Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Hukuk Anabilim Dalı
Özel Hukuk Yüksek Lisans Programı

TÜRK HUKUKUNDA VERİ SORUMLUSU KAVRAMI

Mesut HALICIOĞLU

Yüksek Lisans Tezi

Ankara, 2019

TÜRK HUKUKUNDA VERİ SORUMLUSU KAVRAMI

Mesut HALICIOĞLU

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Hukuk Anabilim Dalı
Özel Hukuk Yüksek Lisans Programı

Yüksek Lisans Tezi

Ankara, 2019

KABUL VE ONAY

Mesut HALICIOĞLU tarafından hazırlanan "Türk Hukukunda Veri Sorumlusu Kavramı" başlıklı bu çalışma, 17.06.2019 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Prof. Dr. Erkan KÜÇÜKGÜNGÖR (Başkan – Danışman)

Doç. Dr. Leyla Müjde KURT (Üye)

Dr. Öğr. Üyesi Burcu G. ÖZCAN BÜYÜKTANIR (Üye)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 12 ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

17/06/2019

Mesut Halıcıoğlu

1"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

(1) Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.

(2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.

(3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

* Tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu tarafından karar verilir.

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, Prof. Dr. Erkan Küçükgüngör danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

Mesut Halıcıoğlu

ÖZET

HALICIOĞLU, Mesut. *Türk Hukukunda Veri Sorumlusu Kavramı*, Yüksek Lisans Tezi, Ankara, 2019.

Veri koruma hukukunun temel amacı, verilerin hukuka aykırı olarak kaydedilmesini önlemek ve bu veriler üzerinde gerçekleştirilen bütün işlemlerin hukuka uygunluğunu sağlamaktır. Avrupa'da 1950'lerde kişisel verilerin önemi ve korunmasına dair farkındalık gelişmeye başlamış ve bu farkındalık düzeyi "Avrupa Birliği Genel Veri Koruma Tüzüğü" ("General Data Protection Regulation" / "GDPR")'nün 2016 yılında kabul edilmesi ile zirve yapmıştır. Bu düzenleme, günümüz dünyasında büyük yankı uyandırmış ve özellikle dev teknoloji firmaları veri koruma otoriteleri tarafından açılan soruşturmalarla yüzleşmek zorunda kalmıştır.

Dünyada veri koruması alanındaki gelişmeleri takiben, Türkiye'de ise 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") ancak 7 Nisan 2016 tarihinde yürürlüğe girmiştir. 7 Nisan 2018 tarihinden itibaren ise Türk veri koruma otoritesinin uygulamalarının da yaygınlaşması ile veri sorumluları, KVKK kapsamında getirilen yükümlülüklere uyum sağlayabilmek için çalışmalar yapmakta ve geç de olsa uyum süreçlerini başlatmış bulunmaktadır. Bu sayede, veri sorumluları ve işleyenler, üstlendikleri hukuki ve cezai sorumluluğun da etkisiyle, KVKK altındaki yükümlülüklerini yerine getirmektedir.

Tezimiz ise, bu açıklamalar ışığında iki bölümden oluşmaktadır. İlk bölümde, "kişisel veri kavramı, kişisel verilerin korunması hakkı, kişisel verilerin korunmasının fonksiyonu" ve "kişisel verilerin korunması hakkının normatif temelleri" irdelenmekte; ikinci bölümde ise tezimizin başlığını oluşturan "Türk hukukunda veri sorumlusu kavramı" tüm yönleriyle değerlendirilmektedir.

Anahtar Sözcükler

Kişisel Veri, Verilerin Korunması, KVKK, Veri Sorumlusu, Gizlilik, GDPR, Bilgi Teknolojileri.

ABSTRACT

HALICIOĞLU, Mesut. *Data Controller Concept Under Turkish Law*, Master's Thesis, Ankara, 2019.

The main purpose of data protection law is to prevent unlawful recording of data and to ensure that all transactions performed on these data comply with the law. In 1950s, an awareness began to develop in Europe regarding the importance of personal data and its protection and this awareness reached its peak with the entry into force of the "General Data Protection Regulation" ("GDPR") in 2016. This Regulation had major repercussions in today's world and giant technology companies have faced investigations initiated by data protection authorities.

Following the global developments in the field of data protection, the Law on the Protection of Personal Data numbered 6698 entered into force in Turkey in April 7, 2016. As of April 7, 2018, with the increasing practices of the Turkish data protection authority, data controllers have begun to carry out projects to provide compliance with their liabilities under the Law on the Protection of Personal Data and the compliance process has been initiated, albeit late. In this respect, data controllers and processors have taken action to fulfill their obligations with the compulsivity of the legal and criminal liabilities issued under the the Law on the Protection of Personal Data numbered 6698.

In the light of this, this thesis is composed of two parts. In the first part, "the concept of personal data, the right to protection of personal data, the function of protection of personal data" and "normative basis of the right to protection of personal data" are examined. In the second part, "the data controller concept under Turkish law", which is also the title of this thesis, is evaluated in all aspects.

Keywords

Personal Data, Data Protection, LPDP, Data Controller, Privacy, GDPR, Information Technology.

İÇİNDEKİLER

KISALTMALAR

108 sayılı Sözleşme: Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşme

95/46/EC sayılı Yönerge- Yönerge : Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin 24 Ekim 1995 Tarihli ve 95/46/EC Sayılı Avrupa Parlamentosu ve Konseyi Yönergesi

AB : Avrupa Birliği

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

B. : Baskı

BM : Birleşmiş Milletler

C. : Cilt

CMK : 5271 sayılı Ceza Muhakemesi Kanunu

E. : Esas

E.T. : Son Erişim Tarihi

GVKT: 2016/679 numaralı Genel Veri Koruma Tüzüğü

K. : Karar

Kanun – KVKK : 6698 sayılı Kişisel Verilerin Korunması Kanunu

Konsey: Avrupa Konseyi

Kurum: Kişisel Verileri Koruma Kurumu

Kurul: Kişisel Verileri Koruma Kurulu

m. : Madde

OECD : Ekonomik İşbirliği ve Kalkınma Örgütü

OECD Rehber İlkeleri: Özel Yaşamın Gizliliğinin ve Sınır ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler

par. : Paragraf

S. : Sayı

T. : Tarih

TBK : 6098 sayılı Türk Borçlar Kanunu

TCK : 5237 sayılı Türk Ceza Kanunu

TMK : 4721 sayılı Türk Medeni Kanunu

vb. : Ve Benzeri

vd. : Ve Devamı

Y. : Yıl

GİRİŞ

İnternet, 20. yüzyılda insan yaşamının bir parçası olmuş ve günümüzde, varlığı yaşamın yadsınamaz bir parçası haline gelmiştir[1]. İnternet denilen dijital evrende, internet kullanıcılarının her hareketi veri üretmekte[2] ve kullanıcıların tercihlerini ve bilgilerini içeren bu hareketler yine internet aracılığıyla toplanmaktadır. O kadar ki, günümüz dünyasında, her saniye başı ortalama 2.751.000 e-mail gönderilmekte, 71.000 Google araması gerçekleştirilmekte, 8.300 tweet atılmaktadır. Dünya üzerinde sayısı her geçen gün artmakla birlikte 4.087.463.860 internet kullanıcısı bulunmakta olup, internet kullanıcıları saniye başı ortalama 65,100 GB internet trafiği oluşturmaktadır[3]. Sadece 2012 yılında dünyada 2,8 zettabayt (trilyon gigabayt)'ın üzerinde veri kullanılmıştır[4].

Kişisel verilerin korunması hukuku özelindeki pek çok çalışma da yukarıda ifade edilen istatistiklere benzer istatistik ve sayılarla başlamakta ve kişisel verilerin korunmasının önemi sayılarla ifade edilmeye çalışılmaktadır. Oysa, kişisel verilerin korunmasının önemi, sayı ve istatistiklerin çok ötesinde, kişinin insan olmasından dolayı sahip olduğu temel hak ve özgürlüklerinin korunması ve kişiye meraklı üçüncü gözlere karşı bir koruma sağlanması amacından ileri gelmektedir.

Jean Luc Godard'ın da ifade ettiği gibi ***"artık sadece iletişim araçları var olup iletişimin kendisi yoktur"*** ve bu sözün gerçekliği modern dünyada çok daha fazla hissedilmektedir. Öyle ki, dijital modern dünyada, günün 24 saatinin uyku dışında kalan çok büyük bölümünde, insanlar sosyal medya veya iletişim araçlarını kullanmakta ve yaşamsal faaliyetlerini bir anlamda bu araçlar olmadan sürdürememektedir. Bu doğrultuda, kişilere ait bilgiler, yalnızca internet aracılığıyla değil, farklı pek çok araçla elde edilmekte ve kişiler çoğu zaman, veri toplama faaliyetinin farkında dahi olmamaktadır. Veri üretiminin ve kişilerin verilerinin bu denli artış göstermesinde, insanoğlunun tüketim alışkanlıklarının son yirmi yılda önemli ölçüde değişmesinin de etkisi büyüktür. Nitekim

---

[1] Küzeci, *Kişisel Verilerin Korunması*, s. 35.
[2] Lessig, *Code Version 2.0*, s. 216.
[3] http://www.internetlivestats.com/one-second/ [Erişim Tarihi: 03.12.2018]
[4] Gantz ve Reinsel, *Big Data*, s. 2.

tüketici verilerinin giderek önemli hale geldiği dünyamızda, tüketiciler kendilerine ait bilgilerin üreticisi ve tüketicisi olmaktadırlar[5].

Kişilerin veri üretme alışkanlıkları bir yana, kişilere ait veriler "diğerleri" tarafından da önemsenmekte ve ilgi çekmektedir[6]. Devletler ve şirketler, kişi verileriyle yakından ilgilenmekte, olabildiğince çok veriye sahip olma yarışına girmektedirler[7]. Devletlerin, kişileri denetim ve gözetim altında tutma arzuları, kişisel verileri devletler için önemli kılmaktadır[8]. Şirketler ise faaliyetleri aracılığıyla elde etmiş oldukları kişisel verileri önemli şirket varlıkları olarak görmektedirler[9]. Büyük verinin varlığına uygun sektörler olan sağlık, hizmet, telekomünikasyon, medya ve eğlence sektörlerinde, şirketlerin kişisel veriye olan açlığı çok daha yüksek düzeydedir[10]. Google araştırma direktörü Peter Norvig'in, Google'ın diğer arama motorlarına göre daha başarılı olma sebebini açıklarken kullandığı "*Şirketin daha iyi algoritmaları yok, sadece daha fazla verisi var*[11]." ifadesi de bu durumu doğrular niteliktedir. İyi analiz edilmiş daha fazla verinin, bir şirketin daha başarılı olmasına sebebiyet vermesi durumu, şirketlerin neden kişilerin verilerine sahip olma konusunda iştah ve arzu duydukları sorusunun cevabıdır.

Bu gelişmeler ışığında, kişisel verilerin korunması hukuku ve dijitalleşme karşısında bireyin korunması, son dönemde pek çok ülke, ulusal, uluslararası ve uluslarüstü kuruluş tarafından önemsenmekte ve dikkate alınmaktadır. Avrupa Birliği ise kişisel verilerin korunmasının dünyadaki gardiyanlarından biri olup bu konuda diğer ülkelerde gerçekleştirilen düzenlemelere de yön vermektedir.

29 Eylül 2017 tarihinde Tallin'de gerçekleşen dijitalleşmenin; güvenlik, devlet, sanayi, ekonomi ve toplum üzerindeki etkilerinin görüşüldüğü AB Dijital Zirvesi'nde ise, kişisel verilerin korunmasının yalnızca ilgili kişiyi değil, tüm dünyayı ilgilendirdiği bir kez daha

---

[5] Acquisti, "Personal Data", s. 8.
[6] Küzeci, *Kişisel Verilerin Korunması*, s. 19.
[7] Küzeci, s. 45-54.
[8] Aksoy, *Kişisel Verilerin Korunması*, s. 76.
[9] Karlıdağ, "Ekonomi Politik Açıdan Kisisel Verilerin Korunması", s. 128.
[10] Davenport, *Big Data*, s. 51.
[11] Halevy, Norvig, ve Pereira, "Effectiveness of Data", s. 9.

gözler önüne serilmiştir. AB tarihinde gündemi tamamıyla dijital konulara ayrılmış ilk zirve olma özelliğini taşıyan zirvede, özellikle Genel Veri Koruma Tüzüğü'nün önemi, kripto paraların arkasındaki teknolojinin yani blok zincirlerinin (blockchain) diğer alanlarda nasıl kullanılmaya başlanacağı, siber güvenlik meseleleri, Facebook skandalı[12] gibi güncel ve önemli konular tartışılmış ve AB'nin korumacı ve kişi haklarını öne çıkaran yaklaşımının kıymetli olduğu sonucuna varılmıştır[13].

Dördüncü sanayi devrimi tartışmalarıyla birlikte ekonominin de temelinde yer almaya başlayan ve "yeni petrol" hatta "yeni para birimi" olarak tanımlanan veri konusu, yukarıda da ifade edildiği şekilde, doğrudan insana ait hakların korunmasıyla ilişkilidir. AB'de 1995 tarihli AB Veri Güvenliği Yönergesi ile başlayan kişisel verilerin korunması hususu, aradan geçen yirmi yılı aşkın süre boyunca üye devletlerin en önemli gündem konularından biri olmuş ve bu hukuk dalındaki uyuma yönelik çalışmalar, kolluk ve güvenlik işbirliği, ticaret, sağlık ve telekomünikasyon alanındaki ikincil düzenlemelerle desteklenmiştir. Bu düzenlemelerin temelinde, her zaman insan olmuş ve kişiler, meraklı üçüncü gözlere karşı korunmaya çalışılmıştır.

Dünyada dijitalleşme ve globalleşmenin çarpan etkisiyle artış gösterdiği günümüzde ise kişisel verilerin korunması artık olmazsa olmaz nitelikte bir konudur. Devletler için kişilerin denetim ve gözetim altında tutulması bakımından önemli olan kişisel veriler, özel şirketler için ise finansal anlamda büyük önem arz etmektedir. "Diğerlerinin", kişinin verilerine bu kadar ilgi duyduğu ve bilgi sistemlerindeki gelişmelere bağlı olarak artan bilgi transferinin yoğun olduğu çağımızda, kişisel bilgilerin korunması hususundaki endişelerde de doğal bir artış olmuştur[14]. Veri sorumlularının çevrimiçi gizlilik davranışlarının, topluma yansıttıkları gizlilik yaklaşımlarıyla çelişkili ve tutarsız olması da kişilerin kişisel verileri bakımından çok daha fazla endişe duymasına sebebiyet

---

[12] "Facebook and Cambridge Analytica Scandal".
"https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html"
[Erişim Tarihi: 16.03.2019]

[13] "Tallin Dijital Zirvesi". https://bulten.ikv.org.tr/?ust_id=8122&id=8129 [E.T: 16.03.2019]

[14] Henkoğlu, *Bilgi Güvenliği*, s. 22.

vermiştir[15]. Kişisel verilerin korunması kavramının ve bu verileri koruma fonksiyonunun önemi de tam bu noktada ortaya çıkmaktadır. Kişisel verinin tanımının tam olarak anlaşılması, fonksiyonunun irdelenmesi ve bu hakkın hukuki temellere oturtulması, kişinin temel haklarının "diğerlerine" karşı korunması için önemlidir.

Bu konunun en temelinde yer alan ögelerden biri ise veri sorumlularıdır. Veri sorumluları; veri korumasına ilişkin yapılan ihlallerde, ilgili kişinin muhatap alacağı ve bu sorumluluğun getirdiği sonuçlara katlanmak zorunda kalacak gerçek ve tüzel kişidir. Veri sorumlusu kadar veri işleyen kavramı da büyük önem arz etmekte olup, bu iki kavram arasındaki ayrım ve farklılıklar, doğrudan uygulamayı etkileyecek nitelikte sonuçlar doğurmaktadır[16]. Veri sorumlularının veri işleme ilkelerine ve koşullarına uygun hareket etmesi ile kişisel verilerin korunması mümkün olabilmekte, aksi durumda ciddi ihlaller ve veri sızıntıları ortaya çıkmaktadır.

Ülkemizde ise kişisel verilerin korunmasına ilişkin düzenleme yapma çabalarının 1989 yılında başladığı söylenebilecekse de ilk kanun komisyonu 1995 yılında kurulmuş ve pek çok denemenin ve zamanaşımına uğrayan kanun tasarılarının ardından "6698 sayılı Kişisel Verilerin Korunması Kanunu", 07.04.2016 tarihi itibariyle yürürlüğe girebilmiştir[17].

Pek çok yönden toplumda kişisel verilerin korunmasına duyulan ihtiyacı karşılamış olan Kanun, bazı yönleriyle ise eleştirilmektedir. Özellikle, uygulama bakımından önemli sorunlar ortaya çıkmış olup, son haliyle bu sorun ve belirsizlikler Türk kişisel verilerin korunması hukukuna tabi veri sorumluları açısından zaman zaman çözümsüz durumlara da sebebiyet vermektedir. Bu doğrultuda, veri sorumlularının Kanun kapsamında yapacakları uyum projeleri büyük önem arz etmekte ve gerçekleştirilecek uyum projeleri

---

[15] Trepte ve diğerleri, "Online Privacy Literacy Scale", s. 334; Acquisti ve Gross, "Imagined Communities"; Taddei ve Contena, "Privacy, Trust and Control"; Trepte ve Reinecke, "Social Web as a Shelter"; Tüfekçi, "Online Social Network Sites".

[16] ICO (The Information Commissioner's Office), "Data Controllers and Data Processors", s. 6. "https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf" [E.T: 01.03.2018]

[17] Bozkurt Yüksel, *Bulut Bilişimde Kişisel Verilerin Korunması*, s. 73-74.

ile hem ilgili kişilerin temel hak ve özgürlükleri korunabilmekte hem de veri sorumluları Kanun kapsamında belirlenen caydırıcı nitelikteki yaptırımlardan kendilerini koruyabilmektedirler.

Bu açıklamalar ışığında, tezimiz iki bölümden oluşmaktadır. İlk bölümde, "kişisel veri kavramı, kişisel verilerin korunması hakkı, kişisel verilerin korunmasının fonksiyonu" ve "kişisel verilerin korunması hakkının normatif temelleri" irdelenecek; ikinci bölümde ise tezimizin başlığını oluşturan "Türk hukukunda veri sorumlusu kavramı" tüm yönleriyle değerlendirilmeye çalışılacaktır.

1.BÖLÜM: KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN KORUNMASI HAKKI, KİŞİSEL VERİLERİN KORUNMASININ FONKSİYONU VE KİŞİSEL VERİLERİN KORUNMASI HAKKININ NORMATİF TEMELLERİ

1.1. KİŞİSEL VERİ KAVRAMI

Kişisel verilerin korunmasının temelini, bu ifadenin en önemli ögesi olan kişisel veri kavramı ve bu kavramın tanımı oluşturmaktadır. Kişisel veri kavramı, veri koruma alanına yönelik uluslararası ve ulusal pek çok metinde tanımlanmıştır. Bu metinler incelendiğinde, kişisel verinin anlamı bakımından benzer bir tanımlamaya yer verildiği görülmektedir. Buna göre, en sade haliyle, kişisel veri, "*kimliği belirli ya da belirlenebilir nitelikteki kişiye ilişkin her türlü bilgidir*"[18].

Tanıma ilişkin ayrıntılı bir inceleme yapıldığında, "*kişinin kimliğinin belirli veya belirlenebilir nitelikte olması*" ve "*bilginin kişiye ilişkin bilgiler olması*" kavramları, kişisel veri kavramının temelini oluşturan sacayaklarıdır. Kişisel veri kavramının anlaşılabilmesi için bu kavramların ayrı ayrı irdelenmesi gerekmektedir.

Bu doğrultuda, ilk olarak, bir kişi içinde bulunduğu insan grubunun diğer üyelerinden ayırt edilebiliyorsa, bu kişinin kimliği belirlidir. Kimliği henüz belirlenmemiş olmakla birlikte, makul bir çaba neticesinde tespitin mümkün olduğu durumlarda, bu kişinin kimliğinin belirlenebilir olduğu kabul edilir (***Genel Veri Koruma Tüzüğü, Giriş Bölümü 26. Paragraf***). Başka bir ifadeyle, "*bir kişinin belirlenebilir kılınması, verilerin doğrudan ya da dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi, yani şahsın o şahıs olduğunun ortaya çıkarılabilmesi özelliğini ifade eder*"[19]. Bu yönüyle, kişisel verilerin korunması da yalnızca gerçek kişiler için geçerli bir kavram olacaktır ve tüzel kişiler bu korumanın dışında bulunacaktır[20]

---

[18] Aksoy, *Kişisel Verilerin Korunması*, s. 19.
[19] Dülger, *Verilerin Korunması*, s. 2.
[20] Korff, "New Challenges to EU Data Protection Law", s. 41.

Bir kişinin kimliğinin belirli veya belirlenebilir nitelikte olmasının yanı sıra bir kişinin hangi bilgilerinin kişisel veri olarak kabul edileceği de önemlidir. Bu doğrultuda, kişinin kimlik bilgileri, etnik kökeni, fiziki özellikleri, sağlığına ilişkin bilgileri, öğrenim geçmişi ve iş tecrübesi, yerleşim yerine ilişkin bilgileri, diğer kişilerle kurmuş olduğu iletişim bilgileri, kişinin felsefi düşüncesi ve dini inancı, siyasi veya sendikal faaliyetlerine ilişkin bilgileri, seyahat bilgileri, adli sicil kaydı, parmak izi, cep telefonundan göndermiş olduğu kısa mesajları, sosyal medya aracılığıyla yaptığı paylaşımları, günlük sosyal alışkanlıkları ve hatta IP adresi dahi[21] kişisel veri olarak kabul edilir[22]. Kişinin özel hayatına yönelik bu bilgilerin yanı sıra kişinin ekonomik ya da mesleki yaşama ilişkin bilgileri de kişisel veri kavramına dâhildir[23].

Özetle, yukarıdaki açıklamalar ve GVKT'nin 4. maddesindeki *Tanımlar* başlığı da dikkate alındığında; kişisel veri kavramı, "*özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı bilgileri ya da fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğe özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir gerçek kişiye ait her türlü bilgi*" olarak tanımlanabilir.

Bu noktada ifade etmek gerekir ki, gerek uluslararası düzenlemelerde gerekse Kanun'da bazı kişisel verilere özel bir önem atfedilmiştir. Kanun'da; 'ilgili kişi' olarak tanımlanan kişisel veri sahibini ayrımcılık riski ile karşı karşıya bırakabilecek ilgili kişinin etnik köken, ırk, cinsel hayat, siyasi düşünce, din ve mezhep, sağlık, felsefi inanç, dernek üyeliği, güvenlik, özel aile bilgileri, ceza ve mahkumiyet, biyometrik veri ve diğer inançlara dair bilgileri, **'özel nitelikli kişisel veri'** olarak kabul edilmiştir. Kanun'da, özel nitelikli kişisel veriler ile ilgili olarak yapılan düzenlemeler, bu türdeki veriler için çok daha yüksek düzey işleme ve koruma önlemleri getirmiş bulunmaktadır.

---

[21] Kişisel Verileri Koruma Kurumu, "KVKK Soru Cevap", s. 18; Dülger, *Verilerin Korunması*, s. 4.

[22] Aksoy, *Kişisel Verilerin Korunması*, s. 39; Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, s. 2.

[23] Kuner, *European Data Protection Law*, s. 92.

1.2. KİŞİSEL VERİLERİN KORUNMASI HAKKI, KISA TARİHİ, KORUMANIN FONKSİYONU VE YÖNTEMİ

1.2.1. Kişisel Verilerin Korunması Hakkı

Dünya genelinde kişisel verilerin korunmasına ilişkin düzenlemelerde, "*kişisel verilerin korunması*" kavramı tercih edilmişse de, gerek Kanun'da gerekse diğer düzenlemelerde korunması amaçlanan menfaat verinin kendisi değildir[24]. Kanun'un 1.madddesi incelendiğinde korunması hedeflenen menfaatin, kişinin "*başta özel hayatın gizliliği olmak üzere temel hak ve özgürlükleri*" olduğu anlaşılmaktadır. Kişisel verilerin korunması bir amaç olmaktan çok, kişinin temel hak ve özgürlüklerinin korunmasının tesis edilmesi bakımından kullanılan önemli bir araçtır[25].

Kişisel veriler, günümüzde insan hayatının her noktasında yaygın olarak işlenmektedir. Teknolojik gelişmeler ise veri işleme hususunun giderek artmasına sebep olan en önemli unsurlardan biri olmaktadır[26]. Paylaşımın/İşlemenin yapıldığı araçların kullanımının sıklığı ve verilerin kişisel verinin sahibi olan kişilerin izni olmaksızın paylaşılması, kişisel verinin sahibi olan kişilerin özellikle özel hayatın gizliliği hakkına[27] ve bu bilgiler ile ilgili karar verme özgürlüğüne[28] önemli ölçüde zarar vermektedir. Bu sebepledir ki, kişisel verilerin korunması bağlamında, öncelik ve önem atfedilen temel hak ve özgürlük, özel hayatın gizliliğidir.

Kişisel verilerin korunmasına yönelik ilk uluslararası düzenlemelerde de bu hak, "*özel hayatın gizliliği hakkı*"nın bir parçası olarak değerlendirilmiş ve bu gizliliğin veya verinin kişinin rızası dışında elde edilmesi hali, özel hayatın gizliliğinin ihlali olarak kabul edilmiştir[29]. Yine, kişilik hakkı, konut dokunulmazlığı ve düşünce özgürlüğü de kişisel

---

[24] Çekin, *Kişisel Verilerin Korunması*, s. 19.
[25] Çekin, s. 19.
[26] Mei, "The EC Proposed Data Protection Law", 305; Tan, "Personal Privacy in the Information Age", s. 662.
[27] Gürsel, *İşçinin Kişisel Verileri*, s. 23.
[28] Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, s. 28.
[29] OECD, "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri".

verilerin korunması hakkı ile yakından ilgili olarak değerlendirilebilecek nitelikteki temel hak ve özgürlüklerdir[30]. Bu doğrultuda, kişinin temel hak ve özgürlüklerinin zarar görmemesi ve ihlallerin önlenmesi amacıyla kişisel verilerin korunmasına ilişkin düzenleme yapma gerekliliği ortaya çıkmıştır.

Bu hakkın ortaya çıkışı ve kişisel verilerin korunması hakkının neyi ihtiva ettiğinden önce, kişisel verinin doğuşunu tetikleyen sebebin ve kişisel verinin korunmasında hangi menfaatin korunduğunun tespit edilmesi uygun olacaktır. Doktrinde, genel olarak ikili bir ayrıma gidilmekte ve kişisel verinin korunması, ekonomik bir hak olarak veya insan hakkı olarak incelenmektedir[31].

Ekonomik hak yaklaşımı, Amerikan Hukuku temelli bir yaklaşım olarak ifade edilebilir[32]. Bu yaklaşımın alt başlığında, kişisel verinin, mülkiyet hakkı[33] veya fikri mülkiyet hakkı[34] ile ilişkilendirildiği teoriler bulunduğu gibi bu teorilerin olumsuz yanlarını bertaraf amacıyla kişisel verilerin güven teorisi yaklaşımı veya kıyasen ticari sır hükümlerinin uygulandığı yaklaşım ile tanımlanması ve ilişkilendirilmesi de söz konusu olmuştur[35]. Ekonomik hak yaklaşımı, insan hakları yaklaşımını kıyasen çok daha ekonomi temelli ve insan haklarını gözetmeyen bir yaklaşım olup, bu yaklaşımda insan haklarını korumaktan çok ticari ilişkilerin sağlıklı bir şekilde yürütülmesi, bilgi edinmenin kolaylaşması, işlem maliyetlerinin minimum seviyede tutulması ön plandadır[36]. Küzeci'ye göre "*kişisel verilerin korunmasına ekonomik değeri temel alan yaklaşımda Amerikan Hukuku'nun kendine özgü yapısı da etkili olmakta ve Amerikan Hukuku'nda kişisel verilerin korunması hakkının Anayasal bir hak olarak tanımlanmaması kişisel verilerin korunması hakkını bilgi toplumundan çok bilgi ekonomisi düşüncesine yakın kılmaktadır*"[37].

---

[30] Çekin, *Kişisel Verilerin Korunması*, s. 20.
[31] Küzeci, *Kişisel Verilerin Korunması*, s. 62.
[32] Küzeci, s. 67.
[33] Samuelson, "Privacy as Intellectual Property", s. 1130.
[34] Küzeci, s. 66.
[35] Bygrave, *Data Privacy Law*, s. 120-21.
[36] Bellia, Berman, Frischmann ve Post, *Cyberlaw: Problems of the Information Age*, s. 615-616.
[37] Küzeci, *Kişisel Verilerin Korunması*, s. 63.

Kişisel verilerin korunması hakkı, bireye ait kişisel verilerin sınır konulmaksızın işlenmesinin başka bir ifadeyle kişisel verilerin sınırsız bir şekilde toplanmasının, kullanılmasının, devredilmesinin, saklanmasının yaratacağı tehlikelere karşı bireyi korumayı hedefleyen ve verilerin nasıl kullanılacağı hakkında bireyin karar verme özgürlüğünü garanti altına alan haktır[38] ve bu tanım, Avrupa'da yaygın olan ve kişisel verilerin korunması hakkını insan hakkı olarak tanımlayan yaklaşımın bir ürünüdür[39]. Bu yaklaşımın merkezinde, insan onuru ve kişinin kendisine ait bilgilerin kullanılması ve bu verilerin geleceğini belirleme hakkı bulunmaktadır ve bu yaklaşımdan doğan kişisel verilerin korunması hakkı yaklaşımı ile kişiye veri üzerinde yapılacak işlemler bakımından koruyucu bir hak verilerek bireyin özneden nesneye dönüşmesi engellenmektedir[40].

Tüm bu açıklamalar ışığında, kanımızca kişisel verilerin korunması hakkını "*bir insan hakkı olarak gören ve özel yaşamın gizliliği ile ilişkilendiren yaklaşım*" kişisel verilerin korunmasını tanımlamak bakımından doğru bir yaklaşım ise de yine kanımızca kişinin verilerinin geleceğini belirleme hakkı, ilgili kişinin kendi bilgileri üzerinde sınırsız bir hakkı olduğu anlamına gelmemektedir. Gerekçesi yasal temellere dayandığı sürece kişinin bu temel hakkı ile diğer kişilerin bilgi edinme hakkı arasında veri sahibinin temel hakkına zarar vermeksizin bir denge kurulmalıdır.

Görüşümüzü destekler nitelikte olan ve temelinde kişiyi insan olarak korumak olan, Avrupa Birliği Temel Hak Şartı ve Avrupa Birliği'nin 95/46/EC sayılı direktifi önemli uluslararası düzenlemelerdir[41]. Uluslararası düzenlemelerin yanı sıra ulusal mevzuatta da kişisel verilerin korunması hakkının tanımı bakımından insan hakkı yaklaşımını görmek mümkündür. Bu durum, Türk Anayasası m. 20/3 ve yine Kanun'a da sirayet etmiştir. Öyle ki, kişisel verilerin korunması hakkını düzenleyici nitelikteki işbu temel normatif kaynaklar, kişisel verilerin korunması hakkını ayrıca ve ayrıntılı bir şekilde bir temel

---

[38] Okur, "İşçinin Kişisel Verilerinin Korunması Hakkı", s. 369-70.
[39] Clarke, "Privacy Protection for the 21st Century".
[40] Şimşek, *Kişisel Verilerin Korunması*, s. 112.
[41] Gürsel, *İşçinin Kişisel Verileri*, s. 38.

insan hakkı olarak düzenlemiş bulunmaktadır. Bu yaklaşım yargı kararlarında da yerini almıştır.

Konuya ilişkin Anayasa Mahkemesi ve Yargıtay Kararları incelendiğinde, kişisel verilerin korunmasının kişiler açısından öneminin altı çizildiği görülmektedir. Örneğin , Anayasa Mahkemesi bir kararında[42]: "*Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır.*" ifadesini hükme bağlamış ve kişinin verilerinin korunmasının kişi ve kişinin temel hak ve özgürlükleri bakımından önemi ifade edilmiştir.

Aynı yönde ve örnek niteliğindeki Yargıtay Hukuk Genel kararı[43] da incelendiğinde, bu kararda, "*kişisel verilerin korunması hakkının temel amacının, bireyin özel yaşamının gizliliğinin güvence altına alınması yoluyla kişiyi korumak olduğu*" görüşünün bulunduğu görülecektir. KVKK'nın yürürlüğe girdiği tarihten sonra hükme bağlanan, İstanbul Bölge Adliye Mahkemesi'nin 23. Hukuk Dairesi 2017/596 E. 2017/527 K. ve 31.03.2017 tarihli ve İzmir Bölge Adliye Mahkemesi 12. Hukuk Dairesi 2016/59 E. 2016/68 K. ve

---

[42] Anayasa Mahkemesi'nin 2013/122 E. 2014/74 K. ve 09.04.2014 tarihli kararı (http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/94117278-50ca-4203-88f372a5537258a5?excludeGerekce=False&wordsOnly=False) [Erişim tarihi: 21.02.2019].

[43] "Yargıtay Hukuk Genel Kurulu, 17.06.2015 tarih ve E. 2014/4-56 K. 2015/1679 sayılı kararı" (www.kazanci.com.tr) [E.T: 21.02.2019].

13.10.2016 tarihli kararlarda da bu yaklaşımı görmek mümkündür[44]. Son olarak, Kurul'un kamuoyu ile paylaştığı tüm kararlarında da kişisel verilerin korunması hakkının temel bir insan hakkı olduğuna yönelik yaklaşım söz konusudur[45].

1.2.2. Kişisel Verilerin Korunması Hakkının Kısa Tarihi

Kişisel verilerin korunmasının fonksiyonunun anlaşılabilmesi ve bu korumanın sınırlarının çizilebilmesi bakımından kişisel verilerin korunması hakkının tarihsel gelişimi önemli bir rol oynamaktadır. Kişisel verilerin korunması hakkının tarihsel gelişimi incelendiğinde, bu hakkın özel hayatın gizliliği hakkı ile doğrudan bir ilişkisi ve hiçbir zaman kopmayacak bir bağı olduğu görülmektedir[46].

Özel hayatın gizliliği insanlık tarihinin en başlarından itibaren var olan bir değerdir. Kişisel verilerin korunmasına yönelik ilkelerin, M.Ö. 5. yüzyılda dahi izlerine rastlanabileceğine yönelik görüşler mevcut ise de[47] esasında bilindiği haliyle kişisel verilerin korunması gereksinimi M.S. 20. yüzyılda bilgi işleme teknolojilerinin geliştirilmesiyle ortaya çıkmıştır. 1960 yılından itibaren bilgi bankalarının ortaya çıkması ve teknolojinin gelişmesiyle, bazı kitaplarda büyük birader olarak tanımlanan devletin[48] kişilerin bilgileri üzerinde hakimiyet kurma ve bu bilgileri izleme, gözetleme alışkanlığı ve isteği büyük artış göstermiş ve bu durumun sınırlanması ihtiyacı ortaya çıkmıştır[49].

Bu ihtiyaca yönelik olarak Avrupa'da ulusal düzeyde yapılan ilk düzenleme, Almanya'nın Hessen eyaleti tarafından yapılan Kişisel Verilerin Korunması Kanunu'dur. Bu kanunda, kişiler, yetkisiz üçüncü kişilere karşı korunmakta ve verinin kaderini tayin etme yetkisi ilgili kişiye verilmekte olup bu düzenleme tarihsel bakımdan ilk olma

---

[44] "İstanbul Bölge Adliye Mahkemesi 23. Hukuk Dairesi 2017/596 E. 2017/527 K. ve 31.03.2017 tarihli kararı" (www.lexpera.com.tr) [E.T: 21.02.2019].

[45] "İzmir Bölge Adliye Mahkemesi 12. Hukuk Dairesi 2016/59 E. 2016/68 K. ve 13.10.2016 tarihli kararı" (www.lexpera.com.tr) [E.T: 21.02.2019].

[46] Gürsel, *İşçinin Kişisel Verileri*, s. 37.

[47] Küzeci, *Kişisel Verilerin Korunması*, s. 107.

[48] Aksoy, *Kişisel Verilerin Korunması*, s. 76.

[49] Çekin, *Kişisel Verilerin Korunması*, s. 5.

özelliğine sahiptir[50]. Bu düzenlemeyi takiben, 1973 yılında İsveç'te İsveç Veri Yasası, 1977 yılında Almanya'da "*Federal Veri Koruma Kanunu*", 1978 yılında Fransa'da "*Veri İşleme ve Hürriyetleri Kanunu*" ve Avusturya'da "*Federal Kişisel Verilerin Korunması Kanunu*" yürürlüğe girmiştir. 1970'li yıllarda hazırlanan bu metinlerde, bilgisayar kullanımının başlamasını takiben bu teknolojinin kullanımının bireyler bakımından ortaya çıkartabileceği sorunlara çözüm bulma gayesinin hâkim olduğu söylenebilir[51]. 1980 yılında ise Avrupa Ekonomik Topluluğu'nun hemen hemen tüm üyeleri bu konuda düzenleme yapmış veya bu konuda belirli hazırlıklar yapmış durumdadır. Yine, 1992 yılında İsviçre'de "*Federal Veri Koruma Kanunu*" yürürlüğe girmiştir. 1980 sonrası yapılan düzenlemelerde kişisel verilerin korumasının, bireyin veri işleme sürecinde her aşamaya dahil olduğu ve kendine ait bilgilerin geleceğini belirleme hakkına haiz bulunduğu bir hak olarak algılanmaya başlandığı görülmektedir[52].

1980 yılından itibaren uluslararası düzeyde düzenlemeler de kabul edilmeye başlamış ve bu tarihten itibaren uluslararası düzenlemeler yaygınlaşmıştır. OECD tarafından 1980 yılında kabul edilen "Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafiğinin Korunmasına İlişkin Rehber İlkeler" bu düzenlemelerin ilkidir. Bu düzenlemeyi takiben, Türkiye'nin de tarafı olduğu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Avrupa Konseyi Sözleşmesi)" ve "95/46/EC sayılı Kişisel Verilerin Korunması Yönergesi" yürürlüğe girmiştir. KVKK'da bu düzenlemelerin etkileri yoğunlukla hissedilmektedir.

"97/66/EC sayılı Telekomünikasyon Alanında İşlem ve Koruma Yönergesi", "200/31/EC sayılı E-Ticaret Yönergesi", "2002/58/EC sayılı Elektronik Telekomünikasyon Alanında Kişisel Verilerin Korunması Yönergesi" ve "2016/679 sayılı Genel Veri Koruma Tüzüğü" ise Yönerge'nin yayımlandığı tarihten sonraki süreçte yürürlüğe girmiş olan düzenlemelerdir. Uluslararası düzenlemeler kronolojik olarak incelendiğinde, kağıt üstünde koruma getiren, bireyi ve bireyin bilgilerini korumayan düzenlemelerden[53],

---

[50] Çekin, s. 5.
[51] Küzeci, *Kişisel Verilerin Korunması*, s. 109.
[52] Küzeci, s. 114.
[53] Mayer-Schönberger, *The Virtue of Forgetting*, s. 231.

gelişen teknoloji ve sektörel faaliyetler karşısında bireyin gerçek anlamda korunmaya çalışılması çabasına evrilen bir süreç olduğu görülecektir[54]. Özellikle "95/46/EC sayılı Yönerge"'den, GVKT'ye kadar geçen süreçte, söz konusu uluslararası düzenlemeler kanalıyla, devletin ve şirketlerin, bireylerin, temel hak ve özgürlüklerine saygı göstermeksizin, onların özel yaşamlarına müdahale etme ve onları gözetleme, fişleme, takip etme, profilleme alışkanlıklarına ve arzularına ve bu alışkanlık ve arzuların gelişen teknoloji ile birlikte daha da yaygınlaşmasına karşı, birey gerçek anlamda korunmaya çabalanmış ve bu doğrultuda yapılan düzenlemeler insan toplumunun modern ihtiyaçlarını da karşılayabilecek nitelikte yapılmaya çalışılmıştır.

Türk Hukuku'ndaki duruma bakıldığında ise, bu konunun çok eski bir geçmişi olduğu söylenemez. "5237 sayılı Türk Ceza Kanunu"nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı biçimde işlenmesine yönelik cezai yaptırım ve düzenlemeler mevcutsa da "Türk Ceza Kanunu"nun yürürlüğe girdiği tarihte verilerin işlenmesinde hukuka uygunluk nedenlerine yönelik hiçbir kanuni dayanak bulunmaması sebebiyle bu dönemde kişisel verilerin korunması kavramının Türk Hukuku'nda var olduğunu söylemek kanımızca pek mümkün değildir. 07.05.2010 tarihinde "5982 sayılı Kanun"un 2. maddesi ile "Anayasa"ya eklenen fıkra ile birlikte, kişisel verilerin korunması hakkı bir temel hak olarak tanımlanmış ve Türk Hukuku'nda yerini almıştır. Nisan 2016 tarihinde yürürlüğe giren Kanun ile birlikte kişisel verilerin korunması hakkının yasal dayanağı oluşturulmuş ve daha sonra KVKK'ya bağlı olarak çıkartılan yönetmelik ve tebliğler ile daha da detaylandırılmıştır.

1.2.3. Kişisel Verilerin Korunması Hakkının Fonksiyonu

Daha önce ifade edildiği üzere, kişisel verinin korunması kavramında korunan değer veri değil, bireyin kendisidir[55]. Bu doğrultuda, bireyin kendisinin korunması amacıyla kişisel verilerin korunması hakkı, pek çok uluslararası ve ulusal mevzuatta bir temel hak olarak belirlenmiştir. Tarihsel gelişime bakıldığında ise, bu temel hakkın, pek çok temel hak ile

[54] Mayer-Schönberger, s. 232.
[55] Gürsel, *İşçinin Kişisel Verileri*, s. 37.

iç içe geçtiği ve ortak payda içinde bulunduğu veya bazı temel haklar ve özgürlükler karşısında bu haklarla arasında bir denge kurulmaya çalışıldığı görülmektedir. Halen günümüzde, kişisel verilerin korunması hakkı temel bir hak olarak tanımlanmışsa da işbu temel hakkın diğer temel haklarla olan ilişkisi doktrinde irdelenmekte ve değerlendirilmektedir[56].

Kişisel verilerin korunması hakkı bakımından, ilişkisel olarak en yakın olduğu "*özel yaşamın gizliliği hakkı*" ile ilişkisinin değerlendirilmesi gerekmektedir. Öyle ki, özel hayatın mahremiyetinin sağlanması bakımından kişiye ait verilerin kişi bakımından güvence altına alınması olmazsa olmaz niteliktedir[57]. Tarihsel gelişim içinde, "*kişisel verilerin korunması hakkı*", "*özel hayatın gizliliği hakkı*"ndan ayrılarak, ayrıca düzenlenen bir hak halini almış ve devletlerin ve uluslararası toplumun ilgili yasal metinlerinde yerini almışsa da iki hak alanı arasındaki yakın ilişki her zaman var olmuştur[58]. Ve fakat, "*kişisel verilerin korunması hakkı*", her ne kadar "*özel yaşamın gizliliği hakkı*"na ilişkin temel nitelikleri özünde ihtiva etmekte ise de günümüzde bilişim sistemlerinin ve teknolojinin gelişmesinin de etkisiyle bu haktan ayrılmış ve ayrı bir insan hakkı halini almıştır[59]. Bu bağlamda, "***veri koruma hukukunun ve kişisel verilerin korunmasının temel amacı verilerin hukuka aykırı olarak kaydedilmesini önlemek ve bu veriler üzerinde gerçekleştirilen bütün işlemlerin hukuka uygunluğunu sağlamaktır***"[60].

Bu hak ile korunan değer kişisel verinin sahibi olan bireyler olup[61], bu koruma doğrultusunda kişiler, kişisel verilerinin işlenmesinden dolayı ortaya çıkabilecek zararlara karşı koruma altına alınmakta ve kendi bilgilerinin kaderini tayin etme hususunda hak sahibi konumunda bulunmaktadırlar. Ancak bu noktada ifade edilmelidir ki, "kişisel verilerin korunması hakkı"nın veya "özel yaşamın gizliliği hakkı"nın içeriği

---

[56] Küzeci, *Kişisel Verilerin Korunması*, s. 73.
[57] Gürsel, *İşçinin Kişisel Verileri*, s. 25.
[58] Prins, "Property and Privacy", s. 227-228.
[59] Lawrence, "The Role of Data Protection", s. 810.
[60] Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, s. 47; Okur, "İşçinin Kişisel Verilerinin Korunması Hakkı", s. 369.
[61] Şimşek, *Kişisel Verilerin Korunması*, s. 95; Gürsel, *İşçinin Kişisel Verileri*, s. 37.

ve kapsamı, genel olarak kişilerin korunması amacını taşısa da, bu hakkın kişilere ait bilgilerin elde edilmesinin tümden engellenmesi gibi toptan yasaklayıcı bir amaç gütmediği de aşikârdır[62]. "Avrupa Birliği Temel Haklar Şartı"nın 52/1. hükmünde işbu temel hakka kısıtlama getirilebileceği ifade edilmiştir. Ve fakat, bir kısıtlamanın söz konusu olması için her türlü sınırlama gibi bu sınırlama da kanun tarafından öngörülmeli, hakkın özüne saygı gösterilmeli ve sınırlandırma ölçülülük ilkesi çerçevesinde gerçekleştirilmelidir. Öyle ki, getirilmek istenen sınırlamalar, eğer gerçekten gerekliyse ve kamu menfaatinin amaçlarını karşılıyor ya da diğer bireylerin hak ve özgürlüklerinin korunması ihtiyacına cevap veriyorsa, bu sınırlamalar hukuka uygun olacak ve uygulamaya konulabilecektir[63]. Bazı yazarlara göre ise, bu sınırlamalar ile iki hak arasındaki duvar hızla erimekte ve incelmekte[64] ve bilişim teknolojilerinin gelişimi ve özel yaşamın gizliliği hakkına yaklaşımın her geçen gün değişmesi sebebiyle "*özel yaşamın gizliliğinin sonu mu geliyor?*" sorusu sıklıkla tekrarlanmaktadır[65].

"Özel yaşamın gizliliği hakkı" dışında, "kişisel verilerin korunması hakkı" bazı haklar ile kesişmektedir. Bu bağlamda, "kişisel verilerin korunması hakkı" ile işbu hakların içeriği ve fonksiyonu iç içe geçmektedir. Özel haberleşmenin gizliliği hakkı bu haklardan bir tanesi olup, bu hak ile kişilerin "*telefon, telgraf, mektup, elektronik posta gibi araçlarla gerçekleştirdikleri özel iletişimin gizliliğinin ve güvenilirliğinin korunması*" amaçlanmaktadır[66]. Özel haberleşmenin gizliliği ile birlikte "kişisel verilerin korunması hakkı" açısından daha özel bir perspektiften kısmi bir güvence sağlanmakta olup, bu güvence iletişimin hem izlenmesini hem de dinlenmesini kapsamaktadır[67]. Yine, ayrımcılık yasağı, din ve inanç özgürlüğü, anonimlik hakkı gibi haklar da kişisel verilerin korunması hakkı bakımından kısmi güvenceler sağlamakta veya kişisel verilerin korunması bu haklar bakımından belirli güvenceler getirmektedir[68].

---

[62] Gürsel, *İşçinin Kişisel Verileri*, s. 37.

[63] Avrupa Birliği Adalet Divanı'nın C92/09 ve C93/09 sayılı kararı, "http://curia.europa.eu/juris/liste.jsf?language=en&num=C-92/09" [Erişim Tarihi: 21.02.2019].; Gürsel, s. 39.

[64] Whitaker, *The End of Privacy*.

[65] Küzeci, *Kişisel Verilerin Korunması*, s. 82.

[66] Henkoğlu, *Bilgi Güvenliği*, s. 22-26.

[67] Küzeci, *Kişisel Verilerin Korunması*, s. 101.

[68] Küzeci, s. 104.

Kişisel verilerin korunması hakkının fonksiyonu, zaman zaman belirli temel haklarla iç içe geçmekte ve kendi başına bir temel hak olarak kişiyi ve kişinin bilgilerini, "***meraklı üçüncü gözlere***" karşı koruma ve kişiye bilgisinin geleceğini tayin etme hakkı tanıyor olsa da yukarıda ifade edildiği üzere bu hak sınırsız bir hak değildir. Bu hakkın sınırsız bir hak olarak tanımlanması da mümkün olamayacağı gibi "düşünceyi açıklama özgürlüğü", "bilgi edinme hakkı", "bilim özgürlüğü" gibi temel hak ve özgürlüklerin varlığı karşısında "kişisel verilerin korunması hakkı" ile diğer Anayasal haklar arasında bir dengenin kurulması zaruridir. Bu denge kurulurken, hassas bir terazinin iki kefesi gibi, haklar ayrı kefelere konularak bir denge testi gerçekleştirilmeli ve ne "kişisel verilerin korunması hakkı" diğer Anayasal hakları işlevsiz kılmalı[69] ne de terazi kefesinin diğer tarafındaki temel haklar aracılığıyla kişisel verinin sahibi ilgili kişinin temel hak ve özgürlükleri ihlal edilmelidir[70].

1.3. KİŞİSEL VERİLERİNİN KORUNMASININ NORMATİF TEMELLERİ

Kişisel verilerin korunması ihtiyacının ortaya çıkması ve bu ihtiyacın toplumlarda yaygın hale gelmesi ile birlikte, kişisel verilerin korunması hakkını korumaya yönelik ulusal ve uluslararası yasal düzenlemeler ortaya çıkmıştır. Yukarıda ifade edildiği üzere, kişisel verilerin korunması hakkının temeli tarihsel olarak çok eskilere dayanmakta ise de kişisel verilerin teknolojik gelişmelerle olan ilişkisinin değişmesi ve bu doğrultuda bireyin daha korunmasız hale gelmesiyle, ilgili yasal düzenlemeler artmış ve yeni çağın petrolü konumundaki verinin korunması amacıyla ulusal ve uluslararası düzenlemeler özellikle son on yıllık süreçte önemli bir artış göstermiştir. Bu bölümde, kişisel verilerin korunması hakkına yönelik önemli nitelikteki düzenlemelere değinilecektir.

---

[69] Küzeci, s. 99.

[70] Tortop, "İletişim ve Bilgi Edinme Hakkı", s. 36.

1.3.1. Uluslararası Düzenlemeler

1.3.1.1. Ekonomik İşbirliği ve Kalkınma Örgütü İlkeleri

"Ekonomik İşbirliği ve Kalkınma Örgütü" (OECD), kişiye ait verilerin korunmasını milletlerarası bir konu olarak ilk kez ele alan kuruluştur. 1961 yılında kurulan ve ekonomik büyümeyi desteklemek, iş alanlarını arttırmak, yaşam standartlarını yükseltmek, finansal dengeyi korumak, başka devletlerin ekonomik gelişimine yardımcı olmak, global ticaretin büyümesi yönünde çalışmalar yapmak gibi[71] amaçlar taşıyan kuruluş, 1980'de yayınlanan "*Özel Yaşamın Gizliliğinin ve Sınır ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler*" ile kişisel verilerin korunmasının ekonomik boyutunun önemini ortaya konmuştur. Söz konusu ilkeler, kişisel verilerin korunması hususunda tüm dünyaya rehberlik etmiş ve dünyadaki düzenlemelerin içeriklerini önemli ölçüde etkilemiştir.

1.3.1.2. Avrupa Konseyi Tavsiye Kararları

Veri işlemenin çeşitlenmesi ve bu konuda gelişmelerin ivme kazanmasını takiben Avrupa Konseyi, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek için belirli ilke ve kurallardan oluşan bir çerçeve oluşturmaya başlamış ve bu kapsamda önemli düzenlemeler yapmıştır. Konsey, 1973 ve1974 yıllarında kabul ettiği iki Tavsiye Kararı ile, kişisel verilerin korunması bakımından gerek özel sektörde ("Özel Sektördeki Elektronik Veri Bankaları Karşısında Kişilerin Durumu") gerekse kamuda ("Kamu Sektöründeki Elektronik Veri Bankaları Karşısında Kişilerin Durumu") dikkate alınması gerekli ilkelerin çerçevesini ve bu sektörlerde veri işlemenin sınırlarını belirlemiştir.

---

[71] Küzeci, *Kişisel Verilerin Korunması*, s. 118.

1.3.1.3. Avrupa İnsan Hakları Sözleşmesi

Kişilere ait verilerin korunması alanında, 1950 tarihinde imzaya açılan ve insan hakları bakımından önemli bir belge de "Avrupa İnsan Hakları Sözleşmesi" (AİHS)'dir. "Kişisel verilerin korunması hakkı" AİHS'de ayrı bir hak olarak öngörülmemekle birlikte, AİHS m. 8 incelendiğinde kişisel verilerin korunması ile doğrudan ilintili olan özel yaşamın gizliliği hakkının açıkça düzenlendiği ve özel yaşamın yanı sıra aile yaşamı, ev ve haberleşme alanları da bu düzenleme ile koruma kapsamında yer almaktadır. AİHS, bu yönüyle önemli bir uluslararası belgedir.

AİHS'de ayrıca düzenlenmiş olan bir hak olmamasına rağmen, AİHM 1980'li yılların ortalarından itibaren pek çok kararında kişisel verilerin korunması hakkını AİHS'nin kapsamına sokmaktadır[72]. Öyle ki, AİHM kişisel özerkliği ve bilgilerin akıbetini belirleme hakkı, AİHS m. 8'de düzenlenen güvencelerin yorumlanmasında temel bir ilke olarak belirlemektedir. Söz konusu kararlarda, *"kişisel verilerinin kullanımı ve kaydı"* bakımından kişilerin denetim hakkına sahip olduğu vurgulanmaktadır[73].

1.3.1.4. 108 Sayılı Sözleşme ve Sözleşmeye Bağlı Olarak Alınan Tavsiye Kararları

Avrupa Konseyi'nin düzenlemeleri arasında bulunan 108 sayılı ***"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşme***"nin ayrı bir yere konulması gerekmektedir. "108 sayılı Sözleşme", Avrupa Konseyi'ne ait kişisel verilerin korumasına ilişkin üye devletlerin imzasına açılan ilk uluslararası nitelikteki düzenlemedir. OECD Rehber İlkeleri'nin aksine taraf devletler için bağlayıcı nitelik taşıyan 108 sayılı Sözleşme'de "kişisel verilerin otomatik sistemler vasıtasıyla işlenmesine karşı kişilerin haklarının korunarak veri korumasının güçlendirilmesi" amaçlanmaktadır[74].

---

[72] Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, s. 19.
[73] Cengiz, "Yaşam Hakkı", s. 401.
[74] Gürsel, *İşçinin Kişisel Verileri*, s. 86.

108 sayılı Sözleşme bağlayıcı nitelikte olmasına karşın, uygulamada taraf devletlerin farklı nitelik ve ölçüde yasal düzenlemeler yapmaları sebebiyle taraf ülkelerin ortak bir hukuk yaratmalarını sağlayamamıştır[75]. Bu sebeple, Avrupa Konseyi 108 sayılı Sözleşme'de öngörülen kişisel verilerin korunmasına yönelik tedbirlerin çeşitli alanlarda hayata geçirilmesi amacıyla toplamda on üç adet Tavsiye Kararını yürürlüğe koymuştur. "23 Nisan 1999 tarihli ve (1999) 5 sayılı İnternette Özel Hayatın Korunması Hakkında Tavsiye Kararı", "13 Nisan 1997 tarihli ve (1997) 5 sayılı Sağlık Verilerinin Korunması Hakkında Tavsiye Kararı", "9 Eylül 1991 tarihli ve (1986) 1 sayılı Sosyal Güvenlik Amacıyla Kullanılan Kişisel Verilerin Korunması Hakkında Tavsiye Kararı" ve "18 Ocak 1989 tarihli ve (1989) 2 sayılı İstihdam Amacıyla Kullanılan Kişisel Verilerin Korunması Hakkında Tavsiye Kararı" bu Tavsiye Kararları kapsamında verilebilecek en önemli örneklerdir. Bu Tavsiye Kararları ile birlikte, kişisel verilerin korunmasına ilişkin olarak, ulusal mevzuatlara katkı sağlayacak uygun ölçütler belirlenmiş ve bu ölçütler, AB tarafından düzenlenecek yönergelere ışık tutmuştur[76].

1.3.1.5. İnsan Hakları Evrensel Beyannamesi ve Birleşmiş Milletler Genel Kurulu İlkeleri

Birleşmiş Milletler bünyesinde oluşturulan uluslararası nitelikte metin ve ilkeler de kişisel verilerin korunması hakkının temelinin dayandığı düzenlemelerdendir. Bu doğrultuda "1948 tarihli BM İnsan Hakları Evrensel Beyannamesi", insan haklarının korunması açısından uluslararası bir standart belirlenmesine yönelik atılan en önemli adımlardan biri olup tıpkı "Avrupa İnsan Hakları Sözleşmesi"nde olduğu gibi "kişisel verilerin korunması hakkı" BM tarafından ilk olarak "özel yaşamın gizliliği hakkı" ile bağlı bir şekilde düzenlenmiştir. Yaygın olarak kabul gören söz konusu belgenin 12. maddesinde özel yaşamın gizliliği hakkı düzenlenmiştir.

---

[75] Aksoy, *Kişisel Verilerin Korunması*, s. 8.

[76] Gürsel, *İşçinin Kişisel Verileri*, s. 87.

Öte yandan BM tarafından kabul edilen genel nitelikli bu düzenlemeye ek olarak, konusu kişisel verilerin korunması olan bazı düzenlemeler de bulunmaktadır. Bu düzenlemelerden en önemlisi, "BM Genel Kurulu"nun 1990 tarihli "*Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler*" adını taşıyan belgedir. Bu ilkelerin amacı üye ülkeleri kişisel verileri korumaya yönelik yasal düzenlemeler yapmaya teşvik etmek ve uluslararası kuruluşların kişisel verilerini bu rehber ilkeler doğrultusunda işlemeye yönlendirmektir. Ayrıca, bu düzenleme ile birlikte kişisel verilerin korunması hakkı kapsamında bir denetim mekanizması oluşturulmuştur ve ilk olması sebebiyle önemlidir[77].

1.3.1.6. Avrupa Birliği Temel Haklar Şartı

"*AB Temel Haklar Şartı*" ile ilk kez Avrupa vatandaşlarının bireysel, siyasal ve ekonomik haklarının tamamı tek bir metinde bir araya getirilmiş ve bu belge, bazı değişikliklerle 2004 yılında "AB Anayasası"nın ikinci bölümüne eklenmiştir[78]. Şart'ın, "kişisel verilerin korunması hakkı" bakımından önemli olmasının sebebi, "kişisel verilerin korunması hakkı"nın ilk kez bir temel haklar belgesinde, özel hayatın gizliliğinden ayrı bir hak olarak açıkça düzenlenmiş olmasıdır[79]. "AB Temel Haklar Şartı"nda "kişisel verilerin korunması hakkı"nın "özel yaşamın gizliliği hakkı"ndan ayrı olarak öngörülmesi, ulusal hukuk sistemlerinde yapılacak yeni düzenlemelere de örnek oluşturmaktadır. Nitekim "kişisel verilerin korunması hakkı", "özel yaşamın gizliliği hakkı"nın kapsamı içerisinde değerlendirilemeyecek bazı hususları da kapsamakta ve koruma altına almaktadır[80].

---

[77] Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, s. 21.
[78] Küzeci, *Kişisel Verilerin Korunması*, s. 159.
[79] Avrupa Birliği Temel Haklar Şartı, m. 8.
[80] Küzeci, *Kişisel Verilerin Korunması*, s. 162.

1.3.1.7. 95/46/EC Sayılı Avrupa Parlamentosu ve Konseyi Yönergesi

"Kişisel verilerin korunması hakkı"nın normatif temellerinden biri de "*Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin 24 Ekim 1995 Tarihli ve 95/46/EC Sayılı Avrupa Parlamentosu ve Konseyi Yönergesi*"dir. AB üyesi ülkelerinin sınırlarını aşan ve kişisel verilerin korunması bakımından etkisi büyük olan bu Yönerge'nin amacı, üye devletler arasındaki kişisel verilerin korunmasına yönelik çeşitliliğe son verilmesidir[81]. Öyle ki, 108 sayılı Sözleşme ve OECD Rehber İlkeleri doğrultusunda düzenlenen kişisel verilerin korunması hususunda ulusların düzenlemelerinde ciddi farklılıklar ortaya çıkmış[82], AB üyesi ülkelerin yasal mevzuatlarının uyumlaştırılması zorunlu bir hal almıştır. Bu doğrultuda, Yönerge'nin 1. maddesi gereğince hem bireylerin temel hakkı niteliğindeki kişisel verilerinin korunması, hem de bu verilerin üye devletler arasında serbest dolaşımının sağlanması amaçlanmıştır[83]. Yönerge ile işlenme şartları önceden belirlenerek önleyici nitelikte bir koruma sağlanmaktadır[84]. Bu yöntem ile kişisel verilere yönelik gerçekleşebilecek ihlallere karşı önceden sistemli bir koruma getirilmekte olup, Yönerge bu özelliği ile de kişisel verilerin korunması açısından önem arz etmektedir. Yine, Avrupa Konseyi Sözleşmesi'nin tarafı olan devletlerin Yönerge'de yer alan ilkeleri iç hukuklarının bir parçası haline getirme zorunluluklarının bulunması ile birlikte, kişisel verilerin korunması bakımından farklı ulusal yasaların tek bir iç Pazar oluşumunu engelleme tehlikesini önlemek de amaçlanmış[85] ve Yönerge ile AB içerisinde doğan uyumlaştırma ihtiyacı giderilmeye çalışılmıştır[86].

Yönerge kapsamında, kişisel verilerin sınırlı amaçlar doğrultusunda ve bu amaçlarla sınırlı ve orantılı olarak, açık, belirli ve meşru sebepler için işlenebileceği düzenlenmiş; aydınlatma yükümlülüğü veri sorumlularına yüklenerek, verilerin korunması bakımından gerekli teknik ve işlevsel tedbirlerin alınması gerekliliği öngörülmüş ve otoriteler

---

[81] Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, s. 25.
[82] Uncular, s. 39.
[83] Manav, "İşçinin Kişisel Verilerinin Korunması", s. 98.
[84] Uygun, "Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması", s. 35.
[85] Küzeci, *Kişisel Verilerin Korunması*, s. 167.
[86] Mayer-Schönberger, *The Virtue of Forgetting*, s. 220.

aracılığıyla veri işleme faaliyetlerinin denetlenmesi gerekliliği ifade edilmiştir[87]. Bu bağlamda, Yönerge ışığında öngörülen temel prensipler, meşruluk, amaca uygunluk, şeffaflık, orantılılık ve gereklilik, güvenlik ve denetim olarak ifade edilebilecektir. Bu düzenlemenin veri sorumlularını zorlayıcı nitelikte yaptırım ve denetimler öngörmesi sebebiyle, Yönerge büyük önem arz etmekte olup, Yönerge'nin ilgili kişiyi koruması ve aynı zamanda kişisel verilerin Avrupa Birliği içerisinde özgürce dolaşmasını sağlayıcı nitelikte olması sebebiyle bu normatif kaynak önem arz etmektedir[88].

Yönerge, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun gerek yapımı sürecinde gerekse yürürlüğe girmesinden sonra yapılan yargılama süreçleri kapsamında kullanılmış olup, özellikle KVKK'nın hazırlanması aşamasında Yönerge büyük oranda örnek alınan düzenleme olmuştur. Yönerge, Türk hukukunun yanı sıra ABAD'ın pek çok kararına da konu olmuş olup verilen bu kararlar bir sonraki bölümde incelenecek olan Genel Veri Koruma Tüzüğü (GVKT)'ndeki düzenlemelere ışık tutmuş ve bu düzenlemelerin GVKT içinde bulunmasına ön ayak olmuştur. Bu hususta verilebilecek en güzel örnek, ABAD'ın Yönerge'deki düzenlemeleri de dikkate alarak 13 Mayıs 2014 tarihinde vermiş olduğu *Google* kararıdır[89]. Bu karar ile birlikte, unutulma hakkı ilk kez gündeme gelmiş ve ilerleyen süreçte de kanuni bir düzenleme halini alarak GVKT'deki yerini almıştır.

Yönerge, AB Hukuku sistematiğinde, yönerge niteliğinde bulunması sebebiyle doğrudan uygulanabilir nitelikte[90] olmaması sebebiyle üye ülkelerin iç hukuklarına geçiş sağlanırken zaman zaman bu konuda sıkıntılar yaşanmış ve AB ülkeleri içinde yeknesak bir veri koruma politikasının oluşturulması amacı tam anlamıyla ve istenen seviyede karşılanamamıştır[91]. Bu durum, zaman zaman problemlere sebebiyet vermiştir[92]. Bu doğrultuda, Genel Veri Koruma Tüzüğü yürürlüğe girmiş olup Tüzük sayesinde yeknesak veri politikası probleminin üstesinden gelinmeye çalışılmıştır.

---

[87] Kuner, *European Data Protection Law*, s. 140.
[88] Dülger, *Verilerin Korunması*, s. 59.
[89] Yavuz, *Unutulma Hakkı*, s. 69-83.
[90] "Regulations, Directives and other acts". https://europa.eu/european-union/eu-law/legal-acts_en [Erişim Tarihi: 16.03.2019]
[91] Küzeci, *Kişisel Verilerin Korunması*, s. 200.
[92] Ercan ve Bostanoğlu, "Veri Güvenliği Ekosisteminde Türkiye", s. 3.

1.3.1.8. Genel Veri Koruma Tüzüğü "GVKT" (Genaral Data Protection Regulation "GDPR")

AB özel hukuku kapsamında kişisel verilerin korunmasının gelişimine bakıldığında ve yukarıda ifade edilen düzenlemeler de dikkate alındığında, Avrupa Birliği'nde bu konuda derin bir kültürel değer birikiminin ve anlayışının bulunduğu görülmektedir. Ve fakat, özellikle "*95/46/EC Sayılı Avrupa Parlamentosu ve Konseyi Yönergesi*"nin yürürlüğe girmiş olduğu 24 Ekim 1995 tarihinden sonra ekonomik ve teknolojik gelişmeler hız kazanmış ve verinin kullanım oranı, miktarı ve toplumdaki rolü de tıpkı ekonomi ve teknoloji gibi hızla değişmiştir.

Bu değişim, kişisel verilerin korunmasına dair düzenlemelerin güncellenmesi ihtiyacını doğurmuştur. Söz konusu güncelleme, Veri Koruma Reformu olarak adlandırılmış olup söz konusu reform, dijital çağda kişilerin temel hak ve özgürlüklerinin güçlendirilmesi ve getirilen kurallarla Avrupa Dijital Pazarı'ndaki şirketlerin işlerini kolaylaştırmak için çok önemli bir adımdır[93]. Ayrıca, Yönerge'nin AB'ye üye ülkeler arasında yeknesak biçimde uygulanmaması ve farklı uygulamalara sebebiyet vermesi de GVKT'nin hazırlanmasındaki en büyük etkenlerden biri olmuştur[94]. Öyle ki, özellikle "Schrems Kararı"[95] ve "İrlanda Dijital Haklar Kararı"[96] gibi kararlar, Yönerge ve Yönerge'nin eki niteliğinde yapılmış olan düzenlemelerin, AB toplumu için artık yeterli olmadığını ve Avrupa'da bireylerin kişisel verilerine ilişkin hakları açısından endişe duyulmaya başlandığını ortaya koymaktadır[97].

---

[93] "Data Protection Reform". "http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm" [Erişim Tarihi: 16.03.2019]

[94] Lambert, *New European Data Protection Rules*, s. 89-94.

[95] Dülger, *Verilerin Korunması*, s. 64.

[96] Dülger, s. 64.

[97] Dülger, s. 64.

Bu gelişmeler neticesinde, Avrupa Parlemontosu tarafından 24 Mayıs 2016 tarihinde, iki yıllık bir geçiş süresi de öngörülerek, Genel Veri Koruma Tüzüğü onaylanarak yürürlüğe girmiştir[98]. Söz konusu düzenlemenin Tüzük olarak yürürlüğe girmesi ile birlikte ve Tüzük'ün doğrudan uygulanabilir olma özelliğinden de faydalanılmak suretiyle, Avrupa Birliği üye ülkelerinin Tüzük ile tamamen uyumlu hale gelmesi, Tüzük ile aykırı düzenlemelere gitmemesi amaçlanmıştır. Böylece, veri koruma politikası üye ülkeler arasında yeknesak bir şekilde uygulanabilecek ve böylece daha çok hukuki belirlilik getirilecek ve kişisel verilerin serbestçe aktarılması konusundaki olası problemler ve engeller ortadan kaldırılabilecektir[99].

GVKT aracılığıyla, Yönerge'de bulunmayan değişiklikler ve kavramlar getirilmiş ve esaslı yenilikler yürürlüğe girerek Avrupa'da veri koruma alanında adeta yeni bir çağ başlatılmıştır. Kısaca ifade etmek gerekirse;

- GVKT ile düzenlemenin uygulanabilirliğinin sınırı coğrafi olarak arttırılmış ve GVKT hükümleri Avrupa Birliği dışındaki ülkelere de uygulanabilir hale gelmiştir. Bu perspektiften bakıldığında, GVKT'nin bulaşıcı bir hastalık olarak tanımlanabilmesi ve bu hastalığın tüm dünyaya yayılmasının muhtemel bir senaryo olduğu söylenebilir[100].

- GVKT ile getirilen diğer önemli bir değişiklik de getirilen hükümlerin ihlal edilmesi halinde öngörülen yaptırımlardır. Özellikle idari para cezaları yönünden incelendiğinde, üye ülkelerin kişisel veri koruma otoritelerine, veri sorumlularına ilişkin yapacakları ve belirli kriterlere dayanan soruşturmalar sonrasında veri sorumlularını bu konuda çalışma yapmaya zorlayıcı nitelikte büyük idari para cezaları kesilebileceğine yönelik düzenlemenin bulunduğu görülmektedir[101]. Öyle ki; GVKT düzenlemesi kapsamında, veri sorumlularının ihlal

[98] Dülger, s. 65.
[99] Voigt ve Von Dem Bussche, *GDPR*, s. 2-3.
[100] Kiss ve Szoke, "New Generation of Data Protection Regulation", s. 322.
[101] Fritsch, "Data Processing in Employment Relations", s. 164.

gerçekleştirmeleri halinde, yıllık gelirlerinin yüzde 4'ü veya 20.000.000 Avro (hangisi daha yüksek ise) para cezası ile karşılaşma ihtimalleri bulunmaktadır. Bu düzenleme ışığında, üye ülkelerin veri koruma otoriteleri tarafından bazı veri sorumlularına önemli büyüklükte idari para cezası uygulamaları gerçekleştirilmiştir. Bu cezaların en dikkat çekici olanlarından biri CNIL tarafından Google'a uygulanan cezadır. 21 Ocak 2019 tarihinde, Fransız Veri Koruma Kurumu CNIL, Google'a kişisel reklamlar hususunda yeterli aydınlatma ve bilgilendirmenin yapılmaması ve gizliliğin ihlali gerekçeleriyle GDPR kapsamında 50 milyon Euro para cezası uygulamıştır[102].

- Tüzük aracılığıyla, veri sahibinden alınması gereken rızanın yeniden tanımlanması ve bu tanımın rıza kavramı bakımından önemli değişiklikler içermesi ve yine aydınlatma yükümlülüğü bakımından getirilen değişiklikler GVKT'nin Yönerge karşısındaki durumu bakımından önemlidir.

- GVKT kapsamında yapılan temel değişiklikler arasında, ihlal bildirimi bakımından yapılan düzenlemeler; erişim hakkı bakımından ilgili kişiye verilen kapsamlı haklar; unutulma hakkı; veri taşınabilirliği; tasarımdan itibaren veri mahremiyeti (privacy by design)[103]; veri sorumluları ve veri işleyenler bakımından veri koruma görevlileri bulundurma zorunluğu gibi yeni kavram ve görüşler de sayılabilir. Getirilen bu yeni kavramlar ile, Avrupa toplumunda uygulamada doğan ihtiyaçlar karşılanmaya çalışılmış ve günün gelişen ve değişen ihtiyaçlarına çözüm getirilmeye çalışılmıştır.

GVKT'nin günümüzde her geçen gün etki alanı genişlemektedir[104]. Bu doğrultuda, GVKT çok yakın bir dönemde yürürlüğe girmişse de bu normatif kaynağın halen toplumun bazı ihtiyaçlarına çözüm sağlayamadığı da ifade edilmelidir. Öyle ki, bizim de

---

[102] Kararın ayrıntısı için bakınız: "https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc" [Erişim Tarihi: 16.03.2019]

[103] Cavoukian, "Privacy by Design".

[104] Örneğin, 1 Şubat 2019 tarihinde yürürlüğe giren AB-Japonya Ekonomik Ortaklık Anlaşması (EOA) ile taraflar önemli bir ticari ortaklık kurdukları gibi, 635 milyon kişiyi kapsayan bu anlaşma ile dünyanın en geniş güvenli veri akışı alanı oluşmuştur. Ayrıntılı bilgi için bakınız: "http://europa.eu/rapid/press-release_IP-19-785_en.htm" [Erişim Tarihi: 17.03.2019]

katıldığımız bir görüşe göre, GVKT, toplumda var olan blockchain teknolojisi, insansız araçlar ve sürücüsüz otomobiller gibi teknolojiler aracılığıyla toplanan kişisel verilerin korunması bakımından herhangi bir düzenleme öngörmemekte olup, bu yönden bireyin ve bireyin verilerinin korunması ihtiyacı bulunduğu söylenebilir.

1.3.2. Ulusal Düzenlemeler

1.3.2.1. Anayasa

"Kişisel verilerin korunması hakkı", Anayasa'nın "Özel Hayatın Gizliliği" başlığı altında ve "özel hayatın gizliliği hakkı" ile düzenlenmiş bulunmaktadır. 12.09.2010 tarihli ve "5982 sayılı Türkiye Cumhuriyeti Anayasası'nın Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun"un 2. maddesi ile "Özel Hayatın Gizliliği" bölümüne eklenen fıkrayla birlikte "kişisel verilerin korunması hakkı" Anayasal bir hak kimliğine bürünmüştür. Bu düzenlemeye göre; "*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. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*".

Anlaşılacağı üzere, ilgili değişiklik sonucunda "kişisel verilerin korunması hakkı" Anayasa'da açıkça düzenlenmiş ve anayasal güvence ile koruma altına alınmış olmaktadır. Bu düzenleme ile kişisel verilerin korunması hakkı genel bir çerçevede belirlenmiş, bu hakka ilişkin düzenlemelerin kanunla yapılacağı ifade edilerek kişilerin kişisel verileri üçüncü kişilere ve bu kişilerin keyfi müdahalelerine karşı koruma altına alınmıştır[105]. Bu bilgiler ışığında, kişisel verilerin korunmasının Anayasa'da temel bir insan hakkı olarak yer alması, Anayasa'yı kişisel verilerin korunması hakkı bakımından önemli bir normatif kaynak haline getirdiği söylenebilecektir.

---

[105] Dülger, *Verilerin Korunması*, s. 70.

1.3.2.2. Türk Medeni Kanunu

Kişisel verilerin korunması açısından, Türk Medeni Kanunu (TMK)'nun m. 23-25 düzenlemeleri önem arz etmekte olup, bu düzenlemeler kişiliğin korunmasına ilişkin hükümler içermektedir. Bu hükümler, doğrudan kişisel verilerin korunmasına yönelik hükümler içermese de "kişisel verilerin korunması hakkı" ile olan doğrudan bağlantısı nispetiyle önemlidir.

TMK'nın 24. maddesinde, "*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.*" düzenlemesi vardır. Yine, TMK 25. maddeye göre, kişilik hakları hukuka aykırı şekilde saldırıya uğrayan kişi hukuki yollara başvurabilmektedir.

1.3.2.3. Türk Ceza Kanunu

"Kişisel verilerin korunması hakkı"na ilişkin olarak, "5237 sayılı Türk Ceza Kanunu"nun (TCK) "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığının dokuzuncu bölümünde bazı cezai hüküm ve düzenlemeler bulunmaktadır. TCK m.132'de "haberleşmenin gizliliğinin ihlali", TCK m.135-138 hükümlerinde "kişisel verilerin hukuka aykırı olarak kaydedilmesi, başkasına verilmesi, yayılması veya ele geçirilmesi ve yok etme yükümlülüğünün yerine getirilmemesi" hallerine ilişkin cezai sorumluluk düzenlenmiştir. Kişisel verilere ilişkin düzenlenen bu suçlar şikâyete bağlı suçlar olup, kişisel verilerin korunmasının TCK aracılığıyla düzenlenmesi ve bu konuda cezai yaptırımların belirlenmesi önem arz etmektedir.

1.3.2.4. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Yukarıda da ifade edildiği üzere, bilişim dünyasındaki gelişmelere paralel olarak, ülkemizdeki veri işleme faaliyetleri de hız kazanmış ve kolaylaşmıştır. Bu denetimden uzak ve kontrolsüz veri akışı, veri işleme sürecinde kişisel verilerin korunması açısından büyük bir güvenlik zafiyetine sebep olmuştur. Özellikle, kişisel verilerin en başta temel bir insan hakkı olarak korunması zorunluluğu, e-ticaret ve diğer ekonomik etkinlik ve eylemde ülkemizin geride kalmaması gerekliliği ve ekonomi dışındaki sektör ve alanlarda da kişisel verilerin korunmasına duyulan ihtiyaç ile birlikte, Türkiye'de kişisel verilerin korunmasına yönelik olarak kapsayıcı ve dağınık olmayan bir kanuni düzenleme yapılması zorunlu hale gelmiştir[106]. Yine, kişisel verilerin korunmasındaki eksiklik sebebiyle AB üye devletleri arasında bilgi akışında da sıkıntı doğmuş[107] olup bu hususta düzenleme yapma zorunluluğu ülkemizin AB üyelik süreci bakımından da bir gerekliliktir[108].

Bu doğrultuda, ülkemizde kişisel verilerin korunmasına ilişkin düzenleme yapma çabalarının 1989 yılında başladığı söylenebilir. Ancak, ilk kanun komisyonu 1995 yılında kurulmuş olup 2000'li yılların başından itibaren ise belirli dönem aralıklarıyla farklı komisyonlar tarafından farklı yasa tasarıları TBMM'ye sevk edilmiş; ancak bu çabalar defalarca sekteye uğramış ve pek çok denemenin ve zamanaşımına uğrayan kanun tasarılarının ardından "6698 sayılı Kişisel Verilerin Korunması Kanunu", 07.04.2016 tarihi itibariyle yürürlüğe girmiştir [109].

Pek çok yönden toplumda kişisel verilerin korunmasına duyulan ihtiyacı karşılamış olan Kanun, bazı yönleriyle ise eleştirilmiştir. Önemli olarak ifade edilebilecek ilk eleştiri, Kanun'un büyük ölçüde Yönerge'den faydalanılarak oluşturulması ve bu yapılırken Yönerge'de bilinçli olarak boşluk bırakılan, uygulamasını ve içeriğini üye devletlerin

---

[106] Küzeci, *Kişisel Verilerin Korunması*, s. 308.
[107] Kişisel Verilerin Korunması Kanunu, Genel Gerekçe, s. 6.
[108] Küzeci, *Kişisel Verilerin Korunması*, 308.
[109] Başalp, *Kişisel Verilerin Korunması*, s. 107-108; Küzeci, *Kişisel Verilerin Korunması*, s. 311-312.

doldurması beklenen noktalarda yasal bir düzenleme yapılmamasıdır[110]. Bu açıdan, konunun içtihatlar ve Kişisel Verileri Koruma Kurulu'nun kararları ile doldurulabileceği ifade edilmişse de en azından içtihatlar yönünden bu durumun çok hızlı ilerlemediği ve ülkemizde Kanun kapsamında henüz yeterli sayıda içtihadın oluşmadığı söylenebilecektir.

Bir diğer eleştiri ise, Kanun'un alt başlığında farklı sektörler bakımından düzenleme yapılması ihtiyacı var ise de Kanun'un ne içeriğinde ne de gerekçesinde böyle bir düzenleme yapılmamış olmasıdır[111]. Bu eleştiri haklı bir eleştiri olup, özellikle iş hukuku ilişkileri bakımından veya diğer pek çok sektörde kişisel verilerin korunması hukukunun sektörel bazdaki ihtiyaçlara ve gerçeklere cevap verecek şekilde düzenlenmesi ve ilgili kişi ile veri sorumlusu arasındaki menfaat dengesi ve hukuki dengenin, hukuki temele oturtulması faydalı olacaktır.

Son olarak, Kanun'da, Tüzük'te ve Avrupa'daki pek çok ulusal düzenlemede yerini alan ve modern dünyanın getirdiği konulardan biri olarak ifade edilebilecek "tasarımda gizlilik" gibi bir yaklaşımın bulunmadığı ve bu durumun, Kanun'un Dünya'daki örneklerinden geride kalmasına sebebiyet verdiği söylenebilir[112]. Yine, unutulma hakkı kavramının da GVKT'de düzenlemesini bulmasına ve doktrinde bazı yazarların bu hakkın Türk Hukukunda üstü kapalı olarak ilgili kişiye tanınan bir hak olarak tanımlandığı görüşlerine[113] rağmen, Kanun'da unutulma hakkı kavramı yer almamaktadır ve bu da bir eksiklik olarak değerlendirilebilecektir. Bu konuda, Kurul Kararları ile hukuki temeller oluşturulmaya çaba gösterilmekte ise de "unutulma hakkı" bakımından Kurul tarafından farklı yaklaşımlar belirlenebilmekte ve menfaat dengesi zaman zaman veri sorumlusu lehine sonuç doğuracak şekilde değerlendirme konusu yapılabilmektedir[114]. Bu tip temel kavramların eksikliğinin yanı sıra, GVKT'den farklı olarak, çocukların kişisel verileri, müşterek veri sorumlusu, bulanıklaştırma, veri koruma

---

[110] Küzeci, *Kişisel Verilerin Korunması*, s. 316.
[111] Küzeci, s. 317.
[112] Cavoukian ve Jonas, "Privacy By Design".
[113] Yavuz, *Unutulma Hakkı*, s. 92.
[114] Kurul'un "Bir Gerçek Kişinin Adının Geçtiği Köşe Yazısının Silinmesi Talebi" başlıklı özet kararı, ayrıntılı bilgi için bakınız: https://kvkk.gov.tr/Icerik/4214/Kurul-Kararlari [Erişim Tarihi: 16.03.2019]

etki değerlendirmesi, veri koruma görevlisi bulundurma zorunluluğu gibi kavram ve düzenlemelerin Kanun'da bulunmaması da Türk kişisel verilerin korunması hukuku açısından eksiklik ve geride kalmışlık olarak değerlendirilebilecek durum ve düzenlemelerdir ***(Genel Veri Koruma Tüzüğü, m. 25, 28, 30, 57)***.

Kanun'un bazı maddelerinin 07 Ekim 2016 tarihi itibariyle yürürlüğe girmesiyle birlikte Kanun bu tarihte tüm maddeleri ile uygulanmaya başlanmıştır. Kanunun Geçici 1. Maddesi'nde "*Kanun'un yayımı tarihinden önce işlenmiş olan kişisel verilerin, yayımı tarihinden itibaren iki yıl içinde Kanun hükümlerine uygun hâle getirileceği*" ifade edilmiştir. Kanun'da öngörülmüş olan iki yıllık geçiş süresi, yalnızca Kanun yürürlük tarihinden evvel elde edilen kişisel verilerin KVKK uyarınca getirilen yükümlülüklere uyumlu hale getirilmesi için öngörülmüş olup, 7 Nisan 2016 sonrası işlenen kişisel veriler için Geçici 1. madde uygulama alanı bulmamış ve veri sorumlularının 7 Nisan 2016 tarihinden sonra işledikleri kişisel veriler ile ilgili sorumlulukları başlamıştır.

7 Nisan 2018 tarihi itibariyle ise Kanun kapsamında veri sorumlusu olarak kabul edilen tüm kişiler bakımından, işlemiş oldukları tüm kişisel veriler ile ilgili olarak Kanun'daki kural ve yükümlülüklere uyma zorunluluğu doğmuştur. Devrim niteliğindeki bu kanun, Türkiye'de daha evvel Anayasa hükmü ve bazı diğer kanunlarda bulunan hükümler ile korunan kişisel verilere ve korunmalarına dair tüm hususları açıklığa kavuşturmuş olup, Avrupa Birliği standartlarına uyum sağlayabilmek adına da bu Kanun ile önemli bir adım atılmıştır.

"Kanun ile kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişisel hakların ihlal edilmesinin önüne geçmek amaçlanmış"[115] olup Kanun'un hazırlık aşamasında, "108 sayılı Sözleşme" ve "Avrupa Birliği'nin 95/46/EC Sayılı Direktifi"nden yararlanılmıştır.

---

[115] "Kişisel Verileri Koruma Kurumu", "KVKK Soru Cevap", s. 12.

Bu temel amaca ek olarak, Kanun'un 1. Maddesinde ifade edildiği üzere, Kanun'un bir amacı da "*kişisel verilerin işlenme şartlarını, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunmasını ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek*"tir. Kanunun gerekçesinde, "kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması" da bu kapsamda değerlendirilmekte olup ayrıca, "kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi" de amaçlar arasında bulunmaktadır[116].

Kanunun kapsamı da Kanunun 2. Maddesinde ifade edilmiştir. Bu düzenlemeye göre, "*Kanun, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin (kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi) parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında*" uygulanacaktır. Kapsam maddesi ile ilgili olarak, özel sektör ile kamu sektörü arasında bir ayrım yapılmamıştır. Kanun'da belirlenen usul ve esaslar tüm sektörler için benimsenmiş ve hatta "Kişisel Verilerin Korunması Kurulu" tarafından yayınlanan rehberlerde "*yurtdışında yerleşik olmakla birlikte Türkiye'de faaliyet gösteren veri sorumluları hakkında da Kanun hükümlerinin uygulanacağı*" ifade edilmiştir[117].

[116] "Kişisel Verileri Koruma Kurumu", s. 15.
[117] "Kişisel Verileri Koruma Kurumu", s. 16.

2. BÖLÜM: TÜRK HUKUKUNDA VERİ SORUMLUSU KAVRAMININ ÖZELLİKLERİ

2.1. KİŞİSEL VERİLERİN KORUNMASI HAKKI VE VERİ SORUMLUSU KAVRAMI ARASINDAKİ İLİŞKİ

Veri sorumlusu kavramı, kişisel verilerin korunması hakkının en önemli kavramlarından biridir[118]. Zira, veri işleme faaliyetine ilişkin tüm sistemler, ölçütler, sınırlar ve yöntemler veri sorumlusu tarafından belirlenmekte olup, veri sorumlusunun varlığı, veri işleme faaliyetinin varlığına sebebiyet vermekte ve ilgili kişi veri işleme faaliyeti kapsamında korunmaktadır. Kişisel verilerin korunması hakkının sacayakları irdelendiğinde, olmazsa olmaz nitelikte bulunan veri sorumlusu kavramı ile kişisel verilerin korunması hakkı arasındaki ilişki 1960'lı yıllardan bugüne büyük bir değişim göstermiş ve veri sorumluları zaman geçtikçe kişisel verilerin korunması bakımından farklı yükümlülük ve sorumluluklar ile yüzleşmek zorunda kalmıştır.

Kişisel verilerin korunması hukukunun gelişimi ve bu hukuk dalı ile ilişkili normatif kaynaklar incelendiğinde, korumanın kapsamının ve kişisel verilerin korunmasına verilen değerin, 1960'lı yıllardan bugüne gerçekleşen teknolojik gelişmeler ve globalleşme ile doğru orantılı bir şekilde değişkenlik gösterdiği görülmektedir. 1980'li yıllarda uluslararası kaynaklarda, ayrı bir hak olarak yerini alan kişisel verilerin korunması hakkı, 1990'lı yıllarda ise daha geniş kitlelere yayılmış ve güncel tartışmalara konu edilmeye başlanmıştır. Veri sorumlusu kavramının önemi de tam bu dönemde farklı bir noktaya gelmiş olup, bu dönemde ispat külfeti ilgili kişiden alınarak veri sorumlusuna yüklenmiş ve sektöre göre farklı özel düzenlemelerle veri sorumlusu tanımı ayrışmaya ve özelleşmeye başlamıştır[119].

Günümüzde ise, insanoğlu teknoloji ile temas ettiği neredeyse her adım ve işleminde veri üretmekte ve dünya üzerinde her saniye milyonlar ile ifade edilen sayılarda veri oluşumu söz konusu olmaktadır. Özellikle, bu durumun, teknoloji çağı ile birlikte büyük bir hız

---

[118] Henkoğlu, *Bilgi Güvenliği*, s. 128.
[119] Mayer-Schönberger, *The Virtue of Forgetting*, s. 13.

kazanması, büyük biraderin yanında küçük biraderlerin de etkin bir şekilde veri avcılığı faaliyetinde bulunma alışkanlığı[120], toplumdaki hemen hemen her sektörde veri koruma hakkını daha önemli hale getirmiş ve temel bir insan hakkı olan "kişisel verilerin korunması hakkı"nın önemli hale gelmesi ile veri sorumlusu kavramının da farklılaşma zorunluluğu hasıl olmuştur.

İş yerleri, bu duruma örnek olarak verilebilir. Örneğin, toplumun her yerinde olduğu gibi, işyerlerinde de veri işleme olanakları çeşitlenmiş ve işyerlerindeki veri işleme faaliyetleri önemli bir şekilde artış göstermiştir. Bu artışın doğal sonucu olarak, işçilerin kişisel verilerinin korunması hakkı üzerinde oluşan müdahaleler de yoğunlaşmıştır[121]. İş sözleşmesindeki bağımlılık ilişkisinin yanı sıra, işçilerin günlük yaşantılarında işverenin emri ve otoritesi altında geçirdikleri sürenin uzunluğu ve bu durum sebebiyle profesyonel yaşam ile özel yaşamı her an ayırabilmenin kolay olmaması nedenleriyle de, işçinin iş ilişkisinde kişisel verilerinin koruma altına alınması büyük bir önem arz eder hale gelmiştir[122].

İş ilişkileri günümüz dünyasında veri sorumlusu ve ilgili kişi ilişkisine verilebilecek yüzlerce örnekten yalnızca bir tanesidir. Veri sorumlusu kavramı, verinin işlendiği her yerdedir. Normatif kavramlar irdelendiğinde, veri işleme faaliyeti kapsamındaki yükümlülükler genelde veri sorumlularına yüklenmektedir[123]. Bu sebepledir ki, kişisel verilerin korunmasının tam olarak sağlanabilmesi ve hakkın tesisi bakımından, veri sorumlusunun tespiti ve veri işleyen kavramından ayrıştırılması da büyük önem arz etmektedir[124]. Ve fakat ifade etmek gerekir ki, veri sorumlusunun tespiti 1990'lı yılların başında çok daha kolayken, bilgisayar teknolojisinin gelişimi ve internet kullanımının yaygınlaşması, ticari ilişkilerin ve haberleşme yöntemlerinin değişimi ve daha kompleks bir hal alması sebepleriyle, bu belirgin durum daha bulanık bir hal almış ve ilişkilerin ve yapıların karmaşıklaşması veri sorumlusu kavramının tespiti ve veri işleyen ile veri sorumlusu kavramı arasındaki çizginin belirgin bir şekilde çizilmesi çok daha

---

[120] Küzeci, *Kişisel Verilerin Korunması*, s. 49-51.
[121] Gürsel, *İşçinin Kişisel Verileri*, s. 157.
[122] Gürsel, s. 159.
[123] Avrupa Birliği Veri Güvenliği Yönergesi, m. 10-15.
[124] Buellesbach ve diğerleri, *European IT Law*, s. 37.

zorlaşmıştır[125]. Öyle ki, günümüzde, aynı anda bir hastanenin, bir sigorta şirketinin ve Sağlık Bakanlığı'nın tek bir veri işleme faaliyetine aynı anda dahil olduğu durumlar yaygın bir şekilde söz konusu olabilmekte ve işlenen verinin hassas nitelikte veri olması durumunu çok daha kompleks bir hale sokmaktadır. İlgili kişinin verilerinin ve özel hayatının gizliliğinin korunması bakımından, işbu ilişkinin doğru bir şekilde analiz edilerek veri sorumlusunun ve varsa veri işleyenin tespit edilmesi hayati bir önem taşımaktadır[126].

Kişisel verilerin korunması hakkının tanımı yapılırken de belirtildiği üzere, kişisel verilerin korunması hakkının içeriği ve kapsamı, veri işleme faaliyetlerinin tümden engellenmesi gibi toptan yasaklayıcı bir amaç gütmemektedir. Kişisel verilerin korunması hakkının ve veri sorumlusu arasındaki ilişkinin en önemli yönlerinden biri de, ölçüsüz müdahalelere karşı ilgili kişiyi korumak ve verilerin nasıl kullanılacağı hakkında ilgili kişiye karar verme özgürlüğü sağlamaktır[127]. Bunun yanında, veri sorumlusunun bilgi edinme hakkı gibi temel haklarının da dikkate alınması gerekmektedir. Bu doğrultuda, kişisel verilerin korunması hakkının uygulanmasında taraflar arasında uygun bir denge tesis edilmelidir[128]. Bu dengenin tesisi de, kişisel verilerinin korunması hakkı ile veri sorumlusu arasındaki ilişkiyi belirleyici nitelikte bir durum olup söz konusu denge, ulusal ve uluslararası normatif temellerde gerekçelendirilerek kanuni temellere oturtulmuştur.

Tüm bu açıklamalar ışığında, tezimizin ikinci kısmında, kişisel verilerin korunması hakkının en önemli parçalarından biri olan veri sorumlusu kavramı tüm yönleriyle açıklanacak olup, veri sorumlusu kavramının Türk Hukuku altında ne şekilde değerlendirildiği de ayrıca irdelenecektir.

---

[125] Kuner, *European Data Protection Law*, s. 71-72; Buellesbach ve diğerleri, *European IT Law*, s. 37.
[126] Colonna, "Europe Versus Facebook", s. 49.
[127] Gürsel, *İşçinin Kişisel Verileri*, s. 160.
[128] Okur, "İşçinin Kişisel Verilerinin Korunması Hakkı", s. 370.

2.2. VERİ SORUMLUSU VE VERİ İŞLEYEN KAVRAMI

2.2.1. Veri Sorumlusu Kavramı

KVKK m. 3(ı) düzenlemesi kapsamında, "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi", veri sorumlusu olarak tanımlanmıştır. İşbu gerçek ve tüzel kişiler, "özel hukuk kişileri ile sınırlı olmayıp kamu otoriteleri veya idareleri ve diğer her türlü kuruluş" da veri sorumlusu sıfatını haizdir[129].

Yukarıda da ifade edildiği üzere, veri sorumlusunun kim olduğunun belirlenmesi ve tespiti pek çok açıdan önem arz etmektedir. Zira, gerek Yönerge ve Tüzük'te gerekse KVKK'da sorumluluk ve görevlerin pek çoğu veri sorumlusu üzerinde bulunmakta olup ihlaller nedeniyle de genellikle veri sorumluları yükümlü tutulmaktadır[130]. Yine, tek bir veri işleme faaliyetinin içinde birden çok veri sorumlusunun bulunması halinde sorumlulukların ayrıştırılması[131] tespiti bakımından da bu husus önem arz etmektedir. Ek olarak, bir veri işleme faaliyeti, kendi içinde analiz edilirken de veri sorumlusu kavramının tespiti önem arz edecektir. Örneğin, işyerlerinde işverenin sağlık verileri bakımından, tüm bu verileri işyeri hekimine aktararak işyeri hekimi ile yapacağı bir protokolle işverenin, işçinin sağlık verileri ile ilişkisini kesmesi ve bu verileri kendi veri sisteminden dışarı çıkarması, uygulamada sıklıkla karşılaşılan bir işlemdir. Bu halde, işveren ve işyeri hekimi bakımından müşterek veri sorumlusu durumunun mu oluştuğu yoksa bu gerçek ve/veya tüzel kişilerin birbirinden ayrı veri sorumluları olarak mı değerlendirileceği sorusunun cevabı, ancak veri sorumlusu kavramının iyi bir şekilde analiz edilerek veri sorumlusunun doğru bir şekilde tespit edilmesi sayesinde verilebilecektir.

---

[129] Gürsel, *İşçinin Kişisel Verileri*, s. 130.
[130] Kuner, *European Data Protection Law*, s. 69-70.
[131] "*Handbook on European Data Protection Law*", s. 55.

Veri sorumlusunun tespiti ise ancak veri sorumlusunu veri işleme faaliyetinin diğer parçalarından ayıran faktörlerin ve ögelerin belirlenmesi ile gerçekleştirilebilecektir. Kişisel verilerin işlenmesine ilişkin kararların alınması yetkisi, veri sorumlusunu ayıran niteliktir. Veri sorumlusu, "kişisel verilerin işlenme amacını ve yöntemini belirleyen kişi olup işleme faaliyetinin "neden" ve "nasıl" yapılacağı sorularının cevabını verecek olan gerçek veya tüzel kişidir". Kişisel verilerin işlenmesinde "amaca karar verme" eylemini gerçekleştirme ve veri işlemede yöntemlere karar verme prosedüründe en azından hukukilik bakımından başlıca noktaları belirleme veri sorumlusunun, veri işlemenin diğer unsurlarından ayrılmasını sağlamaktadır[132]. Veri sorumlusu, veri sisteminde, "verilerin efendisi" olup veri sorumlusu verinin nasıl işleneceği hususunda tasarruf yetkisini elinde bulundurmaktadır[133]. Bu bağlamda; "*kişisel verilerin toplanması ve toplama yöntemi, toplanacak kişisel veri türleri, toplanan verilerin hangi amaçlarla kullanılacağı, hangi bireylerin kişisel verilerinin toplanacağı, toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı ve verilerin ne kadar süreyle saklanacağını*" veri sorumlusu belirleyecek olup[134], veri sorumlusunun tespiti bakımından bu yetki ve amaçların ayrı ayrı sorgulanarak veri sorumlusunun bu analizin ardından tespiti gerekmektedir. Söz konusu amaç ve yöntemlere karar verme durumu, açık bir yasal yetkiye dayanabileceği gibi veri işleme faaliyetinin gerçekleştiği organizasyonun işlevsel rolünden de kaynaklanabilmektedir[135].

Veri sorumlusu tüzel kişi olduğu durumlarda, tüzel kişiliğin içerisinde veri işleme faaliyetlerinden sorumlu olan gerçek kişiler veya tüzel kişiliğin alt birimleri Kanun'un uygulanması bakımından o tüzel kişilik ile arasındaki ilişki bakımından bir değerlendirme yapıldığında veri sorumlusu olarak kabul edilmemektedirler[136]. Ve fakat, bu durum bir tüzel kişilik içinde çalışan işçinin, hiçbir zaman veri sorumlusu sıfatını haiz olmayacağı anlamına gelmeyecektir; zira veri üzerinde hakimiyet kurabilecek her türlü çalışan, müşteri veya tedarikçi veri sorumlusu olabilir[137].

---

[132] "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 32.
[133] Çekin, *Kişisel Verilerin Korunması*, s. 41.
[134] Kiss ve Szoke, "New Generation of Data Protection Regulation", s. 319.
[135] Gürsel, *İşçinin Kişisel Verileri*, s. 134.
[136] Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu ve Veri İşleyen", s. 2.
[137] Çekin, *Kişisel Verilerin Korunması*, s. 41.

Veri sorumlusunun tüzel kişi olması halinde, veri sorumlusu yükümlülüğü ilgili tüzel kişilik üzerinde doğacaksa da veri sorumluları, veri yönetimi konusunda tüzel kişiliği temsil ve ilzama yetkili olan kişi veya kişileri görevlendirebilirler. "*Bu görevlendirme tüzel kişiliğin veri sorumlusu yükümlülüğünü ortadan kaldırmaz ve ilgili gerçek kişileri de veri sorumlusu yapmaz*"[138].

Veri sorumlularına ilişkin bir tartışma konusu da grup şirketi ve bağlı ortakların bulunduğu durumlarda kimin veri sorumlusu olarak değerlendirileceği hususudur. Bu konuda, Kurul yayınladığı rehberler ile konuya açıklık getirmiş olup bir gruptaki her şirket, kişisel verilerin işlenme amaçlarını kendisinin belirlediği ve veri kayıt sisteminin tutulmasından kendisinin sorumlu olduğu hallerde Kanun gereğince "veri sorumlusu" sıfatına sahip olacaktır[139].

Şirketin veri işleme sıfatını haiz olması özellikle kişisel verilerin korunması hakkına bağlı olarak ortaya çıkabilecek medeni hukuk ve ceza hukuku kapsamındaki sorumluluklar bakımından bu sorumluluğun yöneltilmesi sorununu ortaya çıkarmaktadır. Örneğin, bir şirketin yönetim kurulu üyelerinden birinin işçileri kamerayla gizlice izlemesi halinde, yönetim kurulu üyelerinin onayını almayan bu yönetim kurulu üyesi medeni hukuk ve ceza hukuku bakımından sorumlu sayılacaksa da bu durum şirketin veri sorumlusu olduğu sonucunu etkilemeyecektir[140]. Bu durumun, veri sorumlusunun Kanun'da merkezi bir konuma sahip olmasından[141] kaynaklandığı söylenebilir.

Bu noktada ifade etmek gerekir ki, Türk kişisel verilerin korunması hukukunda bulunmayıp gerek GVKT gerekse Madde 29 Çalışma Grubu tarafından yapılan değerlendirmelerde ifade edilen "beraber/müşterek veri sorumlusu kavramı" da veri

---

[138] "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 16; Gürsel, *İşçinin Kişisel Verileri*, s. 134.

[139] Kişisel Verileri Koruma Kurumu, "KVKK Soru Cevap", s. 16.

[140] "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 17; Gürsel, *İşçinin Kişisel Verileri*, s. 181.

[141] Çekin, *Kişisel Verilerin Korunması*, s. 40.

sorumlusu kavramının içinde bulunan mühim bir konudur. GVKT m. 26 ve devamında tanımlanan bu kavram, iki ya da daha fazla veri sorumlusunun veri işleme amaç ve yetkisini birlikte belirledikleri durumda karşımıza çıkmaktadır. ABAD, 5 Haziran 2018 tarihli kararıyla bu kavramı genişletmiştir[142]. Söz konusu karara konu olayda, Almanya'da eğitim faaliyetleri yürüten bir kurumun Facebook üzerinden kullandığı ve pazarlama faaliyetlerini yürüttüğü bir hayran sayfası, Alman veri koruma otoritesi tarafından hem Facebook hem de sayfa yöneticisi tarafından kullanıcıların kişisel verilerinin işlenmesi ile ilgili olarak bilgilendirilmemesi nedeniyle kapatılmış ve bunun üzerine konu, ABAD'ın önüne gelmiş ve ABAD yaptığı değerlendirmede, çerez bilgilerine kişisel veri ile ilgili olarak site yöneticisi erişmese de, çerez toplama amaçlarının ve içeriğinin site yöneticisi tarafından belirlenmesi nedeniyle Facebook ve ilgili hayran sayfası yöneticisinin "beraber veri sorumlusu" olarak tanımlanacağına yönelik hüküm kurmuştur.

Beraber veri sorumlusu kavramı, yalnızca Avrupa'da değil, globalleşmenin sınırlarını genişlettiği ve özellikle internet üzerinden yapılan işlemlerin hızla artış gösterdiği günümüzde, dünyanın her yerinde sıklıkla karşımıza çıkan bir durumdur. Örneğin, ilgili kişinin bir seyahat arama motoru üzerinden, uçak bileti, otel ve araç kiralama rezervasyonu yaptığı bir örneği dikkate aldığımızda bu işlemde dahil buna benzer tüm işlemlerde, seyahat arama motoru, rezervasyonun yapıldığı otel, havayolu şirketi ve araç kiralama şirketi, birlikte veri işlemenin amacına karar vermekte ve yetkilendirmeyi de aralarında gerçekleştirdikleri mutabakat ile sağlamakta olup, bu durumda verilerin üzerinde birlikte ve beraber bir kontrole sahip olmaktadırlar. Bu durumun, kanuni bir temele dayandırılması gerekmekte olup kanımızca Türk Hukukunda da benzer bir düzenlemenin yapılması çağın gereklerine uyum bakımından faydalı olacaktır.

---

[142] Fritz, "Joint Controllership". https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies [Erişim tarihi: 10.02.2019]

2.2.2. Veri İşleyen Kavramı

Veri işleyen kavramı, KVKK m. 3(ğ) başlığı altında tanımlanmış olup buna göre; "*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*" veri işleyendir. Yönerge ile Kanun, veri işleyen bakımından benzer bir yaklaşım göstermektedir ve bu bağlamda, veri sorumlusuna nazaran ayrı bir hukuki kişiliğin varlığı ve veri işleme faaliyetinin bu ayrı tüzel kişilik tarafından veri sorumlusu adına yerine getirilmesi koşullarının bir arada bulunduğu durumda veri işleyen kavramı söz konusu olmaktadır[143].

Veri işleyenin gerçek veya tüzel kişi olması mümkündür. Şirketin organizasyon yapısındaki departmanların ayrı bir hukuki kişiliği bulunmamakta olup bu departmanların veri sorumlusu veya veri işleyen olarak isimlendirilmesi söz konusu olamaz. Veri işleyen organizasyonun dışındaki kişi olup bu kişiler, veri sorumlusunun kişisel veri işlemek üzere yetkilendirdiği ayrı bir gerçek veya tüzel kişiliktir. Bir kuruluşun topladığı kişisel verilerin saklanması için bir bulut hizmeti sağlayıcısıyla sözleşme yapması durumunda, bulut hizmeti sağlayıcısı veri işleyen için verilebilecek iyi bir örnektir. "Zira taraflar arasındaki sözleşme gereği bulut hizmeti sağlayıcısının verileri kendi amaçları için kullanması mümkün olmadığı gibi, kendisi veri de toplamamaktadır". Tek faaliyeti veri sorumlusu kuruluştan gelen kişisel verileri yine kuruluşun talimatlarına uygun olarak saklamaktır. Bu noktada ifade etmek gerekir ki, bulut sistemi sağlayıcısı şirket, kendi sisteminde kendi çalışanları için tuttuğu veriler bakımından ise veri sorumlusu olarak değerlendirilecektir. Böylece, veri işleyen sıfatını haiz bir hukuki kişiliğin aynı zamanda veri sorumlusu kişiliği de bulunabilmesi söz konusudur. Bu kapsamda, bu tür şirketler bakımından, veri işleme faaliyetinin durumu her bir somut olay için ayrıca değerlendirilmeli ve tüzel veya gerçek kişinin sıfatı tespit edildikten sonra gerekli analiz bu tespite uygun bir şekilde gerçekleştirilmelidir.

Veri işleyen bakımından, en önemli koşul ve unsur, işleyicinin veri sorumlusu adına hareket etmesi ve veri sorumlusunun kendisine verdiği yetkiler çerçevesinde hareket

---

[143] "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 25.

etmesi gerekliliğidir. Bu yetkilendirme, belirli görevler için olabileceği gibi daha genel bir devir de söz konusu olabilir[144]. Bu doğrultuda, veri işleyen veri sorumlusunun talimatları doğrultusunda ve ışığında hareket edecek olup bu talimatlar bakımından veri sorumlusu için en uygun teknik ve organizasyonel yapı ve yöntemi de seçecektir[145]. Bu durum, veri işleyene belirli konularda takdir yetkisi tanısa da bu takdir yetkisi, talimatları aşacak nitelikte olamayacaktır[146]. Zira, veri işleme sistemi ile ilgili sorumluluk kendisinde olan veri sorumlusu, bu bakımdan denetleme yetkisini de elinde bulundurmaktadır[147]. Denetleme sorumluluğunun ötesinde veri sorumlusu, veri işleyeni seçerken, veri işleyenin kişisel verilere uygun bir şekilde bakabilme, verileri koruyabilme, talimatlara uygun işleyebilme ve teknik ve idari açıdan gerekli güvenceleri sağlayıp sağlayamadığını değerlendirmeli ve seçimini bu değerlendirme sonrasında gerekli koşulların sağlanması ile yapmalıdır[148].

Kurum tarafından yayınlanan "*Veri Sorumlusu ve Veri İşleyen Rehberi*" isimli rehberde, örnek niteliğinde, veri sorumlusunun, veri işleyene devredebileceği yetkileri ifade edilmiş olup[149] buna göre; "*kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı, kişisel verilerin hangi yöntemle saklanacağı, kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları, kişisel verilerin aktarımının hangi yöntemle yapılacağı, kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot, ve kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri*" devredilebilecek yetkilerdendir. Bu hususlar örnek niteliğinde olup, sayısı arttırılabilir. Bunun yanında, yukarıda da belirtildiği üzere, veri işleyen, veri sorumlusundan devredilen yetkiler bakımından bağımsız olmayıp veri sorumlusu bu yetkileri devretmekle, devrettiği yetkiler bakımından Kanun'da ve sair mevzuatta sayılan yükümlülüklerden de kurtulmuş ve bu sorumlulukları devretmiş sayılmayacaktır[150].

---

[144] Gürsel, *İşçinin Kişisel Verileri*, s. 135.
[145] "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 25.
[146] Zanfir, "Tracing the Right to Be Forgotten", s. 237; aksi görüş için bakınız - Gürsel, *İşçinin Kişisel Verileri*, s. 136.
[147] "*Handbook on European Data Protection Law*", s. 61-62.
[148] Dülger, *Verilerin Korunması*, 143.
[149] Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu ve Veri İşleyen", s. 3-4.
[150] Dülger, *Verilerin Korunması*, s. 21.

Veri işleyen bakımından, bir diğer önemli konu ise sorumluluk hususudur. Kanun'un 12. maddesinin 1. fıkrası uyarınca "*veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır*". Kanunun 12. maddesinin 2. fıkrası uyarınca da "*veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, söz konusu tedbirlerin alınması hususunda bu kişilerle birlikte müteselsilen sorumludur*". Bu noktada ifade etmek gerekir ki, Kanun'da müteselsil sorumluluğa atıfta bulunulmakta ise de Kanun kapsamındaki yükümlülükler, veri sorumlusu üzerinden tanımlanmış olup, ilgili kişinin haklarının veri sorumlusuna karşı ileri sürüleceği düzenlenmiştir[151] ve bu doğrultuda, ilgili kişi, kişisel verileri üzerindeki hakları için veri sorumlusuna başvuracaktır[152].

Kanun'da, kişisel veri işleme faaliyetlerine ilişkin hukuki yükümlülüklerin yerine getirilmesinde veri sorumlusunun yükümlü olduğu bir sorumluluk rejimi benimsenmişse ve veri işleyenin veri sorumlusunun talimatlarını yerine getirdiği açıksa da sorumluluğa ilişkin madde doğrudan müteselsil sorumluluğa ve müşterek olarak gerekli tedbirlerin alınmasına atıfta bulunulmaktadır. Bu konuda yapılan haklı bir eleştiriye göre, Kanun'un yalnızca müteselsil sorumluluğa atıfta bulunmuş olması, Kanun'da ve hukuki pratikte belirli boşluklar doğurmaktadır[153]. GVKT'de ise bulut sistemleri ve bilişim şirketlerinin de yaygınlığı dikkate alınmak suretiyle, veri işleyene ayrı bir başlık açılarak ayrı bir tanımlama yapılmış ve veri işleyene özel yükümlülükler GVKT kapsamında belirlenmiştir ***(Genel Veri Koruma Tüzüğü, m. 24-31)***. Öyle ki, GVKT ışığında, veri işleyenin uygun teknik ve organizasyonel tedbirleri alması, Avrupa bölgesi dışında yer aldığı ancak GVKT'ye tabi olduğu durumlarda AB Temsilcisi ataması, kişisel verileri işleme yetkisi bulunan kişilerin gizlilik taahhüdünde veya yasal gizlilik yükümlülüğü altında bulunmasını sağlaması gibi yükümlülükler veri işleyenden beklenmiş ve yine seçilen veri işleyicisinin sağladığı güvencelerin devam etmesine ilişkin bir süreklilik

---

[151] Kişisel Verileri Koruma Kurumu, "KVKK Soru Cevap", s. 31.
[152] Dülger, *Verilerin Korunması*, s. 21.
[153] Çekin, *Kişisel Verilerin Korunması*, s. 41.

durumu aranmış ve son olarak veri işleme yetki devrinin ancak yazılı sözleşme ile gerçekleştirilebileceği ve bu şekilde ayrıntılandırılacağı ifade edilmiştir[154].

Ülkemizdeki uygulama ve veri işleyenlerin nitelikleri de dikkate alındığında, Türk hukukunda da benzer bir tanımlamaya ihtiyaç duyulduğu aşikardır. Zira, Kanun'un 3. maddesinde veri işleyen tanımlandıktan sonra, veri işleyenin Kanun'da ayrıca bir başlık altında düzenlenmemiş olması ve bu kavram üzerinde kısa atıfların olması uygulama bakımından eksiklik yaratacak niteliktedir. Kanun'un gerekçesinde de bu hususun neden bu şekilde ifade edildiğine dair bir açıklama bulunmamakta olup, söz konusu eksikliğin giderilmesi uygulama açısından daha uygun olacaktır[155].

2.3. KİŞİSEL VERİLERİN İŞLENMESİ, KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDA BENİMSENEN TEMEL İLKELER VE VERİ İŞLEME KOŞULLARI

2.3.1. Kişisel Verilerin İşlenmesi

Kanun incelendiğinde, veri işleme kavramına Kanun'un büyük önem atfettiği ve bu kavramın kişisel verilerin korunması mevzuatı bakımından temel nitelikte bir kavram olduğu görülmektedir.

Kişisel verilerin işlenmesi, Kanun m. 3'te tanımlanmış olup, buna göre, "*kişisel verilerin tamamen veya kısmen, otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem kişisel verilerin işlenmesini*" ifade etmektedir. Bu tanım ışığında, veri işleme faaliyetine ilişkin verilen işlemler tahdidi bir sayımın parçası olarak değerlendirilemeyecek olup sayılan benzer

---

[154] Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu", s. 85 vd.
[155] Çekin, *Kişisel Verilerin Korunması*, s. 41.

haller de veri işleme olarak kabul edilebilecektir[156]. Özetle, verinin ilk defa elde edildiği andan itibaren bu elde etme de dahil olmak üzere, işleme faaliyeti veri işleme sisteminin bir parçası olmak kaydıyla yapılan her türlü işlem veri işleme olarak değerlendirilebilir[157].

Kişisel verilerin işlenmesi bakımından, Kanun otomatik yollar veya otomatik olmayan yollar şeklinde bir atıfta bulunmuş olup verinin bilgisayar ve benzeri bilişim sistemleri üzerinden işlenmesi halinde otomatik yollarla işleme durumu söz konusu olacaktır[158]. Bir şirketin insan kaynakları biriminde, özlük dosyalarının insan kaynakları çalışanlarının bilgisayarında tutulması bu işleme türüne örnek olarak verilebilir. Buna karşın, herhangi bir otomasyon sisteminden yararlanmaksızın işleme hallerinde ise otomatik yollarla olmayan kişisel veri işlemesi söz konusu olacaktır[159]. Ve fakat otomatik olmayan yöntemlerle veri işleme konusunda kıstas yalnızca kişisel verinin otomasyon sistemi kullanılmaksızın işlenmesi değil bu işleme faaliyetinin aynı zamanda veri işleme sisteminin parçası olmasıdır[160]. Bir santralde bulunan ve veri kayıt sisteminin bir parçası olan ziyaretçi defterinde tutulan kayıtlar otomatik olmayan yollarla veri işlemeye örnek olarak verilebilir.

Kişisel verilerin işlenmesi temel kavram olmakla birlikte, kişisel verilerin korunması amacının gerçekleştirilmesi veri işlemenin belirli ilke ve şartlarda gerçekleştirilmesiyle mümkün olabilecektir. Kanun, veri işlemeye ilişkin olarak öncelikle temel ilkeler belirlemiş ve bu ilkelerin yanı sıra kişisel verileri işleme bakımından belirli şartlar öngörmüştür. Ayrıca, özel nitelikli veriler bakımından ise Kanun, bu verilere ayrı bir önem atfetmesi sebebiyle bu verilerin işlenmesi bakımından ayrıca farklı şartlar da öngörmüş bulunmaktadır.

---

[156] Başalp, *Kişisel Verilerin Korunması*, s. 30-31.
[157] Kişisel Verileri Koruma Kurumu, "KVKK Soru Cevap", s. 22.
[158] Dülger, *Verilerin Korunması*, s. 15; Taştan, *Kişisel Verilerin Korunması*, s. 43.
[159] Dülger, *Verilerin Korunması*, s. 15; Başalp, *Kişisel Verilerin Korunması*, s. 31.
[160] Taştan, *Kişisel Verilerin Korunması*, s. 44.

2.3.2. Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler

Kişisel verilerin işlenmesine ilişkin temel ilkeler, Kanun m. 4'te düzenlenmiş olup; ilgili ilkelerin belirlenmesinde 108 Sayılı Sözleşme ve Yönerge temel alınmıştır[161]. Kişisel verilerin korunması temel amaç ise de verilerin işlenmesinde veri kalitesinin sağlanması gerekliliği de önem arz etmekte olup, temel ilkeler aracılığıyla bu gereklilik sağlanmaktadır. Bu ilkeler, kısaca, "*hukuka ve dürüstlük kurallarına uygun olmak, doğru ve gerektiğinde güncel olmak, belirli, açık ve meşru amaçlar için işlenmek, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmak ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek*" olarak ifade edilebilir. Söz konusu ilkeler aşağıda ayrıntısıyla incelenecektir.

2.3.2.1. Hukuka ve Dürüstlük Kuralına Uygun Olmak

Kişisel verilerin hukuka uygun bir şekilde işlenmesi, mevzuattaki düzenlemelere uygun bir şekilde hareket etme zorunluluğunu ifade etmekte olup[162] , KVKK dahil tüm hukuki düzenlemelere uygun şekilde kişisel verilerin işlenmesi gerekmektedir. Bu ilke kapsayıcı nitelikte bir ilke olarak düşünmelidir. Zira, bu ilke, yalnızca konuya ilişkin özel norm niteliğindeki hükümleri değil, genel hukuk kuralları ve evrensel hukuk ilkeleri dahil tüm düzenlemelere uygunluğu içermektedir[163]. Bu ilke, verinin elde edildiği ilk andan itibaren bütün süreçleri kapsayacak nitelikte geçerli bir kural olup, veri sorumlusu veri işlemenin her aşamasında bu ilkeyi göz önünde bulundurmak zorundadır[164].

Kişisel verilerin dürüstlük kuralına uygun şekilde işlenmesi ise, TMK m. 2'de düzenlemesi yapılan, dürüstlük kuralının ve hakkın kötüye kullanılması yasağının kişisel verilerin korunması alanı bakımından bir tezahürüdür[165]. Bu bağlamda, veri sorumlusu, veri işleme faaliyeti esnasında, ilgili kişilerin menfaatlerini ve makul

---

[161] Kişisel Verileri Koruma Kurumu, "KVKK Temel İlkeler", s. 1.
[162] *Handbook on European Data Protection Law*, s. 65.
[163] Dülger, *Verilerin Korunması*, s. 109.
[164] Küzeci, *Kişisel Verilerin Korunması*, s. 207.
[165] Taştan, *Kişisel Verilerin Korunması*, s. 46.

beklentilerini de dikkate alacaktır[166]. Veri sorumlusu, veri işleme faaliyetinde açık ve şeffaf bir şekilde ve makul ve meşru bir amaç ve gerekçe ile veriyi işleyecek, bu esnada gerekli bilgilendirme ve uyarı yükümlüklerini de yerine getirecektir[167]. Veri sorumlusu, kişisel verileri işlerken kendi menfaatleri ile ilgili kişinin hakları arasında bir denge kurmalı ve veriyi orantılı bir şekilde işlemelidir[168]. Yine, veri sorumlusu, kişisel veriyi makul ve meşru amaç ve gerekçesi ışığında gerektiği kadar toplamalı ve işlemelidir. Dürüstlük kuralının, kişisel verilerin korunması alanında tezahür ettiği durumlar kısaca bu şekilde ifade edilebilecekse de bu durumlar somut olaya göre değişkenlik ve farklılık da gösterebilir.

Bu ilke, GVKT'de ise "*hukuka uygunluk, adalet ve şeffaflık*" başlığı altında düzenlenmiş olup, özellikle adalet ve şeffaflık bakımından, Türk Hukukunda dürüstlük kuralına yapılan atfın GVKT'de adalet ve şeffaflık kavramıyla daha somut bir şekilde düzenlendiği ifade edilebilir. Ve fakat, Türk Hukukunda yer alan dürüstlük kavramı ışığında da veri sorumlusu, kişisel verileri yukarıda ifade edilen yükümlülüklerini yerine getirmek suretiyle veriyi adaletli ve şeffaf bir şekilde işlemek zorundadır.

2.3.2.2. Doğru ve Gerektiğinde Güncel Olmak

Kişisel verilerin doğruluğu ve güncelliği, veri sorumlusunun yükümlülükleri arasında bulunmakta[169] olup, söz konusu ilke ile Kanun'da öngörülen ve ileriki bölümlerde ayrıntısıyla ifade edilecek olan ilgili kişinin, verilerin düzeltilmesini talep etme hakkı ile de uyumludur[170].

Kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması bakımından genel kural, veri sorumlusunun ilgili kişinin bilgilerini doğru ve güncel bir şekilde tutması ve bu kuralı temin edecek kanalları açık tutmasıdır.

---

[166] Küzeci, *Kişisel Verilerin Korunması*, s. 207.
[167] Küzeci, s. 207.
[168] Bygrave, *Data Privacy Law*, s. 58.
[169] Gürsel, *İşçinin Kişisel Verileri*, s. 219.
[170] Kişisel Verileri Koruma Kurumu, "KVKK Temel İlkeler", s. 5.

Bu ilke aracılığıyla, ilgili kişinin, veri sorumlusu tarafından tutulan ve "güncel olmayan veya yanlış tutulan" kişisel verilerden dolayı zarar görmesi önlenmeye çalışılmaktadır. Zira, kişisel verilerin korunması ancak doğruluğunu ve güncelliğini yitirmemiş verilerle sağlanabilir[171]. Farklı konulardaki Yargıtay kararları da bu yöndedir. Örneğin, verilerin güncel ve doğru tutulma ilkesinin geçerli olduğu ve bu bakımdan işverenlerin, veriyi elde ettikleri ilk an da dahil olmak üzere veri işleme faaliyetinin her sürecinde işçiye ait kişisel verileri doğru ve güncel tutmakla yükümlü olduğu veya güncel ve doğru tutmak adına gerekli kanalları açık tutmak veya buna uygun sistemleri geliştirmekle mükellef olduğu yönünde kararlar da bu yönüyle önem arz etmektedir[172,173]. Bu durum, verilerin doğru ve güncel tutulması ilkesinin GVKT'deki karşılığında verilerin gerektiği durumlarda güncel tutulması ve verinin mutlak surette doğru tutulması zorunluluğunun da bir gereğidir[174].

Bu noktada ifade etmek gerekir ki, verilerin doğru ve güncel tutulmasının bir yolu da veri öznesinin düzenli aralıkla vereceği beyanlardır. Verinin güncel tutulması ile ilgili olarak ilgili kişinin değişen bilgisini ilgili veri sorumlularına iletmesinin daha kolay ve makul bir yol olacağını savunan görüşler mevcut[175] ise de bize göre veri sorumlusu güncel tutma bakımından uygun bir veri işleme/elde etme yöntemi belirlemeli veya şeffaflık ilkesi çerçevesinde düzenli bilgilendirmenin sağlanabileceği bir veri işleme sistemi kurmalıdır[176]. Ayrıca, veri sorumlusu, veriye ilgili kişi tarafından erişim kanalını da her zaman açık tutmalıdır. Bu durum verinin güncel olmasını sağlayan en temel gerekliliklerden biridir[177].

---

[171] Dülger, *Verilerin Korunması*, s. 131.
[172] "Yargıtay 22. Hukuk Dairesi E. 2015/14162 K. 2016/27896 ve 15.12.2016 tarihli karar" (www.kazanci.com.tr) [Erişim tarihi: 16.03.2019]
[173] Kişisel Verileri Koruma Kurumu, "KVKK Temel İlkeler", s. 5-6.
[174] Dülger, *Verilerin Korunması*, s. 130.
[175] Dülger, s. 133.
[176] Aynı yönde görüş için bknz. Gürsel, *İşçinin Kişisel Verileri*, s. 219.
[177] Gürsel, s. 220.

2.3.2.3. Belirli, Açık ve Meşru Amaçlar için İşlenmek

Veri işleme süreçleri bakımından en önemli ilkelerden biri de veri işleme amacının belirli, açık ve meşru olmasıdır[178]. Bu ilke ışığında, veri işlemenin ve işlenen verinin sınırları belirlenmekte ve belirli bir amaç için toplanan verinin hangi amaçla işleneceği de bu ilke ile belirlenmektedir. Bu ilke, "*verilerin toplanma amacının belirli ve açık olması, verilerin toplanma amacının meşru olması ve verilerin daha sonra işlenme amaçlarının, toplanma amacı ile uyumlu olması*" olmak üzere üç kısımdan oluşmaktadır[179].

Verinin toplanma amacının belirli ve açık olması, ilgili kişilerin maddi ve manevi bütünlüğü, özel hayatın gizliliğinin korunması hakkı, kişiliğini geliştirme hakkı gibi temel değerlerini korumak ve kişiye verilerinin kaderini tayin etmek üzere özgürlük alanı tanımak adına var olan bir ilkedir. Veri sorumlusu, kişisel verilerin amacını tam olarak belirlemeli, bu amacı kapsamında web sitesi, mail, imza gibi kendisine ait araçlarla ilgili kişiyi bilgilendirmeli ve verileri "*ileride bir gün bir ihtimal gerekli olabilir*" düşüncesiyle süresiz, sınırsız ve anonimleştirmeksizin depolamamalıdır[180]. İlgili kişiyi, veri işleme amacı doğrultusunda bilgilendirmeksizin veri işleyen veya belirdiği amaç dışında başka bir amaç ve faaliyet ışığında veri işleme faaliyeti gerçekleştiren veri sorumlusu ise bu ilkeyi ihlal etmiş olacaktır[181]. Söz konusu bilgilendirme yapılırken, veri konularının makul ve yeterli ölçüde aktarıldığından emin olmalı; bilgilendirilen ilgili kişilerin amacı anlama düzeyleri de veri sorumlusu tarafından dikkate alınmalıdır[182].

Kanun'un gerekçesinde de, bu ilkenin, "*veri sorumlusunun, veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kıldığını; aksi durumda, veri sorumlularının, belirttikleri bu amaçlar dışında, başka amaçlarla veri işlemeleri*

[178] Kuner, *European Data Protection Law*, s. 99-100.
[179] Küzeci, *Kişisel Verilerin Korunması*, s. 208.
[180] Küzeci, s. 209.
[181] Kuner, *European Data Protection Law*, s. 100.
[182] Voigt ve Von Dem Bussche, *GDPR*, s. 89.

halinde, bu fiillerinden dolayı sorumlu olacakları" ifade edilmiştir[183]. Veri sorumlusu, amacı belirlerken, öncelikle işlenecek veriler bakımından sınırlamalar belirlemeli, daha sonra işlenecek olan verilerin hangi amaçlar doğrultusunda işleneceğini saptamalıdır[184]. Ve fakat, her şeyden önce ifade etmek gerekir ki, veri sorumlusunun amacını belirlemesinden çok daha önemli olan husus ise bu konuya ilişkin hukuksal düzenlemelerde belirsiz ifadelerden kaçınılması gerekliliği ve hukuksal düzenlemelerin de belirli ve açık olmasıdır[185]. Açık ve somut bir şekilde var olan hukuksal düzenlemeler ancak veri sorumlularının veri işleme amaç ve ilkelerini açık ve belirli hale getirmesini sağlayabilir[186].

Bu ilkenin ikinci kısmını oluşturan verilerin toplanma amacının meşru olması ise verilerin toplanma amacının yasal bir temele dayanmasını, temel hak ve özgürlükler de dahil olmak üzere kanuni yükümlülüklerin gerektirdiği hususlar ile uyumlu bir şekilde ilerlemesini ve verilerin işlenmesinden kaynaklanan çıkar/menfaat ile dengeli olmasını ifade etmektedir[187]. Amacın meşruluğu ise toplumdaki değişimlere bağlı olarak değişiklik gösterebilir ve bu doğrultuda amacın meşruluğu zamanla farklılaşabilir[188].

Kanun'un gerekçesinde ise verilerin meşru amaçlarla işlenmesi, "*veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması şeklinde tanımlanmış ve bu tanım, bir hazır giyim mağazasının, müşterilerinin kimlik ve iletişim bilgilerini işlemesinin meşru amaç kapsamındayken, kan gruplarını işlemesinin meşru amaç kapsamında değerlendirilemeyeceği*" şeklinde örneklendirilmiştir[189]. Bu ilkeye yönelik olarak, Yönerge ve GVKT'de belirli saptamalar gerçekleştirilmiş ve veri işlemenin meşruluğu somutlaştırılmıştır. Bu doğrultuda, "ilgili kişinin rızasının bulunması, ilgili kişinin taraf olduğu bir sözleşmenin ifa edilmesi ya da ilgili kişinin bir sözleşmenin tarafı olmadan önceki isimleri dolayısıyla

---

[183] Kişisel Verilerin Korunması Kanunu, Genel Gerekçe, s. 7-8.
[184] Dülger, *Verilerin Korunması*, s. 117.
[185] Küzeci, *Kişisel Verilerin Korunması*, s. 209.
[186] Dülger, *Verilerin Korunması*, s. 117.
[187] Kuner, *European Data Protection Law*, s. 90.
[188] Voigt ve Von Dem Bussche, *GDPR*, s. 89.
[189] Kişisel Verilerin Korunması Kanunu, Genel Gerekçe s. 7-8.

işlemenin gerekli olması, veri sorumlusunun hukuksal yükümlülüğünü yerine getirmesi için işlemenin gerekli olması" gibi verilerin toplanmasının meşru kılındığı durumlar saptanmıştır[190]. Kanun m. 5'te de verilerin işlenmesini meşru kılan durumlar ifade edilmiş olup, bu durumlar "veri işleme koşulları" başlığı altında ayrıntılı şekilde incelenecektir.

Casus yazılımların, kullanıcıların bilgisi olmaksızın verilerini aktarmaları dolayısıyla meşruluk ilkesiyle bağdaşmayacağına yönelik karar, bu ilkenin ihlaline yönelik olarak verilebilecek örneklerdendir[191]. Yine, "Kişisel Verileri Koruma Kurulu'nun 16/10/2018 tarihli ve 2018/119 sayılı veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesini teminen alınan ilke kararı"[192] ile "sağlık verilerinin Kanun'un 6. maddesinde yer alan işleme şartlarından birine dayanmadan üçüncü kişilere aktarımı hakkında Kişisel Verileri Koruma Kurulu'nun 05/12/2018 Tarihli ve 2018/143 Sayılı Kararı"[193] da meşruluk ilkesinin ihlaline yönelik olarak uygulamadan verilebilecek örneklerdendir.

Verilerin, amacın belirlenmesinin ardından belirlenen amaca uygun olarak işlenmesi ve bu amaçla uyumlu olması ise bu ilkenin son ve kanımızca en önemli parçasını oluşturmaktadır. Zira, bu husus, ilke ile hedeflenen hukuksal yararın gerçekleşmesi için gereklidir[194] ve bu durum sağlandığında, ilgili kişi haklarını etkin bir şekilde kullanabilecektir[195]. Bu bağlamda, kişinin bilgilendirilmesi büyük önem arz etmektedir. Yalnızca verilerinin işlenme amacının farkında olan ilgili kişi, verilerin işlenme sürecini takip edebilir ve bilgilendirme esnasında uygun bulduğu amaç ile verilerin daha sonra işlendikleri amacın uyumlu olduğunu tespit edebilir. Aksi takdirde, kişi verileri

---

[190] Avrupa Birliği Veri Güvenliği Yönergesi, m. 7.
[191] Küzeci, *Kişisel Verilerin Korunması*, s. 212.
[192] "Kişisel Verileri Koruma Kurulu'nun 16/10/2018 Tarihli ve 2018/119 Sayılı İlke Kararı, ayrıntılı bilgi için bakınız: "https://kvkk.gov.tr/Icerik/5299/2018-119" [E.T: 16.03.2019]
[193] "Kişisel Verileri Koruma Kurulu'nun 05/12/2018 Tarihli ve 2018/143 Sayılı Kararı", ayrıntılı bilgi için bakınız: "https://kvkk.gov.tr/Icerik/5364/2018-143" [E.T: 16.03.2019]
[194] Küzeci, *Kişisel Verilerin Korunması*, s. 212.
[195] Dülger, *Verilerin Korunması*, s. 121.

üzerindeki denetim yetkisini kaybedecektir[196]. Kurum da yayınlamış olduğu rehberde, veri sorumlularının ilgili kişiye belirttikleri amaçlar dışında başka amaçlarla veri işlemeleri halinde, bu fiillerinden dolayı sorumluluklarının doğacağını ifade ederek bu konunun Kanun açısından uygulama yöntemini ortaya koymuştur[197]. Ve fakat, Türk kişisel verilerin korunması hukukunda bu ilkeye yönelik olarak kanuni bir alt yapının sağlanmaması, Kanun gerekçesinde bu konuya değinilmemiş olması ve yalnızca Kurum rehberleri ile konunun değerlendirilmiş bulunması bizim de katıldığımız şekilde eleştirilmiştir[198]. İlgili kişinin, temel haklarından olan kişisel verilerin korunması hakkının korunması adına bu hususun kanuni bir düzenleme ile belirlenmesi ve kanuni temele oturtulması uygun olacaktır.

2.3.2.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olmak

Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi, "*işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını*" ifade etmektedir[199]. "İşlenen veri, sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulacak olup, veri sorumlusu tarafından işlenen veriler toplanma ve/veya bunu izleyen işlenme amaçları bakımından yeterli ve onlarla ilgili olacak ve aşırı olmayacaktır"[200].

Kanun'da bu ilkeyi somutlaştıracak nitelikte bir düzenleme bulunmamakta ise de Kanun'un Yönerge dikkate alınarak hazırlandığı ve 108 sayılı Sözleşme'nin de Kanun üzerinde etkisi bulunduğu dikkate alındığında, bu düzenlemelerde, bu ilkeye dair ifade edilen hususların, Türk Hukuku bakımından da dikkate alınabileceği ve uygulanabileceği kanaatindeyiz. Bu bağlamda, bu ilke, verilerin toplanma anından

---

[196] Küzeci, *Kişisel Verilerin Korunması*, s. 213.
[197] Kişisel Verileri Koruma Kurumu, "KVKK Temel İlkeler", s. 7.
[198] Dülger, *Verilerin Korunması*, s. 122.
[199] Kişisel Verilerin Korunması Kanunu, Genel Gerekçe s. 7-8.
[200] Avrupa Birliği Veri Güvenliği Yönergesi, m. 6/1 (c).

itibaren dikkate alınacak[201] ve verilerin saklanma amaçları ortadan kalktığında veya verilerin bu amaç bakımından artık gerekli olmadığı durumlarda veriler silme, yok etme veya anonimleştirme usullerine göre veri sisteminden çıkartılacaktır[202,203]. Bu doğrultuda, veri işlemeye ilişkin ilkeler işlevsel bir şekilde uygulanmalı ve bu doğrultuda gerekli teknik ve organizasyonel önlemler alınmalıdır [204].

Farklı yerlerde, farklı kavramlarla[205] karşılık bulan bu ilke, veri sorumlusunun, belirlediği amaçlara ulaşabilmek için işlenecek verinin gerekli olup olmadığını kesin surette irdelemeli ve eğer veri gerekli değil ise bu veriyi işlememe yoluna başvurmalıdır[206]. Kimi kaynaklarda "veri ekonomisi" olarak da ifade edilen bu işlem kapsamında, veri sorumlusu amaca ulaşmak adına en az miktarda veriyi kullanmalı/işlemeli, gereksiz olan veri kullanılmamalı ve veri kullanımı gerekli olduğu ölçüde sınırlandırılmalıdır[207]. Veri sorumlusu, söz konusu "*veri tasarrufu*"nu veri işlediği her aşamada gözetecek ve her işleme için ayrı ayrı değerlendirerek, gereklilik ilkesi ışığında veriyi işleyecektir.

İlke kapsamında değerlendirilmesi gereken diğer bir husus ise amaçla bağlılık ve amacın sınırlandırılması hususlarıdır. Bu doğrultuda, ilke ışığında kişisel veriler ile işlenmeleri üzerine öngörülen amaç arasında bağlantı olmalı ve amaç ve kişisel verinin niteliğinin birbiriyle ilişkisi olmalıdır[208]. Yine, kişisel veriler işlenirken, işlenme amacı ile sınırlı tutulmalıdır. GVKT'de amacın sınırlandırılması olarak da ifade edilen bu ilke ışığında, veri sorumlusu yalnızca belirlediği amaç ışığında işleme gerçekleştirebilecek ve her türlü amaç için veri işlemesi söz konusu olmayacaktır. Bu yönüyle, amaçla sınırlılık ilkesinin, meşruluk ilkesi ile doğrudan bağlantılı olduğu da ifade edilmelidir.

---

[201] Bygrave, *Data Privacy Law*, s. 60.
[202] Avrupa Birliği Veri Güvenliği Yönergesi, m. 6.
[203] Voigt ve Von Dem Bussche, *GDPR*, s. 91.
[204] Çekin, *Kişisel Verilerin Korunması*, s. 53.
[205] Carey, *Data Protection Guide*, s. 55; Kuner, *European Data Protection Law*, s. 73-74; Bygrave, *Data Privacy Law*, s. 60.
[206] Çekin, *Kişisel Verilerin Korunması*, s. 53.
[207] Küzeci, *Kişisel Verilerin Korunması*, s. 214.
[208] Dülger, *Verilerin Korunması*, s. 125.

Türk Hukuku uygulamasında da bu ilke ışığında, Kurul'un resmi sitesinde kamuoyu ile paylaşılan karar özetleri irdelendiğinde, verilen bir kararda, "işlenme amacının gerektirdiğinden fazla kişisel veri işlenmesi/aktarılması ve veri minimizasyonu ilkesine aykırılık sebebiyle veri sorumlusuna Kurul tarafından idari para cezası verildiği" görülmektedir[209]. Karar kapsamında, "*mahkemece veri sorumlusundan ilgili kişi hakkında bazı kişisel verilerin talep edilmesi ve veri sorumlusunun gereğinden fazla kişisel veri aktarımında bulunması neticesinde, veri sorumlusunun, verilerin işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık oluştuğu ve bu sebeple, ilgili kişiye ait kişisel verilerin güvenliğini sağlayamayan veri sorumlusu adına idari yaptırım uygulandığı*" ifade edilmiştir.

Bu karar yalnızca örnek niteliğinde olup; uygulamada bu ilkeyle bağlantılı olarak veri sorumluları tarafından sıklıkla ihlaller gerçekleştirildiği görülmektedir[210]. Özellikle iş hukuku ilişkilerinde karşılaşılan bu ihlallerde, veri sorumluları genellikle işçiden alması gerektiğinden nitelik ve nicelik olarak çok daha fazla veri talep etmektedir[211]. Örneğin, işverenler, gereği olmamasına rağmen, çalışan adaylarından, "*hangi gazeteyi okudukları*", "*daha önce hangi işyerinde, hangi görevde ve hangi maaşla çalıştıkları*", "*eşlerinin çalıştıkları yer ve aldığı maaş*" gibi bilgileri talep edebilmektedir. Bu tür bilgi talepleri, işe alım sürecinde gerekli olmadıkları gibi, işverenin çalışan adayları bakımından belirleyeceği herhangi bir amaç ve/veya gerekçe ile de açıklanamayacak nitelikteki taleplerdir. İşverenler bakımından, özellikle Türk Hukuku kapsamında bu tür bilgiler, çalışanların rızası dahi alınmaksızın işlenmekte olup, bu durumun amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık oluşturduğu aşikardır.

---

[209] Kişisel Verileri Koruma Kurulu'nun "*İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)*" başlıklı kararı, ayrıntılı bilgi için bakınız: "https://kvkk.gov.tr/Icerik/4214/Kurul-Kararlari" [E.T: 16.03.2019]

[210] Küzeci, *Kişisel Verilerin Korunması*, s. 215-219.

[211] Gürsel, *İşçinin Kişisel Verileri*, s. 179.

2.3.2.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Edilmek

Bu ilke, kişisel verilerin korunması hukukunun temel değerleri bakımından çok önemli ve bu değerler ile yakından ilişkilidir[212]. Bu ilkeye göre, "*kişisel veriler, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilecektir ve veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uygun hareket edecek; aksi durumda verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir*"[213]. Kişisel verinin, işlenme amacı ortadan kalktı ise veya daha fazla saklanması için geçerli bir sebep bulunmuyorsa, veri silinmeli, anonim hale getirilmeli veya yok edilmelidir. "*Bir gün işe yarayabilir*" düşüncesiyle verinin saklanması, bu ilkeye aykırılık oluşturmaktadır. Bu noktada ifade etmek gerekir ki, veri işleme amacının sona ermesinin yanında, veri işleme amacının ortadan kalkması, veya bu amacın gereksiz duruma gelmesi gibi hallerde de söz konusu ilke devreye sokulmalıdır[214].

Bu ilke bakımından, verinin silineceği, anonimleştirileceği veya yok edileceği zamanın belirlenmesi büyük önem arz etmektedir. Bu süre, farklı mevzuatlarda belirlenen süreler ile sınırlandırılabileceği gibi, veri sorumlusu bu süreyi kendisi de belirleyebilir. Bu sürenin makul bir süre olması gerekmektedir[215]. Makul süre yönünden, Kanun ve alt düzenlemelerde, farklı konularda farklı sürelerin belirlendiği de görülmektedir[216]. Bu ilkenin, veri sorumlusu tarafından gerçekleştirilmesi ve takibi zor gibi gözükmekte ise de özellikle uygulamada sıklıkla karşımıza çıkan saklama ve imha politikaları, arşivleme yönergeleri ile bu ilkenin gerçekleştirilmesi mümkün olmaktadır.

---

[212] Küzeci, *Kişisel Verilerin Korunması*, s. 221.
[213] Kişisel Verilerin Korunması Kanunu, Genel Gerekçe s. 8.
[214] Dülger, *Verilerin Korunması*, s. 136.
[215] Dülger, s. 136.
[216] Örnek için bakınız: "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*", m. 11.

Bu ilke, AİHM kararlarına konu olduğu gibi[217] Kurul'un da bu konuda kararları mevcuttur. Kurul tarafından, bu ilke ışığında verilen karar kapsamında, "*veri sorumlusunun, hâlihazırda aktif olmayan müşterisinin (ilgili kişi) kişisel verilerinin silinmesi hususundan talebini yerine getirmediği belirtilmiş ve bu sebeple, veri sorumlusunun tabi olduğu mevzuat uyarınca işlediği kişisel verileri 10 yıl boyunca muhafaza etmesi zorunluluğu bulunduğundan, Kurul tarafından aktif olmayan müşterilerin kişisel verilerinin, Kanun'un 4 üncü maddesinde yer verilen genel ilkelere uygun olarak saklama amacı dışında işlenmemesi gerektiği yönünde veri sorumlusunun talimatlandırılmasına*" karar verilmiştir[218]. Bu bakımdan, veri sorumlularının, söz konusu saklama sürelerine, politikalarında ve veri envanterlerinde yer vermesi gerektiği ve bu sürelere kesin surette uyması gerektiği açıktır.

2.3.3. Kişisel Verilerin İşlenme Koşulları

"Anayasa"da düzenlemesini bulan "kişisel verilerin korunması hakkı" bakımından, yine Anayasa m. 20 aracılığıyla kişisel verilerin işlenme şartları anayasal temele oturtulmuş ve "*kişisel verilerin ancak kanunda öngörülen hallerde ve kişinin açık rızasıyla işlenebileceği*" düzenlenmiştir. Bu düzenleme ışığında, kişisel verilerin işlenmesinin kural olarak yasak olduğu ancak belli durumlarda işlenebileceği söylenebilecektir[219]. Söz konusu Anayasa düzenlemesinin, Kanun'a yansıması ise Kanun'un 5. maddesi ile olmuştur. Yine Kanun'un 6. maddesi aracılığıyla ise "özel nitelikli kişisel veriler" bakımından ayrı şartlar da öngörülmüştür. Yine, Kanun'un 28. maddesinde düzenlenen ve Kanun kapsamında değerlendirilemeyecek hususlar da veri işleme bakımından hukuka uygunluk sebebi olarak görülebilir[220]. Son olarak, TMK m. 24/2 ve TBK m. 63 ve 64'de düzenlenen genel hukuka uygunluk sebepleri de veri işleme bakımından dikkate

---

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

[218] Kişisel Verileri Koruma Kurulu'nun "*İlgili Kişinin Kişisel Verilerinin Silinmesi Talebinin Yerine Getirilmemesi*" başlıklı kararı, ayrıntılı bilgi için bakınız: "https://kvkk.gov.tr/Icerik/4214/Kurul-Kararlari" [E.T: 16.03.2019]; Ayrıca bknz. "*İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi gereğince kişisel verilerin silinmemesi hakkında* başlıklı Kişisel Verileri Koruma Kurulu'nun 05/12/2018 tarihli ve 2018/142 sayılı Kararı." "https://kvkk.gov.tr/Icerik/4214/Kurul-Kararlari" [E.T: 16.03.2019]

[219] Çekin, *Kişisel Verilerin Korunması*, s. 54.

[220] Taştan, *Kişisel Verilerin Korunması*, s. 150.

alınabilecek nitelikteki hukuka uygunluk sebepleridir. Nitekim, genel hukuka uygunluk sebepleri, niteliğine uygun düştüğü ölçüde, her alanda uygulanabilecektir[221].

Veri işleme şartları bakımından dikkat edilmesi gereken bir husus da, işlenme şartlarının, verilerin işlenme ilkelerinden ayrı ve bağımsız düşünülemeyeceğidir. Nitekim kişisel verilerin işlenmesi şartları ve işlenme ilkeleri birbirine sıkı sıkıya bağlı ilke ve şartlardır.

Belirtmek gerekir ki, veri özel nitelikli olsun veya olmasın kanun koyucu ilgili kişinin açık rızasını aramakta olup, açık rızanın olmadığı hallerde ise başka hukuka uygunluk sebepleri aranmaktadır[222].

2.3.3.1. Açık Rıza

Kanunun 5. maddesinde kişisel verilerin hangi hallerde hukuka uygun olarak işlenebileceğine ilişkin veri işleme şartları düzenlenmiştir. Bu doğrultuda kişisel veriler Kanun'da tahdidi olarak sayılan hukuka uygunluk sebepleri saklı kalmak üzere, yalnızca kişinin açık rızası ile işlenebilmektedir[223].

Bu doğrultuda, açık rıza, "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" şeklinde tanımlanabilir[224]. "Açık rıza" kavramında, kişinin verilerinin işlenmesine ilişkin olarak açık onay vermesinden önce, veri sorumlusu kişi, verilerin işlenme nedenleri, amaçları ve veri işleme prosedürü ile ilgili olarak kişiyi gereği gibi aydınlatmalı, bilgilendirmeli ve ilgili kişi buna göre özgür iradesi ile ve yalnızca belirli bir konu ve amaç için kişisel verisinin işlenmesine açık rızasını vererek müsaade etmelidir[225]. Açık rızanın yazılı şekilde alınması şart olmamakla birlikte, ispat

---

[221] Taştan, s. 150.
[222] Çekin, *Kişisel Verilerin Korunması*, s. 54.
[223] Çekin, s. 54.
[224] "*Handbook on European Data Protection Law*", s. 55.
[225] Gürsel, *İşçinin Kişisel Verileri*, s. 198-199.

kolaylığı bakımından açık rızanın yazılı şekilde alınması yolunun tercih edilmesi mümkündür[226].

GVKT'de ise rıza kavramı, ilgili kişinin isteklerinin özgür, somut, bilgilendirmeye dayalı ve kesin olan her türlü gösterge olarak tanımlanmış ve kişisel verinin ancak kişinin bir ifade ya da olumlu eylem sayesinde kendisiyle ilgili kişisel verinin işlenmesini kabul edebileceği düzenlenmiştir ***(Genel Veri Koruma Tüzüğü, m. 4)***. Kanun'da yapılan açık rıza düzenlemesinin, GVKT'de ve GVKT gerekçesinde düzenlendiği şekilde tanımlanmaması ve somut tanımlama bakımından içinde problemler barındırması sebebiyle özellikle internet siteleri aracılığıyla alınan rızalarda uygulamada kafa karışıklıkları oluşmakta, rızanın nasıl alınacağı sorgulanmakta ve bu hususların doldurulması, Kurul tarafından hazırlanan rehberler veya verilecek kararlara bırakılmaktadır. İnternet siteleri kapsamında alınan rızalar yalnızca örnek niteliğinde olup, işçilerin rızasının alınması, somut olarak hangi durumlarda ilgili kişinin rızasına başvurulacağı, çocuktan alınacak rızalar gibi konular ve pek çok diğer konuda da, Kanun'da düzenlemeler bulunmaması sebebiyle boşluklar ve sıkıntılar oluşmaktadır. GVKT düzenlemesinde ise açık rızanın yazılı olarak, elektronik ortamda ya da sözlü verilmesinin mümkün olacağı ayrıca ifade edilmektedir[227].

Açık rızanın esas olarak ve tanımdan da hareketle; "*belirli bir konuya ilişkin olma, bilgilendirmeye dayanma ve özgür iradeyle açıklanmış olma*", şeklinde üç temel unsurdan oluştuğu söylenebilir[228].

"Rızanın belirli bir konuya ilişkin olması", verilen rızanın sınırları belli bir konuda verilmesi anlamını taşımakta olup söz konusu durum, verilerin belirli ve açık amaçlar için işlenmesi ilkesi ile doğrudan bağlantılıdır[229]. Bu bağlamda, "şemsiye rıza" olarak da ifade edilen, belirli amaçlar için alınmamış, çok geniş kapsamlı konuları kapsayacak

---

[226] Gürsel, s. 195.
[227] Çekin, *Kişisel Verilerin Korunması*, s. 55.
[228] Taştan, *Kişisel Verilerin Korunması*, s. 152.
[229] Taştan, s. 153.

şekilde alınan genel rızaların Kanun bakımından bir geçerliliği bulunmamaktadır[230]. Rızanın belirli bir konuda verilebilmesi için, kişiye yöneltilecek rıza beyan formlarının açık, anlaşılır ve öz bir şekilde olması gerekmektedir[231]. Örnek olarak, Şirket tarafından ziyaretçilerini aydınlatma amacıyla hazırlanan bir aydınlatma metninde, "*Kişisel verileriniz, ziyaretiniz kapsamında, Şirket'in santrallerinde veya Şirket içinde KVKK ve başkaca kanunlar bakımından gerekli güvenlik önlemlerinin alınması ve sizlerden gelen talep ve şikayetlerin değerlendirilerek çözüme kavuşturulması amaçlarıyla, ilgili amaçların gerektirdiği ölçü ve zaman dilimi boyunca işlenmekte ve muhafaza edilmektedir.*" ifadelerinin bulunması amacı açıkça ifade etmekte ve amacı da sınırlamaktadır. Bu bağlamda, kişi tarafından bu konuya ilişkin verilecek rıza kanımızca geçerli olacaktır.

Bilgilendirmeye dayanma ise, rızaya ilişkin olarak işlemenin amacının, işleme süresinin, verinin toplama yöntemi, kişinin hakları gibi hususlarda ilgili kişiye veri sorumlusu tarafından bilgi verilmesi anlamını taşımakta olup, bu durum aşağıda ayrıntısıyla açıklanacağı şekilde veri sorumlusunun aydınlatma yükümlülüğünün de bir parçasıdır. Kısaca, kişinin, kendisini veri işleme bakımından etkileyebilecek tüm hususlar hakkında bilgilendirilmesi gerekmektedir[232] Bu kapsamda, bilgilendirmenin sıradan bir kullanıcının[233] anlayacağı şekilde basit bir dille yapılması ve bilginin erişilebilir ve görülebilir nitelikte olması gerekmektedir[234].

Rızanın özgür iradeyle açıklanmış olması ise kişiye gerçek anlamda bir tercih imkanı sunulması, rıza vermemenin sonucu olarak kişinin rıza vermedeki tercih hakkının kısıtlanmaması olarak ifade edilebilir. Bu bağlamda, örneğin, bir hizmetin sunulmasının rıza şartına bağlandığı hallerde, bu rıza geçerli bir rıza olmayacaktır[235]. Uygulamada zaman zaman bu uygulamalar ile karşılaşılmakta ise de kanımızca bir hizmetin sağlanmasının kişinin rızası şartına bağlanması, Kanun'un ve kişisel verilerin

---

[230] Kişisel Verileri Koruma Kurumu, "KVKK Soru Cevap", s. 25.
[231] Taştan, *Kişisel Verilerin Korunması*, 152; Çekin, *Kişisel Verilerin Korunması*, s. 56.
[232] Taştan, *Kişisel Verilerin Korunması*, s. 155.
[233] Altaş, *Başlangıç Hükümleri*, s. 263.
[234] "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 29.
[235] Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenme Şartları", s. 6.

korunması hakkının özüne aykırılık teşkil edecektir. Örneğin, internet üzerinde elektronik ticaret işlemi yürütmekte olan bir internet sitesinin, hizmetlerini sunmak için kişinin rızasını şart koşması ve bunu da onlarca sayfadan oluşan bir rıza beyanı aracılığıyla elde etmesi kesinlikle geçerli bir rıza olmayacaktır. Yine, korkutma ve baskıyla alınan bir rıza beyanı da geçerli olmayacaktır[236]. Ve fakat belirtmek gerekir ki, bu kapsamda veri sorumlusu ve ilgili kişi arasında bir menfaat dengesinin kurulması gerekliliği ticari hayatın zorunluluğu olduğu gibi aynı zamanda kaçınılmazdır. Hizmetin önkoşul olarak kabul görmemesi durumu, hizmetin çok geniş anlamda yorumlanmasını gerektirmez. Örneğin, "*veri sorumlusunun sunduğu ürün veya hizmetin, asıl hizmeti hiçbir şekilde engellemediği ve sunulan hizmetin alınması zorunlu bir hizmet olmadığı ve ilgili kişiler açısından zorunlu tutulmadığı*" hallerde ilgili kişiden rıza almak zorunluluğunu ileri sürmek ve rıza almaksızın bu hizmeti vermemek veri ihlali oluşturmayacaktır[237].

Ayrıca, açık rıza bakımından, kişinin aktif bir eylemi gerekmekte olup bu doğrultuda, örneğin daha önceden varsayılan olarak işaretlenmiş kutucuklar aracılığıyla elektronik ortam üzerinden alınan kişinin rızası da geçerli olmayacaktır[238]. Hülasa, kişinin Kanun kapsamında örtülü olarak verdiği rıza veya susma halinde, bu rıza geçerli bir rıza olmaz[239]. Rızanın geçerliliği, ilgili kişinin açık, bilgilendirmeye dayanan, özgür iradeyle ve aktif bir eylemle verilmiş beyanına bağlıdır.

Rıza bakımından bir önemli konu da rıza gösteren kişinin muhakkak surette ayırt etme gücüne sahip olmasıdır[240]. Bu bağlamda, hukuki işlem ehliyeti ve ayırt etme gücüne sahipliğin birbiri ile karıştırılmaması gerekmektedir. Hukuki işlem ehliyeti, açık rızanın geçerlilik şartı değildir[241]. Türk Hukuku'nda, bu bakımdan bir yaş sınırı getirilmemiş ve konu hukuki boşluk olarak durmakta ise de, GVKT'de, küçüklerin kişisel verilerinin

---

[236] Gürsel, *İşçinin Kişisel Verileri*, s. 200.

[237] "Kişisel Verileri Koruma Kurulu'nun *bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında* başlıklı 25/03/2019 tarihli ve 2019/82 sayılı Kararı". Ayrıntılı bilgi için bakınız: "https://www.kvkk.gov.tr/Icerik/5463/" [Erişim tarihi: 30.05.2019]

[238] "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 35-36.

[239] Çekin, *Kişisel Verilerin Korunması*, s. 58.

[240] Akipek, Akıntürk ve Ateş Karaman, *Kişiler Hukuku*, 1: s. 283.

[241] Çekin, *Kişisel Verilerin Korunması*, s. 57.

işlenmesine ilişkin detaylı düzenlemeler bulunmaktadır. Öyle ki, GVKT'nün ilgili maddesine göre, 16 yaşından küçüklerin kişisel verilerinin işlenmesi için velisinin ya da vasisinin rızası gereklidir ***(Genel Veri Koruma Tüzüğü, m. 8)***. Küçüklerin kişisel verilerinin işlenmesine ilişkin özel bir düzenleme getirilmesi ihtiyacı, onların özellikle korunmaya muhtaç olmasından kaynaklanmakta[242] olup, KVKK'da küçüklerin kişisel verilerinin işlenmesine ilişkin herhangi bir özel düzenleme getirilmemiş olması toplumsal olarak önemli problemlerin ortaya çıkmasına sebep vermektedir[243]. Öyle ki, çocuk yaşta kendisine ait bilgileri bilinçsiz bir şekilde paylaşan bir çocuk, daha sonra bu verilerle ömrü boyunca yüzleşmek zorunda kalabilmektedir[244]. Küçüklerin kişisel verilerinin işlenmesine ilişkin sorunların da kişilik haklarına ilişkin tartışmalar çerçevesinde çözümlenmesi gerektiğine dair görüşler[245] var ise de çocuklar açısından mevcut olan riskler de dikkate alınarak ve çocuğun rıza açıklamasının sonuçlarını öngörebilecek nitelikte olup olmadığı hususu da dikkate alınmak suretiyle bu konuda kısa süre içinde düzenleme yapılması gerekmektedir[246].

Rıza beyanının şekli bakımından, Kanun'da öngörülmüş bir şekil şartı bulunmamaktadır. Bu bakımdan, rızanın yazılı şekilde verilmesi gerekmemektedir. Açık rızanın unsurlarını taşıması kaydıyla rıza her türlü yöntemle alınabilir. Bu bakımdan, ispat yükü veri sorumlusu üzerinde bulunmakta olup veri sorumlusu rıza beyanını aldığını ispat etmekle yükümlüdür.

Son olarak, açık rıza kavramı değerlendirilirken, yukarıda tanımlaması yapılan özel nitelikli kişisel verilerin ayrıca irdelenmesi gerekmektedir. Öyle ki, Kanun, bu verilere, bu veriler ile ilgili ayrımcılık riski bulunmasından dolayı özel bir önem atfetmiş ve bu verilerin işlenmesi bakımından özel şartlar öngörmüştür[247]. Kanun m. 6'ya göre, "*ilgili kişinin açık rızası bulunmaksızın özel nitelikli kişisel verilerin işlenmesi kural olarak yasaklanmıştır*". Özel nitelikli kişisel veriler işlenirken Kanun m. 5'teki hukuka

---

[242] Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu", s. 767.
[243] "GDPR and Children's Rights", s. 2-7.
[244] Çekin, *Kişisel Verilerin Korunması*, s. 63.
[245] Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu", s. 769.
[246] Benzer görüş için bakınız: Çekin, *Kişisel Verilerin Korunması*, s. 63.
[247] Taştan, *Kişisel Verilerin Korunması*, s. 159.

uygunluk nedenleri uygulanmayacaksa da m. 6 kapsamında özel nitelikli kişisel verilerin işlenmesi bakımından hukuka uygunluk nedenleri ayrıca düzenlenmiştir. Bu kapsamda, verilerin işlenme şartları bakımından, açık rıza dışındaki hukuka uygunluk nedenleri, veri sorumluları bakımından büyük önem arz etmektedir.

2.3.3.2. Diğer Hukuka Uygunluk Nedenleri

Kanun'un 5. maddesinin ikinci fıkrası uyarınca, kişinin açık rızası olmasa dahi bazı hallerde kişisel verilerin işlenebilmesi mümkündür. Kişisel verilerin işlenme şartları (hukuka uygunluk halleri), Kanun'da sayma yoluyla belirlenmiş olup, bu şartların genişletilmesi veya yorum yoluyla yeni durumlar oluşturulması söz konusu olamaz. Açık rıza dışındaki durumlar, kısaca; "*işlemenin kanunlarda açıkça öngörülmesi, üstün özel yararın varlığı, sözleşmenin kurulması veya sözleşmenin ifasıyla ilgili olarak işleme, veri sorumlusunun hukuki yükümlülüğünü yerine getirmenin kişisel veriyi işlemeyi zorunlu kılması, kişisel verinin ilgili kişinin kendisi tarafından aleni hale getirilmiş olması, bir hakkın tesisi, kullanımı veya korunması için veri işlemenin zorunlu olması ve veri işlemenin veri sorumlusunun menfaati için zorunlu olması*" şeklinde ifade edilebilir[248].

Sayılan işbu hukuka uygunluk nedenlerinin varlığı halinde, kişiden açık rıza alınmasına gerek yoktur. Öyle ki, Kanun m. 5/2'ye göre "yukarıda ifade edilen şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür". Kurul da, konuya ilişkin olarak yayınlamış olduğu rehberde, "*veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün ise bu faaliyetin, bu şekilde yürütülmesi gerektiğini; aksi takdirde, söz konusu işlemenin, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağını ve ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesinin hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına geleceğini*" ifade etmiştir[249].

---

[248] Taştan, *Kişisel Verilerin Korunması*, s. 152-168.

[249] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 71.

Açık rıza da dahil olmak üzere, kişisel verilerin işlenme şartları her bir kişisel veri işleme faaliyetinin amacının Kanun bakımından hukuki dayanağını oluşturmakta olup veri sorumlusu, açık rıza dışındaki hukuka uygunluk nedenlerinin varlığı halinde ise ilgili kişinin açık rızasını almaksızın veri işleme faaliyetini gerçekleştirecektir.

2.3.3.2.1. İşlemenin Kanunlarda Açıkça Öngörülmesi

Veri işleme faaliyetinin kanunlarda açıkça öngörülmüş olması, Kanun m. 5/2 (a) altında yer almakta olup buna göre, veri sorumlusunun, kişisel verileri işleme faaliyetine yönelik olarak kanunlar altında yükümlülüklerinin bulunması veya veri sorumlusunun görevlendirildiği veya yetkilendirildiği hallerde[250], veri sorumlusu, ilgili kişinin rızasını almaksızın veri işleme faaliyetini gerçekleştirebilecektir. İşçi-işveren ilişkisinde, "İş Kanunu" ve "Sosyal Güvenlik Kanunu"nda düzenlenen özlük dosyası tutma yükümlülüğü, bu konuda verilecek en iyi örneklerden biridir.

İşbu hukuka uygunluk nedeni açısından ifade etmek gerekir ki, veri sorumlusunun yorumuna açık mevzuat düzenlemelerinde nasıl bir yöntem belirlemesi gerektiğine yönelik Kanun'da herhangi bir düzenleme bulunmamaktadır. Bu durum, özellikle iş hukuku uygulamalarında önemli sorunlar yaratmaktadır. Özellikle, işverenler, özlük dosyası tutma kapsamının içinde, yapılacak işin niteliğine bağlı olarak o işte çalışılabileceğine dair sağlık raporunu ve ilgili sağlık testlerini de İş Sağlığı ve Güvenliği mevzuatına göre tutmanın gerekli olabileceği düşüncesiyle, ilgili verileri işçinin rızasını almaksızın tutabilmektedirler. Buna karşın, sağlık verilerine ilişkin olarak, aşağıda ayrıntısıyla açıklanacağı üzere, özel veri işleme şartları bulunmakta olup, ilgili yükümlülük kanunlarda belirlenen bir yükümlülük olmasına rağmen sağlık verisi olması hasebiyle Kanun'daki şartlara uygun olarak işçinin açık rızasıyla özlük dosyasında tutulmalıdır. Belirtmek gerekir ki, bu durumda da işverenler bakımından uygulamada önemli sorunlar oluşmakta ve işveren ticari faaliyetini verimli bir şekilde

[250] Benzer görüş için bknz. Dülger, *Verilerin Korunması*, s. 216.

sürdüremez hale gelmektedir. Bu konunun Kanun altında çıkarılacak yönetmelikler aracılığıyla somutlaştırılması ve bu şekilde veri sorumluları ile ilgili kişi arasında menfaat dengesi kurulması gerektiği düşüncesindeyiz. Bu gerçeklik bir yana, henüz Kanun altında uygulamaya yönelik olarak çok kısıtlı sayıda yönetmeliğin çıkarıldığı durum da dikkate alındığında, kanaatimiz veri sorumlularının, yoruma açık hukuk düzenlemelerini sınırlı bir şekilde kabul etmelerinin, yalnızca kanunlarda ifade edilen konularda veri işlemelerinin, somut duruma göre ve verinin niteliğine bağlı olarak ilgili kişilerden rıza almanın gerekli olup olmadığını değerlendirmelerinin ve kanunlardan açıkça anlaşılmayan işleme faaliyetlerini gerçekleştirmemelerinin uygun olacağı yönündedir[251].

2.3.3.2.2. Üstün Özel Yararın Varlığı

İlgili kişinin, "*fiili imkânsızlık sebebiyle rızasını açıklayamayacak durumda bulunması veya rızasına hukuki geçerlilik tanınamayacak durumlarda olması veya kendisinin ya da başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması hallerinde*", işbu hukuka uygunluk nedeni söz konusu olacaktır ve bu hallerde ilgili kişinin kişisel verileri, kişinin açık rızası olmaksızın işlenebilecektir.

"Hürriyeti kısıtlanan bir kişinin kurtarılması amacıyla kendisinin veya şüphelinin taşımakta olduğu telefon, bilgisayar, kredi kartı, banka kartı veya diğer teknik bir araç üzerinden yerinin belirlenmesi için bu verilerin işlenmesi", işbu hukuka uygunluk nedenine örnek olarak verilebilir[252].

2.3.3.2.3. Sözleşmenin Kurulması veya Sözleşmenin İfasıyla İlgili Olarak İşleme

"Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması koşuluyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin zorunlu olması halinde" işbu

---

[251] Dülger, s. 216.

[252] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 75.

hukuka uygunluk nedeni söz konusu olmaktadır. Bu doğrultuda, ilgili kişilerin bu amaçla sınırlı olmak üzere kişisel verilerinin işlenmesi mümkün olacaktır.

Söz konusu hukuka uygunluk nedeni, anayasal boyut çerçevesinde işaret edilen menfaatler dengesinin somutlaştırılmış hali olarak kabul edilmekte[253] olup işbu düzenleme ile hem veri sorumlusu hem ilgili kişinin haklı menfaatleri dikkate alınmış ve ilgili kişi ile veri sorumlusu arasında bir menfaat dengesi oluşturulmuştur. Taraflar arasında birden fazla sözleşme olması halinde her bir sözleşme bakımından ayrı ayrı değerlendirme yapmak ve veri işleme faaliyetini bu değerlendirmeye göre gerçekleştirmek uygun olacaktır[254].

Düzenlemenin içinde bulunan gereklilik kıstası ise yine veri işleme faaliyeti bakımından önem arz etmektedir ve bu bağlamda, verinin işlenmesinin sözleşmenin kurulması veya ifası için gerekli ve kaçınılmaz olması gerekmektedir[255]. Kira sözleşmesi kapsamında banka bilgileri gibi sözleşmenin ifası bakımından gerekli olan bilgilerin işlenmesi veya bankayla yapılan kredi kartı sözleşmesi kapsamında kart sahibinin maaş bordrolarında bulunan bilgilerin işlenmesi, hukuka uygunluk nedenine örnek olarak verilebilir.

2.3.3.2.4. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesinin Kişisel Veriyi İşlemeyi Zorunlu Kılması

Veri sorumlusunun, "Kanun dışında farklı yasal düzenlemelerden kaynaklanan hukuki yükümlülüğünü yerine getirebilmesi için veri işlenmesinin zorunlu olduğu durumlarda", işbu hukuka uygunluk nedeni geçerli olacaktır. Bir şirketin, asgari geçim indirimi ödemelerine ilişkin olarak, işçisine evli olup olmadığı, bakmakla yükümlü olduğu kaç kişi bulunduğu gibi sorular sonrasında elde ettiği veriler bakımından bu durum geçerli olacaktır. Bu kapsamda ifade etmek gerekir ki, hukuki yükümlülüğün

---

[253] Çekin, *Kişisel Verilerin Korunması*, s. 65.
[254] Çekin, s. 67.
[255] Çekin, s. 68.

hukuken veri sorumlusuna yüklenmiş olması gerekmekte[256] olup veri sorumlusunun sözleşmesel yükümlülüğünü yerine getirmesi için zorunlu olan hallerde ise işbu hukuka uygunluk nedeni dikkate alınmayacaktır[257]. Veri sorumlusunun hukuki yükümlülüğünü yerine getirmenin kişisel veriyi işlemeyi zorunlu kılması hali, Kanun m. 5/2 (a)'da düzenlenen işlemenin kanuni bir yükümlülükten kaynaklanması durumu ile iç içe geçmiş bir hukuka uygunluk nedeni olarak da kabul edilebilir.

2.3.3.2.5. Kişisel Verinin İlgili Kişinin Kendisi Tarafından Aleni Hale Getirilmiş Olması

İlgili kişi tarafından, kişisel verisinin aleni hale getirilmiş olması halinde ve ilgili kişisel veri kamuoyuna açık hale getirildiği durumda söz konusu kişisel veri işlenebilecektir[258]. Bu duruma örnek olarak, "kişinin araç satımı gerçekleştirilen bir internet sitesinde telefon numarasını ve adres bilgilerini paylaşması ve bu bilgilerini kamuya açık şekilde ilan etmesi" verilebilir.

Söz konusu hukuka uygunluk nedeni bakımından iki önemli hususa dikkat edilmesi gerekmektedir. Zira, özellikle "alenileştirme" ibaresinin yorumu, uygulama açısından önemli sonuçlar doğurmaktadır[259]. İlk olarak, kişisel verinin aleni olarak kabul edilebilmesi için "ait olduğu kişinin bu verinin aleni olmasını istemesi ve kişinin alenileştirme iradesinin varlığı" gerekmektedir. Yine, alenileştirme halinde kişisel verinin, "ilgili kişinin alenileştirme amacı dışında da kullanılmaması" gerekmektedir[260]. Bu amacın yorumlanmasında, geniş yorumdan kaçınılması ve kişinin veriyi alenileştirme nedeninin veri işlemede kıstas olarak kabul edilmesi gerekmekte olup kişi tarafından alenileştirilen veriler alenileştirmeye neden olan "amaç ile bağlantılı, sınırlı ve ölçülü olarak" işlenebilecektir[261].

---

[256] Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu", s. 778.
[257] Yücedağ, s. 778.
[258] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 76.
[259] Küzeci, *Kişisel Verilerin Korunması*, s. 347.
[260] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 77.
[261] Küzeci, *Kişisel Verilerin Korunması*, s. 348.

2.3.3.2.6. Bir Hakkın Tesisi, Kullanımı veya Korunması için Veri İşlemenin Zorunlu Olması

"Bir hakkın tesisi, kullanımı ve korunması için veri sorumlusu, veri işlemenin zaruriyetini değerlendirecek akabinde veri işlemenin gerekli olduğu durumlarda ve gerektiği ölçüde" kişinin açık rızasına ihtiyaç duymaksızın veriyi işleyebilecektir. Bu hüküm bakımından, bazı yazarlar, Kanun lafzının kavramsal yerindelik açısından, söz konusu hükmün, hak yerine hukuki talebin tesisi, kullanılması, korunması şeklinde yorumlanmasının daha yerinde olacağına işaret etmektedirler[262]. Kurul tarafından hazırlanan rehberde, işten çıkarılan ya da ayrılan bir çalışana ait gerekli bilgilerin dava zamanaşımı boyunca saklanmasının bu hukuka uygunluk nedenine örnek olarak verileceği ifade edilmişse de kapsamın bu denli geniş tutulmasının göz ardı edilmesinin doğru bir yaklaşım olduğu söylenemez[263]. Bu bağlamda, Kanun uygulamasının topluma ve veri sorumlularına doğru aktarılması bakımından kamusal sorumluluğa sahip olan Kurum'un, uygulamaya ilişkin daha somut örnekleri Rehber'lerine entegre etmesinin, toplumda kişisel verilerin korunması hakkına yönelik uygulamanın daha doğru ve problemsiz bir şekilde ilerlemesine fayda sağlayacağı düşüncesindeyiz.

2.3.3.2.7. Veri İşlemenin Veri Sorumlusunun Menfaati İçin Zorunlu Olması

"İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydı ile veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda, kişisel verilerin işlenmesi" hukuken mümkündür. Şirketin, "çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların çalışma koşulları ve özlük haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağılımında esas alınmak üzere çalışanların kişisel verilerinin işlenmesi" meşru menfaate örnek olarak verilebilir[264].

---

[262] Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu", s. 782.
[263] Küzeci, *Kişisel Verilerin Korunması*, s. 348.
[264] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 77.

Bu hukuka uygunluk nedeni ayrıntılı olarak irdelendiğinde, "*veri sorumlusunun meşru menfaatinin bulunması*" "*veri işlemenin zorunlu olması*" ve "*ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi*" ayrı ayrı değerlendirilmesi gereken hususlardır.

Veri sorumlusunun meşru menfaati, gerçekleştirilecek olan işlenme sonucunda elde edeceği çıkar ve fayda kapsamında değerlendirilmelidir. Meşru menfaat, hukuk düzeni içerisinde izin verilen her türlü hukuki, iktisadi ve kişisel menfaatse[265] de bu menfaatin kişisel verilerin işlenmesi bakımından açık ve somut bir kullanıma yönelik olması gerekmektedir. Bu somutluk, veri işleme faaliyetinin, veri sorumlusunun gerçekleştirdiği güncel aktivitelerle ilgili olması ve bu durumun veri sorumlusuna yakın zamanda fayda sağlaması olarak ifade edilebilir. "Veri sorumlusunun elde edeceği fayda; meşru, ilgili kişinin temel hak ve özgürlüğü ile yarışabilecek yeterli düzeyde etkin, belirli ve hali hazırda mevcut olan bir menfaatine ilişkin olmalıdır"[266].

Verinin işlenmesinin, meşru menfaatin gerçekleşmesi bakımından zorunlu olması da değerlendirilmesi gereken bir diğer kıstastır. Öyle ki, ilgili kişisel veri işlenmeksizin, menfaatin gerçekleşmesi mümkün ise veri işlememe yönünde takdir kullanılması uygun olacaktır.

Son ve en önemli kıstas ise ilgili kişinin temel hak ve özgürlüklerinin zarar görmemesi, bir başka ifade ile menfaat dengesidir[267]. "Veri sorumlusunun meşru menfaatinin olmasının yanı sıra, ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi" gerekliliği hukuka uygunluk nedeninin en kilit kıstasıdır. Bu doğrultuda, öncelikle, veri işlenirken, veri işleme faaliyeti bakımından ilgili kişinin temel hak ve özgürlüklerinin ne olduğu belirlenmeli ve daha sonra veri sorumlusunun menfaati ile bu temel hak ve özgürlükler arasında makul bir menfaat dengesi kurulmalıdır[268]. Veri

---

[265] Çekin, *Kişisel Verilerin Korunması*, s. 72.
[266] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 77.
[267] Çekin, *Kişisel Verilerin Korunması*, s. 73.
[268] Çekin, s. 73.

sorumlusunun meşru menfaatinin, ilgili kişinin hak ve menfaatleri ile karşılaştırması yapıldığında ilgili kişinin temel hak ve özgürlüğünün veri sorumlusunun meşru menfaatinden ağır basması halinde bu hukuka uygunluk nedeni uygulanamayacaktır[269].

Menfaat dengesi değerlendirmesi bakımından, "ilk önce veri sorumlusunun meşru menfaatinin varlığı tespit edilecek, daha sonra, bu menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar vermediği" belirlenecektir. Bu doğrultuda, veri sorumlusunun menfaatinin, ilgili kişinin temel hak ve özgürlükleri karşısında en azından eşit veya üstün gelmesi gerekmektedir. "Veri sorumlusunun meşru menfaati belirlenirken, gerçekleştirilecek olan işlenme sonucunda elde edilecek fayda da dikkate alınarak bir yorumlama yapılmalı, veri sorumlusunun elde edeceği fayda; meşru, ilgili kişinin temel hak ve özgürlüğü ile yarışabilecek düzeyde etkin, belirli ve hali hazırda mevcut olan bir menfaatine ilişkin olmalıdır"[270]. Menfaat dengesinin belirlenmesi bakımından yapılacak değerlendirmenin dayanağı ve kaynağı ise doğrudan ilgili kanuni düzenlemeler ve en başta Kanun'un amaç maddesi olan 1. maddesidir.

2.3.3.3. Özel Nitelikli Verilerin İşlenme Koşulları

Kanun'da, dünyadaki diğer örneklerine benzer olarak özel nitelikli verilere ayrı bir önem atfedilmiş ve ayrımcılık riskinin bertarafı bakımından özel nitelikli kişisel verileri Kanun'da ayrıca düzenlenmiştir. Bu doğrultuda, özel nitelikli kişisel verilerin işlenmesi bakımından da ayrı işleme şartları öngörülmüştür. Bunun nedeni, bu bilgi türlerinin, diğerlerine göre daha hassas nitelikte olması ve daha güçlü bir şekilde korunması gerekliliğidir[271].

Özel nitelikli veriler bakımından da temel kural, verinin işlenmesinin yasak olmasıdır. Bu durum, Kanun m. 6'daki *"Özel nitelikli verilerin, ilgili kişinin açık rızası olmaksızın*

---

[269] Çekin, s. 74.
[270] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 80.
[271] Küzeci, *Kişisel Verilerin Korunması*, s. 350.

işlenmesi yasaktır." ibaresi ile de sabittir. Bu veriler bakımından, ilk hukuka uygunluk nedeni açık rızadır. Açık rıza olmaksızın işlenebilme halleri bakımından ise Kanun ikili bir ayrıma gitmiş ve sağlık ve cinsel yaşama ilişkin veriler ile diğer özel nitelikli veriler için farklı bir rejim öngörülmüştür[272].

Bu ayrıma göre, Kanun m. 6/2 kapsamında, sağlık ve cinsel hayata ilişkin veriler dışındaki veriler, yani ırk, dini ve felsefi inanç, biyometrik ve genetik veriler gibi hassas veriler, kanunda öngörülen hallerde kişinin açık rızası aranmaksızın işlenebilecektir. Kanun'da ifade edilen "kanunda öngörülmesi" halinin, Kanun m. 5/2 (a)'daki "açıkça" ibaresini içermemesi eleştiri konusu[273] yapılmış ve ilgili düzenlemedeki eksikliğin hassas veriler için daha güçlü koruma ilkesine zarar verici nitelikte olduğu ifade edilmişse de bu konudaki görüşümüz, gerek Kanun'un bu verilere özel bir önem atfederek ayrı bir madde ile özel koruma altına almış olması gerekse Kurul tarafından yayınlanan rehberlerin özel nitelikli veriler bakımından ayrı ve yüksek düzeyde koruma alınması gerektiğine yönelik ibareler içermesi sebepleriyle, Kanun m. 6'daki "kanunda öngörülmesi" ibaresinin dar yorumlanması gerektiği ve özel nitelikli verilerin ancak kanunlarda açıkça öngörülmesi halinde açık rıza olmaksızın işlenebileceği yönündedir. Kanun m. 6'nın son fıkrasında yer alan *"özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması"* şartı da bu görüşümüzü desteklemekte olup, söz konusu hüküm ile özel nitelikli veriler bakımından Kanun yüksek koruma yönünde yorum ve işlem yapılması şeklinde düzenlenmiş bulunmaktadır.

"Sağlık ve cinsel hayata ilişkin kişisel veriler bakımından ise Kanun'da ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar

---

[272] Küzeci, s. 353.

[273] Küzeci, *Kişisel Verilerin Korunması*, s. 353.

tarafından ilgilinin açık rızası aranmaksızın işlenebileceğine yönelik bir ibare bulunmaktadır". Söz konusu düzenleme, pek çok haklı eleştiriye konu olmuştur[274].

İlk olarak, bu veriler için yasa ile korunma durumunun öngörülmemiş olması ve amaçların bu denli geniş tutulması, güçlü bir şekilde korunması hedeflenen sağlık ve cinsel hayata ilişkin verilerin kısmen korunmasına yol açmaktadır[275]. Uygulama bakımından ise Kanun ile öngörülmeyen esas ve usullerin, yönetmelik ve tüzük gibi düzenleyici işlemlerle gerçekleştirilmiş olması ve bu konuda hazırlanan yönetmeliklerin[276] Kanun ile farklı usul ve esaslar belirlemesi, Anayasa m. 13 ve 20/3'e aykırılık teşkil etmektedir[277].

İşbu maddenin, ayrıca, Anayasa m. 90/5'e de aykırılık oluşturduğu kanaatindeyiz. Öyle ki, ilgili maddeye göre, "*usulüne göre yürürlüğe konulmuş Milletlerarası Andlaşmalar kanun hükmünde olup, usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin Milletlerarası Andlaşmalar ile kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda Milletlerarası Andlaşma hükümlerinin esas alınacağı*" ifade edilmiştir. 108 sayılı Sözleşme, usulüne uygun olarak yürürlüğe girmiş olan ve Türkiye'nin taraf olduğu bir Milletlerarası Andlaşma olup, 108 sayılı Sözleşme m. 9'da özel nitelikli veriler bakımından istisnalar belirlenmiştir. Belirlenen bu istisnalar, "*devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi, ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması*" şeklindedir. Söz konusu istisnaların ve düzenlenen konunun, temel hak ve özgürlüklerden olan kişisel verilerin korunması hakkı ile ilgili olduğu dikkate alındığında, Kanun m. 6/2 düzenlemesinin, 108 sayılı Sözleşme'deki istisna durumları genişlettiği ve bu durumun da Anayasa m. 90/5'e aykırılık oluşturduğu sarih bir gerçekliktir.

---

[274] Örneğin; Küzeci, s. 249 vd.; Dülger, *Verilerin Korunması*, s. 215 vd.

[275] Küzeci, *Kişisel Verilerin Korunması*, s. 353.

[276] "*Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik*" hakkında, Danıştay tarafından, 06.07.2017 tarihinde ve 09.10.2018 tarihinde olmak üzere iki defa yürütmeyi durdurma kararı verilmiş olup henüz bu konuda yeni bir yönetmelik yürürlüğe konulmamıştır. "(www.kazanci.com.tr)" [E.T:16.03.2019]

[277] Küzeci, *Kişisel Verilerin Korunması*, s. 353.

Bu hususlara ek olarak, özel nitelikli veriler bakımından, belli durumlar için uygulamada belirsizliklerin mevcut olduğu söylenebilir. Bu sorunların bazılarını örnek olarak ifade etmek gerekirse;

- Sağlık verileri bakımından uygulamada pek çok belirsizlik söz konusu olup; ilgili mesleğin doğrudan sağlık verilerinin işlenmesini veya kullanılmasını zorunlu kılması halinde ise veri sorumluları için önemli sorunlar ve çözümü olmayan durumlar ortaya çıkmaktadır. Sağlık verilerinin yoğunlukla işlendiği tıp sektöründe, uygulamadaki çözümsüzlük hali ve söz konusu "kriz" en üst seviyeye çıkmış durumdadır. Özellikle kohort çalışma olarak gerçekleştirilen retrospektif çalışmalar için kullanılacak hasta sağlık verisi örnekleri bakımından önemli bir çözümsüzlük söz konusudur. Retrospektif çalışma, araştırmacının, tarihsel olarak belli bir noktadan belirli bir geçmiş zamana kadar ortak özelliklere sahip hastaların oluşturduğu bir grubu ve bu grubun içinde bulunan hastaların verilerini izlemesi neticesinde ortaya koyduğu kohort çalışmadır[278]. Klinik araştırmalar bakımından veya retrospektif çalışmalar gibi kohort çalışmalarda, hasta verilerinin elde edilmesine dair usul ve esaslara yönelik olarak sağlık sektörü özelinde herhangi bir mevzuat bulunmamaktadır[279]. Bu sebeple, klinik araştırmalar veya kohort çalışmalar kapsamında, uygulanacak mevzuat, Kanun ve Kanun'un konuya uygulanabilecek ilişkili hükümleridir. Yukarıda da ifade edildiği üzere, sağlık verileri ancak ilgili kişinin açık rızası veya kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilmektedir.

---

[278] Disis, "The Immortal Life of Henrietta Lacks".

[279] "2238 sayılı ve 29.05.1979 tarihli *Organ ve Doku Alınması, Saklanması, Aşılanması ve Nakli Hakkında Kanun*"un klinik araştırmalara uygulanabileceği düşünülebilecekse de, gerek ilgili kanun kapsamında yalnızca doku ve organ nakline ilişkin esas ve usullerin düzenlenmiş olması gerekse kanun yürürlük tarihi dikkate alındığında, klinik araştırmalar kapsamında elde edilen kişisel verilere söz konusu kanunun uygulanamayacağı kanaatindeyiz.

Anlaşılacağı üzere, kohort çalışmalar veya klinik araştırmalar kapsamında kullanılacak sağlık verileri bakımından açık rıza dışında başkaca bir hukuka uygunluk nedeni öngörülmemiş olup, özellikle Kanun yayım tarihinden yıllarca önce hastalardan alınmış olan biyopsi veya kan örnekleri gibi hastaya ait sağlık verileri kullanılarak yapılacak retrospektif çalışmalar bakımından açık rıza hususunda önemli bir kanuni boşluk söz konusudur. Öte yandan, uygulamaya bakıldığında, Kanun yayım tarihinden önce, hastalardan klinik araştırma veya kohort çalışma yapmak adına elde edilmiş ve pek çok hastalığın tedavisinin bulunmasının önünü açabilecek nitelikte binlerce sağlık verisi, veri sorumlularının veri sistemlerinde mevcut bulunmaktadır.

1990'lı yılların başından itibaren meme kanseri teşhisi konmuş hastalardan oluşan ve 2010 yılına kadar incelenmiş olan bir hasta grubunu, bu konudaki bir örnek olarak düşündüğümüzde, hastalardan 1990 – 2010 yılları arasında alınmış olan biyopsi örnekleri, Kanun kapsamında belirtilen esas ve usullere uygun olarak elde edilmemiş olacaktır. Ayrıca, hastalardan bu dönemde alınmış veriler bakımından, kohort çalışma kapsamında toplanacak sağlık verilerine dair rıza alınması gibi bir kanuni zorunluk bulunmadığından, Kanun yayım tarihinden önce böyle bir işlemin yapılması da ilgili veri sorumlularından beklenemez. Örneğimizdeki sağlık verileri düşünüldüğünde, ilgili verilerin işlenmesi veya kohort çalışmalar kapsamında kullanılması Kanun'a aykırılık oluşturmaktaysa da bu verilerin, meme kanserinin tedavisi araştırmalarında büyük öneme sahip ve kullanılması zorunlu veriler oldukları açıktır. Bunun yanında, 1990'lı yılların başında biyopsi örnekleri alınan hasta grubunun uygulamada açık rızasının alınması çok da kolay olmamaktadır. Öyle ki, bu hastaların bazıları vefat etmiş durumdayken, bazılarına ise daha önce verdikleri iletişim bilgilerinden ulaşmak mümkün olamamaktadır. Kaldı ki, binlerce verinin sahibi olan binlerce kişiyle tek tek iletişime geçmek ve tek tek açık rıza uygulamasını gerçekleştirmek de çok zor bir uygulamadır. Vermiş olduğumuz örneğe benzer pek çok durum kohort çalışmalar bakımından hali hazırda çözümsüz olarak durmaktadır. Konuya ilişkin özel bir düzenleme bulunmaması sebebiyle, temel mesleki faaliyeti klinik araştırma veya kohort çalışmalar gerçekleştirmek olan

veri sorumluları, faaliyetlerini sürdüremez hale gelmekte veya faaliyetlerini Kanun'a aykırı bir şekilde sürdürmek zorunda bırakılmaktadır.

Bu sorun bakımından, farklı çözüm yolları öngörülebilir. İlk çözüm yolu, uygulamada da sıklıkla başvurulduğu üzere, sağlık verilerinin anonimleştirilmesi yöntemidir. İlk izlenimde, sağlık verilerinin anonimleştirilerek kullanılması makul bir yöntem olarak görünmekte ise de bu yöntemin sakıncalı/sıkıntılı yönleri mevcuttur. İlk olarak, Kanun'da ve Kanun kapsamında yayımlanan ilişkili yönetmelikte anonimleştirme yöntemi için "*Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*" ve "*Kanunun 5 inci ve 6 ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.(**Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m. 7)***" düzenlemelerinin yer aldığı görülmektedir. Bu düzenlemeler birlikte değerlendirildiğinde, yukarıda bahsetmiş olduğumuz retrospektif çalışmalara konu edilecek nitelikteki sağlık verilerinin, anonimleştirmenin ön koşulu olan Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmak ve işlenme şartlarının ortadan kalkmış olmak koşullarını/durumlarını sağlamadığı görülmektedir. Bu bağlamda, yapılacak anonimleştirme işleminin hukuki düzlemde ne kadar uygun olacağı tartışmalıdır. Yine, verilerin anonimleştirilmesi sonrası, sağlık verilerinin klinik araştırmalar veya kohort çalışmalar bakımından değeri azalabilmekte ve tedavi yöntemleri bakımından gerçekleştirilecek çalışmalarda, araştırmacıların elindeki verinin niteliği çalışmanın akıbetini etkileyebilmektedir.

İkinci bir çözüm önerisi ise, GVKT'de de yalnızca atıfta bulunulan ancak düzenlemesi bulunmayan, kanımızca Kanun'da mutlaka düzenlemesinin bulunması şart olan ölülerin dijital verilerinin korunması hususudur. Öyle ki, GVKT Giriş Kısmı bölüm 27 incelendiğinde, GVKT'nin ölü kişiler için uygulanmayacağı ve

fakat üye devletlerin ölülerin dijital verilerinin işlenmesine ilişkin olarak düzenlemeler yapabileceğinin düzenlendiği görülmektedir. Bu kapsamda, bazı Avrupa Birliği üyesi devletler, bu konuda farklı yaklaşımlar göstererek ölülerin dijital verilerinin korunmasına ve akıbetine yönelik düzenlemeler yapmışlardır[280]. Yine, Facebook gibi farklı sosyal medya platformlarında da bu konuya ilişkin kullanıcılara farklı çözüm yöntemleri sunulmaktadır[281]. Bu konudaki düzenleme ihtiyacı, dijital çağın insan hayatı bakımından yadsınamaz bir gerçeklik haline gelmesi ile birlikte, kişilerin dijital ölüm hakkında düşünmeye başlamış olması ile ortaya çıkmıştır. Kişiler her gün paylaştıkları yüzlerce veri ve bilginin öldükten sonra akıbetinin ne olacağı konusunda şüphe ve merak duymuşlar ve normal ölüm ile dijital ölümün farklı kavramlar olduğunun kabul edilmesi bu konuda hukuki düzenlemelerin yapılmasına sebebiyet vermiştir. Farklı ülkelerde, ölülerin verilerinin akıbeti ve ölü kişilerin verilerinin korunmasının önemli davalara konu olması da kanuni düzenlemelerin önünü açmıştır[282]. Yapılan düzenleme ve uygulamaların temelinde ise, ölü kişilerin manevi miraslarının kişilerin anısına uygun bir şekilde korunması düşüncesi yatmaktadır[283] ve bu düzenlemeler kapsamında, ölü kişilerin dijital verilerinin, belirli durumlar bakımından ve belirli şartlar altında müteveffanın mirasçılarına miras olarak bırakılacağı öngörülmektedir. Bu doğrultuda, ölü kişilerin klinik araştırmalar veya kohort çalışmalar kapsamında kullanılacak sağlık verileri bakımından da ilgili düzenlemelerin dikkate alınabileceği ve bu kapsamda kişilerin klinik araştırmalar veya kohort çalışmalar için kullanılacak sağlık verileri bakımından müteveffanın mirasçılarından usulüne uygun rıza alınarak çalışmaların gerçekleştirilebileceği düşünülmektedir. Bu çözüm yolu bakımından öngörülebilecek problem ise yukarıda

---

[280] Örneğin, İtalya Veri Koruma Kanunu 2. maddesinde, ölü kişinin verilerinin bu veriler ile doğrudan menfaati olan kişiler tarafından ve Fransız Veri Koruma Kanunu 40. maddesinde ise ölü kişilerin müteveffanın mirasçıları tarafından belli konularda elde edilebileceği düzenlenmiştir. Ayrıntılı bilgi için bakınız:https://www.gamingtechlaw.com/2018/09/iconsumer-deceased-persons-gdpr-data-protection.html [Erişim Tarihi: 17.03.2019]

[281] Facebook, kişilerin kendilerine hesap varisi atamalarına imkan sağlayan bir "Hesap Varisi Sözleşmesi"ni kullanıcılarına önermekte olup; bu sözleşme aracılığıyla kişiler öldükten sonra hesaplarında belli konularda değişiklik ve paylaşım yapma ve hesaplarındaki belli verilerin elde edilmesi konusunda hesap varisi atama imkanına sahip olmaktadırlar. Ayrıntılı bilgi için bakınız:
"https://www.facebook.com/help/1568013990080948" [E.T: 17.03.2019]

[282] Andrews ve DePellegrin, "HeLa Case".

[283] Korenhof ve diğerleri, "Timing the Right to Be Forgotten", s. 187.

da ifade edildiği üzere, yaşamakta olan hastalardan tek tek alınacak rızaların yanı sıra hayatını kaybetmiş hastaların mirasçılarına ulaşılarak mirasçılardan da tek tek rıza alınmasının zorluğudur. Bu kapsamda, ilgili kişiler ile iletişime geçilmesindeki büyük zorluklar bir yana, bu işlemin uzun bir zaman alacağı ve önemli bir iş yükü getireceği sarih bir gerçekliktir.

Diğer bir çözüm önerisi, klinik araştırmalarda veya kohort çalışmalarda sağlık verileri bakımından rıza alınması sorunu da dahil olmak üzere sağlık verileri bakımından yaşanan sektöre özel sorunlara da çözüm sağlayabilecek nitelikte bir düzenlemenin yürürlüğe konulmasıdır. Öyle ki, klinik araştırmalar veya kohort çalışmalar da dahil olmak üzere tüm bu çözümsüz meseleler, Kanun altında düzenlenecek bir yönetmelik veya Kanun'da yer alacak bir geçiş hükmü ile çözüme kavuşturulabilir. Ancak, Kanun altında düzenlenmiş olan *Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliği* iki defa Danıştay kararlarıyla mülga olduğu[284] gibi, ilgili yönetmelik, klinik araştırmalarda veya kohort çalışmalarda sağlık verileri bakımından rıza alınması sorunu da dahil olmak üzere sağlık verileri bakımından yaşanan spesifik sorunlara yönelik çözümler getirmemiş ve sağlık verileri bakımından daha geniş bir çerçeve çizmiştir. Böyle bir düzenlemenin, ivedilikle hazırlanarak yürürlüğe konulması, konu bakımından büyük önem arz etmektedir.

Son olarak, klinik araştırmalar veya kohort çalışmalar kapsamında Kanun'un yayım tarihinden sonra izlenecek yöntemi de ifade etmek faydalı olacaktır. Bu kapsamda alınacak veriler bakımından, veri sorumlularının Kanun'daki esas ve usullere uygun olarak hastaları doğru bir şekilde aydınlatması ve verilerin elde edilmesindeki amacı belirli, meşru amaçlar ile sınırlı tutması ve bu doğrultuda ilgili kişiden açık rıza alması doğru olacaktır. Bu doğrultuda hazırlanacak aydınlatma metinleri ve rıza formları konusunda ise, Türk Tabipler Birliği'nin hastalardan alınacak rızalar

---

[284] Yukarıda da ifade edildiği üzere, "*Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik*" hakkında, Danıştay tarafından, 06.07.2017 tarihinde ve 09.10.2018 tarihinde olmak üzere iki defa yürütmeyi durdurma kararı verilmiş olup henüz bu konuda yeni bir yönetmelik yürürlüğe konulmamıştır. ("www.kazanci.com.tr") [E.T:16.03.2019]

bakımından belirlediği aydınlatılmış onam kılavuzundan yararlanmak veri sorumluları bakımından faydalı olacaktır[285]. Alınacak rızalar bakımından, kişilerden ölüm sonrası kullanılmak üzere rıza almak da rıza mekanizmasının kolay işlemesi bakımından önemli olacaktır. Öyle ki, ölümden önce kurulan bir güven ilişkisi ölümden sonraya tesir etmeyecektir ve bu sebeple ölümden sonra hassas verilerin açıklanması veya kullanılması, güven ilişkisinin ölümden sonraya da tesir etmesini sağlayacak şekilde bir onayın alınması ile mümkün olabilecektir[286].

- Uygulamada, önemli bir sıkıntı da sağlık verisi tanımının, Kanun'da "tanımlar" başlığı altında yapılmamış olmasından gelmektedir. Öyle ki, sağlık verisi denildiğinde, pek çok veri sağlık verisi olarak kabul edilebilmekte ve sınırları çizilemeyen bir sağlık verisi tanımı, veri sorumlularını önemli yükümlülükler altına sokmaktadır. Örneğin, son on yılda sayısı ve niteliği artış gösteren akıllı teknolojik cihazlar aracılığıyla veya farklı mobil uygulamalar ile elde edilen kalp atışı hızı, vücuttaki oksijen miktarı gibi veriler, Kanun kapsamında sağlık verisi olarak kabul edilebilir. Bu bağlamda, sağlık verisi tanımının Kanun'da yer alması ve bu konuda bir çerçeve çizilmesi büyük fayda sağlayacaktır.

- Yine, uygulamada, hassas veriler bakımından bir diğer problemli konu ise kişilerin fotoğraflarının işlenmesidir. Fotoğrafın özel nitelikli veri mi normal nitelikli bir veri mi olarak kabul edileceği duruma göre değişkenlik göstermekte ise de bu belirsizliğin Kanun aracılığıyla giderilmesi faydalı olacaktır. Örneğin, veri sorumlusu şirketler tarafından yapılan etkinliklerde çalışanların veya etkinliğe katılan kişilerin pek çok fotoğrafı çekilerek, tüm çalışanların veya kamuoyunun ulaşabileceği mecralarda bu fotoğrafların veri sorumlusu tarafından paylaşılması uygulamada sıklıkla karşılaşılan bir durumdur. Bu kapsamda, zaman zaman kişilerin kişisel verilerinin akıbetini belirleme hakkının ihlal edildiği açıktır. Öte yandan, bazı durumlarda da fotoğrafların, veri sorumlusu tarafından işlenmesi zorunlu

---

[285] Ayrıntılı bilgi için bakınız: "http://www.ttb.org.tr/mevzuat/index.php?option=com_content&view=article&id=983:onam&catid=26:etik&Itemid=65" [E.T: 19.02.2019]

[286] "Principles of Consent: Deceased People". "http://www.hra-decisiontools.org.uk/consent/principles-deceased.html" [Erişim tarihi: 19.02.2019]

olabilmektedir. Bu sebeple, veri sorumluları bakımından önemli bir belirsizlik ortaya çıkmaktadır. Bu belirsizliklerin, kanuni düzenlemeler veya Kurul kararları aracılığıyla giderilmesi faydalı olacaktır. Kurul 30 Nisan 2019 tarihi itibariyle yayınlamış olduğu örnek veri envanteri ile fotoğrafı bu envanterde "basit veri" olarak öngörmüş ve çalışmasını bu şekilde kamuoyuyla paylaşmışsa da bu paylaşımın belirsizliği tam olarak gidermediği kanaatindeyiz[287]

2.3.4. Kişisel Verilerin Aktarımı

Kişisel verilerin aktarımı, ayrı bir başlık altında Kanun'da düzenlemesini bulmuşsa da, esasen kişisel verilerin veri sorumlusu tarafından üçüncü bir kişiye aktarılması, veri işleme faaliyetinin bir parçası ve bir türüdür. Kanun m. 8'de yurtiçinde gerçekleştirilen veri aktarımı düzenlemesi yapılmıştır. Kanun'un 5 ve 6. maddelerindeki veri işleme koşulları ve 4. maddede düzenlenen veri işleme ilkeleri bu veri aktarım türü bakımından da geçerlidir. İşbu maddelerde belirtilen maddelere ek olarak, yalnızca özel nitelikli kişisel verilerin aktarımı bakımından yeterli önlemlerin alınması gerekliliği de ek bir koşul olarak belirlenmiş olup, söz konusu "yeterli önlemler" ise Kurul tarafından belirlenecek ve kamuoyu ile paylaşılacaktır.

Kişisel verilerin aktarımı bakımından, en önemli hususlardan biri yurtdışına veri aktarımıdır. Kanun m. 9'da düzenlenen bu husus, güvenli bir şekilde yurtdışına veri aktarımının sağlanması bir yana Kanun'da öngörülen koruma seviyesinin yurtdışında da muhafaza edilmesini amaçlamaktadır[288].

Verilerin yurtdışına aktarımı bakımından, hukuka uygunluk nedenleri belirlenmiş olup bu bağlamda, ilk hukuka uygunluk nedeni ilgili kişinin açık rızasıdır. Açık rızanın en önemli sac ayaklarından olan, ilgili kişinin bilgilendirilmesi yönünden ise kişinin yurtdışına

---

[287] "Kurum'un örnek olarak yayınlamış oluğu veri envanteri örneği." Ayrıntılı bilgi için bknz. "https://kvkk.gov.tr/Icerik/5445/Kisisel-Veri-Isleme-Envanteri-Hazirlama-Rehberi-Kurum-Internet-Sayfasinda-Yayinlanmistir" [Erişim Tarihi: 30.05.2019]

[288] Çekin, *Kişisel Verilerin Korunması*, s. 84.

aktarımın amacı ve aktarılacak ülke gibi veri aktarımını doğrudan ilgilendiren hususlarda veri sorumlusu tarafından bilgilendirilmesi uygun ve hukuken doğru olacaktır[289].

Açık rızanın bulunmadığı hallerde ise Kanun m. 5 ve 6'da sayılan diğer hukuka uygunluk nedenleri başlı başına yeterli olmayıp Kanun, verilerin yurtdışına aktarımı bakımından ikili bir denetim mekanizması öngörmüştür[290]. Buna göre, Kanun, hukuka uygunluk nedenlerinin varlığı halinde, "veri aktarılacak ülkede yeterli korumanın bulunması gerektiğini; veri aktarılacak ülkede yeterli korumanın bulunmaması halinde yeterli korumanın yazılı olarak taahhüt edilmesi ve Kurul'dan izin alınması" şartını aramaktadır. Yazılılık koşulu getirilen taahhüt ile ilgili, Kurul, örnek bir taahhütnameyi resmi internet sitesinde yayınlamış olup; buna göre, ilgili taahhütnamenin, veri aktaran veri sorumlusunun yükümlülüklerini, veri alıcısının yükümlülüklerini, veri konusu kişi grubu ve gruplarına ilişkin bilgileri, veri kategorilerini, veri aktarımının amaçlarını, veri aktarımının hukuki sebebini, alıcı ve alıcı grupları bilgilerini, veri alıcısı tarafından alınacak teknik ve idari tedbirleri, özel nitelikli kişisel veriler için alınan ek önlemleri, veri aktaranın "Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)" bilgilerini ve irtibat kişisi iletişim bilgilerini içermesi gerektiği anlaşılmaktadır[291].

Yeterli korumanın bulunduğu ülkeler Kurul tarafından ilan edilecekse de bugüne kadar Kurul tarafından ilan edilen herhangi bir liste bulunmamaktadır[292]. Bu liste yayınlanana kadar geçecek sürede, veri aktarılan tüm ülkelerin yeterli korumaya sahip olmayan ülke olarak kabul edilerek işlemlerin gerçekleştirilmesi isabetli olacaktır. Mütekabiliyet ilkesinin bir görünümü olan bu madde[293], uygulamada önemli problemlerle yol

---

[289] Çekin, *Kişisel Verilerin Korunması*, s. 85.

[290] Çekin, s. 87.

[291] "Kişisel Verileri Koruma Kurumu'nun 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi kapsamında, yurtdışına veri aktarımında veri sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurlara ilişkin taahhütname". "https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler" [E.T: 17.03.2019]

[292] Avrupa Komisyonu tarafından, 17.03.2019 tarihi itibariyle, "Andorra, Kanada, Arjantin, Faroe Adaları, Guernsey, İsrail, Man Adası, Jersey Adası, Yeni Zelenda, İsviçre, Uruguay ve Amerika Birleşik Devletleri" güvenli ülke olarak kabul edilmiştir. Ayrıntılı bilgi için bakınız: "https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en" [Erişim Tarihi: 17.03.2019]

[293] Çekin, *Kişisel Verilerin Korunması*, s. 86.

açmaktadır. Özellikle internetin yaygınlaştığı ve e-mailler aracılığıyla her gün milyonlarca verinin yurtdışına aktarıldığı günümüzde, Kurul'dan izin mekanizmasının getirilmiş olması, internetin ve modern dünyanın hızı bakımından, ticari faaliyetlerin yavaşlamasına sebebiyet verecek nitelikte ve internet çağının hızına erişemeyecek nitelikte bir koşuldur.

Öte yandan, "*Kurul'a, Türkiye'den yurt dışına yapılacak olan veri aktarımlarında Türkiye Cumhuriyeti'nin veya ilgili kişinin menfaatlerinin ciddi bir şekilde zarar görme ihtimali olduğunun tespit edilmesi halinde, bu veri aktarımını onaylama veya yasaklama imkânının verilmiş olması*" ise verinin, modern dünyanın yeni petrolü[294] olduğu düşünüldüğünde, verinin olabildiğince ülke sınırları içinde tutulabilmesi bakımından önem arz etmektedir. Belirtmek gerekir ki, "Türkiye'nin tarafı olduğu uluslararası anlaşmaların kapsamına giren durumlarda söz konusu onay mekanizması uygulanmayacak olup bu kapsamda, Kanun hükümleri doğrultusunda kişisel veriler yurtdışına aktarılabilecek iken, Türkiye Cumhuriyeti'nin veya ilgili kişinin menfaatlerinin ciddi şekilde zarar görme ihtimali olduğu durumlarda veri aktarımları yine ilgili kamu kurum ve kuruluşlarının görüşü alınmak sureti ile Kurulun iznine tabi tutulacaktır"[295].

2.3.5. Veri Sorumlusunun Yükümlülükleri

Veri sorumlusunun yükümlülükleri bakımından, veri işleme faaliyetinin meşruiyetinin sağlanması en mühim meseledir. Veri işleme faaliyetinin meşru bir şekilde gerçekleştirilmesi, en başta ilgili kişinin haklarının hukuki düzenlemelere konu olması ile söz konusu olmaktadır. İlgili kişinin hakları ile veri sorumlusunun yükümlülükleri birbirini tamamlayıcı niteliktedir[296]. Bu bağlamda, ilgili kişiye Kanun m. 11 aracılığıyla sağlanan;

- "Kişisel veri işlenip işlenmediğini öğrenme,

---

[294] Markou, "EU Cookie Law", s. 229.
[295] Kişisel Verileri Koruma Kurumu, "KVKK Uygulama Rehberi", s. 93.
[296] Çekin, *Kişisel Verilerin Korunması*, s. 89.

- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin kişisel verilerin silinmesini veya yok edilmesini isteme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltildiğinin veya kişisel verilerin silindiğinin ve yok edildiğinin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle ilgili kişinin zarara uğraması hâlinde zararın giderilmesini talep etme,"

hakları ile ilgili kişi, veri sorumlularının hukuka aykırı veri işleme faaliyetlerine karşı korunmaktadır. Kişisel verilerin korunması hakkının ilgili kişi tarafından sağlanmasının ve veri işleme faaliyetinin meşru, veri işleme ilke ve şartlarına uygun bir şekilde yürütülmesinin tek yolu da budur. Bu durumun sağlanması adına, ilgili kişinin hakları da gözetilerek, veri sorumlusu için Kanun tarafından belirli yükümlülükler öngörülmüştür. Bu yükümlülükler, özetle; *aydınlatma yükümlülüğü, veri güvenliğinin sağlanması yükümlülüğü, Kurul'a bildirim yükümlülüğü, Veri Sorumluları Sicili'ne kayıt yükümlülüğü ve diğer yükümlülükler* olarak ifade edilebilir. Bu yükümlülükler yanında, Kanun'da düzenlenmemişse de GVKT'de düzenlemesini bulan bazı yükümlülükler bulunmakta olup, kişisel verilerin korunması hakkının ülkemizde yaygınlaşması ve gelişmesini takiben ve GVKT'nün uygulamasının coğrafi sınırlarının gün geçtikçe kaybolması da dikkate alınarak, ilgili yükümlülüklerin de ülkemizde yakın gelecekte düzenleme bulacağı kanaatindeyiz.

2.3.5.1. Veri Sorumlusunun Aydınlatma Yükümlülüğü

Verilerin belirli, açık ve meşru amaçlar çerçevesinde işlenmesi ilkesi ve verilerin işlenmesi için kişinin açık rızasının alınması ile doğrudan bağlantılı olan ve bu ilke ve şartların gerçekleşmesinin ön koşulu niteliğinde bulunan aydınlatma yükümlülüğü Kanun m. 10'da düzenlemesini bulmaktadır. Bu yükümlülük, dürüstlük kuralı ile de doğrudan ilişkilidir[297]. Buna göre, veri sorumlusu, ilgili kişiyi; "*veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve ilgili kişinin Kanun m. 11'de sayılan hakları konusunda aydınlatmakla yükümlüdür*". Veri sorumlusu, aydınlatma yükümlülüğünde ayrıca, kendisine yöneltilecek itiraz, düzeltme veya tazminat taleplerini de hangi yollarla aldığını ve bu konudaki usul ve esaslar ile ilgili olarak ilgili kişiyi bilgilendirecektir. Şeffaflık ve meşruluk, aydınlatma metninin özünde bulunması gereken ve metin oluşturulurken temel alınması gereken ilkelerdir.

Aydınlatma metninin dili ile ilgili olarak ise Kanun'da bir düzenleme bulunmamaktadır. Ancak ilgili kişi bakımından, her yönüyle anlaşılabilmesi gereken sözlü veya yazılı bir beyanın ilgili kişinin ana dilinde olması doğru olacaktır[298]. Türk hukuku uygulaması bakımından, oluşturulacak aydınlatma metninin Türkçe olması; bunun yanında yabancı ilgili kişiler bakımından İngilizce dilinde bir aydınlatma metninin ayrıca oluşturulmasının Türkiye sınırları içinde veri işleme faaliyeti gerçekleştiren tüm veri sorumluları bakımından faydalı olacağı kanaatindeyiz.

Aydınlatma yükümlülüğü, yazılı olarak gerçekleştirilebileceği gibi, günümüzde daha yaygın kullanıldığı haliyle elektronik ortam üzerinden de gerçekleştirilebilir. Belirli uygulamalar[299], mail imzalar veya internet sitelerindeki metinler aracılığıyla sağlanmaya çalışılmaktaysa da ilgili kişinin ilgili metinleri okumaksızın aydınlatma

---

[297] Şimşek, *Kişisel Verilerin Korunması*, s. 88.

[298] Dehon ve Carey, *Data Protection: A Practical Guide*, s. 44.

[299] Hiperbağlar, çerezler ve tarayıcıların uygulamaları, bu uygulamalara örnek olarak verilebilir.

metnine onay vermesi halinde veya bu işlemi bilinçli ve durumun farkında olarak gerçekleştirmediği durumlarda geçerli olmayacaktır[300]. Bu araçlar bakımından, aydınlatma metninin kanunen yeterli ve gerekli içeriğe sahip olması yetmeyecektir ve fakat, ilgili kişinin durumun farkında olduğunun ispatlanması da hemen hemen imkansızdır[301]. Kanaatimizce, bu imkansızlık, yalnızca elektronik ortam üzerinden alınan onaylar için değil tüm yöntemler bakımından kısmen de olsa geçerlidir.

Aydınlatma metninin uygulaması bakımından da Kurul'un vermiş olduğu bazı kararlar bulunmakta olup, Kurul vermiş olduğu bu kararlarında, veri sorumlularının hazırlamış oldukları aydınlatma metinleri bakımından gerekli düzenlemeleri yapmalarına yönelik yaptırım ve uygulamalar gerçekleştirmiştir[302]

2.3.5.2. Veri Güvenliğinin Sağlanması Yükümlülüğü

"*Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyinin temin edilmesi ve bu yönde gerekli her türlü teknik ve idari tedbirin alınması*" anlamına gelen bu yükümlülük Kanun m. 12'de düzenlemesini bulmuş olup, verinin meşru bir şekilde işlenmesi ve veri güvenliğinin sağlanması bakımından veri sorumlusuna yüklenmiş en önemli yükümlülüklerden biridir.

Teknik ve idari açıdan belirli karar alma süreçlerini içeren ve belirli standartlara uygunluğu gerektiren veri güvenliği, kişisel verilerin korunmasına hizmet etmektedir[303].

---

[300] Küzeci, *Kişisel Verilerin Korunması*, s. 226.

[301] Bergkamp ve Dhont, "Data Protection in Europe and the Internet", s. 84.

[302] "Kişisel Verileri Koruma Kurulu'nun *ilgili kişinin yaptığı başvuruyu cevaplandırmayan ve internet sitesi üzerinden yayımladığı aydınlatma metni mevzuatta düzenlenen şartları taşımayan T.C. Ziraat Bankası A.Ş. hakkında* başlıklı 02/05/2019 tarihli ve 2019/122 sayılı; ve *veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili* başlıklı 26/07/2018 tarihli ve 2018/90 sayılı Kararları". Ayrıntılı bilgi için bakınız: "https://www.kvkk.gov.tr/Icerik/5406/Kurul-Karar-Ozetleri" [Erişim tarihi: 30.05.2019]

[303] Çekin, *Kişisel Verilerin Korunması*, s. 104.

Bu bağlamda, veri koruması bireyin korunması yönelik iken, veri güvenliği verinin korunmasına yöneliktir[304]. Veri güvenliği ve kişisel verilerin korunması birbirine sıkı sıkıya bağlı ayrılmaz iki unsurdur ve Kanun'un amacının gerçekleştirilmesi için en mühim araçlardan biri veri güvenliğinin sağlanması ve bu kapsamda gerekli idari ve teknik tedbirlerin alınmasıdır. Buna göre, veri güvenliğine ilişkin teknolojik araçlar ve bu araçların kullanılmasının maliyeti de değerlendirilerek, veri sorumlusu, veri işleme faaliyetine özgü olan ve korunacak verinin niteliğini de dikkate alarak en uygun güvenlik düzeyini sağlayacaktır[305].

Teknik ve idari tedbirler, veri sorumlusu tarafından veri güvenliğinin sağlanması amacıyla aldığı tüm önlemler olarak ifade edilebilir[306]. Alınacak tedbirler, altyapı, organizasyon, yazılım ve teknik teçhizata ilişkin olabileceği gibi çalışanların düzenli aralıklarla bilgilendirilmesi, sürekli eğitime tabi tutulması, şifrelerin belirli aralıklarla güncellenmesi, şifrelerin yeterli ve gerekli güvenlik gücüne sahip olması, bilgisayarların kontrollerinin tek bir merkezden yürütülmesi gibi tedbirler de olabilir. Örneğin, Kurul'un "*Teknik servis hizmeti veren firmanın müşterilerine verdiği form/takip numarasının son hanelerinin değiştirilmesi yoluyla farklı kişilere ait kişisel verilere ulaşıldığı yolunda Kuruma iletilen ihbarın incelenmesi ve ihbara ilişkin alınan Kurul Kararının yerine getirilmemesi* konulu 14/02/2019 tarih ve 2019/23 sayılı" kararında yeterli teknik ve idari tedbirlerin alınmaması sebebiyle veri sorumlusu idari para cezasıyla cezalandırılmış bulunmaktadır[307].

Kurul, veri sorumlusunun alacağı teknik ve idari tedbirlere ilişkin olarak Ocak 2018 tarihli Kişisel Veri Güvenliği Rehberi yayınlanmış olup bu rehber, "Kanun uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla veri sorumlularının alması gereken teknik ve idari tedbirlere ilişkin başlıca yöntemleri ayrı

---

[304] Küzeci, *Kişisel Verilerin Korunması*, s. 357.

[305] "Avrupa Birliği Veri Güvenliği Yönergesi", m. 17/1.

[306] Benzer tanım için bakınız: Çekin, *Kişisel Verilerin Korunması*, s. 105.

[307] "Kişisel Verileri Koruma Kurulu'nun 14/02/2019 tarih ve 2019/23 sayılı Kararı". Ayrıntılı bilgi için bakınız: "https://www.kvkk.gov.tr/Icerik/5464/2019/52" [Erişim tarihi: 30.05.2019]

ayrı bölümler halinde açıklamaktadır"[308]. Bu bağlamda, veri sorumlusu tarafından doğru donanım ve yazılım sisteminin kullanılmasının yeterli olmadığı, veri güvenliği ilkesinde amacın sağlanması için gerekli organizasyonel kuralların belirlenmesi/idari tedbirlerin alınması gerektiği sarih bir gerçekliktir[309].

Veri sorumlusu, uygun düzeyde ve maliyeti de dikkate alarak gerekli teknolojik yatırımları yapacağı gibi, oluşturacağı veri koruma politikaları ve yönergeleri ile de bu yatırımların işlevselliğini sağlayacaktır. Verinin korunması bakımından teknik tedbirler ve idari tedbirler, veri güvenliğinin ayrılmaz iki parçasıdır. Bizim de katıldığımız bir görüşe göre, veri güvenliğinin sağlanması ve sürdürülebilir şekilde devam ettirilebilmesi için veri sorumlusunun, işlenen verinin niteliği ve kapsamına göre bir veri yönetim sistemi kurması gerekmekte olup idari ve teknik tedbirler de bu sistemin içinde bulunacaktır[310].

Teknik ve idari tedbirlerin yanı sıra, veri güvenliğinin en önemli parçalarından biri de kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı bir şekilde erişilmesini önlemek ve bu kapsamda gerekli denetimleri gerçekleştirmektir[311]. Bu bağlamda, veri sorumlusu, veri güvenliği bakımından gerekli veri yönetim sistemini kurduktan sonra, bu sistemin işlevselliği bakımından gerekli organizasyonel tedbirleri alacak ve verilerin hukuka aykırı bir şekilde işlenmesini önlemek için gerekli denetim mekanizmalarını işletecektir[312]. Buna ek olarak, verilere hukuka aykırı olarak erişilmesini önlemek amacıyla da veri sorumlusu gerekli tedbirleri almalıdır. Tüm bu koruma tedbirleri verilerin mekânsal olarak nerede bulunduğu, fiziksel veya dijital bir veri olup olmadığına bakılmaksızın veri sorumlusunun kurmuş olduğu tüm veri sistemleri için alınmalı ve gerçekleştirilmelidir. Tüm bu tedbirler sayesinde, verilerin güvenliği ve muhafazası sağlanabilecek olup özellikle internetin yaygınlaşması ile birlikte çok daha yaygın hale gelen ve zaman zaman önemli kayıpların da yaşanmasına

---

[308] "Kişisel Verileri Koruma Kurumu", "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)".
[309] Gürsel, *İşçinin Kişisel Verileri*, s. 228.
[310] Çekin, *Kişisel Verilerin Korunması*, s. 106.
[311] Gürsel, *İşçinin Kişisel Verileri*, s. 228.
[312] Çekin, *Kişisel Verilerin Korunması*, s. 108-109.

sebep olan veri sızıntılarının önlenmesi veya bu sızıntıların tespiti ancak bu tedbirlerin alınması ile mümkün olabilecektir[313].

2.3.5.3. Kurula Bildirim Yükümlülüğü

Veri sorumlusunun, Kanun kapsamında bir diğer yükümlülüğü de *"işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurula bildirmek olup Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan etmesidir"*.

Kanun, düzenleme bakımından iki ayrı konuyu, bildirim yükümlülüğü bakımından düzenlemiştir. Veri sorumlusu, bir ihlal veya veri sızıntısı söz konusu olduğunda en kısa sürede Kurul'a bu durumu bildirecektir. Öte yandan, ilgili saldırı/sızıntıya ilişkin bildiri yayınlama hakkı ise Kurum'a aittir[314]. Bildirim hususunda, Kanun tarafından herhangi bir sınır öngörülmemiş olup, böyle bir sınırın öngörülmemesi, uygulamadaki en ufak veri sızıntısının Kurul'a bildirim yükümlülüğünü doğurmaktadır. Çok sık ziyaret edilmeyen bir enerji santralinde bulunan ziyaretçi defterinin kaybolması halinde, verinin niteliği ve sayısına bakılmaksızın ilgili kişilere ve Kurul'a bildirim yükümlülüğü doğmakta olup bildirim yükümlülüğünün bu denli geniş tutulmaması ve bu düzenlemeye bir sınırlama getirilmesi uygun olacaktır.

Doktrinde bu hükme ilişkin olarak yöneltilen diğer eleştiriler ve soruların[315] pek çoğu ise Kurul'un "24.01.2019 tarih ve 2019/10 sayılı Karar"ı sonrasında yanıtlanmış bulunmaktadır[316]. Öyle ki, Kurul, bildirim yükümlülüğü nezdinde kamuoyu ile paylaştığı kararında, veri ihlal bildirimlerinde, "*Kurul'a ve ihlalden etkilenmiş kişilere*

---

[313] Küzeci, *Kişisel Verilerin Korunması*, s. 359.
[314] Çekin, *Kişisel Verilerin Korunması*, 111.
[315] Örneğin bakınız: Çekin, s. 112.
[316] "Kişisel Verileri Koruma Kurulu'nun Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru". Ayrıntılı bilgi için bakınız: "https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi" [Erişim tarihi: 19.02.2019]

bildirim yapılmasındaki amacın, ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamak" olduğunu ifade etmiştir. Bu bağlamda, konuya somut bir yaklaşım getirerek, Kanun düzenlemesindeki "en kısa süre" ibaresinin ne ifade ettiği ve ilgili kişiye bildirimlerde ortaya çıkan ilgili kişiye ulaşılamama durumunda veri sorumlusunun ne yapabileceği konularında çözüm ve belirlemeler ortaya koymaktadır.

Karara göre;

- Kanun'da ifadesini bulan "*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir....*" hükmünde yer alan "en kısa sürede" ifadesinin "72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine",

- "Veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına",

karar verilmiştir.

Bu karar kapsamında, bildirim için belirli bir form da Karar'ın ekinde paylaşılmış olup, veri sorumlularına bu bakımdan belirli bir şekil şartı getirilmiş durumdadır. Getirilen bu şekil şartı ise, Karar'da ayrıca belirtilen veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması hali bakımından ayrı bir önem arz etmektedir. Karar'da, "*yurtdışında yerleşik veri sorumlusu bakımından, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurul'a bildirimde bulunulmasına*" yer verilmişse de Karar'ın ekinde veri

sorumluları tarafından kullanılması öngörülen form yalnızca Türkçe dilinde hazırlanmıştır. Veri sorumlusunun, bu bakımdan İngilizce dilde bir veri ihlali bildirimde bulunması söz konusu olamayacaktır. Bu kapsamda, uygulamadaki olasılıklar da göz önünde bulundurularak en azından ilgili formun İngilizce dilindeki versiyonunun da yabancı veri sorumluları bakımından yayınlanması gerektiği kanaatindeyiz.

2.3.5.4. Veri Sorumluları Siciline Kayıt Yükümlülüğü

Kanun m. 16 gereğince, "Kişisel Verileri Koruma Kurulu'nun gözetiminde, kamuya açık olarak Veri Sorumluları Sicili tutulur ve kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Sicili'ne kaydolmak zorundadır".

VERBİS, Kanun kapsamında kamuya açık olarak tutulmak zorunda olup kamuya açıklık durumu, isteyen kişinin sicil üzerinde inceleme yapabilmesi anlamına gelmektedir. Kamuya açıklık aracılığıyla veri sorumlularının kamu tarafından bilinebilir olması ve ilgili kişilerin hak ihlallerine karşı daha etkili şekilde mücadele etmesine imkân verilmesi[317] amaçlanmakta ise de kamuya açıklık Kurul'a sunulan her türlü bilgiyi kapsamamakta ve hangi bilgilerin kamuya açık olacağı konusunda takdir yetkisi Kurul'a bırakılmaktadır[318].

VERBİS'e kayıt başvurusu yapılırken, veri sorumluları ilgili yönetmelik ışığında ilgili sicile, "*veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgilerini; kişisel verilerin hangi amaçla işleneceğini; veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamaları; kişisel verilerin aktarılabileceği alıcı veya alıcı gruplarını; yabancı ülkelere aktarımı öngörülen kişisel veriler ile ilgili bilgileri; kişisel veri güvenliğine ilişkin alınan tedbirleri ve kişisel verilerin işlendikleri amaç için gerekli olan azami süreleri bildirmekle*" yükümlü olacaktır[319]. Bu düzenleme bakımından, veri

---

[317] Kişisel Verileri Koruma Kurumu, "Veri Sorumluları Sicili Rehberi".
[318] Çekin, *Kişisel Verilerin Korunması*, s. 122; "Veri Sorumluları Sicili Hakkında Yönetmelik", m. 9.
[319] "Veri Sorumluları Sicili Hakkında Yönetmelik", m. 9.

sorumlusunun temsilci atama hali önemlidir. Zira, özellikle, Türkiye'de yerleşik olmayan veri sorumluları açısından veri temsilcisi belirleme zorunluluğu mevcuttur. İlgili düzenlemeye göre, Türkiye'de yerleşik olmayan veri sorumluları;

- "Kurul veya Kurum tarafından yapılan tebligat ve yazışmaları veri sorumlusu adına tebellüğ veya kabul etme,
- Kurum tarafından veri sorumlusuna yöneltilen talepleri veri sorumlusuna iletme, veri sorumlusundan gelecek cevabı Kuruma iletme,
- Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilerin Kanun'un 13 üncü maddesinin birinci fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına alma ve veri sorumlusuna iletme,
- Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilere Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca veri sorumlusunun cevabını iletme,
- Veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapma",

hususlarında asgari temsile yetkili Türkiye'de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi temsilci olarak belirlemekle yükümlü kılınmıştır.

Bu hususa ek olarak, Veri Sorumluları Sicili Hakkında Yönetmelik'te düzenlemesini bulan veri envanteri, ilk olarak veri sorumlusu tarafından sicile sunulması gereken belgeler bakımından tamamlayıcı ve yol gösterici nitelikte kabul edilmişse de daha sonra yapılan mevzuat değişikliğiyle veri envanteri hazırlamak veri sorumlusunun bir yükümlülüğü haline getirilmiştir. Zira, bu düzenlemeye göre, "*veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri*

güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter", veri envanteri olarak tanımlanmıştır. Kişisel veri envanterinde yer verilen bilgiler, kişisel verilerin işlenmesinin her aşamasında veri sorumlusunun yükümlülüklerinin belirlenmesi ve özellikle hukuka uygun davranılıp davranılmadığının tespiti için temel başvuru kaynağı olacağı[320] gibi sicile sunulacak bilgiler bakımından da veri sorumlularına kolaylık sağlayacak ve yol gösterici bir rehber niteliğinde olacaktır. Kaldı ki, envanter hazırlama yükümlülüğü veri sorumlusunun mevzuat uyarınca ayrı bir yükümlülüğüdür.

Kanun'da, "*işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebileceği*" de düzenlenmiştir. Bu bakımdan, VERBİS'e kayıt bakımından Kanun'dan veya Kurul'un yayınladığı kararlardan kaynaklanan belirli istisnalar vardır. Bunlar özetle aşağıdaki gibi ifade edilebilir:

- "Kanunun 28. maddesinin 2. fıkrasında sayılan haller"[321],
- "Kişisel Verileri Koruma Kurulu'nun 02/04/2018 Tarihli ve 2018/32 Sayılı Kararı kapsamında belirtilen veri sorumluları"[322],

[320] Çekin, *Kişisel Verilerin Korunması*, 114.

[321] "Kişisel Verileri Koruma Kurumu", "Veri Sorumluları Sicili Rehberi".

[322] "Bu karara göre; **a)** herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler; **b)** 18/01/1972 tarihli ve 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler; **c)** 04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanuna göre kurumuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler; **d)** 22/04/1983 tarihli ve 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler; **e)** 19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar ve **f)** 1/6/1989 tarihli ve 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler, Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulmuş bulunmaktadırlar."

- "Kişisel Verileri Koruma Kurulu'nun 05/07/2018 Tarihli ve 2018/75 Sayılı Kararı uyarınca arabulucular[323]ve Kişisel Verileri Koruma Kurulu'nun 28/06/2018 Tarihli ve 2018/68 Sayılı Kararı uyarınca 4458 sayılı Gümrük Kanunu uyarınca faaliyet gösteren gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirler"[324] ,

- "Kişisel Verileri Koruma Kurulu'nun 19/07/2018 Tarihli ve 2018/87 Sayılı Kararı uyarınca yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayan gerçek ve tüzel kişiler"[325].

Belirtmek gerekir ki, Kurul kararlarıyla istisna getirilen veri sorumluları, işbu tezin onay tarihi itibariyle Kurul tarafından yayınlanan kararlar ile sınırlı olup daha sonra Kanun m. 16 kapsamında Kurul alacağı yeni kararlar ile başkaca veri sorumlularını da sicile kayıt yükümlülüğünden istisna tutabilir.

"Kişisel Verileri Koruma Kurulu'nun 19/07/2018 Tarihli ve 2018/88 Sayılı Kararı" ile sicile kayıt yükümlülüğünün başlangıç tarihleri de Kurul tarafından belirlenmiş bulunmaktadır[326]. Buna göre:

- "Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Sicili'ne kayıt yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar süre verilmesinin kabulüne",

---

[323] "Kişisel Verileri Koruma Kurulu'nun 02/04/2018 Tarihli ve 2018/32 Sayılı Kararı". "https://www.kvkk.gov.tr/Icerik/4214/Kurul-Kararlari" [Erişim Tarihi: 19.02.2019]
[324] "Kişisel Verileri Koruma Kurulu'nun 05/07/2018 Tarihli ve 2018/75 Sayılı Kararı". "https://www.kvkk.gov.tr/Icerik/4214/Kurul-Kararlari" [Erişim Tarihi: 19.02.2019]
[325] "Kişisel Verileri Koruma Kurulu'nun 28/06/2018 Tarihli ve 2018/68 Sayılı Kararı". "https://www.kvkk.gov.tr/Icerik/4214/Kurul-Kararlari" [Erişim Tarihi: 19.02.2019]
[326] Kişisel Verileri Koruma Kurulu'nun 19/07/2018 Tarihli ve 2018/88 Sayılı Kararı. https://www.kvkk.gov.tr/Icerik/4214/Kurul-Kararlari [Erişim Tarihi: 19.02.2019]

- "Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar süre verilmesinin kabulüne",

- "Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olmakla birlikte ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.01.2019 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 31.03.2020 tarihine kadar süre verilmesinin kabulüne",

- "Kamu kurum ve kuruluşu veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.04.2019 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.06.2020 tarihine kadar süre verilmesinin kabulüne",

karar verilmiştir. Bu kararı takiben, söz konusu kriterleri taşıyan veri sorumlularının, Sicile kayıt yükümlülüğünü yerine getirmesi amacıyla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) 01.10.2018 tarihi itibariyle kullanıma açılmış ve kayıt yapılmaya başlanmış olup Kurul, VERBİS'e kayıt bakımından bir rehber de yayınlamış bulunmaktadır[327].

Son olarak ifade etmek gerekir ki, Kurul tarafından belirtilen istisnalar yalnızca sicile kayıt yükümlülüğü bakımından getirilmiş olup, istisna getirilen veri sorumluları, yalnızca sicile kayıt yükümlülüklerinden muaf tutulmaktadırlar. Bu bağlamda, ilgili veri sorumluları Kanun'dan kaynaklanan diğer yükümlülüklerini yerine getirmek zorundadırlar. Kişisel verilerin korunması da ancak bu şekilde mümkün olacaktır.

[327] Kişisel Verileri Koruma Kurumu, "Veri Sorumluları Sicili Rehberi".

2.3.5.5. Diğer Yükümlülükler

Veri sorumlusunun, yukarıda ifade edilen yükümlülüklerine ek olarak, Kanun'dan kaynaklanan bazı diğer yükümlülükleri de mevcuttur.

Bu yükümlülüklerden ilki, yukarıda ifade edildiği üzere, Kanun m. 4 ve 5'te ifade edilen veri işleme ilke ve koşullarına uygun veri işleme faaliyeti yürütülmesidir[328].

Veri sorumlusunun bir diğer yükümlülüğü ise Kanun m. 5'te düzenlemesini bulan ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek ilkesi ile doğrudan bağlantılı olan ve Kanun m. 7'de düzenlenen kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi yükümlülüğüdür. Bu düzenlemeye göre, "Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir". Kanun kapsamında, "silme, yok etme ve anonimleştirme" de tanımlanmış olup; kısaca, *silme*, "verinin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi"; *yok etme,* "verinin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi"; ve *anonim hale getirme*, "verinin başka veriler ile eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi"dir. Silme, yok etme ve anonimleştirmeye ilişkin esas ve usuller, "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*"'te belirlenmiş olup veri sorumlularının bu yönetmelik kapsamında belirlenen esas ve usuller ışığında gerekli silme, yok etme ve anonimleştirme işlemini gerçekleştirmeleri gerekmektedir[329].

---

[328] Küzeci, "Veri Sorumlusu", s. 367.
[329] Küzeci, "Veri Sorumlusu" s. 367.

Veri sorumlusunun bir diğer yükümlülüğü, yukarıda ayrıntılı bir şekilde açıklanan yurtdışına veri aktarımı kavramından kaynaklanmaktadır. Bu bağlamda, veri sorumluları, yurtdışına veri aktarımı gerçekleştirirken Kanun m. 9 kapsamındaki yükümlülüklerini yerine getirmek suretiyle veri aktarım faaliyetini gerçekleştirebileceklerdir.

Veri sorumlusu için Kanun kapsamında düzenlemesini bulan bir diğer yükümlülük ise ilgili kişiler tarafından yazılı olarak veya Kurul'un belirleyeceği diğer yöntemlerle kendisine iletilen Kanun'un uygulanmasıyla ilgili talepleri cevaplama yükümlülüğüdür. Buna göre, "veri sorumlusu, başvurunun niteliğine göre en kısa sürede ve en geç otuz gün içinde başvuruyu ücretsiz olarak sonuçlandıracaktır". Ve fakat, işlemin belli bir maliyet gerektirmesi hâlinde, veri sorumlusu, söz konusu ücreti başvuruda bulunan ilgili kişiden isteyebilir. Bu düzenlemeye göre, "veri sorumlusu, talebi kabul eder veya gerekçesini açıklayarak reddeder ise bu cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirebilecektir". Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusu tarafından bu talebin gereği yerine getirilecek; başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde ise ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilecektir[330].

Son olarak, Kanun m. 15'te düzenlenen "*Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri gönderilmesi ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak yükümlülüğü ve şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul'un tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesi kararının yerine getirilmesi yükümlülükleri*" de veri sorumlusunun yükümlüklerindendir. Yine, veri sorumlusu, kendi ile ilgili yapılan soruşturma neticesinde Kanun m. 18'de düzenlenen kabahatler

[330] "Veri Sorumlusuna Başvuru ve Kurula Şikayet Sürelerinin Hesaplanmasına İlişkin Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarih ve 2019/9 sayılı Kararı".
"https://www.kvkk.gov.tr/Icerik/4214/Kurul-Kararlari" [E.T: 19.02.2019]

kapsamında idari para cezası ile cezalandırılır ise bu cezanın gereğini yerine getirmekle de yükümlüdür[331].

Bu yükümlülükler yanında, Kanun'da düzenlenmemişse de GVKT'de düzenlemesini bulan bazı yükümlülükler bulunmaktadır. Bu yükümlülükler, kısaca; veri koruma görevlisi bulundurma zorunluluğu ve veri güvenliği risk değerlendirme raporu oluşturulması olarak ifade edilebilir (***Genel Veri Koruma Tüzüğü, m. 35***). Söz konusu yükümlülükler, kişisel verilerin korunması ve veri güvenliğinin sağlanmasının yanı sıra veri koruma denetim mekanizmasının işlevselliği bakımından da büyük önem arz etmektedir. İlgili yükümlülüklerin, Türk hukukunda da kanuni düzenlemesini bulması, anayasal düzenlemelerin tam anlamıyla yerine getirilmesi ve temel bir hak olan kişisel verilerin korunmasının yalnızca kağıt üzerinde değil uygulamada ve hayat gerçekliğinde de mümkün kılınması bakımından önem ve ivedilik arz etmektedir.

2.3.6. Kişisel Verilerin Korunması Mevzuatına Uyum Süreci ve Uyum Projesinin Gerçekleştirilmesi

2.3.6.1. Genel Olarak

Veri sorumlusunun Kanun kapsamında uyması gereken ilke ve kurallar, sahip olduğu yükümlülükleri yukarıda ayrıntılı bir şekilde ifade edilmiştir. İlgili ilke, kural ve yükümlülüklerin yerine getirilmesi ve bu ilke, kural ve yükümlülükler bakımından sürekli işleyen bir mekanizmanın kurulması ise ancak "*uyum projesi*" olarak ifade edilen ve veri koruma hukukunun temel amacını oluşturan[332] uyum süreçleri ile mümkün kılınabilmektedir. İlgili uyum süreçleri Kanun tarafından bir yükümlülük olarak öngörülmemişse de aşağıda ayrıntısıyla açıklanacak olan ve Kanun m. 18'de düzenlenen "Kabahatler" başlığı altındaki idari para cezaları ve diğer yaptırımlar ile veri sorumlusu,

[331] Küzeci, "Veri Sorumlusu", s. 366.
[332] Dülger, *Verilerin Korunması*, s. 383.

ilgili uyum sürecinin gerçekleştirilmesi için bir anlamda baskı altına alınmakta ve zorlanmaktadır[333].

Uyum süreçleri, Kanun'da açıkça düzenlemesini bulmamışsa da Kanun'un Geçici 1. maddesi kapsamında düzenlenen ve Kanun'un yayım tarihinden önce işlenmiş olan kişisel veriler için öngörülmüş yayım tarihinden sonraki iki yılı kapsayacak şekildeki uyum sürecinin bu projelere atıfta bulunduğu düşünülebilir[334]. İlgili geçiş süreci ise ülkemizdeki pek çok veri sorumlusu tarafından hatalı bir şekilde değerlendirilmiş ve veri sorumluları geçiş sürecinin tamamlandığı 7 Nisan 2018 tarihine kadar Kanun'un yayım tarihinden önce veya sonra işlenmiş veriler ile ilgili hiçbir uyum projesi veya çalışması gerçekleştirmemişlerdir. Çoğu veri sorumlusu 7 Nisan 2018 tarihi itibariyle, kişisel verilerin korunması özelinde hiçbir çalışma yapmamışken, bazı veri sorumluları ise bu tarihte, temeli doldurulmamış ve Kanun'daki ilke ve kurallar özümsenmeksizin hazırlanmış aydınlatma metinlerini kısa mesajlar veya e-mailler aracılığıyla ilgili kişilere göndererek Kanun kapsamındaki yükümlülüklerini yerine getirdiklerini düşünmüşlerdir.

Uygulamada gözlemlediğimiz durum, veri sorumlularının mümkün olduğunca bu sorumluluklarından kaçtıkları, ilgili çalışmaları maliyetli ve zaman alan projeler olarak gördükleri ve bu sorumluluktan kaçamayacaklarını anladıkları noktaya kadar bu yükümlülük altına girmeyi tercih etmedikleri yönündedir. Bu yaklaşımın en temel sebebinin, ülkemizdeki bilinç eksikliği olduğu düşüncesindeyiz. 10.12.2018 tarihinde gerçekleşen ve Kurul tarafından düzenlenen "Kişisel Verilerin Korunması Sempozyumu'nda Kişisel Verileri Koruma Kurumu" Başkanı Prof. Dr. Faruk Bilir'in verdiği bilgiler de bu görüşümüzü destekler nitelikte olup Prof. Dr. Faruk Bilir'in açıklamalarına göre 30 Kasım 2018 tarihi itibariyle, Kurum'a 279 şikâyet, 31 ihbar, 24 veri ihlali ve 24 bilgi edinme başvurusu yapılmıştır[335]. İnternet kullanımının fazlasıyla yaygın olduğu ülkemizde her gün milyonlarca kişisel veri üretilmekte olup, sayıların bu

[333] Aksi görüş için bakınız: Dülger, s. 385.
[334] Dülger, s. 385.
[335] Sempozyuma ilişkin ayrıntılı bilgi için bakınız: "https://kvkk.gov.tr/Icerik/5334/II-Kisisel-Verilerin-Korunmasi-Sempozyumu" [Erişim Tarihi: 17.03.2019]

kadar düşük kalmasının kişisel verilerin korunması hususundaki bilinç eksikliğinin bir sonucu olduğu sarih bir gerçekliktir.

Bunun yanında, Kurul'un özellikle Ocak 2019 tarihi itibariyle çok daha etkin bir şekilde denetimlerini gerçekleştirmiş olmaya başlaması, her Çarşamba günü düzenli olarak gerçekleştirdiği seminerler ve farklı şehirlerde farklı sektörlere yönelik olarak gerçekleştirdiği bilinçlendirme toplantıları ve idari para cezalarının yaygın hale gelmesiyle birlikte, veri sorumlularının bu sorumluluktan kaçamayacak duruma gelmelerinin söz konusu olacağı kanaatindeyiz. Özellikle Kurul'un, " "*Facebook nezdinde gerçekleşen veri ihlalinin değerlendirilmesi*" başlıklı ve 11.04.2019 tarih ve 2019/104 sayılı Kararı" ile Facebook'un veri sorumlusu olarak gerekli idari ve teknik tedbirleri almamasından dolayı uyguladığı 1.650.000 TL'lik idari para cezası ile Kurul uygulamaları, yürürlük tarihinden itibaren en üst seviyeye çıkmış bulunmaktadır[336]. Kurul bu cezayla birlikte, bugüne kadarki en yüksek idari para cezasını uygulamış olup bu uygulama bir anlamda veri sorumlularını da yükümlülüklerini yerine getirmesi konusunda itekleyici bir hamle olmuştur.

Bu doğrultuda, Kanun'a uyum sürecinin yürütülmesi gerektiği hususunda hiçbir tereddüt bulunmamaktadır[337] ve Kanun m. 28'de sayılan istisna haller dışında kalan tüm veri sorumluları bu sorumluluklarını yerine getirmelidir. Anayasal bir hak olan kişisel verilerin korunmasının ilgili kişilere sağlanabilmesi için bu gerekli olduğu gibi, Kanun kapsamında veri sorumlularının yükümlülükleri bakımından (*VERBİS'e kayıt yükümlüğü bakımından getirilen kısmi istisnalar dışında*) Kanun m. 28 dışında istisna durumu öngörülmemiş olması da bu hususa işaret etmektedir[338].

---

[336] "Kişisel Verileri Koruma Kurulu'nun *Facebook nezdinde gerçekleşen veri ihlalinin değerlendirilmesi* başlıklı ve 11.04.2019 tarih ve 2019/104 sayılı Kararı". Ayrıntılı bilgi için bakınız: "https://www.kvkk.gov.tr/Icerik/5450/2019-104" [Erişim tarihi: 30.05.2019]

[337] Dülger, *Verilerin Korunması*, s. 386.

[338] Belirtmek gerekir ki VERBİS'e kayıttan muaf olmak, Kanun'a uyum gerçekleştirme yükümlülüğünü ve veri sorumlusunun diğer yükümlülüklerini ortadan kaldırmaz. Benzer görüş için bakınız: Dülger, s. 387.

Son olarak, ifade edilmelidir ki; aşağıda ifade edilen ve uyum projelerinin aşamaları ve içeriklerini ayrıntılı bir şekilde açıklayan bölümün hazırlanmasında pratikte tarafımızca hazırlanan belgelerden faydalanıldığı gibi litaratürde bu konuda yazılan eserlerden de faydalanılmıştır. Ayrıca, kaynak niteliğindeki bu belgelerin hazırlanmasında Kanun ve ilgili mevzuat hükümleri ve Kurul rapor ve rehberleri dayanak olarak kullanılmış olup söz konusu içerik de bu kaynakçaya uygun olarak ifade edilmeye çalışılmıştır.

2.3.6.2. Uyumluluk Sürecinin Tarafları

Uyumluluk sürecinin bir tarafının, veri işleme faaliyetlerini ve veri sistemini Kanun'a uyumlu hale getirmek isteyen veri sorumlusundan oluşacağı izahtan varestedir. Veri sorumlusunun, uyumluluk projesi kapsamında gerçekleştirilecek işlemlere bünyesindeki veri işleyenlerle katılması uygun olacaktır. Bir şirket ile yürütülecek bir uyum projesinde, veri sorumlusu sıfatını haiz şirketin toplantılara katılmasının mümkün olmadığı düşünüldüğünde ilgili şirket bünyesinde kişisel veri işleme faaliyetini yürüten tüm birimlerin uyum sürecinde aktif rol alması gerekmekte ve koordinasyonun sağlanması adına da üst düzey bir yöneticinin ve birim şef/müdürlerinin sürecin içinde bulunması faydalı olmaktadır.

Uyumluluk sürecinin diğer tarafında ise kişisel verilerin korunması ve bilişim hukuku alanlarında uzman hukukçuların bulunması bir zorunluluktur. Zira, Kanun kapsamındaki hukuki kavram ve süreçlerin analiz edilerek, bu hususların veri sorumlularının kendilerine has veri işleme faaliyeti ve veri sistemleri ile hukuki açıdan uyumlu hale getirilmesi için uzman hukukçuların varlığı zaruridir.

Hukukçuların yanı sıra Kanun'da özellikle veri sorumlusu bakımından alınacak olunan teknik tedbirlere atıfta bulunulmuş olması ve veri sorumlusuna idari tedbirlerin yanı sıra maliyet değerlendirmesi de yapılarak verinin korunması bakımından gerekli teknolojik yatırımları yapma yükümlülüğünün yüklenmiş olması, uyumluluk sürecinde veri güvenliği uzmanlarının katılımını ve varlığını da zorunlu kılmaktadır. Zira, bu süreç tek başına hukukçuların veya tek başına veri güvenliği uzmanlarının yürütebileceği bir

süreç olmayıp hem hukuki hem teknik çözümler sunularak veri sistemleri ve veri işleme faaliyetleri Kanun'a uyumlu hale getirilebilecektir[339]. Veri sorumlularına, süreçlerin yürütülmesi için gerekli olan hukukçuların ve veri güvenliği uzmanlarının seçiminde ise veri sorumlularına önemli bir görev düşmekte olup, mesleklerinde ve kişisel verilerin korunması alanında uzman olan kişilerin seçimi Kanun'a uyum süreci bakımından kritik öneme sahiptir.

2.3.6.3. Uyumluluk Süreci Aşamaları

Kanun'a "*uyum projeleri*" veri sorumlularının veri işleme faaliyeti kapasitesine göre, iki ay ile bir yıl arasında süren projeler olup, bu projeler kapsamında 7 Nisan 2016 öncesindeki veriler de dahil tüm veri işleme süreçlerinin analiz edilmesi söz konusu olmakta ve geniş kapsamlı, ayrıntılı bir süreç yürütülmektedir.

Söz konusu projelerin tamamlanması bakımından iki ay ile bir yıl arası süreler öngörülmekte ise de bu yalnızca veri koruma bakımından gerekli analizlerin yapılarak bu konuda bir altyapı oluşturulması bakımından belirlenmiş tahmini bir süre olup, Kanun'a uyumluluk esasında sürekli devam eden ve belirli aralıklarla güncellenmesi gereken bir süreçtir. Öyle ki, yukarıda da ifade edildiği üzere, özellikle Türkiye'de bu alan hukuki altyapısı çok çok yakın bir geçmişte oluşturulmuş bir alandır ve sürekli değişen, değişkenlik gösteren bir yapıya sahiptir. Özellikle, Kurul'un vermiş olduğu kararlar, ilan etmiş olduğu bilgilendirme yazıları aracılığıyla uygulamada zaman zaman önemli değişiklikler olabilmektedir. Bu kapsamda, veri sorumlularının, uyum süreci sonrasında kurmuş oldukları veri yönetim sistemlerini düzenli ve belirli aralıklarla gözden geçirmeleri ve gerektiği ölçüde güncellemeleri, kişisel verilerin korunmasının sürekliliği bakımından büyük önem arz etmektedir. Bu konuda, yukarıda da ifade edildiği üzere, süreç ve sistem bakımından gerekli denetim yükümlülüğü veri sorumlusu üzerindedir.

---

[339] Dülger, *Verilerin Korunması*, s. 389.

Yürütülen proje sonunda, Kanun'a uyumlu hale gelmiş olmakla yetinilmemeli ve aynı zamanda kişisel verilerin korunması konusunda Kanun'un amacına uygun olarak bir bilinç oluşturulmalı ve veri koruma ve yönetim sisteminin kalıcılığı sağlanmalıdır. Bu amacın gerçek kılınabilmesi adına "uyum projeleri" belirli aşamalara bölünmekte ve bu aşamaların adım adım gerçekleştirilmesi ile veri sorumlularının Kanun kapsamındaki yükümlülüklerini yerine getirmesi sağlanabilmektedir. Bilişim hukuku konusunda uzman hukukçular ve veri güvenliği konusunda uzman kişiler, uygulamada farklı metodlar izleyebilmekte ve farklı uygulamaları takip edebilmektedir[340]. Uygulamalar her ne kadar farklı ise de genel olarak, süreç, bir kişinin genel bir sağlık testinden geçirilerek hastalıklarının tespit edilmesi, bu hastalıkların iyileşmesi adına bir reçete yazılması ve tedavi sürecinin uygulanarak hastanın iyileştirilmesi şeklinde resmedilebilir. Bu kapsamda, uyum projesi sonunda, veri sistemlerinin Kanun'a uyumluluğu ve bu sistemlerin devamlılığının sağlanmasının en önemli husus olduğu ve bunun yeterli olacağı kanaatindeyiz. Bu kapsamda, bir uyum projesinde, kanımızca, takip edilecek aşamalar; (i) uyumun kapsamının belirlenmesi ve başlangıç toplantısı, (ii) veri analizi, (iii) sözleşmelerin incelenmesi, (iv) eğitim, bilinçlendirme ve buna bağlı uyum işlemleri, (v) veri politikaları ve yönergelerinin oluşturulması ve politika ve yönergelere ilişkin uyum işlemleri, (vi) final toplantısı, (vii) VERBİS'e kayıt ve denetim şeklinde olacaktır.

2.3.6.3.1. Uyumun Kapsamının Belirlenmesi ve Başlangıç Toplantısı

Uyum projesine başlanmadan önce ilk olarak, veri sorumlusunun böyle bir projeyi gerçekleştirmeye karar vermesi gerekmektedir. Uygulamada veri sorumluları, maliyeti düşünerek bu projeleri gerçekleştirmekten kaçınsalar da bu projeler uzun vadede karşılaşılacak problemlere nazaran çok daha ucuz ve az maliyetli çalışmalardır[341].

---

[340] Dülger, s. 391 vd.

[341] Kuner, *European Data Protection Law*, s. 75-76.

Projenin gerçekleştirilmesine karar veren veri sorumlularının, daha sonra atacakları ilk adım ise uyumun kapsamının belirlenmesidir. Kanun'a uyum projesinin gerçekleştirilmesine ihtiyaç duyan veri sorumlusu, bu projeyi uzman hukukçular ve veri güvenliği uzmanları ile başlatmadan önce, uyum projesinin neleri kapsayacağı, tahmini olarak ne kadar sürede bu projenin hayata geçebileceğini ve sonraki aşamaları belirleyecektir. Bu doğrultuda, uyum projesi kapsamında gerçekleştirilecek ilk adım uyumun kapsamının belirlenmesi olup bu kapsamın belirlenmesi, veri sorumlusunun ancak aşağıdaki bilgiler ve benzerlerini, uzmanlara bildirmeleri ile mümkün olmaktadır:

- İşletmenin organizasyon şeması ve departmanların listesi,
- İşletme dahilinde gerçek kişi verileri ile temas eden (yaklaşık) kişi sayısı ve şirket çalışan sayısı,
- E-ticaret sayfası ve/veya mobil uygulamalarının bulunup bulunmadığı ya da planlanıp planlanmadığı,
- Taşeron ve/veya hizmet sağlayıcılarının tam listesi ve iş kapsamının kısa açıklaması,
- Tescil ve ilan edilmiş yetki devrine yönelik bir yönetim kurulu iç yönergesi bulunup bulunmadığı,
- Bilgi güvenliğine ilişkin bir sertifika alınıp alınmadığı, alındıysa ilgili sertifikanın hangi kurum tarafından verildiği,
- Veri analizi ile ilgili bir çalışma yapılıp yapılmadığı, yapılıyor ise bunun ne şekilde ve ne kapsamda yürütüldüğü,
- Yurtdışına kişisel veri aktarımı olup olmadığı, oluyorsa hangi ülkeler ile ne tür verilerin paylaşıldığı,
- Hizmetler ile ilgili bağlantılı hizmetler sunulup sunulmadığı, sunuluyor ise bunların hangi kapsamda ne tür verileri içerdiği,
- Hizmetlerin sunumunda dış destek ya da organizasyonlara veri aktarılıp aktarılmadığı, aktarılıyorsa hangi kurumlara hangi tür verilerin aktarıldığı,
- Çalışanlara ilişkin elde edilen (cinsel hayat, ırk, dini inanç vs.) özel bilgilerin kategorize edilmesine dair bir uygulama olup olmadığı.

Bu bilgilerin tam ve doğru olarak, projeyi gerçekleştirecek uzmanlara aktarılması büyük önem arz etmektedir. Zira, bu bilgiler, proje ile ilgili olarak bir çerçeve çizilmesi için gerekli olan bilgilerdir. Somut olaya göre değişkenlik göstermekle birlikte, ilgili bilgiler, tahmini olarak projenin ne süreyle ve ne yoğunlukta yürütülmesi gerektiğini ortaya koyabilecek bilgilerdir ve bu bilgilerle projenin kapsamı tahmini olarak belirlenecektir.

Uyumun kapsamının belirlenmesinin ardından, uyum projesinde gerçekleştirilecek ilk çalışma, başlangıç toplantısıdır. Başlangıç toplantısına, organizasyonun yapısına göre her departmandan bir veya iki yöneticinin katılması ve tüm departmanların koordinasyonu ve veri uyum projesinin işleyen bir şekilde sürdürülebilmesi adına üst düzey ve "sözü geçen" bir yöneticinin bulunması faydalı ve doğru olacaktır[342]. Yapılacak toplantıda, ilk hedef, organizasyonun içinde kişisel verilere dokunan departmanlarda yönetici konumunda bulunan kişileri Kanun ve kişisel verilerin korunması kavram ve konuları hakkında bilinçlendirmek ve bu bilinci ilgili yöneticilere aktarmaktır. Bu bilincin aktarılması, projenin devamı ve tam anlamıyla veri güvenliğinin sağlanması bakımından olmazsa olmaz niteliktedir. Zira, organizasyon piramidinde en yukarıdan en aşağıya doğru bir bilinçlendirme gerçekleştirilmesi, projenin tam anlamıyla yürütülmesi için de doğru bir yöntemdir. Bunun dışında, ilgili kişilere, projenin nasıl yürütüleceği, nelerin yapılacağı ve projenin kapsamı ile ilgili olarak da bilgi verilmesi, proje kapsamında daha sonra yapılacak çalışmaların verimli geçmesi ve doğru ilerleyebilmesi için de büyük önem arz etmektedir.

Başlangıç toplantısında, yapılacak olan bir işlem de veri koruma çalışma grubu olarak da isimlendirilen[343] bir "veri koruma komitesi"nin oluşturulmasıdır. Veri koruma komitesi, başlangıç toplantısından önce belirlenebileceği gibi[344], toplantı

---

[342] Dülger, *Verilerin Korunması*, s. 393.
[343] Dülger, s. 393.
[344] Dülger, s. 394.

esnasında veya hemen sonrasında da belirlenebilir. Bu komite, veri sorumlusu tarafından belirlenebilir ve fakat bu konudaki önerimiz, bu komitenin her bir departmanın başındaki yönetici ve tüm yöneticileri koordine edecek olan üst düzey bir yönetici şeklinde oluşturulmasının isabetli olacağı yönündedir.

Veri koruma komitesi, kişisel verilerin şirket içinde hukuka uygun şekilde elde edilmesinden, muhafazası için gerekli her türlü teknik ve idari tedbirlerin alınmasından, kişisel verilerin doğru ve hukuka uygun şekilde işlenmesinden, gerektiğinde güncellenmesinden, denetimden ve ilgili mevzuatın kendisine yüklediği tüm görevlerin yerine getirilmesinden sorumlu olarak atanacaktır. Veri koruma komitesi aracılığıyla, tüzel kişiliği haiz veri sorumlusu adına kişisel verilerin korunması ile ilgili iş ve işlemler yürütülecek ve Kanun'a uyum işlemi gerçekleştirilecektir. İlgili sorumluluğun devri, bir yönetim kurulu kararı ile olabilecekse de söz konusu yetki devri, Kanun kapsamındaki hukuki ve cezai sorumlukların, veri koruma komitesine aktarılabileceği anlamına gelmemektedir[345].

2.3.6.3.2. Veri Analizi

Başlangıç toplantısının ardından, uyum projesinin en önemli çalışmalarından biri veri analizinin gerçekleştirilmesidir. Veri analizi ile şirketin bir anlamda röntgeni çekilerek boşluk analizi gerçekleştirilecek[346] ve yapılması gerekenler tespit edilecektir.

Veri analizinin gerçekleştirilmesindeki en önemli araç veri envanteridir. Bu doğrultuda, bir veri envanteri örneği, ilgili tüm departmanlara gönderilir ve departmanlardan bu envanteri doldurmaları talep edilir. Veri envanterinin muhtevasının kanuni düzenlemesinde, yukarıda da ifade edildiği üzere, kişisel veri amacı, veri kategorisi, aktarılan alıcı grubu, kişisel verinin tutulacağı azami süre,

---

[345] Gürsel, *İşçinin Kişisel Verileri*, s. 135; "Article 29 Data Protection Working Party", "The Concepts of 'Controller' and 'Processor'", s. 32.

[346] Dülger, *Verilerin Korunması*, s. 403.

yabancı ülkelere aktarılan veriler ve veri güvenliğine ilişkin alınan tedbirler yer alacaktır[347]. Bu kapsamda, kanuni altyapı da yalnızca asgari ölçüde envanterde bulunması gereken unsurlar belirlenmiş olup bu başlıklar projenin kapsamı ve veri sorumlusunun organizasyon yapısına göre farklılıklar arz etmektedir. Bu kapsamda, veri sorumlularının, kişisel veri işleme faaliyetlerini somutlaştıracak nitelikte yöntemler izlemeleri ve veri işleme faaliyetlerini ayrıntılı bir şekilde değerlendirmeleri[348], mevcut durumun tespiti ve veri analizi bakımından önemli bir çalışmadır[349]. GVKT'de bu durumun gerçekleştirilmesi için daha somut ve ayrıntılı yaklaşım ve düzenlemeler bulunmakta olup Türk hukukunda da böyle bir düzenlemenin yapılmasının gerekli olduğunu düşünüyoruz. Öyle ki, veri envanterinin ayrıntılı bir şekilde başlıklara ayrılmış olmasıyla uyum süreçleri bakımından faydalı da olmaktadır. Kanuni düzenlemeden farklı olarak, veri envanterinde veri işleme süreçleri, süreçlerin tanımı, verilerin saklama şekli ve yeri, verilerin nasıl işlendiği[350], veri ömrü ve imha yöntemleri gibi başlıkların veri envanterinde bulunması ve envanteri dolduracak kişilere daha ayrıntılı soruların yöneltilmesi sayesinde ilgili amaca ulaşılabilecektir.

Veri envanterinin eksiksiz olarak doldurulması, özellikle veri sistemindeki boşlukların tespiti ve VERBİS'e kayıt işleminin doğru bir şekilde gerçekleştirilmesi bakımından önem arz etmektedir. Kanunen bir yükümlülük olan ve "mevcut durumun" tespiti için çıkarılması zorunlu olan veri envanteri bakımından amaçlara ulaşmak adına departmanlar ile yapılacak bire bir görüşmeler de büyük fayda sağlamaktadır. Öyle ki, envanter ilgili departmanlara iletilmiş ve envanterdeki başlıklar ayrıntılı bir şekilde hazırlanmış olsa da gerek kişisel verilerin korunmasına ilişkin bilincin henüz tam anlamıyla yerleşmemiş olması gerekse envanteri dolduran kişilerin zaman zaman kendi perspektiflerinden bazı veri işleme süreçlerini önemli görmeyerek envantere işlemiyor olmaları sebebiyle envanterin eksik kalması söz konusu olabilmektedir. Bu bakımdan, projeyi yürüten uzman ekibin, departmanlar

---

[347] "Veri Sorumluları Sicili Hakkında Yönetmelik", m. 4/h.
[348] Carey, *Data Protection Guide*, s. 241.
[349] Dülger, *Verilerin Korunması*, s. 395.
[350] Carey, *Data Protection Guide*, s. 241-242.

ile bire bir toplantılar yaparak, envanterde doldurulmuş kısımların üzerinden beraber geçmeleri ve veri işleme faaliyetinde var olup da envantere işlenmemiş ayrıntıları ve bilgileri güncellemeleri gerekmektedir. Uygulamada, yapılan bu toplantıların, boşluk analizi bakımından da büyük fayda sağladığı görülmektedir.

Envanterin hazırlanış aşaması yaklaşık olarak 2 ile 4 hafta arasında gerçekleşmektedir[351]. Bitirilmiş bir veri envanteri, veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirdikleri kişisel veri işleme faaliyetlerine ilişkin mevcut durumu gösterebilmeli ve kişisel verilerin hangi amaçla işlendiği, bu verilerin nasıl ve nerede saklandığı gibi bilgileri göstermektedir. Veri envanteri, veri işleme faaliyeti ve veri sistemindeki durumu olduğu haliyle gösterecek olup bu haliyle veri envanteri aracılığıyla gerçekleştirilecek analiz sayesinde ilgili eksiklikler tespit edilebilmekte ve veri koruma programı kapsamında problemli yönler için gerekli çalışmalar yapılabilmektedir.

2.3.6.3.3. Sözleşmelerin İncelenmesi ve Taahhütnamelerin Hazırlanması

Veri envanterinin çıkarılmasını takiben, bir sonraki çalışma şirket tarafından imza altına alınmış sözleşmelerin ve/veya tip sözleşme örneklerinin incelenmesidir. Sözleşmeler aracılığıyla kişisel veri aktarımı gerçekleştirilen iş modelleri ve faaliyetler tespit edilerek, daha sonra kişisel veri aktarımı gerçekleştirilen iş ilişkileri bağlamında imzalanan sözleşmeler kapsamında protokoller veya tadilnameler hazırlanarak bu kapsamda veri sorumlusunun çalışanlarla ve 3. kişilerle olan ilişkileri bakımından Kanun'a uyum çalışması gerçekleştirilebilecektir.

Bu kapsamda, sözleşme yapılmaksızın sürdürülen ve kapsamında kişisel veri aktarımı da söz konusu olan bazı iş ilişkileri de olabilir. Örneğin, uygulamada, seyahat acentaları ile şirketler arasında sözleşme imzalanmaksızın iş ilişkisinin

---

[351] Envanterin hazırlanması için hazırlama aşamasından önce envanterde gereğinden fazla çabanın harcanmaması veya gereğinden fazla detaya girilmemesi için bir danışmandan görüş alınması avantajlı olacaktır. Benzer görüş için bakınız: Dülger, *Verilerin Korunması*, s. 395.

sürdürüldüğü durumlara sık sık rastlanmaktadır ve bu iş ilişkisi kapsamında özellikle şirketlerden seyahat acentalarına yoğun bir kişisel veri akışı gerçekleşmektedir. Bu doğrultuda, sözleşme yapılmaksızın sürdürülen ve kapsamında kişisel veri aktarımı da söz konusu olan iş ilişkileri ile ilgili protokollerin imzalanması hukuken isabetli olacaktır.

İlgili protokol/tadilnamelerde ise taraflar arasındaki sözleşmeye veya iş ilişkisine atıfta bulunularak bazı taahhütler verilmektedir. Bu kapsamda, taraflar karşılıklı olarak:

- "İş ilişkisi kapsamında aktarılan verilerin, iş ilişkisinin gerektirdiği ölçüde ve bu ilişki kapsamındaki yükümlülüklerin gerektirdiği çerçevede, hizmetin amacına uygun, işlendiği amaçla bağlantılı ve sınırlı olarak işleneceğini",

- "Kişisel verilerin, ilgili iş ilişkisinin sona ermesine ve/veya kanuni yükümlülüklerin yerine getirilebilmesi için gerekli olan süre sonuna kadar muhafaza edileceğini, kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde verilerin silineceğini, yok edileceği veya anonim hale getirileceğini",

- "Özel nitelikli kişisel veriler bakımından Kanun kapsamındaki yükümlülükler ışığında Kanun'un gerektirdiği yüksek seviye veri güvenliğinin sağlanacağını ve bu kapsamda gerekli açık rızaların ilgili kişilerden alınacağını",

- "Verilerin Kanun'a uygun bir şekilde üçüncü kişilere ve yurtdışına aktarılacağını, tarafların kişisel verilere hukuka aykırı olarak erişilmesini ve/veya kişisel verilerin hukuka aykırı olarak işlenmesini önleyeceğini, bu konudaki tüm teknik altyapıyı sağlayacağını, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin edeceğini, her türlü teknik ve idari tedbiri alacağı, Kanun'a ve ilgili mevzuata uygun davranılacağını",

- "İş ilişkisi kapsamında aktarılan tüm kişisel verilerin, kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde re'sen veya ilgili kişinin talebi üzerine imha edileceğini",

- "Çalışanların Kanun kapsamında eğitileceğini ve çalışanlara gerekli uyarıların yapılacağını, çalışanların, iş ilişkisine bağlı olarak verilen hizmet esnasında Kanun ile ilgili ihlaller gerçekleştirmeleri halinde söz konusu ihlallerden çalışanın işvereni olan tarafın sorumlu olacağını",

- "İş ilişkisi kapsamında, taraflardan birinin Kişisel Verileri Koruma Kurulu'na şikâyet edilmesi halinde bu şikayet kapsamında her türlü belge ve bilginin sağlanacağını, kişisel verisi işlenen gerçek kişi tarafından açılacak olan herhangi bir davada da yine her türlü belge ve bilginin sağlanacağını, ayrıca taraflardan birinin kusurundan kaynaklanan bir nedenle davanın aleyhe neticelenmesi halinde dava sonucunda ortaya çıkan zarar ve ziyanın kusur oranında ilk yazılı talep üzerine karşılanacağını",

- "Sayılan yükümlülüklerin yerine getirilmemesi halinde, tarafların sözleşmeyi tek yanlı olarak feshedebileceğini ve bu kapsamda doğmuş ve doğacak tüm zararın tazmin edileceğini",

kabul ve taahhüt edeceklerdir.

İş ilişkileri kapsamında, bir diğer önemli konu da yurtdışına aktarım hususudur. Ticaretin global hale gelmesi ve her geçen gün iş ilişkilerinin coğrafi olarak sınırlarını kaybetmesi sonrasında, yurtdışına veri aktarımı da dünyada olduğu gibi Türkiye için de önemli ölçüde artış göstermiştir. O kadar ki, dış ticaret bakımından ithalat ve ihracatın, gayri safi milli hasıla ve gayri safi yurtiçi hasılaya olan oranlarının son on yılda önemli bir artış göstermesi de bunun ispatıdır[352]. Bu doğrultuda, yurtdışına kişisel veri aktarımının önemli ölçüde artış gösterdiği tartışmasızdır. Bu sebeple, yurtdışına aktarım ile ilgili hususların tespit edilmesi ve bu doğrultuda Kanun

[352] Ayrıntılı bilgi için bakınız: "Türkiye İstatistik Kurumu", "*Yıllara Göre Dış Ticaret İstatistikleri*". "http://www.tuik.gov.tr/PreTablo.do?alt_id=1046" [Erişim Tarihi: 17.03.2019]

kapsamındaki gerekli yükümlülüklerin yerine getirilmesi gerekmekte olup Kanun'a uyumun gerçekleştirilmesi bakımından da yapılacak bu çalışma büyük önem arz etmektedir.

Çalışanlar ile yapılacak taahhütnamelerin veya iş sözleşmelerinin tadilinin ise bu aşamada uygun bir işlem olmadığı düşüncesindeyiz. Çalışanlara, Kanun kapsamında gerekli eğitimler verilmeli, çalışanlar Kanun ve kişisel verilerin korunması konusunda bilinçlendirilmeli, daha sonra ilgili açık rıza formları, aydınlatma metinleri ve tadil metinleri usulüne uygun bir şekilde çalışanlar ile imzalanmalıdır.

2.3.6.3.4. Eğitim, Bilinçlendirme ve Buna Bağlı Uyum İşlemleri

Veri sorumlusu bakımından, uyum projeleri kapsamında gerçekleştirilmesi gereken çalışmalardan biri de eğitim, bilinçlendirme ve bu süreci takiben yapılması gereken diğer çalışmalardır.

Eğitim çalışması bütün çalışanlara yönelik olarak gerçekleştirilmesi gereken bir çalışmadır[353]. Başlangıç toplantısından farklı olarak, ilgili bilinçlendirme belli bir gruba yönelik olarak değil tüm çalışanlara yönelik olarak verilmek zorundadır. "*Kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin, çalışanların sınırlı bilgileri olsa dahi ilk müdahaleyi yapmaları, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır*"[354].

Kişisel veri güvenliğini ihlal etmeye yönelik saldırılara ek olarak, "verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular da kişisel veri güvenliği ihlallerindendir" ve uygulamada bilinç eksikliğinden dolayı çalışanlar tarafından sıklıkla veriler, veri güvenliği ihlali teşkil edecek şekilde üçüncü kişilerle paylaşılabilmektedir. Yine, kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlikleri

---

[353] Dülger, *Verilerin Korunması*, s. 431.

[354] "Kişisel Verileri Koruma Kurumu", "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)".

sebebiyle kötü amaçlı yazılım içeren elektronik posta ekleri açılabilmekte ve bu durum da veri sistemini saldırılara açık hale getirmektedir.

Tüm bu sebeplerle, "çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, farkındalık çalışmaları yapılması ve güvenlik riskleri konusunda bilinçlendirilmeleri" kişisel veri güvenliğinin sağlanması bakımından hayati önem taşımaktadır. Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken gerekli yetkilendirmelerin somut olaya göre belirlenmesi ve her veriye herkesin erişimi olması halinin önüne geçilmesi gerekmektedir.

Veri sorumlusu, tüm çabalarına rağmen, insan faktörünün varlığından dolayı her zaman ihlaller ile karşılaşabilir. Ve fakat, gerekli eğitim ve bilinçlendirmenin yapılması bu riski minimuma indirmek adına önemli bir adımdır. Kişisel verilerin korunması hakkı ve bu hak kapsamındaki kavramlar konusunda bilgi sahibi olan bir kişinin, bu konuda hiçbir bilgisi olmayan bir kişiye göre daha dikkatli olacağı şüphesizdir[355].

Eğitim ve bilinçlendirme konusunda, uygulamadaki sorular genellikle eğitimin ne şekilde ve ne sıklıkta verilmesi gerektiği ve içeriğinin ne olacağı konularında toplanmaktadır. Büyük ölçekli şirketlerde, eğitimin, çalışanların üç veya dört gruba bölünerek, bu şekilde çalışanlara eğitim verilmesi gerektiği ve eğitimin çalışanlara uzman kişiler tarafından verilmesi gerektiği düşüncesindeyiz. Eğitimin içeriğinde ise genel olarak Kanun ve Kanun kapsamındaki düzenlemelere odaklanmak gerekmekte ise de bunun yanında uyum projesinin içeriği, Kanun'a uyulmadığında ortaya çıkabilecek olası senaryolar ve belli başlı uluslararası düzenlemeler hakkında da çalışanların mutlak surette bilinçlendirilmesi gerekmektedir. Eğitim bir seferle sınırlı olmamalı ve kişisel verilerin korunması hususundaki bilincin kalıcı hale gelmesi sağlanmalıdır. Bu konuda farklı yöntemler izlenebilir. Örneğin, eğitimler bir yıllık

[355] Dülger, *Verilerin Korunması*, s. 432.

periyodik aralıklarla tekrarlanabileceği[356] gibi, çalışanlara Kanun ile ilgili mini testler ve/veya hatırlatma mailleri gönderilerek bu konudaki bilinçlerinin kalıcı hale getirilmesi sağlanabilecektir.

Yukarıda ifade edildiği üzere, çalışanların eğitimi, veri güvenliği açısından çok büyük önem arz etmektedir. Bunun yanında, veri sorumlusunun, Kanun kapsamında uyması gereken aydınlatma yükümlülüğü veya açık rıza alınması gibi konularda da eğitim ve bilinçlendirmenin ön koşulu olduğu kanaatindeyiz. Yine, çalışanlar ile yapılacak taahhütnameler veya iş sözleşmelerinde yapılacak tadiller de en azından ilk eğitim verildikten sonra yapılmalıdır kanaatindeyiz. Ancak bu şekilde çalışanların vermiş oldukları açık rızalar veya ilgili metinlere atmış oldukları imzalar tam anlamıyla geçerli ve kişisel verilerin korunması hakkının özüne ve ruhuna uygun olacaktır.

Açık rıza metinleri ile ilgili olarak, ilk yapılması gereken çalışma açık rıza alınması gereken alanların tespit edilmesi ve zorunlu olmayan alanlarda olabildiğince açık rıza alınmasından kaçınılmasıdır[357]. Böylece, hem potansiyel idari para cezaları bertaraf edilecek hem de ilgili kişinin açık rızasını geri alması riski en düşük seviyeye indirilmiş olacaktır. Bu tespit yapıldıktan sonra ise öncelikle çalışanlardan daha sonra açık rıza alınması gereken başkaca durumlar var ise diğer ilgili kişilerden, açık rıza alınmasındaki esas ve usullere uyulmak suretiyle açık rıza alınmalıdır. Yukarıda da ifade edildiği üzere, açık rıza alınan metinlerin yazılı olması veri sorumlusunun ispat yükü bakımından önemli ve gereklidir.

Aydınlatma yükümlülüğü bakımından, açık rıza metinleri bakımından geçerli olan alan tespiti durumu aydınlatma metinleri için de geçerlidir. Bu bakımdan, kişisel verilerin işlendiği veya işleme amacının değiştiği veya farklı amaçlarla farklı verilerin toplandığı her durumda aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir. Bu bakımdan, aydınlatma yükümlülüğünün yerine getirilmesi uyum projesinin en temelinde yer alan ve "canlı" bir yapı olarak sürdürülmesi gereken

[356] Carey, *Data Protection Guide*, s. 245.
[357] Dülger, *Verilerin Korunması*, s. 215.

önemli bir çalışmadır. Aydınlatma metinleri bakımından da aydınlatma yükümlülüğü bakımından gerekli esas ve usullere uyulmak suretiyle ilgili metinlerin hazırlanması gerekmektedir.

Son olarak, çalışanlara imzalatılacak aydınlatma metinleri ve bu kapsamda yapılacak tadiller veya imzalatılacak taahhütnameler de eğitim sonrası yapılması gereken önemli çalışmalardandır. Çalışanlar, aydınlatma metinlerinde verilerin toplanma yöntemleri, toplanma amaçları, aktarım amaçları ve aktarıma konu 3. kişiler, silme ve imha süreleri ve yöntemleri konusunda bilgilendirilmeli ve aydınlatma metinlerinde ayrıca veri güvenliğine ilişkin çalışanlara yönelik uyarı niteliğindeki hükümler de bulunmalıdır. Aydınlatma metnine ilişkin imza alındıktan sonra, çalışanlar ile taahhütnameler imzalanabileceği gibi iş sözleşmeleri bu kapsamda tadil de edilebilir. İş sözleşmesinde kısaca aydınlatma metnine veya metindeki bilgilere de atıfta bulunmak suretiyle veri güvenliğine ilişkin kurallara uyulmaması halinde oluşacak zararla ilgili kusur oranında rücu hakkının saklı olduğu ve bunun fesih sebebi oluşturduğu yönündeki hükümler yeterli ve faydalı olacaktır.

2.3.6.3.5. Veri Politikaları ve Yönergelerinin Oluşturulması, Politika ve Yönergelere İlişkin Uyum İşlemleri

Uyum projesinde, yapılması gereken en mühim çalışmalardan biri de veri politikalarının ve yönergelerinin oluşturulmasıdır. Politikalar, kişisel verilerin koruması bakımından oluşturulacak veri yönetim sisteminde bir rehber niteliğindedir. Bu bakımdan, hazırlanması gereken ilk politika, genel bir "veri politikası"nın oluşturulmasıdır. İlgili politika, kişilere, veri sorumlusunun kişisel verilerin korunması ile ilgili olarak izlemiş olduğu yol haritasını göstermek bakımından önemli bir belge niteliğindedir.

Söz konusu politika, amaç, kapsam ve tanımlar başlıklarının yanı sıra, veri koruma komitesinin görev sorumlularını, veri koruma ilkeleri, ilgili kişilerin hakları, açık rıza alanları, veri güvenliği ve veri paylaşımına ilişkin yöntem, amaç ve ilkeler, kayıt

yöntemleri ve denetim gibi başlıkları da içerecektir. İçerik olarak sade ve anlaşılabilir nitelikte olması gereken bu politika, çalışanların ve diğer 3. kişilerin anlayabileceği bir dilde kaleme alınmalıdır[358]. Hazırlanan bu politika, bir temenni niteliğinde değil, gerçekleri tüm açıklığıyla gösterir nitelikte bir belge olmalıdır ve veri sorumlusu politika içeriğinde bulunan hususları takip ve uygulama konusunda gerekli adımları atmalıdır[359].

Hazırlanacak "veri politikası", aynı zamanda veri sorumlusu tarafından oluşturulacak diğer KVKK politikalarına da bir temel olacak olup veri sorumlusu, veri güvenliğine ilişkin alacağı teknik ve idari tedbirleri, KVKK politikaları ve yönergelerinde ayrıntılı bir şekilde belirleyecektir. Bu belgeler, kısaca, Veri Saklama ve İmha Politikası, Veri İhlali Yönetimi Prosedürü, Kayıt, Dosyalama ve Arşiv Yönergesi, Veri Aktarım ve Veri Güvenliği Politikası, Talep Yönetim Yönergesi, Veri Disiplin Yönergesi olarak ifade edilebilir. Veri sorumlusu, ilgili politika ve yönergelerde belirlediği idari ve teknik tedbirlere uygun davranmakla yükümlü olup, gerektiği ölçüde de ilgili belgeleri güncel tutması, veri güvenliği bakımından büyük önem arz etmektedir. Veri sorumlusu, bu politika ve yönergeleri, tek bir Yönetim Kitapçığı altında birleştirebileceği gibi ayrı ayrı olarak da dosyalama gerçekleştirebilir. Bu politikaların en önemlilerinden biri olan, Veri Saklama ve İmha Politikası bakımından, Kurum, 10 Mart 2019 tarihinde, "Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama ve İmha Politikası" başlığı altında veri sorumlularına örnek olması için kendi politikasını internet sayfasında yayınlanmıştır[360].

Politikaların ve yönergelerin hazırlanmasını takiben, söz konusu belgelerin şirket içinde yürürlüğe konulması ve içeriğinde bulunan gerekli idari ve teknik tedbirlerin uygulanması çok önemlidir. Özellikle, saklama ve imha politikalarında belirlenen sürelere uygun olarak, veri sorumlusunun silme, yok etme veya anonimleştirme işlemlerini gerçekleştirmesi ve bir anlamda yüklerinden kurtulması gerekmektedir.

---

[358] Kuner, *European Data Protection Law*, s. 55.

[359] Kuner, s. 58.

[360] Ayrıntılı bilgi için bakınız: https://kvkk.gov.tr/Icerik/5387/KVKK-Kisisel-Veri-Saklama-ve-Imha-Politikasi [Erişim tarihi: 17.03.2019]

"Bir gün işe yarar" mantığıyla değil, gereklilik ilkesine uygun olarak veri işlemenin önemi ışığında, veri sorumlusu saklama ve imha politikaları dahil tüm politika ve yönergelerde belirlediği önlemleri zaman kaybetmeksizin uygulamaya koymalı ve kişisel verilerin korunmasına yönelik olarak gerekli bilincin yerleşmesi adına gerekli çabayı göstermelidir.

2.3.6.3.6. Final Toplantısı, VERBİS'e Kayıt ve Denetim

Yukarıda ifade edilen uyum çalışmalarının gerçekleştirilmesini takiben, uygulamada, başlangıç toplantısına benzer bir final toplantısı yapılarak, sürecin en başından itibaren final toplantısına kadar geçen sürede ne şekilde işlediği ve neler yapıldığı konusunda bir toplantı daha gerçekleştirilmesinin isabetli olduğu düşüncesindeyiz. Bu sayede, özellikle, projenin bitimini takiben, kişisel verilerin korunması ile ilgili süreçleri ve prosedürleri takip edecek olan Veri Koruma Komitesinin tüm süreci ayrıntılı olarak hatırlamaları faydalı olmaktadır.

Bu toplantıda, ayrıca bir irtibat kişisinin belirlenmesi ve VERBİS'e kayıt işlemlerinin gerçekleştirilmesi de yararlı olmaktadır. İrtibat kişisi, Kurum ile kurulacak iletişim için VERBİS'e kayıt esnasında bildirilen gerçek kişi olup, süreçlere hakim birinin Kurum ile daha sağlıklı bir iletişim yürütebileceği düşünüldüğünde bu kişinin Veri Koruma Komitesi içinden belirlenmesi, Kurum ile daha doğru bir iletişim kurulabilmesi bakımından önemlidir.

VERBİS'e kayıt işleminin ise, uzmanların gözetimi altında ve final toplantısı esnasında yapılması, sistemin içeriğinin veri koruma komitesine aktarılması ve sistemin içinde barındırdığı fonksiyon ve içeriklerin daha iyi anlaşılabilmesi açısından faydalıdır. Bu sebeple, VERBİS'e kayıt işlemlerinin de final toplantısında gerçekleştirilmesi veya bu işlemin ayrı bir toplantı esnasında yapılması gerektiği kanaatindeyiz. VERBİS'e kayıt işleminin son işlem olarak yapılmasının, özellikle veri envanterinin son haline getirilmesi ve VERBİS'e işlenecek bilgiler bakımından önem arz ettiğini düşünüyoruz. Veri sorumlusu, uyuma ilişkin gerekli işlemleri yapmasını

takiben VERBİS'e kaydolduğunda, veri güvenliği bakımından en düşük risk halindeyken bu işlemi yapmış ve Kurul tarafından gerçekleştirilmesi muhtemel soruşturmaları da bir şekilde bertaraf edebilecektir.

Uyum projesinin son aşaması ise denetim aşamasıdır. Uyum projesini takiben gerçekleştirilecek denetim, veri işleyenin denetimi ve şirket için denetim olarak iki başlık altında değerlendirilebilir. Veri sorumlusu, veri işleyen ile yapacağı ve veri aktarımına ilişkin protokolün yanı sıra, veri sorumlusu veri işleyeni düzenli aralıklarla denetlemeli ve yönlendirmelidir[361]. Veri güvenliği ve ihlallerden sorumluluk bakımından bu denetim gerekli bir çalışmadır. Diğer denetim ise uyum projesi tamamlandıktan sonra uyum projesinin ve veri yönetim sisteminin, yapılan çalışmaya uygun işleyip işlemediğinin denetlenmesidir. Bu denetimin yapılmasının bir sebebi de, Türk kişisel veri koruma hukukunun çok yeni bir alan olması sebebiyle yeni düzenlemelere gebe olması ve bu durumun sürekli bir güncellemeyi gerektirmesidir. Denetimlerin, ne sıklıkla yapılacağı veri sorumlusunun yönetim hakkı kapsamında belirleyeceği bir husus olsa da bu sürenin altı ayı geçmemesinin ve uzman hukukçular ve veri güvenliği uzmanları eşliğinde yapılması gerektiğini düşünmekteyiz.

2.3.7. Veri Sorumluları Bakımından Öngörülen Denetim ve Yaptırım Mekanizması

Kanun'da kişisel verilerin korunması amacına uygun olarak hukuki, idari ve cezai yaptırım sistemleri belirlenmiş ve benimsenmiştir. Yaptırım mekanizmaları büyük önem arz etmekteyse de kişisel verilerin korunması bakımından oluşturulan denetim mekanizması çok daha mühim ve uygulayıcı konumundadır. Bu bakımdan, Kanun'da bağımsız bir denetim organı olarak Kişisel Verileri Koruma Kurulu düzenlenmiş bulunmaktadır. Kanun m. 22'de Kurul'un yetkileri ayrıntılı bir şekilde düzenlenmiş bulunmakta olup bu yetki ve görevler, denetim, düzenleme ve yönetim olarak üç başlık altında değerlendirilebilecektir[362]. Bu doğrultuda, Kurul veri sorumlularını kişisel

[361] Dülger, *Verilerin Korunması*, s. 421.
[362] Küzeci, "Veri Sorumlusu", s. 366; Kişisel Verilerin Korunması Kanunu, m. 22.

verilerin korunması hakkı ve Kanun altındaki yükümlülükleri bakımından denetleyecek, kendisine ilgili kişilerden gelen şikayetleri değerlendirecek ve karara bağlayacak, inceleme başlatabilecek ve Kanun altında düzenlenen yaptırımlara karar verecektir. Yine, kişisel verilerin korunması bakımından, kanun altından soyut bir şekilde düzenlenmiş hükümleri somutlaştırmaya yönelik olarak rehberler hazırlayarak kişisel verilerin işlenmesine ilişkin ilkeleri ve önlemleri belirleyecek gerekli düzenleyici işlemleri yürütecektir. Son olarak, yönetim yetkisi kapsamında Kurum ile ilgili idare ve yönetime ilişkin belirli kararları alacaktır[363].

Kurul, Kanun ile düzenlenmiş yetkileri çerçevesinde yaptırım uygulayabilecektir. Ve fakat, yaptırım sistemi yalnızca idari para cezaları ile sınırlı olmayıp Kanun'da öngörülen yaptırım sistemi, *tazminat, idari yaptırım ve cezai yaptırım* olarak üç ayrı yaptırım mekanizmasından oluşmaktadır.

Tazminata ilişkin olarak, Kanun m. 11 kapsamında, "ilgili kişi veri ihlalinden dolayı zarara uğraması halinde zararın giderilmesini talep etme hakkına ve m. 14 kapsamında genel hükümlere göre tazminat talep etme hakkına" sahiptir. Bu doğrultuda, ilgili kişi, "Türk Medeni Kanunu m. 24 ve 25 düzenlemelerinden" yararlanabilir. Kişilik hakları zedelenen kişi, TMK m. 24-25 hükümleri ışığında ilgili kişi, "kişilik haklarına yöneltilen saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini" mahkemeler aracılığıyla talep edebilir. "*İşçi ayrıca maddi ve manevi tazminat isteyebileceği gibi, hukuka aykırı saldırı nedeniyle elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre iadesini de isteyebilecektir*"[364].

Kişisel verilerinin veri sorumlusu tarafından hukuka aykırı olarak işlenmesinin, cezai sonuçları da bulunmaktadır. Kanun m. 17 ile cezai yaptırımlar bakımından Türk Ceza Kanunu'na atıfta bulunularak öngörülmüştür. Bu doğrultuda, Türk Ceza Kanunu'nun 135. maddesi ve 140. maddesi arasındaki hükümler bakımından veri sorumluları için

---

[363] Küzeci, "Veri Sorumlusu", s. 366.

[364] Mollamahmutoğlu, Astarlı, ve Baysal, *İş Hukuku*, s. 720.

cezai yaptırımlar öngörülmüştür. Bu çerçevede TCK m 135'te "*kişisel verilerin kaydedilmesi suçu*", m. 136'da "*verileri hukuka aykırı olarak verme veya ele geçirme suçu*", m. 137'de bu suçların nitelikli halleri, m. 138'de "*verilerin yok edilmemesi suçu*" ve m. 140'da ise bu suçlara ilişkin olarak tüzel kişiler hakkında uygulanacak güvenlik tedbirleri düzenlenerek, kişisel verilerin korunmasının cezai yaptırım mekanizmaları ile de korunması amaçlanmıştır. Kişisel verilerin işlenmesinin ise cezai yaptırım mekanizmaları ile korunmaması ise eleştirilmiştir[365]. Cezai yaptırımlar bakımından ifade etmek gerekir ki, hapis cezası yalnız gerçek kişiler için uygulanabilecek bir yaptırım olup uygulamada zarara neden olan ihlallerin kurumsal politikalardan kaynaklandığı düşünüldüğünde[366] uygulamada hiçbir araştırma ve ayrım yapılmaksızın tüzel kişinin tüm yönetim kurulu üyeleri ve/veya üst düzey yöneticileri hakkında sanık olarak dava açılması halleri hukuka ve hakkaniyete aykırılık oluşturmaktadır. Bu bağlamda, savcılara ve soruşturma makamlarına detaylı ve gerçekçi bir soruşturma yaparak gerçek sorumluların bulunması ve bunlar hakkında dava açılması bakımından önemli bir sorumluluk düşmektedir[367].

Son olarak, işçinin kişisel verilerini hukuka aykırı bir biçimde işleyen veri sorumluları bakımından Kanun'da idari yaptırımlar da öngörülmüştür. Kanun m. 18'de "Kabahatler" başlığı altında düzenlenen idari yaptırımlar yalnızca veri sorumlusu olan gerçek ve tüzel kişiler bakımından öngörülmüştür. Buna göre;

- "Aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar",
- "Veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar",
- "Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar[368]",

---

[365] Dülger, "Türk Ceza Kanunu Bağlamında Kişisel Verilerin Korunması", s. 124.
[366] Küzeci, "Veri Sorumlusu", s. 375.
[367] Dülger, "Türk Ceza Kanunu Bağlamında Kişisel Verilerin Korunması", s. 125.
[368] Örneğin bakınız. "Kişisel Verileri Koruma Kurulu'nun *Kurul Kararının gereğinin süresi içinde yerine getirilmemesi* başlıklı 16/10/2018 tarihli ve 2018/118 sayılı Kararı". Ayrıntılı bilgi için bakınız: "https://www.kvkk.gov.tr/Icerik/5406/Kurul-Karar-Ozetleri" [Erişim tarihi: 30.05.2019]

- "Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar",

idari para cezası verilir. Kabahatler başlığının da, bazı düzenlemeler bakımından kapsayıcı nitelikte olmaması ve bazı yükümlülükler bakımından idari para cezası öngörülmemiş olması eleştirilmiştir[369]. İdari yaptırımlar bakımından belirsiz ve eleştiriye açık bir diğer konu da cezaların eylem bazlı mı kişi bazlı mı gerçekleşeceği sorunsalıdır. Bu kapsamda, ihlal başına idari para cezası belirlenebileceği düşünülse de tavanı belli olmayan bir idari yaptırım mekanizması öngörülmesi hakkaniyete uygun hareket edilmesi ilkesine aykırılık oluşturacağı açıktır. Öte yandan, yükümlülüklerini yerine getirmeyen veri sorumluları bakımından, söz konusu idari yaptırımların, etkili ve caydırıcı nitelikte de olması gerekmektedir. Bu bağlamda, hakkaniyet ve caydırıcılık unsurları arasında bir denge kurulması gerektiği kanaatindeyiz. İdari yaptırım cezası uygulanırken, ihlalin niteliği, ağırlığı ve süresi, işlenilen verinin türü ve işleme amacıyla, ihlalden zarar gören kişi sayısı ve zarar miktarı gibi hususların, verilecek olan kararda belirleyici olması faydalı olacaktır[370].

---

[369] Küzeci, *Kişisel Verilerin Korunması*, s. 371.

[370] Benzer bir uygulama için bakınız: Genel Veri Koruma Tüzüğü, m. 83/2.

SONUÇ

Teknolojik gelişmelerin, özellikle son otuz yıl içinde büyük bir ivme kazanması, veri koruma hukukunun da gelişimini tetiklemiştir. Veri koruma hukukunun ve bu anlamda kişisel verilerin korunmasının temel amacı, verilerin hukuka aykırı olarak kaydedilmesini önlemek ve bu veriler üzerinde gerçekleştirilen bütün işlemlerin hukuka uygunluğunu sağlamaktır. Kişinin bilgileri, adresi, mesleği, medeni durumu, doğum tarihi, tabiiyeti, mahkumiyet durumu gibi kişisel bilgilerinin korunması ve hukuka uygun olarak işlenmesi, veri koruma hukukunun alanına girmekte ve kişilerin temel haklarının korunması açısından büyük önem arz etmektedir.

Avrupa Birliği bünyesinde kişisel verilerin önemi ve korunmasına dair farkındalık oldukça eskiye dayanmaktadır. "1948 tarihli Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi", ve "1950 tarihli Avrupa İnsan Hakları Sözleşmesi"ne baktığımızda kişisel verilerin korunmasına dair çalışmaların mevcudiyeti görülmekte olup, 1995 yılından itibaren kişisel verilerin işlenmesi ve bu türdeki verilerin serbest dolaşımı bakımından bireylerin korunmasına ilişkin "Avrupa Birliği Direktifi 95/46/EC" yürürlüğe girmiştir. Teknolojinin gelişmesi ile ortaya çıkan ihtiyaçların karşılanması adına ise, "Avrupa Birliği Genel Veri Koruma Tüzüğü" ("General Data Protection Regulation" / "GDPR") 2016 yılında kabul edilmiş ve 25 Mayıs 2018 tarihinde "95/46/EC sayılı Direktif"i ilga etmek suretiyle yürürlüğe girmiştir. Bu düzenleme, günümüz dünyasında büyük yankı uyandırmıştır. GVKT ile modern dünyanın doğal sonuçlarından olan yoğun veri akışını düzene sokmak adına kişisel verilerin işlenebilmesi için daha sıkı şart ve kurallar öngörülmüş; yükümlülüklerin ihlali halinde çok daha ciddi cezalar getirilmiştir.

Kişisel verilerin korunması ve hukuka uygun işlenmesi alanında son dönemde evrensel olarak yaşanan en dikkat çekici olay ise Amerika Birleşik Devletleri Kongre'sinde algı yönetimi yapmakla ve Amerika Birleşik Devletleri başkanlık seçimlerine doğrudan etki etmekle suçlanan Facebook'un CEO'su Mark Zuckerberg'in ifade vermesi olmuştur. Bu olaydan sonra, kişisel verilerin korunması hakkı ve veri koruma hukukunun popülerliği tüm dünyada daha yaygın hale gelmiştir. Teknolojinin durdurulamaz biçimde gelişiyor olması ve her gün yeni bir teknolojinin tüketicinin kullanımına sürülüyor olması

sebebiyle bu hukuk dalının ve kişisel verilerin korunması hakkının çok daha önemli bir alan haline geleceği de öngörülmektedir. Kişisel verinin ötesinde, veri her geçen gün dünya için çok daha kıymetli bir hale gelmekte ve ülkeler, kuruluşlar, kişisel verilerin korunmasının ötesinde verinin korunması ve saklanmasını hukuki temele oturtmak adına çalışmalar yapmakta ve düzenlemeler getirmektedirler[371].

Dünyada veri koruması alanındaki gelişmeleri takiben, Türkiye'de uygulamaya giren Kişisel Verilerin Korunması Kanunu yayım tarihinden iki sene sonraya denk gelen ve Kanun'un Geçici 1. Maddesi ile belirlenen geçiş döneminin sonu olan 7 Nisan 2018 tarihinden itibaren büyük yankı uyandırmış ve son dönemde toplumun dikkatini çeken ve popüler hale gelen bir Kanun olarak karşımıza çıkmıştır.

Günümüzde veri sorumluları, KVKK kapsamında getirilen yükümlülüklere uyum sağlayabilmek için çalışmalar yapmakta ve geç de olsa, bünyelerinde uyum süreci başlatmış bulunmaktadır. Bu sayede, veri sorumluları ve işleyenler, üstlendikleri hukuki ve cezai sorumluluğun farkına varmakta ve yükümlülüklerini yerine getirmektedir.

Uyum projeleri, kişisel verilerin korunması bakımından önemli bir çalışma ise de uygulamada veri sorumlularının elini kolunu bağlar nitelikte önemli belirsizlikler mevcuttur. Yine, Türk hukuku uygulaması ve mevzuatında, kişisel verilerin korunması hukuku AB hukuku uygulama ve mevzuatının bazı yönleriyle gerisinde kalmış olup özellikle çocuk verileri, tasarımda gizlilik gibi konuların Türk hukuku düzenlemesinde mevcut olmaması AB'ye uyum süreçlerini de etkilemekte ve bu durum eleştirilmektedir[372]. Kurul kararlarıyla, kişisel verilerin korunması hukuku ile ilgili dünyadaki ileri düzey düzenleme ve uygulamalar takip edilmeye çalışılmakta veya Türk Hukuku uygulaması dünyadaki benzerlerine yaklaştırılmaya çalışılmaktaysa da bu çabanın yakın dönemde önemli bir sonuç doğurması beklenmemektedir.

---

[371] Kişisel veri niteliğinde bulunmayan verilerin serbest dolaşımına ilişkin olarak AB tarafından 2018/1807 sayılı ve 14 Kasım 2018 tarihli "Kişisel Nitelikte Olmayan Verilerin Serbest Dolaşımı Hakkında Tüzük" yayımlanmış bulunmakta olup, ilgili tüzük Mayıs 2019'da yürürlüğe girecektir. Ayrıntılı bilgi için bakınız: "https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1546942605408&uri=CELEX:32018R1807" [E.T: 17.03.2019]

[372] "Turkey 2018 Report".

Bu konudaki kanaatimiz, Kurul'un ve Türk kanun koyucusunun, kişisel verilerin korunması hukuku alanında, uygulama ve mevzuattaki eksikliklerini tespit etmesi ve bu konuda çalışma yapması; toplumu bilinçlendirme çalışmalarının sayısının arttırılarak toplumdaki ilgili kişilerin de bu konuda bilgi sahibi olmasının sağlanması ve veri sorumlularının da menfaatleri göz önünde bulundurularak çözümsüz konulara ilgili kişilerin temel hak ve özgürlükleri ile veri sorumlularının menfaatleri arasında bir denge bulmak suretiyle çözümler bulunması gerektiği yönündedir. Kısa süre içinde olmasa da önümüzdeki on yıllık süreçte, Türk kişisel verilerin korunması hukukunun önemli gelişmelere gebe olduğu ve bu gelişmelerin veri sorumlusu kavramı temelinde ilerleyeceği düşünülmektedir. Bu gelişmeleri takiben, Türk kişisel verilerin korunması hukuku uygulamalarının ve bu hukuk dalındaki teorik tartışmaların, dünyadaki muadillerini yakalayacağı ümit edilmektedir.

KAYNAKÇA

Basılı Kaynaklar

AKİPEK, Jale/AKINTÜRK, Turgut, ATEŞ KARAMAN, Derya. *Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku*. B. 1, C. 1, İstanbul: Beta Yayıncılık, 2011.

AKSOY, Hüseyin Can. *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*. B.1, Ankara: Çakmak Yayınevi, 2010.

ALTAŞ, Hüseyin. *Medeni Hukuk Başlangıç Hükümleri (TMK m. 1-7)*. B. 10, Ankara: Yetkin Basımevi, 2018.

BAŞALP, Nilgün. *Kişisel Verilerin Korunması ve Saklanması*. B. 1, Ankara: Yetkin Basımevi, 2004.

BELLIA, Patricia L./ BERMAN, Paul Schiff/ FRISCHMANN, Brett/ POST, David G. *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age*. B. 5, Amerika Birleşik Devletleri: West Academic Publishing, 2018.

BOZKURT YÜKSEL, Armağan Ebru. *Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing)*. B. 1, Ankara: Yetkin Basımevi, 2016.

BUELLESBACH, Alfred/ GIJRATH, Serge/ POULLET, Yves/ PRINS, Corien. *Concise European IT Law*. B. 2, United Kingdom: Kluwer Law International, 2010.

BYGRAVE, Lee Andrew. *Data Privacy Law: An International Perspective*. B. 1, United Kingdom: Oxford University Press, 2014.

CAREY, Peter. *Data Protection: A Practical Guide to UK and EU Law*. B. 5, United Kingdom: Oxford University Press, 2018.

ÇEKİN, Mesut Serdar. *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*. B. 1, İstanbul: On İki Levha Yayıncılık, 2018.

DAVENPORT, Thomas. *Big Data @ Work*. B. 1, İstanbul: Türk Hava Yolları Yayınları, 2018.

DEHON, Estelle / CAREY, Peter. *Data Protection: A Practical Guide to UK and EU Law*. B. 5, United Kingdom: Oxford University Press, 2018.

DÜLGER, Murat Volkan. *Kişisel Verilerin Korunması Hukuku*. B. 1, İstanbul: Hukuk Akademisi, 2019.

GÜRSEL, İlke. *İşçinin Kişisel Verilerinin Korunması Hakkı*. B. 1, Ankara: Adalet Yayınevi, 2016.

HENKOĞLU, Türkay. *Bilgi Güvenliği ve Kişisel Verilerin Korunması*. B. 1, Ankara: Yetkin Basımevi, 2015.

KUNER, Christopher. *European Data Protection Law, Corporate Compliance and Regulation*. B. 2, United Kingdom: Oxford University Press, 2007.

KÜZECİ, Elif. *Kişisel Verilerin Korunması*. B. 2, Ankara: Turhan Kitabevi, 2018.

LAMBERT, Paul. *Understanding the New European Data Protection Rules*. B. 1, Amerika Birleşik Devletleri: CRC Press, 2017.

LESSIG, Lawrence. *Code Version 2.0*. B. 1, New York: Basic Books, 2006.

MAYER-SCHÖNBERGER, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*. B. 2, Amerika Birleşik Devletleri: Princeton University Press, 2011.

MOLLAMAHMUTOĞLU, Hamdi/ASTARLI, Muhittin/BAYSAL, Ulaş. *İş Hukuku*. 6. bs. Ankara: Turhan Kitabevi, 2014.

OKUR, Zeki. "*Türk İş Hukukunda İşçinin Kişisel Verilerinin Korunması Hakkı*". *İş Dünyası ve Hukuk*, Prof. Dr. Tankut Centel'e Armağan, 2011.

ŞİMŞEK, Oğuz. *Anayasa Hukukunda Kişisel Verilerin Korunması*. B. 1, İstanbul: Beta yayıncılık, 2008.

TAŞTAN, Furkan. *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. B. 1, İstanbul: On İki Levha Yayıncılık, 2017.

UNCULAR, Selen. *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*. B. 1, Ankara: Seçkin Yayıncılık, 2014.

VOIGT, Paul/ VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. İsviçre: Springer, 2017.

WHITAKER, Reg. *The End of Privacy: How Total Surveillance Is Becoming a Reality*. B. 1, Amerika Birleşik Devletleri: The New Press, 2000.

YAVUZ, Can. *İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması - Unutulma Hakkı*. B. 1, Ankara: Seçkin Yayıncılık, 2016.

Elektronik Kaynaklar

Acquisti, Alessandro. "The Economics of Personal Data and the Economics of Privacy". OECD Privacy Guidelines, Aralık 2010. https://www.oecd.org/sti/ieconomy/46968784.pdf.

Acquisti, Alessandro, ve Ralph Gross. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook". Cambridge, 2006. https://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

Andrews, B. J., ve T. DePellegrin. "HeLa sequencing and genomic privacy: the next chapter". *Bethesda Medicine* 3, sy 8 (2013).

Başalp, Nilgün. "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri". *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 21, sy 1 (2015): 77-104.

Bellia, Patricia L., Paul Schiff Berman, Brett Frischmann, ve David G. Post. *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age*. 5. bs. ABD: West Academic Publishing, 2018.

Bergkamp, Lucas, ve Jan Dhont. "Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web". *EDI Law Review*, sy 7 (2000): 71-114.

Cavoukian, Ann. "Privacy by Design The 7 Foundational Principles", Ocak 2011. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

Cavoukian, Ann, ve Jeff Jonas. "Privacy by Design in the Age of Big Data". *Privacy By Design*, 08 Haziran 2012. https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf.

Cengiz, Serkan. "Avrupa İnsan Hakları Mahkemesi Kararları Işığında Yaşam Hakkı". *Türiye Barolar Birliği Dergisi*, sy 93 (2011): 383-404.

Colonna, Liane. "Europe Versus Facebook: An Imbroglio of EU Data Protection Issues". *Law, Governance and Technology*, Data Protection on the Move Current Developments in ICT and Privacy/Data Protection, 24 (2015): 25-51.

Disis, Mary L. "Movie Review of The Immortal Life of Henrietta Lacks". *Journal of American Medical Association* 318, sy 24 (2017): 2410-12.

Dülger, Volkan. "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması". *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* 3, sy 2 (2016): 101-67.

Ercan, Ahmet, ve Melis Bostanoğlu. "AB Veri Güvenliği Ekosisteminin Yörüngesindeki Türkiye'den Notlar". İktisadi Kalkınma Vakfı, Ocak 2018.

Fritsch, Clara. "Data Processing in Employment Relations: Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at TheWorksite". *Reforming European Data Protection Law*, Privacy and Data Protection, sy 20 (2014): 147-71.

Fritz, Gernot. "CJEU Rules on Joint Controllership – What Does This Mean for Companies?", 07 Ağustos 2018. https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies.

Gantz, John, ve David Reinsel. "Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East". International Data Corporation Digital Universe, ubat 2013. https://www.emc.com/collateral/analyst-reports/idc-digital-universe-united-states.pdf.

Halevy, Alon, Peter Norvig, ve Fernando Pereira. "The Unreasonable Effectiveness of Data". IEEE Computer Society, 2009. https://static.googleusercontent.com/media/research.google.com/tr//pubs/archive/35179.pdf.

Handbook on European Data Protection Law. 2018 Edition. Luxembourg: Publications Office of the European Union, 2018.

Karlıdağ, Serpil. "Ekonomi Politik Açıdan Kisisel Verilerin Korunması". *Amme İdaresi Dergisi* 46, sy 1 (Mart 2013): 127-52.

Kiss, Attila, ve Gergely László Szoke. "Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation". *Reforming European Data Protection Law*, Privacy and Data Protection, 20 (2014): 311-33.

Korenhof, Paulan, Jef Ausloos, Ivan Szekely, Meg Ambrose, Giovanni Sartor, ve Ronald Leenes. "Timing the Right to Be Forgotten: A Study into 'Time' as a Factor in Deciding About Retention or Erasure of Data". *Springer Privacy and Data Protection Series*, Reforming European Data Protection Law, 20 (2014): 171-203.

Korff, Douwe. "New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments". European Commision DG Justice, Freedom And Security, 2010. https://papers.ssrn.com/sol3/Data_Integrity_Notice.cfm?abid=1638949.

Kuner, Christopher. *European Data Protection Law, Corporate Compliance and Regulation*. 2. bs. United Kingdom: Oxford University Press, 2007.

Küzeci, Elif. "Veri Sorumlusunun Yükümlülükleri". *Veri Sorumlusunun Yükümlülükleri*. İstanbul, 2019.

Lawrence, Early. "Science, Technology and Human Rights: The Role of Data Protection". *Human Rights in the Twenty-First Century*, A Global Challenge, 2 (1993): 801-15.

Manav, Eda. "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması". *Gazi Fakültesi Hukuk Fakültesi Dergisi* 19, sy 2 (2015): 95-136.

Markou, Christina. "Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination". *Springer Law, Governance and Technology Series*, Data Protection on the Move Current Developments in ICT and Privacy/Data Protection, 24 (2015): 213-49.

Mei, Peter. "The EC Proposed Data Protection Law". *Law and Policy in International Business* 25, sy 1 (1993).

"Principles of Consent: Deceased People", 2018. http://www.hra-decisiontools.org.uk/consent/principles-deceased.html.

Prins, Corien. "Property and Privacy: European Perspectives and the Commodification of Our Identity". *Kluwer Law International*, 2006, 223-57. https://www.recht.nl/doc/10.Prins.pdf.

"Questions and Answers - Data protection reform package", Mayıs 2017. http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm.

"Regulations, Directives and other acts", t.y. https://europa.eu/european-union/eu-law/legal-acts_en.

Samuelson, Pamela. "Privacy as Intellectual Property?" *Stanford Law Review* 52 (Mayıs 2000): 1125-73. http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf.

Taddei, Stefano, ve Bastianina Contena. "Privacy, Trust and Control: Which Relationships with Online Self-Disclosure?" *Computers in Human Behavior 29*, sy 3: 821-26. Erişim 09 Mart 2019. http://isiarticles.com/bundles/Article/pre/pdf/74907.pdf.

Tan, Domingo R. "Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union". *Loyola of Los Angeles International and Comparative Law Review* 21, sy 4 (1999): 661-84. https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1488&context=ilr.

"The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society". European Commision, 23 Haziran 2017. https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf.

The Information Commissioner's Office. "Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Aree". The Information Commissioner's Office, 2018. https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

Tortop, Nuri. "İletişim ve Bilgi Edinme Hakkı". *Amme İdaresi Dergisi* 37, sy 1 (Mart 2004): 29-44.

Trepte, Sabine, ve Leonard Reinecke. "The Social Web as a Shelter for Privacy and Authentic Living". *Privacy Online*, Perspectives on Privacy and Self-Disclosure in the Social Web, Ağustos 2011, 61-75. https://link.springer.com/content/pdf/10.1007%2F978-3-642-21521-6.pdf.

Trepte, Sabine, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, ve Fabienne Lind. "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)". *Reforming European Data Protection Law*, Privacy and Data Protection, 20 (Haziran 2014): 333-66.

Tüfekçi, Zeynep. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites". *Bulletin of Science, Technology & Society* 28, sy 1 (2008): 20-36. https://www.academia.edu/4701484/Can_You_See_Me_Now_Audience_and_Disclosure_Regulation_in_Online_Social_Network_Sites.

Uygun, Murat. "Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması". Yüksek Lisans Tezi, Gazi Üniversitesi, 2010.

Yücedağ, Nafiye. "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri". *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 75, sy 2 (2017): 765-90.

Zanfir, Gabriela. "Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right". *Springer Privacy and Data Protection Series*, Reforming European Data Protection Law, 20 (2014): 227-53.

Raporlar, Rehberler ve İnternet Siteleri

Article 29 Data Protection Working Party. "Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'". Article 29 Data Protection Working Party, ubat 2010. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

"Başrolde Siyaset Yerine Teknoloji: Tallin Dijital Zirvesi", 15 Ekim 2017. https://bulten.ikv.org.tr/?ust_id=8122&id=8129.

Clarke, Roger. "Beyond the OECD Guidelines: Privacy Protection for the 21st Century", 04 Ocak 2000. http://www.rogerclarke.com/DV/PP21C.html.

"Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens", 19 Mart 2018. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

GANTZ, John, ve David Reinsel. "Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East". International Data Corporation Digital Universe, ubat 2013. https://www.emc.com/collateral/analyst-reports/idc-digital-universe-united-states.pdf.

Kişisel Verileri Koruma Kurumu. "100 Soruda Kişisel Verilerin Korunması Kanunu". KVKK Yayınları, Nisan 2018. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf.

Kişisel Verileri Koruma Kurumu. "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)". KVKK Yayınları, t.y. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf.

Kişisel Verileri Koruma Kurumu. "Kişisel Verilerin İşlenme Şartları". KVKK Yayınları, t.y. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8c90423f-97ea-4d81-a7c1-ace74295c2b8.pdf.

Kişisel Verileri Koruma Kurumu. "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler". KVKK Yayınları, t.y. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/d0fbca08-30af-41fe-a7c9-65663b9c5231.pdf.

Kişisel Verileri Koruma Kurumu. "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi". KVKK Yayınları, t.y. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf.

Kişisel Verileri Koruma Kurumu. "Veri Sorumluları Sicili Rehberi". KVKK Yayınları, t.y. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/1ac84b2a-e12f-4dc8-a779-3fb166cb6756.pdf.

Kişisel Verileri Koruma Kurumu. "Veri Sorumlusu ve Veri İşleyen". KVKK Yayınları, t.y. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf.

"Principles of Consent: Deceased People", 2018. http://www.hra-decisiontools.org.uk/consent/principles-deceased.html.

"Questions and Answers - Data protection reform package", Mayıs 2017. http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm.

"Regulations, Directives and other acts", t.y. https://europa.eu/european-union/eu-law/legal-acts_en.

"The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society". European Commision, 23 Haziran 2017. https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf.

The Information Commissioner's Office. "Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Aree". The Information Commissioner's Office, 2018. https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

"Turkey 2018 Report". Commision Staff Working Document. Strasbourg: European Commision, 2018.

Ek -1

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 18/06/2019

Tez Başlığı: **TÜRK HUKUKUNDA VERİ SORUMLUSU KAVRAMI**

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 121 sayfalık kısmına ilişkin, 17/06/2019 tarihinde tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 7'dir.

Uygulanan filtrelemeler:

1- ☒ Kabul/Onay ve Bildirim sayfaları hariç
2- ☒ Kaynakça hariç
3- ☒ Alıntılar hariç
4- ☐ Alıntılar dâhil
5- ☒ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza
18.06.2019

Adı Soyadı:	Mesut Halıcıoğlu
Öğrenci No:	N15229690
Anabilim Dalı:	Özel Hukuk
Programı:	Özel Hukuk Yüksek Lisans Programı

DANIŞMAN ONAYI

UYGUNDUR.

Prof. Dr. Erkan Küçükgüngör

Ek-1

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
MASTER'S THESIS ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF PRIVATE LAW

Date: 18/06/2019

Thesis Title : **DATA CONTROLLER CONCEPT UNDER TURKISH LAW**

According to the originality report obtained by my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 17/06/2019 for the total of 121 pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is 7 %.

Filtering options applied:

1. ☒ Approval and Decleration sections excluded
2. ☒ Bibliography/Works Cited excluded
3. ☒ Quotes excluded
4. ☐ Quotes included
5. ☒ Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Date and Signature
18.06.2019

Name Surname: Mesut Halıcıoğlu
Student No: N15229690
Department: Private Law
Program: Private Law Master's Programme

ADVISOR APPROVAL

APPROVED.

Prof. Dr. Erkan Küçükgüngör

Ek-2

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ ÇALIŞMASI ETİK KOMİSYON MUAFİYETİ FORMU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 18.06.2019

Tez Başlığı: **TÜRK HUKUKUNDA VERİ SORUMLUSU KAVRAMI**

Yukarıda başlığı gösterilen tez çalışmam:

1. İnsan ve hayvan üzerinde deney niteliği taşımamaktadır,
2. Biyolojik materyal (kan, idrar vb. biyolojik sıvılar ve numuneler) kullanılmasını gerektirmemektedir.
3. Beden bütünlüğüne müdahale içermemektedir.
4. Gözlemsel ve betimsel araştırma (anket, mülakat, ölçek/skala çalışmaları, dosya taramaları, veri kaynakları taraması, sistem-model geliştirme çalışmaları) niteliğinde değildir.

Hacettepe Üniversitesi Etik Kurullar ve Komisyonlarının Yönergelerini inceledim ve bunlara göre tez çalışmamın yürütülebilmesi için herhangi bir Etik Kurul/Komisyon'dan izin alınmasına gerek olmadığını; aksi durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza
18.06.2019

Adı Soyadı:	Mesut Halıcıoğlu
Öğrenci No:	N15229690
Anabilim Dalı:	Özel Hukuk
Programı:	Özel Hukuk Yüksek Lisans Programı
Statüsü:	☒ Yüksek Lisans ☐ Doktora ☐ Bütünleşik Doktora

DANIŞMAN GÖRÜŞÜ VE ONAYI

Prof. Dr. Erkan Küçükgüngör

Detaylı Bilgi: http://www.sosyalbilimler.hacettepe.edu.tr
Telefon: 0-312-2976860 **Faks:** 0-3122992147 **E-posta**: sosyalbilimler@hacettepe.edu.tr

EK-2

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
ETHICS COMMISSION FORM FOR THESIS

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF PRIVATE LAW

Date: 18. 06.2019

Thesis Title: Data Controller Concept Under Turkish Law

My thesis work related to the title above:

1. Does not perform experimentation on animals or people.
2. Does not necessitate the use of biological material (blood, urine, biological fluids and samples, etc.).
3. Does not involve any interference of the body's integrity.
4. Is not based on observational and descriptive research (survey, interview, measures/scales, data scanning, system-model development).

I declare, I have carefully read Hacettepe University's Ethics Regulations and the Commission's Guidelines, and in order to proceed with my thesis according to these regulations I do not have to get permission from the Ethics Board/Commission for anything; in any infringement of the regulations I accept all legal responsibility and I declare that all the information I have provided is true.

I respectfully submit this for approval.

Date and Signature
18.06.2019

Name Surname:	Mesut Halıcıoğlu
Student No:	N15229690
Department:	Law
Program:	Private Law Master's Programme
Status:	☒ MA ☐ Ph.D. ☐ Combined MA/ Ph.D.

ADVISER COMMENTS AND APPROVAL

Prof. Dr. Erkan Küçükgüngör