸⁹ Manav, E., (2015), s. 106.

¹⁹⁰ Yüksel, E. (2021, Eylül 11) Kişisel Verilerin Korunması Kanunu'nun İş Hukuku'na Yansıması, [Blog yazısı]. Erişim adresi: https://tr.linkedin.com/pulse/ki%C5%9Fisel-verilerin-korunmas%C4%B1-kanununun-i%C5%9F-hukukuna-yans%C4%B1mas%C4%B1-yuksel?trk=read_related_article-card_title 2021].

3.2.4 İş Sağlığı ve Güvenliği Mevzuatı

6331 sayılı İş Sağlığı ve Güvenliği Kanunu kişisel verilerin korunması bakımından önemli düzenlemeler içermektedir. Zira kanun kapsamında işverenlere yüklenen yükümlülüklerin neredeyse hepsi işçilerin sağlığına ilişkin veriler ile ilişkili olduğundan ve KVKK kapsamında sağlığa ilişkin veriler özel nitelikli veriler kapsamında daha geniş düzeyde bir korumaya tabi olduğundan, İş Sağlığı ve Güvenliği mevzuatı işbu verilerin korunmasına ilişkin düzenlemelere de yer vermiştir.

İş Sağlığı ve Güvenliği Kanunu uyarınca işverenlerin işçilere işe girerken, işten çıkarken ve hatta periyodik aralıklarla sağlık muayenesi yaptırma yükümlülüğü verilmektedir. Bu muayeneler sonucu işçinin sağlığına ilişkin düzenlenen raporlar özel nitelikteki sağlık verilerini içerecektir. Bu duruma karşı 6331 sayılı Kanun, 15. maddesinin son fıkrasında işçilerin özel hayatının ve itibarının korunması açısından sağlık muayenesindeki bilgilerin gizli tutulacağını öngörmüştür. Ayrıca, aynı maddenin üçüncü fıkrasında çalışanlara işbu sağlık muayeneleri sonucu düzenlenen raporlara itiraz hakkı tanınmıştır. İşbu raporlara konu verilerin otomatik analiz edilmesi söz konusu ise bu hükmün kaynağının KVKK m. 11 uyarınca düzenlenen veri sahibinin itiraz hakkı olduğunu söyleyebiliriz¹⁹¹.

Tıpkı işverenlerin işçiye ait sağlık verilerini gizli tutması yükümlülüğü gibi, işyeri hekimlerine ve sağlık personellerine de de aynı nitelikte bir yükümlülük getirilmiştir. Çalışanların kişisel verilerinin bulunduğu kişisel sağlık dosyalarındaki bilgilerin gizli tutulması yükümlülüğü, İşyeri Hekimi ve Diğer Sağlık Personelinin Görev, Yetki, Sorumluluk ve Eğitimleri Hakkında Yönetmelik¹⁹²'in 11. maddesinde işyeri hekimleri bakımından, 18. maddesinde ise diğer sağlık personelleri bakımından öngörülmüş bir yükümlülüktür¹⁹³. İşyeri hekimleri işverenin kadrolu çalışanı olduğunda işverenle birlikte veri sorumlusu sıfatında, işyeri hekimliği hizmetinin farklı bir firmadan hizmet alım yoluyla gerçekleşmesi halinde ise veri işleyen sıfatında olacaktır. KVKK'nın 12. maddesinin ikinci fıkrası uyarınca her iki halde de işveren

¹⁹¹ Gürsel, İ., (2016), s. 158.

¹⁹² İşyeri Hekimi ve Diğer Sağlık Personelinin Görev, Yetki, Sorumluluk ve Eğitimleri Hakkında Yönetmelik, *T.C. Resmi Gazete*, Sayı: 28713, 20 Temmuz 2013 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

¹⁹³ Gürsel, İ., (2016), s. 158.; Velioğlu, A., (2020), s. 64.

ile işyeri hekimi çalışanların kişisel sağlık dosyalarındaki bilgilerin gizli tutulmaması durumunda müştereken ve müteselsilen sorumlu olacaktır.

Kişisel verilerin korunması hususu İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği¹⁹⁴,nin de konusu olmuştur. Söz konusu yönetmeliğin 7. maddesinin 2. fıkrasında iş değiştiren bir çalışanın eski işverenin, yeni işverene çalışana ait kişisel sağlık dosyasını bir ay içerisinde göndermesi yükümlülüğü düzenlenmiştir¹⁹⁵. Bu yükümlülük, KVKK m. 8/3 uyarınca işçiye ait kişisel verilerin aktarılmasına ilişkin bir hukuka uygunluk sebebi oluşturmaktadır.



¹⁹⁴ İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği, *T.C. Resmi Gazete*, Sayı: 28512, 29 Aralık 2012 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

¹⁹⁵ Velioglu, A., (2020), s. 64.

BÖLÜM 4: KİŞİSEL VERİLERİN KORUNMASI KANUNU

4.1 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Türkiye’de kişisel verilerin korunması hususu, 1981’de Avrupa Konseyi’nin 108 sayılı Sözleşme’nin imzalanmasıyla gündeme alınmıştır. 28 Ocak 1981 tarihinde Sözleşme’nin imzalanmış olmasına rağmen iç hukuka dahil edilişi ve Kişisel Verilerin Korunması Kanunu’nun yürürlüğe girmesi 2016 yılına kadar gecikmiştir. 1989 yılında bir komisyon kurulmuş olup çalışmalarını tamamlayamamıştır, aynı şekilde 2000 yılında kurulan bir başka komisyonun üç yıllık çalışması sonucu oluşturduğu kanun tasarısı kabul edilmemiştir. 2008 ve 2014 yıllarında yeniden bir tasarı hazırlanmış ve meclis önüne getirilmiştir. Fakat işbu tasarılar da güncelliğini koruyamadığından tasarı teklifleri onaylanmamıştır. Nihayetinde, “Kişisel Verilerin Korunması Kanunu”nun tasarısı hazırlanmış ve meclis tarafından onaylanarak 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete ile yürürlüğe girmiştir¹⁹⁶.

KVKK’nın tasarısının oluşturulurken çerçeve niteliğinde olan Avrupa Birliği Konseyi’nin 95/46/EC sayılı Direktif’inden esinlendiğinden bahsedilmiştir. Bu noktada, Direktif’in değil de yine kanunla aynı tarihte hazırlanıp kabul edilen Avrupa Genel Veri Koruma Tüzüğü’nün temel olarak alınması gerektiği eleştirileri yapılmaktadır¹⁹⁷. Gerçekten de Tüzük, Direktif’te mevcut olan sorunlar karşısında başarılı olan ve gelişen teknoloji ve internet karşısında güncelliğini koruyan düzenlemelere sahip olduğundan, ayrıca kişisel verilerin korunması açısından kendinden önceki düzenlemelere göre daha yüksek seviyede koruma sağladığından tasarıya kaynak olsaydı daha faydalı ve gelişmiş bir düzenleme yaratılacağından söz edilebilirdi. Doktrinde bu düşüncenin karşıtları, Tüzük’ün henüz yeni imzalanmasından bahisle, pek çok problem yaratabileceği ve uygulamada yetersiz kalabileceği düşüncesini gerekçe göstermektedir¹⁹⁸. Ek olarak, 20 yıldan fazla yürürlükte bulunan Direktif’in birden çok uyumsuzluğun çözümünde araç olarak kullanmasının pek çok emsal karar yaratması ve bu emsal kararların ülkemizdeki

¹⁹⁶ Velioğlu, A., (2020), s. 55.

¹⁹⁷ Tekin, N. (2014) *Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi*. Uyuşmazlık Mahkemesi Dergisi, C. 0(4), s. 241.

¹⁹⁸ [Leyla Keser] (2016, Kasım 23), *Kişisel Veriler Kanunu’nun Getirdikleri* [Video Dosyası]. Erişim Adresi: https://www.youtube.com/watch?v=yyMUPZSXtoY&ab_channel=E-Ticaretve%C4%B0internetHukukuDerne%C4%9Fi

uyuşmazlıklarda da kullanılabilmesi de; Tüzük yerine Direktif'in tercih edilmesinin doğru olduğunu savunanların gerekçelerinden biridir. Son olarak Tüzük'ün uygulama alanının halihazırda üçüncü ülke statüsündeki ülkeleri de, yani Avrupa Konseyi üyesi olmayan ülkeleri de kapsadığı belirtilmektedir¹⁹⁹. Düşüncemize göre Tüzük, 20 yıl boyunca karşılaşılan sorunların ve güncelliğini yitiren hükümlerin tespiti ile üstesinden gelme vesilesiyle hazırlanmış bir düzenlemedir. Dolayısıyla uygulamada yetersiz kalması söz konusu olmadığı gibi, yetersiz kalan uygulamaya getirilen bir çözüm niteliğindedir. Önceki düzenlemelere kıyasla farklı düzenlemeleri bulunduğundan emsal karar bulma sıkıntısıyla karşılaşılabılır, ancak zaten gelişen teknoloji ile daha önce karşılaşılmamış uyuşmazlıklar gündeme geleceğinden, daha önce verilmemiş kararların da verilmesi ve emsal nitelikte kararlar oluşturulması gerekecektir. Ayrıca, Tüzük'ün üçüncü ülkeler üzerindeki bağlayıcılığı, üçüncü ülkeler ile Tüzük'e tabi ülkeler arası veri aktarımı olduğunda gündeme gelmektedir. Bu doğrultuda, Türkiye ile bir başka Avrupa Konseyi'ne üye olmayan ülke arasındaki sınır ötesi veri aktarımında veya Türkiye'nin kendi sınırları içerisindeki veri işleme durumlarında tüzük hükümleri ve Tüzük'ün sağladığı koruma geçerli olmayacaktır. Bu nedenle, en başında Tüzük referans alınarak hazırlanan bir veri koruma mevzuatının daha güncel ve kapsamlı bir koruma sağlayacağı düşüncesindeyiz.

Mevzuatımızın gerekçesinde veri koruma hukukuna dair herhangi bir düzenlemenin bulunmaması hususuna değinilmiştir. Veri koruma düzenlemeleri başka kanunlarda dağınık halde bulunmakla birlikte, Anayasa'da temel hak ve özgürlük olarak düzenlenen kişisel verilerin korunması hakkına ilişkin ayrı bir mevzuat olmaması sorun teşkil etmekteydi. Bunun yanında, kişisel verilerin korunması hakkının ihlalini tespit eden veya ihlallerin denetimi yapan bir kurumun olmaması da işbu alandaki eksikliklerden bir tanesiydi. Aynı zamanda yine mevzuat yokluğundan kaynaklı olarak, Avrupa'da siber suçlarla ilgilenen kuruluş olan EUROPOL ile ülkemizdeki kolluk teşkilatı arasında bilgi paylaşımı yapılamaması sorunu mevcuttu²⁰⁰. Tüm bu sorunlar kanun koyucu tarafından tespit edilmiş ve KVKK'nın gerekçesinde yer almaktadır. Tabii ki de, bunlar mevzuatın hazırlanmasının bütün sebeplerini oluşturmamaktadır. Zira belirli seviyede veri koruması sağlamayan ülkelere veri aktarımı riskli bir işlem olduğundan ve ülkelerin mevzuatlarının çoğunun

¹⁹⁹ Velioğlu, A., (2020), s. 56.

²⁰⁰ Özkan, O., (2020), s. 82.

bunu yasaklaması durumu söz konusu olduğundan, Türkiye'ye sınır ötesi veri aktarımı sekteye uğramayla karşı karşıya gelmekteydi. OECD başlıklı kısımda bahsettiğimiz üzere günümüz teknoloji çağında, her işlemin internet vasıtasıyla sanal ortamlarda gerçekleştiği bir dönemde veri aktarımının sekteye uğraması, ciddi anlamda ticari olumsuzluklara yol açmaktadır. Yabancı sermayenin ülkemize yatırım olarak gelmesi de ancak yeterli seviyede koruma sağlayan bir veri koruma sistemi oluşturulduğunda mümkün olabilir²⁰¹. Dolayısıyla kişisel verilerin korunması mevzuatının hazırlanmasında ekonomik ve ticari sebepler de mevcuttur. Son olarak Türkiye'nin KVKK'nın kabul edilip yürürlüğe girdiği sene 108 sayılı Sözleşme'yi yürürlüğe geçirmesi de bir sebep olarak gösterilebilir. Çünkü 108 sayılı Sözleşme veri koruma mevzuatı oluşturulmasını şart koşturmaktadır.

4.2 6698 Sayılı Kanun'un Kapsamı

Kişisel Verilerin Korunması Kanunu'nun amacı, kişilerin temel hak ve özgürlüklerinin, özellikle mahremiyetleri olmak üzere korunmasının sağlanması adına gerçek ve tüzel kişilerin haklarının ve yükümlülüklerinin düzenlenmesi olarak belirlenmiştir. Bunu takiben 2. maddede Kanun'un kapsamı, verisi işlenen gerçek kişiler ve veri işleyen gerçek veya tüzel kişiler olarak belirlenmiştir. Tıpkı Direktif ve sonraki düzenlemelerde olduğu gibi tabi olan verilerin otomatik olmayan ile kısmen veya tamamen otomatik olan yollarla işlenmesi, yani her yolla işlenen gerçek kişilere ait verilerin işbu kanun kapsamına gireceği düzenlenmiştir²⁰². Veri sahibine ait verileri işleyen tüzel kişi veri sorumlularının da kamu ya da özel olması gerektiği şeklinde de bir ayırım yapılmadığından hem kamu tüzel kişiliklerinin hem de özel hukuk tüzel kişilerinin işbu kanuna tabi olacağını söylemek mümkündür²⁰³. Kapsam bakımından hem konu hem de süje ve obje bakımından Avrupa Genel Veri Koruma Tüzüğü ile benzer olduğu görülmektedir²⁰⁴.

Kapsam konusunda Kanun'un 28. maddesi işbu kanun kapsamına girmeyecek halleri düzenlemektedir. Bunlardan en önemlisi ve belki de en açık olanı, verilerin gerçek

²⁰¹ Velioğlu, A., (2020), s. 83.

²⁰² Toprak, B., (2018), s. 37-38.; Yardımcı, A., (2019), s. 49.; Elbir, N., (2020), s. 118.; Özkan, O., (2020), s. 86., Velioğlu, A., (2020), s. 57.

²⁰³ "...Özel sektör ve kamu sektörü bakımından bir ayırım yapılmamış olup, öngörülen usul ve esasların her iki sektörde de uygulanması benimsenmiştir...", T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü. (2016). *6698 Sayılı KVKK'nın 2. Maddesinin Gereçesi* [Çevrimiçi]. Erişim adresi: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf> (Erişim Tarihi: 06.12.2021.); Velioğlu, A., (2020), s. 57.

²⁰⁴ Özkan, O., (2020), s. 86.

kişiler tarafından kendisi ve kendisiyle aynı konutta yaşayan aile fertleriyle ilgili işlenmesi durumudur. İşbu istisna veri güvenliği ilkesinin ihlal etmemesi ve verilerin üçüncü kişilerle paylaşılmaması şartlarına bağlanmıştır²⁰⁵. Zira aynı konutta yaşayan kişilerin kişisel verileri birbirlerine açık halde olduğundan, bu kişilere ait verilerin birbirleri tarafından işlenmesinde zımnî olarak rızası olduğu kabul edilmelidir. Kanun'da geçen şart, tıpkı Avrupa Genel Veri Koruma Tüzüğü'nde olduğu gibi verilerin işlenmesinde açık rıza bulunmasıdır. Ancak önceden bahsedildiği üzere mevzuatımız çerçeve niteliğinde olan Direktif'ten uyarlanmış olup, Direktif'te geçerli olan "T"²⁰⁶, yani kişinin verilerin işlenmesine sessiz kalması durumunda rızasının olduğu düşüncesi KVKK'nın işbu hükmünde de görülmektedir.

Bir diğer istisna hali ise verilerin resmi istatistik veya anonim hale getirilme suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesidir. Bu halde de veriler halihazırda anonim halde olacağından ve kişilerin verilerine ilişkin herhangi bir ihlal yaşanamayacağından istisna olarak düzenlenmiştir. Kişisel verilerin sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi de kanun kapsamının dışında tutulmuştur. Meğerki, milli savunma, milli güvenlik, kamu güvenliği ve düzeni, ekonomik güvenlik, özel hayatın gizliliği, kişilik hakları hususlarına hâle getirmesin veya veri işleme faaliyeti suç teşkil etmesin. Bu durumda ise ifade özgürlüğü ile diğer menfaatlerin çatışması durumunda ifade özgürlüğünün geri planda tutulduğu görülmüştür²⁰⁷.

Kişisel verilerin milli savunmayı ve güvenliği, kamu düzenini ve güvenliğini veya ekonomik güvenliği sağlamak adına kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler de kapsam dışı tutulmuştur. Bir önceki istisna ile benzer olarak menfaat çatışmasında kamuyu ilgilendiren menfaatlerin ön planda olduğunu görmekteyiz.

Son olarak, kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halinde işbu kanun hükümlerinin uygulanmayacağı düzenlenmiştir.

²⁰⁵ Elbir, N., (2020), s. 119.; Özkan, O., (2020), s. 92.

²⁰⁶ Selek, O., (2019), s. 930.

²⁰⁷ Özkan, O., (2020), s. 93.

Bu bahsedilen 5 adet istisnai hal tamamen KVKK'nın kapsamı dışında tutulmuş olup, Kanun'un kısmen kapsam dışı tuttuğu haller de mevcuttur. Bu noktada kısmen kapsam dışı tutulmanın ne anlama geldiği açıklanmalıdır. İşbu ibare, Kanun'un 28. maddesinin 2. fıkrasında düzenlenen hallerde Kanun'un veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. maddesinin, veri sahibinin haklarını düzenleyen 11. maddesinin ve veri sorumlularının sicile kayıt yükümlülüğünü düzenleyen 16. maddesinin uygulanmayacağı anlamını taşımaktadır. Veri sahibinin zararın giderilmesini talep etme hakkı bu madde de hariç tutulmuş olup, her türlü durumda ilgili kişiler zararlarını talep edebilme haklarına sahiptirler. Aynı şekilde, maddede düzenlenen istisnai hallerin de Kanun'un amacıyla ve temel ilkeleriyle orantılı olmaları şartı aranmaktadır. Dolayısıyla kısmen kapsam dışı tutulan haller mutlak değildir.

Kanun'un 28. maddesinin 2. bendinde düzenlenen kısmen kapsam dışı tutulan hallerden ilki, kişisel verilerin bir suçun önlenmesi açısından ya da soruşturma için gerekli bir faaliyet olması durumudur. Kamu menfaati kişisel verilerin korunması hakkından ve bununla birlikte gelen haklardan daha üst kademede tutulmuştur. Kaldı ki, suçüstü yakalanmak istenen bir şahsın üzerinin aranacağı ya da konutuna baskın düzenleneceği ve evde bulunan tüm verilerinin toplanacağı ve işleneceği bilgisinin; 10. maddede düzenlenen aydınlatma yükümlülüğü uyarınca şüpheli şahısla paylaşılması istenmeyen sonuçlar doğuracaktır²⁰⁸. Bu halde kişisel verilerin korunması hakkının daha üstün bir menfaat uğruna kısıtlanması gerektiği öngörülmüştür.

Bir diğer kısmen kapsam dışı tutulan hal ise kişisel verilerin, ait olduğu veri sahibi tarafından halihazırda alenileştirilmiş durumda olmasıdır. Bu durumda da aydınlatma yükümlülüğü, veri sorumlusunun başvuruları cevaplama yükümlülüğü, veri sorumlusunun bildirim yükümlülüğü gibi yükümlülüklerin uygulama alanı bulamadığını görmekteyiz. Zira, veriler zaten alenileştirilmiş olup, geniş anlamda üçüncü kişilerin kullanımına açılmıştır. Ancak bu durum, önceden de bahsettiğimiz üzere, söz konusu veri sorumlusunun veri sahibinin verisini işlemesi dolayısıyla veri sahibinin zarara uğraması ve bunun sonucunda uğradığı zararın tazminini talep edebilme hakkını bertaraf etmez.

²⁰⁸ Özkan, O., (2020), s. 94.

Kanun, üçüncü hal olarak veri işleme faaliyetinin kanun tarafından yetkili ve görevli kılınmış kurum ve kuruluşlar veya kamu meslek kuruluşları tarafından gerçekleştirilmesi ve işbu faaliyetin denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması durumunda, yukarıda yazılı üç maddenin uygulanmayacağını düzenlemektedir. Kamu meslek kuruluşları Türkiye Orta Doğu Amme İdaresi Enstitüsü (TODAİE) tarafından Türk Diş Hekimleri Birliği (TDB), Türk Eczacılar Birliği (TEB), Türkiye Esnaf ve Sanatkarları Konfederasyonu (TESK), Türk Mühendis ve Mimar Odaları Birliği (TMMOB), Türk Tabipleri Birliği (TTB), Türk Veteriner Hekimleri Birliği, Türkiye Barolar Birliği (TBB), Türkiye Noterler Birliği, Türkiye Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler Odaları Birliği (TÜRMOB), Türkiye Sigorta ve Reasürans Şirketleri Birliği, Türkiye Odalar ve Borsalar Birliği (TOBB), Türkiye Ziraat Odaları Birliği (TZOB), Türkiye Sermaye Piyasası Aracı Kuruluşları Birliği, Türkiye Bankalar Birliği ve son olarak Türkiye Tarım ve Kredi Kooperatifleri Merkez Birliği olarak belirtilmiştir²⁰⁹. Bu durumda işbu kuruluşların mensupları hakkında yapacağı disiplin soruşturmaları ya da denetimlerde işlenecek verilerde Kanun'un söz konusu maddede belirtilen üç adet maddesi uygulanmayacaktır.

Son olarak ise işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması durumu kısmen kapsam dışı tutulan istisnai hal olarak düzenlenmektedir.

4.3 KVKK'ya Özgü Terimlere Dair Tanımlar

Kanun'un 3. maddesi kavramlara ilişkin bir düzenleme olup, veri işleyen ve veri sorumlusu olarak iki tür farklı kavramdan bahsedildiğini görmekteyiz. Kişisel Verileri Koruma Kurumu, işbu kavramları şöyle tanımlamaktadır. Veri sorumluları kişisel verilerin işleme araçlarını ve vasıtalarını belirleyen ve veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişilerdir. Veri işleyenler ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler olarak

²⁰⁹ Deliorman, R. B. ve Kandemir, A. Ü. (2009) *Kamu Kurumu Niteliğinde Meslek Kuruluşları Ve Etik. Yolsuzluğun Önlenmesi İçin Etik Projesi Akademik Araştırma Çalışması*, s. 5.

tanımlanmaktadır.²¹⁰ Bu tanımlarda her ne kadar veri işleyen, veri sorumlusunun organizasyonunun dışında tutulmuş olduğu belirtilmiş olsa da veri sorumluları ve veri işleyenler aynı kişi olabilmektedir²¹¹ ve çoğunlukla aynı tüzel kişi olmaktadır. Yani veri sorumlu tüzel kişi olan şirket olurken, veri işleyen ise o şirkette çalışan insan kaynakları müdürü, güvenlik birimi personeli gibi bir işçi olmaktadır²¹². İşbu kavramlar Tüzük'te “*controller*” (kontrol eden = veri sorumlusu) ve “*processor*” (işleyen = veri işleyen) olarak bulunmaktadır.

Yabancı bir diğer kavram ise veri kayıt sistemidir. Veri kayıt sistemi kavramı Kanun'da kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi olarak açıklanmıştır. Belirli kriterlere göre ibaresinden anlaşılan, bir düzenlilik olması gerektiğidir. Düzensiz aralıklarla toplanan verilerin oluşturduğu ve veri türlerinin ve kategorilerin uyuşmadığı veri topluluklarının bu kanun kapsamında veri kayıt sistemleri oluşturmayacağını söyleyebiliriz.²¹³

4.4 Temel İlkeler

4. maddede ise kişisel verilerin korunması hakkına ilişkin temel ilkelerin düzenlendiğini görmekteyiz. İşbu ilkeler OECD Rehber İlkelerinden itibaren düzenlenen ilkelerle benzer nitelik taşımaktadır. OECD düzenlemesinde sekiz adet olan ilkeler Direktif ile beraber derlenmiş olup, KVKK mevzuatımızda veri işlenmesinde olması icap eden 5 adet ilkedden bahsedilmektedir. İşbu ilkeler, (1) kişisel verilerin işlenmesinin hukuka ve dürüstlük kurallarına uygun olarak yapılması, (2) verilerin işlendiği an doğru olması ve gerektiğinde güncel olması, (3) veri işlemenin belirli, açık ve meşru amaçlar çerçevesinde gerçekleştirilmesi, (4) işlenecek verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve (5) veri mevzuat gereğince işleniyorsa mevzuatta belirtilen süreyle, aksi halde işlendikleri amaç için gerekli olan süreyle muhafaza edilmesi olarak açıklanmaktadır²¹⁴.

İlk unsur olan hukuka ve dürüstlük kuralına uygunluk, kaynağını Türk Medeni Kanunu'nun 2. maddesinden almakta olup; dürüstlük kuralına kıstas olarak orta zekalı,

²¹⁰ Kişisel Verileri Koruma Kurumu. *Veri Sorumlusu Ve Veri İşleyen* [Çevrimiçi]. Ankara. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen> (Erişim Tarihi: 07.12.2021).

²¹¹ Elbir, N., (2020), s. 120.

²¹² Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkara, E., (2021), s. 408.

²¹³ Elbir, N., (2020), s. 121.

²¹⁴ Manav, E., (2015), s. 40-45.

makul ve mantıklı bir bireyin yapacağı davranış belirlenmiştir. Tabii ki, söz konusu özelliklere sahip ortalama bir bireyden, kişisel verileri işlerken veri sorumlusuna yükletilen yükümlülüklerle uygun hareket etmesi beklendiğinden, söz konusu veri sorumlusunun yükümlülüklerinin yerine getirilmemesi durumunda da dürüstlük kuralına aykırılıktan işbu ilkenin ihlal edildiğinden söz edebiliriz²¹⁵.

Verilerin işlendiği an doğru ve gerektiğinde güncel olması hususu oldukça önemli bir durum olup, veri koruma taraflarının her ikisine de yükümlülükler yüklemektedir. Veri sorumlusu bilgilerin doğru ve güncel olduğunu kontrol etmekle, olmadığı takdirde işbu verilerdeki eksikliği gidermek, verileri düzeltmek, anonim hale getirmek veya silmekle mükellef olduğu gibi; veri sahibi ilgili kişi de kendine ait verilerin doğru ve güncel olduğunun denetimini yapmakla ve aksi bir durumda bunu veri sorumlusuna bildirmekle mükelleftir. Bu ilke veri sorumlusunu, ek olarak veri sahibinin verilerinin doğruluğunu ve güncelliğini araştırma yükümlülüğü altına sokmamakta olup; veri sorumlusunun veri sahibine, verilerin doğru veya güncel olmaması ihtimaline karşı verileri düzeltme veya silme imkânı tanınmasının işbu ilkenin sağlanması açısından yeterli olduğu kabul edilmektedir²¹⁶.

Amacın açık, belirli ve meşru olması ilkesi tezatlıkla karşılaşabilmektedir. Zira veri sorumlusu, veri sahibine verilerinin işleniş amacını aktardığında her amacı spesifik olarak yazmakla yükümlü olup, aynı zamanda anlaşılabilir olmalıdır. Uzun ve karmaşık açıklamalar, amaç metnini anlaşılabilir kılacak ve açıklık sağlanamayacaktır. Meşruluk ise işlenen verinin veri sorumlusunun sunduğu hizmet ile bağlantılılığını temsil etmektedir. Örneğin, bir avukatın müvekkilinin tapu işlemleri için müvekkilinden cinsel tercihleri hakkında bilgi almak istemesi, işbu isteğin açık ve belirli olmasına rağmen meşruluk vasfını taşımadığından; yani yapılan işlemlerle bir alakası olmayacağından söz konusu ilkenin varlığından söz edilemez. Ek olarak, amacın değişmesi durumunda, verilen rıza başka bir amaç için verilmiş olduğundan, işbu yeni amaç için tekrardan rıza alınması gerekecektir²¹⁷.

Toplanan verilerin amaçla bağlantılı, sınırlı ve ölçülü olması gerekmektedir. Beraber, bir önceki ilke ile benzerlik bulunmaktadır. Zira işbu ilke gereğince de gerek toplanma gerekse işleme amacının meşru olması gerekmektedir. Anca amacın meşru

²¹⁵ Tolun, Y., (2020), s. 40.

²¹⁶ Tolun, Y., (2020), s. 42.

²¹⁷ Tolun, Y., (2020), s. 43.

olması tek başına yeterli olmamaktadır. Zira bir doktorun, hastasını tedavi etmek amacıyla sağlık verilerini toplaması meşruluk özelliği barındırırken, göğüs hastalığının tedavisine ilişkin gelen hastadan ayak tomografisinin istenmesi amaçla bağdaşmadığından, amaçla sınırlı kalınmadığından ve ölçülü bir istek olmadığından bu ilkeyle uyuşmamaktadır²¹⁸.

Veri sorumlusu tarafından işlenmek üzere toplanan verilerin saklanması mevzuatta öngörülen veya makul bir süreyi aşmaması gerekmektedir. Süre aşımı durumunda veri sorumlusu tarafından yapılması gereken iki davranış bulunmakta olup, bunlar işbu veriyi silmek veya anonim hale getirmektir. Makul sürenin tespitinde, yine dürüstlük kuralı uyarınca ortalama bir bireyin kıstas olarak alınması görüşü mevcuttur²¹⁹. Veri sorumluları amaç için belirledikleri bu süreyi KVKK'nın 16. maddesi uyarınca Veri Sorumluları Sicili'ne kayıt için başvurduklarında bildirmek zorundadır²²⁰.

4.5 Normal Nitelikli Verilerin İşlenmesi

KVKK'nın 5. maddesinde tıpkı Direktif'te düzenlenmiş olduğu gibi kişisel verilerin işlenmesinin yasak olduğu görülmektedir. Kişisel verilerin işlenmesi ancak belirli hallerde hukuka uygun olup, bu hukuka uygunluk halleri 5. madde de düzenlenmiştir. İlk ve en yaygın hukuka uygunluk sebebi ilgili kişi veri sahibinin kişisel verilerinin işlenmesinin rızasının bulunmasıdır. KVKK'daki rıza kavramı Direktif'ten esinlenilmiş olup, esas olarak kişinin özgür iradeyle, özel ve bilgilendirilmiş olarak verdiği onay olarak tanımlanmıştır. Nitekim, Avrupa Birliği'nin Avrupa İnsan Hakları Mahkemesi ile birlikte hazırladığı "Avrupa Veri Koruma Hukuku El Kitabı"nda söz konusu rıza kavramının üç unsura sahip olması halinde gerçekleşeceği belirtilmiştir. Kitaba göre rızanın varlığından söz edilebilmesi için; kişi, rıza verme anında baskı halinde olmamalıdır, rızanın içeriği, kapsamı ve sonuçları hakkında bilgilendirilmiş olmalıdır ve kişiye rızasını her aşamada geri alma imkânı tanınmalıdır²²¹.

²¹⁸ Tolun, Y., (2020), s. 44.

²¹⁹ Tolun, Y., (2020), s. 45.

²²⁰ Kişisel Verileri Koruma Kurumu. (2019) s. 17.

²²¹ Elbir, N., (2020), s. 130.

Rızanın bulunmadığı durumlarda ise kişisel verilerin işlenebileceği haller de mevcuttur. Hatta Kurum'un kanaatine göre, verilerin bu hallere dayandırılarak işlenebilecekken; açık rızaya dayandırılarak işlenmesi hukuka uygunluk ve dürüstlük kuralı ilkesine aykırılık teşkil edeceğinden söz konusu olasılıkta kişisel verilerin işlenmesi hukuka aykırı olacaktır²²². Bu nedenle, Kanun'un 5. maddesinin 2. bendinde düzenlenen hallerin varlığı durumunda, açık rızanın alınmaması gereklidir.

Açık rızanın gerekli olmadığı hallerden ilki kişisel verilerin düzenlenmesinin kanun uyarınca öngörüldüğü hallerdir. Bu hallere örnek olarak 4857 sayılı İş Kanunu'nun 75. maddesi uyarınca çalıştırdığı işçilere ait bilgi ve belgelerin toplandığı bir işyeri özlük dosyası hazırlama yükümlülüğü verilebilir.²²³ Bu durumda, işçilere ait gerek genel nitelikli gerekse özel nitelikli kişisel verilerin işverenler tarafından toplanmasını, saklanmasını ve gerektiğinde belirli mercilere aktarılması, işçilerin rızası olmaksızın yapılması gereken kanunda öngörülmüş hallerden biridir. Aynı şekilde 2559 sayılı Polis Vazife ve Salahiyet Kanunu²²⁴'nun 5. maddesi uyarınca 5/1 kategorisine giren her kişinin "*parmak izlerinin polis tarafından alınacağı*" düzenlenmiştir²²⁵. Parmak izleri, biyometrik veri kapsamında kişiye ait özel nitelikli verilerden bir tanesi olup²²⁶, normal şartlarda işlenmeleri KVKK'nın 6. maddesi uyarınca açık rıza olmaksızın işlenemezler. Fakat tıpkı 5. maddede olduğu gibi, KVKK'nın 6. maddesinin 3. fıkrası da kanunun öngördüğü hallerde özel nitelikli verilerin işlenmesini açık rızaya gerek olmaksızın mümkün kılmaktadır.

Kişisel verilerin işlenmesi yasağının bir diğer istisnası ise kişinin rızasını açıklamasının veya rızasının hukuken geçerli olmasının fiili imkânsızlık sebebiyle mümkün olmaması durumunda kişisel verilerin işlenmesinin veri sahibinin veya üçüncü bir kişinin hayatı ya da beden bütünlüğü için zorunlu olmasıdır. İşbu düzenleme Anayasa'nın kişi dokunulmazlığının düzenlendiği 17. maddesinin 2. fıkrasıyla oldukça benzerlik göstermektedir. Hükme göre tıbbi zorunluluklar halinde kişinin vücut bütünlüğüne müdahalede bulunulabilecektir. Aynı şekilde KVKK'nın öngördüğü işbu hal uyarınca da tıbbi zorunluluk halinde bilinci yerinde olmayan bir

²²² Özkan, O., (2020), s. 131.

²²³ Özkan, O., (2020), s. 132.

²²⁴ 2559 sayılı Polis Vazife ve Salahiyet Kanunu, *T.C. Resmi Gazete*, Sayı: 2751, 14 Temmuz 1934 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

²²⁵ Elbir, N., (2020), s. 136.

²²⁶ Erdinç, G. H. (2020) *Ölçülülük İlkesi Ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi*, *Kişisel Verileri Koruma Dergisi*, C. 2(1), s. 3.

hastadan kan veya doku örneği alınması ve işbu verilerin işlenmesi hukuka uygunluk sebebi olarak düzenlenmiştir²²⁷. Bu durumda dikkat edilmesi gereken en önemli husus verinin işlenmesinin kişilerin hayatı ya da beden bütünlüğü için “zorunlu olması”dır. GDPR düzenlemesinde de böyle bir durum hukuka uygunluk sebebi olarak kabul edilmiş olup, düzenlemede “*gerekli olması*” şartı aranmıştır.²²⁸

Veri sorumlusuna yükletilen hukuki yükümlülüğün yerine getirilmesi için zorunlu veri işleme faaliyetlerinin de hukuka uygun olacağı düzenlenmektedir. İşbu hal ile kanunda öngörülen durumlarda veri işlenmesinin hukuka uygun olması hali çoğu durumda aynı şeyi ifade etmektedir. Buna örnek verilebilecek olan Kurul’un avukatlara yönelik verdiği bir kararda²²⁹; avukatların veri sorumlusu statüsünde olduğu ve mesleklerini icra ederken İcra ve İflas Kanunu²³⁰ ve Avukatlık Kanunu²³¹ gibi kanunlardan doğan yükümlülüklerini yerine getirdiklerini, dolayısıyla veri işlemlerinin rızaya gerek olmaksızın gerçekleştirilebileceği yorumu yapılmıştır²³².

Veri sorumlularına bir hakkın kullanılması veya korunması için veri işleminin zorunlu olması durumunda kişisel verilerin hukuka uygun olarak işlenmesi imkânı tanınmıştır. Madde gerekçesinde çalıştığı yere karşı dava açan bir işçinin işverenin savunmasını ispatlaması amacıyla işçiye ait verilerin kullanılması şeklinde örnek verilmiş olup, çok geniş kapsamlı bir düzenleme olduğundan ve kötü amaçlarla kullanılması ihtimali bulunduğundan, zorunluluk esası oldukça önem taşımaktadır²³³.

Bir başka hukuka uygunluk sebebi olarak veri sorumlusunun meşru menfaatleri için veri işleminin zorunlu olması durumu Kanun’da sayılmıştır. Sayılan diğer hallerden farklı olarak, bu durumda veri sahibi ilgili kişinin temel hak ve özgürlüklerine hanel getirmeme şartı aranmıştır. Zorunluluk ifadesi de tekrardan karşımıza çıkmakla birlikte maddenin gerekçesinde veri sorumlusunun meşru menfaati ile ilgili kişinin meşru menfaati arasındaki dengeye vurgu yapılmaktadır.

²²⁷ Özkan, O., (2020), s. 132.

²²⁸ Özkan, O., s., (2020), 133.; Elbir, N., (2020), s. 138.

²²⁹ Kişisel Verileri Koruma Kurumu, (2020). “*Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında*” *Kişisel Verileri Koruma Kurulunun 14.01.2020 Tarihli ve 2020/26 Sayılı Karar Özeti* [Çevrimiçi]. Erişim Adresi: <https://www.kvkk.gov.tr/Icerik/6697/2020-26> (Erişim Tarihi: 09.12.2021).

²³⁰ 2004 sayılı İcra ve İflas Kanunu, *T.C. Resmi Gazete*, Sayı: 2128, 19 Haziran 1932 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

²³¹ 1136 sayılı Avukatlık Kanunu, *T.C. Resmi Gazete*, Sayı: 13168, 7 Nisan 1969 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

²³² Özkan, O., (2020), s. 137.

²³³ Küzeci, E. (2020) *Kişisel Verilerin Korunması*, 4üncü Bası, İstanbul: Oniki Levha Yayıncılık, s. 400.

Kurul ise, veri sorumlusunun meşru menfaatleri için kişisel verilerin işlenmesinin zorunlu olması halini de hukuka uygunluk sebebi olarak nitelendirmiştir²³⁴. Bunun yanında, Kurul ve Kurum tarafından meşru menfaate ilişkin bazı şartlar düzenlenmiştir. Bunlar; (1) meşru menfaat ile ilgili kişinin temel hak ve özgürlüklerinin yarışabilir seviyede olması, (2) meşru menfaatin mevcut, belirli, veri sorumlusunun güncel aktiviteleriyle bağlantılı ve ona yakın gelecekte fayda sağlayacak nitelikte olması, (3) meşru menfaatin zorunlu olması, (4) meşru menfaatin çok sayıda kişiyi etkilememesi ve kâr ve ekonomik yarar amacına ilişkin olmaması, (5) ilgili kişinin temel hak ve özgürlüklerinin korunması amacıyla her türlü tehlikenin bertaraf edilmesi (bu kapsamda temel hak ve özgürlüklerin ihlali gerekmez, tehlikenin mevcudiyeti bile meşru menfaati geçerli kılmayacaktır.), (6) verilerin veri kayıt sistemindeki amaçlarla sınırlı olarak hukuka uygun işlenmesinin temin edilmesi ve tüm tedbirlerin alınması, (7) 4. maddede düzenlenen genel ilkelere uyulması, (8) meşru menfaat ile ilgili kişinin temel hak ve özgürlüklerinin arasında denge testi yapılmasıdır²³⁵.

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması hali hukuka uygunluk sebebi olarak belirlenmiştir. Tüzük'ün "veri taşınabilirliği" hakkını ve rızanın koşullarını düzenlediği maddelerinde de sözleşmenin kurulması ve ifası için gerekli olması halinde kişisel verilerin işlenmesinden bahsedilmiştir. Sözleşmenin kurulması sözleşme yapılmadan önce verilerin işlenmesini, ifası ise sözleşmeden sonra verilerin işlenmesini ifade ettiğinden ortada iki ayrı durum söz konusudur. Gerekliğin tanımının yapılabilmesi için ise sözleşmenin asıl amacının çözümlenmesi gerekmektedir²³⁶. Kanun'da ise bu duruma ilişkin, sözleşme kurulması durumunda kredi sözleşmeleri yapılabilmesi için bankaların sözleşme öncesi şahısların

²³⁴ Elbir, N., (2020), s. 140

²³⁵ Kişisel Verileri Koruma Kurumu. (2019). "Veri Sorumlusunun Kanuni Yükümlülüğünü Yerine Getirmek İçin İşlediği Kişisel Verileri Meşru Menfaat Çerçevesinde Kullanma Talebiyle Kuruma Yapmış Olduğu Başvuru" Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli Ve 2019/78 Sayılı Karar Özeti [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/5434/2019-78> (Erişim Tarihi: 09.12.2021).

²³⁶ "It is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance.", Article 29 Working Party. (2014). *Opinion 06/2014 On The "Notion Of Legitimate Interests Of The Data Controller Under Article 7 Of Directive 95/46/EC* [Çevrimiçi]. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (Erişim Tarihi: 09.12.2021).

bordrolarını alıp işlemesi, sözleşme ifası durumunda ise borçlunun ödeme yapabilmesi adına alacaklının banka hesap bilgilerini alıp işlemesi örnekleri verilmiştir²³⁷.

Son olarak, veri sahibi ilgili kişinin verilerini alenileştirmiş olması durumunda açık rıza aranmaksızın verilerin işlenebilmesine imkân tanınmıştır. Kanun'un kısmen kapsam dışı olarak düzenlediği bu halde, verilerin kimin tarafından alenileştirildiği büyük önem taşımaktadır. Zira işbu alenileştirme işlemi veri sahibi tarafından gerçekleştirildiyse, o halde verilerin korunmasında hukuki yarar bulunmayacaktır. Lakin üçüncü kişilerin verileri alenileştirmesi meşru bir alenileştirme olmayıp kişisel verilerin korunması hakkının ihlalidir²³⁸. Bunun yanı sıra bir diğer önemli husus ise alenileştirme işlemindeki amaç ile veri işlemenin bağdaşmasıdır. Şayet, bir şahsın verdiği hizmete ilişkin internet sitesi hazırlaması ve iletişim bilgilerini bu sitede paylaşması bize iletişim bilgilerini alenileştirme amacının verdiği o hizmete ilişkin soruları cevaplamak olduğunu anlatmaktadır. Bu şahsın iletişim bilgilerinin günümüzde çokça olduğu gibi çeşitli şirketler tarafından alınıp, reklam amaçlı mesajların gönderilmesi “*verilerin alenileştirilmesi hukuka uygunluk sebebi*” kapsamına alınmayıp, kişisel verilerin korunması hakkının ihlaline yol açmaktadır.

Tüm bu hukuka uygunluk sebepleri kişilerin verilerinin işlenmesine olanak sağlamakta olup, veri sahiplerinin kişisel verilerinin hukuka uygun olarak işlenmesi için yalnızca bu sebeplerin varlığı yeterli olmamaktadır. Veri sorumlusu ve veri işleyen, KVKK'nın 4. maddesinde düzenlenen genel ilkelere de riayet etmekle yükümlüdür. Aksi takdirde veri işleme faaliyeti hukuka aykırılık teşkil edecektir²³⁹.

4.6 Özel Nitelikli Verilerin İşlenmesi

Bu çalışmanın ilk bölümünde bahsedilmiş bulunan hassas verilerin işlenmesi konusu KVKK'da özel nitelikli verilerin işlenmesi başlığı altında 6. maddede düzenlenmiştir. Maddede özel nitelikli veri tanımı yapılmamış olup, özel nitelikli veri kategorisindeki veri türleri sayılmıştır. Bu haliyle Kanun tarafından özel nitelikli veri türleri numerus clausus biçimde belirtilerek sınırlandırılmıştır²⁴⁰. Ancak öncesinde de belirtildiği üzere bu şekilde bir sınırlandırılmanın yapılması faydalı olmayacaktır. Zira

²³⁷ Kişisel Verileri Koruma Kurumu, (2019) s. 19.

²³⁸ Özkan, O., (2020), s. 138.

²³⁹ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 407.; Süzek, S., (2021), s. 420.

²⁴⁰ Elbir, N., (2020), s. 145.; Dursun, Y., (2019), s. 51.

kişilerin fotoğrafları onların sağlıklarına, cinsiyetlerine, ırklarına ve inançlarına ilişkin verilere sahip olmakla birlikte, sırf bu nedenle söz konusu fotoğrafların özel nitelikli veri kapsamına alınması amaca tezat düşecektir. Bu nedenle, bu tip olaylarda amaçsal yorum yapılmasının ve kişisel verileri özel nitelikli olarak değerlendirme amacının tespitinin yapılmasının gerekliliği görülmektedir²⁴¹.

Tıpkı normal nitelikli veriler gibi özel nitelikli verilerin de işlenmesi yasaklanmış olup, bu yasağın kalktığı hukuka uygunluk sebepleri KVKK'nın 6. maddesinde düzenlenmiştir. Özel nitelikli kişisel verilerin işlenmesindeki ilk ve en önemli hukuka uygunluk sebebi açık rızanın bulunmasıdır.

Kanun, özel nitelikli veriler arasında da cinsel hayata ve sağlığa ilişkin veriler ve diğerleri olmak üzere bir ayrıma gitmiştir. Sağlığa ve cinsel hayata ilişkin veriler dışında kalanların da kanun öngörülen hallerde açık rıza bulunmaksızın işlenebileceği düzenlenmiştir. Ayrıca sağlığa ve cinsel hayata ilişkin verilerin ise açık rıza bulunmaksızın ancak, (1) kamu sağlığının korunması, (2) koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, (3) sağlık hizmetleri ile finansmanının planlanması ve yönetimi amaçları mevcutsa, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilir²⁴². Yani, ilgili kişinin özel nitelikte bir verisi işlenirken; öncelikle verinin sağlık veya cinsel hayat ile alakalı olup olmadığının tespiti yapılmalıdır. Eğer alakalı değilse, veri açık rıza veya kanunda öngörülen hal varsa işlenebilecektir. Eğer alakalıysa, veri yine açık rızanın bulunduğu halde veya yukarıda bahsettiğimiz KVKK m. 6/3'te özel olarak belirlenmiş nedenler ve yine özel olarak belirlenmiş kimseler tarafından işlenebilecektir. Bu özel olarak belirlenmiş olan "sır saklama yükümlülüğü bulunan kişiler" mevzuatta düzenlenmiş olmalıdır. Yani, sözleşmesel bakımdan sır saklama yükümlülüğü bulunan kimseler bu fıkra kapsamında alınmayacakları gibi, sağlık ve cinsel hayata ilişkin verileri işleyemezler²⁴³.

Tabii ki, böyle bir düzenlemenin varlığı uygulamada sorunlar yaratmaktadır. Şöyle ki; İş Kanunu'nun 75. maddesi uyarınca işverenlerin, işçilerinin bilgilerini içeren ve işçilere ait işyeri özlük dosyaları düzenlemesi ve muhafaza etmesi

²⁴¹ Tolun, Y., (2020), s. 46.

²⁴² Toprak, B., (2018), s. 71.; Manav, E., (2015), s. 110.; Elbir, N., (2020), s. 145.; Tolun, Y., (2020), s. 46-47.

²⁴³ Özkan, O., (2020), s. 147.

yükümlülüğünün olduğundan bahsetmiştik. İşyeri özlük dosyaları, işçinin sağlığına ilişkin bilgiler de içermektedir. Hatta KKVK'nın 6. maddesinin gerekçesinde, her türlü sağlık kuruluşu, Sağlık Bakanlığı ve Sosyal Güvenlik kurumunun bu amaç için muhafaza ettikleri tüm verilerin sağlığa ilişkin veri olduğu belirtilmiştir. Dolayısıyla işçinin işyeri özlük dosyasında bulunan sağlık raporları, SGK maluliyet evrakları, iş kazası ve meslek hastalığına ilişkin evraklar gibi tüm belgeler sağlığa ilişkin veriler içerdiğinden işlenebilmeleri için KVKK m. 6/3'teki şartların oluşmuş olması gerekmektedir. Ancak, işveren sır saklama yükümlülüğü bulunan bir kişi olmadığı gibi, işçinin işyeri özlük dosyasındaki sağlığa ilişkin verilerin işlenmesi de söz konusu maddede belirlenmiş amaçlarla yapılmamaktadır. Bu doğrultuda işverenlerin bu verileri işleyebilmesinin tek yolu, veri sahibi işçilerin açık rızalarının alınmasıdır. Toplu olarak rıza alınması veri koruma hukuku uyarınca geçerli olmadığından her alınan veri ve alındığı şahıs için ayrı olarak rıza alınması gerekmektedir. Bu durum da hiç pratik olmayan bir sonuç doğurmaktadır.

Avrupa Genel Veri Koruma Tüzüğü'nün 9/2-h maddesinde; veri işlemenin işçinin performansını değerlendirmek için zorunlu olduğu durumların hukuka uygunluk sebebi olarak düzenlenmesiyle bu sorunun önüne geçilmiştir. Yine bahsetmiş olduğumuz ILO Uygulama Kodu'nun 6/7. maddesinde, işçiye ait sağlık verilerinin “işçinin belirli bir istihdam için uygun olup olmadığının belirlenmesinde ve sosyal yardım haklarının belirlenip verilmesi” amacıyla hukuka uygun olarak işlenebileceği düzenlenmiştir. Lakin Tüzük, Türkiye’de geçerliliği olan bir mevzuat olmadığı gibi; düzenlemelerinin de uygulanma imkânı bulunmamaktadır. Aynı şekilde, ILO Uygulama Kodu, bağlayıcılığı bulunmayan, yalnızca tavsiye niteliğindeki bir düzenlemedir. Dolayısıyla düzenlemelerin kanun yerine uygulanması söz konusu değildir²⁴⁴.

İş Kanunu'nun 75. maddesiyle getirilen yükümlülüğün işverenleri sağlık ve cinsel verilerin işlenmesini zorunlu kıldığı görülmektedir. Aynı şekilde yine İş Kanunu'nun 30. maddesiyle işverenlere belli hallerde eski hükümlü ve engelli çalıştırma yükümlülüğü yüklenmiş olup, işbu yükümlülüğün yerine getirilebilmesi için özel nitelikli veri kapsamına giren “kişinin engelli olması” veya “kişinin eski hükümlü olması” bilgilerinin işlenmesi gerekmektedir. 6331 sayılı İş Sağlığı ve Güvenliği

²⁴⁴ Toprak, B., (2018), s. 72.

Kanunu'nun 15. maddesiyle işverenlerin, çalışanlara belirli koşullar sağlandığında sağlık muayenesi yapma ve elde edilen bilgileri gizli olarak saklama yükümlülüğü mevcuttur. Yine İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği'nin 7. maddesi ile işverenlere, işçinin işyeri değiştirmesi durumunda kişisel sağlık dosyasının yeni işverene aktarma yükümlülüğü getirilmiştir. Asbestle çalışılan işyerlerindeki işverenlere, işçilerin asbeste maruz kalma oranlarını içeren kayıtların saklanması ve talep halinde ilgili kişilerle paylaşılması zorunluluğu getirilmiştir. Tüm bu yükümlülükler ışığında, işverenlerin kanunda görülen haller ile yetkili kılındığını söyleyebiliriz²⁴⁵. Ancak özel nitelikli verilerin işverenler tarafından işlenmesi, KVKK'nın 6. maddesinin 3. bendinde belirlenen amaçlar kapsamına halen girmemektedir.

Bu noktada, işyeri hekimi vasıtasıyla açık rıza aranmaksızın işçilerin özel nitelikli verilerinin işlenmesi hukuka uygun olacaktır. Zira hekimler kanun uyarınca sır saklama yükümlülüğü bulunan kişiler olup, işyeri hekimlerinin sağlık verilerini işlemesi düzenlemede belirlenen amaçlar kapsamına da alınabilir. Tabii ki de her işyerinde işyeri hekimi bulunmamaktadır. Bu noktada ise işçilerden açık rıza alınması yoluna gidilecektir. Sağlığa ve cinsel hayata ilişkin verilerin işlenmesi için her seferinde açık rıza alınması zorlayıcı bir durum olsa da, KVKK uyarınca işyeri hekimi bulunmayan işyerlerindeki işverenlerin başka bir imkanı bulunmamaktadır.

Ülkemizde son iki yıldır etkisini gösteren COVID-19 virüsü dolayısıyla sağlığa ilişkin verilerin işlenmesi daha kolay ve pratik hale gelmiştir. İşyerinde semptom gösteren veya hasta olan bir personelin olması durumunda, durum kamu sağlığını ilgilendirdiğinden işçilere ait sağlık verileri açık rıza aranmaksızın işlenebilecektir²⁴⁶.

4.7 Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi

Kişisel verilerin işlenme sebeplerinin ortadan kalkması durumunda KVKK'nın 7. maddesi uyarınca silinmeleri, yok edilmeleri veya anonim hale getirilmeleri gerekmektedir. İşbu yükümlülük, kişisel verilerin işlenme sebebinin ortadan kalkması ile resen olacağı gibi; ilgili kişi veri sahibinin talebi üzerine de gerçekleştirilir²⁴⁷. Zira

²⁴⁵ Toprak, B., (2018), s. 73.

²⁴⁶ Özkan, O., (2020), s. 148.

²⁴⁷ Baskın, O. (2020). *Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, s. 41.

ilgili kişilerin kişisel verilerinin gereğinden uzun süre saklanması o kişinin maddi ve manevi kişilik haklarının ihlaline yol açacaktır²⁴⁸.

Bu maddede bahsedilen silinme, yok edilme ve anonim hale getirilme işlemleri hem KVKK'nın Kişisel verilerin silinmesi ve yok edilmesi işlemi adından da anlaşılacağı üzere internet ortamından kaldırılması veya erişilemez, geri getirilemez veya tekrar kullanılamaz duruma getirilmesi işlemidir. Kişisel verilerin anonimleştirilmesi işlemi ise veriler yok edilmez ve halen üçüncü kişilerin erişimine açıktır. Ancak artık söz konusu anonimleştirilen veriyi, veri sahibi ilgili kişiyle ilişkilendirme imkânı bulunmamaktadır. Anonimleştirme işlemi veriyi ortadan kaldırmadığı için işlem sonrasında bile halen kişi ile bağdaştırılabilme olanağı dolayısıyla doktrinde bazı yazarlar tarafından eleştirilmektedir²⁴⁹.

Kişisel verilerin hangi durumlarda işbu maddeye göre silinip, yok edileceği veya anonim hale getirileceği hususu da önem taşımaktadır. İşleme faaliyetinin kanunun öngördüğü bir durumda yapıldığı zaman, söz konusu kanun hükmü mülga olduğunda veri sorumlularının mülga olan kanun hükmü uyarınca toplayıp işledikleri kişisel verileri imha etmeleri gerekecektir. Yine, kişisel verilerin veri sorumluları tarafından bir saklanma süresi mevcutsa, o süre bitiminde artık verilerin muhafazası hukuka aykırı olacağından imha edilmeleri gerekecektir. Bununla birlikte, herhangi bir kanuna aykırı işleme faaliyetinde söz konusu hükmün evleviyetle uygulanması gerekecektir²⁵⁰. Örneğin, veri sorumlusu tarafından toplanan ve işlenen ilgili kişi veri sahibine ait verilerin toplanma amacı dışında bir amaç için kullanılması durumunda KVKK m. 4 uyarınca düzenlenen amaçla sınırlı olma ilkesi ihlal edildiğinden hukuka aykırı olarak elde edilen kişisel verinin ilgili kişinin talebi üzerine silinmesi veya anonim hale getirilmesi gerekmektedir.

Kanun, ilgili maddenin 3. bendinde kişisel verilerin silinmeleri, yok edilmeleri veya anonim hale getirilmelerine ilişkin usul ve esasların yönetmelikle düzenlendiğini belirtmiştir. Bu doğrultuda veri sorumlularının kişisel verileri imha ederken Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında

²⁴⁸ Gözüm, Z. U. (2019). *Kişisel Verilerin Korunmasının İş İlişkisi Açısından Değerlendirilmesi*. Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, s. 55.

²⁴⁹ Avcı, Y., (2019), s. 80.

²⁵⁰ Avcı, Y., (2019), s. 80.

Yönetmelik²⁵¹ (KVSİYAY) hükümleri uygulanacaktır. Yönetmelik'in 5. maddesi uyarınca veri sorumlularına saklama ve imha politikası düzenleme zorunluluğu getirilmiş olup, Kişisel Verileri Koruma Kurumu tarafından 10.03.2019 tarihinde rehber amaçlı “*Kişisel Veri Saklama ve İmha Politikası*” yayımlanmıştır. Ek olarak, Yönetmelik'in 8., 9. ve 10. maddelerinde kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesi işlemlerinde veri sorumlularının izlemesi gereken süreç ve adımlardan bahsedilmiş olup, veri sorumluların aynı zamanda kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesi aşamalarında gereken her türlü tedbiri almalarına ilişkin yükümlülüğüne vurgu yapılmıştır.²⁵² Bu halde, veri sorumlularının veriyi silme, yok etme, anonim hale getirme işlemlerinden sonra da veriye erişimin yapılıp yapılmadığını, verinin tamamen kaldırılıp kaldırılmadığını veya veriyi halen veri sahibiyile ilişkilendirmenin mümkün olup olmadığını ya da halen veri sahibiyile ilişkilendirilip ilişkilendirilmediğini denetlemesi gerekmektedir. Aksi halde yapılan işlem geçersiz olacaktır. Re'sen yapılacak silme ve yoketme işlemleri KVSİYAY'ın 11. maddesi uyarınca veri sorumlusu tarafından hazırlanmış saklama ve imha politikasında belirlenen periyodik imha süreleri sonunda yapılacaktır. İşbu imha süreleri verinin işleme amacının ortadan kalkması durumunda başlayıp, her türlü halde 6 aydan uzun olamaz²⁵³.

İlgili kişinin talebi ile silinme veya yok etme işleminin yapılması Yönetmelik'in 12. maddesinde düzenlenmiştir. Buna göre, talebin yapıldığı süreyi izleyen 30 gün içerisinde ilgili kişi veri sahibine veri sorumlusu tarafından red veya kabul dönüşü yapılmalıdır. Ayrıca, eğer kişisel veriler üçüncü kişilere aktarılmışsa işbu üçüncü kişiler de talep hakkında ve talep sonucu verilecek karara göre yapılması gereken işlem bilgilendirilmelidir. Talebin kabulü halinde veri sorumlusu tarafından üçüncü kişilerin de kişisel verileri imha etmesi sağlanmalıdır²⁵⁴.

Kanun'un işbu hükmü ile Tüzük'te düzenlenen “*unutulma hakkı*”nın amaçları ve işleyişleri bakımından benzer nitelikte olduğu söyleyebiliriz. Zira, tıpkı KVSİYAY'de açıklandığı üzere; unutulma hakkı da ilgili kişilerin talebi üzerine

²⁵¹ Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik, *T.C. Resmi Gazete*, Sayı: 30224, 28 Ekim 2017 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

²⁵² Özkan, O., (2020), s. 157.

²⁵³ Özkan, O., (2020), s. 157.

²⁵⁴ Özkan, O., (2020), s. 158.; Avcı, Y., (2019), s. 81.

verilerinin bir daha hiç kimse tarafından erişilemeyecek hale getirilmesi olarak tanımlanmaktadır.²⁵⁵

4.8 Üçüncü Kişilere Veri Aktarımı

Kişisel verilerin üçüncü kişilere aktarımı KVKK'nın 8. ve 9. maddelerinde düzenlenmiştir. KVKK'nın tanımlar başlıklı 3. maddesinde veri aktarımı faaliyetinin işleme faaliyeti kapsamı altında olduğu görülmektedir. Buna rağmen kanunda verilerin aktarılması ayrıca düzenlenmiştir²⁵⁶ ve tıpkı işleme hususunda olduğu gibi verilerin aktarılması da kural olarak yasaklanmıştır. Veri aktarımı konusunda Kanun'da yurtiçinde veya yurtdışına aktarım ve genel nitelikli verilerin aktarımı veya özel nitelikli verilerin aktarımı şeklinde 2 önemli ayırım bulunmaktadır.

Yurtiçinde veri aktarımının yapılması 8. madde uyarınca açık rıza şartına bağlanmıştır. Açık rızanın bulunmadığı veya gerekmediği hallerde ise özel ve genel nitelikli veri ayırımına gidilmiştir. Buna göre, aktarılacak veri genel nitelikte veriyse, KVKK'nın 5. maddesinin 2. fıkrasında düzenlenen verilerin açık rıza aranmaksızın işlenebileceği hallerin varlığında, genel nitelikli veri aktarımı da açık rıza aranmaksızın yapılabilmektedir²⁵⁷. Aynı şekilde, aktarılacak veri genel nitelikte veriyse, KVKK'nın 6. maddesinin 3. fıkrasında verilerin açık rıza aranmaksızın işlenebileceği hallerin varlığında, özel nitelikli veri aktarımı da açık rıza aranmaksızın yapılabilecektir. Ancak özel nitelikli verilerin aktarımında ek olarak yeterli önlemlerin alınması şartı da aranmıştır. İşbu yeterli önlemler, KVKK'nın 6. maddesinin 4. fıkrası uyarınca Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarihli Resmî Gazete'de 2018/10 sayılı karar ile yayımladığı "*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*"dir²⁵⁸.

Kişisel verilerin yurtdışına aktarılması da kural olarak yurt içine aktarılması ile aynı prensiplere sahiptir. Esasen açık rıza aranmakta ise de, bir önceki maddede bahsedilen özel ve genel nitelikli verilerin kanunen açık rıza aranmaksızın işlenebileceği hallerin varlığında açık rızaya gerek olmaksızın aktarımı yapılabilmektedir. Bu düzenlemede farklı olarak yeterli koruma kavramına

²⁵⁵ Zewki, H. S. S. (2021). *Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, Gaziantep Üniversitesi, s. 77.

²⁵⁶ Avcı, Y., (2019), s. 76.

²⁵⁷ Özkan, O., (2020), s. 159.

²⁵⁸ Avcı, Y., (2019), s. 77.

değiniştir. Eđer aktarım yapılacak ÷lkede yeterli koruma mevcutsa, özel ve genel nitelikli verilerin kanunen açık rıza aranmaksızın işlenebileceđi hallerin varlığında açık rızaya gerek olmaksızın aktarım yapılabilmektedir. Eđer söz konusu ÷lke yeterli korumayı sağlayamayan bir ÷lke ise, Türkiye'deki aktarımın yapan ve üçüncü ÷lkedeki aktarım yapılan veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurul'un işbu aktarım faaliyetine izin vermesi halinde aktarım gerçekleşebilmektedir²⁵⁹.

Yeterli koruma hususu, Kanun'un yürürlüğe girdiđi tarihten beri muallakta kalan bir konudur. Zira Kanun tarafından veri aktarımı yapılması güvenli ÷lkeler halen ilan edilmemiştir. Haliyle yeterli koruma sağlayan ÷lkelerin tespitinin, ilgili maddenin 4. fıkrasında düzenlenen şartların incelenmesiyle yapılması zorunluluđu vuku bulmuştur. Madde uyarınca yeterli korumanın tespiti için incelenmesi gereken hususlar şu şekilde belirtilmiştir; (1) Türkiye'nin taraf olduđu uluslararası sözleşmeler, (2) veri aktarılan ÷lke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumu, (3) aktarılan kişisel verilerin her birinin niteliđi ile, işleme amacı ve süresi, (4) veri aktarılan ÷lkenin mevzuatı ve uygulaması, (5) veri aktarılan ÷lkedeki veri sorumlusu tarafından taahhüt edilen önlemler²⁶⁰. İşbu hususlar akabinde Kurul'un 02/05/2019 tarihli ve 2019/125 sayılı kararı ile genişletilerek, Kişisel Verileri Koruma Kurumu sitesinde yayımlanmıştır²⁶¹.

Yurt dışına veri aktarımı konusunu bir örnekle izah etmek gerekirse; Türkiye'de bulunan bir hastanenin Amerika'da bulunan bir hastaneye veri aktarımı yapılabilmesi için öncelikle açık rızanın aranmadıđı hususlar incelenmelidir. Zira verinin açık rıza aranmaksızın işlenebilmesi mümkünken veri sahibi ilgili kişinin açık rızasının alınması dürüstlük kuralına aykırılık teşkil etmektedir²⁶². Söz konusu aktarım yurtdışına yapıldıđından ve sağlık verilerinin özel nitelikli veri kapsamında olmasından dolayı, uygulanması gereken hüküm KVKK'nın 9. maddesinin 2. bendidir. Bu noktada, söz konusu sağlık verilerinin işlenmesinin açık rızaya

²⁵⁹ Toprak, B., (2018), s. 81.

²⁶⁰ Tolun, Y., (2020), s. 50.

²⁶¹ Kişisel Verileri Koruma Kurumu. (2019). "*Yeterli Korumanın Bulunduđu Ülkelerin Tayininde Kullanılmak Üzere Oluşturulan Form*" Hakkındaki 02/05/2019 Tarihli Ve 2019/125 Sayılı Kurul Kararı [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkındaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari> (Erişim Tarihi: 13.12.2021).

²⁶² Bkz. s. 71.

dayanmaksızın yapılabileceği hallerin incelemesinin yapılması gerekmektedir. Hastaneler tıbbi teşhis ve tedavi amacıyla veri işlediğinden ve veri işleyen sır saklama yükümlülüğü altında bulunan doktorlar istihdam ettiklerinden KVKK m. 6/3 kapsamında açık rızaya gerek olmaksızın ilgili kişilerin verilerini işleyebilmektedir. Bu tespitten sonra, KVKK'nın ilgili 9. maddesine tekrar dönülüp, Amerika'nın aktarılan veriler açısından yeterli koruma sağlayıp sağlamadığı hususunun değerlendirilmesi yapılmalıdır. Her ne kadar ilgili maddenin 3. fıkrasında Kurul'un yeterli korumayı yapan ülkeleri ilan edeceği düzenlenmişse de, ilanın uzun ve yoğun bir süreç sonrası sonuçlandırılabilmesi gerekçesiyle bu tarihe kadar hiçbir ülke güvenli ülke statüsü altında bildirilmemiştir²⁶³. O zaman KVKK'nın 9. maddesinin 4. fıkrasında belirtilen kriterler değerlendirilerek Amerika'nın yeterli korumayı sağlayıp sağlayamadığı anlaşılmalıdır. Yeterli korumayı sağlayamadığının anlaşılması durumunda hem Türkiye'deki hem de Amerika'daki hastanenin yeterli korumayı sağladığına ilişkin yazılı taahhütlerini Kurul'a sunmaları ve Kurul'dan izin almaları gerekecektir. Ancak, zaten yeterli koruma sağladıklarına ilişkin taahhünamelerinin kriterleri ile Kurul'un izin verilmesi için inceleyeceği kriterler aynı olduğu için yeterli koruma sağlayamayan bir ülkenin hastanesinin Kurul'dan izin alabilmesi mümkün gözükmemektedir. Bu durumda ise son çare, ilgili kişi veri sahibinin açık rızasının alınması olacaktır. Görüldüğü üzere, yurt dışına veri aktarımı, çok faktörlü kimlik doğrulaması misali kademeler oluşan bir koruma sağlamaktadır.

4.9 Veri Sorumlusunun Yükümlülükleri

4.9.1 Veri Sorumlusunun Aydınlatma Yükümlülüğü

Kanun'un veri sorumlularına yüklediği en önemli yükümlülüklerden biri aydınlatma yükümlülüğüdür. Bu yükümlülüğün kapsamı maddede, veri sorumlusunun veya temsilcisinin kimliği, verilerin hangi amaçlarla işleneceği, kimlere ve hangi amaçlarla aktarılabilmesi, verilerin toplanma yöntemi ve hukuki sebebi ve ilgili kişi veri sahibinin 11. maddede düzenlenen haklarıdır. Bilgilendirme hakkı doktrinde “*a priori*” nitelikte hak olarak yorumlanmaktadır. Bu tanım olarak dogma anlamı taşıyan bir hak olup, veri işlemenin hukuka uygunluk sebebi olan açık rızanın şartlarında

²⁶³ Kişisel Verileri Koruma Kurumu. (2020). *Yurtdışına Veri Aktarımı Kamuoyu Duyurusu* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/6828/YURTDISINA-VERI-AKTARIMI-KAMUOYU-DUYURUSU> (Erişim Tarihi: 13.12.2021).

halihazırda açık rızanın unsurlarından olan ilgili kişinin doğru biçimde bilgilendirilmiş olması hususunun yanında, açık rıza aranmayan hukuka uygunluk sebepleri halinde de aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir²⁶⁴. Bu özelliği ile ilgili kişinin talebi ya da başvurusu şartına bağlı değildir. Her türlü durumda veri sorumlusu tarafından re'sen gerçekleştirilmesi gerekmektedir²⁶⁵.

Veri sorumlusunun yükümlülüğünü yerine getirdiğine ve veri sahibinin bilgilendirildiğine ilişkin ispat yükü veri sorumlusuna aittir²⁶⁶. İşbu bilgilendirme her faaliyete ayrı ayrı uygulanmalı ve belirli aralıklarla tekrarlanmalıdır. Yoksa aydınlatma yükümlülüğü ile amaçlanan sonuca ulaşamaz²⁶⁷.

Verilerin üçüncü bir kişiden elde edilmesi halinde de veri sorumlusunun bilgilendirme yükümlülüğünü yerine getirmesi gerekmektedir. İşbu husus esasen Direktif'in 11. maddesinde düzenlenmiş olup²⁶⁸, çerçeve Direktif'in KVKK'nın yaratılışında örnek alındığı düşünüldüğünde uygulamada da bu şekilde yapılması gerekecektir. Bu doğrultuda üçüncü kişiden alınan verilerin kaydedildiği anda ya da söz konusu verilerin üçüncü kişilere aktarılmasından önce bu faaliyet hakkında veri sorumlusunun aydınlatma yükümlülüğü mevcuttur²⁶⁹. Aydınlatma yükümlülüğüne ilişkin esas ve usuller "*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*" de düzenlenmektedir²⁷⁰.

4.9.2 Veri Güvenliğine İlişkin Yükümlülükler

Kanun'un 12. maddesi veri sorumluluklarına veri güvenliğinin sağlanabilmesi için birtakım yükümlülükler yüklenmesi gerektiğini öngörmüştür. Veri güvenliği ilkesi, çalışmamızın "*OECD Rehber İlkeleri*" başlıklı kısmında da bahsettiğimiz üzere 1980 yılından beri veri koruma hukukunun temel ilkelerindedir ve verileri, silinme, yok edilme, açığa çıkarılma gibi istenmeyen unsurlara karşı korunmasını amaçlamaktadır²⁷¹.

²⁶⁴ Elbir, N., (2020), s. 97.

²⁶⁵ Gürsel, İ., (2016), s. 261.

²⁶⁶ Tolun, Y., (2020), s. 86.

²⁶⁷ Gözümlü, Z. U., (2019), s. 101.

²⁶⁸ Gürsel, İ., (2016), s. 262.

²⁶⁹ Toprak, B., (2018), s. 77.; Gürsel, İ., (2016), s. 263.

²⁷⁰ Özkan, O., (2020), s. 167.

²⁷¹ Bkz. s. 29.

Maddeye göre veri sorumlularına her türlü idari ve teknik tedbirleri alması yükümlülüğü, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ve kişisel verilerin muhafaza ederek korumak amaçlarıyla getirilmiştir.²⁷² Bu hükmün lafzındaki idari tedbirler, veri sorumlusunun organizasyonu nezdinde risk ve tehlikelerin saptanması, veri güvenliğine ilişkin bir politika hazırlanıp uygulanması, çalışanlara bu konuya ilişkin eğitimlerin verilmesi ve veri güvenliğinin periyodik olarak denetiminin yapılmasını ifade etmektedir. Teknik tedbirler ise daha çok siber güvenliğe ilişkin olup, bu tedbirlere örnek olarak elektronik ortamda virüs koruma programlarının çalıştırılması, kullanılan bilgisayarlarda çok faktörlü kimlik doğrulaması uygulanması; fiziki ortamda ise veri sorumlusunun verileri tuttuğu yerlere erişimde kontrol uygulanması gösterilebilir²⁷³. Veri işleyenlerin veri sorumlularını işleme faaliyeti ve söz konusu verilerin gizliliğinden sorumlu oldukları konusunda bilgilendirmeleri, gizliliğin ihlali halinin yaptırıma bağlanması da tedbirler arasında gösterilmiştir²⁷⁴.

Maddenin ikinci fıkrasında veri sorumlusu ve veri işleyenin farklı kişiler olması durumunda her ikisinin de müştereken ve müteselsilen sorumlu olduğu düzenlenmiştir²⁷⁵. Bu hükümlerle beraber, veri işleyen ve veri sorumlusu kişilerin de birbirlerini denetlemesi amaçlanmıştır. Zira, birisi tarafından yapılan veri güvenliği ihlali, diğeri için de sonuç doğuracaktır.

Üçüncü fıkrada veri sorumlusunun denetim yükümlülüğünden bahsedilmiştir. Buna göre, veri sorumlusunun birinci fıkra uyarınca idari ve teknik tedbirler alması veri güvenliğinin sağlanması açısından yeterli olmayacaktır. Aynı zamanda bu tedbirlerin uygulandığından emin olunması gerekmektedir. Denetim yükümlülüğü kapsamında denetlenecek hususlar KVKK m. 4 uyarınca temel ilkeler, KVKK m. 5 uyarınca verilerin işleme şartları, kanun kapsamında veri sorumlusuna yüklenen yükümlülükler ve kanunun öngördüğü diğer şartlardır. Veri sorumlusu denetleme işini kendi organizasyonu dışında üçüncü bir gerçek veya tüzel kişiye devredebilir. Bu durum sorumluluğun da devredileceği anlamına gelmemekle beraber, bir önceki

²⁷² Tolun, Y., (2020), s. 76.

²⁷³ Özkan, O., (2020), s. 173-174.

²⁷⁴ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 409.

²⁷⁵ Avcı, Y., (2019), s. 89.

fıkra da belirlenen müşterek ve müteselsil sorumluluk, veri denetleyen ve veri sorumlusu arasında da geçerlidir²⁷⁶.

Dördüncü fıkra sır saklama yükümlülüğü adı altında, veri sorumluların ilgili kişi veri sahiplerine ait kişisel verileri kanuna aykırı olarak paylaşması ve verilerin işleme amacı dışında kullanılması yasaklanmıştır²⁷⁷. Bu hükümde, 8. ve 9. maddelerde düzenlenen veri aktarma yasağının ve 4. maddede düzenlenen amaçla bağlantılı olma ilkesinin ihlali halinde veri sorumlularının sır saklama yükümlülüklerini yerine getiremeyeceklerinden bahsedilmiştir. Fıkra da bahsedilen durumların zaten kanuna aykırılık teşkil edeceği önceki maddelerde düzenlenmiş olsa da, veri sorumluluğunun veri güvenliğini sağlama yükümlülüğü altında tekrar edilmiştir. Bu yükümlülük de hem veri sorumlusu hem de veri işleyen açısından geçerlidir.

Tıpkı çoğu sözleşmenin “*confidentiality clause (gizlilik klozu)*” kısımlarında öngörüldüğü gibi, Kanun veri sorumlularının veri sorumlusu görevlerinden ayrılmaları halinde bile işbu sır saklama yükümlülüğü altında olduklarını belirtmiştir²⁷⁸. Nitekim, bu husus da kanunun diğer hükümlerinden çıkarılabilmektedir. Veri sorumlusu olarak görevi biten gerçek veya tüzel kişi tarafından toplanan kişisel verilerin toplanma amaçları bitmiş olduğundan, akabinde işbu verilerin söz konusu eski veri sorumlusu tarafından saklanması, aktarılması veya genel anlamda işlenmesi yine temel ilkelere aykırılık teşkil edecektir.

Sır saklama yükümlülüğü diğer kanunlarda da öngörülmüştür. İş Kanunu’nun 75. maddesi uyarınca işçilere ait özlük dosyası hazırlama ve saklama yükümlülüğü bulunan işverenlerin, hükmün devamı uyarınca çalışanın gizli kalmasını istediği ve buna hakkı bulunan bilgileri açıklamayacağı düzenlenmiştir. Bu hüküm KVKK ile birlikte yorumlandığında; işverenlerin, işçilerine ait gizli bilgileri işçilerin işten ayrılmasından sonra da ifşa edemeyeceği sonucuna ulaşılmaktadır²⁷⁹.

Beşinci ve son fıkra, veri güvenliği ilkesinin ihlali halinde veri sorumlusu tarafından yapılması gerekenlerden bahsetmektedir. Bu durumda, kanuna aykırı yollarla üçüncü kişiler tarafından verinin elde edildiği bilgisinin en kısa zamanda Kişisel Verileri Koruma Kurulu’na ve ilgili kişi veri sahibine verilmesi gerekmektedir.

²⁷⁶ Avcı, Y., (2019), s. 90.

²⁷⁷ Durun, Y., (2019), s. 55.

²⁷⁸ Özkan, O., (2020), s. 177.

²⁷⁹ Yardımcı, A., (2019), s. 65-66.

Bu yükümlülükle amaçlanan, ilgili kişiye ait verilerin üçüncü kişilere sızması sonucu oluşacak zararın erken müdahale ile en aza indirgenmesidir²⁸⁰. En kısa süre ibaresi Kurul tarafından “72 saate kadar” olarak yorumlanmıştır²⁸¹. 12. maddenin 5. fıkrasında bahsedilen üçüncü kişilerin verileri kanuna aykırı yollarla elde etmesi, Tüzük uyarınca verilerin, imha edilmesini, yok edilmesini ve silinmesini de kapsadığından, bu işlemlerin de mevzuatımız uyarınca üçüncü kişilerin verilere hukuka aykırı erişimi olarak nitelendirilmesi ve öyle yorumlanması gerekmektedir. Önemli olan bir diğer husus da veri sorumlusunun kusurunun işbu yükümlülüğe bir etkisinin olmadığıdır. Bundan anlaşılması gereken şudur: Şayet, veri sorumlusu kişisel verilerin üçüncü şahıslarca kanuna aykırı yollar vasıtasıyla ele geçirildiği durumda gereken ve mümkün olan tüm idari ve teknik tedbirleri aldığından bahisle hiçbir kusurunun olmadığı ispatlansa dahi; veri sorumlusu böyle bir ihlal durumunda, kusur durumuna bakılmaksızın Kurul’a bildirimde bulunmakla yükümlüdür.²⁸²

4.9.3 Veri Sorumluları Sicili’ne Kayıt Yükümlülüğü

Veri Sorumluları Sicili, kamuya açık nitelikte, KVKK’nın 16. maddesi uyarınca veri sorumlularının kişisel verileri işlemeye başlamadan önce kaydolma yükümlülüklerinin bulunduğu bir sicildir. Kamuya açık olması vasfını taşıdığından, şeffaflık, hesap verilebilirlik ve veri işleme faaliyetinin açık olması ilkelerini sağladığı söyleyebiliriz. Çünkü, ilgili kişi veri sahipleri Veri Sorumluları Sicili’nin internet sitesi olan Veri Sorumluları Sicili Bilgi Sistemi’ne (VERBİS) erişerek veri sorumluları hakkında bilgi sahibi olabilmektedir²⁸³.

Sicil’e kayıt zorunluluğuna ikinci fıkrayla bir istisna getirilmiştir. 15 Mayıs 2018 tarihli Resmî Gazete’de yayınlanan 08.04.2018 tarihli ve 2018/32 Karar numaralı Kurul Kararı uyarınca; noterlerin, avukatların, siyasi partilerin, serbest muhasebeci mali müşavirler ile yeminli mali müşavirlerin ve dernekler, vakıflar ve sendikalardan ilgili mevzuata uygun olarak, kendi faaliyet alanlarıyla sınırlı ve sadece kendi mensuplarına ilişkin verileri işleyenlerin Veri Sorumluları Sicili’ne kayıt olma

²⁸⁰ Tolun, Y., (2020), s. 77.

²⁸¹ Kişisel Verileri Koruma Kurumu. (2019). *Kişisel Veri İhlali Bildirim Usul Ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararına İlişkin Duyuru* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi> (Erişim Tarihi: 14.12.2021).

²⁸² Avcı, Y., (2019), s. 92.

²⁸³ Özkan, O., (2020), s. 180.

yükümlülüğü bulunmamaktadır²⁸⁴. Kurul'un bu şekilde bir istisna belirleme yetkisinin olması sadece bu yükümlülüğe ilişkin olup, Kurul'un diğer yükümlülüklerle de istisna getirmesi mümkün değildir²⁸⁵.

Maddenin üçüncü fıkrası Sicil'e kayıt için gerekli bilgileri düzenlemektedir. Kayıt, VERBİS üzerinden gerçekleştirilmekte olup, veri sorumlusunun yerleşim yerine göre Sicil'e vermesi gereken bilgiler değişiklik göstermektedir. Buna göre, veri sorumlusunun yerleşim adresi yurt içinde ise, gerçek kişiler bizzat, tüzel kişiler ise organları vasıtasıyla başvuruda bulunabilirler. Yerleşim yeri yurt dışında bulunan bir gerçek veya tüzel kişi veri sorumlusunun VERBİS sistemine kayıt yapabilmesi için bir veri sorumlusu temsilcisi ataması ve bunu sicile bildirmesi gerekmektedir. Buna ek olarak, her veri sorumlusunun bir irtibat kişisi belirlemesi ve bildirmesi gerektiği de düzenlenmiştir. İşbu irtibat kişinin veri sorumlusunun temsilcisi gibi bir sorumluluğu bulunmayıp yalnızca ilgili kişiler ile veri sorumlusu arasındaki bir araç görevi üstlenmektedir²⁸⁶.

4.9.4 Kişisel Veri Envanteri

Veri Sorumluları Sicili Hakkında Yönetmelik²⁸⁷ ile getirilen veri envanteri hazırlama yükümlülüğü, Veri Sorumluları Sicili'ne kaydolma yükümlülüğü bulunan veri sorumlularına yükletilmiştir. KVKK ile veri koruma hukukuna getirilen yeni bir kavram olan "*kişisel veri envanteri*", veri sorumlularının veri işleme faaliyetlerini, işleme amacı ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri içermelidir. Kurum, bu yükümlülüğün getirilme amacının veri sorumlularına kendilerini denetleme imkânı tanınması olarak açıklamaktadır. Zira kişisel veri envanteri hazırlanarak yukarıda bahsedilen hususlar kontrol edilip envantere yazıldığından, veri sorumlusu tarafından

²⁸⁴ Kişisel Verileri Koruma Kurumu. (2018). *Kişisel Verilerin Korunması Kurulu'nun 08.04.2018 Tarihli ve 2018/32 Karar Numaralı Kararı* [Çevrimiçi]. Erişim adresi: <https://www.resmigazete.gov.tr/eskiler/2018/05/20180515-16.pdf> (Erişim Tarihi: 15.12.2021).; Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 409.

²⁸⁵ Özkan, O., (2020), s. 184.

²⁸⁶ Avcı, Y., (2019), s. 94-95.

²⁸⁷ Veri Sorumluları Sicili Hakkında Yönetmelik, *T.C. Resmi Gazete*, Sayı: 30286, 30 Aralık 2017 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

yapılan yanlışlıkların veya ihlallerin tespit edilmesi ve kaldırılması imkânı bulunmaktadır. Böylece hem veri sahibi ilgili kişilerin kişisel verilerin korunması hakkı koruma altına alınmakta, hem de veri sorumlularına yaptıkları ihlalleri kendileri tespit edip yaptırımlara maruz kalmama şansı verilmektedir. Aynı zamanda böyle bir düzen ile, veri sorumlusuna yapılan başvurular ve sorular kolaylıkla cevaplanabilecektir²⁸⁸.

4.10 İlgili Kişinin Hakları

Kanun'un 11. maddesiyle ilgili kişinin veri sorumlusu nezdinde bulunan verileri üzerindeki hakları düzenlenmiştir. Bu haklar 4 kategori şeklinde ayrılabilir. Bu kategoriler, (1) ilgili kişilerin verilerinin işlenmesi hakkında bilgi edinmesi, (2) verilerinin silinmesi, yok edilmesi veya düzeltilmesini talep etmesi, (3) verilerinin kendi aleyhine bir sonuç doğurması durumunda sonuca itiraz etmesi ve (4) işleme faaliyet doğan zararlarının giderilmesini talep etmesi şeklindedir.

Bilgi edinme hakkı, tıpkı veri sorumlusunun re'sen bilgilendirme yükümlülüğü gibi, ilgili kişilere tanınmış bir haktır. Belirli, açık ve meşru amaç ilkesi ile de bağlantılıdır. Bu hak sayesinde ilgili kişi, veri sorumlusunda bulunan verilerinin ne olduğuna, hangi amaçla işlendiklerine, ne gibi faaliyetlerde kullanıldıklarına, başka kimlerin verilere erişiminin olduğuna ve benzeri hususlara ilişkin bilgi talep edebilmektedir²⁸⁹. İlgili kişinin bilgi edinme hakkının kullanılabilmesi için veri sorumlusunun temel ilkelere de riayet ederek, karmaşık ve belirsiz açıklamalardan uzak bir biçimde ilgili kişiye bilgi vermesi gerekmektedir. Bilgi edinme istemi, yalnızca ilgili kişi veri sahibi tarafından "*kendi verilerine*" ilişkindir. Bu doğrultuda kişiler, ölen yakınları hakkında veri sorumlularına bu hak kapsamında bir bilgi edinme talebinde bulunamazlar²⁹⁰.

İlgili kişi veri sahibine tanınmış bir diğer hak ise verilerinin silinmesini, yok edilmesini ve düzeltilmesini talep edebilme hakkıdır. İşbu hakkın kanuni dayanağı KVKK'nın 7. maddesi olup, çalışmamızın önceki bölümünde açıklanmıştır²⁹¹.

²⁸⁸ Özkan, O., (2020), s. 186-187.

²⁸⁹ Tolun, Y., (2020), s. 75.

²⁹⁰ Özkan, O., (2020), s. 190.

²⁹¹ Bkz. s. 77-79.

Verilerin otomatik yollarla işlenmesi durumunda ilgili kişilerin aleyhine sonuçlar çıkabilmektedir. Bu durumlara örnek olarak işçilerin işyerinde yapılan performans değerlendirmelerinin verileri otomatik ortamda işlemeleri verilebilir. Böyle durumlarda veri sahibi kişilere verilerinin analizinin sonucuna itiraz etme hakkı tanınmıştır. Bu hakkın kullanılabilmesi için işçinin mevcut durumunda daha aleyhe bir konum ya da duruma geçirilmiş olması gerekmektedir. Aynı zamanda itiraz edilecek analizi yapılan verilerin yapılan sonuçla ilintili olması gerekir. Yaptığı işin miktarının az olması sebebiyle işten çıkarılan bir işçinin, işin kalitesine ilişkin veriye itiraz etme hakkı bulunmayacaktır. Çünkü işten çıkarılmasının sebebi işin niteliğine ilişkin değil, niceliğine ilişkin verilerdir.²⁹² Direktif'te işbu husus kişilerin otomatikleşmiş veri işleminin sonuçlarına tabi olmama hakkı olarak düzenlenmiş ve kişilere insani müdahale olmayan kararlara tabi olmama imkânı tanınmıştır.²⁹³

Son olarak, ilgili kişilere kişisel verilerinin korunması hakkının ihlali dolayısıyla oluşan zararlarının giderilmesini talep etme hakkı tanınmaktadır. İşbu zarar maddi ve manevi olabilmektedir. Zira kişisel verilerin kişilik hakkı niteliğinde olduğunun kabulü ile kişinin kişi kişilik hakkının ihlali dolayısıyla manevi tazminat talep hakkına sahip olacaktır. İlgili kişi bu talebini çeşitli yollarla gerçekleştirebilmektedir. Zarar giderilmesi talebi doğrudan zararın kaynaklandığı veri sorumlusuna yapılabileceği gibi, 14. maddenin birinci fıkrasına göre şikâyet adı altında Kurul'a başvuru yoluyla ya da üçüncü fıkra uyarınca yargı yoluna başvurularla işbu talep ileri sürülebilmektedir.²⁹⁴ Bu noktada önemli olan husus, veri sorumlusuna yapılan başvurunun zorunlu, Kurul'a yapılan şikâyetin ise ihtiyari oluşudur. Bu durum, veri sahibinin Kurul'a şikâyet yoluna başvurabilmesi için öncelikle veri sorumlusuna başvuru yolunu tüketmesini gerektirirken, veri sahibinin adli yoldan hak arama olanağına hanel getirmemektedir. Bir diğer deyişle, konunun yargı makamları önüne getirilmesinden önce Kurul'a şikâyet veya veri sorumlusu'na başvuru yolunun tüketilmiş olması şartı aranmamaktadır²⁹⁵. Zararın tazmininin talep edilebilmesi zararı oluşturan fiilin kanuna aykırı olması halinde söz konusu olacaktır. Zaten işbu hakkın

²⁹² Avcı, Y., (2019), s. 84.

²⁹³ Toprak, B., (2018), s. 80.

²⁹⁴ Özkan, O., (2020), s. 194.

²⁹⁵ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraça, E., (2021), s. 411.

ana kaynađı TBK m. 49 olduđundan, ilgili hkm uyarınca hukuka aykırı bir fiil gerekli unsurlardan biri olarak sayılmıřtır.



BÖLÜM 5: İŞÇİLERİN KİŞİSEL VERİLERİNİN KORUNMASI

İşverenlerin işçilere ait verileri işlemesi, birçok kanuni düzenleme tarafından bir yükümlülük olarak düzenlenmektedir. Bu yükümlülükler, KVKK'nın 5. maddesi uyarınca kişisel verilerin işlenmesi için hukuka uygunluk sebebi olan işlemenin kanun ile öngörülmesi durumunu oluşturmaktadır. Aynı şekilde Anayasa'nın özel hayatın gizliliği başlıklı 20. maddesinde kişisel verilerin kanunun öngördüğü durumlarda işlenebileceği düzenlenmiştir. Bir diğer kanunda öngörülme hali, Türk Medeni Kanunu'nun 24. maddesinin ikinci fıkrası uyarınca kanunun öngördüğü durumlarda kişilik haklarına müdahalede bulunulabilmesine ilişkin düzenlemedir. İşverenlerin İş Kanunu m. 75 uyarınca işyeri özlük dosyası hazırlamasına ilişkin yükümlülük de kişisel verilerin kanunun verdiği yetkiyle işlenmesi durumlarından biridir. Bu tür yasal yükümlülüklerle kişisel verilerin işlenmesinin toplum yararı ve kamu düzeni amaçlarını taşıdığı söylenebilir²⁹⁶.

Bununla birlikte, KVKK m. 5'te düzenlenen sözleşmeden doğan işleme zorunluluğu, veri sahibi olan işçinin haklarının korunması amacıyla işleme zorunluluğu, veri sorumlusu sıfatında bulunan işverenin üstün yararı dolayısıyla verilerin işlenmesi ve veri sahibi işçinin açık rıza rızasının bulunması gibi diğer hukuka uygunluk sebepleri de mevcuttur. Dolayısıyla işçilerin kişisel verilerin her zaman işverenler tarafından işleme faaliyetine konu olmaktadır.

İşçi ve işveren arasındaki ikili ilişkide, işveren güçlü olan ve işçi zayıf olan taraf olarak nitelendirilmektedir. Bu nedenle İş Kanunu'ndaki çoğu hüküm “nispi emredici” hükümlerdir. Bu hükümler işçiler açısından asgari haklar sağlayıp, hükümlerin emrettiği hususlar işçi lehine değiştirilebilmektedir. Bu doğrultuda iş hukukunun işçi lehine yorum ilkesinden söz edilebilir. Ancak işçi lehine yorum ilkesi mutlak bir ilke değildir. Zira işçi lehine yorum ilkesi, 1958 tarihli Yargıtay İçtihadı Birleştirme Kararında da “İş Hukukuna ait hükümlerin tefsirinde tereddüt halinde işçinin lehine olan hal şeklinin kabul edilmesi” olarak belirlenmiştir²⁹⁷. İşçilerin menfaatinin gözetildiği kadar işverenlerin menfaatlerine de hanel getirilmemelidir. Öğretide bu durum, sosyal olan ile ekonomik olan arasındaki dengenin korunması²⁹⁸

²⁹⁶ Beytar, E., (2018), s. 157.

²⁹⁷ 26.09.1958 tarihli Resmi Gazetede yayımlanan ve 27.05.1958 Tarihli Yargıtay İçtihadı Birleştirme Kararı.; Çelik, N., Caniklioğlu N., Canbolat, T. ve Özkaraca, E., (2021), s. 28.

²⁹⁸ Süzek, S., (2021), s.19.

şeklinde açıklanmıştır. Dolayısıyla terazinin bir tarafında işçinin kişilik hakları bulunurken, diğer tarafında ise işçinin işverenine sadakat borcu mevcuttur. Kişisel verilerin korunması hakkı da özünde kişilik hakkı niteliğinde temel hak ve özgürlüklerden biri olduğundan terazinin kişilik hakkı tarafında bulunmaktadır. İşçilerin işi esnasında sahip olduğu temel hak ve özgürlüklerin bir kısmını işyerinin dışında bırakarak askıya aldığı düşüncesi mevcuttur. Fakat bazı haklar, işçinin maddi ve manevi varlığının ayrılamaz bir bütünü oluşturduğundan bu durum söz konusu haklar için geçerli değildir. Örnek olarak işçinin sağlık ve vücut bütünlüğü hakkı verilebilir. Kişisel verilerin korunması hakkı da işçilerin işyeri dışında bırakamayacağı haklardan bir tanesidir. Zira temelde bütün bu haklar işçinin bir bütün olarak kişiliğinin korunmasını amaçlamaktadır.²⁹⁹ Bu noktada işçinin kişisel verilerin korunması hususunun işveren-işçi arasındaki ilişkinin temelinde bulunduğu kabulü gerekmektedir.

5.1 Kişisel Verilerin İşlenmesinin İşverenin Gözetme Borcu İle İlişkisi

İşverenin işçiyi gözetme borcu temel olarak İş Kanunu'nda düzenlenen işverene yüklenmiş bir borç değildir. İşbu borcun kaynağı Süzek'e göre Anayasa'nın kişiler vazgeçilmez hak ve özgürlüklere sahip olduğunu düzenleyen 12., kişilerin maddi ve manevi varlıklarını koruma ve geliştirme hakkını düzenleyen 17., herkesin kişi özgürlüğü ve güvenliği hakkının bulunduğunu düzenleyen 19., özel yaşamın gizliliğini düzenleyen 20., din, vicdan, düşünce ve kanaat özgürlüklerini düzenleyen 24. ve 25. maddeleridir³⁰⁰. Gözetim borcu, doğrudan olarak Türk Borçlar Kanunu³⁰¹'nin 417. maddesinde düzenlenmekte olup, işverenlere işçinin kişiliğini korumalarını, işçiye saygı göstermelerini, işyerinde dürüstlük ilkelerine uygun bir ortam yaratmalarını, işçilerin psikolojik ve cinsel tacize maruz kalmaması ile kalanların da daha fazla zarar görmemesi için önlemler almalarını emretmektedir. Fıkranın devamında ise iş sağlığının ve güvenliğinin sağlanması amacıyla tüm önlemlerin alınmasının da işverenin işçisini gözetim borcunu dahil olduğu belirtilmiştir. İşbu gözetim borcu işçinin sadakat borcunun karşılığıdır. Bu hak dar anlamda maddede belirtilen hususları kapsarken, geniş anlamda işçiye iyi niyet ve

²⁹⁹ Elbir, N., (2020), s. 150-158.

³⁰⁰ Süzek, S., (2021), s. 414.

³⁰¹ 6098 sayılı Türk Borçlar Kanunu, *T.C. Resmi Gazete*, Sayı: 27836, 4 Şubat 2011 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

dürüstlük kuralı çerçevesinde davranmayı kapsamaktadır.³⁰² İşçinin bütün kişilik haklarının korunması amaçlandığından kişisel verilerinin korunması da bu borç kapsamında korunması gereken değerlerden biridir³⁰³.

İşverenin gözetim borcu kapsamı yalnızca dış etmenlerle sınırlı değildir. Aynı zamanda işverenin işçilerin kişilik haklarına da müdahale etmemesi gerekmektedir. Müdahale tehlikesine istinaden önlemler alınması gözetim borcunun gereklerini oluşturmaktadır.³⁰⁴

Bu noktada işçinin özel yaşamının gizliliği hakkının sınırsız olmadığını vurgulamakta fayda vardır.³⁰⁵ İşverenin gözetim borcunun işçinin sadakat borcunun bir karşılığı olduğundan bahsedilmiştir. Hatta Fransa hukukunda işverenin gözetim borcu geniş anlamda işçiye sadakat borcu olarak kullanılmakta olup, her iki tarafın da gerçek kişi olduğunu ve birbirlerine sadakat borçlarının bulunduğu kabul edilmiştir³⁰⁶. Tıpkı işverenin gözetim borcu gibi işçinin sadakat borcu da İş Kanunu'nda düzenlenmiş bir yükümlülük değildir. Türk Borçlar Kanunu'nun özen ve sadakat borcu başlıklı 396. maddesi uyarınca işçilerin, işverenlerin haklı menfaatlerinin korunması konusunda sadakatli davranma yükümlülüğü bulunmaktadır. Maddenin devamında bu yükümlülüğün hizmet ilişkisinin devamı süresince işçinin iş sırlarını kendi yararına kullanmaması ve başkasına açıklamamasını da kapsadığı düzenlenmiştir. Bu durumda işverenlerin işçilerin kişisel verilerinin korunması hakkını ihlal etmesi işverenin gözetim borcuna aykırı davranması sonucunu doğuracağı gibi, işçilerin işverenine ait kişisel verileri açığa çıkarması ya da başka türlü kullanması işçinin sadakat borcuna aykırılık teşkil edecektir.

5.2 İşçi Adaylarının İş Sözleşmesinin Kurulmasından Önce Kişisel Verilerinin Korunması

İşçilerin kişisel verileri yalnızca iş sözleşmesinin geçerli olduğu süre boyunca korunmamaktadır. İşçilerin kişisel verileri işe girerken, iş süresince ve işten ayrıldıklarından sonra işveren tarafından yapılan işleme faaliyetlerine konu olmaktadır. Dolayısıyla tıpkı işverenlerinin işçilerinin kişisel verilerini koruması gibi,

³⁰² Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 384.

³⁰³ Veliöğlu, A., (2020), s. 253.

³⁰⁴ Elbir, N., (2020), s. 168.

³⁰⁵ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 386.

³⁰⁶ Elbir, N., (2020), s. 172-173.

işverenlerin işçi adaylarının kişisel verilerini koruması gerekecektir. Bunun yanında işçinin iş sözleşmesi bittiğinde de kişisel verileri üzerindeki korumanın biteceği söylenemez. Bahsettiğimiz üzere, işverenin veri güvenliği ilkesi gereği işçisiyle arasındaki iş ilişkisinin bitmesinden sonra da işçiye ait kişisel verileri başkasına açıklayamama yükümlülüğü mevcuttur. Buna ek olarak, işverenlerin işçilere ilişkin hazırladıkları özlük dosyalarını SGK mevzuatı uyarınca 10 sene saklama yükümlülükleri bulunmaktadır. Bütün bu faaliyetler, işçi, işçi adayları ve eski işçilere ait verilerin işlenmesi niteliğinde olup, veri koruma hukuku kapsamında korumaya tabidir.

İşverenin işe alım sırasında işçi adayına ilişkin sorular sorarak veya araştırma yapmak suretiyle bilgi edinme hakkı mevcuttur. Bu hak konusunda işverenin meşru menfaatinin olduğu kabul edilir. Tabii ki, işverenin bu menfaatinden kaynaklanan bilgi edinme hakkının, işçi adayının kişisel verilerinin korunması hakkını ihlal etmeden kullanılması gerekmektedir. Bu kapsamda işe alımlarda işveren, işçiye bilgi almak için soru sorabileceği gibi; işverenin soramayacağı sorular da bulunmaktadır. Aynı şekilde, işverenin işçinin sosyal medya hesaplarına erişip onun hakkında bilgi edinmesi için hukuka uygunluk sebeplerinin bulunması gerekmektedir. İşçinin sosyal medya hesaplarını özel hayatı için mi, yoksa meslek hayatı için kullandığı ayrımı işverenin işçinin sosyal medyadaki verilerini işleyebilmesi için önem taşımaktadır. İşçilerin sosyal medya hesaplarının aleni olup olmaması sonucu değiştirmeyecektir. Ancak 29. Madde Grubu bazı hallerde işverenin hukuka uygunluk sebebi bulunmaksızın işçiye ait sosyal medyadaki alenileşmiş verileri işleyebileceğini belirtmiştir. Bu durumun yaşanabilmesi için işverenin üstün menfaatinden söz edilmelidir. Örneğin, bir çiçek mağazasında iş başvurusunda bulunan bir şahsın sosyal medyasında çiçek alerjisi olduğuna dair verilere işverence erişilip bu verilerin kullanılması durumunda işverenin üstün menfaatinden söz edebiliriz. Bu noktada işverenlerin işçi adaylarına ait sosyal medya hesaplarındaki verileri işleminin işe alım esnasında sorulacak sorular amacıyla sınırlandırılmak şartıyla hukuka uygun olduğu söylenebilir³⁰⁷.

İşverenlerin iş mülakatlarında işçilere hangi soruları sorabileceğinin sınırları doktrinde belirli değildir. Neticede işçi adayları işe alınmama korkusu içerisinde işverene karşı ekonomik olarak zayıflığı bulunan kimseler olduğundan, işçi-işveren

³⁰⁷ Velioğlu, A., (2020), s. 177-179.

arasındaki ilişkiye oldukça benzerdir. Öncelikli şunu söyleyebiliriz ki, işe alımlarda işçi adaylarına sorulan objektif ve işle alakalı olmayan soruların sorulmaması gerekmele beraber, işçilerin bu soruları cevaplama yükümlülüğü de bulunmamaktadır³⁰⁸. Fransa hukukunda da bu hususa dayanak teşkil eden bir düzenleme mevcuttur. Düzenlemeye göre işverenlerin aday işçiye cinsiyeti veya ailevi durumuyla ilgili soru sorması doğrudan veya dolaylı olması fark etmeksizin yasaklanmıştır. Bu hususta işin yapılması için cinsiyetin veya ailevi durumun gerekliliği istisna durum olarak gösterilmiştir. Bu durumda kadın iç giyime ilişkin mankenlik iş başvurusunun değerlendirilmesi konusunda işçiye cinsiyeti konusunda soru sorulması olağandır. Aynı şekilde askerlik işinde ailevi durum önem taşıdığından mülakata katılan şahsa ailesiyle ilgili sorular sorulmasının kişisel verilerinin korunmasının ihlalini teşkile edeceğini söyleyemeyiz. Zira bol miktarda seyahat gerektiren bir meslek olduğundan bu tür sorularda işçinin yararının gözetildiği de söylenebilir. Bir başka maddede işverenin işçiye sorabileceği soruların yalnızca yapılacak iş için gerekli mesleki yeterliliğe sahip olup olunmadığının tespitine yönelik olabileceği belirtilmiştir³⁰⁹.

İşverenin sormayacağı soruların bulunması gibi, işçilerin sorulan sorulara yanlış cevap vermeme yükümlülüğü bulunmaktadır. Zira İş Kanunu'nun 25/II-a maddesinde, işçinin yanlış bilgilerle işverenini yanıltması ya da işin gerektirdiği özelliklerin kendisinde bulunmamasına rağmen bulunduğunu ileri sürerek işe alınması durumlarının iş akdine işveren tarafca haklı sebeple son verilme sebebi oluşturduğu düzenlenmiştir³¹⁰. İşverenin sözleşmenin esaslı noktalarından biri hakkında yönelttiği soru karşısında işçinin “susması” da yanıltma sayılmaktadır³¹¹. Ancak, işçi adayına kişisel verilerinin korunması kapsamında sorulmaması gereken bir sorunun sorulması durumunda işçi adayının bu soruyu yanlış cevaplama, ileride işçi adayı işe alındığında işverene iş akdinin haklı nedenle feshi hakkını vermeyecektir. Bu durum kimsenin kendi kusuru dolayısıyla hak elde edemeyeceği ilkesine dayandırılmıştır³¹².

³⁰⁸ Beytar, E., (2018), s. 163-164.

³⁰⁹ Elbir, N., (2020), s. 303.

³¹⁰ Beytar, E., (2018), s. 165.

³¹¹ Süzek, S., (2021), s. 695.

³¹² Elbir, N., (2020), s. 307.

5.2.1 Kişisel Duruma İlişkin Sorular

Aday işçinin ekonomik durumuna ve bir önceki işinde aldığı ücrete ilişkin soruların sorulup sorulamayacağı tartışma konusu olmuştur. Kural olarak bu tür soruların sorulamayacağı görüşü yaygın olsa da³¹³, işverenin bu tür soruları sormasında haklı menfaatinin bulunduğu istisnai durumlar da mevcuttur. İşçinin eski işinden aldığı ücreti ile yeni işinin özellikleri arasında bir bağlantı mevcutsa, bu soruların işverence sorulabileceği kabul edilir. İşçinin ekonomik durumunun bozuk olması nedeniyle malvarlığında hacizlerin bulunması ile yeni işinde alacağı maaşın üzerine de haciz konulacağı ve muhasebe biriminin iş yükünü oldukça artıracığı arasında bağlantı olmasından mütevellit işçinin bu ihtimale binaen ekonomik durumu hakkında soru sorulabileceği kabul edilir.³¹⁴ Bu hallerde işçi adaylarına sorulan soruların geçerli olduğu kabul edilmekte ve işçi adaylarından bu soruları doğru şekilde cevaplandırması beklenmektedir.³¹⁵ Aday işçinin ücretine ilişkin sorulan soruya yanlış cevap vermesi ve işe alınmasının ardından ne olacağı hususu tartışmalıdır. Bir görüşe göre bunun işverene, işvereni yanıltma niteliğinde olması nedeniyle işçinin iş akdine işverence haklı nedenle son verebilme imkânı tanıdığı, diğer görüşe göre ise bunun işçi ve işveren arasında bir pazarlık taktiği olduğu, bu nedenle işverene haklı sebeple fesih imkânı tanımadığı şeklindedir. Bu halde yaygın görüş, haklı fesih sebebi oluşturmayacağı yönündedir. Gerekçesi ise ücrete ilişkin yanlış bilginin verilmesinin 25/II-a'da belirtildiği şekilde bir yanıltıcılığa sahip olmaması şeklinde verilmiştir³¹⁶.

Kanımızca diğer görüş uyarınca işçinin eski işinin ücreti hakkında yalan söylemesinin işverence haklı sebeple feshe yol açabileceğinin kabulü gerekmektedir. Öncelikle işçinin işverenine kasıtlı şekilde yanlış bilgi vermesi işçinin sadakat borcuna aykırı bir davranıştır. İşçinin bu davranışının, işveren ile aday işçi arasındaki güveni onarılamayacak şekilde sarstığı kabul edilmelidir. Çünkü işçinin bu şekilde yalan söylemesi, işi ile alakalı konularda da yalan söyleyebileceği konusunda işverende bir düşünce oluşturabilir. İkinci olarak ise işçinin bu davranışının, diğer aday işçilerde hak kaybı oluşturabilme ihtimalidir. Bu durumu örnekle açıklamak isteriz. Aynı iş pozisyonuna dört adet işçinin başvurması durumunda, işçilere eski ücretleri

³¹³ Elbir, N., (2020), s. 305.

³¹⁴ Yardımcı, A., (2019), s. 69-70.

³¹⁵ Toprak, B., (2018), s. 89.

³¹⁶ Beytar, E., (2018), s. 166.; Yardımcı, A., (2019), s. 70.; Manav, E., (2015), s. 115.

sorulduğunda bir işçinin diğerlerinden iki kat fazla ücret beyan etmesi işverende işçinin oldukça nitelikli bir eleman olduğundan mütevellit söz konusu ücreti aldığını düşünebilir. Bu durumda işçi işverende yanlış bir kanaat oluşturarak işvereni yanıltacağı gibi, diğer başvuruçuların önüne haksız şekilde geçmiş olacaktır. Dolayısıyla, yukarıda örnekle de açıkladığımız nedenlerin yanında kanunun lafzının da açık olması sebebiyle, işçinin ücreti hakkında işverene yanlış bilgi vermesi durumunda işveren bakımından haklı fesih sebebi oluşacağı düşüncesindeyiz.

Bunun yanında, aday işçiye rakip firmaların üst düzey pozisyonlarında çalışıp çalışmadığına dair soru sorulmasında işverenin meşru menfaati olduğu gerekçesiyle bir hukuka aykırılık bulunmamaktadır³¹⁷. Medeni durum konusunda işçiye sorulabilecek sorularda ölçülülük ilkesi esas alınmalıdır. Aday işçiye partneriyle ne zaman evleneceği gibi bir soru sorulması özel hayatın gizliliği ve kişisel verilerin korunması konularında da uygun olmayacaktır³¹⁸. Ancak adayın eşinin bulunup bulunmadığı bilgisi, işverene asgari geçim indiriminin uygulanışı hakkında bir ön bilgi vereceğinden bu durumda işverenin bu bilgiye ilişkin soru sorma hakkı olduğu söylenilebilir³¹⁹.

5.2.2 Eğitime İlişkin Sorular

Aday işçinin eğitimine ilişkin sorular, işçinin işi yapabilecek nitelikte olup olmadığının anlaşılması konusunda gerekli sorular olup, bu soruların işveren tarafından aday işçiye yöneltilmesinde herhangi bir sakınca yoktur. Bu tür sorulara işçi doğru şekilde cevap vermelidir. Bu sorulara yanlış cevap verildiği takdirde işverenin iş akdini haklı sebeple fesih hakkı bulunduğu tartışmasızdır³²⁰. Belçika’da özel sektörün geneline uygulanan bir toplu iş sözleşmesi uygulaması bulunmakta olup, bu toplu iş sözleşmesinin 13. maddesi aday işçilerin “*pozisyonun niteliği ve işin ifa edilmesi koşulları*” ile ilgili tüm bilgileri işverenine sağlama yükümlülüğünü düzenlemektedir³²¹. Hukukumuzda da, yazılı olmasa da buna benzer bir uygulamayla; aday işçilerin işverenlerine mesleki yeterlilik, yabancı dil seviyesi gibi bilgileri sağlaması gerektiği kabul edilir. Bu tür bilgilerin aday tarafından sağlanmaması veya

³¹⁷ Beytar, E., (2018), s. 167.

³¹⁸ Manav, E., (2015), s. 155-156.

³¹⁹ Toprak, B., (2018), s. 89.

³²⁰ Beytar, E., (2018), s. 171.

³²¹ Gürsel, İ., (2016), s. 300.

yanlış olarak bildirilmesi, İş Kanunu m. 25/2-a uyarınca işverenin yanıltılması olarak sayılmakta ve işverene haklı sebeple fesih imkanı tanınmaktadır.

5.2.3 Sağlık İlişkin Sorular

Sağlık konusunda da adaya soru sorulabilmesi duruma bağlıdır. Sağlık kamu düzeniyle çok yakın ilişkisi olan bir kavram olduğundan dolayı, özel nitelikli veri olmasına rağmen işverenin bazı durumlarda aday işçinin sağlığına ilişkin verilere erişmesinde menfaati bulunmaktadır. Sağlığa ilişkin sorular işverenin işçilerini denetleme yükümlülüğü kapsamında değerlendirildiğinde işverenlerin aday işçinin sağlığına ilişkin soru sorabileceği ve aday işçilerin bu soruları doğru cevaplaması gerektiği kabul edilmektedir³²². Ancak işverence bu alana ilişkin her türlü sorunun sorulması işçinin kişilik hakkına müdahalede bulunabilmektedir. Dolayısıyla işverenin meşru menfaatıyla işçinin kişilik hakları arasındaki dengenin kurulması gerekmektedir. Bazı mesleklerin güvenli olarak yürütülebilmesi için işçilerin sağlık bilgileri önem taşımaktadır. Örneğin prensip olarak steril olması gereken sağlık laboratuvarına işe başvuran bir şahısta AIDS hastalığı olup olmadığı işin niteliği açısından büyük önem taşımaktadır. İşyerinin niteliği gereği sürekli tozlu ortamda çalışmayı gerektiren bir işe başvuran adayın astım geçmişine ilişkin soru sorulması hem işçinin kendi sağlığı hem de işverenin ileride karşılaşılabileceği bir meslek hastalığı ya da işyeri kazası durumu açısından önemlidir. Bu durumlarda aday işçilerden bu bilgileri kendilerinin vermesi beklenir. Aynı şekilde işçinin asla iyileşmeyecek bir hastalığının bulunması durumunda da işvereni bilgilendirmesi gerekmektedir³²³. İşçinin bu tür hastalıkları bulunmasına rağmen işverenini işe girerken bilgilendirmemesi, işçinin işverenini yanıltılması niteliğinde olduğundan ileride bu husus tespit edildiğinde İş Kanunu m. 25/2-a uyarınca işveren tarafından haklı nedenle fesih yapılabileceği gibi; işçinin bu hastalığına rağmen işyerinde çalışmasında hem kendisi hem de işvereni açısından sakınca olduğundan İş Kanunu m. 25/1-b uyarınca da fesih için haklı sebep oluşmaktadır.

³²² Yardımcı, A., (2019), s. 71.

³²³ Toprak, B., (2018), s. 90.

5.2.4 Engellilik Durumuna İlişkin Sorular

Aday işçinin engelli olup olmadığının sorulması yine sağlığına ilişkin sorular kapsamında değerlendirilmektedir. Ancak İş Kanunu'nun engelli işçi çalıştırma yükümlülüğünü düzenleyen 30. maddesi uyarınca engellilerin ancak "meslek, beden ve ruhi durumlarına uygun işlerde çalıştırılabileceği düzenlenmiştir. Dolayısıyla işverenin, başvuruda bulunan işçi adayının engelli olup olmadığını bilmesi; ona vereceği işi değiştirebileceğinden son derece önemlidir³²⁴. İşverenin işbu kanuni yükümlülük dolayısıyla menfaatinin olduğunu söyleyebiliriz. Bunun yanında çağrı merkezi personeli olarak işe alınacak adayın konuşma engeli, zorluğu veya bozukluğu bulunup bulunmadığına ilişkin soru sormakta işverenin meşru menfaati bulunmaktadır.

5.2.5 Hamileliğe İlişkin Sorular

Kadın adaylara hamileliğe ilişkin soruların sorulup sorulamayacağına dair hukukumuzda üç adet görüş mevcuttur. Bunlardan ilki, kadın işçinin hamileliğinin işverene bir külfet yaratacağı gerekçesiyle işveren tarafından bu tür soruların her koşulda sorulabileceği görüşüdür. Hamilelik sebebiyle izin alacak kadın işçi, işverenin bu durumda gerekli önlemleri önceden almasını sağlayabileceğinden bu görüş uyarınca işveren, aday işçinin kadın olması halinde hamileliğine ilişkin sorular sorabilmektedir. İkinci görüş ise yapılacak işin niteliği hamilelik bilgisi ile bağlantılı ise bu sorunun işverenlerce aday işçiye sorulabileceği, ancak alakalı değilse özel hayatın gizliliğinin ihlalini oluşturacağından sorulamayacağı görüşüdür. Bu görüş uyarınca da mankenlik gibi hamilelik bilgisinin işin niteliğini etkilemesi durumunda işverenin bu bilgiyi edinmek için soru sormasında menfaati olduğu kabul edilir. Üçüncü görüş, iş ile bağlantılı olsun ya da olmasın, kadın aday işçiye bu sorunun sorulmasının cinsiyet ayrımcılığı teşkil etmesinden dolayı sorulmaması gerektiğine dair görüştür. Gerçekten de, Türkiye'nin imzalamış olduğu ve diğer birçok uluslararası sözleşmeler uyarınca işin niteliğinin gerektirmemesine rağmen hamilelik ile ilgili soru sormak eşitlik ilkesine aykırılık teşkil etmektedir³²⁵. Bu üç görüşten kanımızca en makul olanı işverenin aday işçiye her türlü durumda hamileliğe ilişkin soru sorabilmesi görüşüdür. Çünkü, hamilelik durumunda işçiye kanunen verilmesi gereken izin süresi

³²⁴ Velioğlu, A., (2020), s. 183.

³²⁵ Manav, E., (2015), s. 117.

mevcut olup, işveren bu tür durumlarda eleman yetersizliği durumuyla karşılaşabilecektir. Bu durumda yetişmesi gereken işlerin olacağı ihtimali de göz önünde bulundurulduğunda bazı işçilerin fazla mesai yapma durumu gündeme gelecektir. Bütün bunlar önceden planlanarak yapılması gereken işlemler olduğundan işverenin her türlü durumda bu tür soruları sormasında menfaati olduğu görüşünderiz. Ancak aday işçiye sorulan soru sonucunda söz konusu adayın, işveren tarafından hamileliğe ilişkin planı olması nedeniyle işe alınmaması durumu açıkça ayrımcılık teşkil edeceği gibi, Anayasa'nın 10. maddesinde düzenlenen kanun önünde eşitlik ve İş Kanunu'nun 5. maddesinde düzenlenen eşit davranma ilkesinin ihlalini oluşturacaktır. Bu durumda amaçla bağlantılı elde edilmediğinden söz konusu sorunun kişisel verilerin hukuka aykırı işlenmesi niteliğinde olmasının yanında, işveren aleyhine bu davranışından dolayı ayrımcılık tazminatına da hükmedilebilir.

5.2.6 Hükümlülüğe İlişkin Sorular

Hükümlülüğe ilişkin soruların sorulabilmesi hakkındaki doktrin görüşü hükümlülüğe konu suçun iş ile bağlantısının bulunup bulunmamasına bağlıdır. Buna göre, muhasebeci pozisyonuna başvuran aday işçiye mali suçlar hakkında, ilköğretmeni pozisyonuna başvuran aday işçiye çocuk istismarı suçu hakkında sabıklarının bulunup bulunmadığına ilişkin soru işverenlerce sorulabilmektedir. Ancak, aday işçinin işlediği suç adli sicilinden silindiyse işçiye sabıkası hakkında soru sorulması durumunda işçinin sicilinden silinen suçu açıklama ve işvereni bilgilendirme yükümlülüğü bulunmamaktadır³²⁶. Yargıtay kararlarında, işçinin işvereninden sabıkasını gizlemesinin “*işçinin gerçeğe uygun olmayan bilgilerle işverenini yanıltması*” niteliğinde olduğunu ve işveren açısından haklı fesih gerekçesi oluşturduğu belirtilmektedir³²⁷. Yine bir başka kararında Yargıtay; güvenlik görevlisi olarak işe alınan personelin işe alım sürecinde doldurmuş olduğu formda sabıkasını gizlemesinin işveren açısından haklı fesih sebebi oluşturduğunu hükmetmiştir³²⁸.

³²⁶ Gürsel, İ., (2016), s. 323.

³²⁷ Yargıtay 9. HD. E.2000/4727, K.2000/7993, T.06.06.2000, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022); Yargıtay 9. HD. E.1998/16858, K.1998/18293, T.16.12.1998, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³²⁸ Yargıtay 8. HD. E.1998/19393, K.1998/432, T.22.01.1998, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

İş sözleşmesi kurulduktan sonra işçi tarafından suç işlenmesi halinde sicile işlenen bu suç hakkında işverenin bilgilendirilmesi, işçinin sadakat yükümlülüğü altında yapması gerekenlerden biri olarak sayılmaktadır³²⁹. Gürsel'in görüşüne göre, işçinin adli sicil kaydının tüm aday işçilerden değil, sadece işe alınacak aday işçi ile iş sözleşmesi kurulurken söz konusu işçiden istenmesi gerekmektedir³³⁰. Bu halde, diğer aday işçilerin kişilik haklarına müdahalede bulunmadan, müdahale asgari seviyede tutularak işverenin menfaati gözetilmektedir. Dolayısıyla bu görüşe katılıyoruz.

5.2.7 İnanışa, Sendika Üyeliğine ve Siyasi Düşüncelere İlişkin Sorular

İşçilerin dini inanışları ve düşünceleri Anayasa ile koruma altına alınmıştır. Anayasa'nın 24. ve 25. maddeleri uyarınca herkesin din ve vicdan hürriyeti ile düşünce ve kanaat hürriyeti bulunmaktadır. Bunlar temel hak ve özgürlüklerden olup, kimse dinini, inancını, görüşlerini ve düşüncelerini açıklamaya zorlanamaz³³¹. Ayrıca Anayasamızın 51. maddesine göre işçilerin sendikal özgürlüğü de bulunmaktadır. Bu kapsamda, aday işçiye bu tür soruların sorulması kural olarak hukuka uygun olmadığı gibi, aday işçilerin bu sorulara cevap vermeme veya yanlış cevap verme hakkı bulunmaktadır. İşçinin bu soruya yanlış cevap vermesi işvereni yanıltma olarak kabul edilmeyeceği gibi, ileride iş sözleşmesi kurulduktan sonra bu hususun tespit edilmesi durumunda işverene işçinin iş akdini haklı sebeple feshetme hakkı vermez³³².

Neredeyse tüm kurallarda olduğu üzere, aday işçiye siyasi görüşüne, dini inancına ve sendika üyeliğine ilişkin soru sorulma yasağının da istisnası mevcuttur. Nitekim, KVKK kapsamında da özel nitelikli verilerden olan bu verilerin işlenmesinde hukuka uygunluk sebepleri de bulunmaktadır. Dini inanç ve siyasi görüşe ilişkin sorular, işin niteliğine bağlı olarak işverenlerce sorulabilmektedir. Örneğin, dini bir kurumun işe alacağı aday işçiye inancı ile ilgili soru sorması geçerli kabul edilmektedir. İşçinin mevcut olayda inancı yapacağı işi etkileyebilecek nitelikte olduğundan, işverenin bu bilgiyi önceden bilmesi gerekir ve buna göre inancı yapacağı iş doğrultusunda olan bir aday tercih etmesi eşitlik ilkesine aykırılık teşkil etmez. Siyasi görüş konusunda aynı mantık işlemektedir. Bir siyasi görüşe sahip bir aday işçinin, başka siyasi görüşü savunan bir partide işe başlaması yapılacak işi

³²⁹ Velioğlu, A., (2020), s. 184.

³³⁰ Gürsel, İ., (2016), s. 324.

³³¹ Yardımcı, A., (2019), s. 71.

³³² Beytar, E., (2018), s. 173.

etkileyeceğinden ve işverenin menfaatine ters düşeceğinden işverenin bu soruyu sormasında da haklı menfaati olduğu kabul edilir³³³.

Sendika üyeliği, işçiye tanınmış anayasal bir hak olup, işçilerin sendika üyeliği bilgilerine göre tercih edilmeleri tamamen ayrımcılık teşkil etmektedir. Bu nedenle işverenin sendika üyeliğine ilişkin soruları aday işçilere sormaması gerekmektedir. Zira aday işçinin sendika bilgisinin işveren tarafından başvuru değerlendirmede kriter olarak uygulanması Anayasa'nın 10 maddesi ve İş Kanunu'nun 5. maddesi uyarınca ayrımcılık oluşturmaktadır. 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu³³⁴, nun (STİSK) 25. maddesi de bu durumu destekler bir hüküm bulunmaktadır. Hükme göre işçilerin işe alımları; belli bir sendikaya girip girmemeleri, üyeliklerini sürdürmeleri ya da üyelikten çekilmeleri şartına bağlanamaz. İşçilerin işe alımları böyle bir şarta bağlanamayacağından işe alımda bu tür bilgilere ilişkin soruların sorulmasında işverenin menfaatinin bulunmadığı açıktır. Her ne kadar bazı kanuni düzenlemeler, işvereni işçilerine ait sendika bilgilerine erişmeye zorunlu kılsa da³³⁵; işbu kanuni düzenlemelerden kaynaklı yükümlülükler işe alım sürecinde mevcut olmadığından ve bu tür bilgilere iş sözleşmesi kurulduktan sonra da KVKK m. 6/3 uyarınca hukuka uygunluk sebebi bulunduğu gerekçesiyle erişilebileceğinden, işe alım sırasında aday işçinin sendika üyeliğine ilişkin soru sorulması kanımızca her türlü durumda hukuka aykırı olacaktır. İşçilerin bu tür sorulara cevap verme zorunluluğunun bulunmadığı ve cevap vermemesi halinde işe alınmamasının STİSK'nın 25. maddesinin 1. fıkrası uyarınca ayrımcılık teşkil edeceği şüphesizdir³³⁶.

Dolayısıyla genel anlamda, aday işçiye sorulabilecek soruların; dürüstlük kuralının çizdiği sınırlar içerisinde, işçilerin kişisel verilerinin korunması hakkına ve özel hayatın gizliliğine hanel getirmeyecek şekilde, iş ilişkisiyle nedensellik bağı bulunan ve işverenin sormasında haklı bir menfaati bulunan sorular olduğu söylenebilir. Tüm bu sorular karşılığında alınan bilgilerin, aday işçinin işe alınmaması

³³³ Velioğlu, A., (2020), s. 184.

³³⁴ 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu, *T.C. Resmi Gazete*, Sayı: 28460, 7 Kasım 2012 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

³³⁵ “ILO Kodu m. 6/6'ya göre işverenler sendika aidatlarının kontrolü, iş konseylerinin çalışması ve bilgi sağlama yükümlülüğünün yerine getirilebilmesi için işçilerin işyerindeki sendika üyelikleri ve faaliyetleri hakkında bilgi toplayabilir. STİSK'nin 23 ve 24'üncü maddeleri gereği öngörülen güvencelerin kullanılabilmesi içinde işverenlerin hangi işçilerin işçi kuruluşu yöneticisi ya da işyeri sendika temsilcisi olduğunu bilmeleri gerekir ve bu yönde sorulan sorular kanuni bir gerekliliğin sonucu olduğu için geçerli kabul edilir.” Toprak, B., (2018), s. 96.

³³⁶ Süzek, S., (2021), s. 695.

durumunda saklanması için amaç kalmadığından imha edilmesi gerektiği unutulmamalıdır.

5.3 İşçilerin İş Sözleşmesi Süresince Kişisel Verilerinin Korunması

İş sözleşmesi kurulduktan sonra işveren gerek kendi menfaati gerekse kanuni yükümlülükler dolayısıyla işçilerine ait kişisel verileri işlemektedir. Kanunla öngörülen yükümlülükler KVKK uyarınca hem normal nitelikli hem de özel nitelikli verilerin işlenmesi hususlarında hukuka uygunluk sebebi olarak öngörüldüğünden, kanuni yükümlülüklerin yerine getirilmesi amacıyla işlenen kişisel veriler, kişisel verilerin korunması ya da özel hayatın gizliliği haklarının ihlalini oluşturmayacaktır. Ancak işverenin kendinin ve işletmesinin menfaati için işçileri ve işi denetleme amacıyla yaptığı gözetlemeler, işe giriş çıkış denetlemesi, birbirleriyle olan iletişimlerinin elektronik ortamda gözetlenmesi usulüne uygun ve kontrollü yapılmadığında işçilerin kişilik haklarına hanel getirebilmektedir. Dolayısıyla denetim amaçlı yapılan bu kişisel veri toplama ve işleme faaliyetlerinde işçinin kişilik hakları ve işverenin menfaati arasındaki dengenin sağlanması gerekmektedir.

5.3.1 İşçinin Giriş-Çıkışlarının Denetlenmesi

İşe giriş-çıkış için kullanılan elektronik ve biyometrik sistemler mevcuttur. Bu sistemler ile işverenler denetim hakları kapsamında işçilerin giriş çıkışlarını denetlemektedir. Elektronik sistemler, işçinin işe girişinde kart okuyucuya akıllı kart basması, şifre girmesi gibi sistemlerdir. Biyometrik sistemler ise kişilerin karakteristik özelliklerinin kullanılması ile kişinin ayırt edildiği, yüz şekli, retina, parmak izi, ses, avuç içi gibi bilgilerle giriş yapılan sistemlerdir³³⁷. Biyometrik sistemler, kişilerin özel nitelikli verilerini işlediğinden daha güvenli sistemlerdir, ancak verilerin ifşa edilmesi durumunda doğacak zarar daha fazla olduğundan riskleri daha fazladır. Bu nedenle Yargıtay kararları uyarınca biyometrik sistemlerde ölçülülük ilkesi kapsamında değerlendirme yapılmaktadır³³⁸. Ölçülülük ilkesi uyarınca işçiye en az zarar verecek olan sistem tercih edilmelidir. Bu nedenle, işyerinde kart okutma, şifre girme gibi basit uygulamalar ile giriş çıkış tespiti yapılabiliriyorsa, bu yollar tercih edilmelidir. Bu sistemler kullanılabilecekken biyometrik sistemlerin kullanılmasında menfaatin

³³⁷ Beytar, E., (2018), s. 192.

³³⁸ Danıştay 15. D. E.2014/4562, T.11.09.2014, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022).

olmadığı kabul edilir. Biyometrik sistemler ile ilgili en önemli husus, bu sistemler vasıtasıyla kimlik tespiti yapıldıktan sonra toplanılan biyometrik verilerin yok edilmesinin gerekliliğidir³³⁹.

Biyometrik sistemlerle işçilerin biyometrik verileri işlenmektedir ve KVKK m. 6 uyarınca biyometrik veriler özel nitelikli veri kategorisine alınmıştır. Bu nedenle bu sistemlerle söz konusu verilerin işlenebilmesi için hukuka uygunluk sebebi olarak işçilerin açık rızası gerekmektedir. Diğer hukuka uygunluk halleri de mevcuttur, lakin uygulamada işe giriş-çıkışın denetlenmesi için biyometrik sistem ile biyometrik verilerin toplanması için, KVKK'nın 6. maddesinin 3. fıkrasında düzenlenen istisnai hukuka uygunluk hallerinin bulunması pek muhtemel değildir. Hukuka uygunluk sebebinin bulunması, kişisel verilerin işlenmesi hususundaki temel ilkeler gerekliliğini bertaraf etmemektedir. İşçinin biyometrik sistem ile retina verilerinin işlenmesine açık rızası bulunsa dahi, işverenler halen temel ilkelere riayet etmek zorundadır. Yukarıda bahsettiğimiz ölçülülük ilkesi kapsamında, kimlik tespiti işyerinde daha basit bir uygulama ile gerçekleştirilebilecekken biyometrik sistemin tercih edilmesi, işçinin açık rızası bulunsa dahi, KVKK m. 4 uyarınca düzenlenen “işlenen amaçla ölçülü olma” ilkesini ihlal edeceğinden bu sistemlerin hukuka uygunluğundan bahsedilemez³⁴⁰. Nitekim, Sağlık ve Sosyal Hizmet Emekçileri Sendikası'nın Konya Valiliği'ne kamu kurumunda parmak izi ile mesai takibinin yapılması işleminin, söz konusu işlemin temel hak ve hürriyetlerden özel hayatın gizliliği hakkını ihlal ettiği gerekçesiyle iptali istemiyle ikame edilen dava neticesinde, talep Yerel Mahkemece reddedilmiştir. Kararın temyiz edilmesi üzerine Danıştay 5. Dairesi'nin 10.12.2013 tarihli ve 2013/5342 Esas, 2013/9525 Karar sayılı ilamında, parmak izi mesai takip sistemi ile verileri işlenen kamu personellerinin özel hayatlarının gizliliği hakları ile kamu kurumunun personellerinin belirlenen saatler içerisinde çalışıp çalışmadığının tespitine ilişkin parmak izi mesai takip uygulamasındaki menfaati arasındaki denge incelenmiştir. Kararın verildiği tarihte kişisel verilerin işlenmesine ilişkin herhangi bir mevzuat bulunmadığı hususuna değinilmiş olup, kamu yararı ile söz konusu uygulama arasında orantılılık bulunmadığından bahisle anayasal ilke olan ölçülülük ilkesine aykırılık bulunduğu, kamu personellerinin açık rızasının alınmaması nedeniyle hukuka

³³⁹ Beytar, E., (2018), s. 193-194.

³⁴⁰ Üstün, Y. ve Günal, A.N. (2020) *İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi*, Kişisel Verileri Koruma Dergisi, C. 2(2), s. 65.

uygunluk sebebinin de bulunmadığı, dolayısıyla parmak izi mesai takip sistemi uygulamasının kamu personellerinin özel hayatın gizliliği haklarını ihlal ettiğine karar verilmiştir ve söz konusu uygulama iptal edilmiştir.³⁴¹

İşçinin işe giriş-çıkışlarında üstünün aranması da işçilerin özel hayatına müdahalede bulunan bir denetim mekanizmasıdır. Bu nedenle bir sözleşme ilişkisinin veya kanunda düzenlenen halin bulunması üst aranması için gereklidir. Üst aramasının sebebi işyeri sağlığı ve güvenliğini sağlamak ile hırsızlık vakalarını önlemek olabilir. Ancak üst aranması için işçinin açık rızası gerekecektir. Belirli durumlarda açık rızanın aranmaması söz konusu olabilir. Eğer hırsızlık veya işyerine iş sağlığı ve güvenliğini tehlikeye atacak aletler sokulması olayları daha önceden yaşanmışsa üst aranması durumunun nasıl yapılacağı hakkında iki görüş mevcuttur. Bu görüşlerden ilki, daha önceden yaşanmış bir olay bulunduğundan; işverenin üst aramasında kanuna uygunluk amacıyla bir nedeni olduğunu kabul etmektedir. İkinci görüş ise işverenin makul bir sebebi olduğu, ancak yine de üst aramasının açık rıza ile yapılması gerektiğidir. İşverenin makul sebebi olduğu için işçinin üst aramasına izin vermemesi işçinin sadakat borcunu yerine getirmemesi sonucunu doğuracak ve bu durum işverene iş ahdinin feshedilmesi için haklı gerekçe verecektir. Dolayısıyla bu görüşe göre işçinin açık rıza vermesi gerekmektedir. Eğer hırsızlık ya da işyerine iş sağlığı ve güvenliğini tehlikeye atacak aletler sokulması olayları daha önceden yaşanmamışsa, o zaman makul sebep bulunmadığından işçinin açık rızasının alınması gerekecektir. Üst aranması gerçekleştirilirken yalnızca açık rızanın bulunması yetmemektedir. Eşitlik ilkesini ihlal etmemek adına bu uygulamanın bir işçiye yapıp diğerlerine yapılmaması gibi keyfi bir uygulama yapılmamalıdır. Aynı şekilde, üst aranması yaparken elle yoklama yerine metal detektörleri ya da X-ray cihazları tercih edilmelidir³⁴². Yukarıda işçilere yapılan üst aranması uygulamasında açık rıza veya bir hukuka uygunluk sebebi bulunması ve yapılan uygulamanın ölçülü olmasından bahsedilmiş olsa da, işçilere işe giriş-çıkışlarında yapılan üst aranması uygulaması Yargıtay kararlarınca kabul gören bir uygulama olup, arama sonucu elde edilen deliller caiz nitelikte sayılmaktadır³⁴³.

³⁴¹ Danıştay 5. D. E.2013/5342, K.2013/9525, T.10.12.2013, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³⁴² Yardımcı, A., (2019), s. 74-75.

³⁴³ Yargıtay 7. HD. E.2016/27389, K.2016/20430, T.05.12.2016, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022); Yargıtay 7. HD. E.2015/9013, K.2015/19992,

İşçilerin işyerindeki masa, çekmece ve benzeri alanlarının aranması hususunda da Yargıtay, “gizliliğe dair makul beklenti”nin oluşup oluşmadığı hususunu incelemektedir.³⁴⁴ Yargıtay Hukuk Genel Kurulu’nun önüne gelen bir mobbing davasında³⁴⁵, banka personelinin masa çekmecesinin aranması sonucunda banka personel yönetmeliğinde suç olarak nitelendirilmiş evraklara rastlanmıştır. Söz konusu olayda Yargıtay banka personel yönetmeliği hükümlerine atıf yaparak işverenin “gerekli görmesi halinde sözü edilen yerleri açtırma ve inceleme” hakkına sahip olduğunu belirtmiş ve işçilerde “gizliliğe dair makul bir beklenti”nin oluşmadığına kanaat getirerek çekmece aranması hususunda hukuka aykırılık tespit etmemiştir.

5.3.2 İşçilerin Elektronik Ortamda İzlenmesi ve Gözetlenmesi

İşçiler, işçi sınıfının başlangıcından itibaren işverenleri ve amirleri tarafından gözetlenmektedir. Bu gözetleme çeşitli amaçlar için olabilmektedir. İşyerinde hırsızlığın ve diğer suçların önlenmesi, işçilerin işi savsaklamasının önüne geçilmesi, yapılan işin kontrolü ve denetimi bunlardan birkaçıdır. İşyerinde işçilerin gözetlenmesi işverenin yönetim hakkı kapsamında sayılmaktadır. Teknolojinin gelişmesiyle birlikte bizzat şahıslar tarafından gerçekleşen gözetleme, yerini video kameralarla gözetlemeye bırakmıştır. Bu sayede, işçilerin her an gözetlenmesi mümkün hale gelmiş ve işçilerin işlerini savsaklık yapmadan ve dikkatlice yapmalarına ön ayak olunmuştur³⁴⁶.

İşçilerin performanslarını denetleme vasfının yanında işverenler kanuni yükümlülüklerini yerine getirmek amacıyla da işyerinde video kamera ile gözetleme yapabilmektedir. İşyerinde bir hırsızlık iddiası, aynı şekilde cinsel taciz iddiasında, durumun tespit edilmesi için kamera görüntülerinin kullanılması işçilerin zarar görmesini engelleyici niteliği sahip olduğundan işverenin kanuni yükümlülüklerini yerine getirme vasfını haizdir. Nedeni ne olursa olsun, kamera sistemi ile gözetlenme ölçülülük ilkesi uyarınca gerçekleştirilmelidir. Yani, amaç dışında veri işlenmemelidir

T.21.10.2015, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³⁴⁴ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 387.

³⁴⁵ Yargıtay HGK. E.2017/7-3017, K.2018/99, T.24.01.2018, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³⁴⁶ Yardımcı, A., (2019), s. 76.

ve bunun yanında, ulařılmak istenen amaç kamera ile gözetleme dıřında başka bir yöntem ile ulařılabiliyorsa, o yöntem tercih edilmelidir.

Açık rıza bulunmasına rağmen gözetlenmesi mümkün olmayan, tuvaletler, soyunma odaları gibi işçilerin özel ihtiyaçlarını karşıladığı yerler mevcuttur. Bu yerlerin gözetlenmesinde işverenin hiçbir şekilde yararı bulunmadığı gibi gözetlenmesi halinde işçilerin özel hayatının gizliliğı ihlal edileceğinden, söz konusu yerler kati olarak işveren tarafından gözetlenemez.

İşçilerin gözetlenmesi açık ve gizli olmak üzere iki şekilde gerçekleşmektedir. Açık şekilde gözetleme herkes tarafından görülebilecek bir kamera ile işçilerin gözetlenmesini ifade etmektedir. İşçiler tarafından açıkça görülebilmesi, işçinin bu konu hakkında bildirilmesi yükümlülüğünü ortadan kaldırmayacaktır. Her türlü izlenme, bir kişisel veri işlenmesini oluşturduğundan; KVKK m. 10 uyarınca bilgilendirilmelidir. İşçilerin açık rızasının bulunması ve gözetlenmenin ölçülü olması da yetmeyebilir. İzlenme, işçi üzerinde denetildiğı düşüncesiyle sıkı çalışma gibi olumlu etkiler gösterebileceğı gibi; işçinin sürekli gözetim halinde olması yüzünden paranoyaklaşması ve veriminin düşmesi gibi olumsuz etkiler de söz konusudur. Bu durumda işçinin akıl sağlığı kötü etkilendiğinden beden bütünlüğü hakkının ihlal edildiğı kabul edilir. Dolayısıyla, defalarca bahsettiğimiz üzere, işçinin kişilik hakları ile işverenin haklı menfaati arasındaki dengenin sağlıklı biçimde sağlanabilmesi için gözetleme sınırlandırılabilir, ya da kaldırılabilir. Diğer yandan, gizli kamera ile gözetleme, işçinin açık rızası bulursa dahi hukuka aykırılık teşkil etmelidir. İşbu izleme ile elde edilen veriler ve delillerin hiçbirisi caiz değildir³⁴⁷.

Bununla birlikte uluslararası içtihat; gizli kamera ile işçinin gözetlenmesi durumunda işverenin mülkiyet hakkının işçinin özel hayatının gizliliğı hakkının önüne geçtiğı kararlar mevcuttur. Avrupa İnsan Hakları Mahkemesi'nin 05.10.2010 tarihli Köpke kararında, süpermarkette çalışan Karin Köpke adındaki kasiyerin hırsızlık yaptığının işvereni tarafından özel dedektif vasıtasıyla gizli kamerayla tespit edilmesi sonucu kasiyerin işten çıkarılmasının Köpke'nin özel hayatının gizliliğı hakkını ihlal ettiğinden bahisle yapılan başvuruda Mahkeme, işverenin mülkiyet hakkı ile işçinin kişilik hakkı arasında adaletli şekilde denge kurulması gerektiğı, verilerin belirli süre için ve belirli kişi açısından işlendiğini, diğer işçileri de sorumluluktan kurtardığı

³⁴⁷ Beytar, E., (2018), s. 189-192.

gerekçeleriyle başvurunun reddine karar vermiştir³⁴⁸. Yine aynı mahiyette olan Lopez Ribalda kararında ise, yine süpermarkette çalışan 10 adet işçinin hırsızlık yaptığının süpermarketin giriş ve çıkışlarına yerleştirilen kameralarla tespit edilmesinin akabinde iş akitlerine son verilmesi ve adil yargılanma ve özel hayata saygı temel haklarının ihlal edildiği gerekçesiyle işten çıkarılan işçilerin Mahkeme'ye başvuruda bulunması söz konusudur. Mahkeme tarafından öncelikle kabul edilen başvuru, temyiz üzerine yeniden incelenmiş ve bir önceki olayla benzer gerekçelerle başvuruyu reddetmiştir. Ancak kararda işçilerin bilgilendirilmeden kamerayla izlenmeyecekleri konusunda makul bir beklentilerinin olduğunu belirtmiştir³⁴⁹. Sonuç olarak somut olayın incelenerek, terazide işverenin mülkiyet hakkının ağır bastığı durumlarda gizli kamera uygulamasının diğer yükümlülüklerin de yerine getirilmek suretiyle yapılabileceği, işçinin kişilik hakkının ağır bastığı ya da işverence diğer yükümlülüklerin yerine getirilmediği durumlarda ise uygulanmasının ihlale sebebiyet vereceği kabul edilmektedir. Gizli kamera uygulaması, Türk hukukunda ise tolere edilmeyen bir husus olarak karşımıza çıkmaktadır. Danıştay 1. Dairesi, Kocaeli Üniversitesi Araştırma ve Uygulama Hastanesi tarafından morg ünitesinde sözleşmeli memur olarak görev yapan personelin çalışma odasındaki yangın alarmına gizli kamera kurulması ve söz konusu personelin görüntülerinin kaydedilmesi olayında; çalışma odasının bir işçinin kişisel alanı niteliği taşıdığı, bu nedenle gizli kamera yerleştirilmesinin ve söz konusu personelin izlenmesinin Anayasa'nın 20. maddesinde düzenlenen özel hayatın gizliliği hakkının ihlalini oluşturacağı ve TCK'nın 134. maddesi uyarınca işbu uygulamanın suç teşkil ettiği hükmedilmiştir³⁵⁰.

Yukarıda bahsedilen ölçülülük ve önceden bilgilendirilme kriterleri, işçiye iş amacıyla tahsis edilmiş araçların takip sistemi ile izlenmesi hususunda da geçerlidir. Günümüzde birçok işyeri çoğunlukla yüksek pozisyondaki çalışanlarına iş için özel araç tahsis etmektedir. Bu araçların takip edilmesiyle elde edilen işçilerin lokasyon bilgileri kişisel veri niteliğinde olmaktadır. Dolayısıyla işlenmeleri için hukuka uygunluk sebeplerinden birinin mevcut olması ve işleme faaliyetinin temel ilkelere riayet etmesi gerekmektedir. Tıpkı işyerinde bilgisayarların ve telefonların kişisel amaçlı kullanımlarının denetimi gibi araç takip sistemleri de iş amaçlı tahsis edilmiş

³⁴⁸ Üstün, Y. ve Günel, A. N., (2020), s. 71.

³⁴⁹ Has, M. (2021) *AIHM Kararları Bağlamında Görüntü Hakkı*, Anayasa Yargısı, C. 38(1), s. 231-233.

³⁵⁰ Danıştay 1. D. E.2014/232, K.2014/25, T.19.02.2014, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

araçların iş dışında kullanılmasını ve mesai takibini denetlemektedir. Bu uygulama Yargıtay kararlarınca da kabul görmektedir³⁵¹. Bir işçinin rakip firmaya görüşmelere gitmesinin işveren tarafından tahsis edilen araçta bulunan GPS sistemiyle tespit edilmesi sonucu İş Kanunu m. 25 uyarınca işten çıkarılmasının akabinde işverenine karşı ikame ettiği işe iade davası Yerel Mahkemece reddedilmiştir. Yargıtay 9. Hukuk Dairesi, somut olayı değerlendirirken, işçinin rakip firmalara yapmış olduğu görüşmelerin iş tanımında yer aldığını, ancak işçinin GPS kayıt sisteminde kaydedilmiş rakip firmaya yapılan ziyaret sayıları ile ziyaret raporlarındaki sayıların uyuşmadığını tespit ederek “*davacının doğruluk ve bağlılıkla bağdaşmayan davranışları sebebiyle işveren tarafından yapılan feshin haklı nedene dayandığı*” gerekçesiyle kararı bozmuştur. Görüldüğü üzere, araç takip sistemiyle elde edilen kişisel verilerin hukuka uygun olmasıyla beraber, bu şekilde elde edilen deliller de caiz delil niteliğindedir.

5.3.3 İşçinin İletişiminin Gözetlenmesi

İşçiler, işyerlerinde iş telefonları ve bilgisayarlarıyla birbirleriyle veya bir başkasıyla iletişim kurabilmektedir. Bu iletişimin özel ve şahsi amaçlarla yapılması halinde, bu iletişim süresi işveren tarafından işçinin çalışma süresi içerisine alınmayabilir. Özellikle günümüzdeki pandemi döneminde, uzaktan çalışmanın yaygınlaşması sonucu işverenler yapılan işlerin takibini ve denetlemesini işçilerin iş bilgisayarlarını gözetleyerek gerçekleştirmektedir. Dolayısıyla kural olarak mesai saatleri içerisinde telefon ve bilgisayarların şahsi amaçlar için kullanılmaması yasağı mevcuttur. Bu yasağa uyulmadığı takdirde Yargıtay kararlarınca işveren tarafından iş aklının feshi açısından haklı sebep olduğu öngörülmüştür³⁵². Hatta özel kullanımın belirli konularda yapılması durumunda (pornografik içerikleri işyerinin veri taşıyıcısına indirmesi) işverenin, işçinin iş sözleşmesine ihtara gerek olmaksızın haklı nedenle son verebileceği öngörülmüştür. Bu duruma işverenin kamuoyu nezdindeki şöhretinin zarar görebileceği gerekçe olarak gösterilmiştir. İşçiler tarafından işyeri veri taşıyıcısına pornografik içerik indirilmesi halinde, Yargıtay tarafından işçinin özel hayatının gizliliği yerine işverenin menfaatinin gözetildiği anlaşılmaktadır.

³⁵¹ Yargıtay 9. HD. E.2016/17414, K.2017/12165, T.07.07.2017, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³⁵² Yargıtay 9. HD. E.2007/27583, K.2008/5294, T.17.03.2008, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

Ancak bu yasağın istisnaları da mevcuttur. Yargıtay acil durumlarda ya da işin gerektirdiği hallerde bu yasağın ihlal edilebileceğini ve özel amaçlı kullanımın bu durumlarda gerçekleştirilebileceğini belirtmiştir³⁵³. Nitekim uluslararası içtihatlarda da işçilerin özel amaçlı elektronik iletişimlerine belli seviyede izin verilmiştir. Fransa Veri Koruma Otoritesi olan CNIL, 05.02.2002 tarihli raporunda işçilerin iletişim araçlarını üretkenliklerini etkilemeyecek ve işlerini aksatmayacak derecede makul bir seviyede özel amaçlı olarak kullanabileceklerini ifade etmiştir³⁵⁴.

Yargıtay 9. Hukuk Dairesi'nin 2018/10718 Esas ve 2019/559 Karar numaralı ilamında dünyaca ünlü sohbet uygulaması olan Whatsapp uygulaması hakkında şu şekilde yorum yapılmıştır:

*“Öncelikle Whatsapp sistemi, telefon ve internet ortamında internet vasıtası ile iletişimi gerçekleştiren bir sistemdir. Burada kişi, kişiler ile iletişime geçtiği gibi gruplar kurarak grup içerisinde iletişim gerçekleştirilmektedir. Ancak bu sistem kendi içinde korunan ve 3. kişilere kapalı bir konumdadır. Dolayısı ile işçilerin iş akışını bozmadığı ve çalışmaların etkilemediği sürece bir grup kurmaları ve burada iletişim içinde olmaları yasak değildir. İşçilerin bu kapsamda burada iletişimlerinin kişisel veri olarak da korunması esastır.”*³⁵⁵

Görüldüğü üzere CNIL tarafından belirtilen iş ve çalışma akışının bozulmaması şartı Yargıtay uygulamalarında da kabul görmüştür. Bu kapsamda işçilerin Whatsapp uygulamasında bulunan verileri kişisel veri kategorisinde olup, üçüncü kişilerin erişimine kapalı durumda olmasından mütevellit ve iş akışını ve çalışma hayatını olumsuz yönde etkilememesi kaydıyla kişisel verilerin korunması hükümlerine tabi olacaklardır. Yani, işçilerin sosyal medya hesaplarındaki ve Whatsapp gruplarındaki sohbetleri kişisel veri niteliğinde olduğundan; işverenlerin bu verilere ulaşımı hukuka uygun olmak zorundadır³⁵⁶.

Bir önceki başlıkta bahsetmiş olduğumuz kriterler, işçilerin iletişim araçlarının gözlenmesi konusunda da aranmaktadır. İşverenler işçilerin iletişim araçlarını gözetleyebilirler. Ancak bu gözetlemenin hukuka aykırı olarak işçilerin özel yaşamına

³⁵³ Yardımcı, A., (2019), s. 78.

³⁵⁴ Gürsel, İ., (2016), s. 387.

³⁵⁵ Yargıtay 9. HD. E.2018/10718, K.2019/559, T.10.01.2019, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³⁵⁶ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 675.

müdahale aracına dönüşmesi engellenmelidir³⁵⁷. Ayrıca, böyle bir gözetlemenin hukuka uygun olabilmesi için, öncelikle işverenin işçiyi bu konuda bilgilendirmiş olması gerekmektedir. Daha sonra ölçülülük ilkesi kapsamında ve diğer temel ilkelere riayet etmek suretiyle, işçinin özel hayatına yapılan bu müdahale olabildiğince kısa ve öz tutulmalıdır³⁵⁸.

İşverenin işçilerin iletişimini izlemesinin bir yolu da e-posta iletişiminin izlenmesidir. Çoğu kurumsal işyeri işçilerine iş için tahsis edilmiş bilgisayar ve e-posta adresi vermektedir. Uygulamada işverenler işçilere verdiği bilgisayarlara, söz konusu bilgisayarlara erişim sağlayan programlar yüklemektedir. Bunun başlıca sebepleri işçinin işini icra edip etmediğini denetlemenin yanında, işçinin işverenin bünyesinde yasadışı aktivitelerde bulunup bulunmadığının veya rakip firmalara şirket sırlarının aktarılıp aktarılmadığının tespiti olabilmektedir. Bu durumda işçilerin kişisel verileri işverenin erişimine açık olacağından öncelikle işverenin işçiyi, böyle bir programın varlığından ve işçinin bilgisayarındaki iletişimin gözetlendiğinden bildirim yükümlülüğü gereğince haberdar etmesi gerekmektedir. Bu yükümlülüğün yerine getirilmesi işveren tarafından işçinin bilgisayarına sınırsız erişimi hukuka uygun kılmamaktadır. Ölçülülük ilkesi uyarınca gözetlemenin yapıldığı amaçla sınırlı, bağlantılı ve ölçülü kalınmalıdır. Bunun yanında genel olarak bütün kişisel verilerin işlenmesinde olduğu gibi işçinin açık rızası veya hukuka uygunluk sebeplerinden birinin bulunması halinde söz konusu gözetleme hukuka uygun olarak gerçekleştirilebilir³⁵⁹.

İşçinin bilgisayarının gözetlenmesine ilişkin Yargıtay'ın önüne gelmiş bir uyuşmazlıkta, davacı işçinin davalı işverenle arasında bulunan gizlilik sözleşmesine aykırı hareket etmesinden ötürü iş akdinin feshedilmesi sonucunda dava açan işçiye karşı davalı işveren savunmasında işçinin iş amacıyla verilen bilgisayarında bulunan takip programı ve işçinin işyerinde unutmuş olduğu USB cihazından elde edilen bilgilerden işçinin gizlilik sözleşmesini ihlal ettiği ve bunun sonucunda iş akdinin feshedildiği belirtilmiştir.

Somut olayda toplanan delillerle de işçinin işverenle arasındaki gizlilik sözleşmesini ihlal ettiği anlaşılmış olup, bu delillere ulaşma biçimi hususu

³⁵⁷ Süzek, S., (2021), s. 414.

³⁵⁸ Toprak, B., (2018), s. 109.

³⁵⁹ Toprak, B., (2018), s. 109-112.

değerlendirilmiştir. Zira davacı işçi, iş amacıyla kullanılan bilgisayarda herhangi bir takip programı bulunduğu haberi olmadığını ve böyle bir izlemeye rızasının bulunmadığı iddiasında bulunmuştur. Bunun üzerine Yargıtay'ın 22. Hukuk Dairesi, davacının taleplerini reddeden Yerel Mahkeme kararını aşağıdaki gerekçe ile bozmuştur:

“Şu hâlde davacı işçinin, bilgisayarında bulunan klavye yakalayıcısı adı verilen programdan haberinin olmadığı, işverence bu konuda bilgilendirilmediği, davacının rızası hilafına tüm kayıtların özel yahut işe ilişkin bilgi ayrımı olmadan işverence günlük olarak elde edildiğinin anlaşılması karşısında, elde edilen bu bilgilerin fesih sebebi olarak ileri sürülemeyeceği değerlendirilmelidir. İşverenin yönetim hakkının bir sonucu olarak işçiyi elektronik ortamda izlemesi ve takip etmesi her zaman mümkündür. Ancak bunun için işçinin bu izleme hakkında bilgilendirilmiş olması şarttır. İşçinin izlendiğine dair bilgilendirilmemesi veya gizlice izlenmesi, bu izleme neticesinde elde edilen veriler, iş sözleşmesinin işçi tarafından ihlal edildiğini açıkça ortaya koysa dahi, hukuka aykırı olarak kabul edilmelidir. Hal böyle iken, somut olayda işverence gizlice izleme neticesinde elde edilen bilgilerin haklı fesih sebebi olarak ileri sürülmesinin mümkün olmadığı kabul edilmelidir.”³⁶⁰

Görüldüğü üzere, her ne kadar işçinin hareketi İş Kanunu'nun 25. maddesi uyarınca haklı fesih gerekçesi oluştursa da; işçi, feshe konu hareketin tespiti için kullanılan araç hakkında bilgilendirilmediğinden özel hayatın gizliliği hakkı ihlal edildiğinden, tespit edilen deliller hukuken caiz olmayan delil niteliği taşımaktadır. Bu nedenle iş akdinin haklı nedenle feshedilmesi söz konusu olamaz.

Ayrıca, işçilerin işyerinde birbirlerine ilettikleri e-postaların, *“işçilik hakları ile ilgili demokratik talep niteliğinde olduğu”* ve bu nedenle fesih konusu oluşturamayacağı Yargıtay Kararlarınca sabittir³⁶¹. Bu tür durumlarda Yüksek Mahkemece incelenen hususlardan biri iş bu e-posta iletişiminin mesai saatleri içerisinde gerçekleşip gerçekleşmediğidir. Mesai saatleri içerisinde ve şahsi amaçlarla gerçekleşiyorsa işi savaçlama olarak nitelendirilebilecekken, e-posta iletişiminin

³⁶⁰ Yargıtay 22. HD. E.2017/21857, K.2019/9884, T.07.05.2019, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³⁶¹ Yargıtay 9. HD. E.2016/14205, K.2017/9526, T.01.06.2017, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

mesai saatleri dışında gerçekleşmesi halinde işverenin bu iletişimi gözetlemesinde herhangi bir menfaati bulunmadığı gibi, söz konusu kişisel verilerin işlenmesi faaliyetinde herhangi bir hukuka uygunluk sebebi de mevcut değildir.

Bir diğer husus ise işçilere, e-postalarının inceleneyeğine veya gözetleneceğine dair bilgilendirmenin yapıp yapılmadığıdır³⁶². Anayasa Mahkemesi'ne yapılan bir başvuruda, başvuru işçinin e-posta hesabının işverence incelenmesi dolayısıyla özel hayata saygı hakkı kapsamındaki kişisel verilerinin korunması isteme hakkı ve haberleşme hürriyetinin ihlal edildiğini iddia etmiştir. Anayasa Mahkemesi, işveren tarafından işçiye e-postalarının gözetleneceğine dair herhangi bir bildirim yapılmadığını tespit etmiş ve makul gizlilik beklentisinin korunması gerektiği sonucuna vararak başvuru kabul etmiştir³⁶³.

İşçilerin telefon görüşmelerinin işveren tarafından dinlenip kaydedilmesi hem hukuki hem de cezai bakımdan incelenmesi gereken bir husustur. İşçilerin sesi ve telefon görüşmelerinde bahsettikleri bilgiler kişisel veri niteliğinde olduğundan işlenmeleri için açık rızanın veya hukuka uygunluk sebebinin bulunması gerekmektedir. Fakat, kişilerin telefonlarının dinlenmesi ağır bir kişilik hakkı ihlali olduğundan gereklilik ve ölçülülük konusunda inceleme yapılması gerekir. Zira, kişilerin telefon görüşmelerin kaydedilmesi TCK'nın 134. maddesinde bir suç olarak düzenlenmiştir. Bu durumda bir ayırım yapılmalıdır. Eğer işyerinde yalnızca iş amaçlı telefon görüşmelerinin yapılacağı iş sözleşmelerinde işyeri kuralları altında belirlenmişse, işçilerin telefonda konuştukları hususlar yalnızca iş ile alakalı olması gerektiğinden dinlenilmesi halinde özel hayatın gizliliğini ihlal etmemesi gerekmektedir. Dolayısıyla aydınlatma yükümlülüğü ile diğer temel ilkelere riayet ederek telefon görüşmelerinin dinlenmesi ve kaydedilmesi hukuka aykırılık teşkil etmeyecektir. Ancak işyerinde özel amaçlı telefon kullanımlarına belli oranda izin verilmekteyse, yalnızca işçilerin kiminle konuştuğu ve ne kadar süre konuştuğu gibi bilgilerin kaydedilmesi hukuka uygun olacaktır. Konuşmanın içeriğine ilişkin bilgilere erişip işbu bilgilerin kaydedilmesi hukuka aykırılık teşkil edecektir.³⁶⁴

³⁶² Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 387.

³⁶³ AYM B.N.2016/13010, T.17.09.2020, *T.C. Resmi Gazete*, Sayı: 31274, 14 Ekim 2020 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 15.01.2022)

³⁶⁴ Beytar, E., (2018), s. 196.

5.4 İş Sözleşmesi Sona Erdiğinde İşçilerin Kişisel Verilerinin Korunması

İşverenin işçilerin kişisel verilerini işlemesi faaliyeti işçinin iş akdinin sonlanmasıyla sona ermemektedir. Örneğin, Sosyal Güvenlik Kanunu³⁶⁵'nin 86. maddesi uyarınca işverenlere işyeri defter, kayıt ve bilgilerin 10 yıl boyunca saklanmasına ilişkin bir yükümlülük yüklemiştir. İşverenin kamu olması durumunda bu süre 30 yıl olmaktadır. Maddenin devamında Sosyal Güvenlik Kurumu'nun bir talebiyle söz konusu kayıtları 15 gün içerisinde Kurum'a aktarmak zorunluluğu düzenlenmiştir. Yine İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği'nin 7. maddesinde eski işverene, işçinin yeni işverene işçiye ait kişisel sağlık dosyası 1 ay içerisinde gönderilmesi yükümlülüğü öngörülmüştür. Aynı madde uyarınca yeni işveren talep etmese dahi, dosyanın eski işverence işçinin işten ayrılma tarihinin takip eden 15 yıl boyunca saklanması yükümlülüğü mevcuttur. İş Kanunu'nda da 28. madde uyarınca işçinin işten ayrılması halinde yeni işverene ibraz edilmek üzere işçinin iş çeşidini ve süresini belirtir bir çalışma belgesi düzenlemesi gerekmektedir. Bu saklama ve üçüncü kişilere aktarma faaliyetlerinin hepsi KVKK m. 3 uyarınca kişisel verilerin işlenmesi faaliyetidir.

Uygulamada en çok görülen durumlardan biri yeni işverenin, eski işverene işçi ya da işçi aday hakkında sorular sormasıdır. İş sözleşmesinin sonlanmış olması, işçilerin kişisel verilerinin korunmayacağı anlamına gelmez. Öncelikle iş sözleşmesi bittiğinde, işverenin işçinin bazı bilgilerini işleme amacı kalmadığından söz konusu bazı bilgilerin KVKK m. 7 uyarınca silinmesi, yok edilmesi ya da anonim hale getirilmesi gerekecektir. İşverenlerin kanuni yükümlülüklerini yerine getirmek amacıyla bünyesinde sakladığı eski işçisine ait kişisel veriler de KVKK'nın 12. maddesinin 4. fıkrasındaki açık hüküm uyarınca veri sorumlusu görevlerinin bitmesinden sonra dahi başkalarına açıklanamaz. Yeni işveren, aday işçinin rızası bulunmadan yalnızca eski işveren tarafından verilecek bir çalışma belgesi suretiyle aday işçi hakkında bilgi alabilir. Belgenin ibraz edilmesi gereken sürede ibraz edilmemesi veya yanlış bilgiler içermesi durumunda yeni işverenin eski işverenden tazminat talep edebileceği öngörülmüştür³⁶⁶. Söz konusu belgenin eksik verilmesi sonucunda işçi bir zarara uğruyorsa bu zararını, her ne kadar eski işvereniyle

³⁶⁵ 5510 sayılı Sosyal Güvenlik ve Genel Sağlık Sigortası Kanunu, *T.C. Resmi Gazete*, Sayı: 26200, 16 Haziran 2006 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

³⁶⁶ Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 718.

arasındaki borç ilişkisi bitmiş olsa da sözleşmeye aykırılık hükümleri uyarınca eski işverenden talep edebilmektedir³⁶⁷.

Dolayısıyla iş akdi sona ermiş bir işçiye ait kişisel verilerin saklanması kanuni yükümlülüklerin yerine getirilmesi amacıyla hukuka uygunluk sebebi dahilinde mümkündür. Aynı şekilde kanunen yetkili üçüncü kişilere aktarım da yukarıda bahsetmiş olduğumuz kanun maddeleri uyarınca kanuni yükümlülük kapsamında hukuka uygun olmaktadır. Ancak herhangi bir hukuka uygunluk sebebi taşımayan aktarım ve saklama faaliyetlerinin hukuka uygun şekilde yapılabilmesi için işçinin açık rızası gereklidir. Bu halde işçinin açık rızasının da alınmaması; saklama ve aktarma faaliyetlerinin işçinin kişisel verilerinin korunması hakkını ihlal ettiği anlamına gelir.

5.5 İşçilere Ait Kişisel Verilerin Hukuka Aykırı İşlenmesinin Yaptırımları

İşçilerin kişisel verilerinin hukuka aykırı işlenmesi suretiyle işverenlerine karşı hak ve taleplerde bulunma imkânı mevcuttur. Bu hak ve taleplerin yanında gerek Kurul'a gerekse savcılığa şikâyet yoluyla veri sorumlusu işveren hakkında idari ve cezai yaptırım uygulanması mümkündür.

İdari boyutta baktığımız zaman, Kişisel Verilerin Korunması Kanunu'nun 17. maddesinde kanundan doğan yükümlülüklerin yerine getirilmemesi durumunda veri sorumluları hakkında idari para cezaları uygulanması öngörülmüştür. Bu yükümlülükler 10. maddede düzenlenen veri sorumluların aydınlatma yükümlülüğü, 12. maddede düzenlenen veri güvenliğine ilişkin yükümlülükler, 15. maddede düzenlenen veri sorumlusunu şikâyet edilmesi üzerine verilen Kurul kararlarının yerine getirilmesi yükümlülüğü ve 16. maddede düzenlenen Veri Sorumluları Sicili'ne kayıt yükümlülüğüdür³⁶⁸.

Kişisel verilerin korunmasına ilişkin bir başka idari yaptırım da İş Kanunu'nda öngörülmüştür. İşverenler, işçilerinin kişisel verilerin işlenmesinin kanuni yükümlülüğünü düzenleyen 75. maddesi uyarınca işyeri özlük dosyası hazırlamakla yükümlü olup, işbu yükümlülüğün yerine getirmeyen işverenlere İş Kanunu'nun 104.

³⁶⁷ Yargıtay 9. HD. E.2008/17637, K.2010/6143, T.08.03.2010, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

³⁶⁸ Toprak, B., (2018), s. 117-118.

maddesi uyarınca 4.173,00-TL idari para cezası (2022 yılı için) uygulanacağı düzenlenmektedir. Yine İş Kanunu'nda 28. madde uyarınca çalışma belgesi düzenleme ve yeni işverene ibraz etme yükümlülüğüne aykırılık halinde İş Kanunu m. 99 uyarınca çalışma belgesine ilişkin yükümlülüğün yerine getirilmediği her işçi başına 397,00-TL idari para cezası (2022 yılı için) öngörülmüştür. KVKK'da belirlenen ceza miktarının bu denli yüksek olmasına karşın, İş Kanunu'nda belirlenen idari para cezalarının oldukça az miktarda olması eleştiri konusu olmaktadır³⁶⁹.

Cezai boyutta, Türk Ceza Kanunu'nun 132. ile 138. maddeleri arasında kişisel verilerin korunması ve özel hayatın gizliliğinin ihlaline ilişkin suçlar düzenlenmiştir. Zira KVKK'nın suçlar başlıklı 17. maddesi de Türk Ceza Kanunu'nun söz konusu maddelerine atıf yapılmaktadır. Kişisel verilerin hukuka aykırı işlenmesi dolayısıyla suç olarak düzenlenen fiiller; haberleşmenin gizliliğinin ihlal edilmesi, kişiler arasında aleni olmayan konuşmaların hukuka uygunluk sebebi bulunmadan dinlenmesi ve kaydedilmesi, özel hayatın gizliliğinin ihlal edilmesi, kişisel verilerin hukuka aykırı olarak kaydedilmesi, üçüncü kişilere aktarılması, ele geçirilmesi, kanunların belirlediği sürelerin geçmiş olmasına rağmen kişisel verilerin yok edilmemesi olarak belirtilmiştir³⁷⁰.

Kişisel verilere ilişkin suçlarda suçtan zarar görülmesi şartı aranmamaktadır. Suça konu fiilin, hukuka aykırı yollarla gerçekleşmiş olması yeterlidir. Tartışılan bir diğer husus ise, veri işleyen mi veri sorumlusunun mu söz konusu suçlardan cezai bakımdan sorumlu olacağıdır. Veri işleyen, veri işleme faaliyetini veri sorumlusu adına gerçekleştirmektedir. Ancak Kanun kapsamında yükümlülükler bakımından müşterek ve müteselsil sorumlu tutulmuşlardır. Bu doğrultuda, hukuka aykırı yollarla TCK m. 132-138'de düzenlenen suçlardan birinin işlenmesi halinde her ikisinin de sorumlu olacağını söyleyebiliriz. Ancak cezaların şahsiliği ilkesi gereği, bir taraf söz konusu suçun gerçekleşmemesi için gereken her şeyi yaptığını ve tüm tedbir ve önlemleri aldığını, yani kusurunun bulunmadığını ispatlarsa sorumluluktan kurtulabilecektir³⁷¹.

³⁶⁹ Gürsel, İ., (2016), s. 427-428.

³⁷⁰ Belge, A. M. (2017) *Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlali Ve Korunması Yolları*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 19(Özel Sayı), s. 1043-1044.

³⁷¹ Toprak, B., (2018), s. 119.

Uygulamada hukuki boyutta da işverenler, kişisel verileri hukuka aykırı işlemleri halinde birçok yaptırımla karşılaşabilmektedir. Kişisel verilerin korunması hakkı bir kişilik hakkı olduğundan Türk Medeni Kanunu'nun 25. maddesinin sağladığı korumaya tabidir. Hükme göre bir şahsın kişilik haklarına bir saldırı olması durumunda kişiler bu saldırının durdurulmasını mahkemeden talep edebilirler. Dolayısıyla işçiler, verilerinin veri sorumlusu işveren tarafından herhangi bir hukuka uygunluk sebebi bulunmadan işlenmesi durumunda bu işleme faaliyetinin durdurulmasını isteyebilecektir. Hükümün devamında ise saldırının durdurulmuş olması ancak etkilerinin devam ediyor olması halinde saldırının hukuka aykırılığının tespiti mümkün kılınmıştır.

KVKK'nın 11. maddesi zarar gören veri sahibinin veri sorumlusuna karşı zararın giderilmesini talep edebileceğini öngörmüştür. Benzer sonuca TMK'nın 25. maddesi ve akabinde Türk Borçlar Kanunu'nun 49. ve 56. maddelerindeki hükümlerle de ulaşmak mümkündür. Kişisel verileri ihlal edilen işçiler uğradıkları zarar için maddi tazminat davası açabilir. Zira işveren ile işçi arasında bir sözleşme bulunduğundan TBK m. 417 uyarınca gözetme borcuna aykırılıktan sözleşme hükümleri uygulanabilecektir. Bu durumda öğrenildikten itibaren iki senelik, her halde on senelik zamanaşımına tabi olan zararın giderilmesi talebi, sözleşmeye aykırılık dolayısıyla on yıllık zamanaşımına tabi olacaktır. Kişisel verilerin korunması hakkı bir kişilik hakkı olduğundan, manevi tazminat davasının konusunu oluşturabilir. TBK m. 58 uyarınca manevi zarara uğrayan işçinin bu zararının giderilmesi için mahkeme uygun bir miktar paranın manevi tazminat adı altında işçiye ödenmesine karar verebilir. Bu hükümden yola çıkarak, mahkeme tarafından verilecek tazminat şeklinin para olmayacağını; bir özür, saldırıyı kınama, işbu özür ve kınamanın açıklanması gibi tazminat şekilleri de öngörebileceğini söyleyebiliriz³⁷².

İşçilerin kişisel verilerinin hukuka aykırı işlenmesinin, işverenin işçiyi gözetme borcunun ihlalini oluşturacağından bahsedilmiştir. Uygulamada işveren tarafından işçilerin hukuka aykırı şekilde kişisel verilerinin işlenmesinin işçilerin iş ahdini feshetmesi için haklı sebep oluşturduğu kabul edilir. Her ne kadar İş Kanunu'nun işçilerin derhal fesih hakkını düzenleyen 24. maddesinde kişisel verilerin işverence ihlali hususunda bir düzenleme yer almasa da; 24. maddenin 2. kısmı fesih

³⁷² Toprak, B., (2018), s. 120-123.

sebeplerinden “*ahlak ve iyiniyet kurallarına uymayan haller ve benzerleri*”ni düzenlediğinden ve işçinin kişisel verilerinin işveren tarafından hukuka aykırı işlenmesi bu benzer durumlar kapsamında bulunduğundan, işçiler böyle bir durumda iş akitlerine haklı sebeple son verebilme hakkına sahiptir³⁷³.

Kişisel verilerin işlenmesinin işveren tarafından hukuka aykırı biçimde gerçekleştirilmesi, her zaman İş Kanunu m. 24/2’de belirtilen “*ahlak ve iyiniyet kurallarına uymayan haller*”in benzerlerini teşkil etmek zorunda değildir. Kimi zaman, verinin türüne de bağlı olarak ahlak ve iyiniyet kurallarına uymayan hallerden birini de teşkil edebilmektedir.

Örnekle açıklamak gerekirse, veri sorumlusu işverenin işçisine ait kişisel verileri işleme halinde işçinin bu işleme faaliyetine ilişkin bilgi alma hakkı mevcuttur. İşverenin işçinin bu talebine karşın işçiye yanlış bilgi vermesi, hem işverenin aydınlatma yükümlülüğünü ihlal etmesi, hem de İş Kanunu m. 24/2-a maddesi uyarınca “*işçiye gerçeğe uygun olmaya bilgiler veya sözler söylemek suretiyle işçiyi yanıltması*” sonucunu doğuracaktır³⁷⁴.

Bir başka örnek, işverenin işçisine karşı kişisel verilere ilişkin bir suç işlemesidir. İşveren, İş Kanunu m. 75 uyarınca işçisi hakkında işyeri özlük dosyası oluşturmakla mükellef bulunup, işyeri özlük dosyaları içerikleri gereği özel nitelikli veri barındırmaktadır. İşverenin, işçinin işyeri özlük dosyasında bulunan ve açığa çıkarılması halinde işçinin aleyhine durum oluşturacak nitelikte bir verisini sosyal medya platformunda paylaşması TCK m. 136 uyarınca “*verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi*” suçunu oluşturur. Bu durumda işçi iş akdini, İş Kanunu m. 25/2-c’de düzenlenen “*işçiye ve ailesi üyelerinden birine karşı hapsi gerektiren bir suç işlemeye*” gerekçesine dayanarak haklı nedenle feshedebilir³⁷⁵.

Dolayısıyla, örneklerden de anlaşıldığı üzere; işçinin kişisel verilerinin ihlal edilmesi, hükümdeki “*ve benzeri*” ibaresine gerek olmaksızın, ahlak ve iyiniyet kurallarına uymayan haller kapsamına girebilmektedir.

³⁷³ Belge, A. M., (2017), s. 1046.; Çelik, N., Caniklioğlu, N., Canbolat, T. ve Özkaraca, E., (2021), s. 412.

³⁷⁴ Toprak, B., (2018), s. 116.

³⁷⁵ Gürsel, İ., (2016), s. 425.

Kişisel verilerin ihlali dolayısıyla “*ahlak ve iyiniyet kurallarına uymayan haller*” gerekçesiyle işçiye tanınan haklı sebeple fesih, İş Kanunu’nun 26. maddesi uyarınca derhal fesih hakkıdır ve işçi bu hakkını madde gereğince ihlali öğrendikten sonra 6 iş günü içerisinde, her halde 1 yıl içerisinde kullanmak zorundadır. Bu süreler geçtikten sonra işçi tarafında yapılacak fesih, hak düşürücü süre içerisinde derhal fesih hakkı kullanılmadığından haksız fesih hükmünde olacaktır³⁷⁶.

Derhal fesih haklarını kullanan işçiler, bu hakları süresi içerisinde kullandıklarında İş Kanunu m. 26/2 ve TBK m. 437 uyarınca uğradıkları zararın tazminini işverenlerinden talep etme haklarına sahiptir. İşçilerin bu hükme göre talep edebileceği tazminat, TBK m. 49 ve KVKK m. 11/1-ğ talep edebildikleri tazminat ile karıştırılmamalıdır. TBK m. 49 ve KVKK m. 11/1-ğ hükümlerinde öngörülen tazminat, veri sahibinin kişisel verilerinin ihlali sonucu oluşan zararının giderilmesine ilişkindir. Halbuki, İş Kanunu m. 26/2’de belirtilen tazminat, işçinin iş sözleşmesini haklı nedenle feshetmek zorunda kalması sonucu oluşan zararının giderilmesine ilişkindir. Bu doğrultuda, işçilerin kişisel verilerinin ihlali sonucu uğradıkları zararın tazminini talep hakları, İş Kanunu m. 26/1’de öngörülen hak düşürücü süreye tabi olmayacaktır³⁷⁷.

Uygulamada çoğunlukla, işverenler tarafından kişisel verilerin korunması haklarının ihlal edilmesi sonucu işçilerin iş akitlerine son verilmektedir. İşçilerin, işveren tarafında hukuka aykırı şekilde elde edilen kişisel verileri gerekçe gösterilerek iş akitlerinin feshedilmesi durumunda; HMK. m. 189/2 uyarınca hukuka aykırı elde edilen deliller bir vakıanın ispatı için kullanılamayacağından iş akdinin feshi geçersiz olmaktadır. Bu noktada işçiler İş Kanunu’nun 21. maddesi uyarınca işe iade ve bununla birlikte boşa geçen süre ücretlerini talep edebilmektedirler³⁷⁸. Yargıtay’ın konu ile ilgili bir kararında³⁷⁹, satış temsilcili olarak çalışan bir işçinin Whatsapp uygulamasında işyeri ve işyeri yöneticileri hakkında terbiye sınırlarını aşan beyanlarda bulunduğu gerekçesiyle işten çıkarılması söz konusudur. Yargıtay, davalı işverenin işçiye ait Whatsapp konuşmalarını hukuka aykırı yollarla elde ettiği gerekçesiyle bu

³⁷⁶ Süzek, S., (2021), s. 726-727.

³⁷⁷ Uncular, S. (2012). *İş İlişkisinde İşçilerin Kişisel Verilerinin Korunması*. Yüksek Lisans Tezi, Galatasaray Üniversitesi, s. 109.

³⁷⁸ Yücel, O. Ü. (2018). *İşçilerin Sosyal Medya Paylaşımalarının İşveren Tarafından Denetimi Ve İş İlişkisine Etkisi*. Yüksek Lisans Tezi, Ankara Üniversitesi, s. 84.

³⁷⁹ Yargıtay 9. HD. E.2016/14203, K.2017/9524, T.01.06.2017, Kazancı [Çevrimiçi]. Erişim Adresi: <http://www.kazanci.com> (Erişim Tarihi: 15.01.2022)

konuřmaları caiz delil niteliğinde bulmamıř ve davacı iřçinin yapmıř olduđu temyiz bařvurusunu kabul ederek iře iadeye karar vermiřtir.



BÖLÜM 6: SONUÇ

Kişisel veriler, kimliği belirli ya da belirlenebilir kişilere ait her türlü bilgiyi ifade etmektedir. Şahısların kişisel verileri Anayasa'nın 20/3 maddesinde düzenlenen kişisel verilerin korunmasına hakkının konusunu oluşturmakta olup, verilerin hepsi bu korumaya tabidir. Kişisel veriler türlerine göre normal nitelikli veriler ile özel nitelikli veriler olarak ayrılmaktadır. Özel nitelikli veriler, kişilerin sağlığı, ırkı, dini, felsefi inancı, siyasi görüşleri, dernek, vakıf veya sendika üyeliği, cinsel tercihlerine ilişkin veriler olup, bu veriler Kanun'da sayılanlarla sınırlı değildir. Genel olarak, açığa çıkmaları veya başkalarının erişim sağlaması halinde veri sahibi ayrımcılığa maruz kalmak gibi aleyhe sonuçlarla karşılaşacaksa, söz konusu veriler özel nitelikli verilerdir. Özel nitelikli veriler Kanun'da diğer kişisel verilerden daha sıkı bir korumaya tabidir.

Bu verilerle yapılan toplama, saklama, depolama, aktarma, silme, yok etme gibi işlemlerin hepsi kişisel verilerin işlenmesi faaliyetini oluşturmaktadır. İşleme faaliyeti KVKK'da düzenlenen ilkelere riayet etmezse ve belirlenen usullerde gerçekleştirilmezse verilerin hukuka aykırı işlenmesi sonucunu doğuracaktır. Bu ilkeler KVKK'nın 4. maddesinde düzenlenmektedir. Maddeye göre işleme faaliyeti, hukuka ve dürüstlük kurallarına uygun; doğru ve gerektiğinde güncel; belirli, açık ve meşru amaçlar için; mevzu bahis amaçla bağlantılı, sınırlı ve ölçülü olmalı ve ilgili mevzuatta öngörülen ve işlendikleri amaç için gerekli süre boyunca işlenmelidir. KVKK'nın 5. maddesinde kural olarak kişisel verilerin açık rıza olmadan işlenemeyeceği öngörülmüştür. Maddenin devamında kişilerin açık rızası olmaksızın verilerinin işlenebileceği hukuka uygunluk sebepleri düzenlenmiştir. Bu hukuka uygunluk sebeplerinin varlığı durumunda veri sorumlularının ilgili kişi veri sahiplerinden açık rıza almamaları gerekmektedir. İşleme faaliyetinin hukuka uygunluk sebebi mevcutken açık rızaya dayandırılması, temel ilkelerden dürüstlük kurallarına uygunluk ilkesinin ihlalini oluşturacağından kişisel verilerin hukuka aykırı şekilde işlenmesi sonucunu doğuracaktır.

Bununla birlikte, işleme faaliyetinin hukuka uygun bir şekilde gerçekleştirilebilmesi için açık rızanın ya da herhangi bir hukuka uygunluk sebebinin bulunması yeterli olmamaktadır. İşleme faaliyetinin bağlı kalması gereken temel ilkeler ve veri sorumlusunun yerine getirmesi gerektiği yükümlülükleri mevcuttur. Bu

yükümlülüklerden ilki veri sorumlusunun aydınlatma yükümlülüğüdür. Veri sorumlusu, veri sahiplerinin kişisel verilerini toplarken veri toplamasındaki amaç, yöntem, bu verileri aktarılacağı üçüncü kişiler, veri sahibinin sahip olduğu haklar gibi bilgiler ile veri sahibini bilgilendirmek zorundadır. Aksi takdirde verilerin elde edilmesi hukuka aykırı olacağından bu noktadan sonra yapılacak tüm işleme faaliyetleri de hukuka aykırılık teşkil edecektir. Bir diğer yükümlülük veri sahibinin veri güvenliğini sağlamasına ilişkindir. Veri sorumlusu, veri sahibinin kişisel verilerinin hukuka aykırı olarak işlenmesini ve erişilmesi önlemekle yükümlü olup, bu yükümlülüğü yerine getirmek için gereken tüm idari ve teknik tedbirleri sağlamak zorundadır. Bu tedbirlerin alınması konusunda, veri işleyen ve veri sorumlusunun farklı kişiler olması durumunda her ikisinin müşterek ve müteselsil sorumluluğu mevcuttur. Veri sorumlusu ihlal gerçekleştiğinde, ihlali ilgili kişi veri sahibine ve Kurul'a ivedilikle bildirmekle yükümlüdür. Kişisel verilerin işlenmesini takip edebilmek adına 08.04.2018 tarihli ve 2018/32 Karar numaralı Kurul Kararı'nda belirtilenler dışında tüm veri sorumlularının Veri Sorumluları Sicili'ne kayıt yükümlülüğü bulunmaktadır.

Veri sorumlularının yükümlülüklerini yanında Kanun'da ilgili kişi veri sahiplerinin bazı hakları da düzenlenmektedir. KVKK m. 11 uyarınca ilgili kişilerin verilerinin işlenmesi hakkında bilgi edinme, verilerinin silinmesini, yok edilmesini veya anonim hale getirilmesini talep etme, işlenen verilerinin kendi aleyhine sonuç doğurması halinde bu sonuca itiraz etme ve işleme faaliyetinin kendisini zarara uğratması halinde bu zararın tazminini talep etmek hakları mevcuttur. İlgili kişi bu taleplerini veri sorumlusuna başvuru yoluyla iletir. Bu başvuru sonucunda otuz gün içerisinde talebinin sonucuyla ilgili geri dönüş almazsa veya olumsuz ya da yetersiz bir cevap alırsa, ilgili kişi veri sorumlusunu Kurul'a şikayet edebilir.

Kişisel verilerin açık rıza olmaksızın yurtdışına aktarımı hususunda Kanun'un 5/2 ve 6/3 maddelerinde belirlenen hukuka uygunluk sebeplerinin yanında, aktarım yapılacak ülkenin yeterli korumaya sahip olması şartının arandığından bahsedilmiştir. İlgili maddenin devamında yeterli korumanın kriterlerinden bahsedilmiş olup, son fıkrasında yeterli korumaya sahip ülkelerin Kurul tarafından ilan edileceği düzenlenmiştir. Lakin, Kişisel Verileri Koruma Kurumu'nun resmî sitesinde bu hususa dair Kurul tarafından henüz bir belirleme yapılmadığına ilişkin bildiri mevcuttur. Kişisel Verilerin Korunması Kanunu'nun 2016 yılında yürürlüğe girmiş olmasına ve

o yıldan beri uygulanmasına rağmen hala Kurulca yeterli korumanın bulunduğu ülkelerin ilan edilmemesi kanımızca oldukça büyük bir eksiklik. Zira Kanun'un yürürlüğe girmesinden bu yana kişisel verilerin yurtdışına aktarımı gerçekleşmekte olup; Kurul'un herhangi bir belirlemede bulunmaması, bu kişisel veri aktarımlarına ilişkin tehlike yaratmaktadır. Kurul'un yeterli korumaya sahip ülkeleri ilan etmesi, şu ana kadar bu ülkeler dışındaki ülkelere yapılan bütün aktarımları hukuka aykırı hale getirecektir. Bu nedenle Kurul tarafından yabancı ülkelerin veri koruma hukuku düzenlemeleri ivedilikle incelenmeli ve yeterli korumanın bulunduğu ülkeler tespit edilmelidir.

İşçilerin kişisel verilerin korunması, işverenin işçisini gözetme borcu kapsamında bulunan bir yükümlülüğüdür. Bu yükümlülük halihazırda iş sözleşmesi bulunan işçilere uygulanacağı gibi, henüz iş ilişkisi kurulmamış aday işçiler ve iş sözleşmesi bitmiş ve işten ayrılmış olan işçiler için de geçerlidir. Zira işleme faaliyeti, aday işçilerin işe başvurusuyla başlamaktadır. Aday işçinin iletmiş olduğu evraklarda bulunan verilerini işleyen işverenler bu süreci hukuka uygun yürütmekle mükelleftir. Aday işçilere amaç dışında sorular sormaması, yalnızca yapılacak işin niteliği ile ilgili ve gerekli soruları sorması gerekmektedir. Aday işçilerin işe alınmaması halinde onlara ait tüm verilerin KVKK m. 7 uyarınca verilerin işlenmesini gerektiren sebeplerin ortadan kalkması nedeniyle yok edilmesi gerekmektedir. İşleme faaliyeti işçinin işten ayrılması ile sona ermemektedir. İşvereni, işten ayrılmış işçinin kayıtlarını belirli süre tutmakla yükümlü bırakan kanuni düzenlemeler mevcuttur. Dolayısıyla işçilerin verileri, işten ayrılmalarına rağmen işleme faaliyetlerine konu olmaktadır. İşverenlerin, işten ayrılmış işçilere ait kayıtları İş mevzuatı uyarınca 10 yıl, Sosyal Güvenlik mevzuatı uyarınca 15 yıl boyunca saklama yükümlülüğü bulunmaktadır. Veri güvenliği ilkesi gereği işverenlerin bu verileri muhafaza etmesi ve üçüncü kişilerin hukuka aykırı erişimlerin korunması gerekmektedir. Görüldüğü üzere, işçilerin kişisel verilerinin korunması işin süresi ile sınırlı değildir.

Uygulamada işyerlerinde yüz, retina, parmak izi okuma sistemleri gibi biyometrik sistemlerle ve araç takip sistemleriyle mesai takibinin yapıldığı görülmektedir. İşçinin iş sözleşmesinde bu sistemlerle kişisel verilerinin işleneceğine muvafakat verdiği dair hüküm bulunması açık rıza yerine geçmemelidir. Zira, işçiler işe girmek adına bu düzenlemeleri kabul ettiklerinden ötürü kişisel verilerinin işlenmesine rıza gösterdiklerine ilişkin irade beyanlarında sakatlık mevcuttur. Bu

uygulamaların yapılabilmesi için gerekli açık rızanın, işçilerin işe alındıktan sonra işçilerden istenmesi gerekmektedir. Ayrıca işçilere, açık rıza vermedikleri halde aleyhe sonuç doğmayacağı güvencesi verilmelidir. Böylece, halihazırda işe başlamış olan işçi hiç baskı olmaksızın özgür iradesiyle geçerli bir rıza verebilecektir. Ne var ki, işçilerin açık rızasının bulunması işveren tarafından gerçekleştirilen işleme faaliyetini her zaman hukuka uygun hale getirmemektedir. Kişisel verilerin işlenmesi faaliyeti aynı zamanda KVKK m. 4'te düzenlenen temel ilkeler doğrultusunda gerçekleştirilmelidir. Mesai takibinin, işçilerin özel hayatın gizliliği hürriyetlerine daha az müdahale eden bir yöntemle gerçekleştirilmesi mümkünse o yöntem tercih edilmelidir. Aksi takdirde işleme faaliyeti amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil ettiği için hukuka aykırı olacaktır.

Uyuşmazlıkların geneli, işçilerin kişisel verilerinin işverenler tarafından hukuka aykırı elde edilmesi sonucu çeşitli yaptırımlara tabi tutulmalarından ve hatta iş akitlerine son verilmelerinden kaynaklanmaktadır. İşçilerin bu durum karşısında başvurabileceği hukuki yollar ve işverenlerine karşı ileri sürebileceği hak ve talepler mevcuttur. Ancak bu hak ve talepler işçinin kişisel verilerinin ihlal edilmesinden sonra gündeme gelmekte ve bu nedenle tazmin niteliğindedir. Önleyici yaptırımlar olarak KVKK ve İş Kanunu'nda idari para cezaları öngörülmüştür. Lakin, İş Kanunu'nda öngörülen para cezaları çok cüzi meblağlar olduğundan önleyici vasfı taşımamaktadır. KVKK uyarınca öngörülen idari para cezaları çoğu zaman işçiler tarafından bilinmemekte ve dolayısıyla bu yol tercih edilmemektedir.

Tüm bilgiler ışığında, kanımızca işçilerin kişisel verilerinin hukuka aykırı biçimde işlenmesinin önlenmesi için İş Kanunu'ndaki para cezalarının miktarlarının tekrardan düzenlenmesi ve artırılması gerektiği görüşündeyiz. Uygulamaların (parmak izi, araç takip sistemi, üst araması) hangi koşullar altında hukuka uygun olup olmadıkları spesifik olarak belirlenmeli ve içtihat hukukunda yeknesaklık sağlanmalıdır. Zira teknolojinin gelişmesiyle birlikte sürekli yeni denetim mekanizmaları ve bundan kaynaklanan yeni kişisel verilerin işlenmesi yolları oluşmaktadır. Gerekirse bu uygulamalar İş Kanunu'na aktararak usulleri tespit edilmeli veya bu uygulamalara özgü yönetmelikle ve tebliğler hazırlanmalıdır. İşçilere kişisel verilerin korunmasına ilişkin eğitimler verilerek sahip oldukları haklar konusunda bilgilendirilmelidir. Kurul tarafından verilerin idari para cezaları çok daha yüksek miktarlarda olduğundan işverenler üzerinde daha etkili olacak yaptırımlardır.

Ancak Kurul'a şikayet yolunun işçiler tarafından bilinmemesi bu yaptırımları işlerliğini azalmaktadır. Bu husus işçilere verilecek olan eğitimlerle çözülebilir, ancak tek başına yeterli olmayacaktır. Kurul'un denetim mekanizması geliştirilerek işverenlerin işçilerin verilerini işlerken daha hassas ve dikkatli davranması sağlanmalıdır. Veri sorumluları Sicili'ne kaydolmayan işyerleri tespit edilmeli ve veri sorumlularının VERBİS sistemine işlemekte oldukları kişisel verilerle ilgili kategorik bazda yaptıkları bilgi girişleri denetime tabi tutulmalıdır. Bu şekilde kişisel verilerin ihlalleri şikayet yoluna gerek kalmaksızın re'sen Kurul tarafından da tespit edilip, işverenlere verilecek olan yüksek miktarda idari para cezalarıyla başka ihlallerin önüne geçilebilir. Bütün bu hususlar yerine getirildiğinde kişisel verilere ilişkin ihlallerin azalacağı kanaatindeyiz.



KAYNAKÇA

Akkurt, S. S. (2016) *17.06. 2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı Ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı"*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 65(4), ss. 2605-2635.

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

Aksoy, H. C. (2010) *Medeni Hukuk Ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*. İnci Bası. Ankara: Çakmak Yayınevi.

Article 29 Working Party. (2014). *Opinion 06/2014 On The "Notion Of Legitimate Interests Of The Data Controller Under Article 7 Of Directive 95/46/EC* [Çevrimiçi]. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (Erişim Tarihi: 09.12.2021).

Avcı, Y. (2019). *Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, Selçuk Üniversitesi.

Baskın, O. (2020). *Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, Bahçeşehir Üniversitesi.

Belge, A. M. (2017) *Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlali Ve Korunması Yolları*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 19(Özel Sayı), ss. 1025-1051.

Beytar, E. (2018) *İşçinin Kişiliğinin Ve Kişisel Verilerinin Korunması*. İnci Bası. İstanbul: On İki Levha Yayıncılık

Council Of Europe, (1995). *Assembleia Da República [Portuguese Parliament] Act 67/98 Of 26 October* [Çevrimiçi]. Erişim adresi: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af2ea> (Erişim Tarihi: 03.11.2021).

Council Of Europe, (2000). *The Data Protection Act - Act On The Protection Of Privacy As Regards The Processing Of Personal Data, No. 77/2000* [Çevrimiçi]. Erişim adresi:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af22f> (Eriřim Tarihi: 03.11.2021).

Çekin, M. S. (2019) *Avrupa Birlięi Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*. 2nci Bası. İstanbul: On İki Levha Yayınları.

Çelik, N., Caniklioęlu, N., Canbolat, T. ve Özkaraca, E. (2021) *İř Hukuku Dersleri*. 34üncü Bası. İstanbul: Beta Yayıncılık.

Deliorman, R. B. ve Kandemir, A. Ü. (2009) *Kamu Kurumu Niteliğinde Meslek Kuruluşları Ve Etik*. Yolsuzluęun Önlenmesi İçin Etik Projesi Akademik Arařtırma Çalışması

Deniz, M. Ö. (2021) *İřçilerin Özel Nitelikli Kişisel Verilerinin Korunması Ve Bundan Doęan Sorumluluk*, Türkiye Adalet Akademisi Dergisi, C. (45), ss. 355-378.

Dictionnaire juridique de Serge Braudo. *Infans Conceptus definition*. Eriřim Adresi: <https://www.dictionnaire-juridique.com/definition/infans-conceptus.php> (Eriřim Tarihi: 10.01.2022).

Dursun, Y. (2019). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İřçinin Korunması*. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi.

EDPB. (2019). *The CNIL's Restricted Committee Imposes A Financial Penalty Of 50 Million Euros Against Google Llc* [Çevrimiçi]. Eriřim adresi: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (Eriřim Tarihi: 22.11.2021).

Elbir, N. (2020). *Kişilięinin Korunması Bağlamında İřçiye Ait Kişisel Verilerin Korunması*. Doktora Tezi, Ankara Üniversitesi.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizlilięinin Korunması Hakkında Yönetmelik, T.C. Resmi Gazete, Sayı: 31324, 4 Aralık 2020 [Çevrimiçi]. Eriřim Adresi: www.resmigazete.gov.tr (Eriřim Tarihi: 27.12.2021)

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

EUR-Lex. (1995). *Document 31995L0046* [Çevrimiçi]. Erişim adresi: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046> (Erişim Tarihi: 03.11.2021).

General Data Protection Regulation. (2018). *Art. 33 GDPR – Notification Of A Personal Data Breach To The Supervisory Authority* [Çevrimiçi]. Erişim adresi: <https://gdpr-info.eu/art-33-gdpr/> (Erişim Tarihi: 11.11.2021).

Gözüm, Z. U. (2019). *Kişisel Verilerin Korunmasının İş İlişkisi Açısından Değerlendirilmesi*. Yüksek Lisans Tezi, Bahçeşehir Üniversitesi.

Gürsel, İ. (2016). *İşçinin Kişisel Verilerinin Korunması Hakkı*. Doktora Tezi, Dokuz Eylül Üniversitesi.

Han, I. A. (2020) *Veri Sahibinin Kişisel Veri Üzerindeki Hakkının Hukuki Niteliği Işığında Kişisel Verinin Ticarileşmesi*. Genç Hukukçu Araştırmacılar Sempozyumu. İstanbul: On İki Levha Yayıncılık, ss. 509-544.

Has, M. (2021) *AİHM Kararları Bağlamında Görüntü Hakkı*, Anayasa Yargısı, C. 38(1), ss. 205-242.

House Of Lords, *Opinions Of The Lords Of Appeal For Judgment In The Cause, 06.05.2004, Campbell (Appellant) v. MGN Limited (Respondents)* [Çevrimiçi], Erişim Adresi: <https://publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm> (Erişim Tarihi: 09.01.2022)

International Committee of the Red Cross. (2002). *The Missing: Action To Resolve The Problem Of People Unaccounted For As A Result Of Armed Conflict Or Internal Violence And To Assist Their Families, The Legal Protection Of Personal Data & Human Remains* [Çevrimiçi]. Erişim adresi: <https://www.icrc.org/en/doc/resources/documents/misc/5callj.htm> (Erişim Tarihi: 20.05.2021).

International Labour Organization. (2001). *Protection Of Workers' Personal Data* [Çevrimiçi]. Erişim adresi: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/--protrav/---safework/documents/normativeinstrument/wcms_107727.pdf (Erişim Tarihi: 13.11.2021).

İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği, T.C. Resmi Gazete, Sayı: 28512, 29 Aralık 2012 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

İşyeri Hekimi ve Diğer Sağlık Personelinin Görev, Yetki, Sorumluluk ve Eğitimleri Hakkında Yönetmelik, T.C. Resmi Gazete, Sayı: 28713, 20 Temmuz 2013 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

Kaplan, E. T. (1997) *İş Hukukunda Kişilik Haklarının Özellikle Bilgisayarda Toplanan Bilgilere Karşı Korunması*, Ankara Üniversitesi SBF Dergisi, C. 52(01). ss. 367-386.

Kaya, C. (2011) *Avrupa Birliği veri koruma direktifi ekseninde hassas (kişisel) veriler ve işlenmesi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 69(1-2), ss. 317-334.

Kaya, M. B. (2021) *Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi*, İstanbul Hukuk Mecmuası, C. 78(4), ss. 1859-1897.

Kişisel Verileri Koruma Kurumu. (2018). *Kişisel Verilerin Korunması Kurulu'nun 08.04.2018 Tarihli ve 2018/32 Karar Numaralı Kararı* [Çevrimiçi]. Erişim adresi: <https://www.resmigazete.gov.tr/eskiler/2018/05/20180515-16.pdf> (Erişim Tarihi: 15.12.2021).

Kişisel Verileri Koruma Kurumu. (2018). *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli Ve 2018/10 Sayılı Kararı* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/4110/2018-10> (Erişim Tarihi: 06.11.2021).

Kişisel Verileri Koruma Kurumu. (2019). *Kişisel Veri İhlali Bildirim Usul Ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararına İlişkin Duyuru* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi> (Erişim Tarihi: 14.12.2021).

Kişisel Verileri Koruma Kurumu. (2019) *Madde Ve Gereğesi İle Kişisel Verilerin*

Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü. Ankara: KVKK Yayınları.

Kişisel Verileri Koruma Kurumu. (2019). *"Veri Sorumlusunun Kanuni Yükümlülüğünü Yerine Getirmek İçin İşlediği Kişisel Verileri Meşru Menfaat Çerçevesinde Kullanma Talebiyle Kuruma Yapmış Olduğu Başvuru" Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli Ve 2019/78 Sayılı Karar Özeti* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/5434/2019-78> (Erişim Tarihi: 09.12.2021).

Kişisel Verileri Koruma Kurumu. (2019). *"Yeterli Korumanın Bulunduğu Ülkelerin Tayininde Kullanılmak Üzere Oluşturulan Form" Hakkındaki 02/05/2019 Tarihli Ve 2019/125 Sayılı Kurul Kararı* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkındaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari> (Erişim Tarihi: 13.12.2021).

Kişisel Verileri Koruma Kurumu. (2020). *Yurtdışına Veri Aktarımı Kamuoyu Duyurusu* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/6828/YURTDISINA-VERI-AKTARIMI-KAMUOYU-DUYURUSU> (Erişim Tarihi: 13.12.2021).

Kişisel Verileri Koruma Kurumu, (2020). *"Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında"* *Kişisel Verileri Koruma Kurulunun 14.01.2020 Tarihli ve 2020/26 Sayılı Karar Özeti* [Çevrimiçi]. Erişim Adresi: <https://www.kvkk.gov.tr/Icerik/6697/2020-26> (Erişim Tarihi: 09.12.2021).

Kişisel Verileri Koruma Kurumu. *6698 Sayılı Kanun'da Yer Alan Temel Kavramlar* [Çevrimiçi]. Erişim adresi: <https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar> (Erişim Tarihi: 20.05.2021).

Kişisel Verileri Koruma Kurumu. *İlgili Kişi Kimdir?* [Çevrimiçi]. Erişim adresi: <https://kvkk.gov.tr/Icerik/2034/Ilgili-Kisi-Kimdir> (Erişim Tarihi: 20.05.2021).

Kişisel Verileri Koruma Kurumu. *Kişisel Verileri Koruma Kurulu'nun Yapısı ve Görevleri* [Çevrimiçi]. Erişim adresi:

<https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0%20KORUMA%20KURULU%E2%80%99NUN%20YAPISI%20VE%20G%C3%96REVLER%C4%B0.pdf> (Eriřim Tarihi: 18.11.2021).

Kiřisel Verileri Koruma Kurumu. *Kiřisel Verilerin İřlenmesi* [Çevrimiçi]. Eriřim adresi: <https://www.kvkk.gov.tr/Icerik/2048/Kisisel-Verilerin-Islenmesi> (Eriřim Tarihi: 06.11.2021).

Kiřisel Verileri Koruma Kurumu. *Veri Sorumlusu Ve Veri İřleyen* [Çevrimiçi]. Ankara. Eriřim adresi: <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen> (Eriřim Tarihi: 07.12.2021).

Kiřisel Verilerin Korunması Platformu. (2016) *Kiřisel Verilerin Otomatik İřleme Tabi Tutulması Karřısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınırşan Veri Akışına İliřkin Protokol (181 Sayılı Ek Protokol)* [Çevrimiçi]. Eriřim adresi: <https://www.kisiselverilerinkorunmasi.org/mevzuat/kisisel-verilerin-otomatik-isleme-tabi-tutulmasi-karsisinda-bireylerin-korunmasi-sozlesmesine-ek-denetleyici-makamlar-ve-sinirasan-veri-akisina-iliskin-protokol-181-sayili-ek-protokol/> (Eriřim Tarihi: 18.11.2021).

Kiřisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik, T.C. Resmi Gazete, Sayı: 30224, 28 Ekim 2017 [Çevrimiçi]. Eriřim Adresi: www.resmigazete.gov.tr (Eriřim Tarihi: 27.12.2021)

Kulevska, S. (2013, Haziran 24) *The Future of Your Past: A Right to be Forgotten Online?*, [Blog yazısı]. Eriřim adresi: https://www.lumendatabase.org/blog_entries/521

Küzeci, E. (2010). *Kiřisel Verilerin Korunması*. Doktora Tezi, Ankara Üniversitesi.

Küzeci, E. (2020) *Kiřisel Verilerin Korunması*, 4üncü Bası, İstanbul: Oniki Levha Yayıncılık

[Leyla Keser] (2016, Kasım 23) *Kiřisel Veriler Kanunu'nun Getirdikleri* [Video Dosyası]. Eriřim adresi: https://www.youtube.com/watch?v=yyMUPZSXtoY&ab_channel=E-Ticaretve%20internetHukukuDerne%20Fi

Manav, E. (2015) *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 19(2), ss. 95-136.

Özkan, O. (2020). *Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, Ankara Üniversitesi.

Reed, C. ve Angel, J. (2004) *Computer Law*. 5nci Bası. ABD: Oxford University Press.

Resmi Gazete. (2008). *AYM. 2006/167 E., 2008/86 K. Ve 20.03.2008 Tarihli İptal Kararı* [Çevrimiçi]. Erişim adresi: <https://www.resmigazete.gov.tr/eskiler/2008/06/20080625-8.htm> (Erişim Tarihi: 27.11.2021).

Selek, O. (2019) *Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 21(2), ss. 911-951.

Sengenberger, W. (2014) *Uluslararası Çalışma Örgütü*. 1inci Bası. Berlin: Friedrich-Ebert-Stiftung.

Süzek, S. (2021) *İş hukuku*. 21inci Bası. İstanbul: Beta Yayıncılık.

T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü. (2016). *6698 Sayılı KVKK'nın 2. Maddesinin Gerekçesi* [Çevrimiçi]. Erişim adresi: <https://www2.tbmm.gov.tr/d26/1/1-0541.pdf> (Erişim Tarihi: 06.12.2021).

Tekin, N. (2014) *Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi*. Uyuşmazlık Mahkemesi Dergisi, C. 0(4), ss. 222-262.

Tolun, Y. (2020). *Kişisel Verilerin KVKK Ve GDPR Kapsamında Korunması*. Yüksek Lisans Tezi, Kırıkkale Üniversitesi.

Toprak, B. (2018). *6698 Sayılı Kişisel Verilerin Korunması Kanunu Işığında İşçinin Kişisel Verilerinin Korunması*. Yüksek Lisans Tezi, Ankara Yıldırım Beyazıt Üniversitesi.

Türk Dil Kurumu. (2021). *Bilgi* [Çevrimiçi]. Türkiye. Erişim adresi:

<https://sozluk.gov.tr> (Eriřim Tarihi: 19.03.2021).

Uncular, S. (2012). *İř İliřkisinde İřçilerin Kiřisel Verilerinin Korunması*. Yüksek Lisans Tezi, Galatasaray Üniversitesi.

Uncular, S. (2020) *Teknolojinin Etkisiyle Dönüřen İř İliřkisinde Giriř Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme*, Çalıřma ve Toplum, C. 66(3). ss. 1673-1700.

Üstün, Y. ve Günel, A.N. (2020) *İř İliřkilerinde Bazı Yaygın Uygulamaların Kiřisel Verilerin Korunması Kanunu Kapsamında Deęerlendirilmesi*, Kiřisel Verileri Koruma Dergisi, C. 2(2), ss. 62-73.

Velioęlu, A. (2019). *Sosyal Medya Özelinde İřçinin Kiřisel Verilerinin Korunması*. Yüksek Lisans Tezi, İstanbul Üniversitesi.

Veri Sorumluları Sicili Hakkına Yönetmelik, T.C. Resmi Gazete, Sayı: 30286, 30 Aralık 2017 [Çevrimiçi]. Eriřim Adresi: www.resmigazete.gov.tr (Eriřim Tarihi: 27.12.2021)

Yardımcı, A. (2019). *İř Yařamında Kiřisel Verilerin Korunması: Malatya Büyükşehir Belediyesi Ve İlçe Belediyelerinde Çalıřan Personelin Kiřisel Verilerinin Korunmasına Yönelik Algı Örneęi*. Yüksek Lisans Tezi, Fırat Üniversitesi.

Yargıtay ve Danıřtay Kararları, Kazancı, [Çevrimiçi]. Eriřim Adresi: <http://www.kazanci.com> (Eriřim Tarihi: 15.01.2022)

Yörük, O. D. (2019). *AB 2016/679 Sayılı Avrupa Birlięi Genel Veri Koruma Tüzüęü Doğrultusunda Kiřisel Verilerin Korunması*. Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi.

Yücel, O. Ü. (2018). *İřçilerin Sosyal Medya Paylařımlarının İřveren Tarafından Denetimi Ve İř İliřkisine Etkisi*. Yüksek Lisans Tezi, Ankara Üniversitesi.

Yüksel, E. (2021, Eylül 11) *Kiřisel Verilerin Korunması Kanunu'nun İř Hukuku'na Yansıması*, [Blog yazısı]. Eriřim adresi: https://tr.linkedin.com/pulse/ki%C5%9Fisel-verilerin-korunmas%C4%B1-kanununun-i%C5%9F-hukukuna-yans%C4%B1mas%C4%B1-yuksel?trk=read_related_article-card_title_2021].

Zewki, H. S. S. (2021). *Kişisel Verilerin Korunması*. Yüksek Lisans Tezi, Gaziantep Üniversitesi.

1136 sayılı Avukatlık Kanunu, T.C. Resmi Gazete, Sayı: 13168, 7 Nisan 1969 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

2004 sayılı İcra ve İflas Kanunu, T.C. Resmi Gazete, Sayı: 2128, 19 Haziran 1932 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

2559 sayılı Polis Vazife ve Salahiyet Kanunu, T.C. Resmi Gazete, Sayı: 2751, 14 Temmuz 1934 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

4721 sayılı Türk Medeni Kanunu, T.C. Resmi Gazete, Sayı: 24607, 8 Aralık 2001 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

4857 sayılı İş Kanunu, T.C. Resmi Gazete, Sayı: 25134, 10 Haziran 2003 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

5237 sayılı Türk Ceza Kanunu, T.C. Resmi Gazete, Sayı: 25611, 12 Ekim 2004 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

5429 sayılı Türkiye İstatistik Kanunu, T.C. Resmi Gazete, Sayı: 25997, 18 Kasım 2005 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

5510 sayılı Sosyal Güvenlik ve Genel Sağlık Sigortası Kanunu, T.C. Resmi Gazete, Sayı: 26200, 16 Haziran 2006 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

6098 sayılı Türk Borçlar Kanunu, T.C. Resmi Gazete, Sayı: 27836, 4 Şubat 2011 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

6331 sayılı İş Sağlığı ve Güvenliği Kanunu, T.C. Resmi Gazete, Sayı: 28339, 30 Haziran 2012 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu, T.C. Resmi Gazete, Sayı: 28460, 7 Kasım 2012 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim

Tarihi: 27.12.2021)

6698 sayılı Kişisel Verilerin Korunması Kanunu, T.C. Resmi Gazete, Sayı: 29677, 7 Nisan 2016 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

6705 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar Ve Sınraşan Veri Akışına İlişkin Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun, T.C. Resmi Gazete, Sayı: 29703, 5 Mayıs 2016 [Çevrimiçi]. Erişim Adresi: www.resmigazete.gov.tr (Erişim Tarihi: 27.12.2021)

95/46/EC sayılı Direktif Çevirisi. 95/46/EC Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi [Çevrimiçi]. Erişim adresi: <https://kisiselveri.com/9546ec-turkce> (Erişim Tarihi: 20.11.2021).