T.C.
KALKINMA BAKANLIĞI

AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ'NÜN GETİRDİĞİ YENİLİKLER ve TÜRK HUKUKU BAKIMINDAN DEĞERLENDİRİLMESİ

ÇALIŞMA RAPORU - 6

Ayşe Nur AKINCI

İKTİSADİ SEKTÖRLER ve KOORDİNASYON
GENEL MÜDÜRLÜĞÜ

Haziran 2017

T.C.
KALKINMA BAKANLIĞI
Yayın No: 2968

AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ'NÜN GETİRDİĞİ YENİLİKLER ve TÜRK HUKUKU BAKIMINDAN DEĞERLENDİRİLMESİ

Çalışma Raporu - 6

Ayşe Nur AKINCI

İKTİSADİ SEKTÖRLER ve kOORDİNASYON GENEL MÜDÜRLÜĞÜ
Bilgi Toplumu Dairesi Başkanlığı

Haziran 2017

ISBN 978-605-9041-85-0

Bu yayın 300 adet basılmıştır.

İÇİNDEKİLER

YÖNETİCİ ÖZETİ

Kişisel verilerin korunması tüm dünyada uzun yıllardan beri çalışıla gelmiş bir konu olmakla birlikte, konu tarihsel süreç ve teknolojinin gelişimi karşısında hızla boyut değiştirmekte, küresel BİT hizmetlerinin yaygınlaşması ve ülkeler arasında artan veri trafiği nedeniyle sosyal ve iktisadi açıdan uluslararası önemi haiz bir konuma gelmektedir. Zira başta sosyal ağlar, bulut bilişim, büyük veri analizi, lokasyon bazlı hizmetler ve akıllı kart gibi teknolojik gelişmeler ve küreselleşmenin getirdiği zorunluluklar olmak üzere pek çok etken kişisel verilere erişim, verilerin toplanması ve kullanımı yöntemlerini derinden etkilemekte ve değiştirmektedir. Bu nedenle, son yıllarda ülkelerin veri koruma hukuki altyapılarını güncel teknolojik gelişmelerle uyumlaştırma yönündeki çabalarının arttığı görülmektedir.

AB'de 1995 yılında yürürlüğe giren 95/46/AT sayılı AB Veri Koruma Direktifi kişisel verilerin korunması alanında tüm dünyada kabul gören bir çerçeve sunuyordu. Ancak yukarıda ifade edilen gelişmeler sonucunda, Avrupa Komisyonu tarafından üye ülkelerde uygulanmakta olan AB veri koruma kurallarında, Veri Koruma Direktifi'nde benimsenen ilkelerin modernize edilmesi ve gelecekte vatandaşların mahremiyet hakkının garanti altına alınması amacıyla, kapsamlı bir reforma gidilmesi ihtiyacı ortaya çıkmıştır. Bu kapsamda, AB veri koruma kurallarında köklü bir reformu ihtiva eden "Genel Veri Koruma Tüzüğü (General Data Protection Regulation–GDPR)" Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde onaylanmıştır.

Türkiye'de kişisel verilerin korunmasına ilişkin yasal düzenleme çalışmaları 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı "Kişisel Verilerin Korunması Kanunu" ile önemli bir aşama kaydetmiştir. 6698 sayılı Kanun, AB Veri Koruma Reformu kapsamında hazırlanan GDPR metninin Avrupa Parlamentosu'nda kabulünden kısa bir süre önce yürürlüğe girmiştir. Kanun'un yürürlüğe girmesiyle ülkemiz BİT sektörünün başta yurt dışına bilgi toplumu hizmetleri sunabilmesi, kişisel verinin temel girdi olduğu sektörlerde ülkemizin iş potansiyelinin artması, sınır ötesi veri paylaşımı ve adli işbirliği kanallarının etkin çalışmasının sağlanması için önemli bir adım atılmıştır. Ancak, 6698 sayılı Kanun'un güncel AB düzenlemesi olan GDPR'den ziyade 95/46/AT sayılı Veri Koruma Direktifi'ni referans alıyor olması nedeniyle, söz konusu Kanun'un GDPR açısından değerlendirilmesi ihtiyacı ortaya çıktığı düşünülerek bu çalışma hazırlanmıştır.

Çalışma kapsamında öncelikle Veri Koruma Direktifi'nin temel prensipleri ve düzenlemeleri açıklanmış, sonra da GDPR'in bu bağlamda getirdiği yenilikler incelenmiştir. Ardından 6698 sayılı Kanun'un GDPR ile ne ölçüde uyumlu olduğu ve hangi noktalarda farklılaştığı ele alınarak ülkemizdeki mahremiyet mevzuatı ve uygulamalarının GDPR'ye uyum sağlamasına yönelik öneriler geliştirilmiştir. Raporda; 6698 sayılı Kanun'un temel esaslar itibarıyla GDPR'yle büyük ölçüde uyumlu olduğu, söz konusu temel esasların uygulanmasına yönelik tedbirler açısından ise GDPR'nin getirdiği bazı yenilikler açısından eksik kaldığı, bu yeniliklerin bir kısmı Kanun'da değişiklik gerektirirken bir kısmının da Kanun'a istinaden çıkarılacak ikincil düzenlemelerle karşılanabileceği sonucuna varılmıştır.

1. GENEL ÇERÇEVE VE ÇALIŞMANIN AMACI

Sanayi sonrası toplum düzenine geçişle birlikte bilgi ve iletişim teknolojilerinin (BİT) giderek yaygınlaşması kişisel verilerin toplanması, depolanması, işlenmesi ve dağıtılmasını önemli ölçüde kolaylaştırmıştır. Veri işleme teknolojisindeki bu hızlı gelişim ise kamu ve özel sektörün kişisel verilere bakış açısında sürekli bir değişimi doğurmuş, veri koruması politikalarının bu doğrultuda gelişmesini sağlamıştır. Bu süreç kişisel verilerin korunması sorununun bir hukuki düzenleme alanı olarak ortaya çıkmasını doğal olarak beraberinde getirmiştir. BİT sayesinde hızla gelişen otomatik veri işleme teknolojisinin doğurduğu mahremiyet sorunları ilk kez 1960'lı yılların sonlarında kişisel verilerin korunmasına yönelik kanunların ortaya çıkmasına neden olmuştur. Sanayi toplumundan bilgi toplumuna geçiş sürecini yaşamakta olan gelişmiş ülkelerde, başta Amerika Birleşik Devletleri (ABD) ve Avrupa Birliği (AB) ülkeleri olmak üzere, bireysel hak ve özgürlüklerin zarar göreceğine ilişkin endişeler karşısında bu alanda hayata geçirilen hukuki düzenlemeler eliyle kişisel mahremiyetin korunması amaçlanmıştır. Bu çerçevede, bilgi toplumunun en temel sorunlarından biri olan, bireylerin devlet organları ve diğer kişiler karşısında özel yaşam alanına müdahalenin önlenmesi ve kendileri hakkındaki verilerin işlenmesine ilişkin hukuki çerçevenin çizilmesini amaçlayan bir hukuk alanı ortaya çıkmıştır.

Kişisel verilerin korunmasına yönelik ilk ulusal hukuk düzenlemeleri; 1970 yılında Almanya, 1973 yılında İsveç ve 1974 ABD'de yapılan yasa metinleri olarak ifade edilmektedir.[1] 1970'li yıllarda yapılan bu ulusal düzenlemelere paralel olarak 1980'li yıllardan itibaren, başta İktisadi İşbirliği ve Kalkınma Teşkilatı'nın (OECD) kılavuz ilkeleri ve Avrupa Konseyi'nin kişisel verilerin otomatik işlenme karşısında korunması hakkındaki sözleşmesi olmak üzere, uluslararası hukuk belgelerinde kişisel verilerin korunması hakkı kabul edilmiştir. 1980'li yılların sonlarında ise kişisel verilerin korunması hakkı özel hayatın gizliliği genel kavramından bağımsız, ayrı ve öne çıkan bir kamu politikası alanı olarak ele alınmaya başlanmıştır. Söz konusu alanın gelişme gösterdiği bu dönemde göze çarpan temel husus, gelişmiş siyasal ve ekonomik yapıya sahip bu ülkelerde aynı politika alanında benzer hukuki çözümlerin üretildiği, başka bir ifadeyle bu alanda sağlanan politika uyuşması olgusudur.[2] 1990'lı yıllarda ortaya çıkan internet teknolojisi ise beraberinde getirdiği geniş ağ bağlantısı imkânı ve elektronik ticarette kişisel verilerin yoğun kullanımı dolayısıyla daha önce sağlanan bu uyumu bozmuş ve farklı veri koruma mevzuatlarına sahip ülkeler bakımından uyuşmazlıklar baş göstermeye başlamıştır. 11 Eylül saldırıları sonrası güvenlik mülahazalarıyla terörle mücadele kapsamında kişisel verilerin toplanması ve işlenmesi hususunda kararlı ve agresif politikalar ortaya koyan ABD yaklaşımı bu alandaki dönüm noktalarından biri olmuştur. AB tarafında kişisel verilerin korunması temel bir insan hakkı olarak ele alınıp bağımsız denetçi kurumların gözetimine teslim eden yasalar eliyle düzenlenirken ABD tarafında bireylere bir takım haklar tanınmakla birlikte uygulamada yeknesaklığı sağlayacak bağımsız bir kurum oluşturulmamış, yalnızca dar kapsamlı sektörel bazı düzenlemelere yer verilmiştir. Kişisel verilerin korunması konusunda dünyadaki düzenlemelere bakıldığında hukuk tekniği bakımından üç temel yaklaşım ön plana

[1] KÜZECİ, Elif; Kişisel Verilerin Korunması, Ankara, Turhan Kitabevi, 2010.
[2] GÜR, İkbal; Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Ankara, Turhan Kitabevi, 2010, sh. 3.

çıkmaktadır; kişisel verinin korunması hakkında genel bir veri koruma kanunu (data protection act) çıkartmak, farklı sektörlere yönelik özel hayatın gizliliğine ilişkin kanuni düzenlemeler (privacy act) yapmak ve *"Habeas data*[3]*"* yaklaşımını benimsemek.[4] Bu açıdan AB'de ve ülkemizde ilk yaklaşımın ABD'de ise ikinci yaklaşımın benimsendiği görülmektedir.

Kişisel verilerin korunması, 1960'lardan beri çalışıla gelmiş olan bir konu olmakla birlikte konu tarihsel süreç ve teknolojinin gelişimi karşısında giderek boyut değiştirmekte, küresel BİT hizmetlerinin yaygınlaşması ve ülkeler arasında artan veri trafiği nedeniyle sosyal ve iktisadi açıdan uluslararası önemi haiz bir konuma gelmektedir. Bu çerçevede, son yıllarda ülkelerin veri koruma hukuki altyapılarının uyumlaştırılması çabalarının arttığı dikkat çekmektedir. BİT hizmetleri alanında korumacı yaklaşım güden bazı ülkeler veri koruma mevzuatlarını sıkılaştırarak yabancı şirketlerin yerel pazarlarına erişimini zorlaştırmakta, bu yolla yerel BİT şirketlerine avantaj sağlamaya çalışmaktadır. BİT hizmetleri ihracatçısı ülkeler ise ilişkide olduğu pazarların veri koruma alanındaki gereksinimlerini karşılamaya yönelik tedbirler almaktadır. Yoğun kişisel veri kullanımı olan sağlık, sigorta, finans gibi geleneksel hizmetlerde de yurtdışı pazarlara erişim için veri koruma mevzuatı önem arz etmektedir.[5]

Türkiye'de kişisel verilerin korunmasına ilişkin yasal düzenleme çalışmaları 2000'li yılların ilk yarısından itibaren gündemde olmasına ve müteaddit defalar tasarı olarak TBMM'ye sunulmasına rağmen söz konusu kanunlaştırma çalışmaları ancak 2016 yılında tamamlanabilmiştir. 24 Mart 2016 tarihinde Meclis Genel Kurulu'nda kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu" 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Kanun'un yürürlüğe girmesiyle ülkemiz BİT sektörünün başta AB ülkeleri olmak üzere yurt dışına bilgi toplumu hizmetleri sunabilmesi, kişisel verinin temel girdi olduğu finans, sağlık, sigorta gibi sektörlerde ülkemizin iş potansiyelinin artması ve sınır ötesi veri paylaşımı ve adli işbirliği kanallarının etkin çalışmasının sağlanması için büyük bir adım atılmıştır. Kişisel Verilerin Korunması Kanunu'yla, Türkiye'nin AB ülkeleri nezdinde veri koruma bakımından güvenilir ülke statüsüne kavuşma konusunda önemli bir kriter yerine getirilmiştir.

Bilindiği üzere 95/46/AT sayılı AB Veri Koruma Direktifi kişisel verilerin korunması alanında tüm dünyada kabul gören bir çerçeve sunmaktadır. Söz konusu Direktif kişisel verilerin kazara kaybını, yetkisiz kişilerin eline geçmesini ve bu kişilerce yasadışı bir biçimde imha edilmesini önlemek amacıyla uygun teknik ve kurumsal önlemlerin alınmasına yönelik hükümler içermektedir. Bununla birlikte, başta sosyal ağlar, bulut bilişim, lokasyon bazlı hizmetler ve akıllı kart gibi teknolojik gelişmeler ve küreselleşmenin getirdiği zorunluluklar olmak üzere pek çok etken kişisel verilere erişim, verilerin toplanması ve kullanımı

[3] Habeas Data: Bireyler tarafından mahkemeye verilen bir dilekçe kanalıyla, görüntüsünün, özel hayatının ve kişisel verilerinin geleceğini belirleme ve bu verilere erişme haklarının korunmasını sağlayan bir bireysel şikâyet yoludur. Brezilya, Peru ve Arjantin başta olmak üzere Latin Amerika ülkelerince anayasal bir hak olarak kabul edilmiştir.

[4] KAYA, Cemil; İdare Hukukunda Bilgi Edinme Hakkı, Seçkin yayınları, Ankara, 2005, sh.97.

[5] Kalkınma Bakanlığı; Bilgi Toplumu Dairesi Başkanlığı, 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı.

yöntemlerini derinden etkilemiş ve değiştirmiştir. Buna ek olarak 1995 yılında yürürlüğe giren AB Veri Koruma Direktifi'nin 27 AB ülkesinde birbirinden farklı uygulanma biçimleri ortaya çıkmıştır. Bu farklılığı ortadan kaldıracak çerçeve bir düzenlemenin mevcut ülkeler arası farklılaşmayı ve işletmeler bakımından yıllık 2,3 milyar Euro'ya varan tasarruf anlamına gelen pahalı idari yükleri ortadan kaldıracağı öngörülmüştür.

Bu gelişmeler ışığında 2012 yılı Ocak ayı itibarıyla Avrupa Komisyonu tarafından Avrupa Birliği (AB) üye ülkelerinde uygulanmakta olan AB veri koruma kurallarında kapsamlı bir reforma gidilmesi önerilmiştir. Bu reformun amacı 1995 yılından beri uygulanmakta olan Veri Koruma Direktifi'nde benimsenen ilkelerin geliştirilmesi ve gelecekte vatandaşların mahremiyet hakkını garanti altına almak için güncellenmesi olarak belirlenmiştir. Bu amaç kapsamında çalışmalarına dört yıl önce başlanan ve AB veri koruma kurallarında köklü bir reformu ihtiva eden "Genel Veri Koruma Tüzüğü (General Data Protection Regulation–GDPR)" Avrupa Parlamentosu (AP) tarafından 14 Nisan 2016 tarihinde onaylanmıştır. GDPR'nin yürürlüğe girmesinin ardından halen uygulanmakta olan 95/46/EC sayılı AB Veri Koruma Direktifi yürürlükten kalkmıştır. Bu tarihten itibaren söz konusu GDPR hükümleri tüm üye devletlerde doğrudan bağlayıcı hale gelmiştir. Üye devletlerin GDPR hükümlerini ulusal hukuk sistemlerine dâhil edebilmeleri için iki yıllık süre öngörülmektedir.

Bu çalışmada; kişisel verilerin korunması konusunda AB'de 1995 yılından beri uygulanmakta olan Veri Koruma Direktifi genel hatlarıyla anlatılacak, Direktif kapsamında öngörülen kişisel verilerin korunmasına yönelik yasal ve kurumsal yapılar incelendikten sonra 2016 yılında kabul edilen yeni GDPR ve getirilen temel yenilikler ele alınacaktır. Ülkemiz bakımından model düzenlemeleri teşkil eden bu iki hukuki düzenlemenin karşılaştırmalı incelemesinin ardından Türkiye'de kişisel verilerin korunmasına ilişkin var olan yasal ve kurumsal düzenlemeler bütünsel bir bakış açısıyla incelenerek ülkemiz mevzuatının güncel AB mevzuatı karşısındaki hukuki durumu ele alınacak ve AB Veri Koruma Reformunun ülkemiz mevzuatına etkileri değerlendirilecektir. Bu çerçevede, mevcut 6698 sayılı Kanun ve bu Kanun'un uygulanmasından sorumlu Veri Koruma Otoritesi ile ihtiyaç duyulan ikincil düzenlemelere ilişkin öneriler geliştirilecektir.

2. AVRUPA BİRLİĞİ DÜZENLEMELERİ

2.1. 95/46/AT sayılı Veri Koruma Direktifi

2.1.1. Genel Bilgiler

1980'li yıllardan itibaren veri işleme teknolojisinde meydana gelen gelişmeler nedeniyle, AB vatandaşlarının üçüncü kişilere tevdi ettikleri verilerin kontrolü konusundaki tereddütler giderek artarken söz konusu kişisel verilerin ticari amaçlarla kullanımının yaygınlaşması Tek Pazar bakımından üye devletlerde farklı uygulamaların ortaya çıkmasına neden olmuştur. Bu döneme kadar gerek OECD Rehber İlkeleri gerekse Avrupa Konseyi'nin ilgili Sözleşmeleri kişisel verilerin korunması bakımından atılması gereken somut adımları sunamamış, dolayısıyla AB üyesi ülkeler bakımından ulusal kanunlar arasında uyum ve standartlaşma sağlanamamıştır. Tüm bu gelişmeler Avrupa Komisyonu'nun 1990 yılında taslak Veri Koruma Direktifi'ni yayımlaması ihtiyacını doğurmuştur. Komisyon tarafından hazırlanan bu metin daha sonra yapılan çalışmalarla gözden geçirilerek Bakanlar Konseyi tarafından *"Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 95/46/AT sayılı Direktif"* adı altında 20 Şubat 1995 tarihinde kabul edilmiştir.[6] Söz konusu Direktif 24 Ekim 1995 tarihinde onaylanmasının ardından üç yıl sonra yürürlüğe girmiştir. Bu noktada şu hususun ifade edilmesinde fayda bulunmaktadır; Birlik hukuku bakımından kanun yapma araçları arasında yer alan direktifler genellikle doğrudan bağlayıcı değildir. Bu düzenlemeler üye ülkeler bakımından birer uyumlaştırma aracı olarak kullanılmakta olup üye devletlerin bu düzenlemelerde yer alan temel ilkeleri yansıtan ulusal mevzuat hükümlerini kendi hukuk sistemlerine derc etmeleri gerekmektedir. Direktifin kabulünü takiben tüm üyelere ulusal veri koruma düzenlemelerini Direktifle uyumlu hale getirme görevi verilmiş olmaktadır.

Veri Koruma Direktifi kişisel verilerin korunmasına ilişkin ulusal mevzuatların uyumlaştırılarak kişisel verilerin tüm AB ülkelerinde aynı düzeyde ve benzer ilkeler çerçevesinde korunması ve bu yolla kişisel verilerin söz konusu ülkelerde herhangi bir güvenlik riski bulunmaksızın serbest dolaşımını sağlamayı amaçlamaktadır. Böylece bireylerin mahremiyetinin yüksek koruma altına alınması ile bilginin serbest dolaşımının sağlanması arasında bir denge oluşturmaya çalışılmaktadır.

2.1.2. Veri Koruma Direktifi'nin Kapsamı

Yedi temel bölümden oluşan Direktif'te sırasıyla genel hükümler, hukuka uygunluk sebepleri, hukuki tedbirler, sorumluluk ve yaptırımlar, kişisel verilerin üçüncü ülkelere transferi, davranış kuralları, denetleyici (teftiş) otorite ve topluluk düzeyinde uygulama tedbirleri bölümleri yer almaktadır.[7] Direktif'in kapsamını belirleyen 3. maddesine göre bu Direktif bir dosyalama sisteminin parçasını oluşturan ya da oluşturması istenen gerçek kişilere

[6] Direktif'in İngilizce tam metni için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML, (Erişim Tarihi: 29.05.2016).

[7] CİVELEK, YÜKSEL Dilek, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Dpt Uzmanlık Tezi, Nisan 2011, sh. 73.

ait kişisel verilerin, otomatik veya otomatik olmayan araçlarla işlenmesi durumunda uygulama alanı bulmaktadır. Bu kapsamda gerek elektronik ortamda tutulan veriler gerekse elle işlenen kişisel veriler bakımından söz konusu verilerin özel kriterlere göre erişilebilir ve yapılandırılmış olması gerektiği anlaşılmaktadır. Ayrıca burada belirtilmesi gereken bir diğer önemli husus ise Direktif'in koruma konusunun yalnızca gerçek kişiler olduğudur, tüzel kişiler bakımından söz konusu hükümlerin koruma etkisi bulunmamaktadır.

Getirilen koruma ile BİT sektörünün gelişmesinin yanı sıra kişisel verileri işlenen gerçek kişilerin korunması sağlanmaktadır. Veri Koruma Direktifi kapsamında getirilen koruma düzeyi, kuralların uygulanışı bakımından hiçbir fark gözetilmeksizin hem kamu hem de özel sektör için aynıdır.

Direktif, kişisel verilerin işlenmesi hususunda oldukça kapsamlı bir yaklaşımı yansıtmakla birlikte 3(2) maddesinde bu Direktif hükümlerinin uygulama alanı bulmayacağı iki istisnai durum belirlenmiştir. Bunlardan ilki kamu güvenliği, savunma ve devletin güvenliğine ilişkin işlemelerde ve devletin ceza hukuku alanındaki faaliyetleri gibi AB hukukunun uygulama alanı dışında kalan faaliyetlerinde Direktif hükümleri uygulanmayacaktır. İkinci istisnai durum ise gerçek bir kişinin tamamen kişisel veya evi ve ailesiyle ilgili olan veri işlemelerinde Direktif hükümleri uygulanmayacaktır. Bununla birlikte bu madde hükmünde yer alan "kişisel veya evi ve ailesiyle ilgili olan veri işlemelerinde" ifadesinden verilerin belirli sayıda kişiyle paylaşılmaktan ziyade belirsiz sayıda kişiye ifşa edildiği veri işlemelerinin Direktif'in kapsamından çıkarılamayacağı değerlendirilmektedir.

Veri Koruma Direktifi teknoloji tarafsız - teknolojik araçlardan bağımsız olarak - kişisel verinin işlendiği her tür durumda uygulanma imkânına sahiptir.[8]

2.1.3. Veri Koruma Direktifi'ndeki Temel Kavramlar

Veri Koruma Direktifi kendine özgü terminolojisi ile pek çok kavramı içermektedir. Bu bölümde, kişisel veri hukuku bakımından da sıklıkla kullanılmakta olan bu kavramların, kavramsal tartışmalara girilmeksizin, AB Direktifi'ndeki karşılıkları yer almaktadır.

i) *Kişisel Veri*: Direktif'in 2/a maddesinde *"kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri"* olarak tanımlamaktadır. Direktif'te belirlenen kişisel veri kapsamı oldukça geniş olmakla birlikte sınırsız değildir. Yalnızca isim, adres veya kimlik numarası gibi doğrudan bireyin kimliğine atfedilen bilgiler değil elektronik ticaret sırasında gerçekleştirdiği işlem kayıtları, tıkladığı kısayollar, konumunun belirlenmesine yarayan görüntü kayıtları gibi kişisel tercih belirten ve bireye ulaşılmasını sağlayan hemen her türden veri kişisel veri sayılmaktadır.
ii) *Kişisel verilerin işlenmesi (işleme):* Kişisel verilerin otomatik ya da otomatik olmayan araçlarla toplanması, saklanması, elde edilmesi, değiştirilmesi, okunması, sorulması, kullanılması, üçüncü taraflara aktarılması, yayılması ya da

[8] CİVELEK, D., age, sh. 75.

hazır bulundurulması için yapılan işlemlerle verilerin kombinasyonu, bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü müdahale "işleme" kabul edilmektedir. Bu çerçeveden bakıldığında kişisel verilerin işlenmesi tanımı, kişisel verilerin hemen hemen her türlü kullanımını içeren, verinin kayıt altına alınmasından yok edilmesine kadar birçok işlemi ifade etmektedir.

iii) *Kişisel veri dosyalama sistemi:* Merkezileşmiş, merkezileşmemiş yahut fonksiyonel veya coğrafik esasa dayanarak dağılmış ve belirli kriterlere göre erişilebilir her türlü yapılandırılmış kişisel veri dizisine dosyalama sistemi adı verilmektedir.

iv) *Veri kontrolörü:* Direktif'e göre kişisel veri işlemenin amaçlarını ve yöntemini birlikte veya tek başına belirleyen kişi, organ, ajans veya kamu kurumunu ifade etmektedir. Veri kontrolörleri gerçek kişiler olabildiği gibi özel ve/veya kamu kurumu tüzel kişiliğini haiz kişiler de olabilir. Müvekkili hakkındaki kayıtları tutan avukat veri kontrolörünün gerçek kişi olduğu duruma örnek gösterilebilir. Bir tüzel kişi bünyesinde çalışan gerçek kişiye tüzel kişiliğin uhdesinde bulunan kişisel verileri koruma sorumluluğu yüklense dahi söz konusu somut olay bakımından veri kontrolörü olan tüzel kişiliğin kendisi olup, gerçek kişi ancak onun adına tasarrufta bulunan konumundadır. Veri kontrolörü kişisel verilerin işlenmesi konusunda Direktif'e uygun davranmakla yükümlü olup ortaya çıkan hukuka aykırılıklardan doğrudan sorumludur.

v) *Veri işleyicisi:* Veri kontrolörü adına kişisel verileri işleyen gerçek veya tüzel kişilere "veri işleyicisi" denilmektedir. Genellikle veri kontrolörleri, zaman ve maliyet tasarrufu sağlamak amacıyla veri işlemek üzere üçüncü bir taraftan hizmet almaktadır. Bu durumda üçüncü taraf veri kontrolörünün emri üzerine hareket etmekte ancak veri işlemenin amacını kendisi belirlememekte olduğundan bu kişi söz konusu işlem bakımından veri işleyicisi kabul edilmektedir. Bir tüzel yahut gerçek kişinin, kişisel verilerin işlenmesi bakımından aynı anda hem veri kontrolörü hem de veri işleyicisi olması mümkündür. Mesela bir avukatlık şirketi kendi çalışanları hakkındaki veriler açısından 'veri kontrolörü' sayılırken; müvekkil şirketlerinin çalışanlarına ilişkin tutmakta olduğu kişisel veriler bakımından ise 'veri işleyicisi' sayılmaktadır.

vi) *Rıza:* Veri öznesinin karşı tarafa, kendisine ait kişisel veriyi işlemesini özgür iradesiyle kabul ettiğini onaylayan her türlü davranış, işaret veya ifade ile açıklanan irade beyanı Direktif bakımından rıza olarak tanımlanmaktadır. Söz konusu irade beyanının, dışa vurulan, muhatap bakımından objektif bir değerlendirmeyle işlemeye onay vermek şeklinde anlaşılabilen bir davranış olması gerekmekte olup bu anlamda susma rıza olarak değerlendirilemez.

2.1.4. Veri Koruma Direktifi'ndeki Temel İlkeler

Mahremiyet hakkının korunması ve bireyin özel hayatına müdahaleleri önleme ihtiyacıyla ortaya çıkan veri koruma ilkeleri Veri Koruma Direktifi'nin temelini oluşturmaktadır. Söz konusu ilkelerle veri kontrolörünün kişisel verileri işlerken uyması gereken yükümlülükler belirlenmekte, işleme sırasında veri kontrolörüyle veri sahipleri

arasında ortaya çıkan çıkar çatışması dengelenmeye çalışılmaktadır. Direktif'e göre üye devletler, kişisel verileri ancak aşağıdaki temel ilkelere uygun olarak işleyebilecektir:

(a) Adil ve Yasal İşleme: Kişisel veriler adil ve yasalara uygun şekilde işlenecektir.

(b) Amaç ile Sınırlılık: Kişisel veriler; kesin, belirlenmiş ve hukuka uygun amaçlara göre toplanmış olacak ve ilk toplandıkları amaca aykırı olarak daha sonradan işlemeye konu olmayacaktır. Üye devletin gerekli önlemleri alması şartıyla, bu verilerin ilk toplandıkları amacın dışında tarihsel, istatistiksel ve bilimsel amaçlarla daha sonradan işlemeye konu olmaları durumu saklıdır.

(c) İlgililik ve Orantılılık: Kişisel veriler, toplama ve/veya müteakip olarak işleme amaçları için yeterli ve bu işlemlerle ilgili olacak, aşırı olmayacaktır.

(d) Doğruluk ve Güncellik: Söz konusu veriler güncel ve doğru olarak tutulacak; böylece veri kalitesi korunacaktır. Toplanma amaçları veya daha sonraki işleme için yanlış veya eksik olan verinin silinmesi veya düzeltilebilmesi için gerekli tüm makul adımlar atılacaktır.

(e) Süreyle Sınırlılık: Kişisel veriler, toplama amacının veya daha sonraki işlemenin gerektirdiğinden daha uzun süre saklanmayacaktır. Veriler, veriye konu olan kişilerin kimliğinin belirlenmesine müsaade eder biçimde muhafaza edilecektir. Tarihsel, istatistiksel veya bilimsel amaçlarla daha uzun süreli muhafaza edilmesi gereken veriler bakımından uygun koruma önlemleri belirlenecektir.

Direktif çerçevesinde üye ülkelerde kişisel verilerin işlenebilmesine ilişkin şartlar ise Direktifin 7. maddesinde sayılmaktadır. Bu kapsamda veri sahibinin açık ve kesin olarak rızasının alınması, bir sözleşmeden doğan yükümlülüğün yerine getirilmesi, bir kanuni yükümlülüğün yerine getirilmesi, veri sahibinin hayati menfaatlerinin korunması ve kamu yararının gerektirdiği bir işin yerine getirilmesi durumlarında kişisel verilerin işlenebileceği kabul edilmektedir.

Pek çok hukuk sisteminde kişilerin sağlık durumları, cinsel yaşamlarına ilişkin verileri, dini ve felsefi inançları, ırk veya etnik kökenlerini belirten kişisel verileri ve siyasi görüşleri daha üst seviyede bir korunmayı gerekli kıldığından "hassas kişisel veri" olarak tanımlanmaktadır. Direktif'in 8/1. maddesiyle hassas kişisel veri niteliğini haiz verilerin işlenmesinin üye devletler tarafından yasaklanması gerektiği ifade edilmektedir. Söz konusu işleme yasağına ilişkin istisna hükmü ise (veri sahibinin açık rızasının olması durumu gibi) aynı maddenin ikinci fıkrasında düzenlenmektedir. Hassas kişisel verilerin, mahiyetleri itibarıyla, bireylerin toplum içerisinde ayrımcılık veya bir takım mağduriyetlere uğramasına yol açabilmeleri bakımından bu hüküm yüksek önemi haizdir.

Veri Koruma Direktifi'nin kişisel verilerin korunması hukuku bağlamında sahip olduğu en önemli unsurlarından biri de 28. maddesiyle getirmiş olduğu etkin denetim sistemidir. Söz konusu maddeye göre her üye devlet Direktif'te yer alan hükümlerin kendi ülkesindeki uygulamasını izlemek ve bu konuda en az bir kamu kurumunu (Veri Koruma Otoritesi) görevli kılmak zorundadır. Yetkili Veri Koruma Otoritesinin görevlerini yerine getirirken bağımsız olarak hareket edeceği önemle vurgulanmaktadır. Bu kapsamda üye

ülkelere, kişisel verilerin işlenmesi ve bu anlamda bireysel hakların korunması konusunda ikincil düzenlemelerini yaparken veya idari tedbir alırken, Veri Koruma Otoritesine danışılmasını temin etme yükümlülüğü getirilmektedir. Veri Koruma Otoriteleri görevlerini yerine getirirken gerekli tüm bilgilere erişim, bu bilgilerin silinmesini veya yok edilmesini isteme, uyarma ve iç hukuk hükümlerinin ihlali halinde bu ihlalleri yargı aşamasına taşımak üzere kovuşturmaya başlama yetkisi de Direktifte yer almaktadır.

Direktif'te bireylere doğrudan tanınan haklardan (mahremiyet, veri işleme, veri erişim vb.) yararlanılması konusunda direktifin iç hukuka derc edilip edilmediğine bakılmaksızın vatandaşların Direktif'e dayanarak yargı yoluna başvurabilme hakları bulunmaktadır. Zira AB ülkelerinin kendi iç hukuklarını Direktif ile uyumlu hale getirirken bu bölümde yer alan temel ilkeler, asgari şartlar olarak belirlenmiş, daha düşük seviyede koruma önlemleri içeren düzenlemelerin yapılması engellenmiştir. Bununla birlikte, Direktif'in oluşturulmasında oldukça düşük seviyede kalan ülke katkıları ile ülkeler arası görüş farklılıkları gibi sorunlar, Direktif'in iç hukukla uyumlaştırılması konusunda üye ülkelerde bir gönülsüzlüğü de beraberinde getirmiştir. Bu çerçevede, AB ülkelerinin Veri Koruma Direktifi'ni iç hukuka uyarlama konusunda yetersiz kaldığı gözlemlenmektedir.[9] Bu durum, ulusal veri koruma düzenlemeleri ve Direktif'in AB genelinde kişisel verilerin korunması konusunda tek başına yetersiz kaldığı ve dolayısıyla bir reform ihtiyacının ortaya çıktığı fikrini doğurmuştur.

2.2. AB Genel Veri Koruma Tüzüğü (General Data Protection Regulation - GDPR)

2.2.1. Veri Koruma Tüzüğü İhtiyacı ve Genel Bilgiler

2.2.1.1. Veri Koruma Tüzüğü İhtiyacının Ortaya Çıkışı

Mahremiyet kuralları AB özel hukuku içerisinde sahip olduğu önem ve konum bakımından değerlendirildiğinde, söz konusu alanın derin bir kültürel değer birikimini ve anlayışını yansıttığı görülmektedir. Avrupa İnsan Hakları Sözleşmesinin 8. maddesiyle koruma altına alınan özel hayatın gizliliği ve ailenin korunması hakkı ile AB Temel Haklar Şartı'nda yer alan özel hayat ve aile hayatına saygı hakkı (madde 7) ve ayrıca açıkça düzenlenen kişisel verilerin korunması hakkını (madde 8) temel alan AB veri koruma hukuku bakımından 95/46 sayılı Direktif bu amacın en önemli parçalarından birini oluşturmaktaydı. Ancak ekonomik faaliyetler içerisinde verinin kullanımı ve rolünün hızla değişmesi öncelikle düzenleyici çerçevede bir değişimi, yani Direktif'in güncellenmesi ihtiyacını doğurmuştur. Söz konusu düzenlemede yapılacak güncelleme, çok daha yüksek düzeyli bir gizlilik korunmasının sağlaması için gerekli görülmüştür.

Veri Koruma Reformu hareketinin ortaya çıkmasında birden fazla faktör etkili olmuştur. Bu sebeplerden ilki, kural koymanın temel doğasından kaynaklanan ihtiyaç doğrultusunda, yeni teknolojik gelişmelere uygun kurallar koyarak temel politika hedefleriyle daha uyumlu ve daha verimli kazanımların sağlanmasıdır. Veri Koruma Direktifi'nin 1995

[9] HENKOĞLU, Türkay, Bilgi Güvenliği ve Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara, 2015, sh. 60.

yılından beri uygulana geldiği düşünüldüğünde, özellikle 90'lı yılların ortalarından itibaren internetin ticarileştirilmesiyle meydana gelen köklü dönüşümler karşısında bu düzenlemenin 'eski' kaldığı değerlendirilmektedir. Zira bu dönüşüm sırasında hayatımıza hızla giren yeni teknolojiler bir yandan hayal dahi edemeyeceğimiz yararlar sağlarken öte yandan veri toplama, işleme, depolama ve verinin yeniden kullanımı açısından daha önce akla gelmeyen mahremiyet/güvenlik risklerini de beraberinde getirmiştir.[10] AB içerisinde en temel çekincelerden biri verinin sınır-ötesi transferinin oldukça kolaylaşması olmuştur. Zira bu durum doğal olarak yabancı ülke mahremiyet kurallarının uygulanması zorunluluğunu beraberinde getirmiştir. Bunun sonucunda AB vatandaşlarının mahremiyet/gizlilik haklarının olumsuz etkilemesi kaygısı giderek yükselmiştir.

Bu çerçevede, mevcut veri koruma kurallarının güncellenmesi ve yeni dijital dünyayla daha uyumlu hale getirilmesi ihtiyacı, ortaya çıkan somut uyuşmazlıklar ve bu değişimi kaçınılmaz kılan siyasi açmazlar sebebiyle giderek zorunlu bir hal almıştır. Bu olayların başında, konuyla doğrudan olmasa da etkisi bakımından büyük ilgisi olan, 2013 yılında Edward Snowden tarafından ortaya çıkarılan mahremiyet ihlalleri gelmektedir. Söz konusu olayda başta Google, Facebook, Apple ve diğer büyük (ABD merkezli) internet aktörlerinin kullanıcıları olmak üzere milyonlarca kullanıcının erişim bilgileri de dâhil pek çok kişisel verisi Ulusal Güvenlik Ajansı'nın (National Security Agency-NSA) geniş kapsamlı ve derinlikli gözetimlerine konu olmuştur. Bu somut gelişmeler Avrupa Birliği Adalet Divanı'nın (ATAD) mevcut hukuki uygulamalarında önemli bir değişim yaklaşımı benimsenmesine sebep olmasının yanında Avrupa'da bireyin internetteki haklarının korunması konusundaki genel anlayışın da değişmesine neden olmuş ve mahkeme bu çerçevede bir dizi özgün karara imza atmıştır. Bu kapsamda ATAD'ın dönüm noktası sayılan kararları şu şekilde sayılabilir:

- *Google-İspanya Kararı:* Hukuki literatüre "unutulma hakkı" olarak da girecek olan bu uyuşmazlık, bu yönde bir talebin hukuki merciler önüne taşındığı ilk davadır. Söz konusu dava İspanya vatandaşı Mario Costeja Gonzalez tarafından Google İspanya ve Google Inc. şirketine karşı açılmış olup davanın konusu 1998 yılında bir gazetede davacı Gonzalez hakkında yapılan habere ilişkin kısayolun arama motorundan kaldırılması talebidir. Davacı uzun süre önce kendisi hakkında yapılan bu haberin artık "alakasız" bir mahiyette olması gerekçesiyle habere ilişkin linkin kaldırılması gerektiğini savunmuştur. Bu kararda arama motorlarının ve internet aracı hizmet sağlayıcılarının veri kontrolörü sayılması gerektiği ifade edilmiştir.[11] Karar bireyin kişisel verileri konusundaki haklarını savunmaları ve çevrimiçi verileri üzerindeki kontrollerini artırmaları açısından dönüm noktası olmuş, GDPR'da yer alan "unutulma hakkı"nın da çıkış noktası kabul edilmiştir.

[10]GONÇALVES, Anabela Susana de Sousa, 'The Cross Border Regulation of Online Data Privacy and the Judicial Cooperation', Jusletter IT, 26 Şubat 2015, sh 6.
[11] Karar C-131/12, Google Spain SL ve Google Inc. v Agencia Española de Protección de Datos (AEPD) ve Mario Costeja González, Adalet Divanı (Grand Chamber) of 13 Mayıs 2014, ECR [2014] 317, parag. 32-41.

- *İrlanda Dijital Haklar Kararı:* Kamuoyu tarafından daha az bilinen 2014 tarihli bir diğer ATAD kararında ise 2006/24/EC sayılı Veri Saklama Direktifi geçersiz ilan edilmiştir.[12] Bu Direktif sabit, mobil veya internet telefonu ile e-posta iletişimi verilerinin altı aydan iki yıla kadar saklanmasını düzenlemektedir. Söz konusu kişisel verilerin her üye devlet tarafından muhtemel bir soruşturma, araştırma ve suçun kovuşturulması amacıyla kullanılabilmesini sağlayabilecek şekilde hazır tutulmasının sağlanması amaçlanmıştır. Ancak söz konusu veri saklama faaliyetinin makul suç şüphesi bulunmasına gerek olmaksızın yapılması ve üye devletlerin anayasal düzenlemeleri başta olmak üzere pek çok hukuki gerekliliklerıyle çelişmesi, bahse konu Direktif'in yoğun tartışmalara yol açmasına sebep olmuştur. Bu tartışmalar ATAD'ın Direktifi geçersiz ilan eden kararıyla nihayete ermiştir.

- *M.Schrems-Veri Koruma Komisyonu Kararı:* Veri koruma kurallarına ilişkin temel yaklaşımda ve pek çok hukuki düzenlemede değişikliğe gidilmesi ihtiyacının varlığını ortaya çıkaran bir diğer önemli ATAD kararı ise 6 Ekim 2015 tarihinde verilen "Schrems Kararı"dır.[13] Davacı Maximillian Scherms Avusturya vatandaşı olup söz konusu olayda İrlanda Veri Koruma Otoritesini dava etmiştir. Dava konusu uyuşmazlık Scherms'in daha önce, Facebook tarafından kişisel verilerinin ABD'de tutulmasının kendisi bakımından ihlale sebep olduğu gerekçesiyle yapmış olduğu başvurusunun İrlanda Veri Koruma Otoritesi tarafından reddedilmesi üzerine meydana gelmiştir. AB ve ABD arasındaki "Güvenli Liman Anlaşması" kapsamında eşdeğer bir koruma seviyesinin bulunmasının zorunlu olmasına rağmen, bir süredir tartışmalara sebep olan NSA gözetimleri de dikkate alındığında ABD tarafından Scherms'in kişisel verilerinin AB için gerekli olan güvence şartları kapsamında korunmadığı iddia edilmiştir. ATAD yaptığı incelemede, Komisyonun üçüncü bir ülkeyi yeterli koruma düzeyini sağlar bulmasının ulusal veri koruma otoritelerinin Veri Koruma Direktifi kapsamında inceleme ve denetleme yapma gücünü azaltmaması gerektiği, Güvenli Liman Anlaşması'nın yalnızca ABD şirketleri bakımından bağlayıcı olup kamu otoritelerini bağlamayacağı, ABD hukuk kurullarının incelenmesi sonucunda AB vatandaşlarının başta kişisel verileri olmak üzere temel hakları bakımından tehlikeli sonuçların ortaya çıkabileceği değerlendirildiğinden Güvenli Liman Anlaşması geçersiz ilan edilmiştir.

2.2.1.2. AB Veri Koruma Reformuna İlişkin Genel Bilgiler

15 Aralık 2015 tarihinde Avrupa Parlamentosu, AB Konseyi ve Komisyonu arasında tüm AB genelinde veri koruma hukukunun temel çerçevesini belirleyen modern ve uyumlu yeni veri koruma kurallarının kabulü konusunda anlaşmaya varılmıştır. Parlamento'nun Sivil

[12] Toplu Kararlar C-293 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, ve Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl ve diğerleri yargılaması, 8 Nisan 2014, ECR [2014] I-238.

[13] Karar C-362/14, Maximillian Schrems v. Data Protection Commissioner yargılaması, 6 Ekim 2015, ECLI:EU:C:2015:650.

Özgürlükler Komitesi ile Konsey'in Daimi Temsilciler Komitesi'nin (COREPER) de çoğunluğunun kabulü ile onaylanan söz konusu düzenleme AB Konseyi'nin "Sayısal Tek Pazar Stratejisi"nin (Digital Single Market Strategy) uygulanması yönünde atılmış büyük bir adım olarak değerlendirilmektedir.

Reform paketi içerisinde iki temel hukuki düzenleme yer almaktadır;

- *AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/679 sayılı, 95/46/EC sayılı Direktifi yürürlükten kaldıran, kişisel verilerin işlenmesi karşısında gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin Tüzüğü (GDPR),*

- *AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/680 sayılı, Konsey'in 2008/977/JHA Çerçeve Kararını yürürlükten kaldıran, yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına dair Direktifi.*

8 Nisan 2016 tarihinde Konsey tarafından kabul edilen taslak Tüzük ve Direktif metinleri 14 Nisan 2016 tarihinde Avrupa Parlamentosu tarafından onaylanarak kabul edilmiştir. Söz konusu düzenlemeler 4 Mayıs 2016 tarihinde tüm AB resmi dillerinde AB Resmi Gazetesi'nde yayımlanmıştır. GDPR, 24 Mayıs 2016 tarihinde yürürlüğe girmiş olmakla birlikte söz konusu metnin uygulanmaya başlama tarihi 25 Mayıs 2018 olarak belirlenmiştir. Yine Reform paketinde yer alan Direktif, 5 Mayıs 2016 tarihinde yürürlüğe girmekle birlikte AB üye ülkelerince metnin iç hukuklarına derc edilmesi için öngörülen son tarih ise 6 Mayıs 2018 olarak belirlenmiştir.[14]

Komisyonun kişisel verilerin korunmasına ilişkin genel AB yasal çerçevesini gözden geçirirken temel aldığı politika hedefleri şu şekilde ifade edilmektedir:[15]

- Özellikle küreselleşmeden kaynaklanan zorluklar ve yeni teknolojilerin kullanımı karşısında kişisel verilerin etkili bir biçimde korunması amacıyla AB hukuk sisteminin iyileştirilmesi,
- Kişisel veriler konusunda bireysel hakların güçlendirilmesi ve aynı zamanda AB içinde ve/veya dışında kişisel verilerin serbest akışının sağlaması için bürokratik süreçlerin azaltılması,
- Kişisel verilerin korunmasına ilişkin AB hukuku kurallarına netlik ve tutarlılık kazandırılması; bu kuralların yine tutarlı ve etkin bir biçimde uygulanması ve Birliğin tüm faaliyet alanında kişisel verilerin etkin bir biçimde korunması.

[14] http://ec.europa.eu/justice/data-protection/reform/index_en.htm, (Erişim Tarihi: 15.10.2015).
[15] http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, (Erişim Tarihi: 19.10.2015).

2.2.2. Veri Koruma Tüzüğü'nün Getirdiği Temel Değişiklikler

Yeni AB Veri Koruma Tüzüğü ile getirilen önemli değişiklikler aşağıda temel olarak sıralanmıştır:

1- *Üst Seviye Uyumlaştırma:* GDPR üzerinde detaylı bir inceleme yapılması gerekmeksizin yeni kurallar bütününe ilişkin göze çarpan en temel gelişme söz konusu kuralların önceki düzenlemenin aksine bir Direktif şeklinde değil bir Tüzük şeklinde kaleme alınmış olmasıdır. Her iki tür AB düzenlemesiyle de üye ülke mevzuatları arasında üst düzeyde uyum sağlanması mümkün olmakla birlikte; tüzükler, üye ülkelerde doğrudan uygulanma kabiliyetini haiz olup herhangi bir iç hukuk düzenlemesi yapılmasını gerektirmezken direktifler, o hukuki düzenlemeyle elde edilmesi beklenen temel hedefleri ortaya koyar ancak söz konusu hedeflere ulaşılmasına ilişkin araçların seçimini üye devletlerin kendi iç hukuklarına bırakırlar. Ayrıca tüzükler doğrudan ulusal hukuk sistemlerinin parçası haline gelirler ve ulusal kanunlardan bağımsız olarak uygulanma kabiliyetini haiz olup söz konusu tüzüğe aykırı bir ulusal kanun karşısında bağlayıcı olan düzenleme tüzüktür. Bu kapsamda, AB üyesi ülkeler arasında veri koruma hukuku bakımından üst seviyede bir uyumun sağlanmasının yanında iç hukuk düzenlemelerinden kaynaklanan farklılıklar da giderilmiş olmaktadır. Bu güçlü mevzuat uyumunun daha önce bahsedilen AB Sayısal Tek Pazar Stratejisi ile hedeflenen sadeleştirilmiş, sorunsuz ve verimli bir AB dijital ekonomisiyle küresel rekabet avantajı sağlanması amacına ulaşılmasını sağlayacağı değerlendirilmektedir.

2- *Veri İşleyenlerin (data-proccesors) Tamamının Veri İşlemeden Sorumlu Tutulması:* 95/46 sayılı Direktif'te "kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri"nin işlenmesine ilişkin kurallara uymakla yükümlü olan ve hukuka aykırı olarak yapılan iş ve işlemlerden sorumlu olan tek kişi "veri kontrolörü (data-controller)", başka bir ifadeyle veri sahipliğini elinde bulunduran kişi, olarak düzenlenmekteydi. GDPR ile getirilen düzenleme kapsamında, veri kontrolörü olmamakla birlikte bu verileri işleyen herhangi bir şirket ya da birey de (bulut hizmet sağlayıcıları gibi alt hizmet sağlayan üçüncü taraflar da dâhil olmak üzere) verinin hukuka uygun işlenmesinden sorumlu tutulacaklardır. Bu hüküm veri işleme sayılan fiillerin sayıldığı madde hükmüyle birlikte değerlendirildiğinde; kişisel veriye ilişkin gerçekleştirilen her türlü işleme faaliyetinin tüm faillerinin söz konusu işlemeden kaynaklı her türlü veri ihlali ve hukuka aykırılıktan sorumlu olduğu görülmektedir. Bu hükmün uygulanmasının yansımaları oldukça geniş olacağından hem veri sorumluları hem de veri sorumlusunun talebiyle veriyi işleyen üçüncü kişiler bakımından hukuki sorumluluk ortaya çıkmaktadır. Bu kapsamda GDPR hükümlerinin, sunucuları AB dışında yerleşik bulunan ve işleme faaliyetlerini Birlik ülkeleri dışından sürdüren bulut hizmet sağlayıcıları bakımından da bağlayıcı olduğu görülmektedir. GDPR ile getirilen yüksek oranlı para cezaları bu işleyiciler bakımından da bağlayıcıdır.

3- *GDPR Hükümlerinin Küresel Ölçekte Etkiyi Haiz Olması:* Söz konusu düzenlemenin AB tarafından hayata geçirilmiş olması bu hükümlerin yalnızca AB içerisinde yerleşik faaliyet gösteren veri işleyicileri/sorumluları bakımından bağlayıcı olduğu anlamına gelmemektedir. Bilakis küresel anlamda nerede hizmet verdiğine bakılmaksızın AB vatandaşlarına ve GDPR'nin uygulama alanındaki herkese ilişkin verilerin hukuki güvencesi sağlanmış bulunmaktadır.

4- *Verisi İşlenenlere Sağlanan Tazminat Talebi İmkânı:* GDPR kişisel verilerinin işlenmesi sırasında zarara uğrayanlara (hukuka aykırı işleme sırasında veri kaybı gibi) toplu tazminat da dâhil olmak üzere, Amerikan hukuk sisteminde yer alan toplu dava sistemine eşdeğer bir tazminat talebi hakkı tanımaktadır.

5- *AB Vatandaşlarına Ait Kişisel Verilerin Sınır-Ötesi Aktarımının Daha Sıkı Kurallara Bağlanması:* Veri sorumlusuna kendisine verinin paylaşılmasına ilişkin rıza verilmiş olsa dahi, verinin transfer edildiği ülkede yeterli düzeyde koruma sağlandığına ilişkin teminat verilmediği sürece (yeterlilik şartı), GDPR verinin AB dışına transferini yasaklamaktadır. Ayrıca, 95/46 sayılı Direktif hizmet sunucu üçüncü kişilerin yeterlilik koşullarını sağlayıp sağlamadığına ilişkin değerlendirmeyi veri kontrolörüne bırakırken GDPR kapsamında bu değerlendirmeyi ancak veri koruma otoritesi yapabilmektedir.

6- *Uyumlaştırılmış Kullanıcı Hakları:* Veri koruma hukuku kurallarının tanımış olduğu haklar bakımından üye ülke uygulamalarında ortaya çıkan bazı farklılıklar giderilmektedir. Örneğin 95/46 sayılı Direktif hükümleri kapsamında da kullanıcılar kendileri hakkında hangi verilerin tutulduğuna ilişkin bilgi edinme hakkına sahiptiler. Ancak mevcut durumda üye ülke mevzuatları veri kontrolörüne bu konuda farklı uygulama seçenekleri sağlamaktadır. (Örneğin İngiltere'de bu bilgilerin sağlanması için gereken süre 40 gün olarak tespit edilmiştir.) GDPR ile bu farklılık ortadan kaldırılarak söz konusu bilgilerin 20 gün içerisinde kullanıcılara sağlanması gerektiği düzenlenmiştir.

7- *Yeni "Unutulma Hakkı" Kavramı:* GDPR ile getirilen düzenleme kapsamında kullanıcılar kendilerine ait kişisel verilerin silinmesini talep edebilme hakkını haizdir. Uygulanması kulağa basit gelen söz konusu talep, birden fazla sisteme sahip bir veri kontrolörü bakımından kullanıcının bunlardan birinden veya birkaçından silinmeyi talep etmesi durumunda karmaşık bir hal alabilmektedir.

8- *Kullanıcı Haklarına İlişkin Bilgilendirme Yükümlülüğünün Veri Kontrolöründe Olması:* GDPR kapsamında veri kontrolörleri, kullanıcılarını bilgilendirmek ve sahip oldukları yasal haklar konusunda gerekli hatırlatmaları yapmakla yükümlü olup aynı zamanda söz konusu yükümlülüklerini gerçekleştirdiklerini belgelemekle de yükümlü tutulmaktadırlar. Tüzük'te ayrıca kullanıcılara ilişkin kişisel verilerin kontrolörün sistemlerinde yer almasına/kullanılmasına ilişkin

olarak opt-out değil opt-in yaklaşımının tercih edildiği görülmektedir.[16] Bu kuralın ihlal edilmesi durumunda GDPR 95/46 sayılı Direktif'e göre çok daha ağır tazminatlar öngörmektedir.

9- *Daha Sıkı Yaptırımların ve Elverişli Mekanizmaların Öngörülmesi:* GDPR ile getirilen en önemli düzenlemelerin başında veri ihlalleri karşısında öngörülen yaptırımlara ilişkin hükümler gelmektedir. Zira veri koruma kurallarına ilişkin ihlaller karşısında çok daha ağır tazmin yaptırımları ve elverişli sorun çözme mekanizmaları öngörülmektedir. Hâlihazırda örneğin İngiltere'de veri ihlalleri neticesinde verilebilecek en yüksek para cezası 500 bin Pound iken GDPR ile bu rakam 200 milyon Avro veya hizmet sağlayıcının küresel gelirinin yüzde dördü gibi önemli miktarlara ulaşabilmektedir. Ayrıca mevcut iç hukuk düzenlemeleri bakımından veri ihlallerinin kullanıcılara veya veri koruma otoritelerine bildirimleri konusunda birbirinden farklı hukuki yaklaşımlar ve uygulamalar bulunmaktadır. GDPR ile bu konudaki belirsizliğin ve üye ülkeler arası farklılığın ortadan kaldırılması amacıyla söz konusu bildirimin en geç 72 saat içerisinde veri koruma otoritelerine yapılması gerektiği düzenlenmektedir. (33. madde) Bununla birlikte veri ihlali konusunda kullanıcının ne kadar süre içerisinde bilgilendirileceğine ilişkin bir süre öngörülmemiş olup bu konu belirsiz bulunmaktadır.

10- *Güçlendirilmiş Rıza:* Tüzük'ün 32 no'lu resitalinde de ifade edildiği üzere, kullanıcıların çevrimiçi sosyal ağların veya web tarayıcılarının gizlilik ayarlarına ilişkin sessiz kalmaları yahut o zamana kadar herhangi bir itirazda bulunmamış olmaları durumunda varsayılan ayarlar geçerli bir rızanın alındığı anlamına gelmemektedir. Zira kişisel verilerin işlenmesine ilişkin rızanın özgürce, belirli, aydınlatılmış/bir amaca matuf, bilinçli ve açıkça verilmiş olması gerekmektedir. Söz konusu rızanın aynı amaç veya amaçlar için yürütülen tüm işleme faaliyetleri bakımından alınması gerekmektedir. Ayrıca rızanın elektronik araçlarla istendiği durumlarda bu istek, açık, özlü ve uğruna kullanıldığı hizmetten yararlanmayı engellemeyen bir mahiyette olmalıdır.

11- *Veri Taşınabilirliği Hakkı (user-generated content-UGC):* Bu hak ilk kez GDPR'nin 20. maddesiyle tanımlanmış olup madde ile veri sahibi, kişisel verisini tutmaya yetkili bir veri kontrolöründen diğerine taşıyabilme yetkisine sahiptir.

---

[16] "Opt-out" terimi bir işlem/eylemden geri çekilmek anlamına gelirken, "Opt-in" terimi genel anlamda bir seçeneğin bilinçli olarak seçilerek herhangi bir işleme onay verilmesi anlamına gelmektedir. Elektronik sistemlerde tutulan veriler bakımından bugün dünyada bu iki ana yaklaşım kabul edilmektedir:

- *Opt-out yaklaşımı* dünyada ilk olarak ABD'de benimsenmeye başlanmıştır. Bu yaklaşıma göre kişilerden önceden izinleri alınmaksızın sistemde verileri tutulmakta olup kullanıcı bu sistemden ücretsiz, kolay ve çabuk bir biçimde istediği zaman çıkma hakkına sahiptir.
- *Opt-in yaklaşımında* sistemde verisi saklanacak olan kişinin her ne şart altında olursa olsun mutlak suretle izninin alınmış olması gerekmektedir. Opt-in yaklaşımında da Opt-out yaklaşımında olduğu gibi herkesin ücretsiz, kolay ve çabuk biçimde dilediği zaman sistemden ayrılma hakkı bulunmaktadır. Opt-in yaklaşımı AB tarafından benimsenmektedir.

12- *Hassas Verilerin İşlenmesi Bakımından Öngörülen Zorunlu Veri Koruma Görevlisi (Data Protection Officers - DPO):* GDPR'nin 37. maddesi gereğince aşağıdaki koşulların varlığı halinde veri kontrolörleri ve işleyicileri veri koruma görevlisi (DPO) olarak belirlenir:

a) İşleme faaliyeti, yargı faaliyetinin yürütülmesi durumu hariç, bir kamu kurum veya kuruluşunca gerçekleştiriliyorsa,
b) Yapmış oldukları işin doğası gereğince büyük ölçüde veriyi düzenli ve sistematik izlemeyi gerektiren veri işleyicisi veya veri kontrolörlerinin temel faaliyetlerini veri işleme oluşturuyorsa,
c) Veri kontrolörü veya işleyicisinin temel faaliyetlerini 9. maddede sayılan özel nitelikli hassas verilerin işlenmesi veya 10. maddede ifade edilen ceza mahkûmiyeti veya suça ilişkin kişisel bilgilerin işlenmesi durumunda.

Veri koruma görevlisinin veri koruma alanında yeterli uzmanlık bilgisini haiz olması gerekmektedir. Yukarıda sayılan işleme faaliyetlerinden bu görevli sorumludur. GDPR hükmüne göre veri koruma görevlisinin iş akdiyle istihdam edilmesi de mümkündür. Ayrıca bir veri koruma görevlisinin birden fazla şirket veya kamu kurumu adına çalışması mümkündür.

13- *Riskli Veri İşleme Faaliyetleri Bakımından Zorunlu Veri Koruma Etki Değerlendirmesi (Data Protection Impact Assessments - DPIA):* GDPR'nin 35. maddesiyle getirilen bu yeni düzenlemede, özellikle yeni teknolojik veri işleme metodlarının kullanıldığı veri işleme faaliyetlerinin gerçek kişilerin hak ve özgürlükleri bakımından yüksek bir risk içermesinin muhtemel olduğu durumlarda, söz konusu işlemenin kapsamı, niteliği, bağlam ve amacı da dikkate alınarak Tüzük hükümlerine uyumun arttırılması amacıyla veri kontrolörü, öncelikle bir veri koruma etki değerlendirmesi (VKED) yapılmasından sorumlu tutulmaktadır. Maddenin ikinci fıkrasında özellikle hangi durumlarda VKED yapılması gerektiği (otomatik veri işleme sistemlerinin kullanılması, hassas verilerin işlenmesi veya ceza mahkûmiyeti ve suçlara ilişkin veriler gibi.) ayrıntılı olarak açıklanmaktadır. Bu kapsamda 86 no'lu resitalde kişisel veri işleme faaliyetlerinin GDPR hükümlerine uygun olarak gerçekleştirilmesine yönelik alınacak önlemlerin belirlenmesinde söz konusu VKED sonuçlarının dikkate alınacağı ifade edilmektedir. VKED'nin özellikle büyük ölçekli işleme faaliyetlerinde gerekli olduğu vurgulanmaktadır.

Ayrıca bir VKED sonucunda, işleme faaliyetlerinin kontrolörün mevcut teknoloji ve uygulama maliyetleri açısından uygun tedbirlerle hafifletemeyeceği yüksek bir riski içerdiğinin ortaya çıkması durumunda, veri işleme faaliyetinden önce veri koruma otoritesine danışılması gerekmektedir.

95/46 sayılı Direktif'te yer alan veri işleme faaliyetlerinin veri koruma otoritelerine bildirilmesine ilişkin genel hükmün, pek çok idari ve mali yük

getirirken kişisel verilerin korunması konusunda köklü bir çözümü getirmediği görülmüştür. Bu çerçevede, ayrım gözetmeksizin tanımlanan bu genel bildirim yükümlülüğü yerine VKED'nin yapılmasının çok daha amaca matuf olacağı ifade edilmektedir. Zira VKED'de veri kontrolörü, yüksek risk olasılığını ve şiddetini değerlendirmeden önce işlemenin amaç ve kapsamıyla riskin kaynaklarını göz önünde bulundurmaktadır. VKED'nin gerçek kişilerin hak ve özgürlüklerine ilişkin risklerin azaltılmasına imkân veren gerekli önlem ve mekanizmaları içermesi, Tüzük'te öngörülen hükümlerle uyumlu olması ve kişisel verilerin korunması kurallarıyla uyumlu olması gerekmektedir. GDPR'in 95 no'lu resitalinde, veri işleyicilerin de gerekli durumlarda veya kendisinden talep edilmesi halinde, VKED'nin uygulamasından kaynaklanan yükümlülüklerin yerine getirilmesi konusunda veri kontrolörüne yardımcı olması gerektiği ifade edilmektedir.

14- *Başlangıçtan İtibaren (data protection by default) ve Tasarımdan İtibaren Veri Koruması (data protection by design) yaklaşımı:* Tüzüğün resital bölümünde kişisel verilerin işlenmesi bağlamında gerçek kişilerin hak ve özgürlüklerinin korunması amacıyla gerekli teknik ve organizasyonel önlemlerin alınması gerektiği ifade edilmektedir. Bu kapsamda, veri kontrolörü iç işleyişi ile alakalı politikalarını belirleyerek başlangıçtan itibaren veri koruması (data protection by default) ve tasarımdan itibaren veri koruması (data protection by design) ilkelerini karşılamaya yönelik gerekli tedbirleri almalıdır. Bu ilkeye göre veri kontrolörü, gerek veri işleme vasıtalarının belirlenmesi sırasında gerekse veri işleme anında Tüzük'te öngörülen veri koruma kurallarının etkili bir biçimde uygulanması için gerekli araçları kullanarak, örneğin bulanıklaştırma (pseudonymisation)[17] veya asgari veri işleme gibi, uygun teknik ve organizasyonel önlemleri almalıdır. Söz konusu önlemlerin belirlenmesine ilişkin temel hususlar GDPR'nin 25. maddesinde yer almaktadır.

15- *Veri İhlali Riskinin Yüksek Olması Durumunda Hem Veri Koruma Otoritesine Hem de Veri Sahibine Bildirimde Bulunma Zorunluluğu:* Veri kontrolörü veri ihlalinin meydana geldiğini öğrenir öğrenmez, hesap verebilirlik ilkesine uygun olarak, mümkün olan en kısa süre içerisinde (en geç 72 saat) veri koruma otoritesine ihlali bildirmekle yükümlüdür. Ayrıca kontrolör, söz konusu ihlal dolayısıyla hak ve hürriyetleri tehlike altında bulunan veri sahibine de gerekli önlemleri alabilmesi amacıyla gecikmeksizin bildirimde bulunmakla yükümlüdür. Söz konusu bildirimlere ilişkin ayrıntılı değerlendirmeler GDPR'nin 33. ve 34. maddelerinde yer almaktadır.

16- *Veri Kontrolörüne Kurtuluş Hakkı:* GDPR ile veri kontrolörü bakımından getirilen sorumluluğun sınırlarını belirlemek amacıyla kullanılan temel kavram

[17] GDPR kapsamında "pseudonymisation" terimiyle ifade edilen kavramın dilimizde karşılığı bulunmaması dolayısıyla çalışma kapsamında Türkçe "bulanıklaştırma" teriminin kullanımı tercih edilmiştir. Söz konusu teknik terim çalışmanın 3.1.2. no'lu bölümünde ayrıntılı olarak açıklanmaktadır.

"kullanıcıların makul beklentisi" olarak ifade edilmektedir. Şifreleme veya bulanıklaştırmayı yetersiz bulan bir yaklaşımın düzenlemesi olan GDPR bakımından bu hüküm dikkat çekici bir hususa değinmektedir. Veri kontrolörünün veriyi bulut hizmet sağlayıcısına vermeden önce şifrelemesi veya bulanıklaştırması onu sorumluluktan kurtarabileceği anlamına gelmektedir. Zira herhangi bir veri ihlali durumunda şirketlerin kendi şifreleme anahtarlarını tutarak bireylerin veri gizliliği konusundaki "makul beklentilerini" karşılama konusunda gerekli adımları atmış olduklarını veri koruma otoritesine savunma olarak sunabilecekleri değerlendirilmektedir.

2.2.3. Veri Koruma Tüzüğü'nün Kapsamı

Veri Koruma Tüzüğü'nün getirmiş olduğu yeni düzenlemelere yalnızca veri koruma hukukunun karmaşık ve tartışmalı meseleleri olmaları bakış açısıyla değil aynı zamanda yeni dünya düzeninin ekonomi politikalarına etkisi bakış açısıyla da bakılması gerekmektedir. Zira söz konusu düzenleme daha oluşturulma aşamasında endüstri ve sivil toplum kuruluşlarının güçlü ve zorlayıcı mücadelesine sahne olurken AB'nin karar organları Avrupa Komisyonu, Konsey ve Parlamento'nun kendi içindeki çekişmeleri de metnin oluşturulma sürecine yansımıştır. Zira her bir kuruluşun söz konusu Tüzük'ün hayata geçirilmesindeki temel güdüsü birbirinden farklıdır; örneğin Komisyon daha çok ekonomik gelişme ve güvenlik gibi kaygılarla hareket ederken Parlamento'nun önceliği temel bireysel hakların korunmasıdır. Aslında bu gruplar arasında var olan mahremiyetin ne olduğu ve her bir üye devlette nasıl korunması gerektiğine ilişkin görüş ayrılıkları bile GDPR'nin hazırlanması ve kabulü süreçlerinin neden uzun sürdüğünü açıklamaktadır.

173 paragraflık resital bölümü ve 99 maddeden oluşan temel tüzük metniyle yaklaşık 90 sayfadan oluşan GDPR oldukça kapsamlı bir veri koruma çerçevesi sunmaktadır. Bu çalışmanın kapsamı açısından söz konusu düzenlemenin tüm maddelerinin münferiden ele alınması mümkün değildir. Bu nedenle çalışmada, dijital ekonomi üzerindeki etkileri bakımından önemli olduğu değerlendirilen ve GDPR'nin köklü yenilikler öngördüğü şu üç temel özelliğine odaklanılmıştır:

i) Kişisel verilerin ve veri sahiplerinin daha etkin korunması,
ii) Veri işleyenler ile veri kontrolörlerinin artırılmış sorumlulukları,
iii) Uygulanma alanı bakımından daha güçlü düzenlemelere sahip olması.

i) Etkin Kişisel Veri/ Veri Sahibi Koruması

Kişisel veri sahiplerinin hakları kapsamına alınan "unutulma hakkı" GDPR'nin 17. maddesi kapsamında silinme hakkı (*right to erasure)* başlığı altında düzenlenmektedir. Söz konusu madde ile 95/46 sayılı Direktif'in 12. maddesinin (b) bendinde veri sahibine tanınan hakkın kapsamının genişletildiği görülmektedir. Veri sahipleri, verilerinin artık toplanma amacı ile ilgili olarak tutulmasının gerekli olmadığı, veri sahibin rızasının bulunmadığı yahut veri sahibinin verisinin işlenmesini istemediği veya kişisel verinin GDPR'ye aykırı işlendiği durumlarda verilerinin silinmesini veya bundan sonra işlenmemesini talep edebilme hakkına sahiptir. 17. maddenin üçüncü fıkrası ve 65 no'lu resital birlikte değerlendirildiğinde söz

konusu hakkın uygulamasının mutlak olmadığı ve bazı istisnalar tanındığı görülmektedir. Zira bilgi ve ifade hürriyetinin kullanılması için gerekli olması ve belirli yasal istisnalar ile kamu yararı gibi gerekliliklerin bulunması (istatistiksel amaçlar, genel sağlık, bilimsel araştırmalar vb.) durumlarında kişisel verilerin tutulması hukuka uygun olarak değerlendirilmektedir.

GDPR kapsamında düzenlenen unutulma hakkının Google İspanya kararında veri sahipleri bakımından öngörülen haklardan çok daha geniş kurgulandığı görülmektedir. Zira 17. maddenin ikinci fıkrasında veri kontrolörünün, kişisel veriyi başka veri kontrolörleriyle paylaşmış veya kullanımlarına açmış olması durumunda söz konusu verilere ilişkin kısayol, kopya veya çoğaltılmış versiyonları silmeleri bakımından da sorumlu olduğu görülmektedir. Bu kapsamda, veri kontrolörünün somut durum içerisinde teknolojinin elverişli imkânları dâhilinde uygun tedbirleri alması gerektiği vurgulanmaktadır. Unutulma hakkı GDPR kapsamında veri sahiplerine tanınan imkânlar setinin yalnızca bir tanesi olup Tüzük kapsamında veri sahipleri oldukça detaylı hükümler ile korunmaktadır. 12. maddede düzenlenen kişisel verilerin şeffaflığı konusunda tanınan ilave yetkiler, 13, 14 ve 15. maddelerde düzenlenen güçlendirilmiş kişisel veriye erişim hakkı, 20. maddede düzenlenen veri taşıma hakkı ve 21. ve 22. maddelerde tanınan itiraz hakkıyla oldukça detaylı bir korumanın getirildiği görülmektedir. Ayrıca 22. maddenin ilk fıkrasında veri sahiplerine, kendileri bakımından hukuki veya başka önemli etkiler meydana getiren otomatik işlemelere (profilleme de dâhil olmak üzere) konu olmamayı talep edebilme hakkı düzenlenmektedir. Getirilen bu yeni koruma yoluyla özellikle algoritmalar ve diğer otomatik veri işleme yöntemleriyle hukuki anlamda giderek kontrolünü yitiren veri sahiplerine tasarruf alanı tanınmaya çalışılmaktadır. Madde kapsamında söz konusu hakkın sınırları da belirlenmiş bulunmaktadır. Bu kapsamda; veri sahibi ile veri kontrolörü arasındaki sözleşme ilişkisi için gerekli olması, AB ve üye devlet hukukunca veri kontrolörüne bu konuda yetki verilmiş olması veya veri sahibinin açık rızasının bulunması durumları istisnadır.

95/46 sayılı Veri Koruma Direktifi'nde yer almayan veri taşınabilirliği hakkı (data portability) ilk kez GDPR'nin 20. maddesiyle tanımlanmıştır. Bu madde ile veri sahibi kişisel verisini tutmaya yetkili bir veri kontrolöründen diğerine taşıyabilme yetkisine sahiptir. Maddenin ikinci fıkrasında belirtildiği üzere teknik olarak mümkün olması durumunda veriler bulunduğu veri kontrolöründen diğerine doğrudan iletilebilmektedir. Veri taşınabilirliği, veri sahiplerine verileri üzerinde oldukça geniş bir hâkimiyet alanı tanıyan etkileyici bir araç gibi gözükmesine karşın kullanımına dikkat edilmesi gerektiği, zira söz konusu hakkın kişisel veriyi gereğinden fazla erişilebilir kılarak ve piyasadaki oyuncaların kendini düzeltme hakkını ortadan kaldırarak inovasyonun gelişimini engelleyebileceği yönünde eleştiriler yapılmaktadır.[18]

Veri işlemeyi hukuka uygun hale getiren veri sahibinin rızasına ilişkin 4. madde hükmünün de veri sahibinin lehine olacak biçimde düzenlendiği görülmektedir. 7. maddede yer alan 'rızanın şartları' başlıklı düzenlemeye de uygun olarak, veri sahibine karşı yapılan veri işlemeye ilişkin rıza talebinin anlaşılır ve kolay erişilebilir bir biçimde, açık ve sade dille

[18] ENGELS, Barbara, 'Data Portability among Online Platforms', Internet Policy Review 5(2), 2016 sh.2.

yapılması gerekmektedir. Ayrıca veri sahibinin söz konusu rızasını geri alma hakkı her zaman bulunmaktadır. Üçüncü fıkrada belirtildiği üzere rıza nasıl veriliyorsa aynı kolaylıkla geri alınabilecektir (usûlde kolaylık sağlanması). Ancak rıza konusunda getirilen söz konusu düzenleme "kural-uygulama ilişkisi" bağlamında kâğıt üzerinde kalan hakkın uygulamada ne gibi sonuçlar doğuracağının belirsiz olması noktasında eleştirilmektedir. Zira aydınlatılmış veri sahibinin açık rızasını kişisel veri korumasının odağına koymak, zaten uygulamasının çok da etkili olamayacağı öngörüleri varken, giderek daha karmaşık bir hal alan dijital dönüşüm karşısında veri koruma anlamında kifayetsiz kalınacağı yönünde eleştirilmektedir. Nitekim kullanıcıların yalnızca rızalarının olmayışının değil teknolojik ilerleme içerisinde belirli koşullar altında (kuşak, eğitim düzeyi ve finansal durum gibi farklılıkların bu koşulları daha da keskinleştirdiği de göz önüne alındığında) vermiş oldukları her rızanın zaten bu güvenceyi temin edemeyeceği ifade edilmektedir.[19] GDPR ile getirilen tüm bu geniş hak ve yetkiler veri sahiplerine verilerinin kaderini belirleyebilme konusunda oldukça geniş bir alan sağlarken veri işleyenlere ise oldukça detaylı sorumluluklar yüklemektedir.

ii) Veri İşleyenlerin Artırılmış Sorumlulukları

GDPR veri işleyenlerin sorumlulukları konusunda oldukça detaylı hükümler içermektedir. Tüzük kapsamında sorumlulukların yalnızca nitelikleri değişmemiş, sorumlu kişilerin kapsamı da genişletilmiştir. 95/46 sayılı Direktif'te veri kontrolörü ve veri işleyicileri arasında sorumlulukları bakımından ikili bir ayrım söz konusu iken GDPR bu ayrımı ortadan kaldırmaktadır. Direktif'te veri kontrolörü kişisel veri işlemenin amaçlarını ve yöntemini belirleyen kişi iken veri işleyicisi veri kontrolörü adına kişisel verileri işleyen kişiyi ifade etmektedir. Direktif'e göre veri koruma hukukundan doğan sorumlulukların yalnızca veri kontrolörü bakımından geçerli olması uzun yıllar ağır eleştirilere sebep olmuştur. Çünkü bilhassa veri işlemenin amaç ve yöntemini kimin belirlediğinin anlaşılamayacağı kadar karmaşık ilişkiler bakımından veri işleyenlerce hukuki boşlukların kullanılması ile sorumluluktan kurtulunmaktadır. GDPR bu ayrımı ortadan kaldırarak kişisel veri ihlallerine ilişkin durumlarda (sorumluların belirlendiği 30, 31, 32, 33, 79 ve 82. maddelerinde) hem veri kontrolörünün hem de veri işleyicisinin sorumlu olduğunu hüküm altına almaktadır. Ayrıca 26. maddede düzenlenen çoklu sorumlular sistemi ile birden fazla kontrolörün olması durumda sorumluluk rejimi de açıklığa kavuşturulmuştur.

GDPR kapsamında veri kontrolörlerinin oldukça geniş bir sorumluluk alanının bulunduğu görülmektedir. Tüzük'ün 5. maddesinde sayılan temel prensiplere uygun veri işlemenin gerçekleştirilmesi veri kontrolörünün sorumluluğundadır. Yine Tüzük'ün 25. maddesi kapsamında veri kontrolörü bakımından *'Başlangıçtan itibaren ve tasarımdan itibaren veri koruması (data protection by design and by default)'* adında yeni bir yükümlülük türünün tanımlandığı görülmektedir. Maddenin birinci fıkrasına göre veri kontrolörü, veri sahiplerinin korunması bakımından Tüzük'te yer alan önemli prensiplerin (veri minimizasyonu gibi) uygulanmasından ve uygun teknik ve organizasyonel önlemleri (bulanıklaştırma gibi) kullanarak veri koruma hukukundan doğan sorumlulukların etkili bir

[19] BORGESIUS, Frederik J. Zuiderveen, 'Informed Consent: We Can Do Better to Defend Privacy', IEEE Security and Privacy 13, 2015, sh. 103–107.

biçimde yerine getirilmesinden sorumludur. Başka bir ifadeyle belirli amaç için gerekli olan veri işleme faaliyeti bakımından veri kontrolörü söz konusu verinin veri koruma mevzuatına uygun olarak işlenmesi için, başlangıçtan itibaren (by default) uygun teknik ve organizasyonel önlemleri almakla yükümlüdür. Söz konusu yükümlülük verinin toplandığı süre ve işlenmesi faaliyeti kapsamda kişisel verinin saklandığı ve veriye erişilebildiği müddetçe geçerlidir. Madde kapsamında öngörülen önlemler bakımından, başlangıçtan itibaren (by default), kişisel verilerinin bireyin herhangi bir girişimi olmaksızın belirsiz sayıda kişinin erişimine açılmadığının temin edilmesi gerekmektedir.

Özellikle yeni teknolojiler kullanarak gerçekleştirilen ve kişi hak ve hürriyetleri bakımından önemli tehlikeler meydana getiren veri işleme faaliyetlerinde veri kontrolörü kişisel verilerin korunması bakımından öngörülen etkilere ilişkin temel bir değerlendirme yapmak durumundadır. Tüzük'ün 35. maddesiyle getirilen söz konusu değerlendirme faaliyeti 'veri koruma etki değerlendirmesi-data protection impact assessment' (DPIA) olarak adlandırılmaktadır. Bu değerlendirmede, öngörülen veri işleme faaliyetinin, güvenlik önlemleri de dâhil, sistematik olarak açıklanması, işlemenin gerekliliğine ve işleme amaçlarıyla orantılılığına ilişkin değerlendirmenin yapılması ve veri sahibinin hak ve hürriyetlerinin korunmasına ilişkin önlemlerin ele alınması gerekmektedir. DPIA kurumsal uygulaması zorunlu bir yöntemdir. Dolayısıyla, üye ülkelerin veri koruma otoriteleri tarafından DPIA'ya tabi veri işleme faaliyetlerinin bir listesinin oluşturulması gerekmektedir. Böylece veri işleme faaliyetinin söz konusu listede yüksek riskli olarak değerlendirildiği faaliyetler bakımından veri kontrolörünün veri koruma otoritesinden görüş alabilme imkânı ortaya çıkmaktadır. Tüzük'ün 58. maddesine göre söz konusu talebi alan veri koruma otoritesinin görüşüne başvuran veri kontrolörüne yazılı olarak tavsiye vermesi gerekmektedir. Bu yazılı tavsiye kapsamında veri kontrolörüne, uygun olduğu ölçüde geçici önlemler önerilebileceği gibi veri işlemenin yasaklanması gibi kesin önlemler dâhil çeşitli kararlar verilmesi mümkündür.

GDPR kapsamında veri işleyenler bakımından ortaya konulan birçok çözüm mekanizması da bulunmaktadır. Örneğin 37. maddeyle getirilen düzenleme kapsamında bazı veri kontrolörlerinin (işlenen verinin hassas veri olması veya hacimsel olarak çok büyük olması durumlarında) veri koruma görevlisi (*DPO*) olarak belirlenmesi mümkündür veya Tüzük'ün 5. kitabında yer alan gönüllü davranış kuralları yoluyla veri işleyen işletmelere bir takım imkânlar sağlanmaktadır. Zira AB veri koruma kuralları ile sektör çıkarları arasındaki temel dengenin korunması ihtiyacı vakidir. Veri koruma otoriteleri bir yandan söz konusu ihlalleri 'sert' müdahale araçlarıyla yaptırıma tabi tutarken diğer yandan geniş kapsamlı soruşturma, düzeltme, yetkilendirme ve danışmanlığı kapsayan araçlarını kullanabilmektedir. Veri ihlalinin ağırlığına göre değişen oranlarda veri koruma otoriteleri tarafından oldukça yüksek idari para cezaları uygulanabilmektedir. Bu kapsamda 200 milyon Avroya varan para cezalarının yanında, ihlalin teşebbüs aşamasında kalması durumunda, söz konusu şirketin önceki mali yıl küresel cirosunun % 4'üne varan para cezaları öngörülmektedir. Neticede GDPR, şirketler için Avrupa pazarını daha erişilebilir kılma çabasının yanında öngörmüş olduğu hükümlerle çok daha etkili ve sorunsuz bir izleme sistemi sağlamaya çalışmaktadır. Sayısal Tek Pazar Stratejisi bağlamında Tüzük içerisinde 'one-stop shop' hükmü yerini

almıştır. Tüzük'ün 56. maddesinin birinci fıkrası kapsamında veri kontrolörü veya işleyicisinin birden fazla üye devlette faaliyette bulunması durumunda, ana kuruluş merkezinin bulunduğu yer veri koruma otoritesi 'yetkili otorite' olarak adlandırılır ve söz konusu otorite veri kontrolörü veya işleyicisinin tüm üye devletlerde yürüttüğü sınır-ötesi veri işleme faaliyetleri bakımından yetkilidir.

Veri koruma otoritelerinin ele alındığı altıncı bölümün tamamında ulusal veri koruma otoritelerinin rolü ve sorumlulukları tanımlanırken üye devletlerin, başta insan, teknik ve mali kaynaklar olmak üzere, söz konusu kuruluşlara görevlerini etkili olarak yerine getirebilmeleri için gerekli altyapıyı sağlamaları gerektiği vurgulanmaktadır. GDPR'de veri koruma otoritelerine tanınan yüksek idari para cezalarına ilişkin düzenlemeler de bu yaklaşımı destekler mahiyettedir. (m.83) Tüzük'ün yedinci bölümünde düzenlenen, veri koruma otoriteleri arasındaki işbirliği ve uyum konusunda öngörülen mekanizma ile hem uyuşmazlıkların koordineli yorumu ve çözümü hem de GDPR hükümlerinin sınır ötesi uygulanması hedeflenmektedir. Ayrıca bu bölümde yer verilen "Opinion of the Board" hükmü ile öngörülen güçlü bir AB Veri Koruma Platformu'nun (European Data Protection Board) 95/46 sayılı Direktif ile getirilen 29. Madde Çalışma Grubunun yerini alması sağlanmaya çalışılmaktadır.

iii) Uygulanma Alanı Bakımından GDPR

GDPR'nin uygulama alanı Tüzük'ün 3. maddesi ile düzenlenmiş olup AB sınırları içerisinde faaliyet gösteren veri kontrolörleri ile işleyicilerinin faaliyetleri kapsamında gerçekleştirdikleri kişisel veri işlemeleri bakımından, işlemenin birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, GDPR hükümleri uygulanmaktadır. Temel kuralı ifade eden birinci fıkra hükmünün istisnaları ise ikinci fıkrada tanımlanmıştır. Buna göre GDPR hükümleri, veri işleme faaliyeti kapsamında sunulan mal veya hizmetin AB içerisinde sunuluyor olması durumunda veya söz konusu davranışların AB içerisinde gerçekleşmesi kadar davranışların gözlemlenmesi durumunda uygulanır. Yani GDPR, Birlik içerisindeki veri sahiplerine (ücretsiz olsa dahi) mal veya hizmet sunan yahut (AB içerisinde) söz konusu veri sahiplerinin davranışlarını gözlemleyen veri kontrolörleri ve işleyiciler bakımından uygulama alanı bulmaktadır. Bir veri kontrolörü veya işleyicisinin AB içerisinde mal veya hizmet sunup sunmadığının nasıl belirleneceğine ilişkin detaylar GDPR'nin 23 no'lu resitalinde belirlenmektedir. AB içerisinde mal veya hizmet sunmak yalnızca bir internet sitesine veya e-posta kutusuna erişimi ifade etmez, ayrıca birden çok AB üyesinde faaliyette bulunulduğunu ortaya koyan dil ve ödeme cinsi/para birimi seçimi ve/veya AB'deki kullanıcı ya da müşterilerin izlenmesini de ifade eder. Bu maddeye göre bir veri kontrolörü veya işleyicisinin bir veya daha fazla AB üyesi ülkede bireylere veri hizmeti sunması durumunda GDPR'nin uygulanacağı kabul edilir. GDPR metninde kullanılan "davranışların izlenmesi" terimiyle, örneğin bireylerin başta tüketim tercihlerinin ve alışkanlıklarının tespiti amacıyla teknik yöntemlerle internetteki faaliyetlerinin gözetlenmesi ifade edilmektedir. Bu hüküm uygulamada AB dışında faaliyet göstermesine karşın AB tüketicisini hedefleyen şirketlerin GDPR'ye tabi olacakları anlamına gelmektedir. Bu madde kapsamında yaratılan yeni durumun Tüzük'ün kapsayıcı mahiyetinin önemli bir uzantısı olduğu ve uygulama bakımından oldukça önemli bir etkiye sebep olacağı değerlendirilmektedir.

Üçüncü bir ülkenin veya uluslararası organizasyonun Avrupa Komisyonu tarafından "yeterli koruma düzeyine sahip" olarak nitelenmesi durumunda GDPR kurallarının nasıl uygulanacağı hususu tartışılmaktadır (45. madde). Komisyon tarafından alınan bu yönde bir karar tüm AB ülkeleri bakımından bağlayıcı olmasının yanında söz konusu üçüncü ülke bakımından kişisel veri aktarımı için herhangi bir ilave yetkilendirmeye gerek bırakmamaktadır. Komisyonun yaptığı söz konusu değerlendirme Schrems Kararıyla amaçlanan hukuki durumu güçlendirmektedir, zira 104 nolu resitalde de belirtildiği üzere Komisyon söz konusu üçüncü ülkede hukukun üstünlüğü, adalete erişim, uluslararası insan hakları norm ve standartlarına uygunluk, temel sektörel iç hukuk düzenlemeleri, kamu düzenine ilişkin kurallar da dâhil savunma ve ulusal güvenlik ile ceza hukuku mevzuatı bakımından temel bir uygunluk değerlendirmesi yapmak durumundadır. Tüm bu değerlendirme neticesinde üçüncü ülkenin AB'de sağlanan veri koruma çerçevesine uygun yeterli koruma düzeyini sağlayabiliyor olması gerekmektedir. Özellikle veri koruma denetiminin sağlanması bakımından bağımsız bir veri koruma otoritesini haiz bulunulması, üye devletlerin veri koruma otoriteleriyle işbirliği mekanizmalarının hayata geçirilmesi ve bu alanda etkili ve uygulanabilir idari ve hukuki yaptırımların öngörülüyor olması gerekmektedir.

45. maddede tanımlanan anlamda bir yeterli koruma düzeyi kararının bulunmaması durumunda ise 46. maddeye göre kişisel verilerin transferi, ancak uygun önlemlerin alındığı ve veri sahibinin haklarının korunarak buna ilişkin etkili yaptırım mekanizmalarının sağlandığının garanti edildiği durumda mümkündür. Bu yöntem ise hem yasal belirsizlikler dolayısıyla kanıtlanması zor hem de maliyeti bakımından dezavantajlı bir mahiyet arz etmektedir.

2.2.4. Veri Koruma Tüzüğü'ndeki Temel İlkeler

Farklı düzenleme biçimleri şeklinde kabul edilmelerine rağmen temel olarak bakıldığında hem 95/46 sayılı Direktif hem de GDPR aynı amaca hizmet etmektedir. Bu temel amaç; veri işleme ve üye devletler arasında verinin serbest dolaşımı faaliyetleri sırasında gerçek kişilerin temel hak ve özgürlüklerinin korunmasıdır. Söz konusu temel hedefe ulaşılması amacıyla GDPR'de bir dizi temel prensibe yer verilmiştir. GDPR'nin prensipler başlıklı ikinci bölümünde yer alan 5. maddesinde verinin işlenmesi sırasında uyulması gereken temel prensipler ifade edilmektedir. Buna göre;

- Kişisel verilerin hukuka uygun, dürüstlük kurallarına uygun ve veri öznesine karşı şeffaf işlenmesi gerekmektedir. (hukukilik, dürüstlük ve şeffaflık ilkesi; 5.m/1.f/(a))
- Kişisel verilerin belirli, açık ve meşru amaçlarla toplanması gerekmektedir. (amaçla sınırlılık ilkesi; 5.m/1.f/(b))
- Kişisel veriler işleme için gerekli olduğu kadar, ilgili ve ölçülü biçimde işlenmelidir. (veri minimizasyonu prensibi; 5.m/1.f/(c))
- Kişisel verilerin doğru olarak, gerekli hallerde ve güncel tutulması gerekmektedir. (doğruluk prensibi; 5.m/1.f/(d))
- Kişisel verinin işlenmesi amacı için gerekli olandan daha uzun süre tutulmaması gerekmektedir. (veri saklamanın sınırlandırılması prensibi; 5.m/1.f/(e))

- Veri işlemenin güvenli olması gerekmektedir. (bütünlük ve gizlilik prensibi; 5.m/1.f/(f))
- Veri kontrolörü yukarıda sayılan tüm temel prensiplerden sorumludur. (hesap verebilirlik prensibi; 5.m/2.f)

3. TÜRKİYE'DE MEVCUT DURUM

3.1. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

24/03/2016 tarihinde TBMM Genel Kurulu'nda kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu" 07/04/2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Söz konusu kanun ile kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin koruması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi amaçlanmaktadır.

Kanunun yürürlüğe girmesiyle ülkemiz BİT sektörünün başta AB ülkeleri olmak üzere yurt dışına bilgi toplumu hizmetleri sunabilmesi, kişisel verinin temel girdi olduğu finans, sağlık, sigortacılık gibi sektörlerde ülkemizin iş potansiyelinin artması ve sınır ötesi veri paylaşımı ve adli işbirliği kanallarının etkin çalışmasının sağlanacağı öngörülmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'yla, AB ülkeleri nezdinde veri koruma bakımından güvenilir ülke statüsüne kavuşulması konusunda önemli bir kriter karşılanmış bulunmaktadır. Söz konusu Kanun ile bağımsız ve özerk bir Veri Koruma Otoritesinin kurulması ve akabinde ikincil mevzuat düzenlemelerinin hazırlanması öngörülmektedir.

3.1.1. 6698 sayılı Kanun'un Kapsamı

Kanun'un kapsam maddesinde belirtildiği üzere, söz konusu düzenlemelerin uygulanması bakımından kamu ve özel sektör ayrımı yapılmamış olup düzenlenen usul ve esaslar her iki sektör bakımından da uygulama alanı bulmaktadır. Veri sorumlularının, devlet ya da özel sektör fark etmeksizin, kişisel verilerin güvenliğine ilişkin yükümlülükleri Kanun'un 12. maddesinde düzenlenmiştir. Maddeye göre veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek, ayrıca verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin korunması hakkının kapsamına bakıldığında ise bu kanunun uygulaması bakımından bu hakkın temel süjesinin gerçek kişiler olduğu görülmektedir. Kanun'un hem kapsam maddesi olan 2. maddesi hem de kişisel verinin tanımlandığı 3. maddesinden sadece gerçek kişilerle ilişkili verilerin Kanun kapsamında korunduğu anlaşılmaktadır. Söz konusu yaklaşımın hem 95/46 sayılı Direktif'te hem de GDPR'de yer alan AB yaklaşımıyla uyumlu olduğu görülmektedir.

6698 sayılı Kanun'un kapsamına ilişkin dikkat çeken hususlardan biri ise ölmüş gerçek kişilerin kişisel verilerine ilişkin herhangi bir düzenleme öngörmemiş olmasıdır. Zira GDPR kapsamında 27 no'lu resitalde ölmüş gerçek kişilerin verilerinin Tüzük'ün uygulama alanı dışında olduğu açıkça belirtilmiş olup bununla birlikte söz konusu verilerin üye ülkelerin kendi iç hukuk düzenlemeleri yoluyla ölmüş kişilerin kişisel verilerinin işlenmesine ilişkin kurallar öngörebileceği ifade edilmektedir.

3.1.2. 6698 sayılı Kanun'daki Temel Kavramlar

i. *Kişisel Veri*: Kişisel veri kavramının, Kanun'un tanımlar başlıklı 3. maddesinin (d) bendinde "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde tanımlandığı görülmektedir. Bu çerçevede, gerek bir gerçek kişinin doğrudan belirlenmesini sağlayan ad, soyad, nüfus kayıt bilgileri veya adresi gibi bilgileri gerekse kişiyi fiziksel olarak tanımlayıcı bilgileriyle ekonomik ve sosyal özelliklerine ilişkin bilgileri kişisel veri tanımı içerisinde yer almaktadır. Söz konusu Kanun'un gerekçe kısmında, "*mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesinin"* verinin kişisel veri olarak kabulü bakımından yeterli olduğu ifade edilmektedir. Dolayısıyla isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi verilerin kişileri belirli veya belirlenebilir kılacakları gerekçesiyle kişisel veri oldukları belirtilmektedir.

   GDPR düzenlemesinde kişisel veri tanımında esaslı bir değişikliğe gidilmemekle birlikte söz konusu tanımın oldukça detaylı kaleme alındığı ve somut örneklemelerin çeşitlendiği görülmektedir. Tüzük kapsamında kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi kişisel veriyi ifade etmekte olup, doğrudan veya dolaylı olarak, bir gerçek kişinin tanımlanmasına elverişli başta isim, kimlik numarası, konum/yer bilgisi, bir çevrimiçi tanımlayıcı yahut kişinin fizikî, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla hususa işaret eden her türlü veri kişisel veri olarak kabul edilmektedir.

ii. *Kişisel verilerin işlenmesi:* Veri işleme kavramına ilişkin Kanun'un 3. maddesinin (e) bendi kapsamında, "*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* şeklinde oldukça geniş bir tanım yapıldığı görülmektedir. Bu çerçevede kişisel verilerin işlenmesi, verinin ilk defa elde edilmesinden başlayıp veri üzerinde gerçekleştirilen her türlü faaliyeti ifade etmektedir.

   GDPR kapsamında getirilen veri işleme tanımının 95/46 sayılı Direktif ile, küçük farklılıklar dışında, örtüştüğü görülmektedir. Kişisel verilerin veya veri setlerinin otomatik ya da otomatik olmayan araçlarla toplanması, saklanması, elde edilmesi, yapılandırılması, değiştirilmesi, okunması, sorulması, kullanılması, üçüncü taraflara aktarılması, yayılması ya da hazır bulundurulması için yapılan işlemlerle verilerin

kombinasyonu, kısıtlanması ('blocking' kavramı yerine 'restriction'[20] kavramı), silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü müdahale "veri işleme" kabul edilmektedir. Söz konusu tanım kapsamında Tüzük kişisel veriye ilişkin hemen hemen her türlü müdahaleyi veri işleme kabul etmektedir. AB Veri Reformu çalışmalarında getirilmesi amaçlanan temel yaklaşımlardan birinin gelişen yeni teknolojilerin dikkate alınmasının bir yansıması olarak, başta büyük veri teknolojisi gibi yapılandırılmamış veriler ve veri setleri üzerinde yapılan çalışmalarda meydana gelmesi muhtemel kişisel veri ihlallerinin önlenmesi amacıyla söz konusu tanıma "veri setleri" ve "yapılandırma" gibi yeni unsurların ilave edildiği görülmektedir.

iii. *Veri kayıt sistemi:* Bu sistemle kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi kastedilmektedir. Söz konusu kavramın gerek 95/46 sayılı Direktif'te yer alan "kişisel veri dosyalama sistemi" gerekse GDPR'da yer alan "dosyalama sistemi" ile örtüştüğü görülmektedir. Kanunun gerekçesinde de belirtildiği üzere veri kayıt sistemleri gerek elektronik gerekse fiziki ortamda oluşturulabilmektedir.

iv. *Veri sorumlusu:* Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiler veri sorumlusu olarak ifade edilmektedir. Kanun'un 3. maddesinin (ı) bendinde yer alan veri sorumlusuna ilişkin tanımın GDPR kapsamında yer alan veri kontrolörüne karşılık geldiği görülmektedir.

Veri sorumlusu bir veya birkaç gerçek kişi olabileceği gibi şirketler, kamu kurum/kuruluşları veya sivil toplum kuruluşları gibi tüzel kişiler de olabilmektedir. GDPR'deki veri kontrolörüne ilişkin hükme göre işleme amaç ve araçlarının doğrudan AB veya üye ülke kanunlarınca belirlenmesi durumunda, kontrolörün veya belirli ölçütleri karşılaması durumunda sorumlunun kim olacağının AB veya üye ülke kanunlarıyla belirlenebileceği düzenlenmektedir.

v. *Veri işleyen:* Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade etmektedir. Söz konusu tanım GDPR düzenlemesinde öngörülen tanımla aynıdır. Kanun'da yer alan tanım ışığında veri işleyen, kişisel verileri bizzat veri sorumlusu tarafından verilen talimatlar çerçevesinde işleyen bir çalışan olabileceği gibi veri sorumlusuyla aralarında veri işlenme hususunda hizmet sözleşmesi bulunan ayrı bir gerçek veya tüzel kişi de olabilmektedir. Gerekçede yer alan örneğe göre bir muhasebe şirketi, kendi personeliyle ilgili tuttuğu verilerin işlenmesi bakımından veri sorumlusu iken aynı şirketin müşterisi olan şirketlere ilişkin kişisel verilerin işlenmesi açısından veri işleyen olarak kabul edilmektedir.

[20] 'Restriction of processing' kavramı ile neyin ifade edildiği Tüzük'ün 4. maddesinin ikinci fıkrasında açıklanmıştır. Buna göre; veri işlemeye ilişkin kısıtlama (restriction), saklanmakta olan kişisel verilerin gelecekteki işlemelerini sınırlandırmak amacıyla işaretlenmeleri anlamına gelmektedir.

GDPR veri koruma hukukundan doğan sorumlulukların yalnızca veri kontrolörü bakımından geçerli olması ve işleyenlerin sorumluluktan kaçabilmesine imkân tanıyan sorumluluk ayrımını ortadan kaldırarak kişisel veri ihlallerine ilişkin durumlarda (sorumluların belirlendiği 30, 31, 32, 33, 79 ve 82. maddelerinde) hem veri kontrolörünün hem de veri işleyicisinin sorumlu olduğunu hüküm altına almaktadır. Bu yaklaşımın bilhassa veri sorumlusu ve veri işleyen kavramlarının ayırt edilmesinin güç olduğu uygulamada önem arz ettiği değerlendirilmektedir. Ancak 6698 sayılı Kanun'un 18. maddesinin ikinci fıkrasında veri sorumlusu ve veri işleyen açısından farklı bir sorumluluk düzeyi belirlenerek idari cezaların uygulaması bakımından yalnızca veri sorumlularına yaptırım uygulamaktadır. Yine veri sorumluları siciline kaydın yalnız veri sorumluları bakımından gerekli olduğu görülmektedir. Veri işleyenlerin sorumlulukları noktasında benimsenen bu yaklaşım GDPR'de benimsenen geniş sorumluluk alanı yaklaşımıyla farklılık arz etmektedir.

vi. *Açık Rıza:* Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade edilmektedir. Bu çerçevede söz konusu kavram, ilgili kişinin kendisiyle ilgili verilerin işlenmesine, özgür iradesiyle, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak vermiş olduğu rıza beyanını ifade etmektedir. Kanunda yer alan birçok hükümde kişisel verilerin toplanması, işlenmesi ve saklanması bakımından kişinin rızasının alınması gerekmekte, başka bir anlatımla veri işleme faaliyetleri bakımından ilgilinin rızası hukuka uygunluk sebebi mahiyetinde bulunmaktadır. Dolayısıyla veri sorumluları bakımından, alınacak rızanın "açık rıza" tanımıyla uyumluluk arz etmesi elzemdir.

   Kanun'da yapılan rıza tanımının 95/46 sayılı Direktif'te yer alan tanımla uyumlu olduğu görülmektedir. Bununla birlikte GDPR'nin 4. maddesinin 11. fıkrasında ifade edilen rıza tanımına ise bir ekleme yapıldığı görülmektedir. GDPR'ye göre rıza, veri sahibinin beyanı, durumu veya onay ifade eden bir davranışı yoluyla kişisel verilerinin işlenmesini özgür iradesiyle, belirli bir konuda, aydınlatılmış ve açık ('unambiguous' kavramı rıza tanımına girmiştir.) olarak kabul ettiğine ilişkin bir göstergeyi ifade etmektedir. Bu kapsamda rızanın açıkça, kesin bir biçimde verilmiş bulunması ifadesi tanıma girmiş bulunmaktadır.

vii. *Anonim Hale Getirme:* Kanun'un 3. maddesinin (b) bendinde yer alan anonim hale getirme kavramıyla kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi ifade edilmektedir. Bu çerçevede anonim hale getirmede, yapılan işlemler sonucunda belirlenebilir kişi ile veri arasındaki bağ koparılmakta, gerçek kişinin kimliğinin tespiti imkânsız hale getirilerek verinin ait olduğu kişiye ulaşmak mümkün olmamaktadır. Dolayısıyla anonim hale getirilen veriler, kişisel veri sayılmamaktadır. Kanun'un gerekçesinde de ifade edildiği üzere kalan veriler

üzerinden izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğu anlaşılabiliyorsa zaten bu verinin anonim hale getirilmediği kabul edilmektedir.

GDPR kapsamında ise anonimleştirme teriminin yer almadığı, bunun yerine tanımlar başlıklı 4. maddenin beşinci fıkrasında son dönemde gelişen kişisel veri işleme teknolojileriyle yakından ilgili bulunan "bulanıklaştırma (pseudonymisation)" terimine yer verildiği görülmektedir. İlk olarak belirtilmesi gereken husus ise bu iki terimin birbirlerinden oldukça farklı kavramları ifade ettikleridir.[21] Bu çerçevede bulanıklaştırma kavramıyla, kişisel verilerin ek bilgi kullanılmaksızın belirli bir veri süjesine artık atfedilemeyecek biçimde işlenmesi ifade edilmektedir. Maddede söz konusu ek bilgilerin ayrı ayrı tutulması gerektiği ve söz konusu kişisel verilerin belirli veya belirlenebilir bir gerçek kişiye atfedilmemesinin sağlanması konusunda teknik ve idari önlemlerin alınması gerektiği ifade edilmektedir.

Tüzük'ün 26 no'lu resitalinde yer alan açıklamalara bakıldığında, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilebilecek her türlü veriye ilişkin işlemelerin temel veri koruma ilkelerinin uygulama alanında olduğu ifade edilmektedir. Bu kapsamda ilave bilgilerin biraraya getirilmesi vasıtasıyla kişi hakkında tanımlayıcı verilerin elde edilebildiği bulanıklaştırma işleminde de halen kimliği belirlenebilir gerçek kişiler hakkında doğrudan bilgi sağlama imkânının bulunduğuna dikkat çekilmektedir. Bir gerçek kişinin belirlenebilir olup olmadığının tespiti konusunda, gerek veri kontrolörü gerekse bir başkası tarafından verinin ilişkili olduğu kişinin doğrudan veya dolaylı olarak tespitine imkân sağlayan ve kullanılması makul sayılabilecek tüm yöntemler, örneğin seçip ayıklama (single out), hesaba katılmalıdır. Söz konusu belirlemede kullanılan araçların makul olup olmadıklarının tespitinde ise veri işleme sırasında kullanılan teknoloji ve mevcut teknolojik gelişmeler de göz önüne alınarak kimliğin belirlenebilmesindeki zaman ve işlem maliyeti gibi tüm objektif kriterlerin dikkate alınması gerekmektedir. Dolayısıyla GDPR kapsamında veri koruma ilkelerinin anonim veriler bakımından uygulanamayacağı ifade edilmektedir. Zira anonim veri, belirli veya belirlenebilir bir gerçek kişiyle ilgili olmayan yahut verinin konusu artık belirlenemeyecek hale getirilen dolayısıyla da kişisel veri olmayan verileri

[21] Temelde hem anonimleştirme hem de bulanıklaştırma bir kişinin kimliğinin artık izi sürülemez hale getirilmesini ifade etmektedir. Bununla birlikte anonimleştirme terimi bir kişinin kimliğinin bilinmediği veya bu kimliğin kasıtlı olarak gizlendiği durumu ifade ederken bulanıklaştırma belirli bir algoritmayla kişiyi belirleyici verilerin şifrelenmiş verilerle değiştirildiği teknik bir yöntemi ifade etmektedir. Algoritma bir kişi için farklı kaynaklardan birden fazla bilgiyi biraraya getirerek daima aynı pseudonym'i hesaplayabilmektedir. Bu niteliği ise söz konusu kavramı anonimleştirmeden ayırmaktadır. Zira anonimleştirme çözümünde farklı kaynaklardan elde edilen verilerin birleştirilerek kişiyle ilişkilendirilmesi mümkün değildir. (kaynak: https://www.pseudonimiseer.nl/smart_faq/what-is-the-difference-between-anonymization-and-pseudonymization/?lang=en, (Erişim Tarihi: 04.12.2017).

ifade etmektedir. GDPR ise, istatistikî veya bilimsel araştırma amacıyla yapılan işlemeler de dâhil, anonim verilerin işlenmesiyle ilgilenmemektedir.

28 no'lu resitalde bulanıklaştırmanın kişisel verilere uygulanmasının, verinin ilişkili bulunduğu gerçek kişilere yönelik riskleri azaltabileceği ve veri kontrolörleriyle veri işleyenlerin veri koruma yükümlülüklerini yerine getirmelerine yardımcı olabileceği ifade edilmektedir. Bulanıklaştırma teriminin Tüzük'e açıkça girmesi ise diğer önleyici tedbirlerin ve yükümlülüklerin ortadan kalkması anlamına gelmemektedir.

29 no'lu resitalde kişisel verilerin işlenmesi sırasında bulanıklaştırma yapılmasının teşviki amacıyla, söz konusu işlemin gerektirdiği bir dizi önlemin veri kontrolörünce alınması gerekmektedir. Bu kapsamda bilhassa genel veri analizi yapılırken, veri kontrolörünce GDPR hükümlerine uygun işlemenin gerçekleşmesine yönelik teknik ve idari önlemlerin alınması ve verinin belirli veya belirlenebilir birine atfını mümkün kılan ilave verilerin ayrı bir biçimde tutulması şartıyla bulanıklaştırma yapması desteklenmektedir. Ayrıca kişisel verileri işleyen kontrolör söz konusu hususta bünyesinde bulunan diğer yetkilileri de açıkça göstermelidir.

GDPR'nin veri işlemenin hukuka uygun sayıldığı halleri düzenleyen 6. maddesinin 4. fıkrasında yer alan "veri kontrolörünün yapmış olduğu veri işlemenin, kişisel verilerin başlangıçta toplandığı amaçla uyumlu olup olmadığını tespit etmek için belirli hususları da dikkate alacağı" ifade edilerek (e) fıkrasında şifreleme veya bulanıklaştırmayı da içerebilecek uygun önlemlerin varlığının arandığı görülmektedir. Bu çerçevede, bulanıklaştırma teknik çözümüne AB kişisel veri hukuku bağlamında elverişli koruma araçları arasında yer verildiği görülmektedir. Bununla birlikte bilhassa veri işleme ve analizi konusundaki teknolojik gelişmeler dikkate alındığında (büyük veri uygulamaları, nesnelerin interneti, bulut bilişim vb.) kişisel verilerin tamamıyla kişiyi belirlenebilir kılma özelliğinden sıyrılmasının (6698 sayılı Kanun bağlamında anonimleştirilebilmesinin) giderek zorlaştığı hatta imkânsız hale geldiği değerlendirilmektedir. Giderek gelişen ve değişen söz konusu teknolojilerin izlemekte olduğu mevcut eğilim her türlü veri ile kişi arasındaki bağın kurulmasını hızla kolaylaştırmaktadır. TBMM Komisyon Raporlarında da yer alan söz konusu durum karşısında kişisel veri koruma kurallarının uygulanması konusundaki tekniğe ilişkin sorunların uzun bir süre güncelliğini koruyacağı değerlendirilmektedir.

3.1.3. 6698 sayılı Kanun'daki Temel İlkeler

Kişisel verilerin korunmasına ilişkin düzenlemeler yalnızca bireylerin kişisel çıkarlarının korunmasıyla ilişkili olmayıp başta insan onuru, kişiliğin serbestçe geliştirilmesi hakkı ve özel yaşamın korunması gibi temel hak ve özgürlüklerin başında olduğu çok geniş

bir alana hizmet etmektedir.[22] Bu kadar önemli bir hukuki çerçeve sunmaları bakımından söz konusu alana ilişkin bir dizi ortak temel ilkenin kabul edildiği görülmektedir. Kişisel verilerin işlenmesi hususunda bu ilkelere uygun hareket edilmemesi halinde kişisel verilerin iyi niyet kurallarına ve hukuka uygun olarak işlenmediği kabul edilmektedir.

Türk hukuku bakımından kişisel verilerin işlenmesi ile ilgili temel ilkeler 6698 sayılı Kanunu'nun 4. maddesinde yer almaktadır. Maddenin birinci fıkrasında kişisel verilerin ancak Kanun'da ve diğer kanunlarda öngörülen usul ve esaslar çerçevesinde işlenebileceği belirtildikten sonra ikinci fıkrada kişisel verilerin işlenmesiyle ilgili temel ilkeler sayılmıştır:

- Hukuka ve dürüstlük kurallarına uygun olma: Kişisel verilerin korunması hukukunun temel ilkesi olarak değerlendirilen, diğer ilkeleri de kapsayan ve onlara kaynaklık ettiği ifade edilen[23] hukuka ve dürüstlük kurallarına uygun olma ilkesiyle, kişisel verilerin işlenmesinde kanunlara ve diğer hukuki düzenlemelere uygun hareket edilmesi gerektiği ifade edilmektedir.
- Doğru ve gerektiğinde güncel olma: Veri sorumlularınca işlenen kişisel verilerin doğru olması, gerek ilgili kişi gerekse veri işleyen bakımından oldukça önemli olup verilerin doğruluğu hususunda veri sorumlusuna bir sorumluluk yüklenmektedir. Ayrıca verilerin güncelliğinin sağlanması bakımından veri sahibi ile birlikte hareket etmesi beklenmektedir.
- Belirli, açık ve meşru amaçlar için işlenme: Kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi ilkesiyle, veri sorumlusunun kişisel verileri işleme amacını açık ve kesin olarak belirlemesi ve söz konusu amacın meşru olması amaçlanmaktadır. Amacın meşru olması, veri sorumlusunun işlediği verilerin yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma: Veri sorumlularının kişisel verileri toplamadan önce amaçlarıyla bağlantılı olarak verilerin mutlaka kullanıp kullanmaması gerektiğini araştırması, söz konusu kişisel verilerden amacına ulaşmak için yeterli miktarını toplaması ve işlemesi, gereğinden fazla veri toplamaması ve işlememesi gerektiği kuralını ifade etmektedir. Bu çerçevede, belirlenen amacı gerçekleştirmeye elverişli olmayan kişisel verilerin işlenmemesi gerektiği ifade edilmektedir. Ayrıca kişisel verilerin sonradan ortaya çıkması muhtemel ihtiyaçların karşılanması amacıyla işlenebilmesi için, işlemeye ilk kez başlanıyormuş gibi, 5. maddede yer alan işlenme şartlarından birinin gerçekleşmesi gerekmektedir.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme: Kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiğini ifade eden ilkedir.

[22] KÜZECİ, age, sh. 75.
[23] KÜZECİ, age, sh. 212.

Tablo 1: Kişisel Verileri Koruma İlkeleri Bakımından 6698 sayılı Kanun ile GDPR Karşılaştırması

	6698 sayılı Kişisel Verilerin Korunması Kanunu'nda Yer Alan Temel İlkeler		GDPR'de Yer Alan Temel İlkeler
1-	Hukuka ve dürüstlük kurallarına uygun olma	**1-**	Hukuka, dürüstlük kurallarına uygun ve veri öznesine karşı şeffaf işleme
2-	Doğru ve gerektiğinde güncel olma	**2-**	Doğru, gerekli hallerde işleme ve güncel olma
3-	Belirli, açık ve meşru amaçlar için işlenme	**3-**	Kişisel verilerin belirli, açık ve meşru amaçlarla işlenmesi
4-	İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma	**4-**	Veri işleme için gerekli olduğu kadar, ilgili ve ölçülü biçimde işleme
5-	İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme	**5-**	Kişisel verinin işleme amacı için gerekli olandan daha uzun süre tutulmaması
		6-	Veri kontrolörünün sayılan tüm temel prensiplerden sorumlu süje olması (hesap verebilirlik prensibi)

Tablo-1'de görüldüğü üzere temel özellikleri itibarıyla örtüşen gerek 6698 sayılı Kanun'da yer alan temel ilkelerin gerekse GDPR kapsamında yer alan ilkelerin kişisel verilerin işlenmesiyle ilgili teknolojik gelişmelere uyumlu olacak esneklikte kaleme alındığı değerlendirilmektedir. GDPR kapsamında söz konusu ilkelerin uygulanmasından sorumlu olan süje açıkça belirlenerek veri kontrolörünün hesap verebilirliği artırılmıştır. GDPR'nin temel yaklaşımında yer alan artırılmış kişisel veri koruması eğilimine paralel olarak ilkelerin uygulanmasından sorumlu olan veri kontrolörü doğrudan temel ilkeler başlıklı 5. maddede düzenlenmiştir. 6698 sayılı Kanun'da ise doğrudan genel ilkeler başlıklı 4. maddede yer almamakla birlikte veri sorumlusunun yükümlülüklerine ilişkin 12. maddenin lafzından söz konusu alanda veri sorumlusunun yükümlü olduğu anlaşılmaktadır.

3.1.4. 6698 sayılı Kanun'un GDPR'nin Getirdiği Yenilikler Bağlamında Değerlendirilmesi

Yeni AB Veri Koruma Tüzüğü ile AB üyesi ülkeler arasında veri koruma hukuku bakımından üst seviyede bir uyumun sağlandığı ve Birlik üyelerinin iç hukuk düzenlemelerinden kaynaklanan farklılıkların giderildiği görülmektedir. Söz konusu düzenleme sayesinde Birlik ülkeleri bakımından sadeleştirilmiş, sorunsuz ve verimli bir AB sayısal pazarı hedefi bağlamında küresel rekabet avantajı sağlanacağı değerlendirilmektedir. Bu kapsamda ülkemiz mevzuatı bakımından da, bilhassa Veri Koruma Kurulu'nca ortaya konulacak ikincil düzenlemeler bağlamında söz konusu Tüzük'e uyumlu bir genel çerçevenin oluşturulması önem arz etmektedir. Bu kapsamda, bu bölümde GDPR'nin getirdiği temel değişiklikler ülkemiz mevzuatı bakımından değerlendirilmiştir.

Veri İşleyen Tarafların Sorumluluğu

GDPR ile getirilen düzenlemeler kapsamında, veri kontrolörü olmamakla birlikte bu verileri işleyen herhangi bir şirket ya da birey de (bulut hizmet sağlayıcıları gibi üçüncü taraflar da dâhil olmak üzere) verinin hukuka uygun işlenmesinden sorumlu kabul edilmektedir. Bu çerçevede, GDPR kapsamında veri işleme sayılan ve kişisel veriye ilişkin gerçekleştirilen her türlü faaliyetin tüm faillerinin söz konusu işlemeden kaynaklı bütün ihlal ve hukuka aykırılıklardan sorumlu olduğu görülmektedir. Bu hükmün uygulanmasının yansımaları oldukça geniş olacağından hem veri sorumluları hem de veri sorumlusunun talebiyle veriyi işleyen üçüncü kişiler bakımından hukuki sorumluluk ortaya çıkmaktadır. Bu kapsamda GDPR hükümlerinin, sunucuları AB dışında yerleşik bulunan ve işleme faaliyetlerini Birlik ülkeleri dışından sürdüren bulut hizmet sağlayıcıları bakımından da bağlayıcı olduğu görülmektedir. GDPR ile getirilen yüksek para cezaları bu işleyiciler bakımından da bağlayıcıdır.

Yukarıda ifade edildiği üzere, GDPR veri koruma hukukundan doğan sorumluluk bağlamında veri kontrolörü ve veri işleyen ayrımını ortadan kaldırarak kişisel veri ihlallerine ilişkin durumlarda hem veri kontrolörünün hem de veri işleyicisinin sorumlu olduğunu hüküm altına almaktadır. Ancak 6698 sayılı Kanun'un 18. maddesinin ikinci fıkrasında veri sorumlusu ve veri işleyen açısından farklı bir sorumluluk düzeyi belirlenerek idari cezaların uygulaması bakımından yalnızca veri sorumlularına yaptırım uygulamaktadır. Yine veri sorumluları siciline kaydın yalnız veri sorumluları bakımından gerekli olduğu görülmektedir. Veri işleyenlerin sorumlulukları noktasında benimsenen bu yaklaşım GDPR'de benimsenen geniş sorumluluk alanı yaklaşımıyla farklılık arz etmektedir.

Unutulma Hakkı

GDPR ile getirilen diğer bir önemli düzenleme "*unutulma hakkı"dır*. Genel olarak, bireylerin kendilerine ait kişisel verilerini kontrol etme ve mümkün olduğunda silme hakkı olarak ifade edilen unutulma hakkı kavramı GDPR ile ilk kez hukuki bir düzenleme çerçevesine alınmıştır. Bu kapsamda, GDPR'nin 17. maddesinde ifade edildiği üzere veri sahibi, kendisine ait kişisel verilerinin mümkün olan en kısa sürede silinmesini veri kontrolöründen talep edebilme hakkına sahiptir. Bu çerçevede veri kontrolörü söz konusu kişisel verileri gecikmeksizin silmekle yükümlüdür. Hangi durumlarda söz konusu verilerin gecikmeksizin silinmesi gerektiği de 17. maddenin birinci fıkrasında sayılmaktadır. Kişisel verilerin işlenmesinin söz konusu verinin toplanma amaçları veya işleme faaliyeti kapsamında artık gerekli olmaması, veri sahibinin daha önce vermiş olduğu rızayı geri alması ve artık işleme faaliyeti için hukuki bir yetkinin mevcut bulunmaması, kişisel verilerin tamamen hukuka aykırı olarak işlenmesi veya veri kontrolörünün tabi olduğu yasalar bakımından (AB veya üye devlet yasaları) kişisel verileri silmekle yükümlü olunması gibi durumlarda söz konusu hakkın kullanılabileceği ifade edilmektedir. Bununla birlikte aynı maddenin üçüncü fıkrasında söz konusu hakka ilişkin beş istisnaya yer verildiği görülmektedir. Bu istisnalar kapsamında; bilgi ve ifade hürriyeti hakkının kullanılması, veri kontrolörünün tabi olduğu yasalar bakımından işleme faaliyetiyle yükümlü olması veya kamu yararının gerektirdiği haller yahut veri kontrolörünce yürütülen resmi bir görevin gerektirmesi, GDPR'nin 9. maddesinde yer alan toplum sağlığının korunmasına ilişkin hükümlerin uygulanması, arşiv

amaçlı araştırmalarda kamu yararına, bilimsel ve tarihi araştırmalarda kullanılması ile yasal iddiaların oluşturulması, uygulanması ve savunulması hususları yer almaktadır.

GDPR kapsamında kabul edilen unutulma hakkına benzer bir hak münferit olarak henüz 6698 sayılı Kanunda yer almamaktadır. Bununla birlikte GDPR'de yer alan unutulma hakkına benzer bir kavramın ilk kez Yargıtay 4. Hukuk Dairesi'nin 03.07.2013 tarih ve 2013/6256 esaslı kararında tartışıldığı görülmektedir. Karara konu dava cinsel taciz mağduru davacıya ilişkin olup Yargıtay incelemesine konu olmuş, davalılar tarafından davacının isminin kodlanmaksızın bir kitapta yayımlanması dolayısıyla kişilik haklarının ihlal edildiği iddiasıyla açılmıştır. İlk derece mahkemesi ismi kodlanmaksızın eserin yayımlanmasından dolayı davacının bizzat mağdur olması nedeniyle içinde bulunduğu hassasiyeti temel alarak kitapta davacının isminin kodlanmamasının kişilik haklarına halel getirdiğini ifade etmiş, bu kapsamda manevi tazminat talebinin kısmen kabulüne karar vermiştir. Söz konusu Yargıtay kararının ayrışık oyunda "İlerleyen insan hakları trendinde kişilerin arşiv silme talebi ve unutulma hakları gibi modern haklarla donatıldığı da düşünüldüğünde davacının kişilik haklarının ihlal edildiği yine sabittir." açıklaması bulunmaktadır.[24]

Unutulma hakkı kavramının ilk kez açıkça yer aldığı yargı kararı ise Anayasa Mahkemesi (AYM) tarafından 2016 yılında verilmiştir. AYM'nin 03/03/2016 tarih ve B.2013/5653 no'lu kararı kapsamında, hakkındaki haberin internet ortamından silinmesi amacıyla başvuran kişi haklı bulunmuştur. Karar kapsamında *"Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devlet, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfi olarak müdahale etmemek ve üçüncü kişilerin saldırılarını önlemekle yükümlüdür."* ifadesine yer verilmiştir. AYM, internet ortamının sağladığı kolaylıklar gözetildiğinde başvuranın şeref ve itibarının korunması için söz konusu habere erişimin engellenmesi gerektiğine karar vermiştir.[25] AYM'nin söz konusu kararı ülkemiz hukuku bakımından unutulma hakkının uygulaması bağlamında emsal niteliğindedir.

Sonuç olarak, ülkemizde yüksek yargı kararıyla da kabul edilmiş bulunan unutulma hakkı henüz hukuki düzenlemelerde yer almamaktadır. Unutulma hakkının, gerek insan haklarıyla olan yoğun ilişkisi gerekse kişisel verilerin korunması alanında ülkemizce model kabul edilen AB düzenlemeleriyle hüküm altına alınması dolayısıyla ülkemiz mevzuatında da açıkça yer almasının faydalı olacağı değerlendirilmektedir.

Yaptırımlar

GDPR ile getirilen en önemli düzenlemelerin başında veri ihlalleri karşısında öngörülen yaptırımlara ilişkin hükümler gelmektedir. Zira veri koruma kurallarına ilişkin ihlaller karşısında 95/46 sayılı Direktif'e göre çok daha ağır tazmin yaptırımları (200 milyon

[24] AKGÜL, Aydın; Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı", http://tbbdergisi.barobirlik.org.tr/m2015-116-1440, Erişim Tarihi: 27/02/2017.

[25] AYM'nin Unutulma Hakkına ilişkin N.B.B Kararı'nın tam metni için: http://www.anayasa.gov.tr/icsayfalar/basin/kararlarailiskinbasinduyurulari/bireyselbasvuru/detay/pdf/2013-5653.pdf, Erişim Tarihi: 27/02/2017.

Avro veya hizmet sağlayıcının küresel gelirinin yüzde dördü gibi önemli miktarlar) öngörülmektedir. 6698 sayılı Kanun'da ise söz konusu idari para cezalarının daha düşük miktarlarla sınırlı olduğu (en düşük 5 bin Türk lirasından en yüksek 1 milyon Türk lirasına kadar) görülmektedir.

Veri Taşınabilirliği ve Etki Değerlendirmesi

GDPR'nin 20. maddesiyle ile ilk kez tanımlanan "*veri taşınabilirliği hakkı"* kapsamında veri sahibi, kişisel verisini tutmaya yetkili bir veri kontrolöründen diğerine taşıyabilme yetkisine sahiptir. Ayrıca 37. madde kapsamında hassas verilerin işlenmesi bakımından "*zorunlu veri koruma görevlisi"*nin belirlenmesi ve 35. madde kapsamında riskli veri işleme faaliyetleri bakımından *"zorunlu veri koruma etki değerlendirmesi"* öngörülmektedir. 6698 sayılı Kanun'da ise bu kapsamda ayrıca tanımlanmış hükümler bulunmamaktadır. Bu çerçevede, kişisel verilerin güçlü korunması ve veri işleyenlerin sorumluluklarının artırılması eğilimi doğrultusunda bu yönde hükümlerin kanunla tanımlanmasının faydalı olacağı değerlendirilmektedir.

Veri Koruma tedbirleri

GDPR kapsamında kişisel verilerin işlenmesi bağlamında gerçek kişilerin hak ve özgürlüklerinin korunması amacıyla gerekli teknik ve organizasyonel önlemlerin alınmasının gerektiği ifade edilerek "*Başlangıçtan itibaren (data protection by default)" ve "tasarımdan itibaren veri koruması (data protection by design) yaklaşımı"* kavramlarına yer verilmektedir. Bilhassa teknolojik gelişmeler dikkate alındığında bu yaklaşımın 6698 sayılı Kanun'da doğrudan yer almasa dahi özellikle Kişisel Verileri Koruma Kurulunca hayata geçirilecek ikincil düzenlemelerde dikkate alınması önem arz etmektedir.

4. SONUÇ

Veri işleme teknolojilerindeki hızlı gelişim ve internetin toplumsal hayatın ayrılmaz bir parçası haline gelmesi karşısında bir yandan kişisel verilerin korunması hukukunun önemi artmakta diğer yandan veriden değer yaratan ekonomik sistemin faydalarının dikkate alınması gerekmektedir. Bu çerçevede, ülkemizde de temel haklar arasında yer alan kişisel verilerin koruması hakkıyla bireylerin korunmasının yanı sıra teknolojik gelişmelerden, bilgi ekonomisinden ve yenilikçilikten faydalanılması amacı doğrultusunda 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilmiştir. Söz konusu Kanun'un hazırlanması sürecinde AB hukuki düzenlemelerinden faydalanıldığı görülmektedir.

Türkiye'de kişisel verilerin korunması hukukunda temel düzenleme olarak kabul edilen 6698 sayılı Kanun amaç, kapsam ve hükümleriyle birlikte değerlendirildiğinde 95/46 sayılı Direktif ile büyük ölçüde uyumluluk arz etmektedir. Bununla birlikte, 6698 sayılı Kanunun kabulünden kısa bir süre sonra AB Veri Koruma Reformu kapsamında hazırlanan GDPR Avrupa Parlamentosu tarafından onaylanarak kabul edilmiştir. Söz konusu yeni Tüzük'le 95/46 sayılı Direktif'te yer alan hükümlerin modernize edilmesi ve güncellenmesi amaçlanmıştır. Bu çerçevede, 6698 sayılı Kanun'un kurgulanmasında GDPR hükümleri değil, o dönemde yürürlükte bulunan 95/46 sayılı Direktif hükümlerinin esas alındığı görülmektedir.

GDPR, 95/46 no'lu Direktif'le kıyaslandığında, özellikle sorumluluklar, yaptırımlar, kişi hakları ve veri koruma tedbirleri açısından daha sıkı ve kapsamlı düzenlemeler getirmiştir. Başta veri işleyen tarafların artırılmış sorumluluk rejimi, unutulma hakkının kanunla tanımlanması, idari para cezalarına ilişkin yaptırımların artırılması yoluyla caydırıcılığın güçlendirilmesi olmak üzere veri taşınabilirliği ve etki değerlendirmesi ile tasarımdan itibaren güvenlik gibi yenilikçi yaklaşımların 6698 sayılı Kanun'a ve uygulamaya yansıtılmasının faydalı olacağı değerlendirilmektedir. Bu hukuki yaklaşımların bir kısmıyla ilgili uyumlaştırmalar yasal düzenleme gerektirmekle birlikte bir kısmı içinse Kişisel Verileri Koruma Kurumunun yapacağı ikincil düzenlemeler ve uygulama pratikleri yoluyla uyum sağlanabileceği değerlendirilmektedir. Bu çerçevede, 6698 sayılı Kanun tarafından ikincil düzenlemelere bırakılan hususların ele alınmasında Kişisel Verilerin Korunması Kurumu tarafından GDPR hükümlerinin öncelikle dikkate alınmasının faydalı olacağı değerlendirilmektedir.

www.kalkinma.gov.tr

T.C.
KALKINMA BAKANLIĞI
YÖNETİM HİZMETLERİ GENEL MÜDÜRLÜĞÜ
BİLGİ VE BELGE YÖNETİMİ DAİRESİ BAŞKANLIĞI
Haziran 2017

Necatibey Cad. No: 110/A 06100 Yücetepe - ANKARA
Tel: +90 (312) 294 50 00 • Faks: +90 (312) 294 69 77

ISBN NO: 978-605-9041-85-0