T.C.

MARMARA ÜNİVERSİTESİ

AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ

AVRUPA BİRLİĞİ HUKUKU ANABİLİM DALI

AB VE TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI-MEVZUAT UYUMUNA YÖNELİK BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

Bekir GÜRSES

İstanbul-2019

T.C.

MARMARA ÜNİVERSİTESİ

AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ

AVRUPA BİRLİĞİ HUKUKU ANABİLİM DALI

AB VE TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI-MEVZUAT UYUMUNA YÖNELİK BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

Bekir GÜRSES

Danışman: Doç. Dr. Mustafa Tayyar KARAYİĞİT

İstanbul-2019

TEZ ONAY SAYFASI

Marmara Üniversitesi
Avrupa Araştırmaları Enstitüsü Müdürlüğüne

Enstitünüz, Avrupa Birliği Hukuku Anabilim Dalı Türkçe / İngilizce Yüksek Lisans Programı öğrencisi **Bekir Gürses**, tarafından hazırlanan, **"AB ve Türk Hukukunda Kişisel Verilerin Korunması – Mevzuat Uyumuna Yönelik Bir Değerlendirme"** başlıklı bu çalışma, ..4../..8../..2018..tarihin de yapılan savunma sınavı sonucunda **OY BİRLİĞİ / ~~OY ÇOKLUĞUYLA~~, BAŞARILI** bulunarak aşağıda isimleri yazılı jüri üyeleri tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri:

Doç. Dr. Mustafa T. KARAYİĞİT	Danışman	.....
Doç. Dr. Mesut Serdar ÇEKİN	Jüri Üyesi	.....
Dr. Öğr. Üy. Deniz T. APAYDIN	Jüri Üyesi	.....

Onay

Prof. Dr. Muzaffer Dartan
Müdür

09/09/2018..tarih ve 2018/25.sayılı Enstitü Yönetim Kurulu kararı ile onaylanmıştır.

ÖZET

20. yüzyılın ikinci yarısından itibaren bilgi teknolojilerindeki hızlı gelişim ve hızla artan veri akışı trafiği kişisel verilerin yasal düzlemde korunması ihtiyacını beraberinde getirmiştir. Bu süreçte birçok AB üyesi ülke, kendi iç hukukunda düzenleme yapma ihtiyacı hissetmiştir. 80'li yılların başından itibaren ise ortaya çıkan uluslararası düzenlemeler ile birlikte kişisel verilerin korunması adına belli başlı prensipler oluşturulmuştur. 95 yılında 95/46/EC Sayılı AB Direktifi kabul edilmiş ve dolayısıyla AB hukukunda kişisel verilerin korunması üzerine düzenlenmiş ilk çerçeve düzenleme yürürlüğe girmiştir. Nihayetinde 14 Nisan 2016 tarihinde AB Genel Veri Koruma Tüzüğü onaylanmış ve 25 Mayıs 2018 tarihi itibariyle yürürlüğe girmiştir.

Türkiye'de ise 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK) ile birlikte Türk hukukunda kişisel verilen korunmasına ilişkin ilk çerçeve yasa kabul edilmiştir. Söz konusu Kanun'un oluşturulmasında Direktif'in referans alındığını görmekteyiz. Direktif'in yürürlükten kalkmasıyla birlikte Tüzük'ün, Kanun açısından değerlendirilmesinin önemi daha da artmıştır. Bunun yanında Tüzük'ün yer bakımından uygulanma alanı ile ilgili getirmiş olduğu hükümler ve sınır ötesi veri akışının her geçen zamanda daha da arttığı düşünüldüğünde Tüzük'ün, birçok hukuki uyuşmazlıkta Kanun'la etkileşim halinde olacağı kuşkusuzdur. Bu sebepler ışığında Kanun ve Tüzük'ün mevzuatsal uyumuna yönelik karşılaştırmalı olarak değerlendirilmesinin ihtiyacının ortaya çıktığı düşünülerek bu çalışma hazırlanmıştır.

Çalışmada ilk olarak kişisel verilerin korunması hukukunun hukuki niteliği ve tarihsel gelişimi üzerinde durulmuştur. İkinci olarak ise KVKK'daki metodoloji esas alınarak kişisel verilerin korunması hukukunun temel kavram ve prensipleri ile birlikte veri sahibi ve veri sorumlusunun hak ve yükümlülüklerine değinilmiştir. Bu aşamada Tüzük ile Kanun'un mevzuatsal uyumu değerlendirilmiş, benzerlik ve farklılıkları üzerinde durulmuştur. Son olarak ise kişisel verilerin korunma yolları ile düzenleyici kurumlar açısından değerlendirme yapılarak Kanunda eksik olduğu veya değiştirilmesinin gerektiği düşünülen hususlarla ilgili birtakım çözüm önerileri sunulmuştur.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin Korunması, Kişisel Verilerin Korunması Kanunu, Avrupa Birliği Genel Veri Koruma Tüzüğü,

ABSTRACT

Since the second half of the 20th century, the rapid development of information technologies and rapidly increasing data flow traffic has brought the need for legal protection of personal data. In this process, many EU member states felt the need to make regulations in their domestic act. Since the beginning of the 80s, with the emergence of international regulations, certain principles have been established for the protection of personal data. In 1995, the EU Directive no. 95/46 / EC was adopted and the first framework act regulated on the protection of personal data in EU law came into force. Ultimately, the EU General Data Protection Regulation was ratified on 14 April 2016 and entered into force as of the date of 25 May 2018.

In Turkey, with Personal Data Protection Act (PDPA) which came into force in 2016, the first framework act related with personal data protection was adopted in Turkish act. We notice that in the constitution of the act, Directive has been taken as a reference. With the repeal of the Directive, the importance of evaluating the Regulation from the perspective of the act has increased. Besides, considering that cross-border data flow increases more day-by-day and the Provisions of the Regulation about the area of application, the Regulation will certainly interact with the act in many legal disputes. In the light of these reasons, this study has been prepared considering the need for comparative evaluation towards the legislative alignment of the act and Regulation.

In this study, firstly, the legal quality and historical development of personal data protection act are emphasized. Secondly, on the basis of the methodology in PDPA, the basic concepts and principles of personal data protection act as well as the rights and obligations of the data owner and the data officer are mentioned. At this stage, the legislative alignment of the Regulation and the act was evaluated and focused on the points on which they differ. And finally, the ways of protection of personal data and the regulatory authorities have been evaluated and a number of solutions have been proposed regarding the issues that are missing or need to be changed in the act.

Key Words: Personal Data, Personal Data Protection, Personal Data Protection Act, European Union General Data Protection Regulation

ÖNSÖZ

Tez çalışmamda sabır ve özveri ile beni destekleyen değerli danışman hocam Doç. Dr. Mustafa Tayyar Karayiğit'e ve aynı zamanda maddi-manevi desteklerini benden esirgemeyen ve verdiğim her kararda yanımda olan annem Hatice Gürses ve babam Hasan Basri Gürses'e teşekkürlerimi bir borç bilirim.

Bekir Gürses

İÇİNDEKİLER

KISALTMALAR

AB : Avrupa Birliği

ABTHŞ : Avrupa Birliği Temel Haklar Şartı

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

AK : Avrupa Konseyi

AYM : Anayasa Mahkemesi

Bkz. : Bakınız

BAM **:** Bölge Adliye Mahkemesi

BM : Birleşmiş Milletler

C. : Cilt

CMK : 5271 Sayılı Ceza Muhakemesi Kanunu

çev : Çeviren

Direktif : 95/46/EC Sayılı AB Direktifi

Divan : Avrupa Birliği Adalet Divanı

ETS 108 : Kişisel Verilerin Otomatik İşleme Tabi Tutulmasında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi

GVKT : 2016/679 Sayılı ve AB Genel Veri Koruma Tüzüğü

HMK : 6100 Sayılı Hukuk Muhakemeleri Kanunu

Kanun : 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Kurul : Kişisel Verilerin Korunması Kurulu

KVKK : 6698 Sayılı Kişisel Verilerin Korunması Kanunu

m. : Madde

MÖHUK : 5718 Sayılı Milletlerarası Özel Hukuk Ve Usul Hukuku Hakkında Kanun

N. : Numara

s. : Sayfa

S. : Sayı

TBB : Türkiye Barolar Birliği

TBK : 6098 Sayılı Türk Borçlar Kanunu

TCK : 5237 Sayılı Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TTK : 6102 Sayılı Türk Ticaret Kanunu

TMK : 4721 Sayılı Türk Medeni Kanunu

TÜİK : Türkiye İstatistik Kurumu

Tüzük : 2016/679 Sayılı ve AB Genel Veri Koruma Tüzüğü

vb : Ve bunun gibi

VSBT : Veri Sorumlusuna Başvuru Usul Ve Esasları Hakkında Tebliğ

Y. : Yıl

GİRİŞ

Kişisel verilerin korunmasına atfedilen önem, teknolojinin tarihsel seyri ile benzerlikler göstermektedir. Özellikle internet kullanımının artması[1] ile birlikte kişisel verilerin paylaşımında ciddi bir artış görülmüştür. Veri sahiplerinin, kişisel verilerini paylaşmadan modern çağa ayak uydurmasının imkânsızlaşması veri koruma hukukunun gelişimini de beraberinde getirmiştir. Batı Avrupa hukukunda 2. Dünya Savaşı sonrası bireysel hak ve özgürlüklere verilen önem, kişisel verilerin korunması noktasında da diğer dünya ülkelerine nazaran daha hızlı yapısal düzenlemelerin ortaya çıkmasının önünü açmıştır.

Avrupa Birliği[2] üyesi ülkelerin, kişisel verilerin korunması hususunda yapmış olduğu çalışmalar yarım asrı aşkın süredir devam etmektedir. AB'de kişisel verilerin korunması hukukundaki ilk çerçeve hukuki düzenleme 1995'te yürürlüğe giren 95/46/AT sayılı Direktif'tir. İlerleyen konularda daha detaylı anlatılacak olmakla birlikte AB üyesi ülkelerin büyük bir çoğunluğunda çerçeve veri koruma yasaları iç hukuklarına Direktif öncesinde dercedilmiştir. Ulusal hukukların Direktife uygun hale getirilmesi sonrasında ise Birlik hukukunda, kişisel verilerin korunmasının öneminin artması ve daha birçok sebep nedeniyle kapsamlı bir reforma gidilmiş ve AB Genel Veri Koruma Tüzüğü 4 Mayıs 2016 tarihinde yayımlanarak 25 Mayıs 2018 tarihinde yürürlüğe girmiştir.

Türkiye'deki kişisel verilerin korunmasına ilişkin yasal çalışmalar 2000'li yılların başından itibaren yapılmaya başlamış fakat birçok sebeple çerçeve kanun uzun yıllar yürürlüğe girememiştir. 2010 yılında yapılan anayasa değişikliği ile birlikte kişisel verilerin korunması hakkı en üst yasal normdan Türk hukuk sisteminde yerini almıştır. 2016 öncesi oluşturulan kişisel verilerin korunmasına ilişkin yasa tasarılarının

[1] Ocak 2019 itibariyle 7,67 milyar dünya nüfusunun 4,38 milyarının (%57) internet kullanıcısı olduğu, 3,48 milyarının (%45) sosyal medya kullanıcısı olduğu görülmektedir. Aynı çalışmanın 2018 verilerinin incelenmesinde ise 4,02 milyar (%53) internet kullanıcısı ve 3,19 milyar sosyal medya kullanıcısı olduğu görülmektedir. We Are Social 2019 Dünya İnternet, Sosyal Medya ve Mobil Kullanıcı İstatistikleri https://dijilopedi.com/2019-internet-kullanimi-ve-sosyal-medya-istatistikleri/ (15 Mayıs 2019)

[2] Çalışma kapsamında dönem farkı gözetilmeksizin "Topluluk" kelimesi yerine "Birlik" kelimesi kullanılmıştır.

kanunlaşamaması neticesinde 6698 sayılı Kanun ancak 7 Ekim 2016 tarihi itibariyle yürürlüğe girebilmiştir. Gerekçesinde de değinildiği üzere Kanun, birçok hususta 95/46/AT sayılı AB Direktifi'nden esinlenilerek oluşturulmuştur.

Bu doğrultuda sorulması gereken soru 95/46/AT sayılı AB Direktifi'nden esinlenilerek oluşturulan 6698 sayılı Kanun, kişisel verilerin korunması noktasında zamanın ruhunu ve geleceği yakalayabilecek midir? Tüzük'ün kişisel verilerin korunması hukukuna getirdiği temel yenilikler nelerdir? Kanun'un, Tüzük'teki düzenlemeler karşısında eksiklikleri var mıdır? Tüm bu soruların ışığında çalışma kapsamında çoğunlukla Tüzük üzerinden anlatım yapılarak ve Kanun'un durum üzerindeki hükümleri karşılaştırılarak irdelenmiştir. Direktif'in hükümleri ise Kanun ve Tüzük'ten farklılık teşkil ettiği müddetçe değerlendirmeye alınmıştır. Çalışmanın kapsamını mevzuatsal değerlendirme oluşturduğundan Divan, AYM ve Kurul'un önemli kararlarına kısaca değinilmekle yetinilmiştir.

Çalışmanın birinci bölümünde ilk olarak kişisel verilerin korunması hakkının hukuki niteliği üzerinde durulmuştur. Özellikle ABD ve Batı Avrupa hukukundaki kişisel verilerin korunmasının hukuki niteliğine ilişkin bakış açıları irdelenmiştir. Sonrasında ise AB üyesi ülkelerin birinci kuşak veri koruma yasaları ve 80'li yılların başından itibaren yürürlüğe girmeye başlayan kişisel verilerin korunmasına ilişkin uluslararası düzenlemelerin önemli noktaları birlikte anlatılmıştır. AB hukukundaki çerçeve veri koruma düzenlemeleri olan 95/46/AT sayılı AB Direktif'i ve 2016/679 sayılı AB Genel Veri Koruma Tüzük'ünün, ortaya çıkış amacı, kapsamı ve niteliğine ilişkin genel çerçevede bir değerlendirme yapılmıştır. Son olaraksa başta KVKK olmak üzere kişisel verilerin korunması hukukunun Türk hukuk sistemindeki gelişimi üzerinde durulmuş ve Kanun'un ortaya çıkış nedenleri, kapsamı ve amacı ayrıca incelenmiştir.

Çalışmanın ikinci bölümünde kişisel verilerin korunması hukukunda temel kavram ve prensiplerin neler olduğu ile hangi şartlar altında hukuka uygun bir veri işlemesinden bahsedilebileceği irdelenmiştir. Bu bölüm altındaki başlıklar Kanun'un metodolojisi dikkate alınarak oluşturulmuştur. Ancak hemen hemen bütün kavram ve prensiplerin Tüzük'te daha detaylı düzenlenmiş olduğu gerçeğinden, Kanun'daki eksik

kalan hususlar belirtilmiş ve değerlendirme yapılırken Tüzük'ün oluşturduğu iskelet esas alınarak aktarılmaya çalışılmıştır.

Üçüncü bölümde veri sahibinin kişisel verisinin işlenmesinden doğan hakları ve veri sorumlusu ile veri işleyenin yükümlülükleri aktarılmıştır. Tüzük'ün veri sahibinin hakları için getirmiş olduğu yenilikler ve düzenlemelerin daha kapsamlı ve detaylı olduğu göz önüne alınarak alt başlıklar Tüzük'ün oluşturduğu sistem üzerinden açıklanmıştır. Veri sorumlularının yükümlülükleri açısından Tüzük ve Kanun'un ayrı başlıklar altında mevzuatsal karşılaştırmaları yapılmış ve Kanun'daki eksik kalan hususlara ilişkin çeşitli öneriler sunulmuştur.

Dördüncü bölümde ise ilk olarak hak ihlalinin olduğu düşünülen hallerde veri sahiplerinin kişisel verilerinin korunması yolları anlatılmıştır. Veri sorumlusuna başvuru ve denetim makamına başvuru yolları tüzük ve kanunda paralellik arz ettiğinden karşılaştırmalı olarak aktarılmış, ancak cezai ve genel hukuktan kaynaklı düzenlemeleri Tüzük daha çok üye ülkelerin iç hukuklarına bırakmış olduğundan dolayı bu hususlar Türk Medeni Kanunu (TMK) ve Türk Ceza Kanunu'na (TCK) atıflar yapılarak açıklanmaya çalışılmıştır. Son olaraksa düzenleyici kurumların Tüzük ve Kanun kapsamındaki hukuki niteliği, mali ve idari bağımsızlığı üzerinde durulmuştur.

Teknolojik gelişmelerin hızla arttığı ve kişisel verilerin aktarılmasının uluslararası boyutta hız kazandığı günümüzde Tüzük'ün 3. maddesi ve MÖHUK'un 35. maddesini dikkate aldığımızda günümüz itibariyle Kanun ve Tüzük'e uygun hareket edilmesi ve her iki düzenlemenin de mukayeseli olarak ayrıca irdelenmesi önem arz etmektedir. Ayrıca Tüzük'ün yürürlüğe girmesi ile birlikte Direktif yürürlükten kalkmış olup, Türk hukukundaki kişisel verilerin korunması noktasında birtakım hukuki uyuşmazlıklarda Kanun'un eksik kaldığı hususlarda Tüzük'ün, gerek Kurul'a gerekse de yargı mercilerine bağlayıcılığı olmasa dahi yol gösterici olacağı kuşkusuzdur. Tüm bu sebepler ışığında Tüzük'ün Türkiye'deki kişisel verilerin korunması hukukundaki yeri büyük önem arz etmektedir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI KAVRAMININ HUKUKİ NİTELİĞİ, TARİHSEL GELİŞİMİ VE KAYNAKLARI

1. Bir Hak Olarak Kişisel Verilerin Korunması Ve Hukuki Niteliği

Kişisel verilerin korunmasının hukuki niteliğini, özel hayatın gizliliği ve korunması hakkından, (Any. m.20) düşünceyi açıklama özgürlüğüne (Any. m.26), bilim ve sanat hürriyetinden (Any. m.27) mülkiyet hakkına (Any. m.35), bilgi edinme hakkından (Any. m.74) basın hürriyetine (Any. m.28) ve kişinin dokunulmazlığı, maddi ve manevi bütünlüğü hakkından (Any. m.17) kişi hürriyeti ve güvenliği hakkına (Any. m.20) kadar birçok temel hak ve özgürlük ile ilişkilendirerek açıklamak mümkündür. Her ne kadar kişisel verilerin korunması kavramını birçok temel hak ve özgürlükle özdeşleştirebilsek de özünde ikili bir ayrım yapılabilir.[3] İlki kişisel verilerin korunmasını, temel insan hakları içerisinde değerlendiren yaklaşımdır. İkincisi ise ekonomik bir hak olarak değerlendiren yaklaşımdır.[4]

Amerika Birleşik Devletleri hukukunda[5] ikinci yaklaşım ön plana çıkmaktadır. Batı Avrupa hukukundan ve AB hukukundan farklı olarak ABD'de, kişisel verilere özel hayatın gizliliği kapsamında yaklaşılmaktan kaçınılmaktadır.[6] Amerikan hukukunun kendine özgü yapısı, ekonomik temelli bakış açısı, özel yaşamın gizliliği hakkının anayasal haklar arasında değerlendirilmemesi ve içtihatlarla kendisine ancak 19. yüzyılın sonlarından itibaren yer bulabilmesi bu sonucu doğurmuştur.[7] Kişisel verilerin korunmasına ekonomik bir hak yaklaşımı olarak bakan görüşe göre kişisel veriler

[3] Doktrinde üçlü bir ayrım yapılarak mülkiyet hakkı, fikri mülkiyet hakkı ve kişilik hakkı yaklaşımı ekseninde değerlendirmeler de mevcuttur. Doktrinde azınlıkta kalan görüş olmakla birlikte kişisel verilerin korunması hakkını fikri mülkiyet hakkı ile ilişkilendirenler de mevcuttur. Daha detaylı bilgi için bkz. Elif Küzeci, **Kişisel Verilerin Korunması,** 3.Basım, Ankara, 2019, s.62

[4] Küzeci, *Kişisel Verilerin Korunması***,** s.59.

[5] Burada özellikle İngiltere'nin (halen) AB üyesi ülke olması ve kişisel verilerin korunmasına ilişkin yaklaşımının Amerikan Hukukundan farklılık göstermesi göz önüne alınarak Anglo-Sakson Hukuk Sistemi demekten kaçınılmıştır.

[6] İkbal Gür, **Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar Ve Çözüm Yolları**, 1. Basım, Ankara, 2010, s.101.

[7] Küzeci, *Kişisel Verilerin Korunması***,** s.59.

sadece kişiliğin uzantısı değil aynı zamanda kişiliğin ürünüdür.[8] Kişisel verilerin korunmasını mülkiyet hakkı teorisi kapsamında değerlendiren yazarlar bireyin istediği takdirde bu hakkını satabileceğini ve istedikleri kurum ve kişi ile paylaşabileceklerini ve bunun neticesinde de kişisel verilerin ilgili kişilerin tam denetiminde olabileceğini savunmaktadırlar.[9] Gerçekten de kişisel verilerin korunmasını kişisel bir hak kapsamından çıkarıp sadece ekonomik bir hak kapsamında değerlendirildiğinde, ilgili kişi kişisel veriyi bir pazarlık kapsamında paylaşabilecek, verinin hangi işletmelerle hangi şartlar altında paylaşıldığını daha somut bir şekilde denetleyebilecektir. Buna karşılık kişisel verinin korunmasında veri sahibine yüklenen sorumluluk, veriyi isteyen kuruma veya kişiye yüklenen sorumluluğun önüne geçecektir. Bir ihlalin doğması neticesinde ilgili kişi aktif bir rol almaya zorlanacaktır. Bunun yanında "pazarlık" çoğu zaman iki eşit statüdeki kişiler arasında olmayacağından kişisel verisi paylaşılan kişinin sömürülmesi ve bunun neticesinde de zarar görmesi kaçınılmaz hale gelebilecektir.

Kişisel verilerin, kişilik hakkı kapsamında değerlendirilmesi gerektiği görüşünde[10] ise kişinin ve kişisel verilerinin korunması insanlık onuru ve birçok temel hak ve özgürlük çerçevesinde değerlendirilme neticesini ön plana çıkarmaktadır. Bu kapsamda kişisel verilerin korunması hakkı devredilemez ve vazgeçilemezdir. Bu görüşe göre kişisel verilerin korunmasını, tıpkı bir taşınmaz mal alım-satımı yaparmış gibi değerlendirmek ve buna uygun şekilde mevzuat düzenlemeleri getirmek, bilgi edinme hakkını ya da düşünceyi açıklama özgürlüğünü mal haline getirmekten farksızdır.[11] Gerçekten de kişisel verilerin salt iktisadi bir değer ifade eder şekilde kullanılması ve mülkiyet hakkı kapsamında değerlendirilmesi yeterli korumayı sağlamayacaktır. Tabii ki de veri sahibinin temel hak ve özgürlükleri yanında ekonomik çıkarları da korunmalıdır. Fakat bu durum kişinin, kişisel verileri üzerinde mülkiyet hakkının tesis edilebileceği sonucunu doğurmamalıdır. Aksi takdirde kişisel verilerin

[8] Hüseyin Can Aksoy, **Medeni Hukuk Ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, 1. Basım, Ankara, 2010, s. 57.

[9] Daha detaylı bilgi için bkz. ibid., s.57-72

[10] AB hukukunda kişisel verilerin korunmasına ilişkin çerçeve düzenlemeler ileride daha ayrıntılı değinilecek olmakla birlikte kişisel verilerin korunmasını kişilik hakkı kapsamında değerlendirdiklerini görmekteyiz. Aynı şekilde Anayasa m.20. ve KVKK m.1 de kişisel verilerin korunması, kişilik hakkı kapsamında değerlendirilmiştir.

[11] Küzeci, *Kişisel Verilerin Korunması***,** s.65.

korunması hakkından kaynaklı bireyin menfaatlerini zedeleyici bir netice ortaya çıkacak ve bireylerin kendi kişisel verileri üzerindeki denetimleri zorlaşacaktır.

Nitekim ulusal ve uluslararası düzenlemelerde de kişisel verilerin korunmasının, temel insan hakkı olduğu düşüncesi baskındır. Aynı şekilde AB Veri Koruma Direktifi (m.1) ve AB Genel Veri Koruma Tüzüğü (m.1) kişisel verilerin korunmasını temel bir insan hakkı olarak kabul etmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 1. maddesine de aynı durum ele alınmış ve kişisel verilerin başta özel hayatın gizliliği hakkı olmak üzere temel insan hakkı kapsamında değerlendirileceği gerekçesinde de dahil olmak üzere vurgulanmıştır.

2. Kişisel Verilerin Korunması Hukukunun Tarihsel Gelişimi Ve Uluslararası Kaynakları

Bireyi tanımlayan ve diğer insanlardan ayırt edilebilirliğini gösteren her türden husus, bireyin korunma ihtiyacının doğuşuna zemin hazırlamıştır. Bilişim sektöründeki gelişmeler neticesinde bilginin depolanması, aktarımı, paylaşımı kolaylaşmış ve veri sahipleri için riskler her geçen zaman artarak devam etmiştir. Veri sahiplerinin menfaatlerinin korunması için 20. yüzyılın ikinci yarısından itibaren ulusal ve uluslararası boyutta çalışmalar hız kazanmış, bireyler açısından ortaya çıkabilecek hak ihlallerinin önüne geçilmeye çalışılmıştır. Birinci kuşak veri koruma yasalarının yürürlüğe girdiği bu dönem için 2. Dünya Savaşı sonrası Kıta Avrupası'nda insan haklarına verilen önemin de etkili olduğu söylenebilir.

Almanya Hessen Federe Devleti'nde kabul gören 1970 tarihli yasa kişisel verilerin korunması hukukundaki ilk düzenleme olmuş olup sonrasında ise İsveç, Almanya, Danimarka, Norveç ve Fransa mevzuatlarındaki yasal düzenlemeler kendisini izlemiştir.[12] 1980 yılına gelindiğinde AET üyelerinin birçoğunun (İngiltere, İrlanda, İtalya haricinde) kişisel verilerin korunması hukukuna ilişkin çerçeve temel

[12] Hüseyin Murat Develioğlu**, 6698 Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku,** 1. Basım, İstanbul, 2017, s.6

düzenlemeleri yaptığı görülmektedir.[13] Bununla birlikte ABD'de 1970 yılında Adil Kredi Raporlama Yasası yürürlüğe girmiştir. Bu düzenlemenin, kişisel verilerin korunmasına yönelik Batı Avrupa'daki çerçeve yasal düzenlemelerden daha çok finansal verilerin gizliliğinin korunmasını amaçladığı görülmektedir.[14]

Ulusal hukuk sistemlerinde kabul gören birinci kuşak veri koruma yasalarında kişisel verilerin silinmesi, anonimleştirilmesi ve yok edilmesi gibi günümüz mevzuatlarında var olan temel esaslara değinilmemiş olmakla birlikte, veri bankalarının kayıt altına alınması, veri sahibinin kişisel veriye ulaşma ve düzeltilmesini talep etme hakkı koruma altına alınmıştır. Kısaca bu dönemki ulusal düzenlemelerde özel hayatın korunmasına yönelik esaslardan ziyade veri bankalarındaki bilgilerin düzenlenmesinin esas alındığı sonucu çıkmaktadır.[15]

Bu düzenlemeler neticesinde kendi iç hukuklarında çeşitli mevzuat eklentileri yapan üye ülkeler, kişisel verilerin uluslararası aktarımını baskılamakta, her ülke için farklı olabilecek şekilde sadece kişisel verilerin korunmasında yasal güvenceyi sağlayan ülkelere aktarımın önünü açmaktaydılar. Bu durumun başta güvenlik ve ticaret alanında olmak üzere bir takım uluslararası kısıtlamalara sebebiyet verebileceğinden dolayı özellikle 1980 sonrasında uluslararası düzenlemelere ihtiyaç duyulmuştur.[16]

İlk olarak 1980 yılında Ekonomik İşbirliği ve Kalkınma Teşkilatı tarafından "Kişisel Alanın Korunması Ve Sınır Ötesi Kişisel Veri Dolaşımına İlişkin Rehber İlkeleri" (OECD Rehber İlkeleri) kabul edilmiştir. Tavsiye niteliğinde olan ve üye ülkeleri bağlayıcılığı bulunmayan bu ilke kararları, uluslararası arenada yapılan ilk düzenleme olması ve Avrupa ülkeleri dışında da birçok ülkenin katılımıyla oluşturulması açısından önem arz etmektedir. Günümüz bilişim sektörü gelişmeleri ile birlikte 2013 yılında rehber ilkelerinde daha geniş kapsamlı bir güncellemeye gidilmiş[17]

[13] Küzeci, *Kişisel Verilerin Korunması*, s.104.

[14] Gür, s. 131.

[15] Küzeci, *Kişisel Verilerin Korunması*, s.106.

[16] Develioğlu, s.6.

[17] 2013 tarihli Kişisel Alanın Korunması Ve Sınır Ötesi Kişisel Veri Dolaşımına İlişkin Rehber İlkeleri https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf 20.05.2019

olmakla birlikte 1980 yılında yürürlüğe giren metindeki sekiz temel ilke[18] varlığını korumuştur.

1981 yılında imzaya açılan "108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Avrupa Konseyi Sözleşmesi" (EST 108) ise uluslararası bağlayıcılığı olması yanında bireylere, kişisel verileri üzerinde haklar tanımaktadır.[19] Dayanağını Avrupa İnsan Hakları Sözleşmesi (AİHS) 8. maddesinden[20] alan bu sözleşmeyle birlikte otomatik işlenen kişisel verilerin[21] serbest dolaşımının sekteye uğramasının önüne geçilmek istenmiş, gerek yapısal gerekse de mevzuatla ilgili hukuki güvenceyi sağlayan sözleşme tarafı ülkelerin serbest veri aktarımının önü açılmıştır.[22] 1980 tarihli OECD Rehber İlkelerinde olduğu gibi, 2018 tarihinde "Sözleşme +108" ile bir takım yenilemeler getirilmiş ancak henüz yürürlüğe girmemiştir. Türkiye ise 6669 sayılı 30.01.2016 tarihli onaylanmasını uygun bulma Kanununa müteakip Sözleşme'yi onaylamıştır.

1990 yılında kabul edilen "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri"nde de kişisel verilerin korunması tıpkı EST 108'de olduğu gibi BM Evrensel İnsan Hakları Bildirgesi'nin 12. maddesinde yer alan özel yaşamın gizliliği kapsamında değerlendirilmiştir[23]. Kişisel verilerin korunmasına yönelik kamu ve özel hukuk kişilerini kapsayacak şekilde düzenlemeler içeren BM Rehber İlkeleri uygulamanın denetlenmesini sağlayacak yetkili ve bağımsız bir organın kurulmasını

[18] Bu ilkeler 1)Veri toplanmasının sınırlılığı prensibi, 2)Veri niteliği prensibi, 3)Amacın belirliliği prensibi, 4)Kullanımın sınırlılığı prensibi, 4)Veri güvenliği prensibi, 5)Açıklık prensibi, 6)Kişisel Katılım Prensibi, 7)Hesap verilebilirlik prensibidir.

[19] Cristopher Kuner, **European Data Protection Law: Corporate Compliance and Regulation, 2. Basım,** Oxford University Press, 2007, s. 48.

[20] M.8. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

[21] Sözleşme metninde her ne kadar otomatik işlenmeden bahsedilmiş ve elle işleme kapsam dışına çıkarılmışsa da veri işlemenin tamamının otomatik işlenmesi gerekmediği gibi yarı otomatik işlemeler de sözleşme dâhilinde değerlendirilebilecektir. (108 sayılı Avrupa Konseyi Sözleşmesi m. 2-d) Daha detaylı bilgi için bkz. Songül Atak, **Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler**, Türkiye Barolar Birliği Dergisi, S. 87, 2010, s.90-120.

[22] Develioğlu**,** s.9.

[23] M.12. Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır.

belirten ilk uluslararası belge olsa da, etkisinin OECD Rehber İlkeleri ve EST 108'in gerisinde kaldığı söylenebilir.[24]

3. Avrupa Birliği Hukukundaki Düzenlemeler

3.1. Genel Olarak

İkinci Dünya Savaşı'nın etkilerinin devam ettiği süreçte, 20. yüzyılın ikinci yarısının başlarında kurulan Avrupa Birliği'nin kuruluş felsefesi, ekonomik ve siyasi ortaklığa dayanmaktadır.[25] Belirtmek gerekir ki, ABD'den idari ve yapısal anlamda farklılık arz eden AB'de, egemen üye devletler kendilerini uluslararası platformda temsil edebilmektedir. Ortak pazarın gelişmesi ve zamanla ortaya çıkan teknolojik gelişmeler her üye ülkede farklı kişisel verilerin korunması yasalarının ortaya çıkmasına zemin hazırlamıştır. Nitekim bir önceki başlıkta belirtilmiş olunduğu gibi birçok üye devlet kişisel verilerin korunmasına ilişkin mevzuat düzenlemelerini AB dışındaki diğer ülkelere nazaran 1980 öncesinde tamamlamıştır. Bir yandan ortak pazar, diğer yandan da üye ülkelerin kişisel verilerin korunmasına ilişkin yasal düzenlemelerinin ortaya çıkması neticesinde uluslararası veri aktarımını sekteye uğramasını önlemek amacı, Avrupa Birliği'ni, kişisel verilerin korunması alanında yasal düzenlemeler yapmaya itmiştir.[26]

Gerçekten de 1980 sonrasındaki gelişen tek pazar anlayışı ve üye ülkeler arasındaki ticari ve sosyal ilişkilerin artmasıyla birlikte Birlik içerisinde kişisel verilerin korunması hukukunda yeknesaklık ve standartlaşma arayışı doğmuştur. Birlik hukukunda çerçeve düzenlemeler Direktif ve Tüzük olmakla birlikte mevzuattaki diğer gelişmelere de bu başlık altında kısaca değinmek gerekir.[27]

---

[24] Doğan Kılınç, **Anayasal Bir Hak Olarak Kişisel Verilerin Korunması,** Ankara Üniversitesi Hukuk Fakültesi Dergisi, C61, S.3, 2012, s. 1112.

[25] Dinç Engin, **Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye'nin Durumu**, Yüksek Lisans Tezi, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Diyarbakır, 2006, s. 28.

[26] Direktif 8 no.lu gerekçe

[27] Direktif öncesindeyse kişisel verilerin korunmasının gelişimi hususunda, başta Divan olmak üzere Birlik kurumlarının ayrı ayrı katkıları bulunmaktaydı. Konumuzun içeriğini mevzuatsal düzlemde karşılaştırma oluşturduğundan Divan'ın konuya ilişkin içtihatları ve diğer Birlik kurumlarının çalışmaları üzerinde ayrıca durulmayacaktır.

Kişisel verilerin korunması hakkı, 2000 yılında Nice'te kabul edilen Avrupa Birliği Temel Haklar Şartı'nda (ABTHŞ) düzenlenerek asli normlar arasında kendisine yer bulmuştur. Direktif'in kabulü sonrası yaşanan bilişim hukukundaki gelişmeler ve teknolojik ilerlemeler kişisel verilerin korunması hakkını daha üst bir norm ile, yani ABTHŞ'nin 8. maddesinde, düzenlenmesini gerektirmiştir. Bu sebepler ABTHŞ 2. bölüm 8. maddesinde özel hayatın gizliliği bölümünden farklı olarak ayrı bir maddede değerlendirilmiştir. 8. maddeye göre; "*(1). Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.(2) Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.(3) Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.*[28]

Bunların yanında elektronik haberleşme alanında da bir takım düzenlemelere gidilmiştir. Bu süreçte birçok direktif kabul edilmiş olmakla birlikte en önemli iki tanesi 2002 yılında kabul edilmiş olan 202/58/AT Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi ve 2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi'dir. 95/46/EC sayılı Direktif sonrasında ortaya çıkan direktiflerin ortak özelliği, 95/46/EC sayılı Direktif'in zaman içerisinde ekonomik, güvenlik ve teknolojik gelişimler neticesinde oluşan boşluklarını tamamlamaya yönelik olduğudur.[29]

3.2. 95/46/AT Sayılı Kişisel Verilerin Korunması Direktifinin Amacı, Kapsamı Ve Uygulama Alanı

6698 sayılı KVKK dâhil olmak üzere kişisel verilerin korunması hukukuna ilişkin birçok çerçeve düzenlemenin temelini oluşturan Direktif, 1995 tarihinde kabul edilmiştir. Bilişim sektöründeki gelişmeler neticesinde kişisel verilerin paylaşımının belirli bir mevzuat çerçevesinde korunmasını üye ülkelerin birçoğu Direktif öncesinde tamamlamıştır. Ancak üye ülkelerin gerek kişisel verilerin korunmasına bakış açısının

[28] AB Temel Haklar Şartının Türkçe metni için bkz. https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708 20.05.2019

[29] Küzeci, *Kişisel Verilerin Korunması*, s.184.

farklılıkları,[30] gerekse de tek pazar fikrinin AB içerisindeki öneminin her geçen zaman daha da artması Direktif'in ortaya çıkışına zemin hazırlamıştır.

Bunun yanında Direktif'in ilk maddesine bakıldığında kişi hak ve özgürlükleri bağlamında özel hayatın gizliliği çerçevesinde bir insan hakkının korunması olduğu vurgusu da yapılmaktadır.

Direktif'in, AB hukukunun normlar hiyerarşideki yeri de dikkate alındığında bir diğer amacının da, Birlik içerisinde veri koruma hukukunun üye ülkeler açısından mevzuatsal standartlara oturtulmaya çalışıldığını söylemek mümkündür. Böylece Direktifle birlikte çerçevesi belirlenmiş, asgari sınırları çizilmiş kişisel verilerin korunması sayesinde, üye ülkeler açısında da serbest veri akışı sağlanacak ve ülkeler arasındaki veri akışından kaynaklı ekonomik etkileşim sekteye uğramamış olacaktır.

Direktif kamu ve özel kuruluşları kapsayacak şekilde bir koruma sağlamayı amaçlamıştır. Bu konuda Direktif'te var olan ilkelerin diğer uluslararası ve üye ülke düzenlemelerinden çok da farklılık teşkil etmediğini söylemek mümkündür. Bu açıdan meşruluk, amacının sınırlılığı, şeffaflık, orantılılık, güvenlik ve kontrol Direktif'in belirlediği ilkeler arasındadır.

Toplam yedi esas bölümden oluşan Direktif'de, sırasıyla genel hükümler, hukuka uygunluk sebepleri, hukuki tedbirler, sorumluluk ve yaptırımlar, kişisel verilerin üçüncü ülkelere transferi, davranış kuralları, denetleyici (teftiş) otorite ve Topluluk düzeyinde uygulama tedbirleri bölümleri yer almaktadır.[31] Direktif'in kapsamı ise 3. maddede belirtilmiştir. Bu maddeye göre; kişisel verilerin otomatik olarak işlenmesi halinde tamamının ya da bir bölümünün işlenip işlenmediğine bakılmaksızın bu işleme Direktif kapsamında sayılacaktır. Otomatik yollarla işleme yapılmamasına rağmen bir dosyalama sistemine kaydedilen yahut kaydedilebilecek nitelikte işlenmesi mümkün

[30] Direktif öncesinde bakıldığında Batı Avrupa Hukuk Sistemine sahip ülkelerin, çerçeve kişisel veri koruma yasalarına bakıldığında insan hakları ekseninde özel hayatın korunmasının amaç alındığı görülmekteyken, Anglo-Sakson hukuk sisteminin sahip İngiltere'de ise uluslararası ticaretin korunması amacıyla sınırlı bir korumanın esas alındığı görülmektedir. Daha detaylı bilgi için bkz. Küzeci, *Kişisel Verilerin Korunması***,** s.159-162.

[31] Dilek Yüksel Civelek**, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi**, Başbakanlık Devlet Planlama Teşkilatı Uzmanlık Tezi, Bilgi Toplumu Dairesi Başkanlığı, Ankara, 2011, s. 73.

olan veriler de Direktif kapsamında değerlendirilecektir.[32] Madde lafzı itibariyle biraz karmaşık gözükse de aslında neredeyse bütün kişisel veri işlemelerini kapsadığı hükmünü ihtiva etmektedir.[33] Gerçekten de günümüz itibariyle veri işlemelerinin büyük bir bölümünün bilgisayar ortamında işlendiği göz önüne alındığında Direktif kapsamı dışında neredeyse veri işlenme yolunun kalmadığını söyleyebiliriz.

Direktif ile birlikte kişisel verilerin ihlalini önleyici ve bu hususta üye ülkelerin uygulaması noktasında zorlayıcı tedbirler alınması sağlanmıştır. Şöyle ki: önceki mevzuata ilişkin prensip ve ilkeler yönergenin özünde korunmakla birlikte kişisel verilerin korunmasını gözetmek adına bir makamın yaratılması yoluna gidilmiştir. Ayrıca Direktif'in uygulanabilirliği adına 29. maddede yapılan düzenleme ile çalışma grubu oluşturulmuştur. Tüm bunların neticesinde de Birlik içerisinde kişisel verilerin dolaşımı kolaylaşmış ve üye ülkeler arasındaki veri aktarımları kapsamlı bir hukuki zemine oturtulmuştur.[34]

AB hukukunun kaynakları itibariyle direktiflerin, tüzüklerden farklı olarak doğrudan uygulanabilirliği bulunmadığından üye ülkeler kendi iç hukuklarında direktifin kapsam ve amaçlarına uyum sağlamak adına yeniden ulusal düzenlemeler yapma yoluna gitmiştir.[35] Direktif'in, bir hukuk kaynağı olarak çerçeve belirlemesi ve üye devletlere iç hukuki düzenlemeler noktasında takdir yetkisi bırakması gibi nedenlerle, üye ülkeler açısından kişisel verilerin korunması hakkı için öngörülen yeknesak uygulamaların sağlanması amacına ulaşamadığı görülmektedir.[36] Ancak bunun yanında Direktif'in gösterdiği yol, üye ülkelerde çerçeve korumanın sağlanması noktasında önem taşımaktadır. Gerçekten de Direktif öncesinde üye ülkelerin çerçeve yasalarındaki farklılıklar fazla iken direktif sonrasında "sınırlı yeknesaklıktan" söz edilebilir bir seviyeye gelindiği söylenebilir. Bu durum sadece üye ülkeler için değil Türkiye için de geçerlidir. Türkiye dışında birçok ülke de Direktif'den esinlenerek

[32] Direktif m. 3/1

[33] Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, 1. Basım, İstanbul, 2008, s. 43.

[34] David I. Bainbridge, **EC Data Protection Directive**, Butterworths, Birleşik Krallık, 1996, s. 19

[35] Direktifin yürürlüğe girdiği tarihe kadar Yunanistan'da kişisel verilerin korunmasını düzenleyen çerçeve bir yasa yoktu. David I. Bainbridge, s. 17.

[36] Develioğlu**,** s.12.

kendi kişisel verilerin korunması yasalarını oluşturmuşlardır.[37] İleride daha detaylı incelenecek olmakla birlikte 6698 sayılı KVKK'nin özü itibariyle Direktif'e dayanılarak oluşturulduğu görülmektedir. Nitekim Divan'ın Direktif'i esas alarak oluşturduğu içtihatlar, KVKK'nin yürürlüğe girmesi öncesindeki ve sonrasındaki Türk yargı içtihatlarında Direktif'e atıfların yapıldığı görülmektedir.[38]

3.3. Genel Veri Koruma Tüzüğü'nün (GVKT) Amacı, Kapsamı Ve Uygulama Alanı

Direktif sonrasında kişisel verilerin korunması hakkı, ABTHŞ 8. maddesinde ve Avrupa Birliği'nin İşleyişi Hakkında Andlaşma'nın (ABİHA) 16. maddesinde yer almıştır. AB birincil hukukunda kendisine yer bulan kişisel verilerin korunması hakkının, Direktif sonrasında daha yeknesak bir düzenlenme çağrıştıran diğer bir AB ikincil hukuku tasarrufuyla düzenlenmesi ihtiyacı ortaya çıkmıştır.

Tüzük, kişisel verilerin korunmasının bir hak olarak tüm Birlik üyesi ülkeler için benimsendiği bir süreçte günümüz şartlarına uygun şekilde, geleceği yakalayabilecek kapsamda bir düzenleme olarak 2016 yılında yayımlanmıştır. Tüzük ile birlikte üye ülkeler arasındaki kişisel verilerin korunmasına ilişkin farklı yasal düzenlemelerin yeknesaklaştırılması amaçlanmıştır. Gerçekten de AB üyesi ülkelerindeki farklı yasal düzenlemeleri ortadan kaldıracak bir düzenlemenin işletmeler açısından yıllık yaklaşık 2,3 milyar Euro tasarruf sağlayacağı öngörülmüştür.[39]

Direktif sonrasında, bulut bilişim hizmetlerinin geliştirilmesi, akıllı telefonların ortaya çıkması, internetin daha büyük kitleler tarafından kullanılmaya başlanması neticesinde verilerin aktarımında, erişiminde ve toplanmasında Direktif'in etkisiz kaldığı çeşitli problemler ortaya çıkmıştır. Özellikle Google, Facebook gibi arama

---

[37] Nilgün Başalp, **Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri,** Marmara Üniversitesi Hukuk Fakültesi - HAD, C.21, S.1, s. 81.

[38] Ankara BAM 25 Hukuk Dairesi 2018/3033 esas 2018/2010 karar no.lu 12.12.2018 tarihli ilamı, Adana BAM 3. Hukuk Dairesi 2018/429 esas 2018/478 karar no.lu 02.05.2018 tarihli ilamı, Yargıtay Hukuk Genel Kurulunun 2014/4-56 esas 2015/1679 karar no.lu 17.06.2015 tarihli ilamı, Anayasa Mahkemesi'ne yapılan iptal başvurusunu ve başvuru üzerine Anayasa Mahkemesi'nin vermiş olduğu 28.9.2017 tarihli, 2016/125 E., 2017/143 K. sayılı ilamı sayılabilecek kararlar arasındandır.

[39] Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirmesi,** Çalışma Raporu, Kalkınma Bakanlığı, Ankara, 2017, s. 5.

motorları ve sosyal medya ağlarının kullanımının yaygınlaşması ile birlikte bireylerin kişisel verilerin korunması noktasındaki açıklar daha da gün yüzüne çıkmış ve bu durum Divan tarafında da tüzük öncesinde birçok hukuki uyuşmazlığa konu edilmiştir.[40]

Tüzük, 4 Mayıs 2016 tarihinde yayımlanmış ve 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. Çalışmanın konusu kapsamında, Direktif ve Kanun ile birlikte üç sacayağından birini oluşturan Tüzük'ün önemi mevzuat uyumunun karşılaştırılması kapsamında ayrı ayrı başlıklar halinde ele alınacak olmakla birlikte Tüzük ile Direktif'in, AB hukuku kapsamında normlar hiyerarşisindeki farklılıklarına da değinmek gerekir. ABİHA 288. maddenin 2. fıkrasında, tüzükler bütün üye ülkeler için geçerliliği ve bağlayıcılığı olan tüm üye ülkelerde doğrudan uygulanan AB hukuku kaynağı olarak tanımlanmıştır. Direktiflerin ise, aynı maddenin 3. fıkrasında muhatap alınan her üye devleti ulaşılması gereken sonuçları itibariyle bağlayacağı ve iç hukuklarına yansıtılmalarında üye ülkelerin usul ve yöntemlerini serbest olduğu belirtilmiştir. Yani tüzüklerin uygulanabilmesi için direktiflerde olduğu gibi üye ülkelerden aktif önlemler alınması beklenmemektedir. Üye ülkelerin tüzüğün getirdiği düzenlemeleri iç hukuka aktarmaları Birlik hukukunca engellenmiştir.[41] Direktifler, AB hukuku ile üye ülke hukuku arasındaki uyumluluğu sağlamakla AB çatısı altında bütünleşmeye dolaylı olarak tesir etmektedir.[42] Tüzük açısından ise bu etki doğrudan olmaktadır. Genel anlamda, direktifler uyumlaştırma sağlayan çerçeve düzenlemelerken, tüzükler yeknesaklık sağlayan, üye devletlere takdir yetkisi bırakmayan detaylı düzenlemelerdir. Bu sebeple Tüzük ile birlikte Birlik içerisinde daha etkili bir şekilde kişisel verilerin korunması sağlanmaya çalışılmıştır.

Ayrıca ilk çerçeve düzenlemenin Direktif olması, kişisel verilerin korunması hukukunun gelişmekte olan bir hukuk dalı olması sebebiyle yerindedir. Üye ülkelerin bu alandaki deneyimleri ve teknolojik gelişmelerle birlikte kişisel verilerin korunmasında zamanla bütüncül bir yaklaşım ön plana çıkmıştır. Sonuç olarak Direktif

[40] Dava C-362/14, Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650

[41] Henri De Waele, **Implications of Replacing the Data Protection Directive with a Regulation - A Legal Perspective,** (çeviren) *Nurullah TEKİN,* Privacy and Data Protection Dergisi, Radbound Üniversitesi, 2012 s.76.

[42] Kamuran Reçber, **Avrupa Birliği Hukuku Temel Metinleri**, 2. Basım, Bursa, 2013, s. 113.

ile soluk sınırların ve ulaşılması gereken yerin belirlenmesi ve üye ülkelerde mevzuatsal düzenlemelerin yerine getirilmesi sonrasında Tüzük'ün yürürlüğe girmesi mümkün olmuştur.

Kişisel verilerin üye ülkeler arasında aktarılmasının ve dolaşmasının Direktif zamanında gerek Birlik içerisinde gerekse de Birlik dışarısında birçok bürokratik engele takılıyor olması Tüzük'ün ortaya çıkış amaçlarından birisidir. Nitekim bu durum Tüzük'ün ilk maddesinde kişisel verilerin Birlik içerisinde serbest dolaşımının kısıtlanamayacağı ve yasaklanamayacağı belirtilmiştir.[43]

Tüzük'ün 2. maddesinde[44] kapsamı belirtilmiştir. Tüzük'ün lafzı ve ruhundan Direktif'e nazaran daha etkili bir korumanın var olduğunu söyleyebiliriz. Aynı şekilde Direktif'e göre veri sorumlusu ve veri işleyenin kişisel verilerin korunmasındaki sorumluluklarının arttırıldığını da görmekteyiz. Son olarak ise Direktif'e kıyasla daha kazuistik bir düzenlemenin olduğu, uygulama alanının daha detaylı bir şekilde belirlendiği görülmektedir.

İleriki konularda daha detaylı ele alınacak olmakla birlikte Tüzük ile gelen bir kısım değişikliklere değinmekte fayda vardır: Tüzük kapsamına aykırı davranılması halinde yaptırımlar Direktif'e göre ciddi manada arttırılmış ve çeşitlendirilmiştir. Cezalar ciro üzerindeki hesaplamalar neticesinde belirlenebilecektir. Yer bakımından AB dışındaki ülkelerde de uygulanabilirliğinin önü açılmıştır. Veri işleyenler, veri

---

[43] GVKT m.1/3

[44] *(1) Bu Tüzük, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır. (2) Bu Tüzük: (a) Birlik hukuku kapsamına girmeyen bir faaliyet esnasında; (b) üye devletler tarafından Avrupa Birliği Antlaşması'nın V. Başlığının 2. Bölümü kapsamına giren faaliyetler gerçekleştirilirken; (c) tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından; (d) kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkin makamlar tarafından kişisel verilerin işlenmesine uygulanmaz. (3) Birlik kurumları, organları, ofisleri ve ajansları tarafından kişisel verilerin işlenmesine yönelik olarak, (AT) 45/2001 sayılı Tüzük uygulanır. (AT) 45/2001 sayılı Tüzük ve kişisel verilerin bu şekilde işlenmesine uygulanan Birliğin diğer yasal belgeleri 98. madde uyarınca bu Tüzük'ün ilkeleri ve kurallarına uyarlanır.(4) Bu Tüzük ile 2000/31/AT sayılı Direktif'in uygulanmasına ve özellikle de aynı Direktif'in ara hizmet sağlayıcıların yükümlülüklerine ilişkin 12 ila 15. maddelerinde yer alan kurallara halel gelmez.* hükmü yer almaktadır.

işlemeden kaynaklı ihlallerden sorumlu kılınmıştır. Başlangıç ve tasarımdan itibaren veri korunması ve veri mahremiyeti Tüzük ile birlikte yasal bir zemine oturtulmuştur. Veri sahibine kişisel verisinin işlenip işlenmediğini, işleniyor ise hangi amaçlarla işlendiğine erişme hakkı tanınmıştır. Gerekli hallerde veri koruma görevlilerinin atanması şart kılınarak bu yasal zemine oturtulmuştur.

4. Türk Hukukundaki Düzenlemeler

4.1. Genel Olarak

Kanun öncesinde de kişisel verilerin korunmasına ilişkin hususlar çeşitli kanunlarda kendine yer bulmaktaydı. Anayasadaki düzenleme öncesinde de özel hayatın korunması hakkı (m.20.) dayanak alınarak; Polis Vazife Ve Salahiyeti Kanunu 5. madde[45], Vergi Usul Kanunu 148. madde[46], İş Kanunu 75. madde[47], Nüfus

[45] Polis; a) Gönüllü, b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, ç) Türk vatandaşlığına başvuruda bulunan, d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, e) Gözaltına alınan, kişilerin parmak izini alır. Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez. Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilinceye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir. 5271 sayılı Ceza Muhakemesi Kanununun 81 inci maddesi ile 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunun 21 inci maddesi hükümlerine göre alınan parmak izleri de bu sisteme kaydedilir. (a) bendi hariç birinci fıkra ile dördüncü fıkra kapsamına giren kişilerin ayrıca fotoğrafları alınarak, ikinci fıkrada belirlenen esaslara uygun olarak parmak izi ile birlikte sisteme kaydedilir. 1412-1 Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir. Kolluk birimleri, kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir. Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur. Sistemde yer alan kayıtlar gizlidir; altıncı ve yedinci fıkralarda belirlenen amaçlar dışında kullanılamaz. Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir. Parmak izi ile fotoğrafların sistemde kaydedilmesi ve saklanması ile bu kayıtlardan yararlanmaya ilişkin diğer esas ve usûller, İçişleri Bakanlığı tarafından Adalet Bakanlığının görüşü alınarak çıkarılacak yönetmelikle düzenlenir. Daha ayrıntılı bilgi için bkz. Zeynep Bayram, **Kolluğun, Suç Öncesi Ve Sonrası Kişisel Veri Toplama Yetkisi**, Yüksek Lisans Tezi İstanbul, 2009

[46] Kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek ve tüzel kişiler, Maliye Bakanlığının veya vergi incelemesi yapmaya yetkili olanların istiyecekleri bilgileri vermeye mecburdurlar. Bilgiler yazı veya sözle istenilir. Sözle istenen bilgileri vermeyenlere keyfiyet yazı ile tekit ve cevap vermeleri için kendilerine münasip bir mühlet tayin olunur. Bilgi istenmek üzere ilgililer vergi dairesine zorla getirilemez. Memleket dışı imtiyazlarından faydalanan yabancı Devlet memurları bilgi verme mecburiyetine tabi olamazlar.

[47] İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.

Hizmetleri Kanunu 1. madde[48], Elektronik Haberleşme Kanunu 51, 55 ve 56. madde [49], Elektronik İmza Kanunu 12. madde[50], İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun 3. maddede[51] yapılan düzenlemeler bu konuda örnek gösterilebilir.

Türk hukukundaki bu düzenlemelerle birlikte 4721 sayılı Türk Medeni Kanun'u için ayrı bir başlık açmak gerekir. KVKK 1. maddesinde de belirtildiği üzere Kanun'un en önemli amacı özel hayatın ve kişilik haklarının korunmasıdır. Bu durum ise TMK ile bire bir ilişkilidir. Veri sahibinin, kişilik hakkını ihlal eden veri sorumlusu ve veri işleyeninin KVKK dışında ayrıca TMK'dan da sorumluluğu doğacaktır. TMK 24. maddesine göre kişilik haklarına yapılan saldırılar kural olarak hukuka aykırı kılınmış olup, bu saldırılara maruz kalan kimseler hakimden saldırılara karşı koruma

[48] Bu Kanunun amacı; kişinin doğumundan ölümüne kadar kişisel ve medenî durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukukî olayların belirlenip saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamaktır.

[49] Md. 51 Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir. Madde 55 (1) Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz. (2) Elektronik kimlik bilgisi değiştirilmiş cihaz, kart, araç veya gereçlerle, değişiklik yapılması amacına yönelik yazılım, her türlü araç veya gereçlerin ithalâtı, üretimi, dağıtımı veya tanıtımı yapılamaz, bulundurulamaz, aracılık edilemez. (3) Elektronik kimlik bilgisi değiştirilmiş cihaz, kart, araç veya gereçlerle, değişiklik yapılması amacıyla kullanılabilen yazılım, her türlü araç veya gereçlere 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 127 nci maddesi hükümlerine göre el konulur. Madde 56 – (1) Abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz, kendisine veya başkasına yarar sağlamak maksadıyla kullanılamaz. (2) İşletmeci veya adına iş yapan temsilcisine abonelik kaydı sırasında abonelik bilgileri konusunda gerçek dışı belge ve bilgi verilemez. (3) Abonelik tesisi için gerekli kimlik belgeleri örneği alınmadan işletmeci veya adına iş yapan temsilcisi tarafından abonelik kaydı yapılamaz. (4) Abonelik tesisine ilişkin usul ve esaslar Kurum tarafından yönetmelikle belirlenir.

[50] Elektronik sertifika hizmet sağlayıcısı; a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez, 8723 b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz, c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

[51] İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür. (2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkan tarafından iki bin Türk lirasından elli bin Türk lirasına kadar idarî para cezası verilir.(1)(2) (3) (Ek: 6/2/2014-6518/86 md.) Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir.

isteyebilecektir.[52] Nitekim KVKK öncesi yargı içtihatlarına bakıldığında Anayasa'da özel hayatın korunması ilkesi ile TMK 24. maddeye sıklıkla atıf yapıldığı görülür.[53]

Türkiye'de bilişim teknolojilerinin gelişmeye başlamasıyla birlikte, kamu yararı gözetilerek hızlı bir şekilde birçok kamu kurumu ve özel kurum içerisinde veri tabanları oluşturulmuştur. Kamu sektöründe UYAP, E-Devlet, TAKBİS gibi geniş çaplı veri tabanları kurulmuştur. Bu projelerle birlikte vatandaşın aracısız olarak belirli kamu hizmetlerinden yararlanmasının önü açılmıştır. Bunun yanında internet bankacılığı uygulamaları gibi kişilerin verilerinin depolandığı veri tabanları da özel kurum sistemlerinde hızla yaygınlaşmıştır. Kısa süredeki bu hızlı gelişimi ve kişisel verilerin kontrolsüz işlenmeleri de, bireylerin temel hak ve özgürlüklerinin ihlal edilmesine neden olmuştur.[54] Örneğin 2009 yılındaki Yüksek Seçim Kurulu (YSK)'nın askı seçmen listelerinin derlenmesiyle birlikte SEÇSİS üzerinden ülke vatandaşı 50 milyon kişinin bilgileri toplanmış ve satışa çıkarılmıştır.[55] Şuan dahi bazı torrent sitelerinden 2008 itibariyle 18 yaşını geçmiş ve hayatta olan yaklaşık 50 milyon vatandaşın TC kimlik no.su, doğum tarihi, anne baba adı gibi kişisel verilerine ulaşılması mümkündür. Sonuç olarak gelişen ve değişen şartlar altında Türkiye'de kişisel verilerin korunmasına ilişkin çalışmalar geç başlamış olduğu gibi çerçeve kanun tasarıları da 2016 yılına kadar kanunlaşamamıştır.

Kişisel verilerin korunmasının Türk hukuk sistemindeki normlar hiyerarşisinin en üstünde, yani Anayasada, yer bulması 2010 yılındaki anayasa değişikliği ile gerçekleşmiştir. Anayasanın 20. Maddesine *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir.*

[52] 4721 sayılı Türk Medeni Kanun'u m. 24.

[53] Yargıtay 11. Hukuk Dairesi'nin 02.07.2012 tarih 2011/4104 esas 2012/11588 karar no.lu ilamı, Yargıtay 4. Hukuk Dairesi'nin 01.10.2013 tarih 2012/16267 esas 2013/15422 karar no.lu ilamı bu hususta örnek gösterilebilir.

[54] A. Eda Manav, **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması,** Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, Y. 2015, Sa. 2, s.96.

[55] http://www.hurriyet.com.tr/gundem/kimlik-bilgileri-calindi-simdi-ne-olacak-40083035 20.05.2019

Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü eklenmiştir. Böylece yukarıda belirtmiş olduğumuz gibi birçok kanun ve yönetmelikte kişisel verilerin korunmasına ilişkin hüküm yer almış olsa da bu değişiklik ile birlikte kişisel verilerin korunması hakkına anayasal güvence sağlanmıştır. Ayrıca anayasanın başlangıç metninde *"yurttaşların hukuk düzeni içinde onurlu bir hayat sürdürme ve maddi ve manevî varlığını geliştirme hak ve yetkisine doğuştan sahip olduğu"* belirtildiği gibi, madde 17/(1) de ise *"herkesin maddi ve manevî varlığını koruma ve geliştirme hakkına sahip olduğu*" hükmü yer almaktadır.

4.2. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Kanun öncesinde ülkemizde kişisel verilerin korunmasına ilişkin özel bir kanun hazırlama düşüncesi 80'li yılların sonlarına kadar dayanmaktadır. 1989 yılında mecliste bir komisyon oluşturulmuş ancak tamamlanamamıştır. [56] İkinci olarak ise 2000 yılında yeni bir komisyon kurulmuş ve tasarı hazırlanmış ancak kanunlaştırılamamıştır. Üçüncü olarak ise 2008 tarihinde yeniden bir tasarı hazırlanmış ve seçimler nedeniyle kadük kalmıştır. Dördüncü olarak ise 2014 senesinde tekrardan bir tasarı hazırlanmış ve tekrardan seçimler sebebiyle kanun çıkarılamadan hükümsüz kalmıştır.[57] Nihayetinde 2016 yılında yeniden tasarı hazırlanmış, aynı yıl kanunlaştırılmış ve 7 Ekim 2016 tarihi itibariyle yürürlüğe girmiştir.

Kişisel verilerin korunmasına ilişkin çerçeve kanuna ihtiyaç duyulma sebebine 6698 sayılı KVKK'nın genel gerekçe kısmında değinilmiştir. Kısaca özetlemek gerekirse şu şekilde sıralama yapılabilir:

* Ülkemizdeki insan haklarının korunmasına ilişkin algının ve bilincin gelişmesi,

* 2010 anayasa değişikliği sonrası kişisel verilerin korunması hususunda çerçeve bir yasaya duyulan ihtiyaç,

[56] Sedat Erdem Aydın, **AİHM İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu,** Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2014, s. 98.

[57] İbrahim Korkmaz, **Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme**, TBB Dergisi, S.124, 2016, s. 86.

* Bilişim sektöründeki gelişmeler karşısında denetim mekanizmasının yetersiz kalması,

* Gerek 5237 sayılı TCK 135. Maddesi vd. maddelerinin gerekse de 4721 sayılı TMK 24. maddesi vd. maddelerinin kişisel verilerin ihlaline ilişkin hukuki uyuşmazlıklarda soyut kalması,

* AB'ye tam üyelik sürecinde fasıllardan dördünün doğrudan kişisel verilerin korunması ile ilgili olması,

* Europol ile ülkemizdeki güvenlik birimlerinin arasındaki işbirliğinin etkin bir şekilde yapılamaması, bu alanda Türk hukukundaki mevzuat boşluğunun bilgi değişiminin önüne geçmesi,

* Suçlarla mücadeleye yönelik Euro Just ile operasyonel bağlantılarda çeşitli sıkıntıların çıkması ve uluslararası suçlarda AB ve üye ülke yargı organları ile organize hareket edilememesi,

* Ülkemizde yaşayan yabancılar ile yurt dışında yaşayan Türkler açısından askerlik, kimlik, vatandaşlık ve malvarlığı gibi konularda üye ülkeler ve AB ile yaşanan veri paylaşımı problemleri,

* Özellikle sağlık sektörü kuruluşlarınca hassas verilerin sıkça kullanılıyor ve veri tabanında tutuluyor olmasına rağmen var olan mevzuatların yaptırım ve denetim için yetersiz kalması,

* Kişisel verilerin korunmasına yönelik birçok uluslararası düzenlemeye taraf olunmasına rağmen iç hukukta yeterli korumayı sağlayacak düzenlemenin mevcut olmaması KVKK'nın ortaya çıkışına sebebiyet veren problemlerdir.[58]

KVKK'nın 1. Maddesinde de belirtildiği üzere Kanunun en önemli amacı özel hayatın ve kişilik haklarının korunmasıdır. Kişisel verilerin korunmasına ilişkin KVKK, ilgili kişinin temel hak ve hürriyetlerini korurken diğer yandan da veri sorumlularının,

[58] KVKK genel gerekçe.

verileri işleme amacını ve bu amaca yönelik ihtiyaçlarını da dengede tutmalıdır. Tüzüğün ilk maddesini incelediğimizde, *"gerçek kişilerin kişisel verilerinin işlenmesiyle ilgili olarak veri sahiplerinin hak ve özgürlüklerinin korunmasına ilişkin kurallar ve kişisel verilerin serbest dolaşımına ilişkin kurallar belirlenir"* hükmünün yer aldığını görmekteyiz.[59] Kanunun amaç kısmında ise sadece temel hak ve özgürlüklere atıf yapılmış verinin serbest dolaşımına yani madalyonun diğer yüzüne değinilmemiştir.

Çerçeve bir kanunun ortaya çıkışındaki tüm bu sebeplerle birlikte Kanun'un genel gerekçesini ele aldığımızda asıl önemli problemin ekonomik sebepler olduğu görülmektedir. Gerçekten de Direktif'in 25. ve 26. maddelerine bakıldığında yeterli korumanın olmadığı ülkelere veri transferlerinin önüne geçildiğini görmekteyiz.[60] Ayrıca genel gerekçedeki sebeplerin büyük çoğunluğunun temel hak ve özgürlüklerin korunmasından ziyade ticaret, güvenlik, sağlık, sigortacılık, bankacılık ve hukuk alanları gibi birçok alanda uluslararası veri aktarımının sekteye uğramasının önüne geçilebilmesi için Kanun'un ortaya çıktığı vurgulanmaktadır. KVKK ile birlikte Birlik ve üye ülkeler ile veri aktarımı noktasında birçok problemin de nihayete erdirileceği düşünülmektedir.

KVKK'ya duyulan ihtiyacın önemli bir sebebi de veri bankalarının sayısının artması ve ihlallerin önceden önüne geçebilmek için önleyici tedbirlerin alınması gerekliliğidir. KVKK ile gelen önleyici ve zorlayıcı koruma sayesinde kişilerin hakları ihlal edilmeden önüne geçilebilecek ve hem veri işleyen, hem veri sorumlusu, hem de veri sahibi tarafından bir ihlal neticesinde doğacak problemler önceden öngörülebilecektir. Bu sebeple KVKK ile birlikte kişisel verilerin korunması düzen altına alınmakta ve genel ilkeler belirlenmektedir.[61] Sonuç olarak özel bir kanun olan KVKK, kişisel verilerin kullanılmasından kaynaklı kişi hak ve özgürlükleri ile ilgili

[59] GVKT m.1.

[60] İbrahim Korkmaz, s. 85.

[61] Nurullah Tekin- **Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi,** Uyuşmazlık Mahkemesi Dergisi, Sayı 4, s. 250.

genel prensipleri somutlaştırmakta ve kişisel verilerin işlenmesini, hukuka aykırı bir fiilin varlığına karine olarak kabul etmektedir.[62]

5. Tüzük Ve Direktif'in Veri Sorumluları Ve Veri İşleyenleri Açısından Yer Bakımından Uygulanma Alanı

Tüzük'ün yer bakımından kapsamı, Türkiye'deki veri sorumluları ve veri işleyenler için büyük öneme sahiptir. Tüzük ile birlikte getirilen yeniliklerden biri de Tüzük'ün yer bakımından uygulanmasındaki değişikliklerdir. Tüzük'ün 3. maddesinde yer bakımından nasıl bir uygulama esas alınacağı belirtilmiştir. Anılan maddenin ilk fıkrasında *"Bu Tüzük, işleme faaliyeti Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisindeki bir veri sorumlusu veya işleyicinin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır."* hükmü yer almaktadır. Burada üzerinde durulması gereken husus *"işletme faaliyetidir*." İşletme kavramının gerek Türk hukukunda olsun gerekse de AB hukukunda olsun mevzuat temelli farklılıklar içerdiğini görmekteyiz. Örneğin 4857 sayılı İş Kanunu'nun ve 6102 sayılı Türk Ticaret Kanunu'nun işletme kavramına yaklaşımındaki farklılıklar açıkça görülmektedir.[63] Kişisel verilerin korunması hukukunda da Tüzük'teki işletme kavramının temelini Divan'ın *Weltimmo Kararı*[64] ile görmekteyiz. Her ne kadar Direktif'in 2. maddesinde işletme kavramına yer verilmişse de Divan'ın *Weltimmo Kararı'na* kadar bu kavram dar yorumlanmıştır. Tüzük'ün yürürlüğe girmesi ile birlikte ise mevzuat Divan'ın içtihadı ile paralel hale gelmiştir. Divan'ın kararına göre başka ülkenin sınırlarında "gerçek ve etkin bir faaliyet" göstermesi bir işletmenin Direktif kapsamında tutulması için yeterlidir.

---

[62] Develioğlu s. 21.

[63] 4857 sayılı İş Kanunu'nun ve 6102 sayılı Türk Ticaret Kanunu'nun işletme kavramına bakışı ile ilgili detaylı bilgi için bkz.Ahmet Taşkın, **İş Hukukunda İşletme Kavramı**, Çalışma ve Toplum, 2012/1, s. 75-112.

[64] Divan'ın 1.10.15 tarihli C-230/14 sayılı kararına konu olayda Slovakya merkezli Macaristan'da faaliyet gösteren bir emlakçılık şirketin Macaristan da ilgili kişilerin 1 aylık süreyle ücretsiz olarak ilanlarını paylaşmasına müsaade etmiş ve kişisel verilerini toplamıştır. Sonrasında ise ilgili kişilerin sistemden ayrılmak istemleri üzerine şirket kişisel verileri ilgililere geri vermeyi ve silmeyi reddetmiştir. Bunun üzerine Macaristan'daki Kişisel Verilerin Korunması Kurumu şirkete ceza kesmiştir. Bu karara karşı şirketin yargı yoluna başvurmasıyla da Macaristan Yüksek Mahkemesi Divan'a Slovakya kökenli şirket için ceza tesis etmenin 96/46/EC Direktifi'ne göre uygun olup olmayacağını sormuştur. Dava C-230/14 *Weltimmo s. r. o.* v *Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639. (daha detaylı bilgi için bkz. Develioğlu, s. 16 ve 17.)

Tüzük uygulama alanı bakımından Türk hukukunu asıl ilgilendiren kısmın 3. Maddenin 2. Fıkrası olduğunu söylemek gerekir. *"Bu Tüzük, işleme faaliyetlerinin aşağıdaki hususlarla alakalı olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde kurulu olmayan bir veri sorumlusu veya işleyici tarafından işlenmesine uygulanır. (a) Veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması veya (b) Davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi"* hükmü yer almaktadır. Bu fıkra ile belirli şartlar altında işletmesi Türkiye'de bulunan veri sorumlusu ve veri işleyenin, AB'de bulunmasa dahi sorumluluğu doğabilecektir.

3. maddedeki bu hükümle birlikte Tüzük'ün uygulama alanı oldukça genişletilmiştir. Maddenin (a) bendindeki "*Veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın*" tabiri geniş yorumlanmaya açıktır. İcaba davetin dahi bu bent kapsamında değerlendirileceği ve Tüzük'ün uygulama alanı bulacağı bu bent kapsamında ortaya çıkmaktadır. Bunun yanında da "*Birlik içerisindeki söz konusu veri sahiplerine"* ifadesi eklenerek uygulama alanı daraltılmış olup ürün ya da hizmet sunma niyetinde olan kişinin açıkça Birlik içerisinde bulunan gerçek kişilere yönelmiş olması gerekmektedir. Tüzük'ün 3. Maddesinin (b) fıkrasında ise ürün ya da hizmet sunma amacı açıkça zikredilmediği için Birlik üyesi gerçek kişilerin kişisel verilerinin izlendiği her somut olayda Tüzük uygulama alanı bulabilecektir.[65]

Bu fıkrayı bir örnek üzerinden açıklamak gerekirse, Türkiye'de zeytin ticareti yapan bir firmanın internet sitesinin olduğunu, sitenin Türkçe oluşturulduğunu, mal veya hizmet alımının yalnızca Türk Lirası üzerinden sağlandığını ve bu siteden alışveriş yapılması içinde e-posta ve bazı kişisel bilgilerin girilmesi gerektiğini düşünelim. Siteye Almanya'dan giren ve kişisel bilgilerini paylaşıp zeytin almak isteyen ilgilinin siteye sadece Avrupa Birliği'nden ulaşabilmesinin, mal ve hizmet temin etmek istemesinin Tüzük'ün 3. maddesi kapsamında korunması söz konusu değildir. Nitekim Divan'ın

[65] Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu,** 1. Basım, İstanbul, 2018, s. 33.

Weltimmo Kararı da bu yöndedir.[66] Ancak zeytin ticareti ile uğraşan şirketin internet sitesinin içeriğinde AB üye devletlerinin dillerinin ve para biriminin kullanıldığı ve mal veya hizmet sunumunun AB ülkelerine de yönelik olduğu düşünüldüğünde artık şirket tarafından kişisel verilerin ihlaline yönelik fiillerin Tüzük kapsamında olduğu söylenebilecektir. Bu itibarla zeytin ticareti yapan firmanın İtalya'dan getirmiş olduğu zeytini sattığını, internet sitesinin Türkçe oluşturulduğunu mal veya hizmet alımının yalnızca Türk Lirası üzerinden sağlandığını hedef kitlenin doğrudan Türkiye'de olduğunu düşündüğümüzde yine Tüzük kapsamı dışına çıkıldığını söyleyebiliriz.

Sonuç itibariyle kişisel verilerinin işlenmesinde, Tüzük kapsamındaki hak ve özgürlüklerinin ihlal edildiğini düşünen kişi, Tüzük'ün 3. maddesi kapsamında Tüzük'ten doğan haklarını AB'nin yetkili denetim makamından veri işleyen ve veri sorumlusu Türkiye'de olsa bile talepte bulunabilecektir. Burada ilgili kişi KVKK kapsamı ile birlikte Tüzük kapsamındaki haklardan da yararlanabilecek ve hatta Tüzük kapsamından doğan haklarını yabancılık unsuru dikkate alınarak Türk mahkemelerinden de MÖHUK 35. Madde kapsamında talep edebilecektir. Bu nedenle Türkiye'de bulunan veri sorumlusu veya veri işleyenin işletme faaliyeti kapsamında AB'de bulunan veri sahiplerine mal veya hizmet sunması halinde Tüzük'ün de uygulanma ihtimalinin doğacağını öngörmeli ve hak ve yükümlülüklerini Kanun ve Tüzük'ü dikkate alarak oluşturmalıdır.[67]

[66] Dava C-230/14 *Weltimmo s. r. o.* v *Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639. (daha detaylı bilgi için bkz. Develioğlu, s.18.)

[67] Develioğlu, s. 20.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL KAVRAMLARI VE İLKELERİ

1. Kişisel Veri

Kişisel veri kavramı *(personel data)* ilk olarak Türkiye'nin 1981'de imzaladığı, 2016 yılında da onayladığı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'de yer almaktadır.[68] Sözleşme'nin 2. maddesinde gerçek ve tüzel kişi ayrımı yapılmadan *"kişiyi tanımlayan ya da tanımlayabilen her türlü bilgi"* olarak belirtilmiştir. Direktif'in 2. maddesinde ise *"doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgi"* olarak tanımlanmıştır. Tüzük'ün 4. maddesinde tanımlar başlığında kişisel verinin ne olduğu *"tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir"* şeklinde belirtilmiştir. Kanun'un 3. maddesinde ise kişisel verinin, *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"* ifade ettiği belirtilmiştir.

AB hukukundaki çerçeve düzenlemelerde ve 6698 sayılı Kanun'daki tanımda kişisel verinin 4 ana unsurdan oluştuğu görülmektedir. Bir kişisel veriden bahsedilebilmesi için; "kişi", "bilgi", "belirli ya da belirlenebilir olma" ve "ilişkin olma" unsurları incelenmelidir.

1.1. Kimliği Belirli Veya Belirlenebilir Kişi

Kişisel verilerin korunması hakkının özünde özel hayatın korunması olduğu görülür. Özel hayatın korunması hakkı ise modern hukuk sistemlerinde gerçek kişiye aittir. Nitekim bir verinin kişisel veri olduğundan bahsedebilmemiz için Direktif'te de Tüzük'te de Kanun'da da veri sahibinin gerçek kişi olması gerektiğinden bahsedilmiştir. Tüzel kişilerin kişisel verilerinin korunması noktasında Tüzük ve Kanun'un kapsamı dışında kaldığını görüyoruz. Ancak Direktif'i incelediğimizde yine gerçek kişiler

[68] Murat Volkan Dülger-**KVK ve TCK Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması**, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3(2), Güz 2016, s. 105.

üzerinden açıklama yapılsa da[69] Direktif'in AB hukukundaki icrai alanı dikkate alındığında üye devletlerin tüzel kişileri de kapsar şekilde düzenlemeler yapmasına herhangi bir engel bulunmamaktadır.[7071] Aynı şekilde 2002/58/EC sayılı Direktif'te de elektronik haberleşme sektörüne ilişkin korumaların tüzel kişileri de kapsadığını görmekteyiz. 2008 yılındaki kişisel verilerin korunması tasarısında da tüzel kişilerin koruma kapsamına alınması söz konusudur. Anayasa Mahkemesi'nin 4.12.2014 tarih 2013/83 esas 2014/183 karar no.lu ilamında *"Anayasa'nın 20. maddesinde kişisel verilerin kişi bakımından korunma alanının gerçek kişiler ya da tüzel kişileri veya her ikisini içine alıp almadığı konusunda bir açıklık bulunmamaktadır. Maddenin gerekçesinde de buna ilişkin bir değerlendirme yoktur. Her ne kadar Anayasa'nın 20. maddesinde daha ziyade gerçek kişilerin özel hayatı ve bu bağlamda gerçek kişilere ilişkin kişisel verilerin korunma altında bulundurulduğu ileri sürülebilir ise de madde metninde kişisel verilerle ilgili olarak "herkes" tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerekeceği açıktır."* hükmüne yer verilerek tüzel kişilerin de Anayasanın 20. Maddesi kapsamında korunması gerektiğine hükmetmiştir.

Gerçek kişinin kişilik haklarının ne zaman başlayacağı TMK'nın 28. maddesinde[72] belirtilmiştir. Doğumla birlikte kazanılan kişilik hakkı Direktif, Tüzük ve Kanun'da paralellik göstermektedir. Ölüm sonrası kişisel verilerin korunması noktasında ise Tüzük'ün giriş kısmının 27. paragrafı üye ülkelerin iç hukukta bu hususta düzenleme yapabileceğini belirtmiş olmakla birlikte, Kanun'da bu hususa ilişkin

---

[69] 95/46/EC sayılı Direktif m.2.

[70] Danimarka, Avusturya, Lüksemburg ve İtalya bu kapsamda tüzel kişilere ait verileri de kendi ulusal kanunları çerçevesinde koruma altına almışlardır. Hüseyin Can Aksoy, s.19.

[71] Bir görüşe göre tüzel kişilerin verilerinin kişisel verilerin korunması hukuku kapsamında değerlendirilmemesi doğrudur. Korunan hukuk, özü itibariyle özel hayatın korunmasını kapsamaktadır. Özel hayatın gizliliğinin ihlali tüzel kişiler için mümkün değildir. Tüzel kişiler için ancak ticari sırların gizliliğinden söz edilebilir ki, bu durumda 6102 sayılı TTK, 5237 sayılı TCK gibi genel kanunların özel düzenlemeleri dahilinde değerlendirilmesini gerektirir. Nitekim Avrupa İnsan Hakları Mahkemesi'nin B. Company ve diğerleri v. Hollanda kararındaki emsal içtihadında da tüzel kişiliğe sahip şirketlerin yıllık mali tablolarını yayınlamak zorunda kalmalarına ilişkin kanuni düzenlemenin kişisel niteliği söz konusu olmadığından özel hayatın gizliliği kapsamında değerlendirilemeyeceğine hükmetmiştir. Sedat Erdem AYDIN,**AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu,** İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, s. 7., Benzer görüş Elif Küzeci, *Kişisel Verilerin Korunması,* s.316-318

[72] Madde 28- Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder.

herhangi bir düzenleme mevcut değildir. Örneğin genetik hastalığa sahip kişinin alt-üst soyu da aynı hastalığa sahip olabileceğinden, kişinin ölmesi halinde kişisel verilerinin kullanımının serbest kalması o kişi ile aynı kan bağına sahip kişilerin bu hususta ki haklarını ihlal edebilecektir. Bu durumla ilgili her ne kadar Kanun'da bir açıklık bulunmasa da konu 4721 sayılı TMK'nın genel hükümleri ve Kişisel Sağlık Verileri Hakkında Yönetmelik çerçevesinde değerlendirilebilecektir.

Kişisel verinin belirli ya da belirlenebilir olma noktasında Tüzük'ün 4. maddesinde *"tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir"* şeklinde açıklayıcı bir hükme yer verilmiştir. Belirlilik ya da belirlenebilirlik kavramı zamana ve mekana göre değişebilir olan bir kavramdır. Nitekim kişisel verilerin belirlenebilirliğine ilişkin ABAD'ın vermiş olduğu kararlarda da farklılıklar söz konusudur. Örneğin, ISP adreslerinin (internet servis provider) kişisel veri sayılıp sayılmayacağı ile ilgili ilk olarak kişinin kimliğinin tam olarak tespitinin mümkün olduğundan kişisel veri niteliği taşıdığı belirtilmiş,[73] sonraki bir kararında[74] ise makul şartlarda internet erişim sağlayıcısının veri sahibine ait bilgileri elde etme imkanının olduğu takdirde kişisel veri sayılabileceğini belirtilmiştir.[75] Bu sebeple AB ve Türk hukuku mevzuatında, belirlilik ve belirlenebilirlik kavramı tanımlanırken örneklendirici bir tarz izlenilmiş olup, zamanın ve yerin şartlarına göre denetim mekanizmalarının ve yargının emsal içtihatlarıyla somut olaya özgü nitelendirmelerin yapılması daha makul görülmektedir. Örneğin "Mehmet Yılmaz" ismi Türkiye'de belirlenebilirlik için geçerliliği olan bir kişisel veri değilken başka bir ülkede belirlenebilir kişisel veri olabilir. Aynı şekilde bir kişinin DNA örneği bundan bir asır öncesi için belirlenebilir bir kişisel veri sayılmazken bugünkü şartlarda kişisel veridir.

[73] Dava C-70/10 Scarlett Extended, EU:C:2011:771.

[74] Dava C-582/14 Breyer, EU:C:2016:779.

[75] Daha detaylı bilgi için: Mesut Serdar Çekin s. 34-38.

1.2. Bilgi

Bilgi, TDK'ye[76] göre kişinin veriye yönelttiği anlam olarak tanımlanmıştır. Bir veriye "bilgi" denilebilmesi için, veriyi elinde bulunduran kişinin kendisi olup olmadığına bakılmaksızın o veriye anlam yüklenmiş olmalıdır.[77] Kişisel veriyi tanımlarken bilgi hususunda da Kanun, Tüzük ve Direktif'te *"her türlü bilgi*" ifadesi yer almaktadır. Burada her türlü bilgi kavramının geniş yorumlanması gerekir. Yani bu bilgi ticari, siyasi, fiziksel olabileceği gibi, özel hayatı veya aile yaşamına dair de olabilir.

Kişisel verilerin korunması hukukunda bilginin gizli olması gerekmediği gibi bilginin içeriğinden gerçeği yansıtıp yansıtmadığına da bakılmadan kişisel veri kabul edilmektedir. Son olarak bilgi nesnel ya da öznel de olabilir.

1.3. İlişkin Olma

Kişisel verinin, Kanun, Tüzük ve Direktif kapsamında korunabilmesi için bilgi ile belirli ya da belirlenebilir kişi arasında illiyet bağının olması, yani bilginin o kişiye ilişkin olması gerekir. İlişkin olmayı ele alırken bilginin içeriğini, amacını veya nasıl bir sonuç doğuracağını ele almak gerekir.[78] Kanun, Tüzük ve Direktif yönünden ilişkin olma hususunda bir farklılık bulunmamaktadır.

2. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi Tüzük'ün 4. maddesinde *"toplama", "kaydetme", "düzenleme", "yapılandırma", "saklama", "uyarlama veya değiştirme", "elde etme", "danışma", "kullanma", "iletim yoluyla açıklama", "yayma veya kullanıma sunma", "uyumlaştırma ya da birleştirme", "kısıtlama", "silme veya imha*" gibi herhangi bir işlem veya işlem dizisi olarak tanımlanmıştır. Kanunun 3. maddesinde ise *"elde*

---

[76]TDK Sözlük, "Bilgi", http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&kelime=k%C3%B6ken%20bilgisi&guid=TDK.GTS.5b08c55b1ef2e4.37411547 20.05.2019

[77] Furkan Güneş Taştan, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması,** 1. Basım, İstanbul, s.37.

[78] Develioğlu**,** s.39.

edilmesi", "kaydedilmesi", "depolanması", "muhafaza edilmesi", "değiştirilmesi", "yeniden düzenlenmesi", "açıklanması", "aktarılması", "devralınması", "elde edilebilir hâle getirilmesi", "sınıflandırılması" ya da "kullanılmasının engellenmesi" gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir. Görüleceği üzere kişisel verilerin işlenmesi tanımlanırken her iki mevzuatta da fiiller olduğunca geniş ele alınmıştır. Tüzük'te, Kanundan daha fazla fiile yer verilmiş olmasının şu aşamada uygulamada anlam bakımından çokta farklılık yaratmayacağını söylemek yerinde olur. Nitekim Kanun'un gerekçesinde bu durum *"Kişisel verilerin işlenmesi kavramı geniş bir alanı kapsamaktadır. Buna göre kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade etmektedir."*[79] hükmüyle birlikte sayılması mümkün olmayan fillerin bu şekilde önüne geçildiği varsayılmıştır. Yani verilerin işlenmesine yönelik verilen işlemlerin tahdidi işlem olarak değerlendirilmemesi gerekir.

Verilerin otomatik işlenmesi ile anlaşılması gereken otomasyon sistemleri ile işlenme biçimidir ve uygulamada çoğunlukla veri işlemeleri bu şekilde olmaktadır. Kanun ve Tüzük'teki kişisel verilerin işlenmesinin elle ya da otomatik olabileceği ayrıca vurgulanmıştır. Her iki düzenlemeden de çıkarılacak sonuç, bir kişisel veriden bahsedebilmemiz için verinin bulunduğu ortamın bir öneminin olmadığıdır.[80]

3. Veri Sorumlusu Ve Veri İşleyen

Veri sorumlusunun tanımı Kanun'un 3. maddesinde "*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmıştır. Tüzük'ün 4. maddesindeki veri sorumlusu *(controller),* Direktif'e benzer şekilde tanımlanmıştır. Tüzük'ün tanımı, Direktif ve Kanun'a nazaran daha açıklayıcı olsa da özü itibariyle bir farklılık yaratmamıştır. Her üç yasal düzenlemede de kişisel veri sahibinden farklı

[79] 6698 KVKK m.3.

[80] Deniz Alp İmamoğlu, **6698 KVKK Uyarınca Özel Nitelikli Kişisel Verilerin İşlenme Şartları**, İstanbul, 2017, s.11

olarak tüzel kişi kamu kurumu ve kuruluşlarının veri sorumlusu ve veri işleyen olarak değerlendirilmesi mümkündür.

Her üç tanımda da veri sorumlusu kişisel verileri elinde bulunduran kişi olarak tanımlanmamıştır. Çünkü aksi takdirde özellikle bulut sistemi gibi veri tabanına kaydedilen durumlarda bulut sistemi sahibi kurumun veri sorumlusu gibi değerlendirilmesi problemi ortaya çıkacaktır. Dolayısıyla veri sorumlusu ilgili kişinin kişisel verilerini işleme amaçlarını ve hangi vasıtalarla bu verileri işleyeceğini belirleyen kişidir. Aksi bir durum bulut teknolojisi şirketleri gibi veri depolayabilen iştirak ve kuruluşları her işlem karşısında bizzat sorumlu, müşterek veya müteselsil sorumlu durumuna getirecektir. Bununla birlikte bulut teknolojisi şirketin veya veri tabanı olan bir firmanın elindeki bilgileri kullanmaya başlaması durumunda veri sorumlusu haline gelebileceği bilinmelidir.

İşlemenin vasıtalarını ve amacını belirleyen birden fazla kurum, kuruluş, gerçek veya tüzel kişiden bahsediliyorsa bu durumda Tüzük'ün 26. maddesinde de belirtildiği gibi ortak veri sorumluluğu söz konusu olacaktır. Ancak Tüzük'ün 26. maddesine benzer bir hüküm Kanun'da bulunmamaktadır. Bu itibarla aynı durumun ortaya çıktığı hallerde 6098 sayılı Türk Borçlar Kanunu'ndaki genel hükümlerden kıyas yoluyla müşterek ve müteselsil sorumluluktan bahsedilebilecektir.

Tüzük'ün 4. maddesinde, Kanun'dan farklı olarak alıcı *(recipient*) ve üçüncü kişi *(third party)* tanımı yapılmıştır. Buna göre, üçüncü kişi Tüzük'te tanımlanan veri sorumlusu ve veri işleyeni dışında ancak bu kişilerin veya veri sahibinin kontrolü altındaki herhangi bir kişi, kurum veya kuruluştur.[81] Aktarılan ise, kişisel verilerin açıklandığı herhangi bir kişi, kurum veya kuruluştur.[82] Tüzük'te tanımlanan bu iki kişinin ayrımında üçüncü kişilere yapılan aktarımlarda farklı bir hukuki ilişki söz konusu olacağından veri sahibinin açık rızası ya da başka bir hukuka uygunluk halinin bulunması gerekir.

[81] GVKT m.4/(10)

[82] GVKT m.4/(9)

Kanun'da ise üçüncü kişinin tanımı yapılmamakla birlikte bazı kısımlarında üçüncü kişiye değinilmiştir. Bunun yanında veri sorumlularının yükümlülükleri kısmında veri sorumlusu ve *"yetkilendirdiği kişi"* denilerek veri sorumlusunun sorumluluğu altında farklı bir kişi kurum ya da kuruluştan bahsedilmiştir. Ancak sadece bahsedilmekle yetinilmiş ve yetkilendirilen kişinin hukuki sorumluluğu ve hangi şartlar dahilinde yetkilendirileceği ile ilgili bir hükme yer verilmemiştir. Aslında burada değinilen kişinin Tüzük'teki aktarılan kişi ile benzer olduğunu söylemek yanlış olmayacaktır. Bunun yanında Tüzük'ün 4/1-b bendindeki tanımın, günümüzde alanında uzmanlaşmış bilişim şirketleri ile verilerin işlendiği dikkate alındığında yerinde bir hüküm olduğu anlaşılmaktadır.[83] Her ne kadar Kanun'da yetkilendirilen kişinin hukuki statüsüne değinilmemiş olsa da Veri Sorumluları Sicili Hakkında Yönetmeliğin 4. maddesinde tanımı yapılarak kimlerin yetkilendirilen kişi olacağı belirtilmiştir. Birçok hükümde olduğu gibi burada da yetkilendirilen kişinin tanımının kanunla değil de yönetmelikle düzenlenmiş olması önemli bir eksikliktir.

4. Kişisel Verilerin İşlenmesinin Temel İlkeleri

KVKK	GDPR
Hukuka uygun dürüstlük kuralına uygun olma	Hukuka uygunluk, adil olma(hakkaniyet) ve şeffaflık
Doğru ve gerektiğinde güncel olma	Doğruluk ve gereken şekilde güncel olma
Belirli, açık ve meşru amaçlar için işlenme	Amacına uygun biçimde sınırlandırılma
İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma	Verileri ilgili ve ölçülü bir biçimde işleme
İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme	Amacı olan süre kadar saklanması
	Sorumluluk ve hesap verilebilirlik

Kişisel verilerin korunması hukukunda bilişim teknolojilerinin gelişmeye başlamasına ve ihtiyaçlara bağlı olarak değişen ulusal ve uluslararası mevzuatlarda

[83] Mesut Serdar Çekin s. 41.

verilerin işlenmesinin temel hak ve özgürlüklere uygun şekilde yapılabilmesi için bir takım ilkelerin geliştirilmesi gerekmiştir. Birbirinden ayırt edilebilirliği keskin çizgilerle belirlenmemiş bu ilkeler kimi zaman birbirlerini açıklayıcı kimi zamanda birbirlerini tamamlayıcı bir rol üstlenmişlerdir.

Kanun genel anlamda Direktif'e bağlı kalarak ilkeleri belirlemiştir. Tüzük'le Kanun arasındaki farklılıklar bulunsa da genel hatlarıyla birbirine benzer olduğunu söylemek yerinde olacaktır.

Hukuka ve dürüstlük kuralına uygunluk ilkesi Kanun, Tüzük ve Direktif'te kendine yer bulmuştur. Bu ilkeye, kişisel verilerin işlenmesinde diğer ilkeleri de kapsaması ve diğer ilkelerin kaynağı olması sebebiyle kişisel verilen işlenmesindeki ilk temel ilke diyebiliriz.[84] Hukuka uygunluk ilkesi ile kastedilen şey, kişisel verilerin korunmasına ilişkin mevzuata kişisel verinin işlenmesi sürecinin başından sonuna kadar riayet edilmesidir.[85] Bu sürecin içerisine kişisel verinin tanımının yapıldığı KVKK 2. madde, GVKT 4. madde ve Direktif 2. maddedeki bütün süreçler dâhildir.

Kanun'da yer alan *dürüstlük kuralı ilkesi* ve Tüzük'teki hakkaniyet prensibi özü itibariyle birbirinden farklı kavramlar değildir. Türk Medeni Kanunu'nun 2. maddesinde de yer alan bu ilke, bir hukuki ilişkide (yazılı olsun ya da olmasın), güven duygusunun zedelenmemesini öngören genel hukuk ilkesidir.[86] Dürüstlük kuralı bir anlamda özel hukuk alanının sigorta sistemidir.[87]

Şeffaflık ilkesine Kanun'da yer verilmemiştir. Aynı şekilde Direktif'te de temel prensipler arasında şeffaflık ilkesine değinilmemiştir. Tüzük'ün özellikle 13. ve 14. maddesi başta olmak üzere birçok maddesinde şeffaflık hususunda ayrıca değinildiğini ve şeffaflık ilkesine ayrı bir önem atfedildiğini söylemek yanlış olmayacaktır.[88]

---

[84] Akgül Aydın, **Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi,** Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, 2013, s.154.

[85] Küzeci, *Kişisel Verilerin Korunması***,** s.201.

[86] M. Kemal Oğuzman/Nami Barlas, **Medeni Hukuk**, 19. Basım, İstanbul 2013, s.253;

[87] Recep Çakrak/Samet İldeş **Kamu Hukuku Ve Özel Hukuk Açısından Dürüstlük Kuralı Ve Uygulama Alanı,** Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C.2 S.2, 2014, s.48.

[88] Bkz. GVKT m.12, m.13, m.14, m.26, m.40, m.41, m.42, m.43, m.53, m.88.

Şeffaflıkla ilgili Direktif ve Kanun'da ayrı bir madde yer almasa dahi, kişisel verilerin korunmasının dürüstlük kuralı ve hukuka uygunluk prensibi çerçevesinde değerlendirilmesi mümkündür.[89]

Kişisel verilerin toplanma amacının belirli, meşru ve açık olması gerekir. Bu prensip özü itibariyle veri sahibinin bilgilere erişim hakkıyla da bağlantılıdır.[90] Burada amacına uygun toplanma ifadesi Kanun, Tüzük ve Direktif'te de kullanılmıştır. Her ne kadar prensip ifade edilirken kişisel verilerin *"toplanması*" ifadesine yer verilmişse de kastedilen kişisel verinin toplanması dâhil sonrasındaki bütün işlemleri kapsayacak şekilde değerlendirilmesidir. Amaca bağlılık ilkesi bir anlamda bize kişisel verinin hukuka uygunluk prensibine riayet edilip edilmediğini denetleme yetkisi vermektedir.[91] Bu ilke asıl olarak önleyici bir koruma öngörmekle ilgili kişiye kendi verisi üzerinde denetim yapmayı olanaklı kılmaktadır.

Kanun'un 4/(2)-ç bendinde kişisel verilerin işlenmesinde işlendikleri *amaçla bağlantılı, sınırlı ve ölçülü olma prensibi* düzenlenmiştir. Aynı hüküm Tüzük'ün 5/(1)-c maddesinde düzenlenmiş ve aynı prensipler korunmuştur. Bu prensip gereği veri sorumlusu ilgili kişinin verisini toplarken amacına bağlı kalacak şekilde asgari sınırları gözeterek verileri toplamalı ve işlemelidir. Bu ilke öğretide yeterlilik ilkesi, verilerin asgarileştirilmesi, veri ekonomisi[92] veya veri minimizasyonu[93] olarak da adlandırılmaktadır.

Kanun'un 4/(2)-b bendinde kişisel verilerin işlenmesinin *doğru ve gerektiğinde güncel olma prensibi* düzenlenmiştir. Aynı hüküm Tüzük'ün 5/(1)-d bendinde de düzenlenmiş olup aksi durumda gecikmeksizin makul süre içerisinde silinmesinin yahut düzeltilmesinin gerektiği belirtilmiştir. Doğruluk ve güncellik prensibi temel hak ve özgürlükler ile maddi ve manevi zararın oluşmaması adına hem ilgili kişi için veri işleyenin amacına ulaşması adına hem de veri işleyen için önem taşımaktadır. Bu

[89] Küzeci, *Kişisel Verilerin Korunması***,** s. 201..

[90] Ibid.**,** s.203.

[91] Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008, s. 225

[92] Küzeci, *Kişisel Verilerin Korunması***,** s. 208.

[93] Devecioğlu, s. 47.

prensip aynı zamanda Kanun'un 11/(1)-d ve Tüzük'ün 16. maddesindeki ilgili kişinin kişisel verilerinin eksik ve yanlış işlenmiş olması halinde düzeltilmesini isteme hakkıyla doğrudan ilişkilidir.

Kanun'un 4/(2)-d bendinde *kişisel verilerin amacıyla sınırlı süre kadar saklanması prensibi* düzenlenmiştir. Aynı hüküm Tüzük'ün 5/(1)-e bendinde kendisine yer bulmuş olup her iki düzenleme de unutulma hakkı ile doğrudan ilişkilidir. Verilerin işlenmesi hem veri sahibi için hem de veri sorumlusu için başlı başına risk yaratmaktayken, amaca ulaşıldığı takdirde elde tutulmaya devam edilmesi veri güvenliği adına daha büyük riskleri beraberinde getirecektir. Kişisel veriye ihtiyaç duyulmadığı hallerde verinin silinmesi yahut anonimleştirilmesi gerekeceğinden, bu durumun da Kanun'un veri işleme halleri arasında sayılmasından ötürü, ayrıca diğer veri işleme prensiplerine de dikkat etmek gerekecektir. Buradaki sürenin ne kadar olacağı ise öncellikle mevzuatta bu hususta süreye ilişkin bir düzenleme olup olmadığına bakılarak eğer yoksa da dürüstlük prensibi dikkate alınarak belirleneceğinden, gerekmesi durumunda silinmesi gerekecektir.

Tüzük'ün 5/(1)-f bendinde *bütünlük ve gizlilik prensibine* yer verilmiştir. Kanunda kişisel verilerin genel ilkelerinin belirlendiği 4. maddede ise bu hususa ilişkin herhangi bir düzenleme yer almamaktadır. Aynı şekilde Tüzük 5/(2)'de de *hesap verilebilirlik ilkesine* yer verilmiş olup, Kanun'un 4. maddesinde bu hususa ilişin de bir düzenleme mevcut değildir. Kanun'da bütünlük ve gizlilik prensibini ayrı bir prensip olarak görmemekle birlikte özellikle 12/(4) fıkrası ile doğrudan ilişkilidir. Kanun'un 12/(4) fıkrasında veri sorumlusu ve veri işleyenin Kanun'a aykırı olarak kişisel verinin gizliliğini korumakla yükümlü oldukları ve başkalarına açıklayamayacakları düzenlenmiştir. Aynı şekilde hesap verilebilirlik ilkesi de Kanun'un 12. maddesindeki veri güvenliğine ilişkin veri sorumlusu ve veri işleyenine yüklenen yükümlülüklerle doğrudan ilişkilidir. Ancak Tüzük'te, veri sorumlusu ve veri işleyen için sorumlulukların düzenlendiği 4. kısım çok detaylı ve kapsamlı düzenlendiğinden, hesap verilebilirlik ilkesi ayrıca bir kişisel verinin işlenme prensibi olarak belirtilmiştir.

Görüldüğü üzere Kanun ile Tüzük arasında temel prensipler noktasında birçok benzerlikler söz konusudur. Kanun'da şeffaflık prensibi 4. madde kapsamında düzenlenmemiş olsa da ileride daha ayrıntılı inceleneceği üzere bu durum 11. madde kapsamında değerlendirilebilecektir. Nitekim şeffaflık ilkesinin Kanun'da prensip olarak belirtilmemiş olunması dürüstlük prensibi çerçevesinde değerlendirilmesinin de önüne geçmeyecektir. Aynı şekilde Kanun'un 4. maddesi kapsamında değerlendirilmeyen sorumluluk prensibinin 12. maddesine göre değerlendirilmesi de mümkündür.

Kişisel verilerin işlenmesi prensiplerinden amaca bağlılık ilkesine ayrıca değinmekte fayda vardır. Direktif'in uygulanması noktasında temel problemlerden birisi kişisel verinin işlenmesi sonrasında oluşacak amaç değişikliği halinde nasıl bir yol belirlenmesi gerektiğiydi. Kanunu incelediğimizde bu hususa ilişkin ayrıca bir hüküm ihtiva etmediğini görmekteyiz. Gerekçe kısmında ise amaç değişikliği halinde veri sorumlusu veri sahibinin yeniden rızasını almaya çalışacağını ya da Kanun'da öngörülen veri işlemesini haklı kılan hallerin var olması gerektiğine hükmedilmiştir. Tüzük ise amaç değişikliği halinde ilk olarak veri sahibinin rızası olması halinde "uygunluk denetimine" ihtiyaç duyulmayacağını belirtmiştir.[94] Aksi halde 6. maddenin 4. fıkrasında belirtilen haller dikkate alınıp işlenebilecektir. Bu fıkra kapsamında da işlendikleri amaçla sınırlı ve ölçülü olma ilkesinin açıklandığı fıkra kapsamında da görüleceği üzere Tüzük genel ilkeleri somutlaştırma yoluna gitmiştir. Kişisel verilerin prensipler ışığında işlenebilmesi için veri sorumlusuna gerekli önlemleri alması gerektiğini belirtmiştir. Kanun ise genel olarak kişisel verilerin işlenmesi prensiplerini belirtilmekle yetinmiştir. Sonuç olarak Tüzük'te düzenlenip Kanun'da sarih olarak düzenlenmeyen prensiplerin, Kanun'daki diğer prensiplerle ikamesi mümkündür. Ancak Tüzük'ün birçok noktasında atıf yapıldığı da dikkate alınarak şeffaflık, hesap verilebilirlik, amaçla bağlılık, bütünlük ve gizlilik prensiplerinin Tüzük 5. maddede ayrıca belirtilme ihtiyacı hissedilmiş ve ilkelerin uygulanabilirliği noktasında teknik önlemler alınması emredilmiştir.

[94] Mesut Serdar Çekin s. 49

5. Kişisel Verilerin İşlenme Koşulları

5.1. Rıza

Kişisel verilerin korunması hukukunda, kişisel verilerin işlenmesi halinde hukuka aykırılık bir karinedir. Tüzük madde 4/(11) de *"veri sahibinin 'rızası' veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir*" hükmü ile tanımlanmıştır.[95] Kanun'un 3. maddesinde ise açık rıza kavramı *"Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı"* anlatmaktadır. Yine Anayasa'nın değiştirilen 20. maddesinde kişisel verinin istisnalar hariç açık rızasıyla işlenebileceği belirtilmiştir.

Kanun'un gerekçesinde de açık rıza, 95/46 EC sayılı Direktif dikkate alınarak tanımlanmaktadır. Buna göre, *"açık rıza ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır"* şeklinde gerekçelendirilmiştir.

Açık rıza, şüpheye yer vermeyecek şekilde açık, anlaşılır ve kesin olmalıdır. Şüpheye yer vermeyecek şekilde olmasından kasıt sükûtun rıza için yeterli sayılıp sayılamayacağıdır. Hukuk sistemlerinde bazı hallerde susmayı yasal metinler ve yargısal içtihatlar kabul anlamında yorumlamıştır.[96] Öğretide kabul edilen bir görüşe göre, kimi durumlarda şüpheye yer vermeyecek şekilde örtülü irade beyanından kişisel verilerin işlenmesini kabul anlamı taşıyorsa açık rızadan bahsedilebilir.[97]

---

[95] Tüzük öncesinde ise rızanın hukuka uygunluk sebebi olması üye devletlerce farklı olarak tanımlanmıştır. Fransa'ya göre aynı Tüzük'te olduğu gibi verinin işlenmesinin hukuka uygun sayılabilmesi için açık rıza aranırken, Belçika için internet tarayıcısında otomatik ayarları değiştirmemek bu ayarlara uygun olarak kişisel verilerin işlenmesine rıza gösterildiği anlamına gelmektedir. Devecioğlu, s. 47.

[96] 6098 sayılı Türk Borçlar Kanunu'nun 4. maddesinde düzenlenen hükmün bir istisnasını, doktrinde çoğunluğun görüşüne göre bu duruma örnek gösterelebiliriz. "*Kural, susmanın irade beyanı sayılmamasıdır ve icaba cevap vermeyen kişi icabı kabul etmiş olmaz. Ama kanun belli hallerde ret cevabı vermeyi zorunlu kılmışsa ve kişi sükût etmişse artık icabı kabul etmiş sayabilir ve sözleşmenin kurulduğunu söyleyebiliriz.*" (M. Kemal Oğuzman, Turgut Öz, **Borçlar Hukuku Genel Hükümler**, 2014, İstanbul, C. 1, s. 68.)

[97] Benzer görüşte olanlar için bkz. Küzeci, *Kişisel Verilerin Korunması***,** s. 233, Nilgün Başalp, **Kişisel Verilerin Korunması Ve Saklanması**, 1. Basım, Ankara, 2004, s.40.

Tüzük'ün giriş kısmında açık bir irade beyanından ne anlaşılması gerektiği yönünde örneklendirmeye gidilmiştir. Verilen örneğe göre, ilgili kişi internet sitesinde yer alan "kişisel verilerimin işlenmesini kabul ediyorum butonunu" tıklıyorsa *(opt-in)* bu geçerli bir irade beyanıdır. Ancak işaret konulmuş bir halde geliyor ve ilgili kişi için hareketsizlikten, bir işlemeye rıza sonucu çıkarılıyorsa *(opt-out)* bu hukuka uygun bir işleme sayılmayacağı gibi açık rızadan da bahsedilemeyecektir. Bu durumda Tüzük'ün, hareketsiz kalmayı, açık rıza kapsamında kişisel verinin işlenmesini kabul etme olarak değerlendirmediği görülmektedir. Aksi durumda kişisel verinin işlenmesi için irade beyanının açık bir şekilde yerine getirilmesini istemenin pek bir anlamı kalmayacaktır.

Açık rızaya ilişkin diğer bir husus da ilgilinin iradesini bozacak şekilde rızaya mecbur bırakılmamış olmasıdır. Örneğin, işçi-işveren ilişkisinde yahut kiracı-kiralayan ilişkisinde olduğu gibi genel sözleşmenin ortaya konulacağı bazı durumlarda taraflar arasında güç dengesizliği bulunabilir. Bu tarz durumlarda rızanın özgürce ve baskı altında kalmadan verildiğinden bahsedebilmemiz için bazı ek güvencelere yahut yasal düzenlemelere ihtiyaç vardır.[98] Burada veri sahibinin özgür iradesinden bahsedilebilmesi için en önemli ayırt edicilik kendisinin veriyi paylaşmamak adına seçimlik hakkının olup olmadığıdır. Tüzük'ün giriş kısmında kamu kurumu ile ilgili olarak kişisel verilerin işlemesinde kişilerle arasında eşit şartların olmadığı ve bu sebeple daha dikkatli olunması gerektiği belirtilmiştir. Ayrıca Tüzük'ün 7. maddesinin 4. fıkrasında sözleşmenin ifası için gerek olmadığı halde kişisel verilerin işlenmesi şartına bağlı kılınıyorsa bu durumda bağlantı yasağından söz edilebilecektir. İlgili kişinin açık rızasını bozacak şekilde veri sahibinin tekel konumunda olması zorunlu olup olmadığı tartışmalı olmakla birlikte[99] bu hususta Tüzük'te ayrıca bir hükme yer verilmemiştir. Kanaatimizce veri sahibinin başka birisi ile sözleşmeyi ifa etmesi mümkün olduğu hallerde taraflar arasında güç dengesizliğinden söz edilemeyeceğinden özgür iradenin sakatlanmasından bahsedilemeyecek ve verilmiş açık rıza hukuka uygun olacaktır.

[98] Küzeci, *Kişisel Verilerin Korunması*, s.234

[99] Mesut Serdar Çekin s. 49

Açık rıza aynı zamanda genel nitelikte olmamalı ve ilgili kişinin aydınlatılmış bir rıza beyanı bulunmalıdır. Türk Borçlar Kanunu'nda genel işlem şartları 20 ila 25. maddelerde düzenlenmiştir. Genel işlem şartları, sözleşme yapılırken, taraflardan birinin benzer sözleşmeyi çok sayıda yapması sebebiyle tek başına hazırladığı sözleşmeyi karşı tarafa sunmasıdır.[100] Buna örnek olarak bankalardan alınan ihtiyaç kredileri için yapılan sözleşmeler ile GSM operatörü ile tüketicinin yapmış olduğu sözleşmeler gösterilebilir. Bu tarz sözleşmelerde genel itibariyle çok sayıda hükümden oluşan sözleşmeler çoğunlukla tüketicinin yazılı onayına sunulmaktadır. Bu sözleşmeler dürüstlük kuralına aykırılık teşkil edecek şekilde açık ve anlaşılır[101] değilse sözleşme imzalayan lehine yorumlanır.[102] Kanaatimizce aynı durum KVKK kapsamında veri sahibinin kişisel verisinin işleneceği durumlarda alınacak açık rızası için de gereklidir. Yani açık rızası alınacak kişinin aydınlatılmış olması gerekir. Veri sahibinin yeterli bilgiye sahip olması gerektiği Kanun'un gerekçesinde belirtilmiş olduğu gibi Tüzük'te de belirtilmiştir. Bu husus kişisel verilerin korunması hukukunda şeffaflık ve dürüstlük prensibinin birer yansımasıdır.

Açık rızanın yazılı olmasının geçerlilik şartı olduğu Kanun, Tüzük ve Direktif'te düzenlenmemiştir.[103] Bunun yanında açık rızanın yazılı olmaması halinde veri sorumlusunun, kişisel verileri hukuka uygun şekilde işlediğini ispat etmesi zorlaşacaktır. Tüzük, kişisel verilerin hukuka uygun tutulduğunun ispat külfetinin veri sorumlusunda olduğunu açıkça düzenlemiştir. Açık rızanın yazılı düzenlenmesiyle aslında korunan veri sorumlusudur diyebiliriz. Ayrıca ilgili kişi, rızasını her durumda geri alabilir. Rıza geri alınıncaya kadar yapılan her türlü hukuki işlemin geçerliliği devam eder. Açık rıza herhangi bir geçerlilik şartına bağlanmadığı gibi rızanın geri alınması da herhangi bir geçerlilik şartına bağlı değildir.

---

[100] 6098 sayılı TBK m.20.

[101] 6098 sayılı TBK m.25.

[102] 6098 sayılı TBK m.23.

[103] Ancak bazı ulusal düzenlemelerde yazılı rıza beyanı geçerlilik şartı olarak görülmüştür. Almanya Federal Kişisel Verilerin Korunması Yasası'na göre açık rıza beyanı yazılı olmalıdır. Aynı zamanda elektronik ortamda verilen kabullerde de yazılılık unsuru gerçekleşmiş sayılacaktır. Küzeci, *Kişisel Verilerin Korunması*, s.235

Çocukların kişisel verilerinin işlenmesinde nasıl bir yol izleneceği ile ilgili Tüzük'te ayrıca bir hüküm bulunmaktadır. Bu hükme göre en az 16 yaşında olan çocuğun, bilgi toplumu hizmetine[104] ilişkin sunulan hallerde beyanı esas alınabilir. Bu durum için asgari yaş sınırı 16 olarak gösterilmiş olup aksi bir durumda hukuka aykırı bir işlemden söz edilecektir. Çocuğun 16 yaşından küçük olması halinde ise ancak velisi tarafından izin veya icazet verilmesi halinde hukuka uygun bir işlemden bahsedilebilecektir. Tüzük ayrıca 13 yaş asgari sınırı belirterek her ne şartta olursa olsun üye devletlerin yasal düzenlemeyi bu yaşın altında yapamayacaklarını belirtmiştir. Kanun'da çocukların kişisel verilerinin işlenmesine ilişkin bir düzenleme yoktur. Bu sebeple genel hukuk hükümlerine dayanılacaktır.

5.2. Diğer Hukuka Uygunluk Halleri

KVKK	GDPR
Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması	Sözleşmenin kurulması ve ifası için gerekli olması
Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması	Veri sorumlusunun hukuki sorumluluğunu yerine getirebilmesi için gerekli olması
Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması	İşlemenin ilgili kişi veya üçüncü bir kişinin hayati menfaatlerini korumak için gerekli olması
Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması	
İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması	İşlemenin meşru menfaatlere ulaşmak için gerekli olması
İlgili kişinin kendisi tarafından alenileştirilmiş olması	
Kanunlarda açıkça öngörülmesi	İşlemenin kamu yararı için gerçekleştirilen bir görevin ifası veya veri sorumlusunun resmi yetkisini kullanması için gerekli olması

[104] Bilgi toplumu hizmeti Tüzük'ün 4. Maddesinin yönlendirmesi ile (AB) 2015/1535 sayılı Avrupa Parlamentosu ve Konsey Direktifi'nin 1/(1)-b bendinde tanımlanmıştır. Genellikle bir bedel karşılığında; ancak bedel alınması şart olmayıp belirli bir mesafeden, elektronik araçlarla sunulan ve almak için bireysel talebin gerektiği hizmetlerdir. Bkz. Directive (EU) 2015/1535 of the European Parlıament and of the Councıl of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)

Kanun ve Tüzük açık rıza dışında kişisel verilerin işlenmesinin hukuka uygun sayılacağı diğer halleri saymış ve örneklendirmeye gitmeden fıkralar halinde belirtmiştir. Tüzük, açık rızayı diğer hukuka uygunluk halleri ile birlikte değerlendirmiştir. "*İşleme faaliyeti, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve olduğu ölçüde, hukuka uygundur"*[105] hükmü ile birlikte açık rızayı, hukuka uygun bir veri işlemesinin oluşması için gerekli şartlardan biri olarak görüyoruz.

Kanun'un ifadesinde ise rıza öncelikli olarak ele alınmış ve *"Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür"*[106] hükmüne yer verilmiştir. Yani Kanun'un lafzından bir kişisel verinin işlenmesinde öncelikli olarak açık rızanın aranması gerekliliği üzerinde ayrıca durulmuştur. Nitekim 2. fıkranın başlangıç cümlesinin sonunda "*mümkündür*" ifadesiyle bu durum pekiştirilmiştir. Gerçekten de mümkündür ibaresi ile ortaya çıkan hukuki uyuşmazlıklarda hakime takdir yetkisi tanınmış ve salt 6. maddenin 2. fıkrasında sayılan hallerin varlığı halinde bir veri işlemesinin hukuka uygun sayılacağı anlamının önüne geçilmiştir.[107]

5.2.1. Kişisel Verinin İşlenmesinin Sözleşmenin Kurulması Veya İfası İçin Doğrudan Doğruya Gerekli Olması

Tüzük'ün 6/(1)-b bendinde Kanun'un ise 5/(2)-c bendinde veri sahibinin tarafı olduğu bir sözleşmeden dolayı sözleşmenin kurulması ya da ifası için verisinin işlenmesi gerekliyse bu işlemin hukuka uygun kabul edilebileceği düzenlenmiştir.

Her üç yasal metinde de birbirine benzer tanımları yapılan işbu esasın sözleşmeye ilişkin olarak ya sözleşme öncesinde ya da sözleşmenin uygulanması esnasında olması öngörülmüştür. Sözleşmenin neye dair olduğunun bu esasın uygulanabilirliği açısından bir önemi yoktur.

---

[105] GVKT m.6/(1)

[106] KVKK m.5/(2)

[107] Devecioğlu, s.58.

Veri sahibinin verisinin işlenmesinin bu esasa göre hukuka uygun kabul edilebilmesi için sözleşmenin ifası ya da kurulması ile verinin işlenmesi amacının benzer olması ve aynı saikler ile hareket ediliyor olması şarttır.[108] Örneğin bir iş başvurusunda bulunan veri sahibinin, iş akdi yapılması amacıyla kişisel verilerini alan veri sorumlusu, iş başvurusunun reddi halinde yahut akdinin feshinden sonra veriyi reklam veya pazarlama amacıyla kullanması halinde bu madde kapsamında hukuka uygun bir işleme olarak değerlendirilemeyecektir.

5.2.2. Kişisel Verinin İşlenmesinin Veri Sorumlusunun Hukuki Sorumluluğunu Yerine Getirebilmesi İçin Zorunlu Olması

Hukuka uygunluk hallerinden birisi de işlemenin veri sorumlusu için hukuki yükümlülüğünü yerine getirebilmesi adına zorunlu olmasıdır. Bu hukuka uygunluk hali Kanun m. 5/(2)-ç, Tüzük m. 6/(1)-c bentlerinde benzer mahiyette düzenlenmiştir. Buradaki düzenleme Tüzük açısından Birlik ve üye ülkenin hukukundan kaynaklanan yükümlülüklerken Kanun açısından ise Türk hukukundan kaynaklanan yükümlülüklerdendir.

5.2.3. Kişisel Verinin İşlenmesinin Veri Sahibi Veya Başka Bir Kişinin Hayati Menfaatlerinin Korunması Amacıyla İşlenmesinin Gerekli Olması

Tüzük'te işlemenin veri sahibi veya üçüncü bir kişinin hayati menfaatlerini korumak için gerekli olması ilkesi, 6/(1)-d bendinde düzenlenmiştir. Benzer mahiyette düzenleme Kanun'un 5/(2)-b bendinde de mevcuttur. Hayatının veya beden bütünlüğünün korunması için zorunlu olmasını özellikle doğal afetler gibi hallerde kişisel verinin işlenmesinin zorunlu olduğu, ancak ilgilinin rızasının alınmasının mümkün olamadığı durumlarda görmekteyiz. Hem Tüzük'teki hem de Kanun'daki düzenlemede de bu hüküm esas alınarak hukuka uygun bir düzenlemeden bahsedebilmek için hayatı söz konusu olanın kişinin kendisi ya da başka birisi olması

[108] Ibid., s.61.

önemli değildir ve bir hayati menfaatin[109] korunmaya ihtiyacı olması ve bu ikisi arasında illiyet bağının bulunması gereklidir.

5.2.4. Kişisel Verinin İşlenmesinin Kamu Yararı Adına Gerçekleştirilen Bir Görevin Yerine Getirilmesi İçin Veya Veri Sorumlusunun Resmi Yetkisini Kullanması İçin Gerekli Olması

Bu düzenlemede, Tüzük'teki düzenleme ile Kanun arasında farklılık vardır. Kanun'da *"kanunlarda açıkça öngörülmesi"* ifadesi kullanılmıştır. Maddenin gerekçesinde de "*2559 sayılı Polis Vazife ve Salahiyet Kanununun 5 inci maddesi uyarınca şüphelilerin parmak izlerinin alınması; 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetlerine ilişkin verilerini işlemesi"*[110] örnek gösterilmiştir. Kişisel verilerin korunması hakkı özü itibariyle bir insan hakkı olduğundan sınırlandırılması Anayasa'nın 13. maddesine göre yalnızca kanunla yapılabilir. Nitekim madde 5/(2)-a hükmünde bu hususa ayrıca değinilmiş ve kanunda öngörülmesini belirtmiştir. Diğer bir kıstas olarak ise kanundaki kişisel verilerin işlenmesine ilişkin düzenlemenin açık ve anlaşılır olmasının bir anlamda genel bir düzenlemenin buradaki işlemeyi hukuka uygun kılmayacağını belirtmiştir.

Tüzük'ün 6/(1)-e maddesini incelediğimizde ise açıkça Kanun'da düzenlenmesi gibi bir kıstasın olmadığını görmekteyiz. Tüzük'teki hüküm yalnızca kamu kurumlarına ilişkin bir hüküm olmayıp önemli olan kamu yararı için gerçekleştirilen bir görevin olmasıdır. Kamu tüzel kişiliği niteliğindeki meslek kuruluşlarının yapmış oldukları işlemler bu kapsamda değerlendirilebilir.[111] Aynı şekilde veri sorumlusunun kamu personeli olması değil yasal düzenlemenin vermiş olduğu resmi yetkisinin olması gerekir. Tüzük, bu iki hususla ilgili olarak 6. maddenin 2. ve 3. fıkralarında üye ülkelerde ve AB'de detaylı düzenlemelerin yapılabileceğini belirtmiştir.

---

[109] Kanun'un 5/(2)-b bendindeki hükümde hayati tehlikenin yanında *"vücut bütünlüğü"* de bu bent kapsamında hukuka uygunluk hali olarak düzenlenmiştir.

[110] KVKK m.5/(2)-a gerekçe.

[111] Kamu kurumu niteliğindeki meslek kuruluşlarının hukuki niteliği ile ilgili doktrinde farklı görüşler bulunmakla birlikte personeli ve malvarlığı bakımından mahiyeti itibariyle özel hukuk tüzel kişisi olan bu kuruluşların bazı durumlarda kamu gücünü kullanıyor olmaları bu kuruluşları kamu tüzel kişisi haline getirmeyecektir. Kemal Gözler, **İdare Hukuku,** C.1, Bursa, 1. Basım, 2009, s.607.

5.2.5. Kişisel Verinin İşlenmesinin Meşru Menfaatlere Ulaşmak İçin Gerekli Olması

Hükmün benzer işlenişi hem Tüzük'te hem de Kanun'da yer almaktadır. Burada meşru menfaat kısmının geniş yorumlanmaması ilgilinin kişisel verilerinin korunmasına ilişkin temel menfaatlerini korumak adına gereklidir. Meşru menfaatten anlaşılması gereken işlemenin hukuka uygun, veri sahibinin anlayabileceği açıklıkta ve güncel olması gerekliliği Tüzük tarafından gerekçe kısmında açıklanmıştır. Aksi takdirde hukuka aykırı bir şekilde yapılan işlemelerde meşru menfaatten bahsedilemeyecektir. Bunun yanında söz konusu menfaat veri sorumlusunun menfaati olmalıdır. Ayrıca kişisel verinin işlenmesi ile birlikte meşru menfaat arasındaki illiyet bağının olması gereklidir. Ancak ilgili kişinin verisinin işlenmesinin ulaşılacak meşru menfaate en iyi çözüm yolu olması gerekli değildir.[112]

Kanun'da menfaat dengesinin kurulabilmesi için ölçüt "ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi" olarak belirtilmiştir. Zarar verilmemesi kavramını ihlal edilmemesi olarak değerlendirilmesi mümkün olmakla birlikte Direktif'te menfaat dengesinin korunması için zarar verilmemesi kavramı yerine ilgili kişinin temel hak ve özgürlüklerinin veri sorumlusunun menfaatinden daha ağır basması gerektiği (override) belirtilmiştir.[113]

Tüzük 8. maddede veri sahibinin çocuk olması haline ayrıca değinmiş ve bu durumda uygulayıcıların meşru menfaati daha dar kapsamlı değerlendirmesi gerektiğini belirtmiştir. Kanun'da ve de gerekçesinde ise bu hususa ilişkin herhangi bir düzenleme yer almamaktadır.

5.2.6. Kişisel Verinin İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

Kanun'un 5/(2)-d bendinde Tüzük'te belirtilen hukuka uygunluk hallerinden farklı olarak ilgili kişi tarafından kişisel verilerinin alenileştirmesini de rıza dışında hukuka uygunluk sebebi göstermiştir. Kanunun 5. Maddesinin 2. Fıkrası ile ilgili hukuka uygunluk hali sayılan her bent için gerekçede örneklendirmeye gidilmiş

[112] Mesut Serdar Çekin s. 72.
[113] Ibid., s.73.

olmasına rağmen bu bentle ilgili herhangi bir örneklendirme yer almamaktadır. Burada alenileştirilmesi kelimesinin geniş anlamda kullanılmasının yerinde olmayacağı Kurul[114] ve öğreti[115] tarafından kabul edilmektedir. Şöyle ki; evinin satışı için bir internet sitesine kişisel verilerini koyan kişinin bu verilerin internet sitesi sahibi tarafında reklam amacıyla başka kişilere satılması yine hukuka aykırılık teşkil edecektir. Yine aynı şekilde herkese açık bir şekilde sosyal medyada fotoğraflarını paylaşan bir kişinin fotoğrafları değiştirilerek bir reklam malzemesi yapılması yahut kişilik haklarına saldırı oluşturacak şekilde fotoğrafı değiştirerek başka bir amaç için kullanılması hukuka aykırı olacaktır. Bu sebeple ilgili kişinin kişisel verisini alenileştirilmesiyle gerekçede belirtilmiş olduğu gibi, korunan menfaat tamamıyla ortadan kalkmayacak olup, yalnızca alenileştirmeyle sebep olan amaç ile bağlantılı ve sınırlı olması gerekmektedir.[116]

Sonuç olarak Kanun 5/(2) fıkrasındaki düzenlemelerin Direktif ile uyumlu olduğu söylenebilir. Gerek Tüzük'te gerekse de Kanun'da asıl olanın rıza olduğu vurgulanmıştır. Kanunun 5. maddesinin 1. fıkrasındaki "açık rıza olmaksızın işlenemez" hükmü ile Tüzük'ün 6. maddesinde rızanın tanım ve kapsamını belirleme yaklaşımından diğer hukuka uygunluk hallerinin birer istisna gibi yorumlanması gerektiği sonucu çıkarmalıdır. Aksi takdirde Avrupa Temel Haklar Şartı'nın 52/1 ve Anayasa'nın 13. maddesinde düzenlenen orantılılık şartı ihlal edilmiş ve hakkın özüne dokunulmuş olacak ve veri sahibinin menfaatleri zedelenebilecektir.

---

[114] *Ancak, kişisel verinin aleni kabul edilebilmesi için ait olduğu kişinin aleni olmasını istemesi gerekir. Başka bir ifade ile, alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin varlığı gerekir. Yoksa bir kişinin kişisel verisinin herkesin görebileceği bir yerde olması aleni olmasını sağlamaz. Ayrıca, alenileştirme durumunda kişisel verinin amacı dışında da kullanılmaması gerekmektedir.* Bkz. Kişisel Verilerin Korunması Kurulu, **Kişisel Verilerin İşlenme Şartları**, s.11 https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari 20.05.2019

[115] Küzeci, *Kişisel Verilerin Korunması***,** s.345.

[116] Daha detaylı bilgi için bkz. Merve Gözüküçük **Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi,** Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014, s.8-42.

5.3. Özel Nitelikteki Kişisel Verilerin İşlenmesi Açısından Hukuka Uygunluk Halleri

KVKK(m.6)	95/46/AT (m.8)	GVKT(m.9,10)
Irkı Ve Etnik Köken	**Irksal Veya Etnik Köken**	Irksal Ve Etnik Köken
Siyasi Düşünce	**Siyasi Görüş**	Siyasi Görüş
Felsefi İnanç	**Felsefi İnanç**	Felsefi İnanç
Dini Mezhep Ve Diğer İnançlar	**Dinsel İnanç**	Dinsel İnanç
Kılık Kıyafet	-	-
Dernek Vakıf Ve Sendikaya Üyelik	**Sendika Üyeliği**	Sendika Üyeliği
Sağlık	**Sağlık**	Sağlık
Cinsel Hayat	**Cinsel Yaşam**	Cinsel Yaşam Ve Cinsel Yönelim
Ceza Mahkumiyeti Ve Güvenlik Tedbirleri İle İlgili Veriler	**Ceza Mahkumiyeti**	Ceza Mahkumiyeti, Cezayı Gerektiren Suçlara İlişkin Ya Da Güvenlik Tedbirlerine İlgili Verilerin
Biyometrik Veriler	-	Biyometrik Veriler
Genetik Veriler	-	Genetik Veriler

Ulusal ve uluslararası yasal metinlerde ve öğretide *özel koruma gerektiren veri, hassas veri, özel tür veri olarak adlandırılan*[117] özel nitelikli veriler, diğer kişisel verilere nazaran veri sahibinin temel hak ve özgürlüklerini ihlalin daha fazla olabileceği verilerdir. Bu sebeple yasal düzenlemelerde özel nitelikli kişisel veriler ayrı bir korumaya tabi tutulmuşlardır. Özel nitelikli kişisel veriler, Kanun, Tüzük ve Direktif'te tanımı yapılmaksızın sayma yoluna gidilmiştir. Direktif'te özel nitelikteki kişisel verilerin asgari sınırlarının belirlendiğini, üye devletlerin bu durumu genişlettiğini ve bu sınırların üstünde düzenleme yaptığını görmekteyiz.[118]

[117] Örneğin, İngiliz Kişisel Verilerin Korunması Kanununda ve Yunan Kişisel Verilerin Korunması Kanununda Hassas veri, 108 sayılı Avrupa Konseyi Sözleşmesinde özel tür veri, Hollanda Kişisel Verilerin Korunması Kanunda özel kişisel veri, İspanyol veri koruma kanunda özel koruma gerektiren veri olarak tanımlanmıştır. Bkz. Hüseyin Can Aksoy, s. 30.

[118] Genetik veriler, Direktif'te özel nitelikli veri olarak düzenlenmemesine karşın Estonya, Bulgaristan, İzlanda ve Polonya'da var olan kişisel verilerin korunmasına ilişkin düzenlemelerde yer almaktadır. Aynı şekilde biyometrik verilerde Slovenya Slovakya ve Çeyka'daki yasal düzenlemelerde özel nitelikteki veriler arasında yer almıştır. Bunun dışında dernek üyeliği İtalya'da, ten rengi İzlanda'da, milli köken Çekya'da özel nitelikte veriler olarak veri koruma kanunlarında kendilerine yer bulmuştur. Daha ayrıntılı bilgi için bkz. Cemil Kaya, **Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler Ve İşlenmesi**, İÜHFM C.69, S. l-2, 2011, s.319.

Hassas verilere ilişkin benzer düzenleme olarak KVKK öncesinde ve hatta Anayasa'nın 20. maddesindeki değişiklik öncesinde 5237 sayılı TCK'nın 135. maddesinde yapılan düzenleme ile özel nitelikli verilerin kapsamı belirtilmiştir. TCK'nın 135. maddesinin gerekçesinde Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme dayanak olarak gösterilmiştir. Bu madde incelendiğinde, yürürlüğe girdiği tarih itibariyle yürürlükte olan Direktif'in kapsamı dahilinde etnik köken unsuruna TCK'da yer verilmemiş olup, yine Kanun, Tüzük ve Direktif'te yer almayan ahlaki eğilim kavramına ise yer verilmiştir.

Direktif'in özel nitelikteki kişisel verilerin kapsamına genetik ve biyometrik verileri dahil etmediğini görmekteyiz. Biyometrik ve genetik verileri Direktif'in sağlık verileri altında işlediğini, ayrıca belirtme gereğini duymadığını düşünmek yerinde olacaktır. Tüzük'ün özel nitelikli verilere ilişkin düzenlemesini incelediğimizde ise daha kapsamlı bir düzenleme görmekteyiz. Tüzük öncelikli olarak 4. maddesinde genetik verilerin, biyometrik verilerin ve sağlığa ilişkin verilerin tanımını yapmıştır. Sonrasında ise 9. maddede özel nitelikli verilerin neler olduğunu ve hangi istisnai haller halinde işlenebileceğini belirtmiştir.

Kanun ise, açık rıza hali dışında özel nitelikli kişisel verilere ilişkin işleme koşullarında ikili bir ayrıma gitmiştir. İlk olarak sağlık ve cinsel hayata ilişkin kişisel verilerin, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla işlenebileceğini belirtmiştir. Bu işlemeyi yapabileceklerin ise yalnızca sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar olduğunu söylemiştir. Bu şartların sağlanması halinde dolayısıyla kişinin açık rızasına gerek duyulmamıştır.[119]

Kanun'da bu madde kapsamında sayılan sağlık ve cinsel hayata ilişkin verilerin işlenmesi ise *"kanunda öngörülen haller"* kapsamında olacaktır. Kanun özel nitelikte olmayan verilerin işlenme şartlarının düzenlendiği 5. maddede dahi *"kanunlarda açıkça*

[119] KVKK m.6/(3).

öngörülmesini" hukuka uygunluk sebebi olarak belirtmişken özel nitelikteki veriler için açıkça ifadesini kullanmaması bir eksikliktir. Ancak kanunun gerekçesinin ilgili kısmını incelediğimizde yine 5. maddede olduğu gibi kanunun açıkça düzenlemesine atıfta bulunulmaktadır. Ayrıca gerekçede örneklendirme yoluna gidilerek askerlik yapacak kişilerin özel sağlık bilgileri ve sosyal güvenlik kurumunun kanunda belirtilen işlemleri gösterilmiştir.

Tüzük'ün 9. maddesinde ise özel nitelikli kişisel veriler ve işlenmesindeki istisnai haller aşağıdaki şekilde düzenlenmiştir: Kanun'da da yer aldığı gibi, veri sahibinin, verinin işlenmesine açık bir şekilde rıza göstermiş olması gerekir.[120] Veri sorumlusunun iş ve sosyal güvenlik hukuku çerçevesinde yükümlülüklerini gerçekleştirmesi amacıyla ve bu çerçevedeki işleme ile bağlı kalacak şekilde işlemenin gerekli olması halinde işlenebilir. Veri sahibinin fiziksel veya hukuki olarak rıza verememesi halinde veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin söz konusu olması halinde işlenebilir. Verinin işlenmesinin vakıf veya kar amacı gütmeyen bir kuruluşun meşru faaliyetleri çerçevesinde organ dışından açıklanmaması halinde işlenebilir. Özel nitelikteki kişisel veri, veri sahibi tarafından açık bir şekilde alenileştirilmişse işlenebilir. Adli sebeplerle ya da mahkemelerin yasal yetkisi dâhilinde işlenmesi halinde işlenebilir. Veri sahibinin temel hak ve özgürlüklerinin güvence altına alınmış olması halinde Birlik ve üye devlet hukukuna dayalı kamu yararı adına işlenebilir. Sağlık hizmetleri ve kamu sağlığı açısından işleme faaliyetlerinin gerekli olması halinde işlenebilir. Kamu yararına yönelik arşivleme, istatistik, bilimsel veya tarihi araştırmalar doğrultusunda yapılan işlemelerde özel nitelikli verilerin rıza dışında işlenmesi mümkün kılınmıştır.[121]

Direktif, Kanun ve Tüzük'te tıpkı birçok AB üyesi ülkenin kişisel verilerin korunması yasalarında görülebileceği gibi özel nitelikli kişisel verileri sayılabilir ve sınırlı sayıda *(numerus clasus)* düzenlemiştir. Bu durum öğretide eleştiri konusu yapılmıştır. Gerçekten de kimi ülkelerde özel nitelikte kişisel veri kapsamında bulunan mali veriler gerek Tüzük'te gerekse de Kanun'da özel nitelikte bir veri olarak

[120] GVKT m.9/(2)-a.

[121] GVKT m.9/(2)

öngörülmemiştir.[122] Yahut Kanun'da kılık kıyafet özel nitelikte kişisel veri olarak düzenlenmişken ilerleyen zamanda teknolojik gelişmelere bağlı olarak değişen ihtiyaçlar neticesinde yerini başka bir veri türüne bırakabilir. Sınırlı sayıda veri türüne özel nitelikte veri denmesi bazı durumlarda beklenileni karşılamayabilir. Örneğin, Kanun'da "ceza mahkumiyeti ve güvenlik tedbiri"[123] ile ilgili veriler özel nitelikli veriler arasında sayılmıştır. A kişisinin hakaretten kaynaklı olarak hakkında güvenlik tedbiri uygulanması halinde ilgili kişinin bu verisi artık özel nitelikli kişisel veriler arasında sayılabilecektir. Ancak B kişisinin çocuğa cinsel istismardan yargılandığı bir davada tutuklanması,[124] yargılama sonunda da beraat etmesi halinde bu yargılama ve tutukluluğa ilişkin verileri özel nitelikli kişisel veriler arasında değerlendirilmeyecektir. Çünkü güvenlik tedbirleri Kanun kapsamında özel nitelikte kişisel veriler arasında sayıldığı halde tutukluluk, yakalama, gözaltı ve adli kontrol kararı ise 5271 sayılı CMK'da düzenlenmiş koruyucu tedbirler arasında yer aldığından KVKK 7. maddesi kapsamında yer almayacaktır. Bu sebeple kişisel verinin özel nitelikte kişisel verilerden biri olarak değerlendirilebilmesi için hangi koşullarda işlendiği, işlenmesindeki amacı, işlenmesi sonrasında veri sahibi ya da üçüncü bir kişi için doğabilecek muhtemel sonuçlar ve menfaatler dikkate alınmalıdır. Kanun, Tüzük ve Direktif'te olduğu gibi sınırlı sayıda *(numerus clasus)* özel nitelikli kişisel veri düzenlemek yerine aynı verilerin örneklendirici biçimde sayılarak daha kapsamlı ve amaçla bağlantılı şekilde belirtilmiş olması daha uygun olurdu.

Özel nitelikli kişisel verilerin değerlendirilmesinde Divan ve AYM arasındaki bakış açısı farklılıkları da mevcuttur. Divan'ın 2003 tarihli *Lindqvist Kararı*'nda[125] özel nitelikli kişisel verilerin Direktif'te belirtilen unsurlardan daha geniş kapsamlı değerlendirilmesi gerektiğini belirtmiştir. AYM, KVKK yürürlüğe girmeden öncesine ait 3.4.2015 tarihli kararında[126] biyometrik verilerin kişisel veriler arasında

[122] Hüseyin Can Aksoy, s.32.

[123] Güvenlik tedbiri, 5237 sayılı TCK'nın 53 ila 60. maddelerinde düzenlenmiştir.

[124] 5271 sayılı CMK'nın 100 ila 108. maddelerinde göre düzenlenmiş tutuklama, bir koruyucu tedbirdir.

[125] Dava C-101/01 *Bodil Lindqvist*, EU:C:2003:596.

[126] AYM'nin kararında; *Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş,*

değerlendirilemeyeceğini belirtmiştir. KVKK neticesinde AYM'nin bu görüşünde farklılık olacağı kuşkusuzdur; ancak değerlendirildiği tarih itibariyle özel nitelikteki verileri dar kapsamda yorumladığı da aşikârdır.

Tüzükte; Direktif ve Kanun'dan farklı olarak özel nitelikli kişisel verilerin işlenmesinde zorunlu veri koruma görevlisinin atanması öngörülmüştür. Tüzük'ün 37. maddesinde, yargı faaliyetinin yürütülmesi hali hariç işleme, kamu kurumu veya kuruluşlarında yapılıyorsa, veri sorumlusu veya işleyicisinin esas faaliyetleri veri sahiplerinin büyük ölçüde veriyi izlemeyi gerektiren işleme faaliyetlerinden oluşuyorsa ve veri sorumlusu ve işleyenin faaliyetleri Tüzük'ün 9. ve 10. maddesinde belirtilen özel nitelikli verilerin büyük çaplı işlenmesinden meydana geliyorsa veri koruma görevlisinin atanması öngörülmüştür.[127] Veri koruma görevlisi, veri sorumlusunun ve veri işleyeninin çalışanı olabileceği gibi aralarında hizmet sözleşmesi imzalanmış başka bir kişi de olabilir. Aynı veri koruma görevlisinin, başka bir şirketin veri koruma görevlisi de olması mümkündür. Dolayısıyla Tüzük'ün 37. maddesi kapsamında sayılan işlemlerden veri koruma görevlisinin sorumluluğu söz konusudur. 38. maddede zorunlu veri koruma görevlisinin atanmasına neden ihtiyaç duyulduğu belirtilmiştir. Buna göre zorunlu veri koruma görevlisi; kişisel verilerin korunmasına ilişkin tüm konulara makul bir sürede ve uygun şartlar altında müdahil olması amaçlanmış, ilgili kişinin hak ve menfaatleri ihlal edilmeden zamanında önleyici tedbirlerin alınması ön görülmüştür.

---

resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Bu bağlamda itiraz konusu kuralla öngörülen biyometrik yöntemle elde edilen verilerin kişisel veri olduğunda kuşku yoktur. Bununla birlikte söz konusu verilerin, 108 sayılı Sözleşme'nin 6. maddesinde özel olarak belirtilen politik düşünce, dini inanç, sağlık, cinsel yaşam veya ceza mahkûmiyetlerine ilişkin veriler gibi çok hassas verilerden olduğu da söylenemez." hükmüne yer verilmiştir. (AYM'nin 19.3.2015 tarih 2014/180 esas 2015/30 karar sayılı ilamı) *bkz:* http://www.resmigazete.gov.tr/eskiler/2015/04/20150403-8.pdf 21.05.2019

[127] GVKT m.9/(2)-a.

6. Kişisel Verilerle İlgili İşlemler

6.1. Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hâle Getirilmesi

Kanun'da kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi 7. maddede düzenlenmiştir. Maddenin ilk fıkrasında yasal düzenlemelere uygun şekilde yapılan veri işlemelerinin, işleme için gerekli menfaatin ortadan kalkması halinde resen ya da talep halinde silinmesi, yok edilmesi ya da anonim hale getirilmesi öngörülmüştür.[128] Tıpkı kişisel verilerin işlenmesinde olduğu gibi silinmesi ya da anonim haline getirilmesinde de yasal düzenlemelerdeki ilke ve esaslara riayet edilmelidir.

Kanun'un ikinci fıkrasında ise konuya ilişkin diğer kanunlara atıf yapılmıştır. Gerekçe metninde Adli Sicil Kanun'una atıf yapılarak maddenin 2. fıkrası örneklendirilmiştir. Adli Sicil Kanunu'nda hangi şartlar altında kişisel verilerin arşivleneceği 12. maddede belirtilmiştir. Bu durumda özel bir düzenleme olduğundan KVKK'dan önce Adli Sicil Kanunu öncelikli olarak uygulanacaktır.

TCK'nın 138. maddesinde ise veri yok etmeme cezası yer almaktadır. İhmali bir suç olan 138. maddedeki bu hüküm 5271 Sayılı CMK hükümlerinden kaynaklı ise ayrıca ağırlaştırıcı bir suç niteliği taşır. Böylece TCK'nın 138. maddesinin gerekçesinde de belirtildiği üzere kişisel verilerin yok edilmesi için ilgili görevlinin keyfi davranışlarının önüne geçilmek istenmiştir.

Kanun 7. maddesinin son fıkrasında ise usul ve esasların yönetmelikle düzenleneceği belirtilmiştir. Nitekim 28.10.2017 tarihinde Resmi Gazete'de yayımlanan kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi hakkında yönetmelik çıkarılmış ve ayrıntılı bir düzenlemeye gidilmiştir.

Direktif'in 12. maddesine göre ise Kanun ile paralel olarak verilerin silinmesi ve yok edilmesinin ilgili kişi tarafından istenebileceği düzenlenmiştir. Tüzük'ün ise veri

[128] KVKK m.7.

sahibinin haklarının düzenlendiği 3. bölümün 17. maddesinde yer almaktadır. Bu konuya ayrıca veri sahibinin hakları başlığı altında tekrardan inceleneceğinden burada değinilmemiştir.

Verinin anonim hale getirilmesinden ne anlaşılması gerektiğinden Kanun'un 3. maddesinde tanımlar kısmında bahsedilmiştir. Bu tanıma göre anonim veri, kişisel verinin hiçbir halde gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Bu haliyle kişisel veri ile kişisel veri sahibi arasındaki bağ tamamen ortadan kaldırılmaktadır. Aksi halde yani veri sahibinin halen belirlenebilir olduğu durumda verinin anonimleştirilmesinden bahsedilemeyecektir.

Kanunda verilerin anonimleştirilmesi ile ilgili bu tanım Tüzük'te yer almamaktadır. Tüzük'ün tanımlar başlıklı 4. maddesinde veri anonimleştirilmesinden değil psödonimleştirmeden bahsedilmektedir. Kişisel verinin anonimleştirilmesi de psödonimleştirmesi de esas itibariyle veri sahibi ile kişisel veri arasındaki bağı koparmaya yöneliktir. Kişisel verinin anonimleştirilmesi neticesinde veri sahibi ile veri arasındaki bağ tam anlamıyla koparken, kişisel verinin psödonimleştirmesi halinde ise belli algoritmalar kullanılarak aradaki bağ bulanıklaştırılır.

Tüzük'ün giriş kısmının 26. bölümünde kişisel verinin tanımında olduğu gibi kimliği belirli veya belirlenebilir her türlü verinin kişisel veri kapsamında olduğu belirtilmiştir. Buna göre verilerin anonimleştirilmesi halinde söz konusu veri tıpkı Kanun kapsamında değerlendirilemeyeceği gibi Tüzük kapsamında da değerlendirilemeyecektir. Çünkü artık var olan veri, bir gerçek kişiye özgü değildir. Tüzük'ün giriş kısmının 28.ile 29. maddelerinde ise kişisel verileri psödonimleştirmenin veri sahibine olduğu gibi veri sorumlusuna da Tüzük'ten kaynaklı yükümlülüklerini yerine getirmesi için kolaylık sağlayacağı; ancak bu işlemlerin Tüzük'ün kapsamında kalmaya devam edeceği dikkatten kaçmamalıdır.

6.2. Kişisel Verilerin Aktarılması

Kanun'un 8. maddesinde kişisel verilerin, veri sahibinin açık rızası olmaksızın aktarılamayacağı düzenlenmiştir. Özel nitelikte olmayan kişisel verilerin 5. Maddenin 2.

fıkrasında belirtildiği hallerde, özel nitelikteki kişisel verilerin ise "yeterli koruma sağlanırsa" 6. Maddenin 3. Fıkrasında belirtilen hallerde aktarılabileceği belirtilmiştir.

Aslında Kanun ülke içi aktarımda, kişisel verinin işlenme hallerinden olan ve Kanun'un 2. maddesinde tanımı yapılan depolama, değiştirilme, sınıflandırma vs. hallerden farklı bir düzenleme getirmemektedir. Yani bir kişisel verinin Kanun kapsamında nasıl elde edilmesi ya da muhafaza edilmesi gerekiyorsa yurt içi aktarımda da aynı esaslar geçerli olacaktır.

Yurtiçi aktarımı düzenleyen maddede diğer kişisel verilerin işlenmesi hallerinden tek ayrıştığı nokta özel nitelikteki kişisel verilerin aktarımında yeterli korumanın sağlanması halinde aktarımın gerçekleşebileceğidir. Yeterli korumanın nasıl sağlanacağı hususunda gerek Kanun ilgili maddesinde gerekse de ilgili maddenin gerekçesinde açıklayıcı bir hüküm bulunmamaktadır. Bu durum yeterli önlemlerin alınması halinde Kanun'un veri sorumlusu ve işleyenin yükümlülüğüne ilişkin düzenlediği haller gözetilerek 22. maddesi uyarınca Kurul'un denetiminde değerlendirilecektir.

6.3. Kişisel Verilerin Yurt Dışına Aktarımı

Kanun'un, gerekçesinin birçok yerinde belirtildiği gibi yürürlüğe giriş sebeplerinden birisi de yurtdışı kişisel veri aktarımıdır. Tüzük, yurtdışına aktarım konusunda birçok yenilik getirmiştir. Tüzük ve Direktif kapsamında yurtdışına çıkış sözüyle anlaşılması gereken Birlik dışına çıkan kişisel veridir. Gerek Tüzük'te gerekse de Kanun'da yurtdışına aktarımın tanımı yapılmamıştır.

Tüzük ve Kanun, yurtdışına aktarımlarda ikili bir ayrım yapmıştır. Kanun'un 9. maddesinde Kurul'un izninin gerekeceği ve gerekmeyeceği hallerde yurt dışına aktarım düzenlenmiştir. Tüzük 45. maddesinde AB Komisyonu'nun uygunluk kararının gerektiği haller ile 46. maddesinde AB Komisyonu'nun uygunluk kararının gerekmediği halleri düzenlemiştir.

6.3.1. Bir Yeterlilik Kararına Dayalı Yapılan Aktarımlar

Kanun'un 9. maddesinde yurtdışı kişisel veri aktarımında da kural olarak yurtiçi aktarımında olduğu gibi ilgili kişinin açık rızasını aramıştır. İkinci fıkrada ise tıpkı yurtiçi aktarımda olduğu gibi Kanun'un 5. ve 6. maddesindeki haller belirtilmiş ve bu şartların birinin varlığı halinde aktarmanın yapılabileceğine hükmedilmiştir. Sonrasında ise ikili bir ayrıma gidilmiştir. Yurt dışına aktarım için ilk şart olarak yurt dışında aktarılacak yerde yeterli korumanın bulunması aranmıştır.

Yeterli korumayı verme yetkisi 9. maddenin 3. Fıkrası gereğince Kurula aittir. Kurul, yeterli korumanın olduğuna karar verebilmesi için maddenin 4. fıkrasında belirtilen şartların oluşup oluşmadığı kontrol edilecektir. Buna göre kurul: Türkiye'nin taraf olduğu uluslararası sözleşmeleri, kişisel verinin talep edildiği ülke ile Türkiye arasındaki veri aktarımı konusunda karşılıklılık olup olmadığını, somut duruma göre kişisel verinin niteliği ile işlenme amaç ve süresini, kişisel verinin aktarılacağı ülkenin konuya ilişkin yasal düzenlemelerini ve uygulamalarını, kişisel verilerin aktarılacağı ülkedeki veri sorumlusunun taahhüt ettiği önlemleri, ihtiyaç duyulması halinde ilgili kurum ve kuruluşların görüşünü almak suretiyle yabancı ülkede yeterli korumanın bulunup bulunmadığını değerlendirecektir.[129]

Tüzük'ün yurtdışına aktarım kısmı 44. 45. ve 46. maddelerinde Kanun ve Direktif'e nazaran daha detaylıca anlatılmıştır. Tıpkı Kanun'da olduğu gibi Tüzük'ün 45. maddesinde yurtdışı aktarımlarda Avrupa Birliği Komisyonu'nun kararı gereklidir. Uygunluk, yeterlilik kararı *(adequacy decision)* Direktif'in yürürlükte olduğu dönemde üye devletler tarafından ve AB Komisyonu tarafından alınabilmekteydi.[130] Tüzük ile birlikte yeterlilik kararının alınması AB Komisyonu'nun tekeline girmiştir. AB Komisyonu'nun yeterlilik kararı alabilmesi için gerekli şartların neler olduğu Tüzük'ün 45. maddesinde açıklanmıştır. Maddenin içeriği daha detaylı olmakla birlikte Komisyon, veri aktarımı için yeterlilik kararı verecekken özetle; hem genel hem de özel

[129] KVKK m.9/(4).

[130] Abad'ın Maximilian Schrems kararında Direktif ile birlikte AB Komisyonu'nun almış olduğu yeterlilik kararının üye devletlerin ilgili denetim makamları tarafından hükümsüz kılınamayacağı belirtilmiştir. Devecioğlu, s.74. karar için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 22.05.2019

sektörde kişisel verilen korunmasına ilişkin yeterli yasal düzenlemelerin yapılıp yapılmadığını, aktarım neticesinde veri sahibinin zararının oluşması halinde yeterli adli ve idari tazmin imkânının bulunup bulunmadığını, aktarılacak ülkede kişisel verilerin korunması hususunda yeterli denetim makamının oluşturulup oluşturulmadığını göz önüne alarak karar verecektir.[131] Ayrıca AB Komisyonu'nun verdiği kararla birlikte denetim ve yeterlilik şartlarının sağlanıp sağlanmadığını sürekli bir şekilde inceleyebilmesi için en geç dört senede bir vermiş olduğu kararı gözden geçirmesi gerektiği hükme bağlanmıştır. Bu süre azami olarak belirtilmekle birlikte Komisyon, yeterlilik kararını geri alabilir, belli bir müddet için durdurabilir yahut sonradan ortaya çıkan bir problem için sorunun giderilmesini isteyebilir.

6.3.2. Bir Yeterlilik Kararına Dayanılmadan Yapılan Aktarımlar

Kanun yeterli korumaya sahip olmayan verilerin aktarılması için açık rızanın olmadığı hallerde yine Kanun'un 5. ve 6. maddesindeki hallerden en az birinin gerçekleşmiş olmasını, Türkiye'deki ve ilgili ülkedeki veri sorumlularının yeterli bir koruma sağlanacağı hususunda yazılı taahhüt vermiş olmalarını ve Kurul'un bu konuya ilişkin izninin bulunmasını şart koşmuştur.

Kişisel verilerin aktarılmasında yeterlilik kararının aranmayacağı hallere ilişkin düzenleme Tüzük'ün 46. maddesinde düzenlenmiştir. Buna göre veri sorumlusu veya işleyeninin gerekli önlemleri alması ve veri sahibinin kişisel verilerinin işlenmesinden kaynaklı menfaatlerini koruyabilmesi için yeterli yasal düzenlemelerin olması halinde AB Komisyon'u tarafından alınacak yeterlilik şartı olmadan da aktarım yapılabilir.

Tüzük'ün 46. maddesi gerek Direktif'e gerekse de Kanun'a nazaran çok daha kapsayıcı ve kazuistik bir düzenlemeyi öngörmüştür. Buna göre, Tüzük 46/(2) maddesindeki yeterlilik şartı bulunmadan aktarım yapılabilmesi için kamu kurum ve kuruluşları arasında yasal bağlayıcılığı bulunan bir belgenin, bağlayıcı kurumsal

[131] GVKT m.45.

kuralların, standart veri koruma şartlarının, onaylı davranış kuralları ve onaylı belgelendirme mekanizmasının varlığı halinde aktarım yapılabilir.[132]

Bağlayıcı kurumsal kurallar Tüzük'ün 47. maddesinde düzenlenmiştir. Tüzük, ortak ekonomik faaliyet sürdüren özellikle büyük ölçekli kurum veya kuruluşların belirli şartlar altında aktarım yapmasını kolaylaştırmak istemiştir. Aksi takdirde birçok ülkede faal olan bir şirket kendi içerisinde veri aktarımı yaparken dahi büyük sıkıntılarla karşılaşabilecektir. Tüzük'teki bu hükümle birlikte veri aktarımındaki riskler minimuma indirilecek, işbu kurum ve kuruluşların hesap verilebilirliği artacak ve büyük ölçekli şirketler için kolaylık sağlanacaktır. Bağlayıcı şirket kurallarında, Tüzük'teki bu hükme göre; veri sahibinin haklarını ve bu hakların ihlali halinde yasal yolları açıklamalı, diğer kurumlarla hangi şartlar altında veri paylaşabileceğini belirtmeli, Tüzük'te bahsedilmiş olan veri denetleme yetkilileri tarafından gerekli şartlarda denetimleri yapılmalı ve yeri geldiğinde hesap verebilmelidir.[133]

Kanun'da ise Tüzük'te bağlayıcı kurumsal kuralların düzenlendiği gibi bir hüküm yer almamaktadır. Ticari hayatın işleyişi açısından teknolojik gelişmelerle birlikte başta kişisel veriler olmak üzere verilerin aktarımı önemli yer tutmaktadır. Tüzük'ün getirdiği bu sistem güvenli ve hızlı bir şekilde veri aktarımını kolaylaştırmayı hedeflemektedir. Kanun'un ise bu konuda çok geride kaldığı kuşkusuzdur.

Tüzük'te düzenlenen standart veri koruma hükümleri, AB Komisyonu'nun hazırladığı ya da denetim makamının hazırlayıp AB Komisyonu tarafından onaylanan sözleşmelerdir. Bu sözleşmeyi akdeden veri sorumlusu ya da veri işleyen, Komisyon'un yeterlilik kararı olmadan yurtdışı aktarımlarında korumanın sağlanacağını taahhüt eder.[134]

Davranış kuralları Tüzük'ün 40 ve 41. maddelerinde düzenlenmiştir. Davranış kurallarından amaç, farklı sektörlere ilişkin ufak çaplı işletmeler ve KOBİ'lerin durumu göz önüne alınarak hazırlanması amaçlanan kurallardır. Sertifikalar ise veri sorumlusu

[132] Devecioğlu, s.75.

[133] GVKT m.47.

[134] Ibid., s.76.

ve işleyenin kişisel veri işlemelerinin hukuka ve Tüzük'e uygun olduğunu belgelemek adına yetkili makamlardan aldıkları belgelerdir. Her iki durum için de veri sorumlusu ve işleyenden Tüzük'e uygun tedbirleri alması için ayrıca taahhüt alınır.[135]

Sonuç olarak görüldüğü üzere Kanun'da, kişisel verilerin yurtdışına aktarımı noktasında çift aşamalı bir denetimden bahsedebiliriz. Buna göre ilk aşamada Kanun'da öngörülen genel kurallar dikkate alınacaktır. İkinci aşamada ise yurtdışı aktarım için öngörülen özel hususlar dikkate alınacaktır. Bu sebeple Kanun'un 9. maddesinde düzenlenen şartlar, 5. ve 6. maddesinde düzenlenen genel kuralları tamamlayıcı durumdadır.[136] İkinci aşamada uluslararası sözleşmelerden doğan bir yükümlülük söz konusu değilse aktarım yapılacak ülkenin güvenli olup olmadığına bakılacak ve ülke veri aktarımı için güvenli olmadığı takdirde veri sorumlusundan gerekli önlemlerin alınması istenilecektir. Tüzük'te ise yurtdışı veri aktarımlarında AB içerisinde özdenetim mekanizması kurulmak istenmiştir. Kanun'da yer alan "veri sorumlusunun gerekli önlemleri alması" hükmü Tüzük'te daha detaylı irdelenerek veri sorumlusunun yeterli garantiler sunmasına bağlanmıştır.

6.4. İstisnalar

KVKK'nın 28. maddesinde Kanun'un uygulanmayacağı istisnai haller adında ayrı bir madde yer almaktadır.

Kanun'un 28/(1)-a bendinde "*Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi"* hükmü yer almaktadır. Tüzük'ün 2/(2)-c bendinde ise "*tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından yapılan işlemenin tüzük kapsamında değerlendirilmeyeceğini"* söylemektedir. Tüzük'ün ifadesinin daha geniş kapsamlı olduğunu görmekteyiz. İlk farklılık Kanun'da geçen *"kendisiyle ilgili"* ve Tüzük'te geçen "*kişisel*" ifadesi farklılığıdır. Örneğin, bir kişinin

[135] Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu,* s. 87.

[136] Ibid., s.87.

arkadaşlarının doğum günlerini unutmamak adına kayıt altına aldığı notlar Tüzük kapsamında değerlendirilemeyecekken Kanun kapsamında kendisi ile ilgili olmaması sebebiyle kanun kapsamında değerlendirilebilecektir. Diğer farklılık ise kanunda geçen *"aynı konutta yaşayan aile fertleri"* ile Tüzük'te geçen "*ev faaliyetleri*" tabirindeki farklılıktır. Bu durumda ise kişinin ev arkadaşı aile ferdi olmadığından Kanun kapsamında değerlendirilmesi gerekecekken Tüzük kapsamında değerlendirilemeyecektir.[137]

Kanunun 28/(1)-b bendinde *"kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi"* istisna kapsamında düzenlenmiştir. Burada anonim hale getirilmek kelimesi önem taşımaktadır. Kişisel verilerin anonimleştirilmesi halinde artık bu durum Kanun kapsamında değerlendirilmeyeceğine çalışmamızda önceden bahsedilmişti. Bu maddede ise Kanun kapsamındaki bir kişisel verinin sonrasında anonimleştirilmesi halinde Kanun kapsamında değerlendirilemeyecektir. Aslında Kanun'un 3. maddesinde verinin anonimleştirilmesi halinde Kanun kapsamından çıkartılacağı belirtilmiştir. O halde kanaatimce buradan anlaşılması gereken husus veri işlenmeye başlandığı andan itibaren Kanun kapsamında olacağı, ancak istisnada belirtilen hallerden birinin gerçekleşmesi ve verinin de anonimleştirilmesi durumunda artık işlendiği tarihten itibaren verinin kanun kapsamında olmayacağıdır. Aksi takdirde Kanun'un bu hükmünün bir anlamı kalmayacaktır. Bahsettiğim halde ise de işlenme ile anonimleştirilme arasındaki kanuna aykırı bir fiil halinde ilgili kişinin maddi ve manevi bir zararının doğma ihtimali ortaya çıkacaktır. Kanun'un bu hükmünün uygulanmasının Kurul'un vereceği kararlar ışığında şekilleneceği kuşkusuzdur. Tüzük'te ise bu hükme benzer bir hüküm yer almamaktadır.

Kanun'un 28/(1)-c bendinde *"kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi"* halinde Kanun

[137] Elif Küzeci, *Kişisel Verilerin Korunması*, s.329.

kapsamında değerlendirilemeyeceği düzenlenmiştir. Benzer düzenlemeyi, Tüzük'ün başlangıç bölümünün 153. kısmında ve 85. Maddesinde de görmekteyiz.

Kanun'un 28/(1)-ç bendinde *"Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi"* halinde de Kanun'un istisna hali mevcuttur. Benzer hüküm itibariyle Tüzük'ün 2/(2)-b kısmında AB Sözleşmesinin 5. başlığının 2. bölümüne atıf yapılarak bu faaliyetlerin Tüzük'ün kapsamı dışında olduğu belirtilmiştir.

Kanun'un 28/(1)-d bendinde *"Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi"* halinin kanun kapsamında değerlendirilemeyeceği düzenlenmiştir. Kanun'un bu bendi kapsamına önleyici işlemlerin girmediği, bu hususun 28/(1)-ç bendi kapsamında değerlendirilebileceği açıktır. Tüzük'te ise bu husus için ayrıca suçların önlenmesi, soruşturulması, kovuşturulması ve infazı aşamasına ilişkin Direktif kabul edilmiştir. Benzer bir kanuni düzenlemeye özellikle UYAP sisteminin var olması sebebiyle bizde de ihtiyaç duyulduğu kuşkusuzdur.

Genel itibariyle 28. maddede yer alan istisnalara baktığımızda kamu kurum ve kuruluşlarının kişisel verileri işlemesi halinde kanun kapsamında değerlendirileceği alan oldukça daraltılmıştır. Bir anlamda idarenin yapmış olduğu neredeyse bütün kişisel verilerin işlenmesine ilişkin işlemler özellikle 28/(1)-c ve ç bentleri kapsamında değerlendirilebilecektir. Milli savunma, milli güvenlik, kamu düzeni ve ekonomik güvenlik adına kişisel verilerin işlenmesinin KVKK kapsamından çıkarılması elbette yerindedir, ancak bu hususta özel kanunların yapılması ihtiyacı da dikkate alınmalıdır. Kanun'un ve Tüzük'ün lafzı itibariyle istisna tuttuğu alanlar ise benzerdir. Gerçekten de her iki yasal metinde de yargı işlemleri, kamu güvenliği, milli savunma, kamu düzeni gibi sebeplerle çerçeve yasanın dışında bırakılmış unsurlar benzerdir. Ancak Tüzük bu istisnalar için yukarıda da belirtmiş olduğumuz gibi ya ayrı bir direktif düzenleyerek

ikincil düzenlemelerle istisnanın sınırlarını belirleme yoluna gitmiş ya da üye ülkelerden belirttiği hususlarda sınırları belirlemesi için düzenleme yapması istemiştir.

ÜÇÜNCÜ BÖLÜM

HAK VE YÜKÜMLÜLÜKLER

Kanun'un 10. maddesinde veri sorumlusunun aydınlatma yükümlülüğü, 11. Maddede veri sahibinin hakları, 12. Maddede ise veri güvenliğine ilişkin yükümlülükler düzenlenmiştir. Tüzük'ün 3. bölümü olan 12 ila 23. maddelerinde veri sahibinin hakları, 4. bölümü olan 24 ila 44. maddelerinde veri sorumlusu ve veri işleyenin yükümlülükleri işlenmiştir. Tüzük'ün sistematiği daha anlaşılır ve kapsamlı olduğundan bu başlık altında Tüzük anlatılarak aktarılmaya ve Kanun'daki kapsamla karşılaştırılmalı olarak değerlendirilmeye çalışılacaktır.

1. Veri Sahiplerinin Hakları

1.1. Bilgilendirilme Hakkı

Bilgilendirilme hakkı, Tüzük'ün veri sahibinden kişisel verilerin toplandığı durumlarda sağlanacak bilgiler başlığı altında 13. maddede, Kanun'da ise veri sorumlusunun aydınlatma yükümlülüğü başlığı altında 10. maddede işlenmiştir. Her iki yasal düzenlemede de kişisel verileri topladığı andan itibaren, veri sorumlusunun ve varsa veri koruma görevlisinin kimlik ve irtibat bilgileri ile işleme amacı ve işleme faaliyetlerinin neler olduğunu söylemekle yükümlü olduğu belirtilmiştir.

Kanun'daki düzenlemede aydınlatma yükümlülüğü olarak düzenlenmesi ve veri sorumlusunun yükümlülüklerini belirtmesi yasal düzenleme ışığında yerindedir. Tüzük'te ise ilgili maddenin neredeyse sadece ilk fıkrası Kanun'daki düzenlenen maddenin tamamını karşılar niteliktedir. Bilgilendirmeye ilişkin yükümlülük tıpkı Direktif'teki gibi Tüzük'te de ikili bir ayrımla düzenlenmiştir. Tüzük 14. maddede veri sahibinden kişisel verilerin alınmadığı hallerde sağlanacak bilgilerden bahsetmiştir. 14. maddedeki hüküm 13. maddedeki ile paraleldir. Tüzük'te 13. Madde kapsamında, yani veri sahibinden kişisel veriler alınıyorsa veri sorumlusu verinin alındığı andan itibaren maddede belirtilmiş olan bilgileri veri sahibine vermekle yükümlü tutulmuştur. Aksi durumda veri sorumlusu bu bilgileri "makul süre içerisinde ve en geç bir aylık sürede" veri sahibine bildirmelidir. Kişisel verileri, veri sorumlusu veri sahibine ulaşmak için

kullanıyorsa Tüzük kapsamında sayılan bilgileri, iletişime geçtiği anda veri sahibine iletmelidir.

Sonuç olarak kişisel verilerin korunması hukukunda dürüstlük kuralı ve şeffaflık ilkesinin bir getirisi olan ilgilinin bilgilendirilme hakkı ya da veri sorumlusunun aydınlatma yükümlülüğü Tüzük'te bilgilendirmenin nasıl ve ne kadar süre içerisinde yapılacağına kadar ayrıntılı bir şekilde düzenlenmiştir. Kanunda ise hangi konularda bilgilendirilmesi gerektiğinin belirtilmesiyle yetinilmiş ve veri sorumlusunun yükümlülüklerinin neler olduğu açıklanarak sınırlı bir düzenleme getirilmiştir.

1.2. Erişim Hakkı

Erişim hakkıyla birlikte veri sahibi kendi kişisel verilerinin hangi amaçla kullanıldığını, kimlere aktarıldığını, veri sorumlusunun kendisine ait hangi kişisel verilere sahip olduğunu bilerek bilgilerin geleceğini belirleme hakkından istifade edebilir.[138] Erişim hakkı bir anlamda bilgilendirilme hakkı ile iç içedir. Kişisel verileri aydınlatma yükümlülüğünü yerine getiremeyen veri sorumlusu, veri sahibinin erişim hakkını da olumsuz yönde etkileyebilecektir.

Tüzük ve Direktif erişim hakkı konusunda birbirine paralel olmakla birlikte Tüzük'teki düzenlemenin daha detaylı olduğu görülmektedir. Tüzük'ün 15. maddesinde düzenlenen erişim hakkı, işlemenin amaçlarına, işlemeye itiraz etme ve düzeltilme veya silinmesine, denetim makamına şikayette bulunmaya kadar birçok hususu kapsamaktadır. Kanun 11. maddesinde düzenlenen erişim hakkında ise Tüzük'e nazaran daha sınırlı bir sayıma gidilmiştir.

1.3. Düzeltme Talep Hakkı

Kanunun 4/(2)-b bendinde kişisel verilerin işlenmesinde, işlenenleri *doğru ve gerektiğinde güncel olma prensibi* çerçevesinde işleme yükümlülüğü düzenlenmiştir. Aynı hüküm Tüzük'ün 5/(1)-d bendinde de düzenlenmiş olup aksi durumda

[138] Küzeci, *Kişisel Verilerin Korunması,* s.222.

gecikmeksizin makul süre içerisinde silinmesinin yahut düzeltilmesinin gerektiği belirtilmiştir. Düzeltilmesinin talep hakkı da doğruluk prensibiyle doğrudan ilgilidir. Kanun'un 11/(1)-d bendinde veri sahibinin kişisel verilerin yanlış veya eksik düzenlenmesi durumunda bunun düzeltilmesini talep edebileceğini belirtmiştir. Tüzük'te de benzer bir hüküm olmakla birlikte ayrıca makul süre içerisinde düzeltilmesinin gerekeceği belirtilmiştir.

1.4. Unutulma Hakkı

Unutulma hakkı;[139] bireyin, dijital hafızada yer alan fotoğrafı, kimlik bilgisi, adresi ve diğer kişisel içeriklerinin kendi talebi üzerine bir daha geri getirilemeyecek

[139] Bu hakla ilgili Avrupa Birliği hukukunda Divan'ın Google kararı önemlidir. Unutulma hakkına ilişkin olarak Divan'ın kararına esas oluşturan davanın temeli, bir internet kullanıcısının arama motoru Google'a "Mr Costeja González" adlı avukatın adını girdiğinde, "La Vanguardia" isimli günlük bir gazetenin iki farklı tarihli sayfasına link vermesine ve bu link verilen sayfalarda söz konusu kişinin sosyal güvenlik borçlarının iyileştirilmesi için mülkünü satmak zorunda kalmasına ilişkin bilgiler içermesine dayanmaktadır. Şikâyeti inceleyen İspanyol makamları, 2010'da, Google'ın ilgili linkleri kaldırmasını istediyse de gazeteye yönelik herhangi bir karar alınmaması üzerine Google temyize gitmiş, İspanya Yüksek Ulusal Mahkemesi de konu hakkında görüş bildirmesi için davayı Divan'a taşımıştır. Divan, 13 Mayıs 2014 tarihinde verdiği unutulma hakkına ilişkin kararını, 95/46 sayılı Direktif'in ilgili hükümlerine dayanarak almıştır. Direktifin "Veri Kalitesine İlişkin Prensipler" başlıklı 6. maddesine göre; *Üye Devletler, kişisel verilerin adil ve yasal olarak işlenmesini, belirli, açık ve meşru amaçlar için toplanmasını ve bu amaçlarla uyumsuz biçimde başkaca işlenmemesini, toplandığı ve/ veya ayrıca işlendiği amaçlar ölçüsünde ilgili ve yeterli olmasını, doğru ve gerektiği yerde güncel tutulmasını, verilerin toplandığı sırada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca veri öznelerinin tespitine izin veren biçimde tutulmasını, toplanma ve sonrasındaki işlenme, silinme veya düzeltilme amaçlarını göz önünde tutarak verilerin yanlış veya eksik olmamasını sağlayacak tüm makul önlemleri almakla yükümlüdür*; AYM- N.B.B. Başvurusu, bir gazetenin internet arşivinde erişilebilir durumda olan haber ve yayınlar ile ilgili içeriğin yayından kaldırılması yönündeki talebin reddedilmesinin şeref ve itibarın korunması hakkını ihlal ettiği iddiasına ilişkindir. Başvuru yolu 2010 referandumuyla kabul edilen bireysel başvuru imkânıyla sağlanmıştır. Olayı kısa özetleyecek olursak; başvuranın uyuşturucu kullandığı iddiasıyla bir internet haber sitesinin arşiv kısmında 1998 ve 1999 yıllarına ait haberler yayınlanmış ve başvurucu, ilgili haber sitesine başvurarak haberin kaldırılmasını istemiştir. Talebine herhangi bir cevap verilmemesi üzerineyse başvurucu İstanbul 36. Sulh Ceza Hâkimliğine başvuru yapmış ve talebi kabul edilmiştir. Ancak haber sitesinin karara itirazı üzerine İstanbul 2. Asliye Ceza Mahkemesi kararı kaldırmıştır. CMK'ya göre itiraza yönelik verilen kararlar kesin hüküm teşkil ettiğinden ve gidilecek başka bir kanun yolu kalmadığından başvurucu, bireysel başvuru hakkını kullanmış ve konuyu Anayasa Mahkemesine taşımıştır[139]. Bu talep 03.03.2016 tarihinde Anayasa Mahkemesi tarafından kabul edilmiştir; Türk hukukunda unutulma hakkıyla ilgili bir başka önemli kararda Yargıtay Hukuk Genel Kurulu'nun 2014/4-56 esas 2015/1679 karar sayılı 17.6.2015 tarihli ilamıdır. Dava, kişilik hakkına saldırı nedenine dayalı tazminat istemine ilişkindir. Davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekâr olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır ve karar kesinleşmiştir. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayınlanan kitapta yer almıştır. Bunun üzerine mağdur haksız fiil nedeni ile manevi tazminat istemine ilişkin olarak dava açmıştır. Yerel mahkemece istemin bir bölümü kabul edilmiş; karar, taraflarca temyiz olunmuştur. Gerek Yargıtay kararı olsun gerekse de ilk derece mahkemesinin kararı olsun uyuşmazlık konusu kısım tazminatın miktarıyla ilgilidir. Ancak Yargıtay bu hususla birlikte artık 2010 anayasa değişikliğiyle Anayasamıza giren unutulma hakkına da değinmek istemiştir. Sonuç olarak Türk yargısından unutulma hakkını düzenleyen ilk içtihat ortaya çıkmıştır; AYM'nin 03.03.2016 tarihli kararını ve Yargıtay'ın 17.6.2015 tarihli kararları bir anlamda unutulma hakkının tanımı niteliğindedir. Bu içtihatlar, hakkın özüne değinilmesi ve hukuki çerçevesinin çizilmesinde önemli bir rol oynamışlar ve ilerleyen zamanlardaki unutulma hakkına ilişkin hukuki uyuşmazlıkların çözümünde yol gösterici olmuşlardır. Metin itibariyle her içi yargı içtihadı da

biçimde ortadan kaldırılması şeklinde tanımlanmaktadır.[140] Bu hakla veri sahibi, sahip olduğu ve özellikle silinmiş kişisel verilerinin üçüncü kişiler tarafından artık izlenememesini veya takip edilememesini amaçlamaktadır.[141] Bu tanım günümüz itibariyle yeterli gibi görünse de bilişim teknolojilerindeki hızlı gelişimin neticesinde bir takım değişiklikleri de beraberinde getireceği kuşkusuzdur. Bunun örneklerinden birini Direktif ile Tüzük arasındaki farklara bakarak görebiliyoruz. Tüzük'te, Direktif'ten

---

Divan'ın Google Kararı gibi kapsamlı olmamakla birlikte Türk Hukuku kapsamında değeri ve önemi yadsınamaz. Unutulma hakkıyla ilgili mihenk taşı olan bu üç kararda da önemli olan diğer bir konu başka bir hakkın özünün zedelenip zedelenmediği mevzuudur. Burada "kamunun haber alma özgürlüğüyle" kişinin özel hayatının gizliliği hakkının birbiriyle çelişip çelişmediği konusu gündeme gelmektedir. Bu üç kararda, unutulma hakkını kapsayan bir hak olan kişinin özel hayatının gizliliği hakkı lehine hükümler kurulmuştur. Yani Divan bu kararıyla birlikte hakkı zedelenen kişinin durumunu ikiye ayırarak somut olayı değerlendirme yoluna gitmiştir. Eğer hakkı zedelenen kişi toplum nezdinde tanınırlığı olan kişi ise kamunun haber alma hakkı kapsamı daha geniş değerlendirilmeli ve ona göre hüküm kurulmalıdır. Olayda ise kişinin tanınırlığını olmadığı gerekçesiyle burada unutulma hakkını ve özel hayatın gizliliğini öncelikli değerlendirmiştir. Divan kararında değindiği başka bir önemli husus insanlık onuru kavramıdır. Her somut olayda unutulma hakkı talebinin değerlendirilirken kamunun haber alma hürriyeti karşısında unutulma hakkı talebi olan kişinin insanlık onurunun da zedelenip zedelenmediği sorusunu hakimin kendisine sorması gerektiğine değinmiştir. Yani Divan somut olayda Google'ın ilgili veriyi kaldırmaması başvurucunun insanlık onuruna halel getirip getirmeyeceğini sorarak aslında bir anlamda keyfi veri silinmesinin de önüne geçmiş olmaktadır. Bizim anayasamızda ise insanlık onuru kavramı yer almamakla birlikte Anayasa'nın 17. Maddesinde; "*herkes yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir."* hükmü yer almaktadır. İşte AYM, 17. maddedeki "*manevi varlık*" kavramına atıf yaparak, hakkının zedelendiğini iddia eden kişilerin, zarar görüp görmediğinin takdir edilmesi gerektiğini belirtmiştir. Ayrıca AYM, AİHS'nin 8. maddesindeki özel yaşama saygı hakkına da atıf yapmıştır. Yargıtay Hukuk Genel Kurulu'nun 2014/4-56 esas 2015/1679 karar sayılı 17.06.2015 tarihli kararının çerçevesini de AİHS'nin 8. maddesi oluşturmaktadır. Bu karar unutulma hakkıyla ilgili verilmiş bir karar olmakla birlikte AYM'nin kararına karşı oldukça basit ve dar kapsamlıdır. Bunun en büyük sebebi de ilk derece mahkemesinde tarafların manevi tazminatın değerinin temyiz edilmiş olmasından kaynaklıdır. Ayrıca Yargıtay kararında 95/46 Direktifi'ne de atıf yapılmıştır; ancak AYM'de oybirliğiyle alınan karar Yargıtay'da oybirliğiyle alınamamış ve bazı üyeler azınlıkta da kalsalar unutulma hakkının daha dar kapsamda değerlendirmesi gerektiğini vurgulamışlardır. Unutulma hakkının uygulanışı açısından Divan'ın Google kararıyla Yargıtay'ın kararı arasında ciddi fark söz konusudur. Şöyle ki; Divan'ın yorumuna göre hakkı zedelenen kişi arama motoruna konuyla ilgili bir aramada bulunduğunda verilerin silinmiş olduğunu görecektir ve bu durumun başkası tarafından da bulunma imkânının önüne geçecektir. Yani içeriğin Google tarafından çıkarılması söz konusu olacaktır. Ancak Yargıtay'ın verdiği kararda ise bu konuya değinilmemekle birlikte hakkı zedelenen kişinin hak ihlaliyle ilgili yaptığı aramada veri silinmesinden değil bir anlamda engellemeden söz edilebilecektir. Bir örnek üzerinden somutlaştırmamız gerekirse: örneğin A kişisi 95 yılında yüz kızartıcı bir suç işlediğini, cezasını çektiğini ve aradan 22 yıl geçmiş olmasına rağmen internete girip kendi adını yazdığında halen bu suçla ilgili bilgilere rastladığını söyleyerek dava açtığını düşünelim. Bu durumda unutulma hakkı zedelenen kişinin durumunu Divan'ın kararı çerçevesinde değerlendirdiğimiz vakit, başvurucu karar sonrası bir daha internete girdiğinde ve adını yazdığında geçmiş zamanda işlemiş olduğu yüz kızartıcı suçla ilgili hiçbir veri ekrana düşmeyecektir. Yargıtay kararına göreyse kişi sadece adının algoritmadan kaldırılmasıyla kendi bilgisine ulaşamamakla birlikte söz konusu habere erişebilecektir.

[140] Gülener Serdar, **Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı"**, Türkiye Barolar Birliği Dergisi, Y:2012, S:102, s.226.

[141]Weber Rolf H**., "The Right to Be Forgotten, More Than a Pandora's Box",** Journal of Intellectual Property, Information Technology and E-Commerce Law 120, 2(2011), s.121.(alıntılanan), Akgül Aydın, **Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" Ve Ab Adalet Divanı'nın "Google Kararı"** TBB Dergisi 2016 (116) s.21.

farklı olarak veriyi paylaşan kişi veya kurumları da sorumluluk altına alarak veri süjesinin silinme talebini, veri sahibine haber verme yükümlülüğü getirilmiştir.[142]

Tüzük, Direktif ve Kanun'dan farklı olarak unutulma hakkını çok detaylı bir şekilde 17. maddede işlemiştir. Buna göre veri sorumlusu için veriyi elde tutmasının bir amacı kalmamışsa, veri sahibi kişisel verisinin işlenmesi için vermiş olduğu rızayı geri çekmişse, veri sorumlusunun kişisel veriyi işlemesi için meşru bir menfaati yoksa ya da yasadışı bir işleme söz konusuysa ya da yasal zorunluluktan kaynaklı yükümlülüklerin yerine getirilmesi için kişisel verinin silinmesi gerekiyorsa veri sorumlusunun gecikmeksizin ilgilinin kişisel verilerini silmesi gerekir.

Tüzük aynı zamanda veri sorumlusuna kişisel verinin silinmesi yanında kamuya açıklanmış olunması halinde diğer veri sorumlularına da bu verinin silinmesini bildirmekle mükellef tutmuştur. Ancak, özellikle kişisel veriyi işleyen veri sorumlusunun sayısının çok olması halinde veri sorumlusunun ciddi bir yükümlülük altına gireceği düşünüldüğünde "*makul adımları*" atması yeterli görülmüştür. Tüzük'te makul adımların, teknik ve ekonomik önlemlerin veri sorumlusu tarafından ilgili kişiye bildirilmekle yükümlü kılınmasına rağmen işlevsel bir çözüm sunduğunu söylemek mümkün değildir.[143]

Tüzük 17. maddesinde son olarak unutulma hakkının kapsamının dışında kalan durumları düzenlemiştir. Buna göre Birlik hukuku ve üye devlet hukuku kapsamındaki yasal düzenlemelerin yerine getirilmesi adına yapacağı işlemlere, halk sağlığından kaynaklı kamu yararının gözetildiği hallerde, 89. madde göz önüne alınarak arşivleme, istatistik, bilimsel ve tarihsel amaçlarla kullanılması halinde veya bir hakkın korunması veya uygulanması halinde 17. madde kapsamından bahsedilemeyecektir.

Kanun'un 11. maddesinde, 7. maddedeki şartların sağlanması halinde kişisel verinin silinebileceğinden bahsedilmiştir. 7. maddenin ilk fıkrasında yasal düzenlemelere uygun şekilde yapılan veri işlemelerinin, işleme için gerekli menfaatin

[142] Nilgün Başalp, *Avrupa Birliği Veri Koruması Regülasyonun Temel Yenilikleri*, s.99

[143] Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu,* s. 99.

ortadan kalkması halinde resen ya da talep halinde silinmesi, yok edilmesi ya da anonim hale getirilmesi öngörülmüştür.

1.5. İşlemenin Kısıtlanması Hakkı

Tüzük'ün 18. maddesinde düzenlenmiş bu hak kapsamında veri sahibi, veri sorumlusundan kişisel verilerinin kısıtlanmasını isteyebilir. Bu hak kapsamında, veri sahibi kişisel verisinin doğruluğuna itiraz ettiği takdirde veri sorumlusu tarafından kişisel verinin doğruluğu teyit edilinceye kadar kısıtlanabilir. İkinci olarak kişisel verinin işlenmesi yasal değilse, veri sahibi verinin silinmesine itiraz ederse verinin kullanımı kısıtlanabilir. Diğer yandan veri sorumlusunun kişisel veriye bir ihtiyacı kalmamış olması ama veri sahibi için yasal sebeplerden kaynaklı olarak kişisel veriye gereksiminin olması durumunda kişisel verinin kullanımının kısıtlanmasını isteyebilir. Son olaraksa veri sahibi Tüzük'ün 21. maddesindeki itiraz hakkı kapsamında veri sorumlusunun meşru sebeplerinin veri sahibinin meşru sebeplerinden daha baskın olduğu doğrulanıncaya kadar verinin kullanımı kısıtlanabilir.

Kanun'da işleme faaliyetlerinin kısıtlanması hakkı ile ilgili herhangi bir düzenleme bulunmamaktadır. Kanun'un 4/2-d bendindeki kişisel verilerin işlendikleri amaç kapsamında makul süre boyunca muhafaza edilmeleri prensibi bu madde ile bağdaştırılabilirse de Tüzük'ün 18. maddesinde düzenlenen işleme faaliyetlerinin kısıtlanması hakkı gibi değerlendirilmesi mümkün değildir.

1.6. Bildirimde Bulunulmasını Talep Hakkı

Tüzük'ün 19. maddesinde ölçülülük ilkesi ve 16 ila 18. maddelerinde düzenlenen düzeltme talep hakkı, unutulma hakkı ve işlemenin kısıtlanması hakkı kapsamında yapılan işlemleri verilerin açıklandığı kişileri veri sahibine haber verme yükümlülüğü kapsamında olduğunu belirtmiştir. Veri sahibinin bu yükümlülük kapsamında alıcıların kimler olduğunu öğrenme hakkı vardır. Genel itibariyle bu hüküm, veri sahibinin hakkından çok veri sorumlularının yükümlülüğü kapsamında olmakla birlikte Tüzük'ün sistematiğini bozmamak adına ve 16 ila 18. maddeler göz

önünde bulundurularak veri sahibinin hakları bölümünde düzenlenmesi uygun görülmüştür.

Kanun'da 11/(1)-f bendinde ise aynı maddenin d ve e bentlerinde düzenlenen düzeltme ve silinmesini isteme hakkı kapsamında yapılan işlemlerin veri alıcılarına bildirilmesini talep edebileceği belirtilmiştir. Kanun kapsamında bildirilme bir talep hakkı olarak düzenlenmişken Tüzük'te önce veri sorumlusu için bir yükümlülük sonrasındaysa veri sahibi açısından da bir hak olarak bahsedilmiştir. Kanun'da, Tüzük'te olduğu gibi ölçülülük ve imkan dâhilinde kısmı belirtilmemiştir.

1.7. Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı Direktif ve Kanun'da yer almayan Tüzük'le birlikte yasal zemine oturtulan bir haktır. Bu hakka göre veri sahibinin, kişisel verileri elinde bulunduran veri sorumlusundan işlemenin otomatik vasıtalarla gerçekleştiği ve işlemenin bir rızaya ya da sözleşmeye dayandığı hallerde Tüzük'ün 19. maddesinde belirtilen şartlar altında başka bir veri sorumlusuna taşınmasını talep hakkı vardır.

Tüzük veri taşınabilirliğinin sınırlarını daraltmış, kamu yararı adına bir görevin ifası için ve veri sorumlusuna verilen resmi bir yetkiden kaynaklı ise 19. madde kapsamında değerlendirilemeyeceğini belirtmiştir.

Sonuç olarak Tüzük'ün, Kanun'a nazaran veri sahibinin haklarını daha etkin bir şekilde korumayı amaçladığını söyleyebiliriz. Direktif'te bent veya fıkra şeklinde yer alan hükümlerin bir kısmının ayrı bir madde olarak Tüzük'te yer aldığını görmekteyiz. Bu duruma Direktif ile Tüzük arasında geçen zamanda bireysel ve toplumsal beklentilerin neden olduğunu söylemek yerinde olacaktır. Örneğin, unutulma hakkı Direktif'te bir bent kapsamında değinilmişken, Tüzük'te ayrı bir maddede detaylı bir şekilde işlenmiştir. Bunun yanında veri taşınabilirliği hakkı Tüzük'te ilk defa kendine yer bulmuştur. Veri sahiplerinin haklarına getirilen tüm bu yenilikler, veri sahibine kendine ait verilerin kaderini belirleme noktasında çok geniş bir alan

bırakırken, veri sorumlusu ve işleyene ise Direktif'e göre daha detaylı yükümlülükler yüklemektedir.[144]

2. Veri Sorumlularının Yükümlülükleri

2.1. GVKT Kapsamında Veri Sorumlusunun Yükümlülükleri

Tüzük'ün 24. maddesinde ilk olarak genel veri sorumlusu yükümlülüklerine değinilmiştir. Bu maddeye göre veri sorumlusu, veri sahibinin kişisel verisinin işlenmesinden kaynaklı hak ve özgürlükleri açısından doğabilecek zararları önlemek için Tüzük kapsamında gerekli teknik ve hukuksal tedbirleri almakla yükümlü kılınmıştır. Bu maddedeki genel hükümler itibariyle tedbirlerin nasıl alınması gerektiği ve hangi şartlar için alınması gerektiği hususu veri sorumlusuna bırakılmıştır.

Tüzük'ün 24. maddesi, asıl olarak veri sorumlusunun hukuka aykırı bir işlemi karşısında veri sorumlularına ilişkin 24. madde sonrasındaki özel hükümlerin yeterli olmadı hallerde genel bir düzenleme ile sorumluluk alanını genişletmeyi ve veri sorumlularının, sorumluluktan kaçarak hukuka aykırı işlem yapmasının önüne geçmeyi amaçlamıştır. Nitekim 24. maddenin 3. fıkrasıyla birlikte bir anlamda örneklendirme yapılarak veri sorumlusunun, kişisel veriyi işlerken davranış kurallarına (m.40) ve belgelendirme mekanizmalarına (m.42) göre hareket ettiği durumlarda genel yükümlülüğe uygun hareket ettiği sonucu doğacağı ifade edilmiştir.

Tüzük'ün 25. maddesinde ise veri sorumlusunun, Tüzük'ün kişisel verilerin korunmasına ilişkin ilkelerini yerine getirmek ve hukuka uygun veri işlenebilmesi adına tasarım aşamasından itibaren gerekli teknik tedbirleri alması gerektiği belirtilmiştir.[145] Tıpkı 24. maddede olduğu gibi 25. maddenin 3. fıkrasıyla birlikte örneklendirme yapılmıştır. Bu fıkraya göre veri sorumlusu kişisel veriyi işlerken 42. maddeye göre hareket ettiği takdirde genel yükümlülüğüne uygun hareket ettiği sonucu doğacaktır.

Tüzük'ün 26. maddesinin ilk fıkrasında iki veya daha fazla veri sorumlusunun işleme amaçlarını ve yöntemlerini birlikte belirledikleri durumlarda müşterek veri

[144] Ayşe Nur Akıncı, s.21.
[145] Devecioğlu s.101.

sorumluluğunun olacağı belirtilmiştir. AB hukuku ya da üye devlet hukukunca ayrı bir hüküm olmadığı takdirde veri sorumlularının aralarındaki işbölümünün nasıl olacağını bir sözleşme ile hüküm altına almaları istenmiştir. Aynı maddede şeffaflık ilkesine de değinilerek bu anlaşmanın, veri sahibine açık olması gerektiği üzerinde durulmuştur. Veri sorumluları arasındaki ilk fıkrada belirtilen anlaşmanın içeriği ve kapsamının ne olacağı noktasında, Tüzük bir açıklık getirmemiştir. Son fıkrada ise birden fazla sorumlunun bulunduğu hallerde veri sahibinin Tüzük'ten kaynaklı haklarını her iki veri sorumlusuna karşı kullanabileceği belirtilmiştir. Bu hususta Kanun'da ayrıca bir düzenleme olmadığı Türk hukukunda ortak veri sorumlularının 6098 sayılı Türk Borçlar Kanunu çerçevesinde müştereken sorumlulukları bulunduğu belirtilmelidir.

Tüzük'ün 27. maddesindeki düzenlemede Birlik içerisinde bulunmayan veri sorumlusu veya işleyeni için veri sahibinin Birlik içerisinde bulunduğu hallerde temsilci atanması yükümlülüğü getirilmiştir. Tüzük'ün 27. maddesi, 3. maddenin 2. fıkrası dikkate alınarak hazırlanmıştır. Bu maddeye göre veri sorumlusu ve veri işleyen, Birlik içerisinde bulunmasa dahi veri sahibinin Birlik içerisinde olması halinde Tüzük uygulama alanı bulacaktır. Bir anlamda Tüzük'e aykırılık halinde muhatap bulunması adına böyle bir düzenlemeye yer verilmiştir. Temsilci atanması için özel nitelikli kişisel verilerin büyük çaplı işlenmesinin olmadığı, gerçek kişilerin hak ve özgürlüklerinin zarara uğramadığı sonucuna ulaşılıyorsa temsilci atamasının gerekmeyeceği düzenlenmiştir.[146] Bu hükümle birlikte yasal temsilci atanmasının kapsamının oldukça daraltıldığı görülmektedir.

Tüzük'ün 28. maddesinde işleyici başlığı altında veri işleyici ile ilgili ayrıntılı düzenlemelere yer verilmiştir. Maddenin kapsamına göre veri işleyenin başka bir veri işleyen kullanabilmesi için veri sorumlusundan izin alması gerekir. Veri işleyen, veri sorumlusunun talimatlarına uygun hareket etmeli Tüzük kapsamında düzenlenen kişisel verilerin aktarılmasına ilişkin hallerde yine veri sorumlusunun talimatı üzerine davranmalıdır. Veri sahibinin hak ve menfaatlerinin korunmasına yönelik taleplerine

[146] Ibid., s.99.

karşı veri sorumlusuna yardımcı olmalıdır. Kişisel verilere ilişkin yapılan teftişlere görevi gereğince katkı sağlamalıdır.

Tüzük'ün 30. maddesinde kişisel verilerin işleme faaliyeti kayıtlarının tutulmasına ilişkin düzenlemelere yer verilmiştir. Veri sorumlusu ve Tüzük'ün 27. maddesinde belirtilen temsilcisi, kendi kimlik ve iletişim bilgilerinin, işleme amaçlarının ne olduğunun, kişisel veri kategorilerinin, kişisel verilerin aktarılacağı kategorilerin ve bu aktarmaya ilişkin alınan tedbirlerin, son olaraksa Tüzük'ün 32. maddesi gereğince gerekli tedbirlerin kaydını tutmalıdır.

Aynı maddenin 2. fıkrasında ise veri işleyenin tutması gereken kayıtlardan bahsedilmiştir. Bu fıkraya göre veri işleyen, adına işlem yaptığı veri sorumlusunun kimlik ve iletişim bilgilerini, işleme faaliyeti kategorilerini, kişisel veri aktarımlarına ilişkin tedbirleri, son olaraksa yine Tüzük'ün 32. maddesi gereğince gerekli tedbirlerin kaydını tutmalıdır.

İşleme faaliyetine ilişkin kayıtların Tüzük gereğince yazılı tutulması gerektiği belirtilmiştir. Tüzük'ün son fıkrası ile kayıt tutacak yükümlüler sınırlandırılmıştır. Buna göre 250'den az çalışanı olan kurum veya işletmelerin özel nitelikte kişisel veri işlemediği müddetçe veya veri sahibinin hak ve menfaatlerine halel getirmediği sürece Tüzük'ün 30. maddesi kapsamında işleme faaliyetlerinin kayıtlarının tutulma zorunluluğu bulunmamaktadır.

Tüzük'ün 28. ve 30. maddelerinde gerekli hallerde denetim makamlarına yardımcı olunması gerektiği belirtilmiştir. Tüzük'ün 31. maddesinde ise denetim makamları ile işbirliği yapılması yükümlülüğü ayrıca işlenmiştir.

Tüzük, 32. maddede kişisel verileri işlemenin güvenliğini ele almıştır. Gerçek kişilerin hak ve özgürlüklerini dikkate alarak olası risklerin önüne geçmek için veri sorumlusu tarafından risk ile orantılı güvenlik önlemleri alınması gerektiği belirtilmiştir.

Gerçek kişilerin hak ve özgürlüklerini zarara uğratacak şekilde güvenlik ihlalinin olması halinde Tüzük'ün 33. maddesinde veri sorumlusunun gecikmeksizin

denetim makamına haber vermesi gerektiği belirtilmiştir. Veri sorumlusu güvenlik ihlalinin gerçekleştiğini öğrendikten sonra en geç 72 saat içerisinde denetim makamına haber vermelidir. Burada denetim makamına haber verilecek risk düşük olmamalıdır. Aynı maddede işleyenin de güvenlik ihlalinden haberdar olduğu andan itibaren vakit kaybetmeksizin veri sorumlusuna haber vermesi gerektiği belirtilmiştir.

34. maddede ise güvenlik ihlalinin yüksek risk taşıdığı durumlarda gerçek kişinin hak ve özgürlükleri zarara uğrayacaksa veri sorumlusunun, gecikmeksizin veri sahibine haber vermesi gerektiği düzenlenmiştir. 34. maddedeki güvenlik ihlali riskinin 33. maddeye göre ihtimalinin daha yüksek olması gerekir. Aynı 33. maddenin 3. fıkrasında olduğu gibi bildirim yükümlülüğünün hangi halleri kapsadığı. Tüzük'te detaylıca işlenmiştir.

Tüzük'ün 35. maddesinde gerçek kişilerin hak ve özgürlükleri açısından yüksek riskten söz edildiği hallerde veri sorumlusuna işleme faaliyetinden önce veri koruma etki değerlendirilmesi (VKED) yaptırılması yükümlülüğü getirilmiştir. Tüzük'te ayrıca veri koruma etki değerlendirilmesi yapılmasının büyük hacimli şirketler açısından gerektiği belirtilmiştir. Tüzük'ün 36. maddesinde de veri koruma etki değerlendirmesi kapsamında veri sorumlusunun işlemlerinin risk oluşturduğu ve gerçek kişinin hak ve özgürlüklerini ihlal etmesinin muhtemel olduğu hallerde işleme faaliyetinden önce veri sorumlusuna denetim makamına danışması ve ön görüşünün alınması yükümlülüğü getirilmiştir. Denetim makamı, Tüzük'ün ihlal edileceğini düşünüyorsa 8 haftada ve işleme faaliyetinin karmaşıklığı dikkate alınarak en fazla 6 hafta daha uzatarak yazılı tavsiyelerde bulunur.

Tüzük'ün 37 ila 39. Maddelerinde mahkemeler dışında, kamu kurum ve kuruluşlarında veri koruma yetkilisinin atanması öngörülmüştür. Veri koruma yetkilisinin 39. madde kapsamında görevleri belirlenmiştir. Buna göre veri sorumlusu, işleyen ve işleme faaliyeti gerçekleştiren çalışanlara Tüzük ve üye devletlerin veri koruma kanunu kapsamlarında bilgi ve tavsiye vermek, kişisel verilerin korunmasına ilişkin politikalara uyulup uyulmadığını denetlemek, denetim makamı ile işbirliği

yapmak ve gerekli hallerde görüş almak veri koruma yetkilisinin görevi kapsamında belirtilmiştir.

2.2. KVKK Kapsamında Veri Sorumlusunun Yükümlülükleri

Kanun'un gerekçesinde veri sorumlusunun aydınlatma yükümlülüğünün Direktif ile paralel düzenlendiği belirtilmiştir. 10. maddede düzenlenen veri sorumlusunun aydınlatma yükümlülüğü çerçevesinde veri sorumlusu, varsa temsilcisi ile birlikte kimliğini, veri işleme amacını, veri toplamanın yöntemini ve hukuki sebeplerini, kişisel verilerin aktarılması halinde aktarılma amacını ve veri sahibinin 11. madde kapsamındaki haklarını bilgilendirmekle veri sahibine karşı yükümlü tutulmuştur.

Kanun'un 12. maddesinin ilk fıkrasında genel olarak tedbir alma yükümlülüğü düzenlenmiştir. İlk fıkraya göre veri sorumlusu, kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önlemeli ve muhafazasını sağlamalıdır. Oldukça genel bir şekilde ifade edilen bu düzenleme hiçbir şekilde nasıl sorusuna cevap vermemekle birlikte hali hazırda böyle bir düzenleme olmasaydı bile Türk Borçlar Kanunu'nun genel hükümlerinde veri sorumlusunun böyle bir yükümlülük altında olduğu sonucu çıkarılabilirdi.

Kanun'un 12. maddesinin 2. fıkrasında ise veri sorumlusunun 1. fıkraya göre gerekli tedbirlerin alınması noktasında görevlendirdiği başka bir kişi tarafından verilerin işlenmesi halinde müşterek sorumluluğunun bulunduğu belirtilmiştir. Buradaki düzenleme Tüzük'ün 28. maddesinden ayrılmaktadır. Tüzük'ün 28. Maddesinde veri sorumlusunun veri işleyeni seçerken tedbirli davranması gerektiğini belirtmiş ve bir takım ilkeler getirmiştir. Burada ise bir anlamda veri işleyeni seçmede dolaylı olarak yükümlülük getirmiş ama asıl itibariyle veri sahibinin hak ve özgürlüklerinin zarara uğraması halinde müşterek sorumluluğu düzenlemiştir.

Kanunun 12. maddesinin 3. fıkrasında ise veri sorumlusuna genel tedbirleri alma yükümlülüğü getirilmiştir. Bu hükme göre veri sorumlusu Kanun'a uygun işlemlerin yapılması için gereken tedbirleri almalı ve denetimlerini yapmalıdır.

Kanun'un 12. maddesinin 4. fıkrasında ise veri sorumlusu ve veri işleyenin gizlilik yükümlülüğü düzenlenmiştir. Bu hükme göre Kanun'da hukuka uygun kılınmayan bir şekilde kişisel verinin başkasına ifşa edilmesi yasaklanmıştır. İşleme amacı dışında kişisel verilerin kullanılmaması yükümlülüğü getirilmiştir. Bu fıkra kapsamındaki iki yükümlülüğün de veri sorumlusu veya veri işleyenin işinden ayrılmasından sonra da devam edeceği belirtilmiştir. Tüzük'te doğrudan gizlilik yükümlülüğünü düzenleyen bir madde bulunmamakla birlikte Tüzük'ün 38. maddesinde bilgi güvenliği görevlisinin gizlilik yükümlülüğü olduğu belirtilmiş, Tüzük'ün 32. maddesinde veri sorumlusunun, işlemenin güvenliği adına işlemenin teknik sistemlerinin gizliliğine ilişkin yükümlülüğü gibi bir takım gizlilik yükümlülükleri getirilmiştir.

Tüzük'ün 33. ve 34. maddelerine paralel olarak Kanun 12. maddesinin 5. fıkrasında da kişisel verilerin hukuka aykırı bir şekilde başkaları tarafından ele geçirilmesi halinde Kurul'a ve veri sahibine, veri sorumlusu tarafından bildirileceği belirtilmiştir. Kurul'un ise gerekli görmesi halinde uygun vasıtalarla duyurabileceği belirtilmiştir. Her ne kadar bu düzenlemenin Tüzük'ün 33. ve 34. maddesindeki düzenleme ile benzer bir yükümlülüğü düzenlediği görülüyorsa da Kanun'da, Tüzük'te yer alan bildirimin en geç ne kadar süre içerisinde yapılacağı, bildirimin mahiyeti, kapsam ve içeriğinin ne olacağı gibi hususlara değinilmemiştir.

Sonuç olarak diğer birçok yasal düzenlemede olduğu gibi Tüzük'teki düzenlemeler, Kanun ve Direktif'e nazaran daha kapsamlı ve daha detaylıdır. Tüzük'te, Kanun'a kıyasla veri sorumlusunu kişisel verilerin korunması aşamasında aktif olmaya zorlayan bir durum vardır. Aynı zamanda veri sahibinin hakları da güçlendirilerek etkin bir şekilde katılımı sağlanmak istenmiştir. Bu sebeple Tüzük'te daha etkin bir veri koruma sistemi oturtulmaya çalışılmıştır. Etkin bir veri koruma sistemi ise özgür veri akışını kuvvetlendireceği gibi kuşkusuz rekabeti de güçlendirecektir.[147]

Genel itibariyle Tüzük'ün bakış açısı hukuka aykırı işlem olduktan sonra değil daha çok önleyici tedbirler almaya yönelik olduğu görülmektedir. Bu önleyici

[147] Küzeci, *Kişisel Verilerin Korunması,* s.233.

tedbirlerle mutlak bir netice alınması gerekli değildir. Hem Kanun'da hem de Tüzük'te veri sorumlusundan beklenen "gerekli" önlemleri almasıdır. Bu durumda her iki düzenleme içinde uygun güvenlik tedbirleri veri sorumlusu açısından özen sorumluluğu kapsamında değerlendirilmesi gerekecektir.[148] İşte burada Tüzükle Kanun arasındaki fark ortaya çıkmaktadır. "Gerekli önlemler" alınması noktasında veri sorumlusuna yüklenen bu şartın içeriğinin doldurulmasında Kanun'un eksik kaldığını ve bir çerçeve sunamadığını görmekteyiz.

Bir diğer hususta Tüzük'te veri sorumlularının sadece yükümlülüğü arttırılmamış, sorumluluk yüklenen kişilerin kapsamı genişletilmiştir.[149] Direktif'te yükümlülüklerin veri sorumlusu ile veri işleyen bakımından ayrımı söz konusu iken ve veri işleyen, yükümlülüklerin birçoğundan ayrık tutulmuş iken Tüzük'te bu ayrım ortadan kaldırılmış ve birçok maddede sorumluluklar beraber düzenlenmiştir. Kanun'da bu hususa ilişkin ayrıca bir hüküm bulunmamaktadır.

[148] Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu,* s. 105.
[149] Ayşe Nur Akıncı, s.21.

DÖRDÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI YOLLARI VE DÜZENLEYİCİ KURUMLARA İLİŞKİN GENEL BİLGİLER

1. Kişisel Verilerin Korunması Yolları

Direktif, Kanun ve Tüzük'ün ortaya çıkışının sebebi, ilgili kişinin mülkiyet ve özel hayatın korunması hakkı başta olmak üzere kişilik haklarının korunması ile bilginin serbest dolaşımı arasındaki dengenin sağlanmasıdır. Veri korumasına ilişkin yasal düzenlemelerde salt veri sahibinin kişilik hakları üzerine yoğunlaşılırsa veri sorumluları tarafından kişisel verinin işlenmesi imkansızlaşabileceği gibi, bilginin serbest dolaşımına öncelik verildiği takdirde de veri sahibinin temel hak ve özgürlüklerine halel gelebilir. Bu sebeple yasa yapıcılar iki kavram arasındaki dengeyi gözetmek zorundadırlar.

Kişisel verilerin korunması hukukunda bir diğer önemli hususta kişisel verilerin işlenmesinde hukuka aykırılık karinesidir. Veri sahibinin, kişisel verisinin işlenmesi yasal düzenleme ile olur hale getirilmediği müddetçe hukuka aykırı sayılacaktır. Bu sebeple de kişisel verinin işlendiği hallerde genel hukuk ilkesinin dışına çıkılacak ve veri sorumlusu veriyi hukuka uygun olarak işlediğini ispatla mükellef olacaktır.

1.1. Veri Sorumlusuna Başvuru Yoluyla Koruma

Tüzük'te de Kanun'da veri sorumlusunun yükümlülükleri ve veri sahibinin haklarına ilişkin problemlerden dolayı ilgili kişinin, veri sorumlusuna her zaman başvurabileceği düzenlenmiştir. Başvurunun nasıl yapılacağına ilişkin Tüzük ve Kanun'da paralel düzenlemeler yer almaktadır.

Kanun'un 13. maddesinde veri sahibinin yazılı olarak ya da Kurul'un getireceği esaslar[150] doğrultusunda veri sorumlusuna başvurabileceği belirtilmiştir.

[150] Kişisel Verilerin Korunması Kurumu 10 Mart 2018 tarihinde yayımladığı Veri Sorumlusuna Başvuru Usul Ve Esasları Hakkındaki Tebliğ'de (VBST) veri sahibinin yazılı başvurusu dışındaki usul ve esaslar belirtilmiştir.

Başvuru halinde veri sorumlusunun azami 30 gün olmak üzere en kısa sürede cevap vermesi gerekir. Bu başvurunun kural itibariyle ücretsiz olduğu belirtilmekle birlikte Kurul'un belirleyeceği tarifeye göre ücret alınabilir.[151] Kanun'un 3. fıkrasında da veri sorumlusunun, veri sahibinin talebini kabul edebileceği gibi gerekçeli şekilde reddedebileceği de belirtilmiş ve kabul halinde de başvuru için almış olduğu masrafı iade etmesi gerektiğine değinilmiştir.

Tüzük'ün 12. maddesinde şeffaflık ilkesi dikkate alınarak veri sahibinin başvurularında anlaşılır, sade bir dil kullanılması gerektiği ve yazılı başvuru yapılması esas olmakla birlikte bazı hallerde sözlü başvuruda da bulunulabileceği belirtilmiştir. Tıpkı Kanun'da olduğu gibi veri sorumlusunun, başvuruya ilişkin bir ay içerisinde cevap vermesi gerektiği düzenlenmiştir. Talep ve işlemin karmaşıklığı halinde ise bu sürenin en fazla 2 ay daha uzatılacağı düzenlenmiştir. Veri sahibinin benzer taleplerini tekrarlaması, taleplerinin asılsız veya ölçüsüz olması halinde veri sorumlusu belli bir ücret karşılığında bilgi temin edebileceği gibi işlem yapmayı da reddedebileceği hüküm altına alınmıştır. Ancak böyle bir durumda veri sahibi bu sebeplerle denetim makamına başvurursa ispat külfeti Tüzük'e göre veri sorumlusuna aittir.

Tüzük tıpkı 6, 8, 40 ve 57. maddelerde olduğu gibi çocuğun bilgilerine ilişkin taleplerde veri sorumlusunun daha özenli davranması gerektiğini belirtmiştir. Kanun, bu hususa ilişkin ayrıca bir hüküm getirmemiştir. Tüzük'te genel olarak veri sahibinin veri sorumlusuna başvuru imkânının 13 ila 22. maddeleri ile 34. maddesi kapsamındaki hallerden kaynaklı durumlar için olduğu belirtilmiştir. Kanun'daki ifade ise daha kapsayıcı ve soyuttur. Bununla birlikte veri sorumlusuna başvuruyla ilgili Tüzük'te düzenlenen birçok usule ilişkin husus, Kanun'da, Kurum'un 10 Mart 2018 tarihinde yayımladığı tebliğde yer almakla olup daha düşük bir yasal normla düzenlenmiştir.

1.2. İdari Yaptırımlar Yoluyla Koruma

Tüzük'ün 77. maddesinde veri sahibinin, kendisi ile ilişkili veri işlenmesi halinde bunun Tüzük'e aykırı olduğunu düşünüyorsa bulunduğu ülkede "öncelikli

[151] VBST 7. maddede veri sorumlusunun vereceği cevap 10 sayfayı geçtiği takdirde her bir sayfa için 1 TL ücret alınabileceği belirlenmiştir.

olmak" üzere denetim makamına başvurabileceği düzenlenmiştir. Aynı zamanda denetim makamının veri sahibini Tüzük'ün 78. maddesi kapsamında bilgilendirmesi gerektiğini belirtmiştir.

Tüzük'ün 78. maddesine geçmeden önce Kanun'un Kurul'a başvuru sürecine değinmekte fayda vardır. Kanun diğer birçok düzenlemenin aksine 14. ve 15. maddede Kurul'a başvuruyu daha detaylı düzenlemiştir. İlk olarak 14. maddede Kurul'a başvuru için Kanun'un 13. maddesine göre veri sorumlusuna başvuru yapılması gerektiği ön görülmüştür. Böylece Kanun, Kurul'un gereksiz iş yükünün oluşmasını da engellemek istemiştir. Tüzük'te ise veri sorumlusuna başvuru önkoşulu düzenlenmediği gibi 78. maddede denetim makamının resen harekete geçebileceğine ilişkin bir hükümde bulunmamaktadır.

Kanun'da Kurul'a şikâyette bulunulması için veri sorumlusunun cevap vermesinden itibaren 30 gün ve herhalde 60 günlük süre öngörülmüştür. Buradaki herhalde kelimesinden sürenin başlayacağı tarihi Kanun'un 13. maddesinde belirtilmiş olan veri sorumlusuna başvuru tarihinden itibaren başlaması gerekir. Tüzük 78. Maddesinde denetim makamına başvuru süresi ayrıca belirtilmemiştir.

Kanun'da şikayetin Kurul tarafından cevaplanması için 60 günlük, Tüzük'te ise denetim makamı tarafından cevaplanması için 3 aylık süre verilmiştir. Aksi takdirde her iki düzenlemede de yasal yollara başvurulabileceği öngörülmüştür.

Cezaların orantılı, caydırıcı ve etkili olmasına Tüzük'ün hem 83. Hem 84. maddesinde değinilmiş ve ayrı bir önem atfedilmiştir. Cezanın belirlenmesi noktasında denetim makamına geniş takdir yetkisinin verildiğini söylemek yerinde olacaktır. Ceza miktarının belirlenmesinde üye ülkeler arasındaki denetim makamının hükmedebileceği cezalar arasında farklılıklar olabileceğinden, belirli bir standardın ve öngörülebilirliğin sağlanması adına Tüzük'ün 83. maddesinde detaylı bir düzenlemeye gidilmiştir. Kanun'un 18. maddesinde ise verilen idari para cezalarının hangi hallerde alt sınırdan hangi hallerde de üst sınırdan verilebileceğine ilişkin bir düzenleme yapılmamıştır. Buna karşılık 16. maddede benzer nitelikteki ihlallerin fazla olduğunu fark eden Kurul, ilke kararları alabileceği belirtilmiştir.

Tüzük'ün 83. maddesinde düzenlenen idari para cezaları çeşit ve nicelik itibariyle Kanun'un 18. maddesinde düzenlenen hükme göre daha geniştir. Kanun'da, Kurul'un idari para cezasına hükmedebileceği durumların; aydınlatma yükümlülüğüne, veri güvenliğine, bildirim yükümlülüğüne aykırı hareket etmesi ve Kurul'un vermiş olduğu kararı uygulamaması şeklinde 4 farkı halde olabileceği belirtilmiştir. Tüzük'te ise sertifika ve gözetim kurumlarına ilişkin yükümlüklerden, 8. madde kapsamında çocukların kişisel verilerin işlenmesine rızasına ilişkin hükümlere, veri sahibinin hak ve yükümlülüklerinin ihlalinden veri sorumluluklarının yükümlülüklerine kadar birçok ihlali çeşitlendirerek hüküm getirmiştir. Verilen idari para cezasının niceliği itibariyle ise 83. maddede alt sınır verilmeden değişen şart ve ihlallere göre üst sınırı 10.000.000 Euro ve 20.000.000 Euro'ya varıncaya kadar ceza verilebileceği belirtilmiştir. Ayrıca Direktif ve Kanun'dan farklı olarak işletmenin cirosunun %2 ve %4 üne kadar idari para cezasına hükmedilebileceğini de belirtmiştir. İşletmelerin ciroları üzerinden ceza kesilmesinin hakkaniyete daha uygun olacağı kuşkusuzdur. Özellikle dünya çapında birçok ülkenin gayri safi milli hasılasından yüksek olan şirketlerin, hukuka aykırı bir şekilde kişisel verileri ihlal etmesi halinde 10.000.000 Euro ve 20.000.000 Euro gibi değerlerin etkisiz kalacağı kuşkusuzdur.[152] Kanun'daki düzenlemede ise şirketlerin ciroları üzerinden bir değerlendirme yapılmadığı gibi verilebilecek idari para cezasının üst sınırı 1.000.000-TL olarak belirlenmiştir. Ayrıca verilecek cezanın niteliğine göre kanun koyucu 18. maddede alt sınır idari para cezası da belirlemiştir.

1.3. Cezai Yaptırımlar Yoluyla Koruma

84. maddede Tüzük'ün ihlallerinden kaynaklı hallerde cezai hükümlerin üye devletlerin kendi iç hukuklarındaki düzenlemeye uygun olarak gerekli tedbirleri alması gerektiği belirtilmiştir. Her bir ülkenin ayrı ayrı değerlendirilmesi çalışma kapsamında olmadığından bu hususta yalnızca 84. madde hükmü belirtilmekle yetinilmiştir. Buna karşılık üye ülkelerin İngiltere ve İrlanda örneğinde olduğu bir kısmında kişisel verilerin korunmasına ilişkin hürriyeti bağlayıcı cezaların olmadığı ve idari para cezası ile yetinildiği, büyük bir kısmında ise cezaların üst sınırının düşük tutulduğu

[152] Apple'ın 2018 itibariyle cirosunun dünyanın en güçlü ekonomileri sıralamasında 18. Sırada olan ülkemiz ile yarışır durumda olduğu gözükmektedir. https://www.bloomberght.com/haberler/haber/2119143-apple-in-cirosu-turkiye-nin-gsyh-siyle-yarisir 20.05.2019

görülmektedir.[153] Tüzük sadece kişisel verilerin ihlalinden kaynaklı suçlarda cezaların etkili, orantılı ve caydırıcı olması gerektiğini belirtmekle yetinmiştir.

Kişisel verilerin korunmasına ilişkin cezai yaptırımlara ilişkin hususlarda, Birlik üye ülke hukuklarında iki farklı yaklaşım olduğu görülmektedir. Örneğin, Almanya ve İtalya'da kişisel verilerin ihlaline ilişkin cezai yaptırımlar, veri koruma yasalarında yer alırken, Fransa'da ise genel ceza kanunu kapsamında düzenlemeler yapılmıştır.[154] Türk hukukunda ise 2010 anayasa değişikliği öncesindeki TCK'daki hükümler, KVKK sonrasında da varlığını sürdürmüştür. KVKK'nın 17. maddesinde ise 5237 sayılı TCK'nın 135 ila 140. maddelerine atıf yapılmakla yetinilmiştir. TCK'nın 135. maddesinde kişisel verilerin kaydedilmesi suçu, 136. maddesinde verilerin hukuka aykırı olarak verilmesi ve ele geçirilmesi suçu, 137. maddede 135 ve 136 ıncı maddelerde tanımlanan suçların nitelikli hallerini, 138. maddede verilerin yok edilmesi suçu, 139. Maddede bu suçların hangi hallerde şikâyete tabi suçlar kapsamında değerlendireceği, 140. maddede ise bu suçlar kapsamında tüzel kişiler hakkındaki güvenlik tedbirlerinin uygulanması açıklanmıştır.[155]

1.4. Genel Düzenlemelerde Yer Alan İmkânlar Yoluyla Koruma

Tüzük'ün 79. maddesinde veri sahiplerinin, Tüzük'e aykırı işlemlerden kaynaklı olarak yasal yollara başvurabileceği belirtilmiştir. Veri sahibi, maddi ve manevi zararını Tüzük'ün 26. maddesindeki hüküm dikkate alınarak tüm veri sorumlularından isteyebilecektir. Veri sahibinin, maddi ve manevi zararının tazmini için veri işleyene başvurabileceği haller Tüzük'te ayrıca veri işleyenin sorumlu tutulduğu işleme faaliyetine ilişkin işlemlerle sınırlıdır. Tüzük'ün 82. maddesinde veri sahibinin zararının oluşması halinde bu zarardan sorumlu olmadığının ispat külfetinin, veri sorumlusu ve veri işleyene ait olacağını belirtmiştir. Zararın tazminini isteyen veri sahibi, Tüzük'ün 79. maddesinde belirtildiği gibi kendi yerleşim yerinde dava açabileceği gibi, veri sorumlusu ve işleyenin işletmelerinin bulunduğu yer

[153] Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, Rapor, İstanbul Bilgi Üniversitesi, 2014, s.72.

[154] Elif Küzeci, **Kişisel Verilerin Korunması**, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Ankara, 2010, s. 308

[155] TCK kapsamındaki kişisel verilerin korunmasına ilişkin yasal düzenlemeler için ayrıca bkz. Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, 1.Baskı, Seçkin, Ankara, 2019

mahkemesinde de dava açabilecektir. Ancak burada veri işleyen ve veri sorumlusunun işletmelerinin üye devlette bulunması gerektiği ayrıca belirtilmiştir.

Kanun'un 14. maddesinin son fıkrasında kişilik hakkı ihlal edilen kişilerin oluşan bir zararı varsa bu zararının tazminini genel hükümlere göre talep etme imkânının olduğu düzenlenmiştir. Buradaki genel hükümlerden sadece medeni hukuk ve borçlar hukukundan kaynaklı tazminat davası açılabileceği sonucu çıkmamaktadır. Elektronik haberleşme hukukundan, sağlık hukukuna, iş hukukundan, vergi hukukuna ilişkin özellikle anayasal düzenleme sonrasında mevzuata derç edilmiş kişisel verilerin korunması ile bağlantılı bütün hükümler Kanun'un 14. maddesinde belirtilen genel hüküm kapsamında değerlendirilebilinir.

TMK'nın 25. maddesini incelediğimizde, ilk fıkrasında veri sahibi kişisel verilerine yönelik bir saldırı olduğunu düşünüyorsa saldırının önlenmesini isteyebileceği gibi var olan saldırıya sona erdirilmesini de isteyebilir. Bununla birlikte kişisel verilerine yapılan saldırının saldırı son bulmuş olsa dahi hukuka aykırılığının tespitini isteyebilir. Ayrıca veri sahibi bir zararının olduğunu düşünüyorsa 25. maddedeki hükümler kapsamında maddi ve manevi tazminat davası da açabilir.[156] Tıpkı cezai yaptırımlarda olduğu gibi hukuki yaptırımlarda da Tüzük, üye ülkenin genel hukuk kurallarına ve ülke içerisindeki yasal düzenlemelere değinmekten kaçınmıştır. Çalışmanın konusunu teşkil etmediğinden her bir durum için ayrı ayrı değerlendirme yapılamamıştır.

Sonuç olarak Tüzük'te, veri sorumlusuna başvuru ve idari yaptırımlar yoluyla kişisel verilerin korunmasının Direktif ve Kanun'a nazaran daha detaylıca işlendiğini görmekteyiz. Tüzük'ün belirlemiş olduğu prensipler çerçevesinde veri ihlalinin yaşanmaması adına önleyici tedbirler alınması gerektiği hususunda kazuistik bir düzenlemeye gidilmiştir. Tüzük'te özellikle şeffaflık ilkesine veri sahibinin veri sorumlusuna başvuruyu düzenlerken tekrardan değindiğini görmekteyiz. Aynı şekilde Tüzük'ün birçok maddesinde olduğu gibi çocuğun kişisel verilerinin korunmasına

[156] Bu davalara ilişkin ayrıca bkz. Jale G. Akipek, Turgut Akıntürk, Derya Ateş, **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku**, C. 1, 10.Baskı, Beta, İstanbul, 2018, S. 414-435

yönelik önemi bir kez daha vurgulanmış ve ayrıca değinilmiştir. Kişisel verilerin korunma yolları noktasında Tüzük'ü diğer iki düzenlemeden ayıran en önemli hususun veri sorumlusuna, ihlalden kaynaklı daha caydırıcı yaptırımlar olduğu kuşkusuzdur. Maalesef ki, özellikle yüksek ciro sahip şirketlerin veri ihlallerinin önüne geçilmesi noktasında Kanun'da düzenlenen yaptırımların üst haddi dikkate alındığında etkisiz kalabileceği gözükmektedir. Bu sebeple idari para cezalarının daha da caydırıcı olması adına Kanun'un 18. maddesinde Tüzük'e paralel bir düzenleme ile değişiklik yapılması gerekmektedir.

2. Düzenleyici Kurumlar İle İlgili Genel Bilgiler

Tüzük'te bağımsız denetim makamları olarak adlandırılan kurumlar Tüzük'ün 6. kısmının başlangıcı olan 51. ila 68. maddede detaylı bir şekilde düzenlenmiştir. 51. maddede veri sahiplerinin kişisel veriler ile alakalı temel hak ve özgürlüklerini korumak adına en az bir tane bağımsız denetim makamı oluşturması ön görülmüştür. 52. maddede ise denetim makamının yetkilerini kullanırken bağımsız olması gerektiği vurgusu yapılmıştır. Ülkemizdeki bağımsız denetim makamının karşılığı Kişisel Verilerin Korunması Kurumudur. Kişisel Verilerin Korunması Kurumu'nun kamu tüzel kişiliğine sahip olduğu, idari ve mali özerkliğinin bulunduğu ve Başbakanlıkla[157] ilişkili olduğu Kanun'un 19. maddesi kapsamında belirtilmiştir.

Tüzük'teki denetim makamının kurulmasına, yetki ve görevine ilişkin hükümler 54 ila 59. maddeleri arasında detaylı bir şekilde düzenlenmiştir. Kanun'da ise 22. maddede ve 26/04/2018 Resmi Gazete yayım tarihli Kişisel Verilerin Korunması Kurumu Teşkilat Yönetmeliği ile Kurum'un görev ve yetkileri anlatılmıştır. Ayrıca Birlik içerisindeki yardımlaşma işbirliği ve yetki dağılımını sağlamak adına Tüzük'te bir takım düzenlemelere yer verilmiştir. Buna göre üye ülkeler arasındaki işbirliğini sağlamak için Tüzük'ün 60. maddesinde, karşılıklı yardımlaşmayı sağlamak için Tüzük'ün 61. maddesinde, ortak denetim makamları arasında ortak operasyonların

[157] 15 Temmuz 2018 tarihli ve 30479 sayılı Resmi Gazetede yayımlanan "Bakanlıklara Bağlı, İlgili ve İlişkili Kurum ve Kuruluşlar ile İlgili 2018/1 Sayılı Cumhurbaşkanlığı Genelgesi ile kurum Adalet Bakanlığı ile ilişkilendirilmiştir. Ayrıca 9 üyeli Kurul'un önceden 2 üyesi Bakanlar Kurulu 2 üyesi Cumhurbaşkanı tarafından seçiliyorken bu değişiklikle birlikte 4 üyenin Cumhurbaşkanınca seçilmesi öngörülmüştür.

gerçekleştirilmesi için Tüzük'ün 62. maddesinde, Tüzük'ün üye ülkelerde birbirinden farklı uygulamaların ortaya çıkmasına mahal vermemek ve tutarlılık mekanizmasının sağlanması için Tüzük'ün 63 ila 65. maddelerinde, istisnai hallerde aciliyet prosedürünün işlemesi için Tüzük'ün 66. maddesinde bir takım düzenlemelere yer verilmiştir. Bu düzenlemelerin Türk hukukunda uygulama alanı ve mevzuatsal karşılaştırması mümkün olmadığından çalışma kapsamında değerlendirilmemiştir. Bununla birlikte Avrupa Birliği Verilerin Korunması Kurumu, Tüzük'te bahsedilen başka bir kurumdur. Teşkilat yapısı itibari ile her üye devletin denetim makamı başkanlarından oluşan bu Kurum, üye ülkeler arasındaki koordinasyonun sağlanması, uyuşmazlıkların ve problemlerin çözüme kavuşturulması amacıyla ortaya çıkmıştır.[158]

Gerek Tüzük için gerekse de Kanun için kurumlar üzerinde durulması gereken en önemli husus bağımsızlık konusudur. Direktif ve Tüzük'te denetim makamının bağımsız olması gerektiği noktasında birçok düzenleme söz konusudur. Aynı hususa Kanun'un gerekçesinde de birçok noktada dikkat çekilmiştir. Bağımsızlık sadece Kurul'un oluşturulması aşamasında değil mali işler noktasında da önemlidir. Nitekim 2017 faaliyet raporunu incelediğimizde Kurum'un kadrosunda 24 kadrolu personelin olduğu, ayrılan toplam kadronun ise 195 olduğu görülmektedir.[159] Bu sayı başta Kanun'daki hükümler olmak üzere Kurul'a yüklenen görev ve yetkilerin karşısında çok düşük olduğunu söylemek yerinde olacaktır. Aynı durumu Birleşik Krallık için değerlendirdiğimizde 2011 verilerine göre 319 personel çalıştığı anlaşılmaktadır.[160] Diğer yandan 2019 yılı Merkezi Yönetim Bütçe Kanunu'nda Kişisel Verilerin Korunması Kurumu'na ayrılan bütçenin yeni kurulan bir Kurum olmasına rağmen 33.770,00-TL olduğu,[161] Birlik üyesi ülkelere baktığımızda ise 2011 yılı itibari ile veri koruma kurumlarına ayrılan bütçelerin İtalya'da 24.500,00 Euro, Birleşik Krallıkta ise 22.395,00 Euro olduğu görülmektedir. Sonuç olarak mali ve kadro durumu dikkate alındığında Kişisel Verilerin Korunması Kurumu'nu, AB üyesi ülkelerin kurumları ile

[158] Devecioğlu s.148.

[159] 2017 yılı Kişisel Verilerin Korunması Kurumu'nun faaliyet raporu, s. 30 https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/2017-Faaliyet-Raporu.pdf 20.05.2019

[160] Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, s.85.

[161] Bkz. http://www.resmigazete.gov.tr/eskiler/2018/12/20181231M1.pdf syf 15.

karşılaştırdığımızda çok daha geride kaldığını söylemek yerinde olacaktır. Gerçekten de Kurum'un ve çerçeve yasanın Türk hukukuyla yeni yeni ve hızlı bir şekilde etkileşime geçtiği günümüzde mali ve idari yapıdaki bağımsızlık ayrı bir önemi vardır. Aksi takdirde "bağımsız" bir veri koruma otoritesinin olmaması, başta Birlik olmak üzere birçok oluşum ve ülkede ülkemizin "güvenilir ülke" statüsü kazanımının önüne geçecektir. Özellikle AB ve Türkiye arasındaki kişisel verilerin aktarımı hususunda sıkıntıların yaşanmaması adına Kişisel Verilerin Korunması Kurumu'nun merkezi otoriteden bağımsızlığı önem taşımaktadır.

SONUÇ

Ülkemizde 2010 yılı anayasa değişikliği ile birlikte kişisel verilerin korunması hakkı anayasal zemine oturtulmuştur. Her ne kadar Anayasa'nın 20. maddesindeki değişiklik öncesinde birçok yasal metinde kişisel verilerin korunması hakkına ilişkin düzenlemeler söz konusuysa da 6698 sayılı KVKK ile birlikte Anayasa'daki bu hüküm somutlaştırılmıştır. 95/46/AT Sayılı Direktif referans alınarak 2016 yılında 6698 sayılı KVKK yürürlüğe girmiştir. Aynı yıl AB Genel Veri Koruma Tüzüğü onaylanmıştır.

Tüzük'le birlikte AB üyesi ülkelerin iç hukuklarındaki kişisel verilerin korunmasına ilişkin farklılıkların, AB hukukunda daha üst bir yasal normla giderilmeye çalışıldığı görülmektedir. Tüzükle birlikte Birlik hukukunda kişisel verilerin korunması noktasında zamanın ruhu ile birlikte geleceğin yakalanması hedeflendiği ortadadır. Gerçekten de kişisel verilerin işlenmesi, veri sahibinin hakları ve veri sorumlusunun yükümlülükleri ile kişisel verilerin korunması yollarına kadar ve daha birçok hususta kazuistik düzenlemelerin yapıldığı anlaşılmaktadır.

Çalışmamızın başından itibaren işaret edildiği gibi kişisel verilerin korunması hakkı, Birlik üyesi birçok ülkede, çerçeve yasal düzenlemeler ile yaklaşık 40 küsur yıldır koruma altına alınmıştır. Bu noktada Türk hukukunda kişisel verilerin korunması hakkına ilişkin çerçeve düzenlemenin çok geç yürürlüğe girdiğini söyleyebiliriz. KVKK'nın yürürlüğe girmesi kişisel verilerin korunması adına birçok eksikliği tamamlayıcı olmakla beraber yine birçok maddesinde uygulamanın usulü belirtilmeden işleyişin Kurul'a bırakıldığına ya da sonradan konu hakkında ikincil düzenleme yapılması gerektiğine şahit olmaktayız. Nitekim Kanun'un yürürlüğe girdiği tarihten itibaren şu zamana kadar Kanun dayanak alınarak çok sayıda yönetmelik, tebliğ ve Cumhurbaşkanlığı kararnameleri ile kişisel verilerin korunmasına ilişkin yeni hükümler yürürlüğe girmiştir. Kanun'un esasa ilişkin hükümlerinden ziyade usule ilişkin hükümleri genel itibariyle ikincil düzenlemelere bırakılmıştır. Bir anlamda Kanun "ne" sorusuna cevap vermiş; ancak "nasıl" sorusuna cevap vermekten kaçınmıştır. Tabii ki, Türk hukuk sisteminde kanunun normlar hiyerarşisindeki yeri genel itibariyle soyut

hükümler sunmasından ibarettir. Ancak diğer yandan da kişisel verilerin korunması hakkı anayasal düzlemde bir insan hakkıdır. Bu sebeple de temel hak ve özgürlüklere ilişkin düzenlemelerin ancak kanunla sınırlandırılabileceği gözden kaçmamalıdır. Özellikle de kurulu idari yaptırımları, veri sorumlusunun yükümlülükleri ve veri sahibinin haklarına ilişkin hükümlerde Kanun'da yapılacak yeni düzenlemelere ihtiyaç vardır. Tüm bu hususların yanında ayrıca Kanun'daki genel istisnai hükümlerin çok sayıda olması özellikle kamu adına yapılan kişisel verilerin işlenmesine ilişkin işlemlerde neredeyse kamu kurum ve kuruluşları devre dışı bırakılmıştır.

Tüzük'ün, Kanun karşısında bağlayıcılığı olmamakla birlikte önümüzdeki süreçte uygulamada yol gösterici olacağı kuşkusuzdur. Gerçekten de Kanun'un özellikle hak ve yükümlülükler noktasındaki hükümleri o kadar genel boyuttadır ki uygulaması neredeyse tamamen Kurul'un ve yargı mercilerinin inisiyatifine bırakılmıştır. Veri sorumlusu içinde veri sahibi içinde bir hak ihlalinin olup olmadığı noktasında öngörülebilirlik oldukça kısıtlıdır. Yani birçok noktada Kurul ve yargı mercileri, bir çerçeve yasa olmasına rağmen halen, çoğunlukla hukukun genel hükümlerine bakarak karar verebilecek durumdadır. Bunun yanında hak ihlallerini önleyici tedbirler Tüzük'e nazaran sınırlı sayıda düzenlenmiştir. Sonuç olarak Türkiye için sağlıklı bir veri koruma politikası hedefleniyorsa öncelikle hakkın özüne dokunmayan ve kanunda eksikliğini belirttiğimiz birçok hususun kanuna derç edilerek sair hususların ise ikincil düzenlemelerle yerine getirilmesi gerekmektedir. Bununla birlikte Kanun'un gerekçesinde de değinilmiş olunduğu gibi nasıl ki Direktif, Kanun'un oluşturulmasında referans kaynak alındıysa Tüzük'te bağlayıcılığı olmamakla birlikte Kurul'un kararlarında da dikkate alınması gerekmektedir.

KAYNAKÇA

Resmi Belgeler, Davalar Ve Elektronik Kaynaklar

- Anayasa Mahkemesi 2013/5653 esas no.lu 3.3.2016 karar tarihli ilamı
- Anayasa Mahkemesi 2014/180 esas 2015/30 karar no.lu 19.3.2015 tarihli ilamı
- Anayasa Mahkemesi 2016/125 esas 2017/143 karar sayılı 28.9.2017 tarihli ilamı
- Bölge Adliye Mahkemesi (Ankara) 25. Hukuk Dairesi 2018/3033 esas 2018/2010 karar no.lu 12.12.2018 tarihli ilamı
- Bölge Adliye Mahkemesi (Adana) 3. Hukuk Dairesi 2018/429 esas 2018/478 karar no.lu 02.05.2018 tarihli ilamı
- C-101/01 Bodil Lindqvist ECLI:EU:C:2003:596
- C-362/14, Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650
- C-230/14 Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, EU:C:2015:639.
- C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ECLI:EU:C:2014:317
- C-362/14, Maximillian Schrems v Protection Commissioner ECLI:EU:C:2015:65
- C-70/10 Scarlett Extended, EU:C:2011:771
- C-582/14 Breyer, EU:C:2016:779

❖ Yargıtay 4. Hukuk Dairesi 2012/16267 esas 2013/15422 karar no.lu 01.10.2013 tarihli ilamı

❖ Yargıtay 11. Hukuk Dairesi 2011/4104 esas 2012/11588 karar no.lu 02.07.2012 tarihli ilamı

❖ Yargıtay Hukuk Genel Kurulu 2014/4-56 esas 2015/1679 karar no.lu 17.06.2015 tarihli ilamı

❖ Dünya İnternet, Sosyal Medya ve Mobil Kullanıcı İstatistikleri https://dijilopedi.com/2019-internet-kullanimi-ve-sosyal-medya-istatistikleri/ (Erişim Tarihi: 20.05.2019)

❖ Kimlik bilgilerinin çalınması ile ilgili haber http://www.hurriyet.com.tr/gundem/kimlik-bilgileri-calindi-simdi-ne-olacak-40083035 (Erişim Tarihi: 20.05.2019)

❖ Kişisel Verilerin Korunması Kurulu, Kişisel Verilerin İşlenme Şartları, https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari (Erişim Tarihi: 20.05.2019)

❖ 2017 yılı Kişisel Verilerin Korunması Kurumu'nun Faaliyet Raporu, https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/2017-Faaliyet-Raporu.pdf (Erişim Tarihi: 20.05.2019)

❖ 2019 yılı Merkezi Yönetim Bütçe Kanunu, http://www.resmigazete.gov.tr/eskiler/2018/12/20181231M1.pdf (Erişim Tarihi: 20.05.2019)

❖ 2013 tarihli Kişisel Alanın Korunması Ve Sınır Ötesi Kişisel Veri Dolaşımına İlişkin Rehber İlkeleri https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Erişim Tarihi: 20.05.2019)

❖ AB Temel Haklar Şartının Türkçe metni https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708 (Erişim Tarihi: 20.05.2019)

Kitaplar Ve Makaleler

❖ Akgül, Aydın. Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, 2013.

❖ Akgül, Aydın. Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" Ve Ab Adalet Divanı'nın "Google Kararı", Türkiye Barolar Birliği Dergisi, Y:2016, S:116, s.11-38.

❖ Akıncı, Ayşe Nur. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirmesi, Çalışma Raporu, Kalkınma Bakanlığı, Ankara, 2017.

❖ Akipek, Jale G.; Akıntürk, Turgut; Ateş, Derya. Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, C. 1, 10.Baskı, Beta, İstanbul, 2018.

❖ Aksoy, Hüseyin Can. Medeni Hukuk Ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, 1. Basım, Ankara, 2010.

❖ Atak, Songül. Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, Türkiye Barolar Birliği Dergisi, S. 87, 2010, s.90-120

❖ Aydın, Sedat Erdem. AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, 2014.

❖ Bainbridge, David I.. EC Data Protection Directive, Butterworths, Birleşik Krallık, 1996.

❖ Başalp, Nilgün. Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Dergisi, C.21, S.1, 2015, s. 77-105.

❖ Başalp, Nilgün. Kişisel Verilerin Korunması Ve Saklanması, 1. Basım, Ankara, 2004.

❖ Bayram, Zeynep. Kolluğun, Suç Öncesi Ve Sonrası Kişisel Veri Toplama Yetkisi, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, İstanbul, 2009.

❖ Civelek, Dilek Yüksel. Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Başbakanlık Devlet Planlama Teşkilatı Uzmanlık Tezi, Bilgi Toplumu Dairesi Başkanlığı, Ankara, 2011.

❖ Çakrak, Recep; İldeş, Samet. Kamu Hukuku Ve Özel Hukuk Açısından Dürüstlük Kuralı Ve Uygulama Alanı, Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C.2 S.2, 2014, s.47-76.

❖ Çekin, Mesut Serdar. Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 1. Basım, İstanbul, 2018.

❖ Develioğlu, Hüseyin Murat. 6698 Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, 1. Basım, İstanbul, 2017.

❖ Dinç, Engin. Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye'nin Durumu, Yüksek Lisans Tezi, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Diyarbakır, 2006.

❖ Dülger, Murat Volkan. KVK ve TCK Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3(2), 2016, s. 101-167.

❖ Gözler, Kemal. İdare Hukuku, C.1, Bursa, 1. Basım, 2009.

❖ Gözüküçük, Merve. Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014, s.8-42.

❖ Gülener Serdar. Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı", Türkiye Barolar Birliği Dergisi, Y:2012, S:102, s.221-240.

❖ Gür, İkbal. Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar Ve Çözüm Yolları, 1. Basım, Ankara, 2010.

❖ Hafızoğulları, Zeki; Özen, Muharrem. Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar, US-A Yayıncılık, Ankara, 2010.

❖ Henri, De Waele. Implications of Replacing the Data Protection Directive with a Regulation - a Legal Perspective, Privacy & Data Protection, Cilt: 12, Sayı: 4, 2012, (çeviren) Nurullah Tekin, Küresel Bakış, Yıl: 4, Sayı: 13, 2014.

❖ İmamoğlu, Deniz Alp. 6698 KVKK Uyarınca Özel Nitelikli Kişisel Verilerin İşlenme Şartları, İstanbul, 2017.

❖ Kaya, Cemil. Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler Ve İşlenmesi, İÜHFM C.69, S. l-2, 2011, s.319-334.

❖ Ketizmen, Muammer. Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara, 2008.

❖ Kılınç, Doğan. Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C61, S.3, 2012, s.1089-1169.

❖ Korkmaz, İbrahim. Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, Türkiye Barolar Birliği Dergisi, Y:2016, S:124, s.82-152.

❖ Kuner, Cristopher. European Data Protection Law: Corporate Compliance and Regulation, 2. Basım, Oxford Universty Press, 2007.

❖ Küzeci, Elif. Kişisel Verilerin Korunması, 3.Basım, Ankara, 2019.

❖ Küzeci, Elif. Kişisel Verilerin Korunması, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Ankara, 2010.

❖ Manav, Eda. İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. 19, Y. 2015, Sa. 2, s.95-136.

❖ Oğuzman, M. Kemal; Barlas, Nami. Medeni Hukuk, 19. Basım, İstanbul 2013.

❖ Oğuzman, M. Kemal; Öz, Turgut. Borçlar Hukuku Genel Hükümler, İstanbul, C. 1, 2014.

❖ Reçber, Kamuran. Avrupa Birliği Hukuku Temel Metinleri, 2. Basım, Bursa, 2013.

❖ Sert, Şeyma. Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, 1.Baskı, Seçkin, Ankara, 2019.

❖ Şimşek, Oğuz. Anayasa Hukukunda Kişisel Verilerin Korunması, 1. Basım, İstanbul, 2008.

❖ Taşkın, Ahmet. İş Hukukunda İşletme Kavramı, Çalışma ve Toplum, 2012/1, s. 75-112.

❖ Taştan, Furkan Güneş. Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 1. Basım, İstanbul, 2017.

❖ Tekin, Nurullah. Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi, Uyuşmazlık Mahkemesi Dergisi, Sayı 4, 2014, s. 222-262.

❖ Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, Rapor, İstanbul Bilgi Üniversitesi, 2014.

❖ Weber Rolf H., "The Right to Be Forgotten, More Than a Pandora's Box", Journal of Intellectual Property, Information Technology and E-Commerce Law 120, 2011.