(AB) 2016/679 SAYILI AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ DOĞRULTUSUNDA KİŞİSEL VERİLERİN KORUNMASI

Onur Doğan YÖRÜK

Haziran 2019

İZMİR EKONOMİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

(AB) 2016/679 SAYILI AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ DOĞRULTUSUNDA KİŞİSEL VERİLERİN KORUNMASI

Onur Doğan YÖRÜK

Haziran 2019

Lisansüstü Eğitim Enstitüsü Onayı

Doç. Dr. Efe BİRESSELİOĞLU
(Lisansüstü Eğitim Enstitüsü Müdürü)

Bu tezin Yüksek Lisans derecesi için gerekli şartları sağladığını onaylarım.

Prof. Dr. Huriye KUBİLAY
(Özel Hukuk Anabilim Dalı Başkanı)

Tez tarafımızdan okunmuş, Yüksek Lisans derecesi için kapsam ve kalite yönünden uygun olduğu kabul edilmiştir.

Dr. Öğr. Üyesi Özge ÖZSOY
(Tez Danışmanı)

Yüksek Lisans Sınavı Jüri Üyeleri

Doç. Dr. Burçak YILDIZ

Dr. Öğr. Üyesi Özge ÖZSOY

Doç. Dr. Zeynep ŞİŞLİ

ÖZET

(AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması

YÖRÜK Onur Doğan

İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü Özel Hukuk Tezli Yüksek Lisans Programı

Danışman: Dr. Özge ÖZSOY

Haziran 2019

Kişisel verilerin arz ettiği önem, teknolojik gelişmelere de paralel olarak, gün geçtikçe artmaktadır. Kişisel verilerin işlenmesinin kolaylaşması ve bunlara duyulan ihtiyacın artması, bireylerin bu işleme faaliyetleri karşısında korunmasını ve kişisel verilerinin akıbeti üzerinde söz sahibi olma haklarının güvence altına alınmasını gerektirmiştir. Bu çerçevede, 1970'li yıllardan itibaren Avrupa, ulusal ve uluslararası düzeyde kişisel verilerin korunması hukukunun bağımsız bir hukuk dalı olarak gelişimine sahne olmuş, 1995 yılında yürürlüğe giren 95/46/AT sayılı Direktif ile, AB düzeyinde bir kişisel verilerin korunması çerçeve hukuku oluşturulmuştur. Direktif zamanla, özellikle internetin yaygınlaşması sonucunda, işleme yöntemlerinin değişmesi ve kişisel verilere duyulan ihtiyacın artması karşısında yetersiz kalmaya başlamış, bunun üzerine AB kişisel verilerin korunması hukukunda, uzun bir sürecin ardından (AB) 2016/679 sayılı AB Genel Veri Koruma Tüzüğü'nün temelini oluşturduğu bir reform gerçekleştirilmiştir. Tüzük, tarihsel gelişim süreci içerisinde kişisel verilerin korunması hukukunun bir parçası haline gelmiş ilkelere yer vermekle birlikte, unutulma hakkı başta olmak üzere halen hukuk çevrelerinde yoğun tartışmalara konu olan ve gelecekte de olması beklenen önemli yenilikler de getirmektedir. Türkiye'nin oluşturmaya yeni başladığı kişisel verilerin korunması kültürü bakımından da Tüzük'ün yarattığı etkinin iyi değerlendirilmesi yararlı olacaktır. Çalışmanın konusunu, Tüzük'te düzenlendiği haliyle AB kişisel verilerin korunması hukuku oluşturmaktadır. Bu kapsamda öncelikle, anılan hukuk dalının

konusu ve temel kavramı olan kişisel veri ve ilişkili kavramlar tanımlanmış, ardından kişisel verilerin korunması hukukunun ulusal ve uluslararası düzeyde gelişimi ve kaynakları incelenmiş, son olarak, AB veri koruma reformu ve Tüzük ile oluşturulan kişisel verilerin korunması çerçeve hukuku, ABAD içtihatları ışığında ele alınmaya çalışılmıştır.

Anahtar Kelimeler: Kişisel veri, kişisel verilerin korunması, kişisel verilerin işlenmesi, (AB) 2016/679 sayılı AB Genel Veri Koruma Tüzüğü, unutulma hakkı.

ABSTRACT

Data Protection Under The Regulation (EU) 2016/679 (The General Data Protection Regulation - GDPR)

YÖRÜK Onur Doğan

Izmir University of Economics Institute of Post-Graduate Education LLM Programme in Private Law (with Thesis)

Supervisor: Dr. Özge ÖZSOY

June 2019

Personal data, paralleling technological developments, becomes more important everyday. As data processing became easier and the demand for it grew, protecting the individuals against processing of their data and their right to determine the fate thereof became necessary. Within this context, Europe witnessed the development of data protection as an independent field of law, on a national and international level, starting in 1970s. In 1995, an EU-wide data protection legal framework was formed with Directive 95/46/EC. Over time, Directive became insufficient for meeting new requirements stemming from the evolving processing methods and increasing demand for data, particularly because of Internet becoming common; leading to a long reform process, for which the EU General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) provides a foundation. GDPR retains the main principles that became a part of data protection law during its development, and introduces new concepts, such as the right to be forgotten, that have been extensively discussed among legal circles, and the discussions are expected to continue. Analysing GDPR's impact well would be beneficial for Turkey, who has recently developed its own data protection culture. This study explores the EU data protection framework laid out by GDPR. Within this scope, it defines personal data, the centric term of data protection law, and related terms before reviewing the national and international development and resources of data

protection law. Finally, it endeavours to explore the data protection framework established by GDPR, in light of European Union Court of Justice decisions.

Keywords: Personal data, personal data protection, processing of personal data, EU General Data Protection Regulation (Regulation (EU) 2016/679), the right to be forgotten.

TEŞEKKÜR

Bilim dünyasına ilk adımım olmasını umduğum tezimin yazım aşaması boyunca yardımlarını ve desteğini hiçbir zaman esirgemeyen, yorumları ve yapıcı eleştirileriyle yoluma ışık tutan danışmanım Sayın Dr. Özge ÖZSOY'a, gerek lisans gerek lisansüstü eğitimim boyunca engin deneyimlerinden yararlanma fırsatı bulduğum, akademik ve mesleki gelişimimde katkısı bulunan tüm hocalarıma, avukatlık stajı ile yüksek lisansı bir arada yürütebilmem için anlayışla her türlü kolaylığı sağlayan, bir anlamda bu tezin yazılabilmesini mümkün kılan Av. Feyza AKGÜN'e, manevi destekleri ile bu zorlu süreci kolaylaştıran tüm arkadaşlarıma ve nihayet, hayatımın her döneminde yanımda olan, bundan sonra da yanımda olacaklarından hiçbir şüphe duymadığım aileme teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR

AAET: Avrupa Atom Enerjisi Topluluğu (Euratom)

AB: Avrupa Birliği

ABA: Avrupa Birliği Antlaşması (Maastricht Antlaşması)

ABAD: Avrupa Birliği Adalet Divanı

ABİA: Avrupa Birliği'nin İşleyişi Hakkında Antlaşma

AEPD: Agencia Española de Protección de Datos (İspanya Veri koruma Kurumu)

AET: Avrupa Ekonomik Topluluğu

AİHM: Avrupa İnsan Hakları Mahkemesi

AİHS: İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi (Avrupa İnsan Hakları Sözleşmesi)

AK: Avrupa Konseyi

AKÇT: Avrupa Kömür ve Çelik Topluluğu

AT: Avrupa Topluluğu

AY: Anayasa

APEC: Asia-Pacific Economic Cooperation (Asya-Pasifik Ekonomik İşbirliği)

BDSG: Bundesdatenschutzgesetz (Almanya Federal Veri Koruma Kanunu)

BM: Birleşmiş Milletler

BVerfG: Bundesverfassungsgericht (Alman Federal Anayasa Mahkemesi)

C: Cilt

DMCA: Digital Millennium Copyright Act (Dijital Milenyum Telif Hakkı Yasası)

DPD: 95/46/AT sayılı ve 24 Ekim 1995 tarihli Bireylerin Kişisel Verilerin İşlenmesine Karşı Korunması ve Bu Tür Verilerin Serbest Dolaşımına Dair Avrupa Parlamentosu ve Konsey Direktifi (AB Veri Koruma Direktifi, Direktif)

dpn: Dipnot

E: Esas

ed: Editör

eds: Editörler

ETS 108: Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Avrupa Konseyi Sözleşmesi)

GDPR: (AB) 2016/679 sayılı ve 27 Nisan 2016 tarihli Gerçek Kişilerin Kişisel Verilerinin İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin 95/46/AT sayılı AB Direktifi'ni Yürürlükten Kaldıran Avrupa Parlamentosu ve Konsey Tüzüğü (AB Genel Veri Koruma Tüzüğü, Tüzük)

İHEB: İnsan Hakları Evrensel Bildirgesi

K: Karar

KVKK: Kişisel Verilerin Korunması Kanunu

m: Madde

OECD: Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)

OJ: Official Journal of the European Union (Avrupa Birliği Resmi Gazetesi)

par: Paragraf

RG: Resmi Gazete

RİG: Reform İzleme Grubu

S: Sayı

s: Sayfa

T: Tarih

TBMM: Türkiye Büyük Millet Meclisi

TMK: Türk Medeni Kanunu

vd: ve devamı

yuk: Yukarıda

BİRİNCİ BÖLÜM
GİRİŞ

Kişisel verilerin korunması, kişisel verilerin toplanmasındaki giderek hız kazanan artışa rağmen, halen önemi yeterince anlaşılamamış bir kavram olarak karşımıza çıkmaktadır. (AB) 2016/679 sayılı ve 27 Nisan 2016 tarihli Gerçek Kişilerin Kişisel Verilerinin İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 95/46/AT sayılı AB Veri Koruma Direktifi'ni Yürürlükten Kaldıran Avrupa Parlamentosu ve Konsey Tüzüğü'nün kabul edilmesi ve yürürlüğe girmesi konuyu yeniden gündeme taşımış, gerek Avrupa'da gerekse Türkiye'de konuya ilişkin çalışmalar hız kazanmış, tartışmalar yoğunlaşmıştır.

Kişisel veriler günlük hayatta sanıldığından çok daha yaygın bir şekilde, çoğu zaman farkında bile olmaksızın saklanması ve işlenmesi amacıyla veri öznelerince[1] paylaşılmaktadır. Sadece internette gezinmek bile girilen internet sitelerinin çerezler aracılığıyla veri öznesinin internetteki faaliyetlerini ve tercihlerini izleyerek kişinin internet kullanım alışkanlıklarına dair bilgi edinebilmesi için yeterli olmaktadır. Kişisel veriler sadece dijital olarak değil, fiziksel yollarla da toplanıp saklanmaktadır; ancak, teknolojik gelişmeler, bu işin yapılabilirliği yönünden bir değişim yaratmıştır.[2] Bilişim teknolojileri, yapay zeka, dijital iletişim ağları ve veri işleme ve analiz yöntemlerindeki ilerlemeler, toplanabilen ve işlenebilen verilerin miktarını, çeşitlerini ve veri toplama hızını önemli ölçüde artırmıştır.[3] Böyle bir ortamda, Devletin yanı sıra şirketler, bankalar, dernekler gibi akla gelebilecek her türlü oluşum, kişilerin adı, adresi ve iletişim bilgileri, tüketim alışkanlıkları, malvarlıkları, kişisel zevkleri gibi sayısız konuda kolayca bilgi sahibi olabilmektedir.

---

[1] AB Genel Veri Koruma Tüzüğü'nün "kişisel veri" kavramını tanımladığı 4 üncü maddesinin birinci fıkrasının orijinal metni, "verinin ilişkin olduğu belirli veya belirlenebilir gerçek kişi"yi veri öznesi ("data subject") olarak ifade etmiştir. Veri öznesi ve kişisel verilerin korunmasına ilişkin başlıca diğer kavramlar çalışmanın birinci bölümünde incelenmiştir.

[2] Elif **Küzeci** (2010), Kişisel Verilerin Korunması, 2. Baskı, Turhan, Ankara, s. 2.

[3] Kathryn C. **Montgomery** / Jeff **Chester** / Tijana **Milosevic** (2017), "Children's Privacy in the Big Data Era: Research Opportunities", Pediatrics, C. 140, S. Supplement 2, s. 118.

Kişisel verilerin toplanması, saklanması ve en önemlisi dağıtılması her zaman veri öznelerinin rızası dahilinde gerçekleşmemektedir. Hatta aksine daha sık rastlandığı söylenebilir. Bu noktada, bireylerin kişilik hakkı ihlallerine karşı güvence altına alınması, dolayısıyla kişisel verilerin korunmasına yönelik hukuki düzenlemeler yapılması ihtiyacı doğmuştur. Bununla birlikte, kişisel verilerin toplanması, analiz edilmesi ve paylaşılmasından doğan menfaatlerin hukuk düzenince tamamen göz ardı edilmesi de söz konusu olamaz. O halde cevap aranması gereken soru, toplumsal menfaatler uğruna kişisel özgürlüklerden mi vazgeçileceği, yoksa kişilik haklarının korunması idealiyle verilerin işlenmesinden doğan menfaatlerden mi feragat edileceğidir. İşte hukukun görevi de tamamen sona ermesi mümkün olmayan şeffaflık ve gizlilik arasındaki bu çatışmaya bir denge getirmektir. Kişisel verilerin korunmasına ilişkin gerek ulusal gerek uluslararası ölçekteki hukuk kurallarının tespitinde bu amaç gözetilmelidir. Bu anlayış, AB Genel Veri Koruma Tüzüğü'nde de benimsenmiştir.[4]

Teknolojideki gelişmeler, kaçınılmaz olarak Türkiye'de de etkisini göstermiştir. 2016 yılı itibariyle Türkiye nüfusunun yüzde 58'i internet kullanıcısı olup, Türkiye dünyada internetin en fazla kullanıldığı 14'üncü ülke konumundadır.[5] 2000 yılında yaklaşık her 100 kişiden 25'inin cep telefonu hattı bulunmaktayken, 2017 yılında bu oranın yaklaşık 4 kat arttığı görülmekte, her 100 kişiden 96'sının cep telefonu hattı bulunduğu tahmin edilmektedir.[6] Akıllı telefon kullanımı da buna paralel olarak gitgide yaygınlaşmaktadır. 2022 yılında Türkiye'de 61.34 milyon akıllı telefon kullanıcısı olacağı öngörülmektedir ki bu 2015 yılındaki kullanıcı sayısının (28.69 milyon) iki katından fazlasına tekabül eder.[7] 2018 itibariyle Türkiye'de aktif 51 milyon sosyal medya kullanıcısı bulunmaktadır. İstatistikler sosyal medyanın en

---

[4] "…The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality…" Tüzük, Gerekçe 4.

[5] Internet Users by Country (2016) - http://www.internetlivestats.com/internet-users-by-country/ (Erişim tarihi: 2/12/2018)

[6] Mobile cellular subscriptions (per 100 people) - https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2017&locations=TR&start=2000 (Erişim tarihi: 2/12/2018)

[7] Forecast of smartphone user numbers in Turkey from 2015 to 2022 (in million users) - https://www.statista.com/statistics/566218/predicted-number-of-smartphone-users-in-turkey/ (Erişim tarihi: 2/12/2018)

yaygın internet kullanım amacı olduğunu, en sık ziyaret edilen sitelerin ve kullanılan uygulamaların sosyal medyaya yönelik olduğunu göstermektedir.[8] Tüm bu bilgiler ışığında, Türkiye için bir kişisel verilerin korunması kanununa duyulan ihtiyaç açıktır. Bu doğrultuda, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 24 Mart 2016'da kabul edilmiştir. Tüzük, KVKK'nın yürürlük tarihinden tam bir hafta sonra kabul edilmesine karşın KVKK Tasarısı hazırlanırken, Direktif ile uyumun amaçlandığı ve bu düzenlemeden yararlanıldığı görülmektedir.[9] Ancak Tüzük'e yönelik gelişmelerin de hiç dikkate alınmadığı söylenemez.[10] KVKK'nin hazırlanmasında Avrupa ile ilişkilerden doğan gereksinimlerin de etkili olduğu,[11] konuya ilişkin AB düzenlemelerinden yararlanıldığı ve uygulama açısından AB'nin sahip olduğu tecrübe dikkate alındığında, Türk kişisel verilerin korunması hukukunun AB hukukundan bağımsız değerlendirilmesi söz konusu olamaz. Kaldı ki Tüzük'ün bazı hükümleri AB sınırları dışında, AB vatandaşı olmayan kişiler açısından da uygulama alanı bulabilmektedir; şüphesiz ki Türkiye ve Türk vatandaşları da bu kapsamdadır.

Çalışmanın konusu, özellikle 2016/679 sayılı AB Genel Veri Koruma Tüzüğü başta olmak üzere AB müktesebatında ele alındığı şekliyle kişisel verilerin korunması olup çalışma üç bölümden oluşmaktadır. Birinci bölümde, kişisel veri ve çalışma boyunca karşılaşılacak ilişkili diğer kavramlara dair açıklamalar yapılarak, bu kavramlar çeşitli boyutlarıyla ele alınmıştır. İkinci bölümde, Avrupa'da, Türkiye'de ve dünyada kişisel verilerin korunması hukukunun gelişimi incelenmiş, kişisel verilerin korunması hukukunun ulusal ve uluslararası kaynakları üzerinde durulmuştur. Üçüncü bölümde ise, Tüzük'ün kabulüne giden süreçte Avrupa

---

[8] Ayrıntılı istatistikler için bkz. Hootsuite & We are Social, Digital in 2018 in Western Asia, slayt 180 vd. - https://www.slideshare.net/wearesocial/digital-in-2018-in-western-asia-part-1-northwest-86865983 (Erişim tarihi: 2/12/2018)

[9] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 80. Bundan sonra "Tasarı" olarak anılacaktır.

[10] KVKK Tasarısı'na dair Adalet Komisyonu Raporu'nda (Tasarı, s. 66) ve Tasarı'nın 6. maddesine ilişkin muhalefet şerhinde (Tasarı, s. 85) Tüzük anılmıştır.

[11] Türkiye'nin AB'ye uyum ve tam üyelik süreçlerinde kişisel verilerin korunmasına ilişkin çalışmalar hakkında detaylı bilgi için bkz. Dilek **Yüksel Civelek** (2011), Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi), T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı Yayınları, Ankara, s. 126 vd.

Birliği'nde kişisel verilerin korunması ve Tüzük ile oluşturulmuş Avrupa Birliği kişisel verilerin korunması hukuku çerçevesi, yeri geldikçe Direktif'ten farkları da incelenerek ve ABAD içtihatlarıyla desteklenerek değerlendirilmiştir.

İKİNCİ BÖLÜM
KİŞİSEL VERİ KAVRAMI

AB Genel Veri Koruma Tüzüğü ve kişisel verilerin korunmasına ilişkin gerek ulusal gerek uluslararası diğer tüm hukuki düzenlemeler, kişisel verilerin hukuka uygun olarak toplanmasını ve işlenmesini sağlamayı amaçlar. Bu nedenle kişisel verilerin korunması hukuku esaslarının ve normlarının incelemesine geçilmeden önce, kişisel veri ve konuya ilişkin diğer temel kavramlar üzerinde durmak yerinde olacaktır.

I. KİŞİSEL VERİ

I.A. Tanım

AB Genel Veri Koruma Tüzüğü'ndeki tanıma göre kişisel veri, belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgidir (GDPR §4/1). AB Veri Koruma Direktifi de aynı tanıma yer vermişti (DPD §2-a). Ulusal ve uluslararası pek çok düzenleme bu tanımı benimsemiştir.

Türk hukukunda, 7 Nisan 2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesinin (ç) bendinde kişisel veri, Tüzük ve Direktif'te yer alan tanımla paralel olarak kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. 9 Nisan 2014 tarihli Anayasa Mahkemesi kararıyla dayanak Kanun maddesinin iptali sonucu hükümsüz kalan 24 Temmuz 2012 tarih ve 28363 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 3. Maddesinin (h) bendinde de belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler şeklinde benzer bir tanım yapılmıştı.

Kimi hukuk düzenlerinde, farklı ifade tarzları kullanılmış olsa da kişisel veri konusunda anlam itibariyle Tüzük ile örtüşen tanımlara rastlanmaktadır. Örneğin

Hong Kong Kişisel Veri Gizlilik Yönetmeliği, yaşayan bir birey ile doğrudan veya dolaylı olarak ilişkili, ilgili bireyin kimliğinin doğrudan veya dolaylı olarak tespit edilebildiği, erişilebilir ve işlenebilir nitelikte veri şeklinde bir tanım yapmıştır.[12]

I.B. Kişisel Verinin Unsurları

Yukarıdaki tanımdan hareketle, kişisel verinin varlığından söz edebilmek için öncelikle doğal olarak bir verinin bulunması gerekir. Bir verinin kişisel veri olması, o verinin ilişkilendirilebileceği belirli bir gerçek kişinin varlığına ya da varlığının tespit edilebilmesine (o kişinin belirlenebilmesine) bağlıdır. Şu durumda kişisel verinin unsurları veri, gerçek kişi, kişinin belirli ya da belirlenebilir olması ve ilişkin olma olarak sayılabilir.[13]

I.B.1. Veri

Veri, özellikle olgu ve sayılardan oluşan, incelenmek ve değerlendirilmek üzere toplanan, karar vermede yardımcı olmak üzere kullanılan ya da elektronik olarak bilgisayarlarda saklanabilen veya bilgisayarlarca kullanılabilen bilgidir.[14]

Veri koruma hukuku anlamında hangi verilerin kişisel veri kabul edilebileceğine geçmeden önce, verinin benzer anlamlı, birbirinin yerine geçer ("interchangeable") şekilde kullanılabilen enformasyon ve bilgi kavramlarıyla ilişkisi üzerinde durmak gerekir.

---

[12] Stephen Kai-yi **Wong /** Guobin **Zhu** (eds.) (2016), Personal Data (Privacy) Law in Hong Kong - A Practical Guide to Compliance, City University of Hong Kong Press, Hong Kong, s. 9.

[13] Aynı yönde bkz. Hüseyin Murat **Develioğlu** (2017), Avrupa Birliği Genel Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha, İstanbul, s. 30; Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 Haziran 2007, s. 6 vd. Bunların dışında işlenebilirliğin de kişisel veri unsuru olarak düzenlendiği hukuk sistemleri bulunmaktadır ancak işlenebilirlik kişisel veriye özgü bir özellik değildir.

[14] Cambridge Advanced Learner's Dictionary & Thesaurus © Cambridge University Press - https://dictionary.cambridge.org/dictionary/english/ (Erişim tarihi: 5/12/2018)

I.B.1.a)Veri Enformasyon, Bilgi

Veri ("data"), enformasyon ("information") ve bilgi ("knowledge") kavramları arasındaki ilişki tartışmalıdır.[15] Bu kavramlar arasında hiyerarşik bir ilişki bulunduğu, bunların bilgeliğe ("wisdom") giden aşamalar olduğu görüşü ilk olarak Russell Ackoff tarafından ortaya atılmıştır[16] ve sistem bilimlerinde oldukça yaygın olarak kabul görmektedir. Bilgi veya bilgelik piramidi olarak anılan bu model kısaca, "verinin işlenmesi ile enformasyona, enformasyonun anlamlandırılması ile bilgiye, nihayet bilginin yorumlanması ile de bilgeliğe ulaşılır" şeklinde özetlenebilir.[17] Bu özetten hareketle enformasyon, verinin işlenmiş ve anlamlandırılabilir hali, bilgi ise anlam yüklenmiş ve karar almada kullanılabilecek halidir denilebilir. Veri enformasyonun, enformasyon ise bilginin hammaddesidir.[18] Ancak hemen belirtilmelidir ki, bu tanımlar genelgeçer değildir ve çok farklı tanımlara da rastlamak mümkündür.[19]

Bilgi piramidi modelinin, sistem bilimleri ve bilişim alanlarında önemi büyük olmakla birlikte, veri koruma hukukuna uygulanabilirliği pek yoktur. Veri koruma hukukunun kapsamını, verinin buradaki anlamı ile sınırlamak, ulaşılmak istenen amaca ters düşecektir, çünkü bu sınırlama, verinin işlenmesinin ardından hukukun koruma alanından çıkması anlamına gelir. Sadece anlamlı ve kullanılabilir hale getirilmiş (işlenmiş) verinin (enformasyon ve bilginin) hukuken korunmasını kabul etmek de doğru bir yaklaşım olmaz, şayet kişi hakkındaki önemsiz veriler ve

---

[15] **Küzeci**, s. 10.

[16] R. L. **Ackoff** (1999), "From Data to Wisdom", Ackoff's Best, John Wiley & Sons, New York, s. 170-172.

[17] Yöneltilen eleştiriler ve farklı yorumları da dahil olmak üzere model hakkında ayrıntılı bilgi için bkz. Martin **Frické** (2018), "Knowledge pyramid: the DIKW hierarchy", International Society for Knowledge Organization (ISKO) Encyclopedia of Knowledge Organization (IEKO). - http://www.isko.org/cyclo/dikw#3.2 (Erişim tarihi: 8/12/2018)

[18] A. Semih **İşevi** / Burçin **Çelme** (2002), "Bilgi Çağında Yeni Hazine: Entelektüel Sermaye ile Rekabeti Yakalamak", I. ÜNAK Genel Konferansı (ÜNAK2002) 19 Mayıs Üniversitesi Samsun 10-12 Ekim 2002, Araştırma ve Teknoloji Genel Müdür Yardımcılığı, 2002 Ulusal ve Uluslararası Bildiriler. Şişecam, İstanbul, s. 12. - http://eprints.rclis.org/7194/1/bilgidunyasiES.pdf (Erişim tarihi: 15/12/2018)

[19] bkz. **Küzeci**, s. 11 vd., Aydın **Akgül** (2013), Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi (Yayımlanmamış Doktora Tezi), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, s. 6 vd.

yayımlanmış veriler de onun kişisel verilerini oluşturur.[20] Veri o haliyle bir önem arz etmese bile, işlenebilir nitelikte ise, işlenmiş haliyle önem arz edecektir. İşevi ve Çelme'ye göre, kendi başına veri çok yararlı olmamakla birlikte, gereksinim duyan birey için anlamlı hale getirilmiş, verinin bir yeniden sunumu olan, enformasyon ise yararlıdır.[21] Nitekim, veri ile bilgi arasında sadece şekil farklılığı bulunduğunu savunan yazarlar da vardır.[22] Verinin işlenme yönteminin, yani elle mi bilgisayar ile mi işlendiğinin kişisel verinin belirlenmesi açısından bir önemi yoktur.

Sonuç olarak, veri, enformasyon ve bilgi kavramları arasında farklılıklar bulunmakla birlikte, ifade ettikleri anlam bakımından keskin bir ayrım bulunmamaktadır ve sistem bilimleri alanında dahi kavramlar arasındaki farklılıklar giderek belirsizleşmekteyken ve tanımlar üzerinde uzlaşılamamışken, hukuk alanında böyle bir terminolojik ayrımda ısrar etmek gereksizdir, kaldı ki uygulamada da karşılığı yoktur ve istenmeyen sonuçlara yol açabilir.[23] Tüzük'ün benimsediği de dahil olmak üzere pek çok kişisel veri tanımında "…her türlü bilgi…" ifadesinin kullanıldığı da göz önüne alındığında, ayrımın gereksizliği daha iyi anlaşılacaktır.

I.B.1.b)Kişisel Veri Kapsamına Giren Bilgiler

Kişisel verinin kapsamına, belirli veya kimliği belirlenebilir nitelikte olmak koşuluyla, bir kişiye ilişkin "her türlü bilgi" girer.[24] Buna göre, kişinin kimliği, fiziksel özellikleri, sağlık durumu, bireysel yaşantısı, tüketim alışkanlıkları, iş hayatı gibi pek çok konudaki bilgiler kişisel veri niteliğindedir.

Kişisel veriler nesnel veya öznel olabilir. Nesnel veriye örnek, olarak kişinin adı-soyadı ya da kan grubunu gösteren belge verilebilir. Öznel veriler ise kişinin yaşantısı, değerleri gibi hususlara ilişkin veriler olmakla birlikte özellikle nesnel

---

[20] Mehmet Hanifi **Bayram** (2011), Avrupa Birliği ve İnternet Hukuku, Seçkin, Ankara, s. 23.

[21] **İşevi** / **Çelme**, s. 12.

[22] Örneğin Kurt'a göre, veri, bilginin, bilgisayarın anlayıp işleyebileceği halidir, bkz. Levent **Kurt** (2005), Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin, Ankara, s. 38.

[23] **Küzeci**, s. 12-13.

[24] **Akgül**, s. 9.

verilerden hareketle varılan görüşler veya değerlendirmelerdir. Kişinin kredi yönünden güvenilirliği, sigorta yönünden ölümle sonuçlanabilecek bir riskinin bulunup bulunmaması, iş performansı bunlara örnek verilebilir.[25]

Kişisel veriler doğru veya yanlış olabilir. Gerek Direktif'te (DPD §10, 11) gerekse Tüzük'te (GDPR §16, Gerekçe 65) kişiye yanlış veya yanlış işlenmiş bilgilerin düzeltilmesi hakkının tanınmış olması, bilginin doğruluğunun veya yanlışlığının kişisel veri sayılma açısından bir önemi olmadığını göstermektedir. Kişiler, bu haklarını farklı yollarla kullanabilirler.[26]

Verinin hangi yolla ortaya çıktığı ve hangi formatta olduğu da kişisel veri kapsamına girip girmediği yönünden önem taşımamaktadır. Yazılı, sayısal, görsel, fotoğraf bazlı ya da işitsel her türlü verinin kişisel veri niteliğinde olması mümkündür.[27]

Kişinin biyolojik özelliklerine, fizyolojik yapısına ve imza gibi kişiye özgü bazı karakteristiklere ilişkin biyometrik veriler de kişisel veridir.[28] Bu tarz verilerin özelliği, kişiye dair bir bilgi olmalarının yanı sıra, kişiye özgü olmaları nedeniyle o kişinin belirlenmesinde ya da o kişiye dair başka bilgilere ulaşılmasında kullanılabilmeleridir. Örneğin, A'nın parmak izi örneği, A'ya ilişkin bir kişisel veri olmakla birlikte, aynı parmak izine bir nesnede rastlandığı takdirde A'nın bu nesneye dokunduğu, ya da bu nesneye dokunanın A olduğu bilgilerine ulaşılabilir.[29] [30]

Bir kişiyle ilişkilendirilemeyen (anonim) ya da ilişkilendirilemeyecek şekilde değiştirilmiş (anonimleştirilmiş) veriler kişisel veri kabul edilmemektedir. Anonim

---

[25] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 6, **Develioğlu**, s. 37, **Yüksel Civelek**, s. 16.

[26] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 6.

[27] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 7-8, **Develioğlu**, s. 38, **Yüksel Civelek**, s. 16-17.

[28] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 8, **Yüksel Civelek**, s. 17.

[29] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 8-9, **Yüksel Civelek**, s. 17.

[30] Biyometrik doku kaynağı olsalar da insan dokuları, kişisel veri değildir, bkz. Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 9.

veriyle sıklıkla karıştırılan psödonimize veriler ise kişinin dolaylı olarak belirlenmesinde kullanılabileceğinden kişisel veri kapsamındadır. Psödonimizasyon, Tüzük'te, kişisel verilerin ek verilerden yararlanmaksızın belli bir veri öznesi ile ilişkilendirilemeyecek şekilde, ek verilerin ayrıca saklanması ve kişisel verinin belirli veya belirlenebilir bir gerçek kişi ile ilişkilendirilmesinin önlenmesi için gerekli önlemlerin alınması koşuluyla işlenmesidir (GDPR §4/5).[31]

I.B.2.Gerçek Kişi

Hukuk düzeni açısından kişi, hak sahibi varlık anlamını taşır.[32] Kişiliğin gerçek kişilik ve tüzel kişilik olmak üzere iki türü bulunmaktadır. Gerçek kişiler insanlardır. Tüzel kişiler ise, çeşitli sosyal gerçekler ve gereksinimler göz önünde bulundurularak hukuk düzenince kendilerine kişilik tanınmış, belirli bir amaç doğrultusunda bir araya gelmiş insan veya mal topluluklarıdır.[33]

AB Genel Veri Koruma Tüzüğü'ndeki kişisel veri tanımı, verinin bir gerçek kişiye ilişkin olduğunu açıkça belirtmektedir. AB hukukunda veri koruma kurallarından sadece gerçek kişiler yararlanır ve AB kişisel verilerin korunması hukuku ile sadece gerçek kişiler korunur.[34] Nitekim Tüzük'ün 14'üncü Gerekçesi tüzel kişilere ilişkin kişisel bilgilerin Tüzük kapsamında olmadığını belirtmiştir. Bununla birlikte, tüzel kişilerin tamamen korumadan mahrum oldukları söylenemez. 95/46/AT sayılı Direktif de temel olarak gerçek kişilere uygulanmakla birlikte, ulusal

---

[31] Anonim veri ile psödonimize veri arasındaki fark, anonim verinin diğer bilgiler yardımıyla bir kişiyle ilişkilendirilebilir olmamasıdır. Bir örnekle açıklamak gerekirse, bir hastanedeki tıbbi kayıtlardan kişilerin isimleri, adresleri, doğum tarihleri gibi tüm verilerin silinmesi halinde mevcut kayıtlar anonim hale gelecektir. Ancak bu veriler silinmeden önce bir algoritma ile kayıtlara bir referans numarası verilmişse verinin psödonimize edilmesi söz konusudur. İlk durumda, ortada tıbbi kayıtlar bulunmaktadır ancak kime ait olduklarının mevcut diğer verilerden yola çıkarak anlaşılması mümkün değildir. İkinci durumda verilerin kime ait olduğu yine gizlenmiştir ancak bu veriler tamamen ayırt edilemez değildir ve aynı algoritma ile silinen verilere ulaşılması olasılığı vardır, bkz. Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, s. 22.

[32] Mustafa **Dural** / Tufan **Öğüz** (2018), Türk Özel Hukuku, Cilt: II, Kişiler Hukuku, 19. Baskı, Filiz, İstanbul, s. 5; M. Kemal **Oğuzman** / Özer **Seliçi** / Saibe **Oktay-Özdemir** (2012), Kişiler Hukuku, 12. Baskı, Filiz, İstanbul, s. 2.

[33] **Dural** / **Öğüz**, s. 8; **Oğuzman** / **Seliçi** / **Oktay-Özdemir**, s. 2.

[34] Handbook on European Data Protection Law (2018), s. 84. - http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law (Erişim tarihi: 24/10/2018),

mevzuatta tüzel kişilerin kişisel verilerin korunmasına ilişkin düzenlemeler bulunuyorsa bu düzenlemelerin Direktif'ten etkilenmeyeceğini belirtmişti.[35] Keza , 108 sayılı AK Sözleşmesi, taraf devletlerin tüzel kişilerin çıkarlarını korumak amacıyla Sözleşme kapsamını bu doğrultuda genişletmesine imkan tanımaktadır.[36] Avrupa Birliği üye ülkelerinden Avusturya, Danimarka, İtalya ve Lüksemburg ile birlik üyesi olmayan İzlanda, Norveç ve İsviçre'de veri koruma yasaları, tüzel kişileri de korumaktadır.[37] Nihayet, AİHM'nin, AİHS m. 8 uyarınca tüzel kişilerce yapılmış başvurular hakkında verdiği kararlar bulunmaktadır.[38]

Tüzük'ün 27 nci Gerekçesi, Tüzük'ün ölen kişilerin kişisel verileri açısından geçerli olmadığını, ancak Üye Devletlerin ölen kişilerin kişisel verilerini koruyucu düzenlemeler getirebileceğini belirtmiştir. Bulgaristan ve Estonya, bu yönde düzenlemelerin kabul edildiği Üye Devletler arasındadır. İsveç ve Birleşik Krallık ise sadece hayatta olan kişilerin verilerini kişisel veri kabul eden bir yaklaşım benimsemiştir.[39]

Daha önce de bahsedildiği gibi, Türk hukukunda da aynı kişisel veri tanımı kabul edilmiştir (KVKK m. 3-ç). Dolayısıyla Türk hukukunda da kişisel verilerin korunmasından yararlanma imkanı, gerçek kişilere tanınmıştır. Kişilik ölümle sona erdiğinden (TMK m. 28/1), ölen kişinin kişisel verileri KVKK kapsamında değildir.

---

[35] bkz. Direktif, Gerekçe 24.

[36] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, s. 12. - https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 (Erişim tarihi: 3/12/2018)

[37] Hüseyin Can **Aksoy** (2010), Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak, Ankara, s. 19.

[38] AİHS m. 8, "Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir" hükmünü içermektedir. AİHM, tüzel kişiler açısından konut dokunulmazlığı ve yazışmanın gizliliğinin ihlaline dair başvuruları kabul etmektedir, bkz. Handbook on European Data Protection Law, s. 85. Tüzel kişiler, verilerinin gizliliğinin bu maddeye aykırı fiillerle ihlali halinde AİHM'ye başvurarak korumadan yararlanabilmektedir. Bu çerçevede bkz. S*ociété Colas Est et al.* v *France*, 37971/97, 16 Nisan 2002.

[39] Edina **Harbinja** (2013), "Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?", SCRIPTed, C. 10, S. 1, s. 26 vd. - http://script-ed.org/?p=843 (Erişim tarihi: 15/12/2018)

Bu çerçevede meselenin, medeni hukukta ölüm sonrası kişilik hakkı değerlerinin korunmasına ilişkin tartışmalar çerçevesinde çözümlenmesi gerekecektir.[40]

I.B.3.Kişinin Belirli ya da Belirlenebilir Olması

Bir kişi topluluğu içerisinde diğer kişilerden ayırt etmenin mümkün olduğu kişi, belirlenebilir kişidir. Tüzük'te belirlenebilir kişi; kişisel verinin tanımı içerisinde, isim, kimlik numarası, konum bilgisi, çevrimiçi tanımlayıcı ("identifier") gibi tanımlayıcılar ya da fiziksel, fizyolojik, genetik, mental, ekonomik veya sosyal kimliğe ilişkin faktör ya da faktörler yardımıyla doğrudan ya da dolaylı olarak belirlenebilen gerçek kişi olarak tanımlanmıştır (GDPR §4/1).

Sözü edilen bilgilerin kişiyi hangi ölçüde belirlenebilir kıldığı, bilginin niteliği, kişinin içinde bulunduğu kişi topluluğunun özellikleri, belirlemenin yapıldığı bağlam gibi hususlara göre farklılık gösterir. Örneğin, isim, kişinin doğrudan belirlenebilmesini sağlayan en güçlü tanımlayıcıdır,[41] ancak kişinin ismini bilmek her zaman o kişiyi belirleyebilmek için yeterli olmamaktadır. Kişi yaygın rastlanan bir ad-soyad kombinasyonuna sahip ise, aynı ismi paylaştığı kişilerden sadece bu bilgiden yola çıkarak ayırt edilmesi mümkün değildir. Buna karşılık, daha az kalabalık bir grupta, örneğin bir işyerindeki çalışanlar arasından seçilebilmesi için yeterli olabilir. Kimi zaman da ismi bilinmeyen kişilerin belirlenebilirliği söz konusu olabilir. Örneğin; yaşı, mesleği, adresi bilinen bir kişinin bu bilgiler ışığında dolaylı olarak tespit edilmesi mümkündür. Gözlem yoluyla elde edilebilecek bilgiler bile belli koşullarda tanımlayıcı nitelik kazanabilir. "Yeşil kazaklı, kot pantolonlu ve gözlüklü öğrenci" denildiği zaman bu bilgiler ilgili öğrencinin sınıftaki diğer öğrencilerden ayırt edilmesini sağlayabilir. Şu durumda, kişinin eldeki veriler ışığında belirlenebilir olup olmadığı somut olayın koşulları göz önüne alınarak değerlendirilmelidir.[42]

---

[40] Nafiye **Yücedağ** (2017), "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 75, S. 2, s. 766-767.

[41] Handbook on European Data Protection Law, s. 89.

[42] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 13, **Develioğlu**, s. 33 vd., **Küzeci**, s. 10.

Direktif'in 26'ncı Gerekçesine göre, kişinin belirlenebilir olup olmadığının tespitinde, veri sorumlularının ya da belirlemeyi yapacak kimselerin kullanması makul surette beklenebilecek her türlü araç göz önünde tutulacaktır. Tüzük'ün de aynı sayılı Gerekçesinde aynı ifade yer almaktadır. Madde 29 Çalışma Grubu, 4/2007 sayılı Görüşünde bu kriter açısından işlemenin amacı, şekli, verinin işlenmesinden beklenen menfaat, kişinin menfaatleri, kurumsal riskler ve teknik yetersizlikler gibi hususların yanı sıra, teknolojinin geldiği son durumun ve gelecekte yaşanması muhtemel gelişmelerin de dikkate alınması gerektiğini açıklamıştır. Örneğin işlenen verinin on yıl süreyle saklanması gerekiyorsa, bu zaman zarfında, örneğin dokuzuncu yılda verinin belirleyici hale gelebileceği, dolayısıyla kişisel veriye dönüşebileceği öngörülerek gerekli önlemler alınmalıdır.[43]

I.B.4.İlişkin Olma

Verinin bir kişiye ilişkin olması, o veri yardımıyla o kişiyle bir bağlantı kurulabilmesi anlamına gelir.[44] Buna göre verinin içeriği, amacı veya sonucundan en az biri yönünden kişi ile bağlantılı olması aranır. Bu bağlantının kurulması çoğu zaman kolaydır, örneğin bir kişiyle yapılan görüşmenin videosu, o kişinin görüntüsünü içerdiğinden o kişiye ilişkindir.[45] Bazı hallerde bağlantı, nesnelere, olaylara veya durumlara ilişkin bilgiler sayesinde dolaylı olarak anlaşılabilir. Örneğin bir taşınmazın değeri, tek başına kişisel veri koruması kapsamında değildir. Ancak taşınmazın kime ait olduğu biliniyorsa, bu bilgi o kişinin malvarlığına ilişkin olup vergi mükellefiyetinin belirlenmesinde kullanılacağından amaç yönünden bağlantı kurulmuş olur ve kişisel veri haline gelir.[46]

---

[43] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 15 vd.

[44] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 9, **Develioğlu**, s. 38.

[45] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 9.

[46] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, s. 9, **Yüksel Civelek**, s. 18.

I.C. Özel Nitelikli Kişisel Veriler (Hassas Veriler)

Bazı kişisel verilerin işlenmesi, nitelikleri gereği temel hak ve özgürlükler açısından önemli tehditler oluşturabilir.[47] Kişinin ırksal veya etnik kökenine, siyasi görüşlerine, dini inancına ve felsefi görüşlerine, sendika ve meslek birliği üyeliklerine ilişkin veriler, yalnızca kişiyi belirlemek amacıyla işlenmesi halinde kişinin genetik ve biyometrik verileri ile fiziksel ve ruhsal sağlığına, cinsel yaşamına ve cinsel yönelimine ilişkin veriler Tüzük'ün "Özel Veri Türlerinin İşlenmesi" başlıklı 9'uncu maddesinde özel nitelikli veriler olarak sayılmış ve bu verilerin işlenmesi, maddenin devamında sayılan istisna halleri dışında yasaklanmıştır.[48]

II. KİŞİSEL VERİLERİN İŞLENMESİ

II.A. Tanım

Tüzük'teki tanımıyla işleme; veriler üzerinde toplama, kaydetme, organize etme, yapılandırma, saklama, uyarlama veya değişiklik yapma, geri kazanma, başvurma, kullanma, aktarma, yayma veya farklı yollardan ulaşılabilir hale getirme, gruplandırma veya birleştirme, erişimi kısıtlama, silme veya imha etme gibi işlemlerin gerçekleştirilmesidir (GDPR §4/2). Bu işlemler sınırlayıcı olarak sayılmamıştır, veri üzerindeki her türlü işlemin verinin işlenmesi kapsamında olduğu söylenebilir. İşlemlerin otomatik (elle işlem yapılmadan, yapay zeka aracılığıyla işleme) ya da otomatik olmayan (elle işleme) yöntemlerle yapılmasının bir önemi yoktur.[49] Direktif ve KVKK'daki tanımlar da Tüzük'ün tanımıyla paralellik göstermektedir (DPD §2/b, KVKK m. 3/e).

Otomatik olmayan yollarla işlenen verilere Tüzük'ün uygulanabilmesi için, bu verilerin bir veri kayıt sisteminin parçası olması gerekir. Veri kayıt sistemi ("filing

---

[47] Tüzük, Gerekçe 51.

[48] Direktif'in aynı başlıklı 8. maddesi de paralel bir düzenleme içeriyordu. Tüzük ile genetik ve biyometrik veriler ile cinsel yönelime ilişkin bilgiler de düzenleme kapsamına alınmıştır.

[49] 108 sayılı Avrupa Konseyi Sözleşmesi'nin konusunu otomatik işlenen veriler oluşturduğundan, bu sözleşmede yalnızca otomatik işlemenin tanımına yer verilmiştir. Buna göre, otomatik işleme, verilerin kısmen veya tamamen otomatik yollarla saklanması, veriler üzerinde mantıksal ve/veya aritmetik işlemler yapılması, verilerin değiştirilmesi, silinmesi, geri kazanılması veya yayılmasıdır (ETS 108 §2/c).

system"), Tüzük'te, bir fonksiyonel ya da coğrafi temele dayalı olarak merkezlenmiş, merkezlenmemiş veya dağıtılmış halde bulunan, belirli kriterler çerçevesinde erişilebilen her türlü kişisel veri grubu olarak tanımlanmıştır (GDPR §4/6). Belirli kriterlere göre organize edilmemiş (bir veri kayıt sistemi teşkil etmeyen) veriler veya veri grupları Tüzük kapsamında değildir.[50]

II.B. Kişisel Verilerin İşlenmesinden Sorumlu Kişiler

Kişisel verilerin korunmasının merkezinde, korumanın konusu olan gerçek kişi yer alır. Bu kişiyi belirtmek için genellikle veri öznesi ("data subject") veya ilgili kişi ifadeleri kullanılır.[51] Verilerin işlenmesinin etkileri bu kişi üzerinde görülür. Bu etkilerden sorumluluk ise, verilerin işlenmesi sürecinde aktif rol oynayan gerçek ve tüzel kişilerdedir. Bu kişilerin başlıcaları veri sorumlusu ("data controller") ile veri işleyen ("data processor") olup, kimi durumlarda üçüncü kişi ("third party") veya alıcı ("recipient") olarak anılan kişiler de sürece dahil olmaktadır.

II.B.1. Veri Sorumlusu

Veri kontrolörü veya veri denetçisi olarak da anılan[52] veri sorumlusu, veriyi toplama, saklama, işleme, kullanma ve yayma yetkilerine sahip kişidir. Tüzük'teki tanımda ise veri sorumlusunun tek başına veya başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi, kamu kurum ve kuruluşu ya da diğer örgüt olduğu belirtilmiştir ki bu, aynı yetkinin farklı bir ifadesidir. Veri sorumlusu, verinin neden ve nasıl toplanacağını, saklanacağını, kullanılacağını, kısacası işleneceğini belirler, dolayısıyla verilerin işlenmesinden başlıca sorumlu kişidir. Direktif'in tanımı da aynı yöndedir (DPD §2/d). KVKK'nın

---

[50] Tüzük, Gerekçe 15.

[51] **Küzeci**, s. 16.

[52] 22 Nisan 2008 tarih ve 1/576 Esas sayılı Kişisel Verilerin Korunması Kanun Tasarısı'nda "veri kütüğü sahibi" ifadesi kullanılmıştı, ancak gerek Direktif gerekse Tüzük anlamında herhangi bir sahiplik ya da verileri elde bulundurma kriteri öngörülmemiştir. Nitekim 6698 sayılı KVKK olarak yasalaşan 26 Şubat 2014 tarih ve 1/1009 sayılı Kişisel Verilerin Korunması Kanun Tasarısı'nda da benzer bir yaklaşım benimsenerek "veri sorumlusu" ifadesi tercih edilmiştir.

tanımı amaçları ve vasıtaları belirlemenin yanında veri kayıt sisteminin kurulması ve yönetilmesinden sorumluluktan da söz etmektedir (KVKK m. 3/ı).

İşlemenin amaç ve araçlarının AB veya Üye Devlet hukuklarında belirlendiği hallerde, veri sorumlusunun kim olduğu ya da hangi kriterlere göre atanacağı da ilgili hukuk tarafından belirlenebilir (GDPR §4/7).

Tanımdan anlaşıldığı gibi veri sorumlusunun yetki ve sorumluluklara başkalarıyla birlikte sahip olması mümkündür. Bu hallerde ortak veri sorumluluğundan ("joint controller") söz edilir (GDPR §26). Ortak veri sorumluları, Tüzük'ten doğan yükümlülükleri bakımından işbölümü yapmak ve işbirliği içinde hareket etmek zorundadır.

II.B.2.Veri İşleyen

Veri sorumluları, verileri onun adına işlemesi için farklı kişilere yetki verebilir. Veri sorumlusundan aldığı yetkiyle, veri sorumlusu adına işlemeyi gerçekleştiren gerçek veya tüzel kişiler, kamu kurum ve kuruluşları ile diğer örgütler, veri işleyenlerdir (GDPR §4/8, DPD §2/e, ETS 108 §2/f, KVKK m. 3/ğ).

Veri sorumlusu ve veri işleyen sıfatlarının, aynı somut olay açısından aynı kişide birleşmesi mümkün değildir. Veri işleyen, işlemenin amaçlarını ve vasıtalarını kendisi belirleyebiliyorsa o kişi artık bir veri sorumlusudur.[53] Bununla birlikte, bir işleme sürecinde veri işleyen konumunda olan kişinin, farklı bir veri işleme sürecinin veri sorumlusu olması söz konusu olabilir. Kişinin hangi olayda hangi sıfatla hareket ettiği, her veri grubu veya işleme süreci açısından ayrı ayrı değerlendirilmelidir.[54]

II.B.3.Üçüncü Kişi

Üçüncü kişiler, Direktif ve Tüzük'teki tanımlar uyarınca, veri öznesi, veri sorumlusu ve veri işleyenin dışında, veri sorumlusu ya da veri işleyenin doğrudan emri altında kişisel verilerin işlenmesine yetkili gerçek veya tüzel kişiler, kamu

---

[53] Handbook on European Data Protection Law, s. 101.

[54] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 Şubat 2010, s. 25.

kurum veya kuruluşları ya da diğer örgütlerdir (GDPR §4/10, DPD §2/f). KVKK'da üçüncü kişinin tanımı yapılmamakla birlikte üçüncü kişilerin anıldığı hükümlere yer verilmiştir (KVKK m. 11/1-ç, f, 16/2, 28).

Madde 29 Çalışma Grubu'nun 1/2010 sayılı görüşüne göre, üçüncü kişi kavramı, kişisel verilerin korunması bakımından, veri işleme yetkisi veya meşruiyeti bulunmayan (örneğin veri sorumlusu, veri işleyen ya da bunların çalışanı olmayan) kişileri kapsayacak şekilde yorumlanmalıdır. Buna göre, kişisel veri üçüncü kişiye ister hukuki ister hukuka aykırı şekilde geçsin, yani bu kişiye ister yetki verilsin ister verilmesin, bu kişinin sorumluluğundan söz edilebilecektir. Örneğin, bir şirketin çalışanı, görevlerini yerine getirirken yetkisinin olmadığı bir veriye eriştiği takdirde, artık bu kişinin "üçüncü kişi" olduğu ve verinin aktarılmasının ve işlenmesinin hukuka uygun olup olmamasına ilişkin tüm sonuçların bu kişi üzerinde doğduğu kabul edilmelidir.[55]

II.B.4.Alıcı

Alıcılar, üçüncü kişi olsun olmasın, kişisel verilerin açıklandığı gerçek ve tüzel kişiler, kamu kurum ve kuruluşları ile diğer örgütlerdir (GDPR §4/9, DPD §2/g). Kamu kurum veya kuruluşları, AB veya Üye Devlet hukuku uyarınca bir soruşturma kapsamında kişisel verileri alıyorsa, alıcı kabul edilmezler, ancak işlemeyi kişisel verilerin korunmasına ilişkin kurallara uygun yapmak zorundadırlar. KVKK'da alıcının tanımına yer verilmemiştir.[56]

Alıcının üçüncü kişiden farkı, verilerin açıklanmasının hukuka uygunluk koşulları açısından önemlidir. Örneğin, bir veri sorumlusunun ya da işleyenin, işleme sürecinde görev alan çalışanlarına kişisel verileri açıklaması herhangi bir ek koşul aranmaksızın hukuka uygundur. Ancak veri sorumlusundan ve işleyenden ayrı

---

[55] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", s. 31.

[56] 2008 tarihli Tasarı'nın 3. maddesinin a fıkrasında alıcı, "kişisel verileri belirli bir soruşturma çerçevesinde alan makamlar hariç olmak üzere, üçüncü kişi olsun veya olmasın verinin açıklandığı herhangi bir gerçek veya tüzel kişi ile kişi topluluğu, kamu kurum ve kuruluşu" olarak tanımlanmıştı.

üçüncü kişiler, ancak somut olay açısından gerekli şartların yerine gelmesi halinde elde ettikleri veriyi kullanabilirler.[57]

III. KİŞİSEL VERİLERİN KORUNMASI

III.A. Genel Olarak

"Verilerin korunması" deyimi Almanca "Datenschutz" sözcüğünden türemiş olup, pek çok dile bu şekilde girmiştir, örneğin İngilizce'deki "data protection" ve Fransızca'daki "protection des données", bu sözcüğün doğrudan karşılığıdır.[58] Kimi yazarlarca bu terimin, ilgili normların koruduğu hukuki menfaatleri ifade etmekte yetersiz kaldığı savunulmaktadır.[59] Bu görüş yerindedir, şayet gerek Birlik hukukunda gerekse Üye Devletlerin ulusal hukuk sistemlerinde ilgili mevzuat incelendiğinde düzenlemelerin alelade verilerin değil, kişisel verilerin, dolaylısıyla aslında kişilerin korunmasının amaçlandığı görülmektedir. 95/46/AT sayılı Direktif'in bireylerin korunmasına yönelik bir düzenleme olduğu tam başlığında belirtilmişti. Direktif'i yürürlükten kaldıran (AB) 2016/679 sayılı Tüzük'ün de aynı şekilde gerçek kişileri korumayı amaçladığı başlığında ifadesini bulmuştur. Üye Devletlerin iç mevzuatlarında ise genellikle "verilerin korunması" terimi kullanılsa da, ilgili düzenlemelerde kişisel verilerin konu edildiği belirtilmektedir.[60] Tüm bu hususlar dikkate alındığında, "kişisel verilerin korunması" teriminin korumanın amacını ve kapsamını daha iyi karşıladığı söylenebilir.

Kişisel verilerin korunması, kişisel veri niteliği taşıyan bilgilerin toplanması, depolanması, değiştirilmesi, yok edilmesi, kamuya açıklanması ve üçüncü kişilere aktarılması işlemlerinin, hangi amaç ve yöntemler izlenerek yapılabileceğinin belirlenmesini ve bu yapılırken bir ihlal olması halinde, hangi hukuki yollara

---

[57] Handbook on European Data Protection Law, s. 111.

[58] **Küzeci**, s. 13.

[59] Bkz. Lee A. **Bygrave** (2004), "Privacy Protection in a Global Context - A Comparative Overview", Scandinavian Law Studies, C. 47, s. 321.

[60] Örneğin bkz. United Kingdom Data Protection Act 2018 §1/1, BDSG §1/1.

başvurulabileceğinin düzenlenmesini ifade etmektedir.[61] Farklı bir ifadeyle, kişisel verilerin işlenmesine ilişkin esaslara somut bir çerçeve kazandırılması ve verileri işlenen kişinin, bu süreçte doğabilecek zararlar karşısında korunmasıdır.

III.B.Kişisel Verilerin Korunması İhtiyacı

Kişisel verilere çok farklı nedenlerle, çok farklı kişiler veya gruplarca ihtiyaç duyulabilmektedir. Günümüzde bilgi, güç ile eşdeğer tutulduğundan, kişisel veriler, hem kamu sektörü hem de özel sektör tarafından toplanmakta ve çeşitli amaçlarla kullanılmaktadır.[62] Kamu sektörü açısından kamu hizmetlerinin iyileştirilmesi veya ceza soruşturmalarının yürütülmesi, özel sektör açısından ise çalışanların performansının arttırılması, hitap edilen kitlenin ve alışkanlıklarının belirlenmesi, bu amaçlara örnek verilebilir. Bununla birlikte, yukarıda açıklandığı gibi, kişisel verilerin korunması aslında kişinin veri üzerindeki haklarının korunması amacına yönelmiştir. Bu nedenle kişisel verilerin korunması her şeyden önce bir haktır. Bu hak kişisel verilerin korunması hukukunun koruduğu menfaattir.

Kişisel verilere duyulan ihtiyaç ne kadar haklı sebeplere dayanırsa dayansın, bu verilerin toplanması ve işlenmesi çeşitli riskleri de beraberinde getirmektedir. Kişinin aleniyetten uzak kalmasını istediği bilgilerin toplanması veya işlenmesi suretiyle ulusal ve uluslararası birçok metinde[63] korunan özel yaşamın gizliliği hakkı ihlale uğrayabilir. Nitekim AİHM de kişisel verilerin toplanıp depolanmasının, AİHS'nin 8'inci maddesi kapsamına gireceğini kabul etmiştir.[64] Rotaru v. Romania kararında,[65] bir kamu otoritesinin kişinin özel hayatını ilgilendiren bilgileri depolamasının, özellikle bilginin kişinin uzak geçmişine ilişkin olduğu hallerde, 8. madde anlamında bir özel yaşama müdahale söz konusu olacağını, Amann v.

---

[61] **Aksoy**, s. 119.

[62] **Aksoy**, s. 75.

[63] AY m. 20 vd., AİHS m. 8, İHEB m. 12.

[64] Ali **Korkmaz** (2014), "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması", Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi, C. 16, Özel Sayı 1, s. 100.

[65] *Rotaru* v *Romania*, 28351/95, 4 Mayıs 2000. - http://hudoc.echr.coe.int/eng?i=001-58586 (Erişim tarihi: 4/2/2019)

Switzerland kararında[66] da, depolanan verinin kullanılıp kullanılmadığının ihlalin oluşumu açısından önemli olmadığını belirtmiştir. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland kararında[67] ise, kişinin, AİHS m. 8 ile güvence altına alınan özel hayatına ve aile hayatına saygı hakkından yararlanabilmesi için, kişisel verilerinin korunmasının hayati önem taşıdığını ifade etmiştir. Anılan kararların dışında, AİHM'nin kişisel verilerin AİHS m.8'e aykırı toplanması veya işlenmesi iddialarına dair çok sayıda kararı bulunmaktadır.[68]

Özellikle bilişim teknolojilerinin hızlı ve tahmin edilemez bir şekilde gelişmesi sonucu, kişisel verilerin toplanması ve işlenmesinde otomasyon giderek yaygınlaşmaktadır. Teknolojik gelişmeler her ne kadar önemli kolaylıklar sağlasa da, beraberinde ciddi riskler getirmekte, varolan riskleri de güçlendirmektedir. Günümüzde milyonlarca kişinin verileri kolaylıkla toplanabilmekte ve depolanabilmekte, ancak bu sistemlerdeki en ufak bir açığın varlığı, tüm bu verilerin istenmeyen kişilerin eline geçmesine yol açabilmektedir.[69] Öyle ki, kimi zaman sadece kişinin kendi erişiminde olan veriler bile tehlike altındadır.[70]

---

[66] *Amann* v *Switzerland*, 27798/95, 16 Şubat 2000. - http://hudoc.echr.coe.int/eng?i=001-58497 (Erişim tarihi: 4/2/2019)

[67] *Satakunnan Markkinapörssi Oy and Satamedia Oy* v *Finland*, 931/13, 27 Haziran 2017. - http://hudoc.echr.coe.int/eng?i=001-175121 (Erişim tarihi: 4/2/2019)

[68] Bu kararlar ve kısa özetleri için bkz. European Court of Human Rights Factsheet on Personal Data Protection, Şubat 2019. - https://www.echr.coe.int/Documents/FS_Data_ENG.pdf (Erişim tarihi: 4/2/2019)

[69] Örneğin 2011 yılında Sony'nin online platformu PlayStation Network'e yapılan hacker saldırısı sonucunda 77 milyon kullanıcının isimleri, adresleri, doğum tarihleri gibi kişisel bilgileri ele geçirilmişti. Bu saldırı tarihteki en büyük veri ihlallerinden biri kabul edilmektedir. Bkz. PlayStation data breach deemed in 'top 5 ever' - https://www.cbc.ca/news/technology/playstation-data-breach-deemed-in-top-5-ever-1.1059548 (Erişim tarihi: 5/2/2019)

[70] Örneğin 31 Ağustos 2014 tarihinde, Apple'ın bulut bilişim sistemi iCloud'daki bir açık kullanılarak çok sayıda ünlünün 500'e yakın özel fotoğrafı sızdırılmıştı. Olayda özel hayatın gizliliğinin tartışılmaz bir ihlali söz konusu olsa dahi, çoğu mağdur, telif haklarının ihlaline dayanarak ilgili makamlara başvurmuş, çoğu platform fotoğrafları ABD'nin en sıkı uygulanan yasalarından DMCA'ye aykırılık gerekçesiyle kaldırmıştır. Google ise arama sonuçları için sadece DMCA doğrultusundaki taleplerle hareket etse de fotoğrafları kendi platformlarından (YouTube, Blogger, Google+) "gizliliğin ihlali" nedeniyle kaldırdığını açıkça belirtmiştir, bkz. Rebecca **Fallon** (2015), "Celebgate: Two Methodological Approaches to the 2014 Celebrity Photo Hacks", Thanassis **Triopanis** / Athena **Vakali** / Laura **Sartori** / Pete **Burnap** (eds.), Internet Science: Second International Conference, INSCI 2015, Brussels, Belgium, May 27-29, 2015, Proceedings, s. 50.

Kişisel verilerin, veri öznelerinin kendi rızalarıyla açıkladıkları kişiler ve kurumlar karşısında da korunması gerekir. Kişisel verilerin işlenmesinden sorumlu kişiler, bilinçli veya bilinçsiz olarak, verileri toplama amacına aykırı olarak kullanabilmekte, kasıtlı veya kasıtsız olarak, veri öznelerinin rıza göstermediği kişilerin erişimine açabilmektedir. Veritabanlarının en değerli varlıklarından biri olduğunun farkına varıp verilerini satmaya başlayan şirketlerin sayısı giderek artmaktadır.[71]

Nihayet, kişilerin herhangi bir veri ihlaliyle karşı karşıya kalmamaları için gerekli önlemlerin alınmaması halinde, kişiler bilgilerini paylaşmakta tereddüt eder hale gelecek, bunun sonucu olarak da yukarıda sayılan, kişisel verilere ihtiyaç duyulan alanlarda aksaklıklar görülmeye başlanacaktır. Kişisel verilerin korunmasına, bu aksaklıkların önlenmesi bakımından da ihtiyaç duyulmaktadır. Dolayısıyla kişisel verilerin korunmasındaki amaç sadece veri öznelerinin haklarının değil, bilginin serbest dolaşımının da güvence altına alınması ve çatışan bu iki menfaat arasında bir denge kurulmasıdır. Kişisel verilerin korunması bu yönüyle bilginin serbest dolaşımının sınırını belirlemekte, veri sahiplerinin kişisel verilerinin işlenmesine rıza göstermek zorunda olduklarını ortaya koymaktadır.[72]

---

[71] Daniel J. **Solove** (2004), The Digital Person: Technology and Privacy in the Information Age, New York University Press, s. 19. Hem kişilerin rızaları dahilinde açıkladıkları verilerin farklı bir toplama amacıyla kullanıldığı, hem de kişilerin rızaları dışında verilerinin toplandığı güncel bir örnek olarak Facebook - Cambridge Analytica olayı gösterilebilir. 87 milyona yakın kişiyi etkileyen veri ihlali, 2018 yılının Mart ayında eski bir Cambridge Analytica çalışanının ihbarıyla ortaya çıkmıştır. Akademik kullanım amaçlı ve rıza dahilinde veri toplayan "thisisyourdigitallife" adlı uygulama, kullanıcıların Facebook arkadaş listesindeki diğer kişilerin de verilerini toplamış, bu veriler aracılığıyla veri öznesi seçmenlerin profilleri çıkartılarak seçim kampanyasında kullanılmıştır. Facebook CEO'su Mark Zuckerberg, 10 Nisan 2018 tarihli tanık ifadesinde kullanıcıların zarar görmemesi için yeterince önlem almadığını belirtmiştir. Bkz. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach - https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, The Cambridge Analytica scandal affected nearly 40 million more people than we thought - https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/ (Erişim tarihi: 5/2/2019)

[72] **Aksoy**, s. 75.

ÜÇÜNCÜ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI HUKUKU

I. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TARİHSEL GELİŞİMİ

I.A. Kişisel Verilerin Korunmasına İlişkin İlk Düzenlemeler

Kişisel verilerin korunmasına yönelik bazı ilkeler uzun zamandır kabul görmektedir. Ancak bu köklü ilkelerin birçoğu belirli meslek mensupları ile bireyler arasındaki güven ilişkisinden kaynaklanmıştır. Bunun en bilinen örneği, M.Ö. 5. yüzyılda gelişen hekimlerin sır saklama yükümlülüğüdür. Hekimler yanında din adamları, avukatlar, bankacılar gibi farklı meslek grupları için de benzer ilkelerin gelişiminin oldukça eskiye dayandığı söylenebilir.[73]

Kişisel verilerin tutulması yüzyıllardır süregelen bir uygulama olmasına rağmen, modern anlamda kişilerin verilerin korunması hukukunun ortaya çıkması ise yüzyıllar sonra olmuştur. Bunun nedenlerinden biri, gerek toplama yöntemlerinin gerekse kullanım amaçlarının oldukça kısıtlı olması ve uygulamanın çok yaygın olmamasıdır. Bu durum, bilgisayarların ortaya çıkışıyla paralel olarak 20. yüzyıl ortalarında değişmiştir. 1960'lı yıllardan itibaren, kayıtlar bilgisayar ortamında kolaylıkla tutulabilir ve depolanabilir hale gelmiş, devlet ve kişisel veri toplayan diğer kişi ve kurumlar bu imkanlardan yararlanarak elde ettikleri verileri içeren veritabanları oluşturmaya başlamıştır. bunun temel hak ve özgürlüklerden biri olan özel yaşamın gizliliği açısından oluşturduğu tehditler filozofların, hukukçuların ve konuyla ilgilenen diğer kişilerin dikkatini çekmiştir.[74] Bu tehditlerin ortadan kaldırılması ve veri toplayıcılarının veri özneleri karşısında aşırı güçlenmesinin önlenmesi yönünde kaçınılmaz bir talep oluşmuştur. İşte kişisel verilerin korunmasına yönelik ilk düzenlemelerin, dolayısıyla kişisel verilerin korunması hukukunun ortaya çıkmasının nedeni, bu talebe cevap verme arzusudur.

---

[73] **Küzeci**, s. 107.

[74] **Solove**, s. 15.

Verilerin korunmasına ilişkin ilk hukuki düzenleme, 7 Ekim 1970 tarihinde Almanya'nın Hessen eyaletinde yürürlüğe girmiştir (Hessen Kişisel Verilerin Korunması Kanunu, Hessische Datenschutzgesetz). Ancak Almanya'da federal düzeyde bir veri yasasının kabulü 1977'de gerçekleşmiş, Alman Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz, BDSG) olarak anılan bu yasa 1 Ocak 1978'de yürürlüğe girmiştir. Ulusal düzeyde dünyada ilk kanun, 11 Mayıs 1973'te İsveç'te Veri Kanunu (Datalagen) adıyla kabul edilmiştir.

1974 yılında ABD'de federal düzeyde bir Özel Hayatın Gizliliği Yasası (The Privacy Act of 1974) yürürlüğe girmiştir. Bu yasa federal kurumların kişisel veri toplaması, kullanması ve yaymasına ilişkin düzenlemeler getirmiş, ancak bu hükümlere çeşitli istisnalar getirmesi nedeniyle eleştirilmiş ve nihayetinde Avrupa'da yürürlüğe giren kanunlardaki gibi kurumsallaşmış bir veri koruma düşüncesi uygulamaya geçirilememiştir.[75]

Yukarıdaki gelişmeleri müteakip, diğer Avrupa ülkelerinde de kişisel verilerin korunması konusuna hukuki bir boyut kazandırma çalışmaları başlamıştır. Bu doğrultuda 6 Ocak 1978'de Fransa (Veri İşleme, Veri Dosyaları ve Bireysel Özgürlükler Kanunu, Loi informatique et libertés), 1 Ocak 1980'de Avusturya (Avusturya Federal Veri Koruma Yasası, Bundesgesetz über den Schutz personenbezogener Daten), 12 Temmuz 1984'te Birleşik Krallık (Birleşik Krallık Veri Koruma Yasası, Data Protection Act 1984), 13 Temmuz 1988'de İrlanda, 19 Haziran 1992'de İsviçre (İsviçre Federal Veri Koruma Yasası, Bundesgesetz über den Datenschutz) kişisel verilerin korunması kanunlarını yürürlüğe koymuşlardır. Bu kanunlar üzerinde zaman içinde değişen ihtiyaçlar doğrultusunda değişiklikler yapılmış ya da yeni kanunlar çıkarılmıştır.[76] 2018 itibariyle tüm AB üyesi devletlerde

---

[75] **Küzeci**, s. 111.

[76] Özellikle 1995 yılında kabul edilen DPD ile uyumlaştırma kapsamında kanunların yenilendiği görülmektedir. Örneğin 1973 tarihli İsveç Veri Kanunu, 1998 yılında (Kişisel Veri Kanunu (Personuppgiftslag) ile yürürlükten kaldırılmış, İngiltere'de de benzer şekilde yeni bir Veri Koruma Kanunu (Data Protection Act 1998) kabul edilmiştir.

bu kanunlar ya Tüzük ile uyumlu yeni kanunlarla değiştirilmiş ya da uyumlaştırma kapsamında çok ciddi değişikliklere uğramışlardır.[77]

Zaman içinde, veri toplayıcıları ile veri öznesi arasında güç dengesi kurmayı amaçlayan anlayış terk edilmiştir. Kişisel verilerin korunması, özel yaşamın gizliliği hakkının bir yansıması olarak ele alınmaya başlanmıştır. Portekiz ve İspanya, 1974 ve 1978 tarihli Anayasalarında bu yaklaşımla kişisel verilerin işlenmesinin, bireylerin onur ve mahremiyetlerini korumak adına sınırlandırılacağını anayasalarında belirtmişlerdir. Avusturya, Macaristan ve İsveç gibi devletlerde de benzer düzenlemeler yapılmıştır.[78]

Kişisel verilerin korunmasının bağımsız bir hak olarak ön plana çıkmasında, özellikle Alman Federal Anayasa Mahkemesi'nin 15 Aralık 1983 tarihli Nüfus Sayımı Kararı'nın[79] etkisi büyük olmuştur. Mahkeme, anılan kararda 1982 yılında kabul edilen Nüfus Sayım Kanunu'nu (Volkszählungsgesetzes 1983) anayasaya aykırı bularak yürürlükten kaldırmıştır. Kanun kişisel verilerin korunmasına ilişkin potansiyel sorunları dikkate almayan bir tarzda hazırlanmıştı ve toplanan bilgilerin nüfus sayımı dışında amaçlarla da kullanılabileceğini öngörüyordu. Mahkeme, kişilerin kendilerine ait verilerin geleceğini belirleme hakkından (informational self-determination, informationelle Selbstbestimmung) söz etmiş, bu yaklaşım gerek Almanya'da gerekse diğer Avrupa ülkelerinde karşılık bulmuştur.[80] Günümüzde veri öznesini veri işleme sürecinin aktif bir elemanı olarak kabul eden düzenlemelerin temelinde bu karara gerekçe oluşturan ilkeler yer almaktadır. Buna göre artık bireylerin kişisel verilerinin işlenmesi sürecinin dışında kalma şansı yoktur.[81]

---

[77] Üye Devletlerde uyumlaştırma kapsamında hazırlanan yeni kanunlar ve özetleri için bkz. EU Member State GDPR Implementation Laws and Drafts - https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/ (Erişim tarihi: 8/3/2019)

[78] **Küzeci**, s. 113.

[79] BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 ("Volkszählungsurteil").

[80] Karar hakkında ayrıntılı bilgi ve bir inceleme için bkz. Gerrit **Hornung** / Christoph **Schnabel** (2009), "Data Protection in Germany I: The population census decision and the right to informational self-determination", Computer Law & Security Report, C. 25, S. 1, s. 84 vd. - https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Hornung/Hornung___Schnabel__Data_protection_in_Germany_I__CLSR_2009__84.pdf (Erişim tarihi: 8/3/2019)

[81] **Küzeci**, s. 114.

I.B. Kişisel Verilerin Korunması Hukukunun Uluslararası Boyutta Gelişimi

I.B.1. Genel Olarak

Kişisel verilerin korunmasına yönelik ulusal düzenlemelere uluslararası birtakım standartlar getirilmesi ihtiyacına ilk olarak Avrupa Komisyonu, 1973 yılında dikkat çekmiştir. Komisyon, o zamanki adıyla Avrupa Topluluğu'nun[82] vatandaşların korunmasını sağlamak adına tüm üyelerin üzerinde uzlaştığı ortak temel kurallar belirlemesi gerektiğine işaret etmiş, uzlaşıya varılmasının daha sonra birbiriyle çelişen ulusal hukuk düzenlemelerini uyumlaştırmak zorunda kalmaktan daha iyi olacağını ifade etmiştir.[83]

1980'li yıllar, kişisel verilerin korunmasına ilişkin uluslararası düzeyde çalışmaların başladığı ilk dönemdir. Bu hususta OECD'nin çalışmaları büyük rol oynamıştır. OECD'nin 23 Eylül 1980 tarihinde kabul ettiği "Gizliliğin Korunması ve Sınırötesi Kişisel Veri Dolaşımına İlişkin Rehber İlkeler"[84] (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), kişisel verilerin korunmasına ilişkin uluslararası ilk metin olması yönünden büyük bir öneme sahiptir. OECD Rehber İlkeleri, 2013 yılında dönemin ihtiyaçları dikkate alınarak güncellenmiştir.

28 Ocak 1981 tarihinde Avrupa Konseyi, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni (ETS 108) imzaya açmış, bu sözleşme 1 Ekim 1985 tarihinde yürürlüğe girmiştir.

14 Aralık 1990 tarihinde, Birleşmiş Milletler Genel Kurulunca, "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler"[85] (United Nations guidelines concerning computerised personal data files) kabul edilmiştir.

---

[82] Bundan sonra "Topluluk" olarak anılacaktır.

[83] Commission of the European Communities, Communication of the Commission to the Council on Community Policy on Data Processing, Gerekçe 39; Orla **Lynskey** (2015), The Foundations of EU Data Privacy Law, Oxford University Press, s. 47.

[84] Bundan sonra OECD Rehber İlkeleri olarak anılacaktır.

[85] Bundan sonra BM Rehber İlkeleri olarak anılacaktır.

BM, OECD ve AB'deki çalışmalar, Avrupa dışında da yankı bulmuş, bunun sonucunda Asya'da Asya-Pasifik Ekonomik İşbirliği'nce (APEC) 2004 yılında bir Özel Hayatın Gizliliği Çerçeve Belgesi[86] kabul edilmiştir. Örgütün misyonuyla paralel olarak,[87] bu çerçeve belgede kişisel verilerin korunması ekonomik ve ticari bağlamda ele alınmıştır. APEC Çerçeve Belgesi'ni, sınırötesi veri dolaşımına ilişkin standartlar getirmeyi amaçlayan çalışmalar izlemiştir. Bu doğrultuda 2007 yılında Pathfinder projesi hayata geçirilmiş, 2011 yılında APEC Sınırötesi Gizlilik Kuralları[88] sistemi kabul edilmiştir.[89]

I.B.2.Avrupa Birliği'ndeki Gelişmeler

Avrupa Birliği düzeyinde kişisel verilerin korunması alanına yönelik faaliyetlerin en önemlisi, 24 Ekim 1995 tarihinde, 95/46/AT sayılı Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi (DPD)'nin kabul edilmesidir. Temel bir düzenleme niteliğinde olan bu direktif, ilerleyen yıllarda daha özel kapsamlı 97/66/AT sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Direktifi,[90] 2000/31/AT sayılı E-Ticaret Direktifi,[91] 2002/58/AT sayılı Özel Yaşamın Gizliliği ve Elektronik

---

[86] APEC Privacy Framework, 2004/AMM/014rev1, 29 Ekim 2004. Bundan sonra APEC Çerçeve Belgesi olarak anılacaktır.

[87] https://www.apec.org/About-Us/About-APEC/Mission-Statement (Erişim tarihi: 9/3/2019)

[88] APEC Cross-Border Privacy Rules (APEC CBPR)

[89] Ellyce R. **Cooper** / Alan Charles **Raul** (2017), "APEC Overview", Alan Charles **Raul** (ed.), The Privacy, Data Protection and Cybersecurity Law Review, 4. Baskı, Law Business Research Ltd, Londra, s. 26 vd.

[90] *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*, OJ L 024, 30 Ocak 1998.

[91] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* ('Directive on electronic commerce'), OJ L 178, 17 Temmuz 2000.

İletişim Direktifi,[92] 2006/24/AT sayılı Veri Saklama Direktifi[93] gibi direktiflerle desteklenmiştir.

95/46/AT sayılı Direktif, kişisel verilerin korunması mevzuatında Birlik içi yeknesaklığı sağlayamamış, özellikle internetin ortaya çıkışı ve Birlik içinde yaygınlaşması sonrası yukarıda anılan risklerin katlanarak arttığı bir ortamda ihtiyaçlara cevap veremez hale gelmiştir. Bunun üzerine Avrupa Komisyonu, 4 Kasım 2010 tarihli açıklamasında,[94] hızlı teknolojik gelişmeler ve globalleşme sonucu köklü değişikliklere uğrayan dünyada kişisel verilerin korunmasında yeni güçlükler ortaya çıktığını ifade ederek, Birlik'in konuya kapsamlı ve tutarlı bir yaklaşım geliştirmesi gerektiğini belirtmiştir. Bu açıklama Komisyon için aynı zamanda bir yol haritasıdır: Komisyon, 2011 yılında yeni bir kişisel verilerin korunması düzenlemesi teklifi sunacak, mevcut düzenlemelerin yeni düzenlemeyle uyumlu hale getirilmesine gerek olup olmadığını tespit edecek ve yeni mevzuatın Üye Devletlerce iç hukuka doğru ve tam olarak geçirilip geçirilmediğini sıkı bir şekilde takip edecektir.[95]

Gerekli çalışmaların tamamlanmasının ardından 2012 yılında Komisyon, Bireylerin Kişisel Verilerinin İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Tüzüğü (Genel Veri Koruma Tüzüğü) ve Bireylerin Kişisel Verilerinin Yetkili Makamlarca Suçları Önleme, Soruşturma, Tespit Etme ve Kovuşturma veya Cezaların İnfazı Amacıyla

---

[92] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* ('Directive on privacy and electronic communications'), OJ L 201, 31 Temmuz 2002.

[93] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, OJ L 105, 13 Nisan 2006. Bu direktif 8 Nisan 2014 itibariyle ABAD'ın C-293/12 ve C-594/12 sayılı kararı ile geçersiz kılınmıştır. Karar için bkz. http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3596495 (Erişim tarihi: 9/3/2019)

[94] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union* - COM(2010) 609. Açıklama metni için bkz. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF (Erişim tarihi: 9/3/2019)

[95] COM(2010) 609, s. 18 vd.

İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi'ni[96] içeren yeni bir kişisel verilerin korunması çerçeve mevzuatı önerisi sunmuştur. İki taslak da 12 Mart 2014 tarihinde Avrupa Parlamentosu tarafından üzerinde değişiklikler yapılarak kabul edilmiştir. 27 Nisan 2016'da Avrupa Birliği Konseyi ve Avrupa Parlamentosu tarafından iki düzenleme de (AB) 2016/679 sayılı Tüzük ve (AB) 2016/680 sayılı Direktif olarak kabul edilerek 4 Mayıs 2016'da Avrupa Birliği Resmi Gazetesi'nde yayınlanmıştır.[97] (AB) 2016/679 sayılı Tüzük, 25 Mayıs 2018 tarihinde uygulanmaya başlanacağını (§99), (AB) 2016/680 sayılı Direktif ise 6 Mayıs 2018 tarihine kadar Üye Devletlerin iç hukuklarını bu direktifle uyumlu hale getireceklerini belirtmiştir (§63/1).

Anılan düzenlemeler, Avrupa Birliği kişisel verilerin korunması hukukunda yeni bir dönemin başlangıcı olmuştur. GDPR ile kişilerin verileri üzerindeki hakimiyetleri güçlendirilmiş, unutulma hakkı ("the right to be forgotten") başta olmak üzere veri öznelerine yeni haklar tanınmış, verilerin işlenmesinin hukuka uygunluğu sıkı şartlara bağlanarak güçlü yaptırımlar öngörülmüştür. Direktif'in sağlamakta yetersiz kaldığı yeknesaklığın sağlanması yolunda önemli bir adım atılmıştır. (AB) 2016/680 sayılı Direktif ise, Tüzük standardında bir düzenleme değildir ve yarattığı etki de Tüzük ile kıyaslandığında oldukça sönük kalmıştır, ancak bundan direktifin önemsiz ya da gereksiz bir düzenleme olduğu anlaşılmamalıdır. Nitekim bu direktif Tüzük'te yer almayan bir alanı düzenlemekte, kolluk faaliyetleri karşısında bireylerin haklarını, bu faaliyetleri de aksatmayacak şekilde güvence altına almayı amaçlamaktadır.[98]

---

[96] *Directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.*

[97] OJ L119, s. 1-88, 89-113.

[98] (AB) 2016/680 sayılı Direktif'in içeriği ve hakkındaki eleştirileri detaylı bir biçimde ele alan bir çalışma için bkz. Gülşah **Bostancı Bozbayındır** (2018), "Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, S. 2018/2, s. 51 vd.

I.C. Türkiye'de Kişisel Verilerin Korunması Hukukunun Gelişimi

I.C.1. KVKK'nın Kabulü Öncesindeki Durum

I.C.1.a) Genel Olarak

Türkiye, yukarıda açıklanan ulusal ve uluslararası gelişmeleri gereği gibi takip edememiş, anılan devletlere kıyasla kişisel verilerin korunmasına hukuki bir zemin kazandırmakta oldukça yavaş kalmıştır. 28 Ocak 1981'de ETS 108'i imzalayan Türkiye, bu sözleşmeyi ilk imzalayan devletlerden biridir, ancak sözleşmeye taraf olan son AK üyesi devlettir. Bunun nedeni, sözleşmenin imzalandıktan 35 yıl sonra, 30 Ocak 2016 tarihinde, TBMM'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun'u kabul etmesiyle onaylanmış olmasıdır. Kanun, 18 Şubat 2016 tarihinde Resmi Gazete'de yayımlanmış,[99] onay belgesi 2 Mayıs 2016 tarihinde AK'ye ulaşmış ve 1 Eylül 2016 itibariyle sözleşme Türkiye açısından yürürlüğe girmiştir.[100]

Uzun bir süre boyunca Türk hukukunda doğrudan veya dolaylı olarak kişisel verilerin korunmasına ilişkin hükümler mevzuat içerisinde dağınık bir halde yer almıştır. Örneğin 5237 sayılı Türk Ceza Kanunu'nun 135-140. maddeleri arasında, kişisel verilerin hukuka aykırı olarak kaydedilmesi, başkalarına verilmesi, yayılması, ele geçirilmesi ve yok edilmemesi şeklinde suçlar düzenlenmiştir. Bunun dışında Türk Medeni Kanunu'nun kişiliğin korunmasına ilişkin hükümleri (m. 23-27) kişisel veriler açısından da uygulanabilir nitelikte hükümlerdir. Kişisel verilerin ihlali nedeniyle Türk Borçlar Kanunu'nun haksız fiil hükümleri (m. 49 vd.) uyarınca maddi ve manevi tazminat talep edilmesi de mümkündür.[101] Anılan düzenlemelerle kişisel veriler açısından bir koruma sağlanmıştır, ancak doğrudan konuya ilişkin bir

---

[99] RG S. 29628.

[100] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/TUR?p_auth=dyD32ldD (Erişim tarihi: 12/3/2019)

[101] Farklı kanunlarda yer alan ilgili düzenlemeler hakkında daha fazla bilgi için bkz. **Aksoy**, s. 112 vd.

temel kanunun eksikliği yakın geçmişe kadar hissedilmiş, bu süreçte ciddi ve telafi edilmesi oldukça güç veri ihlalleriyle karşılaşılmıştır[102]. Gelişim süreci aşağıda incelenecek 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kabulü, Türk hukukunda önemli bir boşluğu doldurmuştur.

I.C.1.b)Kişisel Verilerin Korunmasının Anayasal Dayanağı

1982 Anayasası, 2. maddesinde Türkiye'nin "insan haklarına saygılı, demokratik bir hukuk devleti" olduğunu açıklamıştır. Bu ideali doğrultusunda, herkesin kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahip olduğunu hüküm altına almıştır (m. 12). Kişisel verilerin korunması, kişinin maddi ve manevi varlığı (AY m. 17), özel yaşamın gizliliği ve korunması (AY m. 20), haberleşme hürriyeti (AY m. 22), din ve vicdan hürriyeti (AY m. 24), düşünce ve kanaat hürriyeti (AY m. 25) başta olmak üzere pek çok temel hak ve özgürlük ile yakından ilişkilidir. Bu anlamda, her ne kadar bağımsız bir temel hak ve özgürlük olarak düzenlenmemiş olsa da, kişisel verilerin korunması, bu hakların bir tezahürü olarak Anayasal dayanağa sahip olmuştur. Nitekim Anayasa Mahkemesi de 1996/68 E.-1999/1 K. sayılı kararında kişisel verilerin AY m. 20'de düzenlenen özel yaşamın gizliliği ile doğrudan ilişkili olduğunu teyit etmiştir.[103]

12 Eylül 2010 tarihli referandumda, aynı yılın Mayıs ayında hazırlanan Anayasa reform paketinin[104] kabul edilmesi ile, Anayasa'nın özel yaşamın gizliliğini düzenleyen 20. maddesine, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.

---

[102] Örneğin Nisan 2016'da, ironik olarak 6698 sayılı KVKK'nın yürürlüğe girmesinden hemen önce, yaklaşık 50 milyon Türk vatandaşının sızdırılan isim, adres, T.C. kimlik numarası gibi bilgilerini içeren bir veritabanı (Turkish Citizenship Database) oluşturulduğu haberi geniş yankı bulmuştur. Bkz. Turkish authorities 'probing huge ID data leak' - https://www.bbc.com/news/technology-35978216 (Erişim tarihi: 12/3/2019)

[103] **Yüksel Civelek**, s. 141.

[104] 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, RG T. 13/5/2010, S. 27580.

Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." fıkrası eklenerek[105] kişisel verilerin korunması, bağımsız bir hak olarak doğrudan Anayasal dayanağa kavuşturulmuştur.

I.C.2. Veri Koruma Kanunu Hazırlama Çalışmaları ve KVKK'nın Kabulü

Türkiye'de kişisel verilerin korunmasına yönelik kanun çalışmalarının 1989 yılında başladığı belirtilmektedir.[106] 13 Eylül 1995 tarihinde, veri koruma kanunu tasarısı hazırlamak üzere bir komisyon kurulmuştur. 2000 yılına gelindiğinde çalışmaların tamamlanamamış olması üzerine, aynı yıl yeni bir komisyon kurulmuştur. Bu komisyonun 2003 yılında hazırladığı tasarı Adalet Bakanlığınca 22 Nisan 2008 tarihinde TBMM'ye sunulmuştur. Tasarı Adalet Komisyonu'nda görüşülse de, seçimlerin yenilenmesinden önce yasalaşamaması sonucu hükümsüz kalmıştır. Ancak çalışmalar hız kesmeden devam etmiş, Adalet Bakanlığınca kurulan yeni komisyon tarafından güncellenen tasarı, 8 Haziran 2012 tarihinde Başbakanlığa gönderilmiştir.[107] 26 Aralık 2014 tarihinde Başbakanlık tarafından TBMM'ye gönderilen tasarı da yine seçimlerin araya girmesi sonucu yasalaşamamıştır. 18 Ocak 2016 tarihinde tekrar TBMM'ye gönderilen tasarı, 24 Mart 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu olarak kabul edilerek, 7 Nisan 2016 tarihinde Resmi Gazete'de yayınlanarak yürürlüğe girmiştir.[108]

---

[105] 5982 s. Kanun, m. 2.

[106] **Küzeci**, s. 311.

[107] T.C. Avrupa Birliği Bakanlığı, 27. RİG Toplantısı Basın Bildirisi, Bursa, 11 Kasım 2012. - https://www.ab.gov.tr/files/sib/rig/27__rig_basin_bildirisi.pdf (Erişim tarihi: 12/3/2019)

[108] RG T. 7/4/2016, S. 29677.

II. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN KAYNAKLARI

II.A.Genel Olarak

Kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin temelinde, İHEB, BM Uluslararası Bireysel ve Siyasal Haklar Antlaşması, AİHS, Amerika İnsan Hakları Sözleşmesi gibi uluslararası belgelerde düzenlenen, özel yaşamın gizliliği başta olmak üzere çeşitli temel insan hakları yer almaktadır.[109] Yukarıda üzerinde durulduğu gibi, bu ilkelerden hareketle, çeşitli ülkelerde 1970'lerden itibaren ulusal düzeyde doğrudan kişisel verilerin korunmasını düzenleyen kanunlar hazırlanmaya başlanmış, 1980'lerden itibaren ise uluslararası örgütlerin çalışmalarıyla bu alana yönelik uluslararası standartlar kabul edilmiştir.

Ulusal düzeyde, kişisel verilerin korunması hukukunun çıkış noktasını oluşturan ilkeler ve temel insan hakları dayanağını ve güvencesini ulusal anayasalardan almaktadır. Bunun dışında, kişisel verilerin korunmasına ilişkin esaslar genellikle kanunlarla düzenlenmektedir. 2019 itibariyle, Türkiye dahil 107 ülkede kişisel verilerin korunması kanunları yürürlüktedir.[110] Türkiye'de bu alana ilişkin en temel düzenleme, 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur.

II.B.Kişisel Verilerin Korunması Hukukunun Uluslararası Kaynakları

Bu başlık altında, kişisel verilerin korunmasının, uluslararası örgütlerin çalışmalarının ürünü olan ve tarihsel gelişimine yukarıda değinilen OECD Rehber İlkeleri, 108 sayılı AK Sözleşmesi, BM Rehber İlkeleri ve APEC Çerçeve Belgesi'nde ele alınışı incelenmiştir. 95/46/AT sayılı Direktif ve (AB) 2016/679 sayılı Tüzük, üçüncü bölümün konusunu oluşturduğundan burada ayrıca değinilmemiştir.

---

[109] **Bygrave**, s. 332, **Küzeci**, s. 128.

[110] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (Erişim tarihi: 27/3/2019)

II.B.1.OECD Rehber İlkeleri

OECD Rehber İlkeleri'nin 1980 yılında kabul edilen ilk hali,[111] giriş kısmında, amacını OECD üyesi devletler arasında serbest veri akışını ilerletmek ve üye devletler arasında ekonomik ve sosyal ilişkilerin gelişiminin önünde haksız engeller oluşmasının önüne geçmek olarak ifade etmiştir. Bu çerçevede, üye devletler için özel yaşamın gizliliğini ve sınırötesi veri akışını düzenlerken dikkate alınacak ilkeler belirlemiştir. Bu ilkeler uyulacak asgari standartlar olup, özel yaşamın gizliliği ve bireysel özgürlüklerin korunmasına yönelik ek önlemlerle desteklenebilirler (OECD Rehber İlkeleri m. 6). Kabul edilen sekiz temel ilke şunlardır:

Toplamada sınırlılık ilkesi (m. 7): Kişisel verilerin toplanması birtakım sınırlamalara tabi olmalıdır. Veriler hukuka uygun ve meşru olarak, gerektiğinde veri öznesinin bilgisi ya da rızası dahilinde toplanmalıdır.

Veri kalitesi ilkesi (m.. 8): Kişisel veriler kullanım amaçlarına uygun olmalı, yine bu amacın gerektirdiği ölçüde doğru ve tam olmalı, güncel tutulmalıdır.

Amacın belirtilmesi ilkesi (m. 9): Kişisel verilerin hangi amaçla kullanılacağı, en geç verilerin toplanması anında belirtilmiş olmalıdır.

Kullanımda sınırlılık ilkesi (m. 10): Kişisel veriler, belirtilen amacın dışında açıklanmamalı, erişime açılmamalı veya herhangi bir şekilde kullanılmamalıdır. Veri öznesinin rızasının (m. 10/a) ya da kanuni yetkinin (m. 10/b) varlığı halleri bunun istisnalarıdır.

Güvenlik ilkesi (m. 11): Kişisel veriler; kaybolma, yetkisiz erişim, yok olma, kullanım, değiştirme ya da açıklama gibi risklere karşı makul güvenlik önlemleri ile korunmalıdır.

Açıklık ilkesi (m. 12): Kişisel verilere ilişkin gelişmeler, uygulamalar ve politikalar yönünden genel bir açıklık politikası benimsenmelidir. Kişisel verilerin niteliğini, kullanım amaçlarını ve veri sorumlusunun kimliğini tespit etme imkanı herkes için mevcut bulunmalıdır.

---

[111] Tam metin için bkz. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim tarihi: 27/3/2019)

Bireysel katılım ilkesi (m. 13): Bireyler, veri sorumlularından ve diğer ilgililerden ellerinde kendilerine ilişkin verilerin bulunup bulunmadığını öğrenme (m. 13/a); makul süre içinde, makul bir ücret karşılığında kendilerine gönderilmesini isteme (m. 13/b); bu isteklerinin reddedilmesi halinde nedenlerinin kendisine açıklanmasını isteme ve ret kararına itiraz etme (m. 13/c); kendine ilişkin verileri sildirme, düzelttirme, tamamlama ya da değiştirme (m. 13/d) haklarına sahip olmalıdır.

Hesap verilebilirlik ilkesi (m. 14): Veri sorumluları, sayılan ilkeleri hayata geçiren önlemlere uyma yönünden sorumlu tutulmalıdırlar.

OECD Rehber İlkeleri'nin 2013 yılında yeniden düzenlenen şeklinde de yukarıdaki ilkeler korunmuştur.[112] Yeni metinde gizlilik yönetim programı ("privacy management program"), veri güvenliği ihlal bildirimi ("data security breach notification") gibi yeni kavramlar düzenlenmiş, ayrıca mevcut esaslar güncellenmiş ve özellikle hesap verilebilirlik ilkesi, veri sorumlularının hangi güvenlik önlemlerini alabilecekleri açıklanarak genişletilmiştir.[113]

OECD Rehber İlkeleri, tavsiye niteliğinde, bağlayıcılığı olmayan ilkelerdir ve Üye Devletler bu ilkeleri iç hukuklarına uygun gördükleri şekilde aktarabilecekleri gibi hiç aktarmamayı da seçebilirler. İlkelerin bağlayıcılığının olmaması nedeniyle etkisi sınırlı olmuş, ulusal kanunlarda farklılıklar görülmeye devam etmiştir.[114]

II.B.2.108 Sayılı Avrupa Konseyi Sözleşmesi (ETS 108)

ETS 108'in 1 inci maddesinde sözleşmenin amacı, "her bir tarafın ülkesinde, uyruğu veya ikamet yeri ne olursa olsun her gerçek kişinin temel hak ve

---

[112] OECD Rehber İlkeleri'nin güncellenmiş tam metni için bkz. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Erişim tarihi: 28/3/2019)

[113] OECD Rehber İlkeleri'nin 2013 metnindeki tüm yenilikler ve bir değerlendirme için bkz. Monica **Kuchewsky** (2013), What does the revision of the OECD Privacy Guidelines mean for businesses?, MLex Ab Extra. - https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf (Erişim tarihi: 28/3/2019)

[114] **Lynskey**, *The Foundations*, s. 48.

özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almak" olarak açıklanmıştır.[115] Bu anlamda, ETS 108 ile özel yaşamın gizliliği hakkını güvence altına alan AİHS (m. 8) arasında yakın bir ilişki olduğu söylenebilir. Hatta ETS 108'in kabulünde, AİHS bünyesindeki güvencelerin sınırlı kalacağı düşüncesi etkili olmuştur.[116]

ETS 108, yalnızca kamu sektörü veya özel sektör tarafından otomatik yollarla işlenen kişisel veriler yönünden uygulama alanı bulmaktadır (§3/1). Otomatik işlemenin tanımında (§2/c) "…kısmen veya tamamen otomatik yollarla…" ifadesine yer verilmesi, kısmen elle işlenen kişisel verilerin de ETS 108 kapsamında korunduğu şeklinde yorumlanabilir.[117] Bunun yanı sıra tarafların ETS 108'in uygulama alanını otomatik yollarla işlenmeyen kişisel verileri de kapsayacak şekilde genişletmeleri mümkündür (§3/c).

OECD Rehber İlkeleri'nde olduğu gibi, ETS 108 ile de kişisel verilerin korunmasına yönelik birtakım asgari standartlar öngörülmüştür. Sözleşmenin hiçbir hükmünün tarafların daha kapsamlı bir koruma sağlamasına engel olduğu şeklinde yorumlanmaması gerektiği de belirtilmiştir (§11). ETS 108'in getirdiği temel ilkeler şu şekilde sıralanabilir:

Veri kalitesi (§5): Otomatik yollarla işlenecek kişisel veriler meşru ve hukuka uygun olarak toplanmalı ve işlenmelidir (§5/a). Veriler belirli ve meşru amaçlar için saklanmalı, bu amaçlarla bağdaşmayan amaçlarla kullanılmamalıdır (§5/b). Saklanacak veriler saklama amacı için yeterli ve amaçla ilgili olmalı, gereğinden fazla veri saklanmamalıdır (§5/c). Veriler doğru ve gerekli olduğu hallerde güncel olmalıdır (§5/d). Veriler, veri öznesinin kimliğinin anlaşılmasına imkan verecek şekilde saklanmalı, amacın gerektirdiğinden uzun süre tutulmamalıdır (§5/e).

---

[115] Sözleşmenin Türkçe tam metni için bkz. http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/ak/turkce/108_tur.pdf (Erişim tarihi: 28/3/2019) Sözleşmenin İngilizce orijinal metni için bkz. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 (Erişim tarihi: 28/3/2019)

[116] **Küzeci**, s. 134.

[117] Ayrıca bkz. Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, par. 31.

Hassas kişisel veriler (§6): Kişinin ırksal kökenine, politik görüşlerine, dini inancına ilişkin verilerin yanı sıra sağlığına, cinsel yaşamına ve ceza mahkumiyetlerine ilişkin veriler iç hukukta gerekli önlemler alınmadığı sürece otomatik yollarla işlenemez.

Veri güvenliği (§7): Otomatik yollarla işlenen verilerin yok edilmesi, kaybedilmesi, yetkisiz erişim, değiştirilmesi veya yayımlanması gibi tehlikelere karşı uygun güvenlik önlemleri alınmalıdır.

Veri öznesi için ek güvenceler (§8): Veri öznesi; kendisine ilişkin otomatik yollarla işlenmiş verilerin varlığı ve veri sorumluları hakkında bilgi alma (§8/a), makul süre içinde verinin saklanıp saklanmadığına dair bilgi alma ve verinin kendisine gönderilmesini isteme (§8/b), verilerin düzeltilmesini veya ulusal hukuka aykırı işleme söz konusuysa silinmesini isteme (§8/c), taleplerinin reddedilmesi halinde hukuk yollarına başvurma (§8/d) haklarına sahiptir.

ETS 108, OECD Rehber İlkeleri'nden farklı olarak bağlayıcı nitelikte bir sözleşmedir ve Taraf Devletler açısından, Sözleşme ile öngörülen ilkeleri iç hukuklarına aktarma yükümlülüğü bulunmaktadır. Bu yükümlülük ifadesini, Sözleşmenin 4 üncü maddesinde bulmuştur.

Çıkış noktası Avrupa olsa dahi, ETS 108, Avrupa devletleri arasındaki bir anlaşmadan daha fazlası olarak planlanmıştır.[118] Nitekim 23 üncü maddede AK üyesi olmayan devletler için de Sözleşme'ye katılma imkanı tanınmıştır. 10 Nisan 2013 tarihinde Sözleşme'yi onaylayan Uruguay, AK üyesi olmadan Sözleşme'ye katılan ilk Devlet olmuştur.[119]

II.B.3.BM Rehber İlkeleri

BM Rehber İlkeleri ile, kişisel verilerin korunması kanunu bulunmayan BM Üyesi Devletleri bu kanunları kabul etmeye, uluslararası örgütleri ise kişisel verileri

[118] **Bygrave**, s. 333.

[119] Taraf devletlerin tam listesi için bkz. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=B16DdX3Y (Erişim tarihi: 28/3/2019)

bilinçli, meşru ve özel yaşamın gizliliğine saygılı bir şekilde işlemeye teşvik etmek amaçlanmıştır.[120] BM Rehber İlkeleri tavsiye niteliğinde olup, Üye Devletler açısından bir bağlayıcılığı bulunmamaktadır.[121]

BM Rehber İlkeleri'nin uygulama alanı, kamuya açık veya özel bilgisayarlarda bulunan, gerçek kişilere ilişkin verilerdir. Bununla birlikte, bilgisayarda tutulmayan veya elle işlenen verileri ya da tüzel kişilere ilişkin verileri de kapsayacak şekilde uygulama alanı genişletilerek iç hukuka dahil edilmesi de mümkündür (BM Rehber İlkeleri m. 10).

Tıpkı OECD Rehber İlkeleri ve ETS 108 gibi, BM Rehber İlkeleri de ulusal hukukta sağlanması gereken asgari güvenceleri belirlemektedir. On maddeden oluşan BM Rehber İlkeleri'nin öngördüğü ilkeler, hukuka uygunluk ve dürüstlük ilkesi (m. 1), doğruluk ilkesi (m. 2), amacın belirtilmesi ilkesi (m. 3), ilgili kişilerin erişimi ilkesi (m. 4), ayrımcılık yapmama ilkesi (m. 5) ve güvenlik ilkesidir (m. 7). Bu ilkelerin istisnaları 6 ncı maddede sayılmış, 8 inci maddede Üye Devletlerde ilkelerin uygulanmasının denetimi ve ilkelere aykırılık halinde uygulanacak yaptırımlar ve başvurulacak hukuki yolların nasıl düzenleneceği belirtilmiştir. İki ülke arasında hangi koşullar altında serbestçe sınırötesi veri akışı gerçekleştirilebileceği, 9'uncu maddede düzenlenmiştir.

BM Rehber İlkeleri, OECD Rehber İlkeleri ve ETS 108 ilkelerine kıyasla çok daha sınırlı bir etki yaratabilmiştir. Ancak doğrudan kişisel verilerin korunması üzerine ilk BM çalışması olması ve kişisel verilerin korunmasına ilişkin ilkelerin uygulanmasını denetleyecek yetkili ve bağımsız bir veri koruma organının kurulmasını öngören ilk uluslararası hukuk belgesi olması[122] yönünden önem arz etmektedir.

---

[120] **Bygrave**, s. 335.

[121] BM Rehber İlkeleri'nin tam metni için bkz. https://www.refworld.org/pdfid/3ddcafaac.pdf (Erişim tarihi: 28/3/2019)

[122] **Küzeci**, s. 126-127.

II.B.4.APEC Çerçeve Belgesi

APEC Çerçeve Belgesi, OECD Rehber İlkeleri'nden esinlenerek hazırlanmıştır, ancak APEC Çerçeve Belgesi'nde öngörülen ilkeler OECD Rehber İlkeleri ile birebir aynı değildir.[123] İlkeler üzerindeki çalışmalar APEC üyesi devletlerin Avrupa normlarına uymaksızın kişisel verilerin korunmasına yönelik kendi yaklaşımlarını geliştirmeye hazır olduklarını göstermektedir.[124]

APEC Çerçeve Belgesi ile, kişisel verilerin korunmasına ilişkin olarak, Üye Devletlerin üzerinde uzlaşması gereken asgari standartlar öngörülmüştür. Bu standartlar tavsiye niteliğinde olup, Üye Devletlerin iç hukuklarına aktarma zorunlulukları yoktur.

APEC Çerçeve Belgesi ile dokuz temel ilke öngörülmüştür. Diğer uluslararası belgelerde yer almayan bazı yeni ilkeler düzenlendiği gibi, diğer uluslararası belgelerde yer alan bazı ilkeler ayrıca düzenlenmemiş olup farklı ilkeler altında işlenmiş bulunmaktadır.[125] APEC Çerçeve Belgesi'nin temel ilkeleri kısaca şu şekildedir:

Zararın önlenmesi ilkesi (m. 14): Koruma, bireylerin kişisel verilerinin yanlış toplanmasından ve kullanılmasından kaynaklanan zararları önleyecek şekilde tasarlanmalıdır. İhlallere karşı başvurulabilecek hukuki yollar, zarar oluşma olasılığı ve zararın boyutuyla orantılı olmalıdır.

Bildirim (m. 15-17): Veri sorumluları, kişisel verilere ilişkin uygulamaları ve politikaları hakkında açık ve kolayca erişilebilir bildirimlerde bulunmalıdır. Bildirim, kişisel verilerin toplanmasından önce veya toplama anında, bu mümkün olmadığı takdirde mümkün olan en kısa sürede yapılmalıdır.

Veri toplamada sınırlılık (m. 18): Kişisel verilerin toplanması, toplama amacının gerektirdiği verilerle sınırlı olmalı; bu veriler hukuka uygun ve meşru

---

[123] **Cooper** / **Raul**, s. 29.

[124] **Bygrave**, s. 338.

[125] Örneğin "zararın önlenmesi ilkesi" APEC Çerçeve Belgesi'ne özgü bir ilke olup (bkz. **Küzeci**, s 151, dpn. 199), OECD Rehber İlkeleri'nde yer alan amacın belirtilmesi ilkesi ve açıklık ilkesi APEC Çerçeve Belgesi'nde düzenlenmemiştir. Bununla birlikte amaçla sınırlılık, kişisel verinin kullanımı ilkesi altında ele alınmıştır (bkz. **Cooper** / **Raul**, s. 29).

yollarla, uygun düştüğü hallerde ilgili bireyin bilgisi ve rızası dahilinde toplanmalıdır.

Kişisel verinin kullanımı (m. 19): Toplanan kişisel veriler sadece toplama amacı ve bununla uyumlu diğer amaçlar doğrultusunda kullanılmalıdır. İlgili bireyin rızası (m. 19/a), ilgili kişinin istediği bir ürün veya hizmetin sağlanmasında kişisel veriye ihtiyaç duyulması (m. 19/b) ve kanun veya başka bir hukuk normundan kaynaklanan yetki (m. 19/c) halleri bunun istisnalarıdır.

Seçim (m. 20): Uygun düştüğü ölçüde, bireyler için, kişisel verilerinin toplanması, kullanılması ve yayınlanmasına yönelik açık, ucuz ve kolay erişilebilir seçim mekanizmaları oluşturulmalıdır.

Kişisel verinin bütünlüğü (“integrity”) (m. 21): Kişisel veriler tam, doğru ve kullanım amacının gerektirdiği ölçüde güncel olmalıdır.

Güvenlik önlemleri (m. 22): Veri sorumluları, ellerindeki kişisel verileri, tehlikenin olasılığı, düzeyi ve verilerin hassasiyeti ile orantılı güvenlik önlemleri ile korumalıdır.

Erişim ve düzeltme (m. 23-25): İlgili kişiler, veri sorumlularından, ellerinde kendisine ilişkin kişisel verilerin bulunup bulunmadığını öğrenebilir, verilerin kendisine gönderilmesini isteyebilir, verilerin düzeltilmesini, tamamlanmasını, değiştirilmesini veya silinmesini talep edebilirler (m. 23). 24 üncü maddede istisna halleri sayılmış, 25 inci maddede ise, talepleri reddedilen kişilere ret gerekçelerinin açıklanması gerektiği belirtilmiştir.

Hesap verilebilirlik (m. 26): Veri sorumluları, yukarıda sayılan ilkeleri hayata geçirmek için alınan önlemlere uyulmasından sorumludur. Kişisel veriler başka kişi veya kurumlara aktarılacaksa, veri sorumlusu, aktarılan kişi ve kurumların bu kişisel verileri yukarıdaki ilkeler çerçevesinde koruyacağını güvence altına almak için gerekli özeni göstermeli ve gerekli adımları atmalıdır.

DÖRDÜNCÜ BÖLÜM
AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

I. 95/46/AT SAYILI DİREKTİF VE AB VERİ KORUMA REFORMU

I.A. Direktif'in Amacı

Direktif'in kabul edildiği 1995 yılına gelindiğinde, kişisel verilerin korunmasının anavatanı olan Avrupa'da zaten çoğu ülke kişisel verilerin korunması kanunlarını çok önceden hazırlamış ve yürürlüğe koymuş bulunmaktaydı. Ayrıca bağlayıcı bir AK sözleşmesi olan ETS 108 de çoğu Avrupa Devletince usulüne uygun olarak onaylanmış ve bu devletlerin iç hukukunun bir parçası haline getirilmişti. Avrupa'da kişisel verilerin korunması alanında ulusal ve uluslararası düzeyde belirli standartlara ulaşılmış olmasına karşın, AB bünyesinde yeni bir düzenlemeye, ulusal düzenlemelerde görülen farklılıkların, özellikle 7 Şubat 1992'de imzalanan, Maastricht Antlaşması olarak da anılan Avrupa Birliği Antlaşması[126] ile resmiyet kazanan "dengeli ve sürdürülebilir ekonomik ve sosyal gelişimin sağlanması amacıyla iç sınırların olmadığı bir alan yaratma (ortak pazar)" hedefi açısından engel oluşturacağı düşüncesi,[127] buna paralel olarak da Birlik üyesi ülkelerin veri koruma düzenlemeleri arasındaki farklılık ve çelişkilerin giderilmesi ve uyumun sağlanması adına açık ve kalıcı bir düzenleme yapılmak istenmesi[128] nedeniyle ihtiyaç duyulmuştur.

Direktif'in kabulünde AB'nin malların, kişilerin, sermayenin ve hizmetlerin serbest dolaşımı ilkesine dayanan bir ortak pazar oluşturma hedefi rol oynasa da, kişisel verilerin korunmasına yönelik bir düzenleme olması nedeniyle Direktif,

---

[126] Treaty on European Union, OJ C 191, 29 Temmuz 1992.

[127] **Küzeci**, s. 167, Murat **Uygun** (2010), Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması (Yayımlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, s. 33.

[128] **Yüksel Civelek**, s. 72.

doğası gereği bireylerin temel haklarının korunmasını da amaç edinmektedir. Bu husus Direktif metninde de ifade edilmiştir.[129]

Direktif'in iki amacı birbiriyle sanıldığından daha yakın bir ilişki içindedir. Üye Devletlerin hukuk sistemlerinin uyumlaştırılması tüm Üye Devletlerde yeterli bir koruma sağlayacak, bu sayede sınırötesi veri akışlarına insan hakları yönünden bir itiraz söz konusu olmayacaktır. Bununla birlikte, yakın geçmişe kadar uygulamada bu iki amaç eşit değerlendirilmemiş, ABAD, Direktif'in ekonomik amaçlarını ön planda tutan bir yaklaşım benimsemiştir. Bu durum özellikle 2009 yılında Lizbon Antlaşması'nın kabulü sonrasında değişmiş, Tüzük'ün hazırlık sürecinde bu yaklaşım benimsenmemiştir.[130]

I.B. Direktif'in Kapsamı

Direktif, 34 madde ve "Son Hükümler" dahil sekiz bölümden oluşmaktadır. İlk bölüm amaç, tanımlar, kapsam ve uygulanacak ulusal hukuku kapsayan genel hükümlere ayrıldıktan sonra, Direktif'te sırasıyla kişisel verilerin işlenmesinin hukuka uygunluğuna ilişkin genel kurallar (§5-21), hukuk yolları, sorumluluk ve yaptırımlar (§22-24), üçüncü ülkelere veri aktarımı (§25-26), davranış kuralları ("code of conduct") (§27), denetim kurumları ve Bireylerin Kişisel Verilerin İşlenmesi Karşısında Korunması Çalışma Grubu'nun (Madde 29 Çalışma Grubu) kurulması ve görevleri (§28-30) ile Avrupa Topluluğu düzeyinde alınacak önlemlerin belirlenmesi usulü (§31) düzenlenmiştir.[131]

Direktif'in en büyük yeniliğinin, Direktif'in uygulanmasını sağlamak üzere Üye Devletler yönünden bir kamu kurumunu (denetim kurumu, supervisory authority) görevlendirme yükümlülüğü getirmesi olduğu söylenebilir. Bunun dışında, kuruluşuna dayanak oluşturan maddenin adıyla anılan Madde 29 Çalışma Grubu da Direktif'in önemli yenilikleri arasındadır. Madde 29 Çalışma Grubu, Üye Devletlere

---

[129] Direktif, Gerekçe 3.

[130] **Lynskey**, *The Foundations*, s. 46 vd.

[131] Çalışmanın ana konusunu Tüzük oluşturduğundan ve Tüzük'ün Direktif ile benzerlik ve farklılık gösterdiği noktalar üzerinde durulurken Direktif'teki düzenlemelere de değinileceğinden ilgili düzenlemeler burada ayrıca incelenmemiştir.

ve Avrupa Komisyonu'na tavsiyelerde bulunmakla birlikte, Direktif'in Üye Devletlerce yeknesak şekilde uygulanmasını gözetmek ile görevlendirilmiştir.[132]

Direktif'in kapsamı ve konu yönünden uygulama alanı, 3 üncü maddede düzenlenmiştir. Anılan madde uyarınca Direktif, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesine ve bir veri kayıt sisteminin parçasını oluşturan ya da oluşturması amaçlanan kişisel verilerin otomatik olmayan yollarla işlenmesine uygulanır. Buna göre, tamamen veya kısmen otomatik yollarla işlenen kişisel veriler yönünden Direktif, ayrıca bir kriter aranmadan uygulama alanı bulacaktır. Elle işlenen veriler ise, ancak verilere kolay erişim imkanı sağlamak adına, bireylere ilişkin özel kriterler doğrultusunda şekillendirilmiş bir veri kayıt sistemi içerisinde saklanıyorsa ya da böyle bir sistem içerisinde saklanmak amacıyla toplanmış olmak koşuluyla Direktif kapsamına girer.[133]

Direktif, ABA'nın V. ve VI. Başlıkları kapsamındaki konular gibi Topluluk hukukunun konusunu oluşturmayan alanlar,[134] kamu güvenliği, ulusal savunma ve Devletin ceza hukuku kapsamındaki faaliyetleri ile gerçek kişilerin kişisel veya ailevi faaliyetleri yönünden uygulanmamaktadır (DPD §3/2).

Üye Devletlerin Direktif esasları doğrultusunda iç hukuk sistemlerinde benimsedikleri düzenlemeler, 4 üncü maddede sayılan hallerde uygulanacaktır.

I.C. AB Veri Koruma Reformu ve Tüzük ile Gelen Yenilikler

(AB) 2016/679 sayılı Tüzük ve (AB) 2016/680 sayılı Direktif'in kabulüne uzanan AB Veri Koruma Reformu, henüz öneri aşamasındayken bile hukuk ve iş

---

[132] **Develioğlu**, s. 11.

[133] Direktif, Gerekçe 15.

[134] ABA ile öngörülen AB, üç sütunlu bir yapıdan oluşuyordu. Birinci sütunu, kollektif olarak Avrupa Toplulukları adıyla anılan AKÇT, AAET ve bu Antlaşma ile Avrupa Topluluğu'na dönüştürülen AET oluşturmaktadır. İkinci sütun, ortak dış politika ve güvenlik politikasını, üçüncü sütun ise adli konularda ve içişlerinde işbirliğini temsil etmektedir. ABA'nın V. ve VI. Başlıkları, sırasıyla ikinci ve üçüncü sütunun alanına giren konuları düzenlemektedir. Üç sütun teorisi ile ilgili olarak bkz. Enver **Bozkurt** / Arif **Köktaş** (2018), Avrupa Birliği Hukuku, 7. Baskı, Legem, Ankara, s. 33 vd.

dünyasında geniş yankı bulmuş,[135] gündem oluşturmuştu. Kişisel verilerin korunması hukukuna dair bugüne kadarki en geniş kapsamlı reform çalışmalarının ürünü olan Tüzük, etkileri Avrupa'nın ötesinde de hissedilecek köklü yenilikler getirmiştir.

İlk bakışta dikkat çeken yenilik, kişisel verilerin korunmasına ilişkin esasların bir direktif ile değil, tüzük ile düzenlenmiş olmasıdır. Bu tercihte 95/46/AT sayılı Direktif'in, kişisel verilerin korunması düzenlemeleri yönünden Birlik içi yeknesaklığı sağlamakta yetersiz kalması etkili olmuştur. AB hukukunda direktifler, vardıkları sonuç yönünden Üye Devletler için bağlayıcıdır,[136] ancak Üye Devletlerde uygulanabilmeleri için ulusal uygulama işlemine ihtiyaç vardır.[137] Bunun anlamı, Üye Devletlerin direktif esaslarını iç hukuklarına aktarmalarıdır ki bunun hangi usul ve yöntemlerle yapılacağı Üye Devletlere bırakılmıştır (ABİA m. 288). Bunun doğal bir sonucu olarak, 95/46/AT sayılı Direktif, tüm Üye Devletler yönünden bağlayıcı esaslar getirse de, iç hukuka aktarma ve uygulama yönünden Üye Devletler arasında farklılıklar ortaya çıkması kaçınılmaz olmuştur. Tüzükler ise herhangi bir yasal veya idari düzenleme olmaksızın Üye Devletlerde uygulanabilen, bütünüyle bağlayıcı düzenlemelerdir[138] ve Birlik hukukunun tüm Üye Devletlerde aynı şekilde uygulanmasını sağlamanın bir aracıdır.[139] Bu anlamda direktif yerine tüzük tercih edilmesi, tüm Üye Devletlerde aynı kurallar aynı şekilde geçerli olacağı için, yorum farklılıklarının önüne geçmek ve yeknesaklığı sağlamak adına isabetli olmuştur.[140] Yeknesaklık, gerçek ve tüzel kişiler yönünden, tüm Üye Devletlerde farklı düzenlemeler ile karşı karşıya kalmak yerine, AB sınırları içerisinde geçerli tek bir

---

135 W. Gregory **Voss** (2012), "Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments", Business Law Today, s. 1.

136 **Bozkurt** / **Köktaş**, s. 185.

137 Lale Burcu **Önüt** (2017), Avrupa Birliği Hukukunun Üye Devletlerde Uygulanması, Seçkin, Ankara, s. 172.

138 **Önüt**, s. 170.

139 **Bozkurt** / **Köktaş**, s. 184.

140 Üye Devletlerin, yine Tüzük'te öngörülen koşul ve sınırlar çerçevesinde, Tüzük'te bulunmayan düzenlemeler getirme olanakları bulunduğu da ifade edilmelidir. Örneğin, Tüzük'ün 12 ila 22 nci maddeleri arasında veri öznelerine tanınan haklar, 23 üncü madde esaslarına uygun olarak Üye Devletlerce sınırlanabilmektedir. Bunun dışında Tüzük, ölen kişilerin kişisel verilerinin korunması örneğinde olduğu gibi, Üye Devletlere kimi hususlarda Tüzük'ten daha geniş kapsamlı düzenlemeler yapma imkanı tanımaktadır.

düzenleme çerçevesinde hareket etme kolaylığı sağlamıştır. Şirketlerin ve bireylerin 28 Üye Devletin farklı denetim kurumu yerine tek bir ulusal denetim kurumuyla muhatap olmasını ifade eden tek durak ilkesi ("one-stop-shop") de yeknesaklığı sağlamak üzere atılan adımlar arasındadır.[141]

Tüzük ile gelen bir diğer önemli yenilik, Madde 29 Çalışma Grubu'nun yerine geçmek üzere[142] Avrupa Veri Koruma Kurulu'nun ("European Data Protection Board") oluşturulmasıdır. Avrupa Veri Koruma Kurulu, Üye Devletlerin denetim kurumlarının başkanları ile Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor) veya bunların temsilcilerinden oluşan (GDPR §68/3), tüzel kişiliği haiz (GDPR §68/1), bağımsız (GDPR §69) bir kurumdur. Avrupa Veri Koruma Kurulu'nun oluşturulmasının, Tüzük'ün AB sınırları içerisinde etkin bir şekilde uygulanmasını güvence altına alma ve Üye Devletler arasında bu yönde işbirliğini sağlama hedeflerine yönelik bir yenilik olduğu söylenebilir. Bu çerçevede, Tüzük'ün 63 vd. maddelerinde getirilen diğer bir yenilik olan istikrar mekanizması ("consistency mechanism") da önem arz etmektedir.

Tüzük ile veri sorumlularının ve veri işleyenlerin sorumlulukları artırılırken, veri öznelerine kişisel verileri üzerinde daha fazla kontrol imkanı sağlanmıştır.[143] Veri sorumluları ve veri işleyenler açısından veri koruma yetkilisi ("data protection officer") atama, veri koruma etki değerlendirmesi yapma ("data protection impact assessment") ve ön danışma gibi yükümlülükler öngörülürken, tasarımsal gizlilik ("privacy by design") ve varsayılan gizlilik ("privacy by default") gibi yeni ilkeler kabul edilmiştir.[144] Bu ilkeler, veri işleme sürecinin başlangıçtan itibaren, kişisel verilerin korunmasına öncelik verilecek şekilde yürütülmesini amaçlar. Bu

---

[141] Nilgün **Başalp** (2015), "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 21, S. 1, s. 86.

[142] **Başalp**, s. 86, dpn. 31.

[143] **Develioğlu**, s. 13.

[144] "Tasarımsal gizlilik" ve "varsayılan gizlilik" yerine doktrinde "başlangıçtan itibaren veri korunması" ve "tasarımdan itibaren veri korunması" (bkz. **Develioğlu**, s. 101-102), "tasarımda gizlilik" ve "varsayılan gizlilik" (bkz. **Küzeci**, s. 203), "tasarımla veri koruma ve varsayılan ayarlarla veri koruma" (bkz. **Başalp**, s. 92) gibi farklı terimler de kullanılmaktadır. Çalışmamızda, "privacy" kelimesinin doğrudan karşılığının "gizlilik" olması ve ilkelerden, gizliliğin sağlanmasının tasarımın doğal bir sonucu olması gerektiğinin anlaşılması nedeniyle "tasarımsal gizlilik" ve "varsayılan gizlilik" terimleri tercih edilmiştir.

doğrultuda, veri işleme sistemlerinin yanı sıra ürün ve hizmetler, verilerin gizliliğini güvence altına alacak şekilde tasarlanmalıdır. Veri özneleri açısından ise, rızanın şartlarının daha ağır ve daha açık şekilde düzenlendiği, unutulma hakkı başta olmak üzere yeni haklar ve güvenceler getirildiği görülmektedir.

II. (AB) 2016/679 SAYILI AB VERİ KORUMA TÜZÜĞÜ'NDE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ESASLAR

II.A.Tüzük'ün Uygulama Alanı

Tüzük'ün ilk maddesi, Tüzük'ün amaçlarını ve konusunu düzenler. Buna göre Tüzük, gerçek kişilerin kişisel verilerin işlenmesi karşısında korunmasına ve kişisel verilerin serbest dolaşımına ilişkin kuralları belirler. Gerçek kişilerin, kişisel verilerinin korunması başta olmak üzere temel hak ve özgürlüklerini koruma altına alır. Dolaysıyla, Tüzük'ün kişi yönünden uygulama alanına gerçek kişilerin dahil olduğu anlaşılmaktadır.

Tüzük; konu, yer ve zaman yönünden uygulama alanını da ayrıca düzenlemiş bulunmaktadır. Buna göre, Tüzük'ün konu yönünden uygulama alanı GDPR §2, yer yönünden uygulama alanı GDPR §3, zaman yönünden uygulama alanı GDPR §99 esasları çerçevesinde belirlenecektir.

II.A.1.Konu Yönünden Uygulama Alanı

Tüzük, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesine ve bir veri kayıt sisteminin parçasını oluşturan ya da oluşturması amaçlanan kişisel verilerin otomatik olmayan yollarla işlenmesine uygulanır (GDPR §2/1). Direktif'in aynı yöndeki düzenlemesinde olduğu gibi (DPD §3), burada da ikili bir ayrım söz konusudur. Tüzük, tamamen veya kısmen otomatik yollarla işlenen kişisel veriler yönünden, ayrıca bir kriter aranmadan uygulama alanı bulur. Elle işlenen veriler yönünden ise, ancak verilere kolay erişim imkanı sağlamak adına, bireylere ilişkin özel kriterler doğrultusunda şekillendirilmiş bir veri kayıt sistemi içerisinde

saklanıyor olma ya da böyle bir sistem içerisinde saklanmak amacıyla toplanmış olma koşulu aranır.[145]

Tüzük, GDPR §2/2'de sayılan hallerde uygulama alanı bulmaz. Buna göre, kişisel verilerin, Birlik hukukunun kapsamı dışında kalan bir faaliyet doğrultusunda (GDPR §2/2-a), Üye Devletlerin ABA'nın V. Başlığı'nın 2. Bölümü kapsamındaki faaliyetleri sırasında[146] (GDPR §2/2-b), gerçek kişilerce tamamen kişisel veya ailevi bir faaliyet esnasında (GDPR §2/2-c) ve yetkili makamlar tarafından kamu güvenliğine karşı tehditlerin önlenmesi ve bunlara karşı tedbirler alınması da dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infazı kapsamında işlenmesi (GDPR §2/2-d) hallerinde Tüzük uygulanmayacaktır.

Tüzük, kişisel verilerin AB organ, kurum ve kuruluşlarınca işlenmesi hallerinde de uygulanmamaktadır. Bu hallerde, (AT) 45/2001 sayılı Tüzük'ün[147] uygulanacağı, ancak anılan Tüzük ve kişisel verilerin bu şekilde işlenmesine uygulanan diğer AB düzenlemelerinin GDPR §98 doğrultusunda GDPR ile öngörülen ilke ve kurallara uygun hale getirileceği ifade edilmişti (GDPR §2/3). (AT) 45/2001 sayılı Tüzük, (AB) 2018/1725 sayılı ve 23 Ekim 2018 tarihli Tüzük'ün[148] 99 uncu maddesi uyarınca 11 Aralık 2018 itibariyle yürürlükten kaldırılmış bulunmaktadır. Bu tarihten itibaren GDPR §2/3 kapsamında kişisel veri işlenmesine (AB) 2018/1725 sayılı Tüzük uygulanmaktadır.

Tüzük, 2000/31/AT sayılı E-Ticaret Direktifi'nin, özellikle 12 ila 15. inci maddeleri arasında yer alan, aracı hizmet sağlayıcılarının sorumluluğuna ilişkin kurallarının uygulanmasına etki etmeyecektir (GDPR §2/4).

---

[145] Tüzük, Gerekçe 15.

[146] Anılan bölümde AB Ortak Dış Politika ve Güvenlik Politikası esasları düzenlenmiştir.

[147] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[148] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21 Kasım 2018.

II.A.2. Yer Yönünden Uygulama Alanı

II.A.2.a) Genel Olarak

Yer yönünden uygulama alanına ilişkin özel hükümler öngörmeyen Direktif'ten farklı olarak,[149] Tüzük, yer yönünden uygulama alanına ilişkin esasları üçüncü maddesinde düzenlemiştir. Anılan maddenin birinci fıkrasına göre, Tüzük, kişisel verilerin işlenmesinin, veri sorumlusu veya veri işleyenin AB sınırları içerisindeki bir kuruluşunun faaliyetleri kapsamında gerçekleştirildiği hallerde uygulanacaktır. İşlemenin fiziken AB sınırları içerisinde gerçekleşip gerçekleşmediğinin bir önemi yoktur. Kişisel verileri işlenen gerçek kişilerin AB vatandaşı olması da zorunlu değildir. Hatta veri sorumlusu ya da veri işleyen tamamen AB dışındaki kişilerin verilerini işlese dahi, veri işleme faaliyetini AB sınırları içerisinde gerçekleştirdiği takdirde, Tüzük hükümlerine uymak zorundadır.[150]

Avrupa Veri Koruma Kurulu, Tüzük'ün yer yönünden uygulama alanına ilişkin 3/2018 sayılı Rehber İlkeleri'nde, kuruluş kriterinin nasıl yorumlanacağını açıklığa kavuşturmuştur.[151] Buna göre, ilk olarak, GDPR §3/1 anlamında bir "kuruluş" bulunup bulunmadığı belirlenmelidir. Bu belirlemede esas alınabilecek bir kuruluş tanımı Tüzük'te yer almamakla birlikte, Tüzük'ün gerekçesinde, kuruluş ifadesinden süreklilik arz eden bir düzen içerisinde etkili ve somut faaliyetlerin anlaşılacağı ifade edilmiştir. Bu düzenin hukuki statüsü (örneğin tüzel kişiliğinin bulunup bulunmadığı) dikkate alınmaz.[152] Aynı ifadeye Direktif'te de yer verilmişti.[153]

---

[149] DPD §4 ile, Üye Devletlerin iç hukuklarına aktardıkları Direktif esaslarına ilişkin düzenlemelerinin yer yönünden uygulama alanı düzenlenmiştir.

[150] Mesut Serdar **Çekin** (2018), Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha, İstanbul, s. 29-30.

[151] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

[152] Tüzük, Gerekçe 22.

[153] Direktif, Gerekçe 19.

Veri sorumlusunun veya veri işleyenin, AB sınırları içerisinde bir kuruluşunun varlığı tespit edildikten sonra, işlemenin bu kuruluşun faaliyetleri kapsamında gerçekleşip gerçekleşmediği belirlenmelidir. Tüzük'te işlemenin kuruluş tarafından değil de kuruluşun faaliyetleri kapsamında yapılmasından söz edildiğine dikkat edilmelidir. Veri sorumlusu ve veri işleyen, işleme doğrudan kuruluş eliyle yapılmasa dahi, kuruluşun faaliyetleri kapsamında yapılıyorsa, Tüzük'e tabi olurlar. Bu ifadeden ne anlaşılması gerektiği, somut olayın koşullarına göre belirlenecektir.[154] Örneğin, Türkiye'de faaliyet gösteren bir veri sorumlusunun ya da veri işleyenin, AB sınırları içerisinde veri işlemek dışında bir amaçla kurulmuş olsa dahi, bir kuruluşu mevcutsa ve bu kuruluşun esas işi ile doğrudan ilişkili bir veri işleme faaliyeti söz konusuysa, Tüzük uygulama alanı bulacaktır. Bu yönde, ABAD'ın Google Spain kararı önem arz etmektedir.[155] Karara konu olan olayda, Google Inc., ABD merkezli bir tüzel kişi olup, Google Spain, Google Inc.'in reklam ürün ve hizmetlerinin satış ve promosyon faaliyetlerini gerçekleştirmek üzere kurulmuş, ayrı tüzel kişiliği haiz bir alt kuruluştur. ABAD, Google Spain tarafından yürütülen pazarlama faaliyetleri ile Google Inc. tarafından arama motorunun (Google Search) işletilmesi arasında ekonomik anlamda yakın bir ilişki bulunduğu ve arama motorunun sadece önceden işlenmiş verileri gösterdiği ve bu veriler üzerinde herhangi bir işlem yapmadığı halde arama motoru işleten tüzel kişilerin veri sorumlusu tanımı içerisinde yer aldığı değerlendirmesinde bulunmuş ve Google Spain'in veri işleyen olarak AB hukuku çerçevesinde sorumlu olacağını kabul etmiştir. Esas etkisi unutulma hakkı açısından görülmekle birlikte,[156] karar, kuşkusuz Tüzük'ün yer yönünden uygulama alanının ne şekilde yorumlanacağının tespiti bakımından da önemli bir etki doğurmuştur.[157]

---

[154] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), s. 6.

[155] *Google Spain SL and Google Inc*. v *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, 13 Mayıs 2014. - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (Erişim tarihi: 17/4/2019)

[156] Kararın unutulma hakkı açısından etkisi aşağıda değerlendirilecektir.

[157] Aynı yönde diğer önemli bir karar için bkz. *Weltimmo s.r.o.* v *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, 1 Ekim 2015. - http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2863454 (Erişim tarihi: 17/4/2019)

Veri sorumlusunun veya veri işleyenin AB sınırları içerisinde bir kuruluşunun ve bu kuruluşun faaliyetleri kapsamında gerçekleşen bir kişisel veri işleme faaliyetinin varlığı halinde, Tüzük, bu verilerin fiziksel işleme yerinin AB sınırları içerisinde bulunup bulunmadığından bağımsız olarak uygulanacaktır. Örneğin, Estonya merkezli bir bilişim şirketi, AB sınırları içerisinde sunduğu bir hizmetini Türkiye'de de sunmaya karar verdiği takdirde, Türkiye'deki müşterilerin kişisel verilerinin toplanması ve işlenmesi Türkiye'de gerçekleşse dahi, AB sınırları içerisinde yer alan bir kuruluşun faaliyetleri kapsamında yürütüldüğünden, Tüzük'ün uygulama alanı içerisindedir.

II.A.2.b)AB Sınırları Dışındaki Veri Sorumluları ve Veri İşleyenler Yönünden Uygulama

Veri sorumlularının veya veri işleyenlerin GDPR §3/1 anlamında AB sınırları içerisinde bir kuruluşu bulunmadığı takdirde, GDPR §3/2 ve 3/3 düzenlemeleri dikkate alınacaktır. Özellikle GDPR §3/2, uygulamada daha sık rastlanan ve AB'nin ekonomik hedefleri ile de ilişkili bir düzenlemedir. Anılan düzenleme, AB içerisinde kuruluşu bulunmayan bir veri sorumlusu veya veri işleyen tarafından, AB sınırları içerisindeki veri öznelerinin kişisel verilerinin, bu kişilerce bir ücret ödenmesi gereksin gerekmesin bu kişilere bir ürün veya hizmet teklifinde bulunulması (GDPR §3/2-a) ya da bu kişilerin AB sınırları içerisindeki davranışlarının izlenmesi ("monitoring") (GDPR §3/2-b) ile ilişkili olacak şekilde işlenmesi hallerinde uygulanacaktır. AB sınırları içinde bulunan gerçek kişilere yönelik hedefleme ("targeting")[158] uygulamalarına yönelik olan bu düzenleme, Tüzük'ün yer yönünden uygulama alanını genişletmeye elverişlidir.[159]

GDPR §3/2 düzenlemesinin uygulama alanının incelenmesinde ilk olarak, "AB sınırları içerisindeki veri özneleri" ifadesinin kapsamı belirlenmelidir. Bu ifadeden sadece AB vatandaşları ve AB'de ikamet eden veri özneleri mi

---

[158] Hedefleme, en basit tanımıyla, pazarı müşteri gruplarına ayırdıktan sonra hangi müşteri grubuna hizmet edileceğinin seçilmesidir. - Philip **Kotler** / Gary **Armstrong** (2011), Principles of Marketing, 14. Baskı, Pearson, s. 188.

[159] **Çekin**, s. 31.

anlaşılmalıdır? Yoksa herhangi bir nedenle, geçici olarak AB sınırları içinde bulunan, uyruğu ve ikametgâhı AB dışındaki bir gerçek kişi de bu madde kapsamında mı değerlendirilecektir? Gerek Tüzük'ün gerekçesi,[160] gerekse Avrupa Veri Koruma Kurulu,[161] ikinci yorumu işaret etmektedir. Buna göre, örneğin, iş nedeniyle veya turistik gezi amaçlı olarak geçici süreliğine bir AB ülkesinde bulunan bir Türk vatandaşı, bu madde kapsamında AB sınırları içerisindeki bir veri öznesidir.

"AB sınırları içerisindeki veri özneleri" ile kimlerin ifade edildiğinin açıklığa kavuşturulmasının ardından, ürün veya hizmet teklifinin ya da izleme faaliyetinin bu kişileri hedefleyip hedeflemediği tespit edilmelidir. Ürün veya hizmet teklifi söz konusu ise, tekliften, teklifte bulunan kişinin AB sınırları içerisinde yer alan kişilerle bir hukuki ilişki kurma iradesinin varlığı anlaşılmalıdır. AB sınırları içerisinde veri sorumlusunun internet sayfasına ya da e-posta adresi veya diğer iletişim bilgilerine ulaşılabilmesi, böyle bir iradeden söz etmek için yetersizdir; aynı şekilde, veri sorumlusunun veya veri işleyenin kuruluşunun bulunduğu bir ülkenin dilinin kullanılması da bu iradenin yokluğu yönünde fikir oluşturmaktadır. Bununla birlikte, AB sınırları içerisinde konuşulan bir veya birden fazla dilin kullanılması,[162] bir veya birden fazla Üye Devletin para birimi ile ödeme kabul edilmesi veya AB sınırları içerisindeki müşterilerden bahsedilmesi, veri sorumlusunun, AB sınırları içerisindeki veri öznelerine ürün veya hizmet teklifinde bulunma iradesinin bir göstergesi olabilir.[163]

---

[160] Tüzük, Gerekçe 14.

[161] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), s. 13.

[162] Bu husus çoğu zaman veri sorumlusu açısından ilgili iradenin varlığı yönünde kanaat oluştursa da, diğer hususlar gözetilmeden bu yorumun yapılması yanıltıcı olabilir. Örneğin, İngilizce, AB dışında da yaygın konuşulan bir dildir ve sadece dolar üzerinden ödeme kabul eden, ABD dışına ürün satışı yapmayan bir internet sitesi, AB sınırları içinde konuşulan bir dil kullanılmış olmasına rağmen, AB sınırları içindeki veri öznelerinin hedeflenmediği açıktır. AB ülkelerinden sipariş kabul etmekle birlikte özellikle bu ülkelerdeki müşterileri hedef alan reklam faaliyetleri bulunmayan, ayrıca Üye Devletlerce kullanılan para birimleriyle ödeme kabul etmeyen bir internet sitesi yönünden ise, ürün veya hizmet teklifinin özellikle AB sınırları içerisindeki veri öznelerini hedeflediği yönünde yeterince güçlü bir kanaat oluşturmak mümkün olmadığından Tüzük bu internet sitesinin kişisel veri işleme faaliyetlerine uygulanmayacaktır, bkz. Tüzük, Gerekçe 23; **Çekin**, s. 32-33.

[163] Tüzük, Gerekçe 23.

Davranışların izlenmesi hali açısından ise, amacının bir önemi olmaksızın izlemenin gerçekleşmesi, izlenen davranışların AB sınırları içerisinde gerçekleşmesi koşuluyla, Tüzük'ün uygulanması için yeterlidir. İzleme çeşitli yollarla yapılabilmektedir, ancak kişilerin internet kullanımı kuşkusuz bu anlamda özel bir öneme sahiptir; nitekim Tüzük de gerekçesinde sadece kişilerin internette izlenmesinden söz etmektedir.[164] Bununla birlikte, Tüzük'ün internet hareketlerinin izlenmesi dışındaki hallerde, örneğin yaşlı ve hastalara yardımcı olmak amacıyla tasarlanmış bir sistem aracılığıyla bu kişilerin sağlık durumunun takip edilmesinde, uygulama alanı bulmayacağı şeklinde bir yorum yanlış olur. GDPR §2/3-b düzenlemesinde ya da Gerekçe'de, AB sınırları içerisindeki gerçek kişilerin hedeflenmesi yönünde bir ifade yer almamaktadır, ancak "izleme" ifadesinden veri sorumlusunun belli bir amacı olduğu ve topladığı kişisel verileri bu amaç doğrultusunda kullanacağı anlaşılmaktadır.[165] Kişinin sevdiği ya da sevmediği şeyler, alışkanlıkları hakkında analiz yapılıyor ya da tahminde bulunuluyorsa, gözlemleme faaliyeti gerçekleşmiş sayılacaktır.[166] Gerçekten de, özellikle internet sayfalarında, kişilerin önceki ziyaret ettiği sayfalar veya ilgi alanları ile ilişkili reklamlar gösterilmesi, bir "hedefleme"nin var olduğunun işaretidir. Yaşlı ve hastaların sağlık durumunun takip edilmesi örneğinde, hedeflemenin varlığı daha kolay anlaşılabilmektedir, izleme amaçları ve izlenen kişi belirgindir.

Son olarak, GDPR §3/3 düzenlemesinin üzerinde durmak gerekir. Anılan düzenlemeye göre, veri sorumlusunun AB sınırları içerisinde bir kuruluşu bulunmamakla birlikte, uluslararası hukukun gereği olarak Üye Devletlerin hukukunun uygulandığı bir yerde bulunuyorsa, Tüzük uygulama alanı bulur. Bunun tipik örneği elçiliklerdir. Örneğin, Romanya'nın Türkiye'deki elçilikleri, AB sınırları içerisinde yer almamakla birlikte, uluslararası hukuk ilkeleri uyarınca bu elçiliklerde Romanya hukuku geçerlidir ve bu elçiliklerin kişisel veri işleme faaliyetleri Tüzük'e tabi olacaktır. Aynı şekilde, uluslararası hukuk kuralları çerçevesinde gemiler, tescilli oldukları ve bayrağını taşıdıkları ülkenin toprağı kabul edilmektedirler. Dolayısıyla,

---

[164] Tüzük, Gerekçe 24.

[165] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), s. 18.

[166] **Çekin**, s. 32.

uluslararası sularda, bir Üye Devletin bayrağını taşıyan gemilerde kişisel verilerin işlenmesine Tüzük uygulanacaktır.[167]

II.A.3.Zaman Yönünden Uygulama Alanı

Tüzük, 99 uncu maddesinde, Avrupa Birliği Resmi Gazetesi'nde yayımlanmasını izleyen yirminci günde yürürlüğe gireceğini düzenlemiştir. Yukarıda belirtildiği gibi, Tüzük, 4 Mayıs 2016 tarihli Avrupa Birliği Resmi Gazetesi'nde yayımlanmıştır, dolayısıyla 24 Mayıs 2016 itibariyle yürürlüktedir. Aynı madde, Tüzük'ün uygulama tarihini ise 25 Mayıs 2018 olarak belirlemiştir. Bu tarihe kadar Direktif uygulanmaya devam etmiştir. Uygulama için daha ileri bir tarih öngörülmesinin amacı, Üye Devletlere, Tüzük'ün sorun yaşanmadan uygulanmaya başlanması için gerekli hazırlıkları yapmak üzere süre tanınmasıdır. 25 Mayıs 2018 tarihi itibariyle Direktif'in uygulaması sona ermiştir ve Tüzük, tüm Üye Devletler için doğrudan ve tümüyle bağlayıcı olacak şekilde yürürlüktedir.

Tüzük, yürürlüğe girmesinden sonra, Üye Devletlerin Direktif döneminde yaptıkları, üçüncü ülkelere veya uluslararası örgütlere veri aktarımına yönelik uluslararası sözleşmelerin akıbetinin ne olacağını da düzenlemiştir. Buna göre, Tüzük'ün yürürlük tarihinden önce, dönemin mevzuatına uygun olarak yapılmış sözleşmeler, üzerinde değişiklikler yapılıncaya, değiştirilinceye ya da kaldırılıncaya kadar yürürlükte kalacaktır (GDPR §96).

II.B.Kişisel Verilerin İşlenmesine Hakim Olan İlkeler

Çalışmamızın ikinci bölümünde, kişisel verilerin işlenmesine yönelik ilkelerin, konuya yönelik farklı belgelerde, farklı tarzlarda ele alınışı üzerinde durulmuştu. Bu belgeler incelendiğinde, farklı kapsam ve bağlamlarda esasen ortak ilkelerden söz edildiği görülmektedir. Bu ilkeler, kişisel verilerin korunması hukukunun dayandığı temel ilkeler olup, kaçınılmaz olarak Tüzük'te de yer almıştır. Tüzük'ün uygulama alanı bulduğu hallerde, bu ilkelere uyulmadığı takdirde hukuka

[167] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), s. 19.

uygunluk koşullarının varlığına rağmen hukuka aykırı bir işlemeden söz edilecektir.[168]

Kişisel verilerin işlenmesine hakim olan ilkeler Tüzük'ün 5 inci maddesinde, hukuka uygunluk, dürüstlük ve şeffaflık ilkesi, amacın sınırlanması ilkesi, veri minimizasyonu ilkesi, doğruluk ilkesi, saklamanın sınırlanması ilkesi, bütünlük ve gizlilik ilkesi ve hesap verilebilirlik ilkesi olarak sayılmıştır.

II.B.1.Hukuka Uygunluk, Dürüstlük ve Şeffaflık İlkesi

Hukuka uygunluk, dürüstlük ve şeffaflık ilkesi, GDPR §5/1-a'da düzenlenmiştir. Bu üç kavram farklı ilkeleri ifade etmekle birlikte, tek bir ilke olarak kabul edilebilecek kadar iç içedir. Dürüstlük ve şeffaflık ilkelerine uygunluk, hukuka uygunluğun bir gereği olmakla birlikte, hukuka uygunluğun veya şeffaflığın bulunmadığı yerde dürüstlükten de söz edilemez.

Hukuka uygunluk ve dürüstlük, Direktif'te de temel bir ilke olarak yer almaktaydı (DPD §6/1-a). OECD Rehber İlkeleri (m. 7), 108 sayılı AK sözleşmesi (§5/a), BM Rehber İlkeleri (m. 19) ve APEC Çerçeve Belgesi (m. 18) de kişisel verilerin hukuka uygun ve meşru yollarla toplanması ve işlenmesi gerektiğini ifade etmektedir. Bu ilke Türk hukukunda da kabul edilmiştir (KVKK m. 4/2-a). Şeffaflık ise ilk defa Tüzük ile düzenlenmiş olup, bu ilkenin bir parçası haline getirilmiştir.

Hukuka uygunluk ile kastedilenin Tüzük, ulusal kanunlar ve diğer bağlayıcı hukuk normlarına aykırılığın bulunmaması olduğu kuşkusuzdur. Hukuka uygunluğun bir koşulunun da kişisel verilerin korunmasının temel ilkelerine uygunluk olduğu göz önüne alındığında, diğer tüm ilkelerin bu ilke ile doğrudan ilişkili olduğu sonucuna ulaşılacaktır. Nitekim hukuk kurallarının bir amacı da ilkelerin nasıl uygulanacağını belirlemek, ilkeleri somutlaştırmaktır.

Dürüstlük, bir kimseden namuslu, dürüst ve makul bir insan olarak beklenen davranışı ifade eder.[169] Dürüstlük kuralı, hukukun başlıca evrensel ilkelerinden olup Türk hukukunda ifadesini, TMK m. 2'de bulmuştur. Kişisel verilerin işlenmesinde,

---

[168] **Develioğlu**, s. 44.

[169] Kemal **Oğuzman** / Nami **Barlas** (2013), Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar), 19. Baskı, Vedat, İstanbul, s. 253.

veri sorumlularının dürüstlük kuralına uygun hareket etmesi gerektiği bir gerçek olmakla birlikte, kişisel verilerin korunması hukuku bağlamında "dürüstlük" daha özel bir anlamı karşılamaktadır.[170] Tüzük de dahil olmak üzere, uluslararası belgelerde, buradaki anlamıyla dürüstlüğü ifade etmek üzere "fair" (adil) sözcüğü kullanılmıştır. Veri sorumluları, veri öznelerine karşı adil bir tutum içerisinde olmalı, bu kişilerin menfaatlerini ve makul beklentilerini dikkate almalı, tarafların menfaatleri arasında bir denge gözetilmelidir.[171]

Şeffaflık; kişisel verilerin işlenmesine ilişkin her türlü bilgi ve açıklamanın kolay ulaşılabilir ve kolay anlaşılır olması, açık ve sade bir dil kullanılarak ifade edilmesidir.[172] Şeffaflığın bu ilkenin bir parçası olarak düzenlenmesi, Direktif'teki düzenlemenin iyileştirilmesi şeklinde yorumlansa da,[173] yukarıda belirtildiği gibi, zaten şeffaflığın bulunmadığı yerde dürüstlük ilkesine uygunluktan söz etmek oldukça güç olacaktır. Veri sorumlularının, veri işleme sürecine ilişkin bilgileri veri özneleriyle paylaşmaması, dürüstlük ilkesinin gerektirdiği menfaat dengesinin mevcudiyetini şüpheli hale getirecektir. Şeffaflık ilkesi kapsamında veri sorumlularının veri özneleri ile paylaşmaları gereken bilgiler, Tüzük'ün 13 ve 14 üncü maddelerinde düzenlenmiştir.

---

[170] **Çekin**, s. 45.

[171] **Çekin**, s. 45, **Küzeci**, s.207-208.

[172] Tüzük, Gerekçe 39.

[173] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the data protection reform package, par. 114. - http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf (Erişim tarihi: 20/4/2019), **Develioğlu**, s. 45.

II.B.2.Amacın Sınırlanması İlkesi

İfadesini GDPR §5/1-b'de bulan amacın sınırlanması ilkesi[174] uyarınca, kişisel veriler belirli, açık ve meşru amaçlarla toplanmalı, bu amaçlara aykırı olacak şekilde işlenmemelidir. Bu tanımdan hareketle, ilkenin üç unsuru amacın belirli ve açık olması, amacın meşru olması ve işlemenin amaca uygun olması olarak sayılabilir.[175]

Amacın belirli ve açık olması, Tüzük'ün 13 ve 14 üncü maddelerinin de bir gereğidir. Anılan maddeler uyarınca, kişisel verilerin işlenme amacı ve yasal dayanağı, veri sorumlularının veri özneleri ile paylaşması gereken bilgiler arasındadır (GDPR §13/1-c, 14/1-c). Amaç, kişisel verilerin işlenmesinin hukuka uygunluğunun belirlenmesinde rol oynayacağı gibi, veri sorumlusunun alması gereken güvenlik önlemlerinin yeterliliği de belirlenen amaç veya amaçlar çerçevesinde değerlendirilecektir.[176] Amaç, en geç kişisel verilerin toplanması anında belirlenmiş ve veri öznesine, kuşkuya ve yoruma yer bırakmayacak şekilde açıklanmış olmalıdır. Gelecekte ortaya çıkması olası bir amaca dayanılarak veri toplanamaz. Küzeci'ye göre, kişisel verilerin gelecekte ihtiyaç duyulabilecekleri düşüncesiyle saklanması, bütün bir toplumu potansiyel suçlu konumuna sokar.[177] Bu husus aşağıda incelenecek olan veri minimizasyonu ilkesi ile de yakından ilgilidir.

Amacın meşru olması, kişisel verilerin yasal bir dayanağa istinaden toplanmasını ve bu yasal dayanaklar ile getirilen esas ve ilkelere aykırı olmayan bir amaç doğrultusunda işlenmesini ifade eder. Tüzük'e göre kişisel verilerin işlenmesi,

---

[174] Bu ilke "amaçla sınırlı olma" (bkz. **Develioğlu**, s. 45, Ayşe Nur **Akıncı** (2017), Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, T.C. Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, s. 8), "amaca bağlılık" (bkz. **Çekin**, s. 45), "belirli, açık ve meşru amaçlar için toplanma" (bkz. **Küzeci**, s. 208), "belirli amacın bulunması ve amaca bağlı kalınması" (bkz. **Akgül**, s. 154, 156) olarak da ifade edilmektedir. OECD Rehber İlkeleri m. 9 ve BM Rehber İlkeleri m. 3, "amacın belirtilmesi" ("purpose specification") terimini kullanırken, KVKK m. 4/2-c, "belirli ve meşru amaçlar için işlenme" ifadesini tercih etmiştir.

[175] Aynı yönde bkz. **Küzeci**, s. 208.

[176] **Çekin**, s. 46.

[177] **Küzeci**, s. 209.

6 ncı maddede sayılan hallerde meşru ve hukuka uygun olacaktır.[178] Bu hukuka uygunluk halleri aşağıda incelenecektir.

İşlemenin amaca uygun olması, kişisel verilerin toplandıktan sonra belirtilen amaçla uyumlu olmayan farklı bir amaçla işlenmemesi ve işlemenin, belirtilen amacın gereklerine uygun bir şekilde yapılmasıdır. Buna göre, belirtilen amaç dışındaki amaçlarla da işleme yapılabilir, ancak bunun için yeni amaç, ilk amaçla bağdaşıyor olmalıdır. Bu koşulun gerçekleşip gerçekleşmediği, diğer ilkeler de göz önünde tutularak yorumlanmalıdır. Tüzük'te ayrıca, 89 uncu maddenin 1 inci fıkrasında öngörülen önlemlerin alınmış olması koşuluyla, kamu yararı, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla yapılacak sonraki işlemelerin, ilk amaçla uyumsuz sayılmayacağı şeklinde bir istisna hali düzenlenmiştir (GDPR §5/1-b).

Son olarak, amaç değişikliği üzerinde durmak gerekir. Kimi hallerde, ilk belirtilen amacın değişmesi söz konusu olabileceği gibi, ihtiyaçlar doğrultusunda yeni amaçlar da doğabilir. Direktif, amaç değişikliğinin hangi esaslara göre yapılacağını düzenlememişti. Tüzük'e göre ise, kural olarak, yeni amaçlar yönünden veri öznesinin rızası aranır. Şayet amaç değişikliği veri öznesinin rızasına dayanmıyorsa, veri sorumlusu, GDPR §6/4 çerçevesinde bir değerlendirme yaparak yeni amacın ilk amaçla uyumlu olup olmadığını belirlemelidir. Buna göre, kişisel verilerin toplandığı ilk amaç ile sonraki işlemenin amacı arasındaki her türlü bağlantı (GDPR §6/4-a), kişisel verilerin toplandığı bağlam ve özellikle veri özneleri ile veri sorumlusu arasındaki ilişki (GDPR §6/4-b), kişisel verinin yapısı, özellikle özel nitelikli kişisel veri ya da ceza mahkumiyetine ve suçlara ilişkin veri olup olmadığı (GDPR §6/4-c), sonraki işlemenin veri öznesi açısından olası sonuçları (GDPR §6/4-d) ve şifreleme ya da psödonimizasyon[179] gibi koruyucu önlemlerin var olup olmadığı (GDPR §6/4-e), veri sorumlusunun değerlendirme yaparken dikkate alacağı unsurlardır.

---

[178] GDPR §5/1-b amacın "meşru" ("legitimate") olmasından söz ederken, GDPR §6 işlemenin "hukuka uygunluğunun" ("lawfulness") koşullarını belirlemektedir. Bu yönüyle Tüzük, 7 nci maddesinde işlemenin meşruluğunun koşullarını sayan Direktif'ten ayrılmaktadır. Kullanılan kavramlar arasında terminolojik ayrımlar bulunsa da (bu konuda bkz. **Küzeci**, s. 209 vd., dpn. 19), iki düzenlemenin yöneldikleri amaçlar ortaktır.

[179] Psödonimizasyon kavramı ile ilgili olarak bkz. dpn. 31.

II.B.3.Veri Minimizasyonu İlkesi

Tüzük'ün adlandırmasıyla veri minimizasyonu ilkesi, kişisel verilerin, işlenme amaçları açısından yeterli, bu amaçla ilgili ve amacın gerekleri ile sınırlı olmasını ifade eder (GDPR §5/1-c). Bu ilke daha önce Direktif'te (DPD §6/1-c) ve otomatik yollarla işlenen kişisel verilerin saklanma amacı açısından ETS 108'de (§5/ c) yer almıştır. KVKK, kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmasını genel ilkeleri arasında saymıştır (m. 4/2-ç), ancak Kanun'da bu ilkeyi somutlaştıran bir hüküm mevcut değildir.[180] Veri sorumluları yönünden bu ilkenin nasıl uygulanacağı ya da hangi durumlarda bu ilkeye uyulmuş sayılacağı düzenlenmemiştir. Tüzük ise, 25 inci maddesinin 1 inci fıkrasında, veri sorumlularına, tasarımsal gizliliğin sağlanmasının da bir gereği olarak, veri minimizasyonu ilkesinin gerçekleştirilebilmesi için gerekli teknik ve kurumsal önlemleri alma yükümlülüğü getirmiştir.

Veri minimizasyonu ilkesi uyarınca, sadece işleme amacı açısından uygun kişisel veriler, amacın gerektirdiği miktarı aşmayacak şekilde toplanmalıdır. Toplanan veriler, amaca ulaşmak için mümkün olan en az ölçüde kullanılmalıdır. Bu ilkeye özellikle iş başvurularında, internet ortamındaki kayıt sayfalarında ve form doldurulması gereken diğer hallerde dikkat edilmeli ve amaca ulaşmak için gerekenden fazla bilgi istenmemelidir.[181] Örneğin takma adların kullanıldığı bir forum sitesine kaydolmak isteyen kişilerden vatandaşlık numaralarının istenmesi bu ilkeye aykırılık teşkil edecektir. Kamusal alanlarda güvenliğin sağlanması gibi nedenler de bu ilkenin ihlaline gerekçe oluşturmaz. Örneğin, toplu taşıma araçlarını kullanacak kişilerden parmak izi alınması bu ilkeye aykırıdır. Aynı şekilde, güvenlik kameralarının güvenliği sağlanmak istenen alanın dışını da görüş alanı içine alması durumunda, amacın gerektirdiğinden fazla kişisel veri toplanması söz konusu olacaktır.[182]

---

[180] **Çekin**, s. 53.

[181] **Develioğlu,** s. 47, **Küzeci**, s. 214-215.

[182] **Küzeci**, s. 215.

Koşullar ve ihtiyaçlar, aynı amaç doğrultusunda yeni veriler toplanmasını ya da toplanan verilerin yeni amaçlarla kullanılmasını gerektirebilir. Bu hallerde de veri sorumluları, veri minimizasyonu ilkesi çerçevesinde hareket etmelidir.

II.B.4.Doğruluk İlkesi

GDPR §5/1-d uyarınca, kişisel veriler doğru ve gerekli hallerde güncel olmalı; doğru olmayan kişisel veriler, işlenme amaçları da göz önünde tutularak gecikmeksizin silinmeli ya da düzeltilmelidir. KVKK de bu ilkeyi aynen kabul etmiştir (m. 4/1-b).

Kişisel verilerin doğruluğu, her şeyden önce, veri öznesinin haklarının ve menfaatlerinin korunması yönünden önemlidir. Yanlış veya eksik tutulan kişisel veriler, veri öznelerinin temel hak ve özgürlüklerine, ekonomik menfaatlerine ve/ veya manevi bütünlüğüne zarar verebilir.[183] Bu tür veriler, aynı zamanda veri sorumlusunun kişisel verileri işleme amacına ulaşmasını engelleyeceğinden veya güçleştireceğinden, doğruluk ilkesi, veri sorumluları açısından da olumludur.

Kişisel verilerin gerektiğinde güncel olması da bu ilkenin bir gereğidir. Verilerin güncel olmasının gerekli olup olmadığı somut olayın koşullarına göre belirlenecektir. Kişisel verilerde ya da kişisel verilerin ilişkin olduğu gerçek kişinin durumunda bir değişiklik olmadığı takdirde, verilerin güncellenmesine ihtiyaç yoktur.

Kişisel verilerin doğruluğunun, veri öznesinin çıkarları ile yakın ilgisinin de bir sonucu olarak, Tüzük'te veri öznelerine kendilerine ilişkin doğru olmayan kişisel verilerin gecikmeksizin düzeltilmesini isteme hakkı tanınmıştır (GDPR §16).

II.B.5.Saklamanın Sınırlanması İlkesi

Bu ilke, kişisel verilerin hangi şekilde ve ne kadar süreyle saklanması gerektiğini belirler. Buna göre, kişisel veriler, veri öznelerinin belirlenmesine olanak tanıyan şekilde, işleme amaçlarının gerektirdiğinden daha uzun süre boyunca

[183] **Develioğlu**, s. 48, **Küzeci**, s. 219.

saklanmamalıdır (GDPR §5/1-e). Bu ilke KVKK'de de aynı şekilde benimsenmiştir (m. 4/1-d).

Bu ilke, amacın sınırlanması ve veri minimizasyonu ilkeleri ile yakından ilgilidir. Kişisel veriler amaca ulaşılmasının ardından daha fazla tutulmamalıdır, ya da bu verilerin veri öznesi ile ilişiği kesilmelidir (anonimleştirilmelidir). Ayrıca mevcut amaçla ilgisi bulunmayan kişisel veriler, gelecekte ortaya çıkması olası amaçlar gerekçe gösterilerek toplanmamalı ve saklanmamalıdır. Örneğin, bir dergi abonesinin kişisel verileri, kişi aboneliğini iptal ettikten sonra tekrar abone olma ihtimali göz önünde tutularak saklanamaz. Ancak, kişisel verilerin tutulmasının hangi noktadan sonra gereksiz hale geldiğinin tespiti, her zaman bu örnekteki kadar kolay olmamaktadır. Böyle durumlarla karşılaşıldığında güçlük yaşanmaması için, hangi verilerin hangi amaçlarla ne kadar süre saklanabileceğine ilişkin bir veri saklama politikası ("data retention policy") geliştirilmesi mümkündür.[184] Bu ilkenin bir görünümü, aşağıda incelenecek olan unutulma hakkıdır.

GDPR §89/1'de öngörülen gerekli teknik ve kurumsal önlemlerin alınmış olması koşuluyla, veri sorumluları, yalnızca kamu yararı, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla yapacağı sonraki işlemelerde kullanmak koşuluyla, kişisel verileri daha uzun süreyle saklayabilirler (GDPR §5/1-e).

II.B.6.Bütünlük ve Gizlilik İlkesi

GDPR §5/1-f'de ifadesini bulan bütünlük ve gizlilik ilkesine göre, kişisel veriler, kaybolmaya, imha edilmeye veya hasara uğramaya karşı koruma da dahil olmak üzere, uygun ölçüde güvenliği sağlanacak şekilde, gerekli teknik ve kurumsal önlemler alınarak işlenmelidir. Bu ilke, Direktif'te düzenlenmemişti. KVKK'nin de genel ilkeler arasında bu ilkeye ayrıca yer vermediği belirtilmelidir.

Tüzük'te veri sorumluları ve veri işleyenler açısından öngörülen yükümlülüklerin bu ilkenin somutlaştırılmasına yönelik olduğunu söylemek mümkündür. Özellikle 24 üncü maddede belirtilen kişisel verilerin işlenmesinin

---

[184] **Küzeci**, s. 222. Tüzük ile uyumlu bir veri saklama politikası şablonu için bkz. https://www.privacy-advocaat.nl/public/documents/246/template-data-retention-policy.pdf (Erişim tarihi: 23/4/2019).

Tüzük'e uygun yapılması için gerekli teknik ve kurumsal önlemlerin alınması ile 25 inci maddede düzenlenen tasarımsal gizlilik, bu anlamda önemlidir. Bu ilke kapsamında alınabilecek önlemlere örnek olarak, kişisel verilerin psödonimize edilmesi, şifrelenmesi ve mevcut önlemlerin yeterli olup olmadığının düzenli olarak kontrol edilmesi verilebilir.[185]

II.B.7.Hesap Verilebilirlik İlkesi

Hesap verilebilirlik ilkesi, esasen, veri sorumlusunun, yukarıda sayılan tüm ilkelerle uyumlu bir şekilde hareket etmesini ve bunu ispatlayabilmesini ifade eder (GDPR §5/2). Bu ilke, daha geniş şekilde, veri sorumlusunun, normal şartlar altında işleme faaliyetlerinde kişisel verilerin korunması kurallarına uyulmasını güvence altına alan önlemler alma ve bu önlemlerin alındığını veri öznelerine ve denetim kurumlarına ispatlayan belgeleri hazır bulundurma yükümlülüğü olarak açıklanabilir.[186]

Veri sorumlularına ve veri işleyenlere getirilen işleme faaliyetlerinin kayıtlarını tutma yükümlülüğü (GDPR §30), gerekli olduğu hallerde veri güvenliği yetkilisi atanması (GDPR §37 vd.), tasarımsal gizlilik (GDPR §25), bu ilkenin hayata geçirilmesini sağlamaya yönelik düzenlemelerdir.

II.C.Hukuka Uygunluk Halleri

II.C.1.Genel Olarak

Tüzük uyarınca, kural olarak, kişisel verilerin işlenmesi hukuka aykırıdır. Bu durum, GDPR §6/1'in ifade tarzından anlaşılmaktadır. GDPR §6'da sayılan hallerin varlığı, kişisel verilerin işlenmesini hukuka uygun hale getirir ve işleme faaliyeti, bu hallerin olanak tanıdığı ölçüde hukuka uygun kabul edilir.

Kişisel verilerin işlenmesini hukuka uygun kılan başlıca neden, veri öznesinin rızasıdır. Rızanın geçerlilik şartlarına yönelik 7 ve 8 inci maddelerinde özel

---

[185] Handbook on European Data Protection Law, s. 131.

[186] Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173, 13 Temmuz 2010, s. 2.

düzenlemelerin yer alması, Tüzük'te rızaya verilen önemin bir göstergesidir. Ancak rızanın tek hukuka uygunluk nedeni olmadığı da belirtilmelidir. GDPR §6/1, rıza dışında farklı hukuka uygunluk nedenleri de saymıştır. Bunun dışında, GDPR §9 özel nitelikli kişisel verilerin işlenmesi, GDPR §10 ceza mahkumiyetine ve suçlara ilişkin kişisel verilerin işlenmesi ve GDPR §11 ise veri öznesinin kimliğinin belirlenmesine gerek olmayan hallerde kişisel verilerin işlenmesi ile ilgili olarak özel hukuka uygunluk koşulları öngörmüştür.

II.C.2.Veri Öznesinin Rızası

II.C.2.a)Genel Olarak

Veri öznelerinin kişisel verileri üzerindeki tasarruf haklarının kaçınılmaz bir sonucu olarak, bu kişilerin kişisel verilerinin işlenmesine yönelik rızaları, işlemenin hukuka uygunluğunun bir gereğidir. Rıza, Tüzük'te, veri öznesinin özgür iradesiyle, belirli bir konuda, bilgisi dahilinde ve yoruma açık olmayacak şekilde, kişisel verilerinin işlenmesine yönelik onayını ifade eden bir davranışı olarak tanımlanmıştır (GDPR §4/11). Tanımdan hareketle, rızanın temelini, veri öznesinin özgür iradesinin oluşturduğu söylenebilir. Tüzük'te, baskı altında kalmadan, hile veya aldatma yoluyla manipüle edilmeden verilen bir rıza aranmıştır. Kuşkusuz bu, ancak veri öznesi neye rıza verdiğini biliyorsa mümkündür, bu nedenle rızanın konusu ve sınırları belli olmalı, veri öznesi, veri sorumlusunca işlemenin amaçları ve yöntemlerine dair yeterince aydınlatılmış olmalıdır.

Tüzük, rıza beyanının ne şekilde yapılacağına dair belli bir koşul öngörmemiştir. Rıza sözlü, yazılı ya da elektronik yollarla açıklanabilir. Buna göre, örneğin, bir internet sitesinde bir kutucuğun işaretlenmesi bir rıza beyanı olabilir. Ancak rızayı kuşkuya ve yoruma yer bırakmayacak şekilde ifade eden bir davranışın varlığı şarttır; veri öznesinin sessiz kalması ya da önceden işaretlenmiş kutucuklar, rıza teşkil etmez.[187] Bu çerçevede, objektif olarak rıza anlamına gelen ve karşı

[187] Tüzük, Gerekçe 32.

tarafça da rıza olarak kabul edilebilecek dışa yönelik her türlü eylem, geçerli bir rıza beyanının varlığı sonucunu doğuracaktır.[188]

Rızanın ayrıca kişisel verilerin işlenmesinin yöneldiği amacın veya amaçların bütününü kapsaması gerekir. Bu amaçların tümüyle belirlenmesi, her zaman kişisel verilerin toplanma anında mümkün olmamaktadır. Özellikle bilimsel araştırmalar için kişisel verilerin toplanmasında bu durumla karşılaşılmaktadır. Bu nedenle, veri öznelerine, bilimsel araştırmaların sadece belli bir kısmı için rıza beyan etme imkanı tanınmalıdır.[189]

II.C.2.b)Rızanın Şartları

Rızanın şartları, Tüzük'ün 7 nci maddesinde düzenlenmiştir. Bu şartlar, rızanın şekline ya da içeriğine ilişkin olmayıp, hangi koşullar altında rızanın varlığından söz edilebileceğini belirler. Bu anlamda ilk olarak, kişisel verilerin işlenmesi rızaya dayanıyorsa, veri sorumlusunun, veri öznesinin kişisel verilerinin işlenmesine rıza gösterdiğini ortaya koyabilmesi aranır (GDPR §7/1). Direktif'te böyle bir düzenleme bulunmamakla birlikte, Direktif'in yürürlükte olduğu dönemde de, rızaya dayanan veri sorumlularına, rızanın varlığını ispatlamalarını gerektirecek durumlarla karşılaşmaları ihtimali nedeniyle, rızanın varlığına dair delillerin oluşturulması ve saklanması tavsiye edilmekteydi.[190]

Rıza, farklı hususları da içeren yazılı bir beyan içerisinde açıklanacaksa, rıza talebi, diğer hususlardan açıkça ayırt edilebilecek şekilde, anlaşılır ve kolay erişilebilir olarak yazılmalı, açık ve sade bir dil kullanılmalıdır. Beyanda, Tüzük'ün ihlalini oluşturan kısımlar bulunuyorsa, bu kısımların bağlayıcılığı yoktur (GDPR §7/2).

Rıza her zaman geri alınabilir. Ancak rızanın geri alınması geriye etkili değildir, rızanın geri alınmasından önce bu rızaya dayanarak yapılan işleme

---

[188] Nilgün **Başalp** (2004), Kişisel Verilerin Korunması ve Saklanması, Yetkin, Ankara, s. 39 (naklen, **Uygun**, s. 56'dan).

[189] Tüzük, Gerekçe 33.

[190] Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP 187, 13 Temmuz 2011, s. 21.

faaliyetlerinin hukuka uygunluğu geri almadan etkilenmez. Veri özneleri, rıza vermeden önce bu konuda bilgilendirilmiş olmalıdır. Rızanın geri alınabilmesi, veri öznelerinin kişisel verilerinin geleceğini belirleme hakkının doğal bir sonucudur. Dolayısıyla Tüzük, rızanın geri alınmasının, rızanın verilmesi kadar kolay olması gerektiğini ifade etmiştir (GDPR §7/3).

Rızanın özgürce verilmesi gerektiğinden yukarıda söz edilmişti. Rızanın özgürce verilip verilmediğinin belirlenmesinde, diğer hususların yanında, bir sözleşmenin ifasının, ifa için gerekli olmayan kişisel verilerin işlenmesi rızasına bağlanıp bağlanmadığı oldukça önemlidir (GDPR §7/4). Aynı şekilde, veri sorumlusu, sözleşmenin ifası için gerekli olan işleme faaliyetleri için verilmiş rızayı, bunların ötesinde bir işleme yapacak şekilde genişletemeyecektir.[191]

II.C.2.c)Çocukların Kişisel Verilerinin İşlenmesinde Rıza

Direktif'te, çocukların kişisel verilerinin korunmasına yönelik herhangi bir düzenleme bulunmamaktaydı. Tüzük'te çocukların kişisel verilerinden açıkça söz edilmesi yeni ve kimilerine göre gecikmiş bir gelişmedir.[192]

Tüzük'ün 8 inci maddesi, bilgi toplumu hizmetlerinin[193] doğrudan çocuklara sunulması halinde çocuğun rızasının geçerliliğini özel olarak düzenlemektedir. Buna göre, çocuğun rızasına dayanılarak kişisel verilerinin işlenebilmesi için, çocuk en az 16 yaşında olmalıdır. Çocuk 16 yaşından küçük ise, işleme, ancak çocuğun velayetini elinde bulunduran kişinin rızası veya onayı varsa, bu rıza veya onayın kapsamı ile

---

[191] Article 29 Working Party, Opinion 15/2011 on the definition of consent, s. 8.

[192] Paul **Lambert** (2017), Understanding the New European Data Protection Rules, Taylor & Francis, s. 249.

[193] GDPR §4/25, "bilgi toplumu hizmeti"nin tanımı için, (AB) 2015/1535 sayılı Direktif'in (Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17 Eylül 2015) tanımına atıfta bulunmuştur. Anılan tanıma göre bilgi toplumu hizmetleri, kural olarak bir ücret karşılığında, uzaktan, elektronik yollarla ve talep üzerine gerçekleştirilen hizmetlerdir. İnternet üzerinden mal veya hizmet sağlanması, çevrimiçi bilgilendirme hizmetleri ve e-posta yoluyla ticari bildirimler gönderilmesi bilgi toplumu hizmetlerine örnek verilebilir, bkz. Claudia Andrea **Hernández Sánchez** (2005), The Meaning of the Information Society Services in the E-Commerce Directive, Oslo, s. 6. - https://www.duo.uio.no/handle/10852/20433 (Erişim tarihi: 1/5/2019)

sınırlı olmak üzere hukuka uygun olacaktır (GDPR §8/1). Veri sorumluları, çocuğun velisinin rıza veya onayının bulunduğunu doğrulamak için, mevcut teknolojileri de dikkate alarak, makul bir çaba göstermelidir (GDPR §8/2).

Tüzük, Üye Devletlere, yaş sınırını 13 yaşa kadar indirme imkanı tanımıştır (GDPR §8/1). Bu düzenleme, Üye Devletlerin sözleşmeler hukuku kurallarının çocuklar yönünden uygulanmasını etkilemez (GDPR §8/3).

II.C.3.Diğer Hukuka Uygunluk Halleri

GDPR §6/1'in (b) bendinden itibaren, rıza dışında kişisel verilerin işlenmesini hukuka uygun hale getiren nedenler sayılmıştır. Buna göre, işleme, veri öznesinin taraf olduğu bir sözleşmenin ifa edilmesi veya sözleşme kurulurken veri öznesinin isteği doğrultusunda adımların atılabilmesi (GDPR §6/1-b), veri sorumlusunun üzerine düşen bir hukuki sorumluluğu yerine getirebilmesi (GDPR §6/1-c), veri öznesinin ya da başka bir gerçek kişinin hayati menfaatlerinin korunabilmesi (GDPR §6/1-d), kamu yararı için yapılan bir görevin yerine getirilebilmesi ya da veri sorumlusunun resmi yetkilerini kullanabilmesi (GDPR §6/1-d) veya veri öznelerinin temel hak ve özgürlüklerini ihlal etmemek koşuluyla veri sorumlusunun ya da üçüncü kişilerin meşru menfaatleri için gerekli olduğu hallerde hukuka uygun olacaktır. Bu düzenleme, Direktif'in 7 nci maddesindeki düzenleme ile paraleldir.

II.C.3.a)Sözleşmenin İfası veya Veri Öznesinin İsteği Doğrultusunda Adımlar Atılması

Kişisel verilerin işlenmesi, veri öznesinin taraf olduğu bir sözleşmenin ifa edilebilmesi için gerekliyse, ya da sözleşmenin kurulmasından önce, veri öznesinin talebi doğrultusunda işlemler yapılması kişisel verilerinin işlenmesini gerektiriyorsa, bu kapsamdaki işleme faaliyetleri hukuka uygundur (GDPR §6/1-b). Bu hükmün

amacı, veri sorumlusunu, sözleşme ilişkisi kurduğu ya da kurmayı düşündüğü kişi ile ilgili gerekli bilgileri alması halinde doğacak risklere karşı korumaktır.[194]

Bu düzenleme, sözleşme öncesinde ve sözleşme sonrasında uygulanabilmektedir. Sözleşme öncesinde, düzenlemenin uygulama alanı bulabilmesi için veri öznesinin talebi doğrultusunda hareket ediliyor olmalıdır, veri sorumlularının ya da üçüncü kişilerin kendi inisiyatifleriyle hareket etmeleri halinde düzenleme uygulanmaz. Sözleşme sonrasında ise, sözleşme ilişkisi çerçevesinde veri öznesinin, verilerinin işlenmesine rızasının bulunduğunu kabul etmek gerekmektedir.[195] Ancak, sadece sözleşmenin kuruluşu veya ifası için gerekli olan işleme faaliyetleri için hukuka uygunluktan söz edilebilir. Veri sorumlusunun, sözleşmeye dayanarak bu sınırın ötesine geçen işleme faaliyetleri hukuka uygun değildir. Bir işleme faaliyetinin sözleşmenin kuruluşu veya ifası için gerekli olup olmadığı, sözleşmenin amacı ve içeriği göz önüne alınarak belirlenecektir.[196]

II.C.3.b)Hukuki Sorumluluğun Yerine Getirilmesi

Kişisel verilerin işlenmesi, veri sorumlusunun üzerine düşen bir hukuki sorumluluğu yerine getirebilmesi için gerekli olduğu hallerde hukuka uygundur (GDPR §6/1-c). Sorumluluk, AB veya Üye Devlet hukukundan kaynaklanmalıdır ve işleme bu mevzuatın amacına uygun olmalıdır.[197] Vergi veya sosyal güvenlik hukukundan doğan sorumlulukları gereği işverenlerin, işçilerinin ücret bilgilerini vergi kurumlarına ya da diğer ilgili makamlara bildirmeleri örnek verilebilir.[198]

Veri sorumlusunun, sorumluluğunu yerine getirip getirmeme konusunda seçim yapma imkanı bulunmamalıdır. Ayrıca, bir işleme faaliyetinde bulunmaksızın

---

[194] **Develioğlu**, s. 60.

[195] **Uygun**, s. 57.

[196] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 Nisan 2014, s. 17.

[197] **Develioğlu**, s. 63.

[198] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, s. 19.

sorumluluğun yerine getirilmesi mümkün olmamalıdır. Nitekim böyle bir durumda, işlemenin gerekliliğinden söz edilemeyecektir.

Nihayet, kişisel verilerin işlenmesi, ancak sorumluluğun sınırları ölçüsünde hukuka uygundur. Sorumluluğun yerine getirilmesi için ihtiyaç duyulmayan işleme faaliyetleri, bu düzenleme kapsamında değildir. Sorumluluğun kaynağını oluşturan mevzuat ile işlemeye konu olan kişisel veri türleri, veri özneleri, saklama süresi gibi hususlar belirlenerek hukuka uygunluğun sınırları çizilebilir.[199]

II.C.3.c)Hayati Menfaatlerin Korunması

Kişisel verilerin işlenmesi, veri öznesinin ya da farklı bir gerçek kişinin hayati menfaatlerinin korunması için gerekli ise, hukuka uygundur (GDPR §6/1-d). Bu hukuka uygunluk sebebi, farklı bir sebebe dayanılamadığı, özellikle veri öznesinin rızasının alınmasının mümkün olmadığı hallerde geçerlilik kazanmaktadır. Aynı hüküm, sadece veri öznelerini kapsayan şekilde Direktif'te de yer almasına rağmen (DPD §7/d), hangi durumlarda uygulama alanı bulacağına dair bir açıklama yapılmamıştı. Tüzük ise, Gerekçesinde, salgın hastalıkların izlenmesi gibi insancıl amaçlar ile doğal veya insan kaynaklı afetler gibi acil durumlarda kişisel verilerin işlenmesinin hem kamu yararı hem de veri öznesinin hayati menfaatleri yönünden gerekli olabileceğini belirtmiştir.[200]

Hayati menfaatlerin neler olduğu konusunda Tüzük'te bir açıklama bulunmayıp, hayati menfaat kavramı yoruma açıktır. Bazıları hayati menfaat kapsamına sadece kişinin hayatının korunmasını alırken, kimileri de hangi menfaatin hayati olduğunun kişiden kişiye veya toplumdan topluma değişebileceğini öne sürmektedir.[201] Madde 29 Çalışma Grubu, hayati menfaat ifadesinin, hükmün uygulama alanını "ölüm-kalım meseleleri ya da en azından yaralanma veya başka bir

---

[199] Tüzük, Gerekçe 45.

[200] Tüzük, Gerekçe 46.

[201] **Uygun**, s. 58.

şekilde kişinin sağlığına zarar verme riski oluşturan tehdit halleri" ile sınırladığı ve hükmün dar yorumlanması gerektiği görüşündedir.[202]

II.C.3.d)Kamu Yararına Görevin Yerine Getirilmesi ve Resmi Yetkilerin Kullanılması

Kişisel verilerin işlenmesi, kamu yararı için yapılan bir görevin yerine getirilebilmesi için ya da veri sorumlusuna tanınmış resmi bir yetkinin kullanılması için gerekli olduğu hallerde, hukuka uygundur (GDPR §6/1-e). Bu düzenleme, hukuki sorumluluğun yerine getirilmesi ile karıştırılmamalıdır. Kamu yararına görev, hukuki bir sorumluluk da teşkil edebilir, ancak bu düzenlemenin kapsamı çok daha geniştir. Veri sorumlusunun, mevzuatta kendisine herhangi bir sorumluluk öngörülmemiş olmasına rağmen, kamu yararını gözeterek kendi inisiyatifiyle yaptığı işlemeler, somut olayda "gereklilik" unsurunun bulunması halinde bu madde kapsamına dahil edilecektir. Ayrıca düzenlemenin sadece kamu sektöründeki değil, özel sektördeki veri sorumluları yönünden de geçerli olduğu belirtilmelidir.

Resmi bir yetkinin kullanılması, veri sorumlusunun doğrudan kendisine tanınan bir yetki ile hareket etmesi şeklinde olabilir. Örneğin, kamu kurumu niteliğindeki meslek kuruluşları, mesleki denetim yetkilerini kullanırken ya da yaptırımlar uygularken üyelerinin kişisel verilerini işlerse, bu işleme hukuka uygundur. Veri sorumlusunun resmi yetkisi bulunmamakla birlikte, resmi yetkiye sahip üçüncü kişilerin yetkileri dahilinde hareket etmesi de mümkündür. Örneğin, veri sorumluları, kendilerinden resmi yetkilerini kullanabilmek adına veri öznelerinin kişisel verilerinin paylaşılmasını talep eden kamu kurumları ile bu bilgileri paylaşırsa, resmi yetkinin kullanılması hukuka uygunluk nedeni oluşur. Ancak kişisel verilerin kamu kurumları tarafından işlenebilmesi için bu organların yasal bir düzenleme ile yetkilendirilmiş olması gerekmektedir.[203]

---

[202] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, s. 20.

[203] **Uygun**, s. 58.

II.C.3.e)Veri Sorumlusunun ya da Üçüncü Kişinin Meşru Menfaatleri

Kişisel verilerin işlenmesi, veri sorumlusu ya da üçüncü kişi tarafından ulaşılmak istenen meşru menfaatlere ulaşılabilmesi için gerekli olduğu hallerde, hukuka uygundur (GDPR §6/1-f). Aynı düzenleme ile bu hukuka uygunluk halinin sınırı da çizilmiştir; buna göre, veri öznesinin kişisel verilerinin korunmasını gerektiren temel hak ve özgürlükleri, meşru menfaatlerin önüne geçmemelidir. Düzenlemede de belirtildiği gibi, bu husus, özellikle veri öznesinin çocuk olduğu hallerde önem taşımaktadır. Meşru menfaatler ileri sürülerek çocukların kişisel verileri işlenemez, çocukların kişisel verilerinin işlenmesinde bu hukuka uygunluk sebebine dayanılamaz.[204] Bu hukuka uygunluk sebebi, kamu kurumlarınca gerçekleştirilen işleme faaliyetleri yönünden de geçerli değildir, çünkü kamu kurumlarınca gerçekleştirilen işleme faaliyetleri kanun koyucu tarafından yasal bir temele dayandırılmış olmalıdır.[205] Direktif'te ise kamu kurumları yönünden bu tarz bir sınırlama bulunmamaktadır.

Meşru menfaatlerin, hak ve özgürlüklerin önüne geçip geçmediğinin değerlendirmesi yapılırken, somut olayın bütün şartları dikkate alınır.[206] Veri sorumlusunun amacı, işlenen verinin türü, işlemenin hangi şekilde yapıldığı gibi hususlar bu değerlendirmede önem arz eder.

II.C.4.Özel Hukuka Uygunluk Halleri

Bazı kişisel veri türlerinde ve işleme faaliyetlerinde, kişisel verilerin işlenmesinin hukuka uygunluğu Tüzük'te özel olarak düzenlenmiştir. 9 uncu maddede özel nitelikli kişisel verilerin işlenmesi, 10 uncu maddede ceza mahkumiyetine ve suçlara ilişkin kişisel verilerin işlenmesi ve 11 inci maddede veri

---

[204] **Lambert**, s. 247.

[205] Tüzük, Gerekçe 47.

[206] **Develioğlu**, s. 67.

öznesinin kimliğinin belirlenmesine gerek olmayan hallerde kişisel verilerin işlenmesinde hukuka uygunluk şartları düzenlenmiştir.

II.C.4.a)Özel Nitelikli Kişisel Verilerin İşlenmesi

Veri öznesi açısından hassas veri kabul edilen bazı verilerin daha nitelikli bir korumaya tabi tutulması, ulusal ve uluslararası pek çok belgede benimsenmiş bir yaklaşımdır. Direktif, ETS 108 ve BM Rehber İlkeleri, bu tarz bir koruma öngören uluslararası belgelerdendir.[207] Türk hukukunda da özel nitelikli kişisel verilerin işlenmesi ayrıca düzenlenmiştir (KVKK m. 6).

Tüzük, Direktif'in 8 inci maddesinde yer alan düzenlemeye, kapsamını genişleterek 9 uncu maddesinde yer vermiştir. Anılan düzenleme uyarınca, kişinin ırksal veya etnik kökenine, siyasi görüşlerine, dini inancına ve felsefi görüşlerine, sendika ve meslek birliği üyeliklerine ilişkin veriler, yalnızca kişiyi belirlemek amacıyla işlenmesi halinde kişinin genetik ve biyometrik verileri ile fiziksel ve ruhsal sağlığına, cinsel yaşamına ve cinsel yönelimine ilişkin verilerin işlenmesi yasaktır (GDPR §9/1).[208] Maddenin devamında ise, bu yasağın istisnaları düzenlenmiştir.

Veri öznesinin rızası, Tüzük'te belirlenen ilk istisnadır. Veri öznesinin rızasının aranması, veri öznelerinin kişisel verileri üzerindeki denetim hakkının bir gereği olduğu gibi, düşünce özgürlüğü ile de ilişkilidir.[209] Rızanın, GDPR §7'de düzenlenen geçerlilik şartlarına uygun olması gereklidir. AB ya da Üye Devlet hukukunda, yasağın veri öznesi tarafından kaldırılamayacağı öngörülmüşse, rızaya dayanan işleme faaliyetleri hukuka uygun olmayacaktır (GDPR §9/2-a).

Veri sorumlusunun iş, sosyal güvenlik veya sosyal koruma hukukundan kaynaklanan yükümlülüklerini yerine getirmesi ya da veri sorumlusunun veya veri

---

[207] **Küzeci**, s. 249-250.

[208] DPD §8/1, genetik ve biyometrik verilerin işlenmesine dair bir hüküm içermemekle birlikte, cinsel yönelime ilişkin verilere de özel nitelikli veriler arasında yer vermemiştir.

[209] **Küzeci**, s. 258.

öznesinin[210] belirli haklarını kullanması kapsamında özel nitelikli kişisel verilerin işlenmesi, hukuka uygundur (GDPR §9/2-b). Ancak, hakların ve yükümlülüklerin yasal bir dayanağı olmalıdır. İşverenin, işçinin sendika kesintisini yapmak gibi bir yasal görevinin bulunması, bu istisna haline örnek verilebilir.[211]

Veri öznesinin ya da başka bir kişinin hayati menfaatlerinin korunması için özel nitelikli kişisel verilerin işlenmesinin gerekli olması, bir istisna hali teşkil eder. Ancak, bu istisna haline yalnızca, veri öznesinin fiziksel ya da hukuki olarak rıza göstermesi mümkün değilse dayanılabilecektir (GDPR §9/2-c).

Kâr amacı gütmeyen kuruluşlar, örgütler veya diğer kurumlar; politik, felsefi, dini ya da sendikal amaçlarla ve gerekli güvenlik önlemleri alınmak koşuluyla meşru faaliyetler çerçevesinde, özel nitelikli kişisel verileri işleyebilirler. Ancak işleme faaliyeti yalnızca mevcut veya eski üyelerle ve amaç doğrultusunda kuruluş ile düzenli bağlantı halindeki kişilerle sınırlı olmalı, veri öznelerinin rızası olmaksızın veriler kuruluş dışına açıklanmamalıdır (GDPR §9/2-d).[212]

Veri öznelerinin özel nitelikli kişisel verilerini kamuya kendileri açıklamaları halinde, bu özel nitelikli kişisel veriler yönünden hukuka uygunluk sebebi oluşur (GDPR §9/2-e).

Bir yasal hakkın kurulması, kullanılması ya da savunulması için gerekli olduğu hallerde, özel nitelikli kişisel verilerin işlenmesi hukuka uygundur. Ayrıca, mahkemelerin, yargı yetkilerinin kullanımı kapsamında gerçekleştireceği işleme faaliyetleri de hukuka uygundur (GDPR §9/2-f).[213]

Önemli kamu yararının bulunduğu hallerde, özel nitelikli kişisel verilerin işlenmesi hukuka uygundur. Ancak önemli kamu yararı, AB veya Üye Devlet hukukuna dayanmalı, işleme faaliyeti varılmak istenen amaçla orantılı olmalı, kişisel verilerin korunması hakkının özüne saygılı olmalı ve veri öznelerinin temel hak ve

---

[210] DPD §8/2-b, veri öznesinin haklarının kullanıldığı halleri istisna kapsamında saymamıştır.

[211] **Küzeci**, s. 259.

[212] DPD §8/2-d, eski üyelerin özel nitelikli kişisel verilerinden söz etmemiştir.

[213] DPD §8/2-e, mahkemelerin yargı yetkisini kullandığı halleri bu istisna kapsamında saymamıştır.

özgürlükleri yönünden uygun ve spesifik güvenlik önlemleri öngörülmelidir (GDPR §9/2-g).

Koruyucu hekimlik ile iş ve meslek hekimliği faaliyetleri, işçilerin çalışabilirliğinin ölçülmesi, tıbbi teşhis, sağlık ve sosyal bakım hizmetlerinin sağlanması kapsamında kişisel verilerin işlenmesi, AB veya Üye Devlet hukukuna ya da gerekli önlemler alınmak koşuluyla bir sağlık çalışanı ile yapılan sözleşmeye dayanıyorsa, hukuka uygundur (GDPR §9/2-h). Bu düzenleme kapsamındaki işleme faaliyetleri yalnızca sır tutma yükümlülüğü ("professional secrecy") altındaki sağlık çalışanlarınca yapılabilir (GDPR §9/3).

Kamu sağlığına ilişkin bir kamu yararı söz konusuysa, özel nitelikli kişisel verilerin işlenmesi yönünden hukuka uygunluk sebebi oluşur. Sınırötesi bir sağlık tehdidinin varlığı (salgın hastalık gibi), bu hallerden biridir. Ancak, işleme faaliyetleri dayanağını AB veya Üye Devlet hukukundan almalı, sır tutma yükümlülüğü başta olmak üzere, veri öznelerinin temel hak ve özgürlüklerinin güvence altına alınması için uygun ve spesifik önlemler alınmalıdır (GDPR §9/2-i).

Kamu yararı için arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla, GDPR §89/1 esasları da göz önüne alınarak, AB ya da Üye Devlet hukuku çerçevesinde, varılmak istenen amaçla orantılı ve kişisel verilerin korunması hakkının özüne saygılı olarak, veri öznelerinin temel hak ve özgürlüklerinin güvence altına alınması için uygun ve spesifik önlemler alınarak, özel nitelikli kişisel veriler hukuka uygun olarak işlenebilir (GDPR §9/2-j).

Üye Devletler; genetik veriler, biyometrik veriler ve sağlığa ilişkin veriler yönünden, yukarıda sayılanlar dışında istisna ve sınırlama halleri öngörebilirler (GDPR §9/4).

II.C.4.b)Ceza Mahkumiyetlerine ve Suçlara İlişkin Kişisel Verilerin İşlenmesi

Tüzük, 6 ncı maddesinde saydığı hukuka uygunluk hallerinin varlığında, ceza mahkumiyetlerine, suçlara ve güvenlik önlemlerine ilişkin kişisel verilerin işlenmesini, yalnızca resmi makamların kontrolü altında ya da AB ya da Üye Devlet

hukukunun yetkilendirdiği hallerde mümkün kılmıştır. Ayrıca, ceza mahkumiyetlerine ilişkin kapsamlı siciller, yalnızca resmi makamların kontrolü altında tutulmalıdır (GDPR §10).

II.C.4.c)Kimlik Belirlenmesini Gerektirmeyen İşleme Halleri

Veri sorumlusunun amacı, başlangıçtan itibaren ya da sonradan, bir veri öznesinin kimliğini belirlemesini gerektirmiyorsa, veri sorumlusu, yalnızca Tüzük'e uygun hareket etmek amacıyla veri öznesinin kimliğini belirlemeye yönelik verileri saklamak, toplamak ya da işlemek zorunda değildir (GDPR §11/1).

Bu maddenin uygulama alanı bulduğu hallerde, veri sorumlusu, veri öznesinin kimliğini belirleyebilecek durumda olmadığını ortaya koyabiliyorsa, mümkünse veri öznesini bilgilendirmelidir. Bu durumda, Tüzük'ün 15 ila 20 nci maddeleri, veri özneleri bu maddelerde yer alan haklarını kullanmak amacıyla veri sorumlusuna kimliklerini belirlemeye yönelik verileri temin etmedikçe, uygulanmayacaktır (GDPR §11/2).

III. TÜZÜK'TE HAKLAR VE YÜKÜMLÜLÜKLER

III.A.Veri Öznesinin Hakları

Tüzük'te, 12 ila 22 nci maddeler arasında veri öznesinin hakları düzenlenmiştir. Ayrıca 77 nci madde ve devamında, veri öznelerinin hukuki çarelere başvurmalarına ilişkin esaslar belirlenmiştir.

III.A.1.Bilgi Edinme Hakkı

Veri öznelerinin, kişisel verilerinin işlenmesi konusunda bilgi edinme hakkının varlığı, veri öznelerinin Tüzük'ten ya da yasalardan doğan haklarını

kullanabilmesi ve kişisel verilerinin geleceğini belirleyebilmesi adına büyük önem arz eder.[214]

GDPR §12, veri sorumlularının, veri öznelerine, GDPR §13 ve 14'te sayılan bilgileri sağlaması gerektiğinden söz etmektedir. Kişisel veriler, doğrudan veri öznesinden toplanmışsa GDPR §13/1'de sayılan aşağıdaki bilgiler veri öznelerine sağlanmalıdır:

- Veri sorumlusunun ve mümkün olduğu hallerde temsilcinin kimliği ve iletişim bilgileri (GDPR §13/1-a),
- Mümkün olduğu hallerde veri koruma yetkilisinin iletişim bilgileri (GDPR §13/1-b),
- Kişisel verilerin işlenmesindeki amacın yanı sıra işlemenin yasal dayanağı (GDPR §13/1-c),
- İşleme veri sorumlusunun ya da üçüncü kişinin meşru menfaatine dayanıyorsa, dayandığı meşru menfaat (GDPR §13/1-d),
- Varsa, kişisel verilerin alıcıları ya da alıcı grupları (GDPR §13/1-e),
- Veri sorumlusu, kişisel verileri üçüncü ülkelere ya da uluslararası örgütlere aktarmak niyetindeyse, bu husus; Avrupa Komisyonu'nun aktarım yönünden bir yeterlilik kararı bulunup bulunmadığı, GDPR §46, 47 veya 49/1-b düzenlemeleri uyarınca veri transferi hallerinde alınan güvenlik önlemleri; ve bunlar erişime açıksa bir kopyasını nasıl edinebileceğine ilişkin bilgiler (GDPR §13/1-f).

Bunların dışında, GDPR §13/2, işlemenin dürüstlük ve şeffaflığının sağlanabilmesi için aşağıdaki bilgilerin veri öznelerine sağlanmasını öngörmüştür:

- Kişisel verilerin saklanacağı süre; bu mümkün değilse, sürenin tespitinde kullanılacak kriterler (GDPR §13/2-a),
- Veri sorumlusundan kişisel verilere erişim, kişisel verilerin düzeltilmesini ya da silinmesini talep etme, veri öznesine ilişkin işlemenin sınırlandırılmasını isteme

[214] **Develioğlu**, s. 83.

ya da işlemeye itiraz etme ve veri taşınabilirliği (“data portability”) haklarının varlığı (GDPR §13/2-b),

- İşleme rızaya dayanıyorsa, rızanın geri alınmasına kadar olan işlemlerin hukuka uygunluğu etkilenmemek kaydıyla her zaman rızayı geri alma haklarının varlığı (GDPR §13/2-c),
- Denetim kurumlarına şikayette bulunma hakkı (GDPR §13/2-d),
- Kişisel verilerin sağlanmasının yasal veya sözleşmesel bir sorumluluğun gereği olup olmadığı ya da bir sözleşmenin kurulması için gerekli olup olmadığı, bunun yanı sıra veri öznesinin kişisel verilerini sağlama yükümlülüğü altında olup olmadığı ve böyle bir yükümlülüğün varlığı halinde verilerin sağlanmamasının doğuracağı sonuçlar (GDPR §13/2-e),
- Profil çıkarma (“profiling”)[215] dahil olmak üzere otomatik karar alma (“automated decision-making”) uygulamalarının varlığı, uygulamanın dayandığı mantık hakkında anlamlı bilgi; işleme faaliyetinin veri öznesi açısından önemi ve beklenen sonuçları (GDPR §13/2-f).

GDPR §14, kişisel verilerin doğrudan veri öznesinden toplanmadığı hallerde veri öznesine sağlanması gereken bilgileri saymıştır. Bu düzenleme, GDPR §13 ile büyük ölçüde paraleldir, ancak GDPR §14/1-d hükmü işleme faaliyetinin meşru menfaatlere dayandığı hallerden söz etmek yerine, ilgili kişisel veri türlerinin veri öznesine bildirilmesini öngörmüştür. Meşru menfaatlere dayanılan hallerde, bu meşru menfaatler, işlemenin dürüstlüğünün ve şeffaflığının sağlanması adına veri öznesine sağlanması gereken bilgiler arasında sayılmıştır (GDPR §14/2-b). Kişisel verilerin hangi kaynaktan alındığı ve mümkün olan hallerde bu kaynağın kamuya açık olup olmadığı, veriler veri öznesinden toplanmamışsa, veri öznesine bildirilmelidir (GDPR §14/2-f).

Veriler, veri öznesinden toplanmışsa, sayılan bilgiler verilerin toplanması anında veri öznesine sağlanmalıdır (GDPR §13/1, 2). Veriler farklı bir kaynaktan

---

[215] Tüzük’teki tanımıyla profil çıkarma; kişisel verilerin, gerçek kişilerin çeşitli kişisel özelliklerini değerlendirme, özellikle iş performansını, ekonomik durumunu, sağlık durumunu, kişisel tercihlerini, ilgi alanlarını, güvenilirliğini, davranışlarını, konumunu ve hareketlerini belirleme ya da tahmin etmede kullanılacak şekilde otomatik yollarla işlenmesidir (GDPR §4/4).

toplanmış ise, bildirim makul bir süre içinde, ancak en geç bir ay içinde yapılmalıdır (GDPR §14/3-a). Veriler, veri öznesiyle iletişim amacıyla kullanılacaksa, en geç ilk iletişim sırasında bildirim yapılmalıdır (GDPR §14/3-b). Eğer verilerin bir alıcıya açıklanması planlanıyorsa, en geç ilk açıklama sırasında bildirim yapılmış olmalıdır (GDPR §14/3-c).

Veri öznesi, sayılan bilgilerden zaten haberdar ise, bu düzenlemeler uygulanmaz.

III.A.2.Erişim Hakkı

Bilgi edinme hakkının yanı sıra dürüstlük ve şeffaflık ile de yakından ilişkili[216] bir hak olan erişim hakkı, Tüzük'ün 15 inci maddesinde düzenlenmiştir. Anılan maddenin ilk fıkrasına göre, veri öznesi, kişisel verilerinin işlenip işlenmediğinin kendisine bildirilmesini isteyebileceği gibi, kişisel verilerine erişimini ya da maddenin devamında sayılan şu bilgilerin kendisine sağlanmasını talep edebilir:

- İşlemenin amaçları (GDPR §15/1-a),
- İlgili kişisel verilerin türleri (GDPR §15/1-b),
- Üçüncü ülkelerdeki alıcılar ve uluslararası örgütler başta olmak üzere, kişisel verilerin açıklandığı ya da açıklanacağı alıcılar ya da alıcı grupları (GDPR §15/1-c),
- Mümkün olduğu hallerde, kişisel verilerin saklanması planlanan süre, bu mümkün değilse, sürenin tespitinde kullanılacak kriterler (GDPR §15/1-d),
- Veri sorumlusundan kişisel verilerin düzeltilmesini ya da silinmesini talep etme, veri öznesine ilişkin işlemenin sınırlandırılmasını isteme ya da işlemeye itiraz etme haklarının varlığı (GDPR §15/1-e),
- Denetim kurumlarına şikayette bulunma hakkı (GDPR §15/1-f)i

[216] Erişim hakkı, veri öznelerinin bilgi edinme hakkını tamamlamakta, veri öznelerinin kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğini öğrenmesine olanak sağlamaktadır, bkz. **Develioğlu**, s. 87-88.

- Kişisel veriler veri öznesinden toplanmamışsa, kaynağa dair elde bulunan tüm bilgiler (GDPR §15/1-g),
- Profil çıkarma dahil olmak üzere otomatik karar alma ("automated decision-making") uygulamalarının varlığı, uygulamanın mantığı hakkında anlamlı bilgi, işleme faaliyetinin veri öznesi açısından önemi ve beklenen sonuçları (GDPR §15/1-h),
- Üçüncü ülkelere ya da uluslararası örgütlere kişisel verilerin aktarılması söz konusuysa, 46 ncı madde uyarınca alınan uygun güvenlik önlemleri hakkında bilgiler (GDPR §15/2).

Veri sorumluları, işlenen kişisel verilerin bir kopyasını, ücretsiz olarak veri öznesine verecektir. Ancak, veri öznesinin birden fazla kopya talep etmesi halinde veri sorumlusu makul bir ücret isteyebilir (GDPR §15/3).

Erişim hakkının kullanılması, başkalarının hak ve özgürlüklerini olumsuz etkilememelidir (GDPR §15/4). Örneğin, ticari sırlar ve yazılımlar üzerindeki telif hakları başta olmak üzere fikri mülkiyet hakları bakımından olumsuz bir etki meydana gelmemesine dikkat edilmelidir. Ancak, bu hususların göz önüne alınması, veri öznesine bilgi verilmesinin reddi anlamına gelmemelidir.[217] Bu haklar ile veri öznesinin hakları arasında bir denge sağlanmalıdır.[218]

Veri öznesi, özellikle çevrimiçi hizmetler ve çevrimiçi tanımlayıcılar bağlamında, erişim hakkını kullanmak isteyen veri öznesinin kimliğini doğrulamak için tüm makul olanakları kullanmalıdır. Sadece olası taleplere cevap verebilmek amacıyla kişisel verileri saklamamalıdır.[219]

III.A.3.Düzeltme Hakkı

Özellikle kişisel verilerin elektronik ortamda tutulmasının yaygınlaşmasıyla, kişisel verilerin yanlış ve eksik tutulması olasılığı da artmaktadır.[220] Kişisel verilerin

---

[217] Tüzük, Gerekçe 63.

[218] **Küzeci**, s. 229.

[219] Tüzük, Gerekçe 64.

[220] **Lambert**, s. 194.

doğru ve gerektiğinde güncel olmasını ifade eden doğruluk ilkesinin ve veri öznelerinin kişisel verilerinin geleceğini belirleme haklarının da bir gereği olarak, Tüzük'te, veri öznelerine, kendilerine ilişkin gerçeği yansıtmayan kişisel verilerin haksız bir gecikme olmaksızın düzeltilmesini veri sorumlularından talep etme hakkı tanınmıştır. Kişisel verilerin işlenmesindeki amaç da göz önüne alınarak, veri öznesinin tamamlayıcı bir beyanda bulunmak suretiyle eksik kişisel verilerinin tamamlanmasını talep etmesi de düzeltme hakkı kapsamındadır (GDPR §16).

Veri sorumluları, imkansız olmadığı ya da orantısız bir çaba gerektirmediği hallerde, kişisel verilerin düzeltildiğini, kişisel verileri açıkladığı her alıcıya bildirmekle ve veri sorumlusunu bu alıcılar hakkında bilgilendirmekle yükümlüdür (GDPR §19).

III.A.4.Unutulma Hakkı

Unutulma hakkı, veri taşınabilirliği hakkı ile birlikte Tüzük'te öngörülen iki yeni haktan biridir.[221] Bununla birlikte, unutulma hakkının bütünüyle yeni bir hak olmadığı, kişisel verilerin korunması hukukunda uzun süredir var olan kuralların yeniden adlandırılması olduğu görüşünü savunanlar da vardır. Direktif'in de 12 nci maddesinde, veri öznelerine, düzeltme, silme ve engelleme haklarını tanıdığı belirtilmelidir. Ayrıca henüz yeni bir kavram olan "unutulma hakkı" ile tam olarak neyin ifade edildiği de tartışmalıdır. Doktrinde, unutulma hakkının farklı tanımları bulunduğu gibi,[222] kişisel verilerin korunması konusuna yaklaşımların farklılık göstermesi nedeniyle unutulma hakkı da farklı hukuk sistemlerinde farklı şekillerde ele alınmıştır.[223] Aynı durumu ifade etmek için farklı kavramların kullanılmasıyla

---

[221] **Voss**, s. 4.

[222] Armağan Ebru **Bozkurt Yüksel** (2016), "İnternet ve Unutulma Hakkı", 4.Uluslararası Bilişim Hukuku Kurultayı 2016 Bildiriler Kitabı, İzmir, s. 26.

[223] Farklı hukuk sistemlerinin unutulma hakkına yaklaşımı için bkz. **Bozkurt Yüksel**, s. 26 vd. Dünya genelinde farklı hukuk sistemleri, özellikle AB ve Amerikan anlayışı arasındaki farklılıklar için bkz. Julia **Kerr** (2016), "What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What It Means for the Future of the Right to Be Forgotten", Chicago Journal of International Law, C. 17, S. 1, s. 233 vd.

karşılaşıldığı gibi,[224] tartışmalar böyle bir hakkın var olup olmadığına kadar götürülebilir.[225]

Unutulma hakkının Tüzük'teki düzenlenişine geçmeden önce, ABAD'ın konu üzerindeki tartışmaları alevlendiren ve Tüzük'teki düzenleme üzerinde de etkili olmuş Google Spain kararı[226] üzerinde durmak gerekir. Karara konu olan olayda, İspanyol vatandaşı Mario Costeja González, sosyal güvenlik borçları nedeniyle evinin açık arttırmaya çıkarıldığına dair bir gazete ilanının internette de yayınlanması üzerine, bilgilerin artık önemsiz olduğu gerekçesiyle silinmesini, ayrıca Google Spain ve Google Inc.'den de, ilgili sayfaların arama sonuçlarından çıkarılmasını talep etmiştir. Talepleri yerine getirilmeyen González, AEPD'ye başvurmuş, AEPD gazetedeki yayının hukuki dayanağı olduğu gerekçesiyle gazeteye karşı yapılan başvuruyu reddetmiş, ancak Google Spain ve Google Inc. yönünden, linklerin arama sonuçlarından kaldırılmasına karar vermiştir. Google karara karşı İspanyol mahkemelerine başvurmuş, davanın görüldüğü İspanyol mahkemesi ise ABAD'a başvurarak, AB kişisel verilerin korunması hukuku uyarınca arama motorlarının bu yönde bir sorumluluğu olup olmadığını, varsa bu sorumluğun kapsamının tespitini istemiştir. ABAD, arama motoru işleten kişilerin veri sorumlusu tanımı kapsamında olduğuna ve veri öznelerinin silme hakkı uyarınca AB kişisel verilerin korunması hukuku kapsamında veri sorumlularının ilgili sorumluluklarının bu kişiler için de geçerli olacağına karar vermiştir. Buna göre, arama sonucunun yönlendirdiği sayfada veriler hukuka uygun olarak yer alsa bile, arama motorları bu sayfayı arama sonuçlarından kaldırmak zorundadır. Özellikle ABAD'ın düşünceyi açıklama özgürlüğü yönünden yaratacağı etkiyi dikkate almaması nedeniyle, en çok eleştirilen

---

[224] Tüzük'ün unutulma hakkını düzenleyen 17 nci maddesinin başlığı "silme hakkı" ("right to erasure") olup, "unutulma hakkı" ifadesine parantez içinde yer verilmiştir. Ancak ilk taslakta doğrudan "unutulma hakkı" ifadesi kullanılmıştı. Tüzük'ün hazırlık sürecinde unutulma hakkının nasıl düzenleneceğine yönelik tartışmalar için bkz. **Başalp**, s. 97-99.

[225] **Küzeci**, s. 231.

[226] Kararın tam adı için bkz. yuk. dpn. 155.

karar bu olmuştur.[227] [228] Arama motorlarının sorumluluğunun varlığını ve kapsamını tespit ettikten sonra, ABAD, veri öznelerine Direktif'te tanınan hakkın kapsamını incelemiş, özel yaşamın gizliliği ve kişisel verilerin korunması haklarının kural olarak veri sorumlusunun ekonomik çıkarlarının ve kamunun haber almadaki yararına üstün olacağı sonucuna varmıştır. Ancak "kural olarak" ifadesinden de anlaşılabileceği gibi, istisnalar söz konusu olabilmektedir.[229] Silinmesi istenen kişisel verilerin eksik veya yanlış olmasına gerek yoktur, tutulmasının gereksiz olması, hatta veri öznesinin verilerinin tutulmasından rahatsız olması dahi yeterlidir. Kişisel verilerin tutulmasının ne zaman gereksiz hale geldiği, somut olayın koşullarına göre değerlendirilmelidir. Madde 29 Çalışma Grubu, kararın ardından, kararın uygulanmasına ilişkin bir rehber yayınlamıştır.[230]

Google Spain dışında, ulusal ve uluslararası diğer pek çok içtihadın gelişimine katkıda bulunduğu[231] unutulma hakkı, Tüzük'ün 17 nci maddesinde, son derece geniş kapsamlı olarak düzenlenmiştir. Buna göre,

- Kişisel verilerin, toplanma ya da başka bir şekilde işlenme amacı doğrultusunda artık gerekli olmaması (GDPR §17/1-a),

---

[227] Orla **Lynskey** (2015), "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja González", The Modern Law Review, C. 78, S. 3, s. 522-523.

[228] Google Spain kararına yönelik diğer bazı eleştiriler, ABAD'ın Direktif bağlamında "arama motoru" kavramını yanlış yorumladığı (bkz. **Kerr**, s. 221 vd.) ve kişisel verilerin korunması hakkının bilgi alma hakkı gibi bazı yarışan haklarla bağdaştırılamadığıdır (bkz. **Lynskey**, *Control over Personal Data*, s. 530).

[229] ABAD, C-131/12, par. 97.

[230] Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v AAgencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12.

[231] ABAD'ın Bodil Lindqvist kararı (*Bodil Lindqvist* v *Åklagarkammaren i Jönköping*, C-101/01), unutulma hakkı bakımından etki doğuran en eski kararlardandır. Olayda, İsveç'te bir kilisede çalışan Bodil Lindqvist, internet sayfasında, cemaat üyelerinin, aralarında özel nitelikli verilerin de bulunduğu kişisel bilgilerini, ilgili kişilerin rızası olmadan yayınlamış, ayrıca İsveç'teki veri koruma otoritesini de bilgilendirmemiş, bunun sonucunda hakkında soruşturma başlatılmıştır. Dava her ne kadar Lindqvist'in Direktif'e aykırı işleme faaliyetlerinden kaynaklansa da, Direktif'e aykırı işleme ile ifade özgürlüğü arasındaki denge de kararda tartışılmıştır. Nitekim Tüzük'ün 85 inci maddesi, Tüzük'te kişisel verilerinin korunmasına yönelik olarak veri öznelerine tanınan haklar ile ifade özgürlüğü ve bilgi edinme hakkı gibi haklarla bağdaştırılmasına ilişkin bir hükümdür. Karar için bkz. http://curia.europa.eu/juris/liste.jsf?num=C-101/01 (Erişim tarihi: 7/5/2019). Ayrıca İsviçre Federal Mahkemesi'nin içtihatları da unutulma hakkının gelişiminde önemli rol oynamıştır, bu konuda ayrıntılı bilgi için bkz. **Başalp**, s. 94 vd.

- Veri öznesinin, kişisel verilerinin işlenmesine rızasını geri alması ve farklı bir hukuka uygunluk sebebinin olmaması (GDPR §17/1-b),
- GDPR §21 esasları çerçevesinde veri öznesinin işlemeye itiraz etmesi ve veri sorumlusunun üstün gelen meşru bir dayanağının bulunmaması (GDPR §17/1-c),
- Kişisel verilerin hukuka aykırı olarak işlenmesi (GDPR §17/1-d),
- Veri sorumlusunun AB ya da Üye Devlet hukukundan kaynaklanan bir sorumluluğunun, kişisel verilerin silinmesini gerektirmesi (GDPR §17/1-e),
- Kişisel verilerin, bir çocuğa bilgi toplumu hizmetlerinin sunulmasına ilişkin olarak toplanması (GDPR §17/1-f) hallerinde veri özneleri, kendilerini ilgilendiren kişisel verilerin gecikmeksizin silinmesini talep edebileceklerdir. Veri sorumluları da haksız bir gecikme olmaksızın bu talebi yerine getirmekle yükümlüdür.

Veri sorumluları, silinmesi talep edilen kişisel verileri kamuya açmış olmaları halinde, mevcut teknolojik imkanlar ve bu teknolojilerin uygulanmasının yol açacağı masrafları göz önüne alarak, veriyi işleyen diğer veri sorumlularına, verilerin silinmesi talebini bildirmek için gerekli makul adımları atmalıdır (GDPR §17/2).

Tüzük, bu hakkın istisnalarını da aynı maddenin üçüncü fıkrasında düzenlemiştir. Buna göre,

- İfade özgürlüğünün ya da bilgi alma hakkının kullanılması (GDPR §17/3-a),
- Veri sorumlusunun AB ya da Üye Devlet hukukundan kaynaklanan bir sorumluluğu, kamu yararına bir görev ya da resmi bir yetkinin kullanılmasının, silinmesi istenen kişisel verilerin işlenmesini gerektirmesi (GDPR §17/3-b),
- Özel nitelikli kişisel verilerin işlenmesine ilişkin esaslara uyulmak koşuluyla, kamu sağlığına ilişkin nedenlerin varlığı (GDPR §17/3-c),
- İlgili kişisel verilerin silinmesi, bu amaçlara ulaşılmasını imkansız hale getirecek ya da önemli ölçüde güçleştirecekse, kamu yararı nedeniyle arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla kişisel verilerin işlenmesi (GDPR §17/3-d),

- Bir yasal hakkın kurulması, kullanılması ya da savunulması (GDPR §17/3-e) hallerinde, işlemenin bu haller kapsamında gerekli olduğu ölçüde, veri sorumlusu, veri öznesinin kişisel verilerinin silinmesi talebini yerine getirmekle yükümlü değildir.

Son olarak veri sorumluları, imkansız olmadığı ya da orantısız bir çaba gerektirmediği hallerde, kişisel verilerin silindiğini, kişisel verileri açıkladığı her alıcıya bildirmekle ve veri sorumlusunu bu alıcılar hakkında bilgilendirmekle yükümlüdür (GDPR §19).

III.A.5.İşlemenin Sınırlandırılması Hakkı

Tüzük'teki tanımıyla işlemenin sınırlandırılması ("restriction of processing"), saklanan kişisel verilerin, gelecekte işlenmesinin önüne geçmek amacıyla işaretlenmesidir (GDPR §4/3). Veri özneleri, işlemenin sınırlandırılmasını, Tüzük'ün 18 inci maddesi uyarınca talep edebilecektir.

Veri öznesinin hangi hallerde ve koşullarda işlemenin sınırlandırılmasını talep edebileceği, anılan maddenin birinci fıkrasında sayılmıştır. Buna göre, veri öznesi, kişisel verilerin doğruluğuna itiraz ederse, veri sorumlusundan, verilerin doğruluğunu tespit etmesi için yeterli bir süre boyunca işlemeyi sınırlandırmasını talep edebilecektir (GDPR §18/1-a).

Hukuka aykırı işleme hallerinde de veri öznesi, kişisel verilerinin silinmesine karşı çıkarak işlemenin sınırlandırılmasını talep edebilir (GDPR §18/1-b).

Veri sorumlusunun, işleme amaçları doğrultusunda kişisel verilere ihtiyacının olmadığı hallerde, veri öznesi, bir yasal hakkının kurulması, kullanılması ya da savunulması için kişisel verilere ihtiyaç duyuyorsa, veri öznesi yine işlemenin sınırlandırılmasını talep edebilecektir (GDPR §18/1-c).

Nihayet, veri öznesi, aşağıda incelenecek olan itiraz hakkını kullandığında, veri sorumlusunun meşru menfaatlerinin, veri öznesinin meşru menfaatlerine üstün gelip gelmediğinin belirlenmesine kadar işlemenin sınırlandırılmasını talep edebilir (GDPR §18/1-d).

Yukarıda sayılan hallerde işleme sınırlandırılmış ise, ilgili kişisel veriler, yalnızca veri öznesinin rızası; yasal hakların kurulması, kullanılması ya da savunulması; başka bir gerçek ya da tüzel kişinin haklarının korunması veya AB ya da bir Üye Devletin kamu yararına ilişkin sebepler doğrultusunda işlenebilir. Kişisel verilerin saklanması bu düzenleme kapsamında değildir (GDPR §18/2).

Kişisel verilerinin işlenmesi sınırlandırılmış olan veri öznesi, bu sınırlamanın kaldırılmasından önce bilgilendirilmelidir (GDPR §18/3). Ayrıca veri sorumluları, imkansız olmadığı ya da orantısız bir çaba gerektirmediği hallerde, işlemenin sınırlandırıldığını kişisel verileri açıkladığı her alıcıya bildirmekle ve veri sorumlusunu bu alıcılar hakkında bilgilendirmekle yükümlüdür (GDPR §19).

III.A.6.Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı, unutulma hakkı ile birlikte Tüzük'te öngörülen iki yeni haktan biridir.[232] Direktif'te veri taşınabilirliği ya da buna benzer bir hak düzenlenmemiş olup, ayrıca ABAD içtihatlarında Tüzük'te düzenlendiği haliyle veri taşınabilirliği ya da buna benzer bir hakkın varlığından da söz edilmemektedir.[233] Bu hususlar göz önüne alındığında, veri taşınabilirliği hakkının ilk kez Tüzük'te düzenlenen bütünüyle yeni bir hak olduğu söylenebilir.[234]

Veri taşınabilirliği hakkı, Tüzük'ün 20 nci maddesinde düzenlenmiştir. Buna göre, veri öznesi, veri sorumlusuna temin etmiş olduğu kişisel verilerinin; düzenli, yaygın kullanılan ve makinelerce okunabilen bir formatta kendisine verilmesini isteyebilir ve veri sorumlusu tarafından zorluk çıkarılmaksızın farklı bir veri sorumlusuna aktarabilir (GDPR §20/1). Böylelikle veri öznelerinin kişisel verilerini bir elektronik hizmet sağlayıcısından diğerine kolaylıkla aktarmasına imkan

---

[232] **Voss**, s. 4.

[233] **Lynskey**, *The Foundations*, s. 129.

[234] Bununla birlikte Hustinx'e göre, veri taşınabilirliği esasen, mevcut bir hak olan kişisel verilerin bir kopyasını talep etme hakkının özel bir halidir, bkz. Peter **Hustinx** (2013), "EU Data Protection Law - Current State and Future Perspectives", High Level Conference: "Ethical Dimensions of Data Protection and Privacy", Centre for Ethics, University of Tartu/ Data Protection Inspectorate, Tallinn, s. 11. - https://edps.europa.eu/sites/edp/files/publication/13-01-09_speech_tallinn_en.pdf (Erişim tarihi: 8/5/2019)

tanınarak, bu değişikliğin yol açacağı masraflar azaltılmaktadır.[235] Tüzük'ün teknik olarak mümkün olduğu hallerde, kişisel verilerin doğrudan bir veri sorumlusundan diğerine aktarılabileceğini öngörmesi de (GDPR §20/2) bu amaca yöneliktir.

Veri taşınabilirliği hakkı, ancak işlemenin rızaya dayandığı ya da bir sözleşmenin kurulması veya ifası için gerekli olduğu (GDPR §20/1-a) ve otomatik yollarla gerçekleştiği (GDPR §20/1-b) kullanılabilir.

Veri taşınabilirliği hakkının kullanılması, veri öznesinin, unutulma hakkı çerçevesinde kişisel verilerin silinmesini talep etmesini etkilemez. Bu hak, kişisel verilerin işlenmesinin veri sorumlusunun kamu yararına bir görev yerine getirmesi ya da resmi yetkilerini kullanması için gerekli olduğu hallerde, hakkın niteliği gereği[236] kullanılamayacaktır (GDPR §20/3). Ayrıca bu hakkın kullanılması, başkalarının hak ve özgürlüklerini olumsuz etkilememelidir (GDPR §20/4).

III.A.7.İtiraz Hakkı

Veri özneleri, kendilerine ilişkin kişisel verilerin işlenmesine, Tüzük'ün 21 inci maddesi doğrultusunda itiraz edebilirler. Bu hak daha önce, Direktif'in 14 üncü maddesinde düzenlenmişti.

Veri öznesi, içinde bulunduğu duruma ilişkin nedenlerle, kamu yararına görevin yerine getirilmesi veya resmi bir yetkinin kullanılması ya da veri sorumlusunun veya diğer kişilerin meşru menfaatlerine dayanan işleme faaliyetlerine her zaman itiraz edebilir. Bu hükümler çerçevesinde gerçekleştirilen profil çıkarma işlemleri de bu kapsamdadır. Veri öznesinin itirazı halinde, veri sorumlusu, ancak veri öznesinin hak ve özgürlüklerine üstün gelen bir dayanağın varlığını ya da işlemenin bir hakkın kurulması, kullanılması ya da savunulması için gerekli olduğunu ikna edici bir şekilde ortaya koyduğu takdirde işlemeye devam edebilecektir (GDPR §21/1). Kamu yararı nedeniyle arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla kişisel verilerin işlenmesi halinde de işlemeye itiraz mümkündür, ancak bu hallerde, işleme, kamu yararına bir görevin yerine getirilmesi için gerekli olmamalıdır (GDPR §21/6). İtiraz hakkı, amaçla ilişkili

[235] **Lynskey**, *The Foundations*, s. 38.

[236] Tüzük, Gerekçe 68.

olduğu ölçüde, doğrudan pazarlama ("direct marketing")[237] amacı çerçevesinde gerçekleşen işleme ve profil çıkarma faaliyetlerine karşı da kullanılabilir (GDPR §21/2). Bu durumda kişisel veriler artık bu amaç doğrultusunda işlenemez (GDPR §21/3).

En geç veri öznesiyle ilk iletişim kurulma anında, veri öznesi, itiraz hakkının varlığından açıkça haberdar edilmeli, bu husus, açık ve diğer bilgilerden ayrı bir şekilde bildirilmelidir (GDPR §21/4). Yukarıda da belirtildiği gibi, itiraz hakkından veri öznesinin haberdar edilmesi, bilgi edinme hakkı çerçevesinde, işlemenin dürüstlük ve şeffaflığının sağlanmasının da bir gereğidir (GDPR §13/2-b). Bu hususun, bildirimin nasıl yapılması gerektiği de açıklanarak tekrarlanmasının, Tüzük'te itiraz hakkına verilen önemin bir göstergesi olduğu söylenebilir.

Bilgi toplumu hizmetleri çerçevesinde itiraz hakkı, otomatik yollarla kullanılabilir (GDPR §21/5).

III.A.8.Otomatik Bireysel Karar Alma ("Automated Individual Decision-making") Uygulamalarına Konu Olmama Hakkı

Tüzük'te "otomatik bireysel karar alma" şeklinde bir kavram doğrudan tanımlanmamış olmakla birlikte, 22 nci maddede yer alan "yalnızca otomatik yollarla işlemeye dayanan karar" ifadesinden, bu tarz kararların alınmasının ifade edilmek istendiği anlaşılmaktadır. Anılan madde uyarınca, veri özneleri, profil çıkarma da dahil olmak üzere, yalnızca otomatik yollarla kişisel verilerinin işlenmesine dayanan ve kendileri hakkında hukuki sonuçlar doğuran ya da benzer şekilde onları ciddi derecede etkileyen[238] kararlara konu olmama hakkına sahiptir (GDPR §22/1). Benzer

---

[237] "Doğrudan pazarlama" kavramının tanımına Tüzük'te yer verilmemiştir. Doktrinde, "hedeflenen müşteri ya da müşteri gruplarıyla doğrudan, sıklıkla karşılıklı olarak bağlantı kurulması" şeklinde bir tanım mevcuttur, bkz. **Kotler** / **Armstrong**, s. 496. Bunun dışında, Direktif'in 30 uncu Gerekçesi, "ticari olarak veya bir yardım kuruluşu veya örneğin, siyasal nitelikli başka bir dernek veya vakıf tarafından gerçekleştirilen pazarlama amacıyla kişisel verilerin üçüncü bir kişiye açıklanması koşulları" şeklinde bir ifadeye yer vermiştir, bkz. **Küzeci**, s. 236, dpn. 134.

[238] "Ciddi derecede etkileme" kriteri Tüzük taslak aşamasındayken eleştirilmiş, ancak bu ifade Tüzük'ün son halinde herhangi bir değişikliğe uğramadan yer almıştır. Bu konuda bkz. **Develioğlu**, s. 97.

bir düzenleme Direktif'in 15 inci maddesinde de yer almış, bu tarz uygulamaların hangi amaçlar doğrultusunda yapılabileceği de örnek olarak sayılmıştır. Buna göre, otomatik bireysel karar alma uygulamalarının, kişinin iş performansı, kredi verilebilirlik durumu, güvenilirliği, tavır ve tutumu gibi kişisel özelliklerinin değerlendirilmesi bu amaçlar arasındadır (DPD §15/1). Tüzük'te ise tüm bu faaliyetler "profil çıkarma" kapsamına girdiğinden[239] tekrar sayılmamıştır.

GDPR §22, ikinci fıkrasında bu hakkın istisnalarını da saymıştır. Buna göre, otomatik bireysel kararların, veri öznesi ile veri sorumlusu arasında bir sözleşmenin kurulması ya da ifası için gerekli olması (GDPR §22/2-a); AB ya da veri sorumlusunun tabi olduğu Üye Devlet hukukunun izin vermesi ve veri öznesinin hak ve özgürlükleri ile meşru menfaatlerini güvence altına almaya yönelik uygun önlemler öngörmesi (GDPR §22/2-b) ya da veri öznesinin rızasına dayanması (GDPR §22/2-c) hallerinde, veri öznesinin bu hakkını kullanması sınırlandırılmıştır. Otomatik bireysel kararların sözleşmenin kuruluşu veya ifası için gerekli olması ya da veri öznesinin rızasına dayanması hallerinde, veri sorumlusu, veri öznesinin hak ve özgürlükleri ile meşru çıkarlarını güvence altına almaya yönelik uygun önlemler almalı, veri öznesine en azından sürece bir insanın müdahalesini isteme, görüşünü belirtme ve karara itiraz etme haklarını sağlamalıdır (GDPR §22/3).

Özel nitelikli kişisel verilere dayanan otomatik bireysel kararlar yönünden, kural olarak, yukarıda sayılan istisna halleri geçerli değildir. Bu tarz otomatik bireysel kararların alınması yalnızca, veri öznesinin rızasının varlığı ya da ciddi kamu yararı için gerekli olması hallerinde mümkündür. Veri öznesinin hak ve özgürlükleri ile meşru menfaatlerini güvence altına almak için uygun güvenlik önlemlerinin alınmış olması da gerekmektedir (GDPR §22/4).

III.A.9.Sınırlama Halleri

Tüzük, 23 üncü maddesinde, yukarıda sayılan hakların, AB ya da veri sorumlusunun tabi olduğu Üye Devlet hukukunda hangi hallerde ve ne şekilde sınırlanabileceğini düzenlemiştir. Buna göre, sınırlama, temel hak ve özgürlüklerin

[239] Tüzük, Gerekçe 71.

özüne saygılı olarak, demokratik bir toplumda gerekli ve ölçülü bir önlem olması koşuluyla, aşağıdaki hallerde mümkündür:

- Ulusal güvenlik (GDPR §23/1-a),
- Savunma (GDPR §23/1-b),
- Kamu güvenliği (GDPR §23/1-c),
- Kamu güvenliğine karşı tehditlere karşı ya da bunların önlenmesi amacıyla güvenlik önlemlerinin alınması da dahil olmak üzere, suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması ile cezaların infazı (GDPR §23/1-d),
- AB ya da Üye Devletin kamu yararına ilişkin diğer önemli amaçları, özellikle parasal, bütçesel ve vergilendirmeye ilişkin olanlar da dahil olmak üzere önemli ekonomik ya da finansal menfaatler, kamu sağlığı ve sosyal güvenliğe ilişkin menfaatler (GDPR §23/1-e),
- Yargı bağımsızlığının ve yargılama faaliyetlerinin korunması (GDPR §23/1-f),
- Kanunla düzenlenen mesleklerde etik kuralı ihlallerinin önlenmesi, soruşturulması, tespiti ve kovuşturulması (GDPR §23/1-g),
- a, e ve g bentlerinde sayılan hallerde, bu hallere ilişkin izleme, denetleme ve düzenleme faaliyetleri ile kimi durumlarda resmi bir yetkinin kullanılması (GDPR §23/1-h),
- Veri öznesinin ya da başkalarının hak ve özgürlüklerinin korunması (GDPR §23/1-i),
- Medeni hukuktan kaynaklanan hakların icrası (GDPR §23/1-j).

Sınırlama öngören düzenlemelerde yer alması gereken hususlar, GDPR §23/2'de düzenlenmiştir. Buna göre, bu düzenlemelerde asgari olarak, ilgili olduğu hallerde, şu hususlara ilişkin özel hükümlere yer verilmelidir:

- İşlemenin amaçları ya da işleme kategorileri (GDPR §23/2-a),
- Kişisel veri türleri (GDPR §23/2-b),
- Getirilen sınırlamaların kapsamı (GDPR §23/2-c),

- Kişisel verilerin kötüye kullanılmasının, hukuka aykırı erişiminin ya da transferinin önlenmesine yönelik güvenlik önlemleri (GDPR §23/2-d),
- Veri sorumlularının ya da veri sorumlusu kategorilerinin belirlenmesi (GDPR §23/2-e),
- İşlemenin ya da işleme kategorilerinin doğası, kapsamı ve amaçları göz önüne alınarak, kişisel verilerin ne kadar saklanacağı ve uygulanabilir güvenlik önlemleri (GDPR §23/2-f),
- Veri öznelerinin hak ve özgürlüklerine yönelik riskler (GDPR §23/2-g),
- Sınırlamanın amacını etkilemediği sürece, veri öznelerinin sınırlama hakkında bilgilendirilme hakkı (GDPR §23/2-h).

III.A.10.Hukuki Çarelere Başvurma Hakkı

Tüzük'ün 77 ila 84 üncü maddeleri veri öznelerinin başvurabileceği hukuki çareler ile Tüzük'ün ihlalinden kaynaklanan zararların tazminine ve veri sorumlularına uygulanacak yaptırımlara ilişkin esasları düzenler. Veri öznelerinin başvurabileceği hukuki çareler burada incelenecek olup, tazminat ve yaptırımlara ilişkin esaslar çalışmanın devamında, "Veri Sorumlusunun Yükümlülükleri" başlığı altında incelenecektir.

III.A.10.a)Denetim Kurumuna Şikayette Bulunma Hakkı

Tüzük'ün 77 nci maddesi uyarınca, kişisel verilerinin işlenmesinin Tüzük'ü ihlal ettiği iddiasındaki her veri öznesi, özellikle mutad meskeninin veya işyerinin bulunduğu ya da iddia edilen ihlalin gerçekleştiği Üye Devletin denetim kurumuna, şikayette bulunabilir. Bu hakkın kullanılması, idari çarelere ya da kanun yollarına başvurma hakkının kullanılmasına engel değildir.

Denetim kurumu, şikayette bulunan veri öznesini, şikayetine dair gelişmeler ve şikayetin sonucu hakkında bilgilendirir. Denetim kurumu ayrıca, 78 inci madde kapsamında veri öznesinin kanun yollarına başvurma imkanı konusunda da bilgi verecektir (GDPR §77/2).

III.A.10.b)Kanun Yollarına Başvurma Hakkı

Veri özneleri, denetim kurumlarının kendilerini bağlayan kararlarına karşı kanun yollarına başvurabilecekleri gibi, Tüzük'e aykırı işleme sonucunda Tüzük'te yer alan haklarının ihlal edildiği iddiasıyla veri sorumlularına ya da veri işleyenlere karşı da başvurabilirler. Denetim kurumlarına karşı kanun yollarına başvuru hakkı 78, veri sorumluları ya da veri işleyenlere karşı kanun yollarına başvuru hakkı ise 79 uncu maddede düzenlenmiştir.

Yetkili denetim kurumunun şikayeti değerlendirmemesi ya da üç ay içinde veri öznesini şikayete dair gelişmeler ve şikayetin sonucu hakkında bilgilendirmemesi halinde, diğer çarelere başvurma hakkı etkilenmeksizin veri özneleri, denetim kurumuna karşı yasal yollara başvurabilir (GDPR §78/2). Başvuru, denetim kurumunun bağlı olduğu Üye Devlet mahkemelerine yapılacaktır (GDPR §78/3).

Diğer çarelere başvurma hakkı etkilenmeksizin, veri özneleri, Tüzük'e aykırı işleme sonucunda Tüzük'teki haklarının iddia edildiğini düşünen tüm veri özneleri, veri sorumlularına ya da veri işleyenlere karşı da kanun yollarına başvurabilecektir (GDPR §79/1). Başvuru, veri sorumlusunun ya da veri işleyenin kuruluşunun yer aldığı Üye Devlet mahkemelerine yapılacaktır. Bunun dışında, veri öznesinin, mutad meskeninin bulunduğu Üye Devlet mahkemelerine başvurma seçeneği de bulunmaktadır, ancak bunun için veri sorumlusu ya da veri işleyen, kamu gücünü kullanan bir Üye Devlet kamu makamı olmamalıdır (GDPR §79/2).

Veri özneleri, hukuki çarelere başvuru haklarını kullanırken, bir Üye Devlet hukukuna uygun olarak kurulmuş, kamu yararına çalışan, kişisel verilerin korunması hukukundan kaynaklanan hak ve özgürlükleri koruma alanında aktif olan ve kar amacı gütmeyen kuruluş, örgüt ve dernekler tarafından temsil edilebilirler. Bu kurumlar veri öznesi tarafından temsil için yetkilendirilebilirler, ancak Üye Devlet hukukunda bu kurumlara, Tüzük'ten kaynaklanan bir hakkın ihlal edildiğini düşünüyorlarsa, veri öznesi tarafından yetkilendirilmeksizin de bu hakları kullanma imkanı tanınabilir (GDPR §80).

III.B. Veri Sorumlusunun ve Veri İşleyenin Yükümlülükleri

Tüzük'ün 24 ila 43 üncü maddeleri, veri sorumlularının ve veri sorumlusu adına çalışan veri işleyenlerin yükümlülüklerini, oldukça geniş kapsamlı olarak düzenlemiştir. 82 nci madde ve devamında ise, kişisel verilerin Tüzük'e aykırı olarak işlenmesinden kaynaklanan zararların tazmini ile idari ve cezai yaptırımlara ilişkin esaslar düzenlenmiştir.

III.B.1. Veri Sorumlusunun Genel Sorumluluğu

Tüzük, "Veri Sorumlusunun Sorumluluğu" başlıklı 24 üncü maddesinde, veri sorumlusunun genel olarak tedbir alma sorumluluğu üzerinde durmuştur. Veri sorumlusu, işleme faaliyetinin doğası, kapsamı ve amaçlarının yanı sıra gerçek kişilerin hak ve özgürlüklerine karşı, olasılık ve şiddet bakımından farklılık gösteren riskleri de göz önüne alarak, işlemenin Tüzük'e uygun yapılabilmesi için gerekli teknik ve kurumsal önlemleri almalı, gerektiği takdirde bu önlemleri gözden geçirmeli ve güncellemelidir. İşleme faaliyeti açısından ölçülü olmak kaydıyla, uygun veri koruma politikalarının benimsenmesi de bu önlemler arasındadır (GDPR §24/2).

Tüzük'te, hangi önlemlerin alınması gerektiği, önlemlerin ne şekilde alınması gerektiği ya da hangi koşullarda önlemlerin alınmış sayılacağı konusunda bir hüküm yer almamaktadır. Bununla birlikte, 40 ıncı maddede düzenlenen davranış kurallarının belirlenerek bunlara bağlı kalınması ya da 42 nci madde esasları çerçevesinde sertifika alınmış olması, veri sorumlusunun öngörülen yükümlülüklerine uygun hareket ettiğinin ortaya koyulmasında kullanılabilir (GDPR §24/3).

III.B.2. Tasarımsal Koruma ve Varsayılan Koruma

AB Veri Koruma Reformu incelenirken, tasarımsal gizlilik ve varsayılan gizlilik ilkeleri üzerinde kısaca durulmuştu. Tasarımsal gizlilik kavramının ilk olarak

Ann Cavoukian tarafından ortaya atıldığı bilinmektedir.[240] Cavoukian, tasarımsal gizliliğin sağlanabilmesi için uyulması gereken yedi temel ilke öngörmüştür. Buna göre,

- Tasarımsal gizlilik kapsamında alınacak önlemler reaktif değil proaktif olmalıdır. Zararların tazminine değil önlenmesine yönelik olmalıdır.
- Gizlilik varsayılan olmalıdır. Sistemler, bireylerin gizliliklerini sağlamak adına herhangi bir işlem yapmasını gerektirmeyecek şekilde tasarlanmalıdır.
- Gizlilik, tasarımın bir parçası olmalı, sonradan eklenmiş olmamalıdır.
- Tasarım, tamamen fonksiyonel olmalı, gizlilik ile güvenlik arasında seçim yapmak zorunda bırakmamalıdır.
- Verinin yaşam döngüsü boyunca, toplanmasından yok edilmesine kadar gizliliği gözetilmelidir.
- Sistemin tüm parçaları ve işlemleri, kullanıcılar ve hizmet sağlayıcılar için görülebilir ve şeffaf olmalıdır.
- Sistem, kullanıcının gizliliğini ve diğer menfaatlerini ön planda tutmalıdır.[241]

Yukarıdaki ilkeler ışığında,[242] Tüzük, "Tasarımsal ve Varsayılan Koruma"[243] başlıklı 25 inci maddesinin birinci fıkrasında, veri sorumlularına; teknolojinin geldiği son durum, uygulama masrafları, işleme faaliyetinin doğası, kapsamı ve amaçlarının yanı sıra gerçek kişilerin hak ve özgürlüklerine karşı, olasılık ve şiddet bakımından

---

[240] **Lambert**, s. 329.

[241] Ann **Cavoukian** (2010), "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D", Identity in the Information Society, C. 3, S. 2, s. 249-250.

[242] Tüzük'te yer alan düzenlemenin amacının sadece sayılan ilkelerin değil, kişisel verilerin korunması ilkelerinin hayata geçirilmesi olduğu da ifade edilmelidir. Tasarımsal gizliliğin temel ilkeleri dikkate alınacak ve mümkün olduğu ölçüde uygulanacaktır, ancak düzenleme, sistemleri tasarlayan kişilerden ziyade veri sorumlularına ilişkindir. Bu anlamda, düzenlemenin kapsamı, bu yedi ilke ile öngörülenden daha dardır, bkz. Aurelia **Tamò-Larrieux** (2018), Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, Springer, s. 86.

[243] "Tasarımsal ve varsayılan gizlilik" ve "tasarımsal ve varsayılan koruma" kavramlarının birbirinden ne ölçüde farklılık gösterdiği konusunda farklı görüşler bulunmaktadır. Kimi yazarlar tasarımın verilerin korunmasını ve gizliliğini sağlayacak şekilde yapılmasını, bireylerin kişisel verileri üzerindeki kontrolünün arttırılmasından farklı görürken, bu iki olgunun bir madalyonun iki yüzü olduğu da ifade edilmektedir, bkz. **Lynskey**, *The Foundations*, s. 262.

farklılık gösteren riskleri de göz önüne alarak, hem işleme yöntemlerinin belirlenmesi hem de işleme faaliyeti sırasında, kişisel verilerin korunması ilkelerine uyulmasına yönelik uygun teknik ve kurumsal önlemleri alma yükümlülüğü getirmiştir. Bu önlemler etkin bir şekilde uygulanacak ve işleme faaliyetine entegre edilecektir. Bu hüküm ile, tasarımsal gizlilik ilkesinin, kişisel verilerin korunması bakımından hayata geçirilmesi (tasarımsal koruma) amaçlanmıştır.

Veri sorumluları ayrıca, yalnızca işlemenin her belirli amacı için gerekli olan kişisel verilerin işlenmesini güvence altına almak üzere, uygun teknik ve kurumsal önlemleri almakla yükümlüdür. Bu yükümlülük, toplanan kişisel veri miktarı, işlemenin kapsamı, verilerin saklama süresi ve erişilebilirliği yönünden de söz konusudur. Önlemler, özellikle bireysel müdahale olmaksızın kişisel verilerin belirsiz sayıda gerçek kişinin erişimine açık olmamasını sağlamalıdır (GDPR §25/2). Bu hüküm de, varsayılan gizlilik ilkesinin, kişisel verilerin korunması hukuku bakımından hayata geçirilmesi (varsayılan koruma) amacına yöneliktir.

III.B.3.Ortak Veri Sorumluluğu

Tüzük'te, ortak veri sorumululuğu halinde yükümlülüğe ilişkin esaslar 26 ncı maddede düzenlenmiştir. Buna göre, yalnızca ortak veri sorumluluğundan kaynaklanan özel bir yükümlülük bulunmamaktadır. Tüzük'te öngörülen, özellikle veri öznelerinin haklarını kullanması ile 13 ve 14 üncü maddeler uyarınca veri öznesine bilgi verilmesine ilişkin yükümlülükler çerçevesinde her veri sorumlusuna düşen yükümlülük, şeffaf bir şekilde belirlenecektir. Bu çerçevede veri öznesi için bir iletişim noktası da belirlenebilir. Bu hüküm, AB veya Üye Devlet hukukunda yükümlülük dağılımının belirlenmediği hallerde geçerlidir.

Ortak veri sorumlularının görevleri ve bunlar arasındaki ilişki, veri öznelerine tam olarak yansıtılmalı, anlaşmanın esası veri öznelerine açık olmalıdır (GDPR §26/2). Veri özneleri, yükümlülük dağılımı ne şekilde yapılmış olursa olsun, Tüzük'te kendisine tanınan hakları, ortak veri sorumlularından her birine karşı kullanabilir (GDPR §26/3).

III.B.4. Temsilci Atama Yükümlülüğü

Tüzük'ün 27 nci maddesi uyarınca, veri sorumlusunun ya da veri işleyenin, AB sınırları içinde kuruluşunun bulunmadığı hallerde, veri sorumlusu ya da veri işleyen, yazılı olarak AB sınırları içinde bir temsilci atamakla yükümlüdür. Temsilci, GDPR §3/2 kapsamında kişisel verileri işlenecek olan veri öznelerinin bulunduğu Üye Devletlerin birinde yer almalıdır (GDPR §27/3). Veri sorumlusu ya da veri işleyen, temsilciyi, kendisiyle birlikte ya da kendisi yerine, özellikle veri özneleri ve denetim kurumları tarafından, işlemeye ilişkin konularda ve Tüzük'e uyulmasının sağlanmasına yönelik amaçlarla yapılacak başvurular yönünden sorumlu kılacaktır (GDPR §27/4).

Temsilci atama yükümlülüğü, işlemenin sürekli olmaması, geniş kapsamda özel nitelikli ya da cezai mahkumiyet ve suçlara ilişkin kişisel verilere yönelik olmaması; doğası, bağlamı, kapsamı ve amaçları göz önüne alındığında gerçek kişilerin hak ve özgürlüklerine yönelik bir risk oluşturmasının olası görülmediği hallerde söz konusu değildir (GDPR §27/2-a). Ayrıca kamu kurumları ve makamları yönünden de böyle bir sorumluluk yoktur (GDPR §27/2-b).

III.B.5. Veri İşleyenlerin Görevlendirilmesine İlişkin Esaslar

Veri sorumlusunun veri işleyenleri hangi esaslara göre seçeceği ve bu veri işleyenlerin tabi olacağı yükümlülükler, Tüzük'ün 28 inci maddesinde son derece detaylı olarak düzenlenmiştir. Buna göre veri sorumluları, ancak uygun teknik ve kurumsal önlemleri, işlemenin Tüzük'te öngörülen koşulları karşılamasını ve veri öznelerinin haklarının korunmasının güvence altına alınmasını sağlayacak şekilde uygulayacağına ilişkin yeterli güvence sağlayan veri işleyenleri görevlendirebilir (GDPR §28/1).

Görevlendirilen veri işleyenler, önceden veri sorumlusundan yazılı olarak genel veya özel izin almadığı takdirde başka bir veri işleyen görevlendiremez. Genel iznin varlığı halinde, veri işleyen, yeni veri işleyenler görevlendirilmesine ya da görevli veri işleyenlerin değiştirilmesine ilişkin yapmayı düşündüğü değişiklikleri

veri sorumlusuna bildirerek, veri sorumlusunun bu değişikliklere itiraz etmesine fırsat tanımalıdır (GDPR §28/2).

Veri işleyen tarafından gerçekleştirilecek işleme faaliyetleri, bir sözleşmeyle ya da AB veya Üye Devlet hukuku kapsamındaki diğer bir hukuki işlemle düzenlenmiş olmalıdır. Hukuki işlem, veri işleyen yönünden veri sorumlusu karşısında bağlayıcı olmalı; işlemenin konusunu, süresini, doğasını ve amacını, kişisel veri türlerini ve veri öznesi gruplarını ve veri sorumlarının hak ve yükümlülüklerini belirtmelidir (GDPR §28/3). Sözleşme ya da diğer bir hukuki işlemle öngörülen esaslar, veri işleyenin görevlendireceği diğer veri işleyenler yönünden de geçerli olacaktır (GDPR §28/4). Hukuki işlem, elektronik format da dahil olmak üzere yazılı olarak yapılmalıdır (GDPR §28/9).

III.B.6.Veri Sorumlusunun ya da Veri İşleyenin Talimatıyla Veri İşleyenlerin Yükümlülüğü

Tüzük'ün 29 uncu maddesine göre, veri sorumlusunun ya da veri işleyenin emri altında çalışan ve kişisel verilere erişimi olan kişiler, veri sorumlusunun talimatı olmaksızın bu verileri işlememelidir. AB ya da Üye Devlet hukukunun gerektirdiği haller istisnadır.

III.B.7.İşleme Kayıtlarının Tutulması Yükümlülüğü

Tüzük'ün 30 uncu maddesi, veri sorumluları ve varsa temsilcileri yönünden, sorumlulukları dahilindeki işleme faaliyetlerinin kayıtlarını tutma yükümlülüğü öngörmüştür. Kayıtlar, maddenin birinci fıkrasında sayılan aşağıdaki bilgilerin tamamını içermelidir:

- Veri sorumlusunun ve varsa ortak veri sorumlusunun, temsilcinin ve veri koruma yetkilisinin adı ve iletişim bilgileri (GDPR §30/1-a),
- İşleme amaçları (GDPR §30/1-b),
- Veri öznesi gruplarına ve kişisel veri türlerine ilişkin açıklama (GDPR §30/1-c),

- Üçüncü ülkelerdeki alıcılar ve uluslararası örgütler de dahil olmak üzere, kişisel verilerin açıklandığı ya da açıklanacağı alıcı grupları (GDPR §30/1-d),
- Üçüncü ülkelere ya da uluslararası örgütlere veri aktarımı söz konusuysa, hangi ülkeye ya da uluslararası örgüte aktarım yapıldığı ve yeterlilik kararı olmaksızın aktarım yapılıyorsa, uygun güvenlik önlemlerinin alındığının belgelenmesi de dahil olmak üzere söz konusu veri aktarımına ilişkin bilgiler (GDPR §30/1-e),
- Mümkün olduğu hallerde, farklı kişisel veri türlerinin silinmesi için planlanan süre (GDPR §30/1-f),
- Mümkün olduğu hallerde, işlemenin güvenliği için alınan teknik ve kurumsal önlemlerin genel bir açıklaması (GDPR §30/1-g).

Maddenin ikinci fıkrası, veri işleyenler ve temsilcileri yönünden kayıt tutma yükümlülüğü öngörmüştür. Buna göre bu kişiler; hangi veri sorumlusu adına hareket ettikleri ile kendilerinin ve varsa veri sorumlusunun temsilcisi ile veri koruma yetkilisinin adı ve iletişim bilgileri (GDPR §30/2-a), her veri sorumlusu adına gerçekleştirilen işleme faaliyeti kategorileri (GDPR §30/2-b), üçüncü ülkelere ya da uluslararası örgütlere veri aktarımı söz konusuysa, hangi ülkeye ya da uluslararası örgüte aktarım yapıldığı ve yeterlilik kararı olmaksızın aktarım yapılıyorsa, uygun güvenlik önlemlerinin alındığının belgelenmesi de dahil olmak üzere söz konusu veri aktarımına ilişkin bilgiler (GDPR §30/2-c) ve mümkün olduğu hallerde, işlemenin güvenliği için alınan teknik ve kurumsal önlemlerin genel bir açıklaması (GDPR §30/2-d) dahil olmak üzere, veri sorumlusu adına yaptıkları tüm işleme faaliyetlerinin kayıtlarını tutacaktır.

Kayıtlar, elektronik format da dahil olmak üzere yazılı olarak tutulacak ve denetim kurumlarının talebi halinde veri sorumlusunun ya da veri işleyenin temsilcisi tarafından bu kurumlara sunulacaktır (GDPR §30/3, 4).

Maddenin son fıkrası, kayıt tutma yükümlülüğünün istisnalarını düzenlemiştir. Buna göre, 250'den az çalışanı olan şirketler ve kuruluşlar, kayıt tutma yükümlülüğü altında değildir. Ancak bunun için işleme faaliyetlerinin veri öznelerinin hak ve özgürlükleri yönünden bir risk oluşturmasının olası olmaması,

sürekli olmaması ve özel nitelikli verilere veya ceza mahkumiyeti ve suçlara ilişkin kişisel verilere yönelik olmaması gerekir.

III.B.8.Denetim Kurumlarıyla İşbirliği Yükümlülüğü

Tüzük'ün 31 inci maddesi, veri sorumluları, veri işleyenler ve varsa bunların temsilcileri yönünden, denetim kurumlarının bu yönde bir talebinin olması halinde, görevlerinin yerine getirilmesinde bu kurumlar ile işbirliği yapma yükümlülüğü öngörmüştür.

III.B.9.Kişisel Verilerin Güvenliğinin Sağlanması

Tüzük'ün 32 ila 34 üncü maddeleri, "Kişisel Verilerin Güvenliği" başlığı altında, işleme faaliyetinin güvenliğinin sağlanması ve bir veri ihlali söz konusuysa, bu ihlalin denetim kurumuna ve veri öznesine bildirilmesi yükümlülüklerini düzenlemektedir.

III.B.9.a)İşleme Faaliyetinin Güvenliğinin Sağlanması

Tüzük'ün 32 nci maddesi uyarınca, veri sorumlusu ve veri işleyen; işleme faaliyetinin doğası, kapsamı ve amaçlarının yanı sıra gerçek kişilerin hak ve özgürlüklerine karşı, olasılık ve şiddet bakımından farklılık gösteren riskleri de göz önüne alarak, işlemenin risk düzeyi ile orantılı olacak ölçüde güvenliğini sağlamak üzere uygun teknik ve kurumsal önlemleri almalıdır. Bu düzenleme ile kişisel verilerin herhangi bir şekilde ele geçirilmesinden doğacak riskler ortadan kaldırılmak istenmiştir.[244]

Tüzük, uygun kabul edilebilecek önlemlerden bazılarını örnek olarak saymıştır. Buna göre, kişisel verilerin psödonimleştirilmesi ve şifrelenmesi bu kapsamdadır (GDPR §32/1-a). İşleme sistemlerinin ve hizmetlerinin devamlı olarak gizliliği, bütünlüğü, erişilebilirliği ve dayanıklılığının sağlanabilmesi (GDPR §32/1-b), fiziksel ya da teknik bir kaza halinde hızlı bir şekilde kişisel verilerin yeniden

[244] **Develioğlu**, s. 107.

erişilebilir hale getirilebilmesi (GDPR §32/1-c), teknik ve kurumsal önlemlerin düzenli olarak test edilmesi ve ne ölçüde etkili olduğunun değerlendirilmesi (GDPR §32/1-d) Tüzük'te sayılan diğer önlemlerdir.

Sağlanması gereken güvenlik seviyesinin tespitinde, herhangi bir veri işleme türü için piyasada mevcut bulunan güvenlik araçları, masraflar ve işleme faaliyetinin veri öznelerinin temel hak ve özgürlükleri için oluşturduğu riskler dikkate alınacaktır.[245] Aktarılan, saklanan ya da başka bir şekilde işlenen kişisel verilerin kazayla veya hukuka aykırı olarak imha edilmesi, kaybı, değiştirilmesi, yetkisiz olarak açıklanması ya da bu kişisel verilere yetkisiz erişim özellikle dikkate alınması gereken risklerdir (GDPR §32/2).

Veri sorumlusu veya veri işleyenler ayrıca, 29 uncu madde uyarınca kendilerinin talimatıyla çalışan ve kişisel verilere erişimi olan kişiler yönünden de gerekli önlemleri alacaktır (GDPR §32/4).

III.B.9.b)Bildirim Yükümlülüğü

Veri sorumluları, ne kadar sıkı ve kapsamlı önlemler almış olursa olsun, kişisel veri ihlallerinin[246] önlenebilmesi her zaman mümkün olmamaktadır. Bu hususu dikkate alarak, Tüzük, bir kişisel veri ihlalinin söz konusu olduğu hallerde, veri sorumluları için, hızlı bir şekilde ihlalin denetim kurumlarına ve veri öznelerine bildirimde bulunma yükümlülüğü öngörmüştür. Bu düzenlemenin, söz konusu ihlallerin yol açtığı zararların azaltılmasına katkıda bulunacağı,[247] veri öznesi

---

[245] Handbook on European Data Protection Law, s. 165.

[246] Kişisel veri ihlali ("personal data breach"); aktarılan, saklanan ya da herhangi bir şekilde işlenen kişisel verilerin, kazayla ya da hukuka aykırı olarak imha edilmesine, kaybına, değiştirilmesine, yetkisiz olarak açıklanmasına ya da bu kişisel verilere yetkisiz olarak erişilmesine yol açan bir güvenlik ihlalidir (GDPR §4/12). Bu tanım daha önce, 2002/58/AT sayılı Direktif'te, elektronik iletişim hizmetlerinin sağlanmasına ilişkin olarak işlenen kişisel veriler yönünden yer almıştı, bkz. **Lynskey**, *The Foundations*, s. 207. Anılan direktif hakkında ayrıntılı bilgi için bkz. **Uygun**, s. 85-87; **Küzeci**, s. 190-195.

[247] **Voss**, s. 4-5.

yönünden şeffaflığın sağlanmasında etkili bir araç olacağı ve veri sorumlularını hukuki ve teknik standartlara uymaya teşvik edeceği[248] ifade edilmiştir.

Denetim kurumuna bildirim ve veri öznesine bildirim Tüzük'te ayrı düzenlenmiş bulunmaktadır. Tüzük'ün 33 üncü maddesi, denetim kurumuna bildirim yükümlülüğünü, 34 üncü madde ise veri öznesine bildirim yükümlülüğünü düzenler.

III.B.9.b)(1)Denetim Kurumuna Bildirim Yükümlülüğü

Tüzük'ün 33 uncu maddesi, gerçek kişilerin hak ve özgürlükleri için risk oluşturma olasılığı yüksek bir kişisel veri ihlalinin varlığı halinde, veri sorumlusuna, gecikmeksizin yetkili denetim kurumuna bildirimde bulunma yükümlülüğü öngörmektedir. Mümkün olduğu hallerde, bildirim, ihlalin öğrenilmesinden itibaren 72 saat içinde yapılmalı, bunun mümkün olmadığı hallerde nedenleri de bildirilmelidir. Ayrıca veri işleyen, ihlalden haberdar olduğunda gecikmeksizin veri sorumlusuna haber verir (GDPR §33/2).

Bildirimin asgari olarak içermesi gereken hususlar, maddenin üçüncü fıkrasında sayılmıştır. Buna göre; mümkün olduğu hallerde, etkilenen veri öznesi grupları ve sayısı ile kayıtların türleri ve yaklaşık sayısı dahil olmak üzere ne tür bir veri ihlalinin söz konusu olduğuna ilişkin açıklama (GDPR §33/3-a), veri koruma yetkilisi ya da daha fazla bilgi alınabilecek başka bir kişinin iletişim bilgileri (GDPR §33/3-b), ihlalin olası sonuçları (GDPR §33/3-c) ve ihlalin olası olumsuz sonuçlarının azaltılmasına yönelik önlemler de dahil olmak üzere, veri sorumlusu tarafından alınan veya alınması teklif edilen önlemler (GDPR §33/3-d) bildirimde yer almalıdır.

Tüm bilgilerin aynı anda sağlanması mümkün değilse, haksız bir gecikme olmamak koşuluyla bilgiler aşamalı olarak sağlanabilir (GDPR §33/4).

Son olarak, veri sorumlusu, her kişisel veri ihlalinin, bunların etkilerinin ve bu etkilerin giderilmesine yönelik işlemlerin kaydını tutar. Denetim kurumu,

---

[248] Gerrit **Hornung** (2012), "A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012", SCRIPTed, C. 9, S. 1, s. 76. - http://script-ed.org/?p=406 (Erişim tarihi: 19/10/2018)

kayıtlardan, veri sorumlusunun bildirim yükümlülüğüne uygun hareket ettiğini doğrulayabilmelidir (GDPR §33/5).

III.B.9.b)(2)Veri Öznesine Bildirim Yükümlülüğü

Tüzük'ün 34 üncü maddesine göre, gerçek kişilerin hak ve özgürlükleri için yüksek bir risk oluşturması olasılığı bulunan bir kişisel veri ihlali söz konusu olduğunda, veri sorumlusu, haksız bir gecikme olmaksızın ihlali veri öznesine haber verir. Bildirim açık ve sade bir dil kullanılarak yapılmalı, asgari olarak 33 üncü maddenin üçüncü fıkrasında sayılan son üç hususu içermelidir (GDPR §34/2). Aşağıdaki koşullardan herhangi birinin varlığı halinde bildirim yapılmasına gerek yoktur:

- Veri sorumlusu, uygun teknik ve kurumsal koruma önlemlerini almış ve ihlalden etkilenen kişisel veriler üzerinde uygulamış olması (GDPR §34/3-a),
- Ortaya çıkması olasılığı bulunan yüksek riskin ortaya çıkmayacağını güvence altına almak için yeterli önlemleri almış olması (GDPR §34/3-b),
- Bildirimin orantısız bir çaba gerektirmesi (GDPR §34/3-c). Bu durumda bir kamu açıklaması yapılabilir ya da veri öznesinin aynı ölçüde etkin olarak bilgi alabileceği farklı bir bildirim yöntemi izlenebilir.

Bildirim yapılmadan önce, denetim kurumu gerekli değerlendirmeyi yaparak yukarıda sayılan koşulların gerçekleşip gerçekleşmediğini belirleyebilir (GDPR §34/4).

III.B.10.Veri Koruma Etki Değerlendirmesi ve Ön Danışma Yükümlülüğü

Veri koruma etki değerlendirmesi yapılması ve değerlendirme sonucunda gerekli olduğu hallerde denetim kurumuna başvurulması (ön danışma - "prior

consultation"), ilk kez Tüzük ile öngörülmüş yükümlülüklerdir.[249] Veri koruma etki değerlendirmesine ilişkin esaslar 35 inci maddede düzenlenirken, ön danışma ise 36 ncı maddenin konusunu oluşturmaktadır.

III.B.10.a)Veri Koruma Etki Değerlendirmesi

Tüzük'ün 35 inci maddesi uyarınca, özellikle yeni teknolojilerin kullanıldığı işleme faaliyetlerinde, işlemenin gerçek kişilerin hak ve özgürlükleri yönünden yüksek risk oluşturma ihtimalinin bulunduğu hallerde, işleme öncesinde planlanan işleme faaliyetlerinin kişisel verilerin korunması yönünden etkilerini değerlendirecektir. Tek bir değerlendirme, benzer riskler taşıyan birden fazla işleme faaliyetine yönelik olabilir. Tüzük'ün gerekçesinde, bu risklerin neler olabileceği belirtilmiştir. Buna göre, ayrımcılık, kimlik hırsızlığı ya da dolandırıcılık, maddi zarar, itibarın zedelenmesi, mesleki gizlilik çerçevesinde korunan kişisel verilerin gizliliğinin yitirilmesi, psödonimizasyonun yetkisiz olarak geri alınması ve diğer önemli sosyal ve ekonomik dezavantajlar olası risklerdir.[250]

Veri koruma etki değerlendirmesinin özellikle gerekli olduğu haller, 35 inci maddenin 3 üncü fıkrasında düzenlenmiştir. Buna göre, aşağıdaki hallerde veri koruma etki değerlendirmesi yapılması özellikle gereklidir:

- Sistematik ve kapsamlı olarak, gerçek kişiler üzerinde, profil çıkarma dahil otomatik bireysel kararlar alma amacıyla işleme yapılması (GDPR §35/3-a),
- Geniş çaplı olarak özel nitelikli kişisel verilerin veya ceza mahkumiyeti ve suçlara ilişkin kişisel verilerin işlenmesi (GDPR §35/3-b),
- Kamuya açık bir alanın geniş çaplı olarak izlenmesini gerektiren bir işleme yapılması (GDPR §35/3-c).

---

[249] Direktif'in 20 nci maddesi, veri öznelerinin hak ve özgürlüklerine ilişkin belirli riskler oluşturması olasılığı bulunan, kısmen veya tamamen otomatik yollarla gerçekleştirilen işleme faaliyetlerinin denetim kurumlarınca kontrol edilmesine (ön kontrol - "prior checking") yönelik bir düzenleme içermektedir.

[250] Tüzük, Gerekçe 75.

Denetim kurumları, hangi işleme faaliyetleri yönünden veri koruma etki değerlendirmesinin gerekli olup olmadığını belirleyebilir, hatta değerlendirme gerektiren işlemelerin belirlenmesi bir yükümlülük olarak öngörülmüştür (GDPR §35/4, 5).

Değerlendirme raporunda asgari olarak yer alması gereken hususlar, 35 inci maddenin 7 nci fıkrasında sayılmıştır. Anılan düzenleme uyarınca; planlanan işleme faaliyetinin ve mümkün olduğu hallerde veri sorumlusunun menfaati de dahil olmak üzere işleme amaçlarının sistematik bir açıklaması (GDPR §35/7-a), işleme faaliyetinin ulaşılmak istenen amaçlar doğrultusunda gerekli ve ölçülü olup olmadığının değerlendirmesi (GDPR §35/7-b), veri öznelerinin hak ve özgürlüklerine yönelik risklerin değerlendirmesi (GDPR §35/7-c) ve bu risklere karşı alınması planlanan önlemler (GDPR §35/7-d) raporda yer alması gereken asgari hususlardır, ancak hukuki ya da teknik sebeplerle Tüzük'te belirtilenlerin dışında başka noktalara da yer verilmesi isabetli olabilir.[251]

Mümkün olduğu hallerde veri sorumluları, veri öznelerinin ya da temsilcilerinin de planlanan işleme faaliyeti hakkında görüşünü almalıdır (GDPR §35/9). Ayrıca gerekli olduğu hallerde, en azından olası riskler yönünden bir değişiklik görüldüğü takdirde veri sorumları, değerlendirmeyi gözden geçirmelidir (GDPR §35/11).

III.B.10.b)Ön Danışma

Tüzük'ün 36 ncı maddesi uyarınca, veri koruma etki değerlendirmesi sonucunda, veri sorumlusu tarafından gerekli önlemler alınmadığı takdirde yüksek risk taşıdığı anlaşılan işleme faaliyetlerinde, veri sorumlusu işlemeye başlamadan önce denetim kurumuna başvurmalıdır. Denetim kurumu, işleme faaliyetinin Tüzük'ü ihlal edeceği ve özellikle veri sorumlusunun riskleri tanımlama ve azaltmada yetersiz kaldığı görüşündeyse, başvurunun kendisine ulaşmasından itibaren en fazla sekiz haftalık bir süre içinde, veri sorumlusuna ve varsa veri işleyene tavsiyelerini yazılı olarak sağlar ve 58 inci maddede belirtilen her türlü yetkisini kullanabilir. Denetim

[251] **Çekin**, s. 118.

kurumu bu süreyi, söz konusu işleme faaliyetinin karmaşıklığına bağlı olarak altı hafta uzatabilir, ancak süreyi uzattığını, nedenleriyle birlikte, başvurunun kendisine ulaşmasından itibaren bir ay içinde veri sorumlusuna ve varsa veri işleyene bildirecektir. Bu süreler, denetim kurumunun danışma faaliyetini yerine getirmek için talep ettiği bilgiler sağlanana kadar askıya alınabilir (GDPR §36/1, 2).

Veri sorumluları, başvuruları kapsamında denetim kurumuna aşağıdaki bilgileri sağlamakla yükümlüdür:

- Mümkün olduğu hallerde, işlemeye dahil olan veri sorumlusu, ortak veri sorumluları ve veri işleyenlerin sorumlulukları (GDPR §36/3-a),
- Planlanan işlemenin amaçları ve yöntemleri (GDPR §36/3-b),
- Tüzük uyarınca veri öznelerinin hak ve özgürlüklerini korumak için alınan önlemler ve sağlanan güvenceler (GDPR §36/3-c),
- Varsa veri koruma yetkilisinin iletişim bilgileri (GDPR §36/3-d),
- Veri koruma etki değerlendirmesi raporu (GDPR §36/3-e),
- Denetim kurumunun talep ettiği diğer her türlü bilgi (GDPR §36/3-f).

Denetim kurumuna danışma yükümlülüğü, veri sorumlusunun danışma yükümlülüğünden farklılık göstermekle birlikte, Üye Devletler yönünden de söz konusudur. Kişisel verilerin işlenmesine ilişkin kanun ya da diğer bir hukuki düzenleme taslağı hazırlayan Üye Devletler, hazırlık sürecinde denetim kurumuna danışmak durumundadır (GDPR §36/4). Üye Devletler ayrıca, kamu yararına görev yapan veri sorumluları yönünden, bu kapsamdaki işleme faaliyetleri için denetim kurumuna başvurma ve önceden izin alma yükümlülüğü getirebilirler (GDPR §36/5).

III.B.11.Veri Koruma Yetkilisi Atama Yükümlülüğü

III.B.11.a) Genel Olarak

Veri koruma yetkilisi atanmasına ilişkin hükümler öngörülmesi, Direktif döneminde Üye Devletlerin inisiyatifine bırakılmış durumdaydı (DPD §18/2). Nitekim Direktif döneminde, Almanya gibi bazı Üye Devletlerde veri koruma

yetkilisi atanması zorunlu kılınmıştır.[252] Tüzük ile,[253] artık belirli durumlarda bir veri koruma yetkilisi görevlendirilmesi, AB sınırları içinde kuruluşu bulunan tüm veri sorumluları ve veri işleyenler yönünden geçerli bir yükümlülük haline gelmiştir.

İşleme faaliyetinin kamu kurumlarınca gerçekleştirildiği hallerde, bir veri koruma yetkilisi atanmalıdır. Yargı yetkisi çerçevesinde hareket eden mahkemeler yönünden bu yükümlülük geçerli değildir. Veri sorumlularının veya veri işleyenlerin esas faaliyetleri,[254] doğası, kapsamı ve/veya amaçları gereği veri öznelerinin geniş kapsamlı olarak, düzenli ve sistematik olarak izlenmesini ya da özel nitelikli veya ceza mahkumiyetlerine ve suçlara ilişkin verilerin işlenmesini gerektiriyorsa, bu veri sorumluları ve veri işleyenler de veri koruma yetkilisi atama yükümlülüğü altındadır (GDPR §37/1). Sayılan haller dışında veri koruma yetkilisi atanmasını gerektiren haller, AB ya da Üye Devlet hukukunda belirlenir (GDPR §37/4).

Veri koruma yetkilisi, kişisel verilerin korunması hukukuna hakimiyet ve aşağıda incelenecek olan, Tüzük'ün öngördüğü görevleri yerine getirme kabiliyeti başta olmak üzere profesyonel beceriler dikkate alınarak belirlenecektir (GDPR §37/5). Bunun dışında veri koruma yetkilisi ile veri sorumlusu ya da veri işleyen arasındaki hukuki ilişkinin niteliğinin belirlenmesi taraflara bırakılmıştır (GDPR §37/6). Belirlenen veri koruma yetkilisinin iletişim bilgileri yayımlanacak ve denetim kurumuna bildirilecektir (GDPR §37/7).

III.B.11.b)Veri Koruma Yetkilisinin Görevleri

Veri koruma görevlisinin asgari olarak yerine getirmesi gereken görevler, Tüzük'ün 39 uncu maddesinde, aşağıdaki şekilde sayılmıştır:

---

[252] **Hornung**, s. 77.

[253] GDPR §37-39.

[254] "Esas faaliyet" kavramının tanımı ya da neleri kapsadığına ilişkin olarak Tüzük'te bir ifade yer almamaktadır. Çekin'e göre, esas faaliyet kavramı, veri sorumlusunun amacına ulaşabilmesi için gerekli olan bütün işlemler olarak tanımlanabilecektir, bkz. **Çekin**, s. 113.

- Tüzük ve AB ya da Üye Devlet mevzuatındaki diğer kişisel verilerin korunması kuralları çerçevesinde yükümlülüklerini yerine getiren veri sorumlusuna ya da veri işleyene ve bunların çalışanlarına bilgi ve tavsiye vermek (GDPR §39/1-a),
- Sorumluluk dağılımı, bilinçlendirme faaliyetleri ve işleme faaliyetlerinde görev alacak çalışanların eğitimi ve buna ilişkin denetimler de dahil olmak üzere; Tüzük'e, AB ya da Üye Devlet mevzuatındaki diğer kişisel verilerin korunması kurallarına ve veri sorumlusunun ya da veri işleyenin politikalarına uygun hareket edilip edilmediğini takip etmek (GDPR §39/1-b),
- Talep halinde, veri koruma etki değerlendirmesine ilişkin tavsiyelerde bulunmak ve uygulanmasını takip etmek (GDPR §39/1-c),
- Denetim kurumlarıyla işbirliği yapmak (GDPR §39/1-d),
- Ön danışma da dahil olmak üzere, işlemeye ilişkin hususlarda denetim kurumlarının iletişim kuracağı kişi olarak görev yapmak ve gerekli olduğu hallerde diğer konular hakkında da denetim kurumuna danışmak (GDPR §39/1-e).

Veri sorumlusu ve veri işleyen, veri koruma yetkilisinin, kişisel verilerin korunmasına ilişkin her türlü mesele ile aktif olarak ilgilendiğinden emin olmalı, görevlerini yerine getirmesinde veri koruma yetkilisine gerekli desteği sağlamalıdır. Veri koruma yetkilisine görevlerini yerine getirmesine ilişkin talimat verilemez. Veri koruma yetkilisi, yalnızca ve doğrudan en üst düzey yönetime karşı sorumludur. Veri özneleri, Tüzük'ten kaynaklanan haklarının kullanımına ilişkin olarak veri koruma yetkilisiyle iletişime geçebilirler. Veri koruma yetkilisi, AB ya da Üye Devlet hukuku uyarınca görevlerinin yerine getirilmesi konusunda gizlilik ve sır saklamakla yükümlü olmalıdır, ancak menfaat çatışmasına neden olmadığı sürece farklı görevler ve yükümlülükler yerine getirmesinin önünde bir engel yoktur (GDPR §38).

III.B.12. Tazminat Yükümlülüğü ve Yaptırımlar

Yukarıda da üzerinde durulduğu gibi, Tüzük'ün 77 ila 84 üncü maddeleri veri öznelerinin başvurabileceği hukuki çareler ile Tüzük'ün ihlalinden kaynaklanan zararların tazminine ve veri sorumlularına uygulanacak yaptırımlara ilişkin esasları

düzenler. Veri öznelerinin başvurabileceği hukuki çareler yukarıda incelenmiş olup,[255] tazminat ve yaptırımlara ilişkin esaslar bu bölümde incelenmiştir.

III.B.12.a)Tazminat Yükümlülüğü

Tüzük'ün 82 nci maddesi uyarınca, Tüzük'ün ihlalinden dolayı maddi veya manevi zarar gören herkes, gördüğü zararın veri sorumlusu ya da veri öznesi tarafından tazmin edilmesini isteyebilir.[256] Zarara neden olan ve Tüzük'e aykırı işleme faaliyetine dahil olan her veri sorumlusu, zararın tazmininden sorumludur. Veri işleyenler ise ancak, Tüzük'te doğrudan kendileri için öngörülmüş yükümlülükleri ihlal ettikleri ya da veri sorumlusunun hukuka uygun talimatları dışında ya da bu talimatlara aykırı hareket ettikleri takdirde sorumlu olacaklardır (GDPR §82/1, 2). Veri sorumluları ve veri işleyenler, zarara neden olan olayın meydana gelmesinde hiçbir şekilde kusurları bulunmadığını ispatladıkları takdirde tazminat yükümlülüğünden kurtulabilirler (GDPR §82/3).

Zarara neden olan işleme faaliyetine dahil olan birden fazla veri sorumlusu ya da veri işleyen varsa, veya veri sorumlusu ve veri işleyen birlikte müdahilse, veri öznesinin zararının etkili bir şekilde tazmininin sağlanması için bu kişilerin tümü müteselsilen sorumlu kılınmıştır (GDPR §82/4). Nitekim zararın tamamını karşılayan veri sorumlusu ya da veri işleyenin, diğer sorumlu kişilere rücu hakkı bulunmaktadır (GDPR §82/5).

Tazminat için başvurulacak mahkeme, 79 uncu maddenin 2 nci fıkrası uyarınca belirlenecektir.

III.B.12.b)Yaptırımlar

Tüzük'ün 83 üncü maddesi, idari yaptırımların uygulanmasına ilişkin esasları ayrıntılı bir biçimde düzenlemiştir. Buna göre denetim kurumları, her somut olay için

---

[255] Bkz. s. 87 vd.

[256] Çekin'e göre, bu sorumluluk esasen, borçlar hukukundaki haksız fiil sorumluluğunun özel bir görünümüdür, bkz. **Çekin**, s. 101.

etkili, ölçülü ve caydırıcı olacak şekilde Tüzük'ün öngördüğü yaptırımları uygulayacaktır. Yaptırım miktarının belirlenmesi denetim kurumunun takdirine bırakılmakla birlikte, bu miktarın belirlenmesinde denetim kurumunun dikkate alacağı hususlar maddenin ikinci fıkrasında şu şekilde sayılmıştır:

- İhlalin doğası, ağırlığı ve süresi (GDPR §83/2-a),
- İhlalin kasıtlı veya ihmal sonucu gerçekleşip gerçekleşmediği (GDPR §83/2-b),
- Veri sorumlusunun ya da veri işleyenin veri öznelerinin zararlarının giderilmesine yönelik her türlü faaliyeti (GDPR §83/2-c),
- Veri sorumlusunun ya da veri işleyenin tasarımsal ve varsayılan veri koruması ile kişisel verilerin güvenliğinin sağlanması yükümlülükleri kapsamında alınan önlemler dikkate alınarak belirlenen sorumluluk derecesi (GDPR §83/2-d),
- Varsa veri sorumlusunun ya da veri işleyenin daha önceki ihlalleri (GDPR §83/2-e),
- İhlalin ve olumsuz etkilerinin azaltılmasına ilişkin olarak denetim kurumuyla ne ölçüde işbirliği yapıldığı (GDPR §83/2-f),
- İhlalden etkilenen kişisel veri türleri (GDPR §83/2-g),
- Denetim kurumunun ihbarı nasıl haber aldığı, özellikle veri sorumlusunun ya da veri işleyenin bildirimde bulunup bulunmadığı, bulunduysa bildirimin kapsamı (GDPR §83/2-h),
- Veri sorumlusunun ya da veri işleyenin, kendilerine denetim kurumunca verilen emirlere ne ölçüde uyulduğu (GDPR §83/2-i),
- 40 ıncı madde uyarınca davranış kurallarına uyulup uyulmadığı ya da 42 nci madde uyarınca sertifika alınıp alınmadığı (GDPR §83/2-j),
- Somut olaydaki ağırlaştırıcı veya hafifletici nedenler, örneğin ihlalin doğrudan ya da dolaylı olarak neden olduğu maddi menfaatler ya da önlenen zararlar (GDPR §83/2-k).

Tüzük'ün birden fazla hükmünün aynı işleme faaliyeti ya da bununla bağlantılı işleme faaliyetleri ile ihlal edilmesi halinde toplam ceza, en ağır ihlal için öngörülen cezadan fazla olamaz (GDPR §83/3).

Tüzük'te, yaptırımların üst sınırları belirlenirken ikili bir ayrım yapılmıştır. Buna göre, 83 üncü maddenin 4 üncü fıkrasında sayılan hükümlerin ihlali halinde, 10.000.000 Euro ya da bir işletmenin varlığı söz konusu ise ve önceki mali yılın dünya çapındaki toplam cirosu bu rakamı aşıyorsa, bunun yüzde 2'si üst sınır olmak üzere idari para cezası uygulanacaktır. 83 üncü maddenin 5 inci ve 6 ncı fıkrasında sayılan hükümlerin ihlali halinde, 20.000.000 Euro ya da bir işletmenin varlığı söz konusu ise ve önceki mali yılın dünya çapındaki toplam cirosu bu rakamı aşıyorsa, bunun yüzde 4'ü üst sınır olmak üzere idari para cezası uygulanır. Kamu kurumlarına yönelik idari para cezası verilmesine ilişkin esasları her Üye Devlet kendi iç hukukunda belirler (GDPR §83/7). İdari para cezalarına karşı kanun yollarına başvurma imkanı ve adil yargılanma hakkı da Tüzük ile güvence altına alınmıştır (GDPR §83/8).

Son olarak, Tüzük'ün 84 üncü maddesi, Üye Devletlere, etkili, ölçülü ve caydırıcı olması koşuluyla, Tüzük'te düzenlenmeyen yaptırımlar öngörme imkanı tanımıştır.

IV. AB DIŞINA KİŞİSEL VERİ AKTARIMI

IV.A. Genel Olarak

Sınırötesi veri aktarımı olarak da anılan[257] AB dışına kişisel veri aktarımı, daha önce Direktif'in 25 ve 26 ncı maddelerinde düzenlenmiş, kural olarak yeterli koruma sağlamayan üçüncü ülkelere veri aktarımı yasaklanmıştı. Bu hüküm, gerek katı yapısı gerekse uygulanmasındaki güçlükler nedeniyle hukukçular ve iş çevrelerince eleştirilmişti.[258] Özellikle AB ile ABD arasındaki veri aktarımının iki bölge arasındaki ticari faaliyetlere olan olumsuz etkisi, 2000/520/AT sayılı Avrupa

[257] **Lambert**, s. 341.

[258] **Küzeci**, s. 175. Farklı devletlerin sınırötesi veri aktarımına ilişkin düzenlemelerin uyumlaştırılmasındaki güçlüklere yönelik olarak bkz. Priscilla M. **Regan** (2003), "Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows", Journal of Social Issues, C. 59, S. 2, s. 263-282.

Komisyonu Kararı[259] ile Güvenli Liman Gizlilik İlkelerinin ("Safe Harbour Privacy Principles") kabul edilmesine neden olmuştur. Buna göre, bu ilkeleri kabul eden ve bu ilkeler çerçevesinde hareket eden Amerikan şirketleri ile AB arasında yeterli koruma sağlanmış kabul edilerek veri aktarımı yapılabilecekti.[260] Güvenli Liman anlaşması, ABAD tarafından Ekim 2015 tarihli Schrems kararı[261] ile geçersiz hale getirilmiştir.

AB dışına kişisel veri aktarımı, Tüzük'te, üçüncü ülkelerin yanı sıra uluslararası örgütlere yapılacak aktarımları da kapsayacak şekilde, 40 ila 50 nci maddeler arasında düzenlenmiştir. Direktif'te olduğu gibi, Tüzük de Avrupa Komisyonu'nun, sağladığı koruma düzeyini yeterli bulduğu üçüncü ülkelere kişisel veri aktarımına izin vermektedir (GDPR §45). Bununla birlikte, 46 ncı madde uyarınca, Komisyon'un yeterlilik ("adequacy") kararı bulunmadığı hallerde dahi, veri sorumlusunun ya da veri işleyenin uygun güvenlik önlemlerini alması ve verilerin aktarılacağı ülkede veri özneleri yönünden hakların ve etkili hukuki çarelerin öngörülmüş olması koşuluyla aktarım mümkündür. Bunların dışında 47 nci maddede, yukarıda belirtilen uygun güvenlik önlemlerinden biri olan bağlayıcı kurumsal kurallara ("binding corporate rules") ilişkin esaslar düzenlenmiş, 48 ve 49

---

[259] 2000/520/EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, 25 Ağustos 2000.

[260] Güvenli Liman anlaşması ile öngörülen sistem hakkında daha ayrıntılı bilgi için bkz. **Küzeci**, s. 180 vd.

[261] *Maximilian Schrems* v *Data Protection Commissioner*, C-362/14. Olayda Avusturya vatandaşı Max Schrems, 2013 yılında Edward Snowden'in ABD'nin dünya çapındaki izleme faaliyetleri ortaya çıkarmasının ardından (bkz. Revealed: how US and UK spy agencies defeat internet privacy and security - https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Erişim tarihi: 10/5/2019)), Facebook'un İrlanda merkezli alt şirketi Facebook Ireland'ın kişisel verilerini ABD'ye aktarmasının yasaklanması için İrlanda Veri Koruma Sorumlusuna başvurmuştur. Başvuru, aktarımın Güvenli Liman anlaşması kapsamında olduğu gerekçesiyle reddedilmiş, Schrems'in bunun üzerine başvurduğu İrlanda mahkemesi, olayı ABAD'a taşımıştır. ABAD, mahkemenin bu yönde bir talebi olmamasına rağmen, Güvenli Liman anlaşmasının temelini oluşturan 2000/520/AT sayılı Avrupa Komisyonu Kararı'nın geçerliliğini de incelemiş ve geçersiz olduğu kanısına varmıştır. Karara ilişkin daha ayrıntılı bilgi ve bir inceleme için bkz. João **Marques** (2016), ""And [they] built a crooked h[arbour]" – the Schrems ruling and what it means for the future of data transfers between the EU and US", UNIO - EU Law Journal, C. 2, S. 2, June 2016, s. 54-70.

uncu maddelerde ise AB hukukunda izin verilmeyen veri aktarımları ile istisna halleri hükme bağlanmıştır.

IV.B. Yeterlilik Kararı Doğrultusunda Veri Aktarımı

Tüzük'ün 45 inci maddesine göre, bir üçüncü ülkeye ya da uluslararası örgüte kişisel veri aktarımı, Komisyon tarafından söz konusu üçüncü ülke, bu ülkenin bir bölgesi ya da bir veya birden fazla belirli sektörü, ya da uluslararası örgütün yeterli düzeyde koruma sağlaması halinde mümkündür. Bu kapsamdaki veri aktarımları için ayrıca izin alınması gerekmez.

Yeterli korumanın ne olduğu ve hangi durumlarda sağlanmış kabul edileceğine dair Tüzük'te bir ifade yer almamaktadır.[262] Ancak, Komisyon'un korumanın yeterliliğini değerlendirirken dikkate alması gereken hususlar aynı maddenin ikinci fıkrasında sayılmıştır. Buna göre; hukukun üstünlüğü, temel hak ve özgürlüklere saygı, kamu güvenliği ve ceza hukukuna ilişkin düzenlemeler de dahil olmak üzere ilgili mevzuat ve bu mevzuatın uygulanması, sonraki aktarımlar için öngörülen esaslar, veri özneleri için etkili ve icra edilebilir hakların ve hukuki çarelerin öngörülmüş olup olmaması, bir ya da birden fazla bağımsız denetim kurumunun varlığı ve etkinliği, üçüncü ülkenin veya uluslararası örgütün özellikle kişisel verilerin korunması alanına ilişkin olanlar olmak üzere uluslararası bağlılıkları ve taraf olduğu bağlayıcı sözleşmeler gibi pek çok unsur, bu bağlamda Komisyon tarafından dikkate alınacaktır. Komisyon, incelemesi sonucunda yeterlilik kararı verirse, bu karar, üçüncü ülkedeki ya da uluslararası örgütteki ilgili her türlü gelişme dikkate alınarak, dört yılda bir yeniden değerlendirilir. Bu gelişmeler Komisyon tarafından düzenli olarak takip edilecektir (GDPR §45/3, 4). Komisyon, değerlendirme sonucunda üçüncü ülke ya da uluslararası örgütün sağladığı korumanın yetersiz hale geldiği kanaatine varırsa, kararını gerektiği ölçüde geri alabilir, üzerinde değişiklik yapabilir ya da askıya alabilir. Bu karar geriye etkili değildir (GDPR §45/5). Direktif döneminde alınmış yeterlilik kararları da Komisyon

[262] ABAD, *Schrems* kararında bu ifadeden AB hukukunda sağlanan korumaya temelde eşdeğer ("essentially equivalent") bir koruma sağlanmasının anlaşılacağını açıklamıştır, bkz. ABAD, C-362/14, par. 96.

tarafından Tüzük esaslarına göre üzerinde değişiklik yapılana, değiştirilene ya da kaldırılana kadar geçerlidir (GDPR §45/9).

Komisyon, Avrupa Birliği Resmi Gazetesi'nde ve internet sayfasında, yeterli koruma sağlayan üçüncü ülkelerin, bu ülkelerin belirli bölgelerinin ya da sektörlerinin ve uluslararası örgütlerinin bir listesini yayınlar (GDPR §45/8). 2018 yılı itibariyle Andorra, Arjantin, ticari işletmeler yönünden Kanada, Faroe Adaları, Guernsey, Man Adaları, İsrail, Jersey, Yeni Zelanda, İsviçre ve Uruguay hakkında yeterlilik kararı bulunmaktadır.[263]

IV.C. Uygun Önlemlere Tabi Veri Aktarımı

Kimi hallerde, Komisyon tarafından hakkında yeterlilik kararı verilmemiş bulunan bir üçüncü ülkeye ya da uluslararası örgüte veri aktarımı mümkün olabilmektedir. Tüzük'ün 46 ncı maddesi uyarınca, bu ülkelere ve uluslararası örgütlere, yalnızca veri sorumlusunun ve veri işleyenin uygun güvenlik önlemlerini aldığı takdirde ve veri özneleri bakımından icra edilebilir hakların ve etkili hukuki çarelerin bulunması koşuluyla veri aktarımı yapılabilecektir.

Anılan maddenin ikinci fıkrası, uygun önlemlerin ne şekilde alınabileceğini düzenlemiştir. Buna göre, uygun önlemler, denetim kurumunun özel bir iznine gerek olmadan, aşağıdaki yollarla alınabilir:

- Kamu kurum ve kuruluşları arasında bağlayıcı ve icra edilebilen bir anlaşma yapılması (GDPR §46/2-a),
- 47 nci madde esaslarına uygun olarak bağlayıcı kurumsal kurallar belirlenmesi (GDPR §46/2-b),
- Komisyon ya da Komisyon onayıyla denetim kurumu tarafından belirlenen standart veri koruması hükümleri (GDPR §46/2-c, d),
- Veri öznelerinin haklarına ilişkin olanlar da dahil olmak üzere veri sorumlusu ya da veri işleyenin bağlayıcı ve icra edilebilir taahhütlerinin yanında, 40 ıncı

[263] Handbook on European Data Protection Law, s. 255.

madde kapsamında belirlenmiş davranış kuralları veya 42 nci madde kapsamında sertifikasyon mekanizması (GDPR §46/2-e, f).

Yukarıda sayılanların dışında, üçüncü fıkraya göre, denetim kurumundan izin alınmak koşuluyla, özellikle veri sorumlusu ya da veri işleyen ile üçüncü ülke veya uluslararası örgütteki veri sorumlusu, veri işleyen ya da alıcı arasındaki sözleşme hükümleriyle ya da kamu kurum ve kuruluşları arasındaki idari anlaşmalara, veri özneleri açısından icra edilebilir ve etkili hakları da içeren hükümler eklenmesi yoluyla uygun önlemler alınabilecektir.

Direktif döneminde, Üye Devletler ya da denetim kurumları tarafından Direktif'e uygun olarak verilen kararlar, ilgili denetim kurumu tarafından üzerinde değişiklik yapılana, değiştirilene ya da kaldırılana kadar geçerlidir (GDPR §46/5).

IV.D.AB Hukukunun İzin Vermediği Aktarımlar ve İstisna Halleri

Tüzük'ün 48 inci maddesi, AB hukukunun izin vermediği bir veri aktarımının gerçekleşmesi halinde ne olacağını hükme bağlamıştır. Buna göre, bir üçüncü ülkede verilen ve veri sorumlusunun ya da veri işleyenin kişisel verileri aktarmasını veya açıklamasını gerektiren ilamlar ya da idari kararlar, yalnızca üçüncü ülke ile AB ya da Üye Devlet arasındaki bir uluslararası anlaşmaya (örneğin bir hukuki yardımlaşma antlaşmasına) dayanıyorsa tanınabilir ve icra edilebilir.

Nihayet, 49 uncu madde, Komisyon tarafından verilmiş bir yeterlilik kararı bulunmadığı ve uygun güvenlik önlemlerinin de alınmadığı hallerde, bir üçüncü ülkeye ya da uluslararası örgüte hangi hallerde aktarım yapılabileceğini düzenlemiştir. Buna göre, aşağıdaki hallerden birinin varlığı halinde, aktarım hukuka uygun kabul edilebilecektir:

- Veri öznesinin veri aktarımına açık rızası (GDPR §49/1-a),
- Veri aktarımının, veri öznesinin, veri sorumlusu ya da veri işleyen ile yaptığı bir sözleşmenin ifa edilebilmesi ya da sözleşmenin kuruluşundan önce veri

öznesinin isteği doğrultusunda gerekli adımların atılabilmesi için gerekli olması (GDPR §49/1-b),

- Veri aktarımının, veri sorumlusu ya da veri işleyen ile başka bir gerçek veya tüzel kişi arasında, veri öznesi lehine bir sözleşmenin kurulması ya da ifası için gerekli olması (GDPR §49/1-c)
- Veri aktarımının, kamu yararına ilişkin önemli nedenler yönünden gerekli olması (GDPR §49/1-d),
- Veri aktarımının, bir hakkın kurulması, kullanılması ya da savunulması için gerekli olması (GDPR §49/1-e),
- Veri aktarımının, veri öznesinin fiziksel ya da hukuki olarak rıza vermesinin mümkün olmadığı hallerde, veri öznesinin ya da diğer kişilerin hayati menfaatlerinin korunabilmesi için gerekli olması (GDPR §49/1-f),
- Veri aktarımının, kamuyu bilgilendirmek amacıyla, genel olarak ya da meşru menfaatini ortaya koyabilen herkes tarafından incelenmeye açık bir sicil tarafından, AB ya da Üye Devlet tarafından konuya ilişkin olarak belirlenen koşulların yerine getirildiği ölçüde yapılması (GDPR §49/1-g).

Yukarıda sayılan hallerden herhangi birine de dayanmayan bir veri aktarımı; yalnızca tekrar eden bir aktarım olmaması, sınırlı sayıda veri öznesine yönelik olması, veri sorumlusunun, veri öznesinin menfaatleri ya da hak ve özgürlüklerinin önüne geçmeyen meşru menfaatlerinin gerçekleşmesi için gerekli olması, veri sorumlusunun gerekli değerlendirmeleri yaparak uygun önlemleri alması halinde gerçekleştirilebilir. Bu kapsamdaki aktarımlar, denetim kurumuna ve veri öznesine bildirilir.

AB ya da Üye Devlet hukukunda, Komisyon'un yeterlilik kararının bulunmadığı hallerde kamu yararına ilişkin önemli nedenlerle belirli kişisel veri türlerinin aktarımına sınırlamalar getirilebilir. Bu sınırlamalar Komisyon'a bildirilir (GDPR §49/5).

V. DENETİM KURUMLARI

V.A.Genel Olarak

Üye Devletler yönünden, kişisel verilerin korunmasına ilişkin kuralların uygulanmasını denetlemek üzere bağımsız bir denetim kurumunun görevlendirilmesi, Direktif'te, kişisel verilerinin işlenmesi karşısında korunmasının zorunlu bir bileşeni olarak ifade edilmişti.[264] Gerçekten de, o dönemde yürürlükte olan diğer uluslararası belgeler ile karşılaştırıldığında, bağımsız denetim kurumlarına ilişkin en ayrıntılı düzenlemenin Direktif'te bulunduğu görülür.[265] Tüzük ise, aynı anlayışla,[266] çok daha geniş kapsamlı düzenlemeler getirmektedir. Denetim kurumlarının kuruluşu, üyelerinin atanması, görevleri, yetkileri ve işbirliği ve istikrar ("consistency") mekanizmalarının yanı sıra, tüzel kişiliği haiz bir AB organı olan Avrupa Veri Koruma Kurulu'nun kuruluşu ve işleyişine ilişkin esaslar Tüzük'ün 51 ila 76 ncı maddeleri arasında ayrıntılı olarak düzenlenmiştir.

V.B.Denetim Kurumlarının Kuruluşu

V.B.1.Denetim Kurumlarının Bağımsızlığı

Tüzük'ün 51 inci maddesi uyarınca, her Üye Devlet, gerçek kişilerin temel hak ve özgürlüklerinin korunması ve AB içi serbest veri akışının kolaylaştırılması amacıyla, Tüzük'ün uygulanmasını denetlemek üzere bir veya birden fazla bağımsız denetim kurumu belirlemek zorundadır. AB genelinde Tüzük'ün istikrarlı bir şekilde uygulanmasını sağlamak üzere, denetim kurumlarının birbirleriyle ve Komisyon ile işbirliği yapmaları da öngörülmüştür.

Görevlendirilecek denetim kurumlarının görevlerini yerine getirirken bağımsız hareket edeceği Direktif'te de (DPD §281/1) ifade edilmiştir. Gerçekten de, denetim kurumlarının kuruluş amaçları doğrultusunda kendilerine verilen görevleri

---

[264] Direktif, Gerekçe 62.

[265] **Küzeci**, s. 272.

[266] Tüzük, Gerekçe 117.

etkili biçimde yerine getirebilmeleri, bu kurumların bağımsızlığının sağlanmasına bağlıdır. ABAD da kimi kararlarında denetim kurumlarının bağımsızlığının önemine dikkat çekmiştir.[267] Tüzük'te, bağımsızlıktan ne anlaşılması gerektiği ve bağımsızlığın kapsamı 52 nci maddede düzenlenmiştir. Buna göre, denetim kurumları, Tüzük'ten kaynaklanan görevlerini yerine getirirken ve yetkilerini kullanırken tamamen bağımsız olmalıdır. Denetim kurumu üyeleri, doğrudan veya dolaylı dış etkilerden uzak olmalı, hiç kimseden talimat almamalı veya istememelidir. Üye Devletler, denetim kurumlarına görevlerini etkin bir şekilde yerine getirmeleri için gerekli kaynakları ve altyapıyı sağlamakla, ayrıca kendi seçtikleri çalışanlardan oluşan bir personeli olduğunu ve bu personelin sadece denetim kurumu üyelerinden talimat aldığını güvence altına almakla yükümlüdür (GDPR §52/4, 5).

Denetim kurumu üyeleri, görevleriyle bağdaşmayan davranışlardan uzak durmalı ve bu nitelikte başka işlerde çalışmamalıdır (GDPR §52/3). Ayrıca denetim kurumlarının bağımsızlığı, finansal veya yargısal denetim ve kontrole tabi tutulamayacakları anlamına gelmemektedir.[268] Nitekim Tüzük, bağımsızlıklarını etkilememek üzere, denetim kurumlarının Üye Devletler tarafından finansal denetime tabi tutulacağını öngörmüştür (GDPR §52/6).

V.B.2.Denetim Kurumlarının Kuruluşuna ve Üyelerin Atanmasına İlişkin Esaslar

Tüzük'ün 54 üncü maddesi uyarınca, Üye Devletler, denetim kurumlarının kuruluşunu, denetim kurumuna üye seçilebilmek için gerekli nitelik ve koşulları, bu üyelerin atanmasına ilişkin kuralları ve prosedürleri, görev sürelerini ve kaç dönem için yeniden seçilebileceklerini ve görevleri sırasında uymaları gereken kuralları kanunla belirleyecektir. AB ve Üye Devlet hukukuna uygun olarak, denetim kurumu üyeleri, görevleri süresince edindikleri gizli bilgiler yönünden, görevleri süresince ve sonrasında, gizlilik yükümlülüğü altındadır (GDPR §54/2).

---

[267] Bu konuda bkz. **Küzeci**, s. 274-275.

[268] Tüzük, Gerekçe 118.

Denetim kurumu üyelerinin nasıl atanacağına ilişkin esaslar, Tüzük'ün 53 üncü maddesinde düzenlenmiştir. Anılan maddeye göre, üyelerin ataması, şeffaf bir prosedür izlenmek koşuluyla, Üye Devletin parlamentosu, hükümeti, Devlet başkanı veya Üye Devlet hukukuna göre atanacak bağımsız bir organ tarafından yapılır. Üyeler, görevlerini yerine getirebilmek ve yetkilerini kullanabilmek için, özellikle kişisel verilerin korunması alanında, gerekli nitelikleri, tecrübeyi ve becerileri haiz olmalıdır (GDPR §53/2).

Denetim kurumu üyelerinin görevi, AB ve ilgili Üye Devlet hukukuna uygun olacak şekilde, görev süresinin dolması, istifa ya da zorunlu emeklilik ile sona erer. Bunların dışında üyelerin görevden alınması, ancak görevin ciddi şekilde kötüye kullanılması ya da görevleri yerine getirmek için gerekli koşulların artık sağlanmaması hallerinde mümkündür (GDPR §53/3, 4).

V.C.Denetim Kurumlarının Görev ve Yetkileri

V.C.1.Denetim Kurumlarının Yetkisinin Kapsamı

Tüzük'ün 55 inci maddesi uyarınca, her denetim kurumu, Tüzük'ten kaynaklanan görev ve yetkileri yönünden, kendi Üye Devletinin sınırları içinde yetkilidir. Bu özellikle veri sorumlusunun ya da veri işleyenin ilgili Üye Devletteki kuruluşunun faaliyetleri bağlamındaki, kamu sektörü veya özel sektör kurumlarının kamu yararı çerçevesindeki ve AB sınırları içinde kuruluşu bulunmayan bir veri sorumlusu ya da veri işleyenin ilgili Üye Devlet sınırları içerisindeki veri öznelerini etkileyen işleme faaliyetleri bakımından geçerli olup, şikayetlerin değerlendirilmesi, Tüzük'ün uygulanmasına yönelik soruşturmaların yürütülmesi ve kişisel verilerin korunmasına yönelik bilinçlendirme faaliyetleri de bu kapsamdadır.[269] Ancak denetim kurumlarının, mahkemelerin yargı yetkisi dahilinde gerçekleştirdikleri işleme faaliyetlerini denetleme yetkisi bulunmamaktadır (GDPR §55/3).

Sınırötesi veri işleme faaliyetlerinde, Üye Devlet yalnızca bir denetim kurumu belirlemişse bu kurum, birden fazla denetim kurumu belirlemişse, veri sorumlusunun ya da veri işleyenin ana işletmesinin ya da işletmelerinden birinin tabi

[269] Tüzük, Gerekçe 122.

olduğu denetim kurumu, baş denetim kurumu ("lead supervisory authority") olarak görev yapar (GDPR §56/1). Tek durak ilkesi olarak da anılan bu düzenleme sayesinde, AB sınırları içinde birden fazla kuruluşu bulunan ya da birden fazla Üye Devlette faaliyet gösteren veri sorumluları ve veri işleyenler, tek bir denetim makamı ile muhatap olacaktır.[270] [271] Ancak bir şikayet veya ihlal, yalnızca bir Üye Devlette yer alan bir kuruluşa ilişkin ise ya da bu Üye Devlet sınırları içerisindeki veri öznelerini önemli ölçüde etkiliyorsa, o Üye Devletin denetim kurumu da şikayeti veya ihlali değerlendirebilecektir (GDPR §56/2). Bu durumda gecikme olmaksızın baş denetim kurumuna bilgi verilir ve baş denetim kurumu üç hafta içinde şikayeti veya ihlali kendisinin değerlendirip değerlendirmeyeceğine karar verir. Kendisinin değerlendireceğine karar verirse, aşağıda incelenecek olan işbirliği mekanizması uygulanır, ancak baş denetim kurumu, bu yönde bir karar vermese dahi sınırötesi işleme faaliyetleri yönünden veri sorumlusunun ve veri işleyenin tek muhatabıdır (GDPR §56/4, 6).

V.C.2.Denetim Kurumlarının Görevleri

Tüzük'ün 57 nci maddesi, her denetim kurumunun, kendi yetki alanında yerine getirmesi gereken görevleri saymıştır. Anılan hüküm son derece kapsamlı olup, Tüzük'te öngörülen diğer görevler saklı kalmak kaydıyla denetim kurumları için yirmi iki görev öngörmektedir. Bunlardan en önemlileri şu şekilde sayılabilir:

- Tüzük'ün uygulanmasını sağlamak ve denetlemek (GDPR §57/1-a),
- Kişisel verilerin işlenmesine yönelik bilinçlendirme faaliyetleri yürütmek (GDPR §57/1-b),
- Üye Devlet hukuku çerçevesinde gerçek kişilerin hak ve özgürlüklerinin korunmasını sağlamaya yönelik hukuki ve idari önlemlerin alınmasında devlet organlarına ve diğer kurumlara tavsiyeler vermek (GDPR §57/1-c),

---

[270] **Develioğlu**, s. 138.

[271] Bu düzenleme, AB sınırları içerisinde kuruluşu bulunmayan veri sorumluları ve veri işleyenler yönünden uygulanmaz.

- Veri sorumlularını ve veri işleyenleri Tüzük'ten kaynaklanan yükümlülükleri konusunda bilinçlendirmek (GDPR §57/1-d),
- Talep üzerine, veri öznelerine Tüzük'ten kaynaklanan haklarının kullanımı için bilgi vermek ve gerektiğinde buna ilişkin olarak diğer Üye Devletlerdeki denetim kurumlarıyla işbirliği yapmak (GDPR §57/1-e),
- Şikayetleri değerlendirmek ve makul bir süre içinde şikayette bulunanları şikayetlerinin sonucu hakkında bilgilendirmek (GDPR §57/1-f),
- Tüzük'ün uygulanmasında istikrarı sağlamak için diğer denetim kurumlarıyla işbirliği yapmak (GDPR §57/1-g),
- Veri koruma etki değerlendirmesi gerektiren halleri belirlemek ve bu hallerin bir listesini çıkarmak (GDPR §57/1-k),
- Ön danışma sonucunda işleme faaliyetinin Tüzük'ü ihlal edeceği ve özellikle veri sorumlusunun riskleri tanımlama ve azaltmada yetersiz kaldığı görüşünde olduğu işleme faaliyetlerine ilişkin tavsiyeler vermek (GDPR §57/1-l),
- Tüzük ihlallerinin ve bu kapsamda aşağıda incelenecek olan düzeltici yetkiler uyarınca alınan önlemlerin kayıtlarını tutmak (GDPR §57/1-u),
- Kişisel verilerin korunmasına ilişkin diğer her türlü görevi yerine getirmek (GDPR §57/1-v).

Tüzük, denetim kurumlarının görevlerini veri öznelerine çeşitli kolaylıklar sağlayacak şekilde yerine getirmelerini sağlamak için, maddenin devamında çeşitli hükümler getirmiştir. Buna göre, şikayetlerin denetim kurumuna iletilmesi kolaylaştırılmalıdır. Denetim kurumu bu kapsamda, diğer başvuru yöntemlerini ortadan kaldırmadan, şikayetlerin elektronik ortamda iletilmesini sağlayabilir (GDPR §57/2). Denetim kurumunun görevlerinin yerine getirmesi, veri özneleri ve mümkünse veri koruma yetkilileri için ücretsizdir, ancak özellikle tekrarlayan nitelikleri nedeniyle açıkça dayanaktan yoksun ve aşırı nitelikteki talepler, bu durum denetim kurumu tarafından ispatlanmak koşuluyla, makul bir ücrete tabi tutulabilir (GDPR §57/3, 4).

Son olarak, denetim kurumları, faaliyetlerinin yıllık raporlarını hazırlamakla ve raporları Üye Devlet hukukunun öngördüğü Devlet organlarına iletmekle

yükümlüdürler. Bu raporlar kamunun, Komisyon'un ve Avrupa Veri Koruma Kurulu'nun erişimine açık olmalıdır (GDPR §59).

V.C.3.Denetim Kurumlarının Yetkileri

Tüzük'ün 58 inci maddesi, denetim kurumlarının yetkilerini, soruşturma yetkileri (GDPR §58/1), düzeltici yetkiler (GDPR §58/2) ve danışmanlık yetkileri dahil olmak üzere diğer yetkiler (GDPR §58/3) olmak üzere üçe ayırarak saymıştır.

V.C.3.a)Soruşturma Yetkileri

Tüzük'ün 58 inci maddesinin birinci fıkrasına göre, denetim kurumlarının soruşturma yetkileri şunlardır:

- Veri sorumlularına, veri işleyenlere ya da varsa bunların temsilcilerine, görevlerinin yerine getirilmesi için gerekli bilgileri vermesini emretmek (GDPR §58/1-a),
- Veri koruma teftişi yapmak suretiyle soruşturmalar yürütmek (GDPR §58/1-b),
- 42 nci maddenin 7 nci fıkrası doğrultusunda verilen sertifikaları değerlendirmek (GDPR §58/1-c),
- Tüzük'ün ihlali yönündeki iddiaları veri sorumlusuna ya da veri işleyene bildirmek (GDPR §58/1-d),
- Veri sorumlusu ya da veri işleyenden, görevlerinin yerine getirilmesi için gerekli tüm kişisel verilere ve bilgilere erişim sağlamak (GDPR §58/1-e),
- AB ya da Üye Devlet hukukuna uygun olarak, her türlü kişisel veri işleme aracı dahil olmak üzere, veri sorumlusunun ya da veri işleyenin işyerine erişim (GDPR §58/1-f).

V.C.3.b)Düzeltici Yetkiler

Tüzük'ün 58 inci maddesinin ikinci fıkrasında, denetim kurumlarının düzeltici yetkileri şu şekilde sayılmıştır:

- Planladıkları işleme faaliyetleri Tüzük'ü ihlal edebilecek veri sorumlularını ya da veri işleyenleri uyarmak (GDPR §58/2-a),
- İşleme faaliyetleri Tüzük'ü ihlal etmiş veri sorumlularına ya da veri işleyenlere kınama vermek (GDPR §58/2-b),
- Veri sorumlularına ya da veri işleyenlere, veri öznelerinin Tüzük'ten kaynaklanan haklarının kullanımı doğrultusundaki taleplerine uymalarını emretmek (GDPR §58/2-c),
- Veri sorumlularına ya da veri işleyenlere, gerektiği hallerde belli bir şekilde ya da belli bir zaman içerisinde, işleme faaliyetlerini Tüzük hükümlerine uygun hale getirmelerini emretmek (GDPR §58/2-d),
- Veri sorumlularına, kişisel veri ihlallerini veri öznelerine bildirmelerini emretmek (GDPR §58/2-e),
- İşleme yasağı da dahil olmak üzere, geçici veya kesin sınırlamalar getirmek (GDPR §58/2-f),
- Tüzük'te veri öznelerine yönelik öngörülen ilgili haklar çerçevesinde kişisel verilerin düzeltilmesini ya da silinmesini ve bu işlemlerin kişisel verilerin açıklandığı kişilere bildirilmesini emretmek (GDPR §58/2-g),
- 42 ve 43 üncü madde esasları çerçevesinde verilen sertifikaları geri almak ya da sertifikayı veren kuruma bu yönde emir vermek, ya da koşullar artık sağlanmıyorsa sertifika verilmemesini emretmek (GDPR §58/2-h),
- Sayılan yetkilere ek olarak, ya da bunların yerine, somut olayın koşullarını dikkate alarak, idari para cezası vermek (GDPR §58/2-i),
- Üçüncü ülkelere ya da uluslararası örgütlere kişisel veri akışlarının askıya alınmasını emretmek (GDPR §58/2-j).

V.C.3.c)Diğer Yetkiler

Tüzük'ün 58 inci maddesinin üçüncü fıkra uyarınca, denetim kurumları ayrıca aşağıdaki yetkilere sahiptir:

- Ön danışma kapsamında veri sorumlularına tavsiyeler vermek (GDPR §58/3-a),
- Kendiliğinden ya da talep üzerine, ulusal parlamentoya, Üye Devlet hükümetine ya da Üye Devlet hukuku çerçevesinde diğer kurumlara ve kamuya görüşlerini bildirmek (GDPR §58/3-b),
- Üye Devlet hukukunda, kamu yararı için yerine getirilen bir göreve ilişkin işleme faaliyetlerinde denetim kurumundan izin alınması öngörülmüşse (GDPR §36/5), gerekli izni vermek (GDPR §58/3-c),
- 40 ıncı madde kapsamındaki davranış kuralları taslak halindeyken bunlar hakkında görüş bildirmek ve bunları onaylamak (GDPR §58/3-d),
- Sertifika veren kurumların akreditasyonu ile birlikte, sertifika vermek ve sertifika verilmesi için belirlenen kriterleri onaylamak (GDPR §58/3-e, f)
- Kişisel verilerin korunmasına yönelik standart hükümler belirlemek (GDPR §58/3-g),
- Üçüncü ülkelere uygun önlemlere tabi veri aktarımı hallerinde, buna yönelik sözleşme hükümleri ile idari anlaşmaları ve bağlayıcı kurumsal kuralları onaylamak (GDPR §58/3-h, i, j).

V.D.Denetim Kurumları Arasında İşbirliği ve İstikrar Mekanizması

Yukarıda da belirtildiği gibi, Tüzük, denetim kurumlarını, Tüzük'ün etkin bir şekilde ve istikrarlı olarak uygulanmasını sağlamak üzere, diğer denetim kurumları ile işbirliği yapmakla görevlendirmiştir. İşbirliği, aynı Üye Devlet içerisinde baş denetim kurumu ile diğer denetim kurumları arasında söz konusu olabileceği gibi, ilk kez Tüzük ile öngörülen istikrar mekanizması kapsamında bir Üye Devletin denetim kurumu ile diğer Üye Devletlerdeki denetim kurumlarının ve Komisyon'un birlikte hareket etmesi de mümkündür.

V.D.1.Denetim Kurumları Arasında İşbirliği

Tüzük'ün 60 ıncı maddesi uyarınca, baş denetim kurumu konumundaki denetim kurumu ile diğer denetim kurumları, bu madde çerçevesinde işbirliği

yapmak ve gerekli her türlü bilgiyi birbirlerine sağlamak zorundadırlar. Özellikle soruşturma yürütmek ve farklı bir Üye Devlete bağlı veri sorumlularının ya da veri işleyenlerin uyguladığı önlemleri denetlemek üzere, 61 inci madde çerçevesinde karşılıklı yardımlaşabilecekleri gibi, 62 nci madde uyarınca ortak hareket etmeleri de mümkündür (GDPR §60/2).

V.D.1.a)Karşılıklı Yardımlaşma

Tüzük'ün 61 inci maddesi uyarınca, denetim kurumları, Tüzük'ün istikrarlı bir şekilde uygulanabilmesi için birbirleriyle yardımlaşmalı ve gerekli bilgileri birbirlerine sağlamalı, ayrıca etkin bir işbirliği için gerekli önlemleri almalıdır. Komisyon, maddenin 9 uncu fıkrası doğrultusunda karşılıklı yardımlaşmanın şeklini ve usulünü belirleyebilir.

Her denetim kurumu, diğer bir denetim kurumunun karşılıklı yardımlaşma talebine, haksız bir gecikme olmaksızın ve en geç bir ay içinde cevap vermek zorundadır. Bu talepler gerekli tüm bilgilerin yanı sıra, işbirliğinin amacını ve nedenlerini de içermelidir. Denetim kurumları, karşılıklı yardımlaşma taleplerini, talebin yöneldiği konu yönünden yetkisiz olmadıkça veya talebi kabul etmesi AB ya da bağlı bulunduğu Üye Devlet hukukunu ihlal etmedikçe reddedemez.

Karşılıklı yardımlaşma talebine bir ay içinde cevap verilmemesi halinde, talepte bulunan denetim kurumu, 55 inci madde kapsamında bağlı bulunduğu Üye Devlet sınırları içerisinde birtakım önlemler alabilir. Bu durumda, 66 ncı madde kapsamında aciliyet prosedürünün uygulanma koşullarının gerçekleştiği kabul edilir ve Avrupa Veri Koruma Kurulu'ndan bu konuda acil bir görüş ya da bağlayıcı bir karar istenebilir (GDPR §61/8).

V.D.1.b)Ortak Faaliyet

Tüzük'ün 62 nci maddesi uyarınca, gerekli olduğu hallerde denetim kurumları, ortak soruşturmalar ve icrai önlemler dahil olmak üzere, ortak faaliyetler yürütmelidir. Buna göre, veri sorumlusunun ya da veri işleyenin birden fazla Üye

Devlet sınırları içerisinde kuruluşunun bulunduğu, veya işleme faaliyetlerinin birden fazla Üye Devletin sınırları içinde bulunan çok sayıda veri öznesini önemli ölçüde etkileme olasılığının bulunduğu hallerde, ilgili tüm Üye Devletlerin denetim kurumları ortak faaliyetlere katılma hakkına sahiptir. Baş denetim kurumu, ilgili tüm denetim kurumlarını ortak faaliyetlere katılmaya davet etmekle ve bu denetim kurumlarından gelen katılım taleplerine gecikme olmaksızın cevap vermekle yükümlüdür. Üye Devlet hukuku dahilinde ve yardım alınan denetim kurumunun da izin vermesi halinde, bu denetim kurumu yürütülen ortak faaliyet kapsamında yetkilendirilebilir ya da soruşturmanın yürütüldüğü Üye Devlet hukukuna uygun olarak ve bu Üye Devletin denetim kurumunun gözetimi dahilinde, yardım alınan denetim kurumu kendi yetkilerini de kullanabilir (GDPR §62/3). Bu durumda, bu Üye Devlet, destek alınan denetim kurumu çalışanlarının davranışlarından ve faaliyetler sırasında verdikleri zararlardan sorumlu olacaktır (GDPR §62/4). Destek alınan denetim kurumunun bağlı olduğu Üye Devlet, zararı karşılayan Üye Devlete, karşıladığı bedelin tamamını iade edecektir, ancak bunun dışındaki hallerde Üye Devletler, ortak faaliyetler sırasında meydana gelen zararlara ilişkin olarak, birbirlerinden tazminat talep etmekten kaçınmalıdır (GDPR §62/5, 6).

Baş denetim kurumu, bir ay içinde ilgili tüm denetim kurumlarını ortak faaliyetlere katılmaya davet etmezse ya da bu denetim kurumlarından gelen katılım taleplerine cevap vermezse, ilgili denetim kurumları, 55 inci madde kapsamında bağlı bulunduğu Üye Devlet sınırları içerisinde birtakım önlemler alabilir. Bu durumda, 66 ncı madde kapsamında aciliyet prosedürünün uygulanma koşullarının gerçekleştiği kabul edilir ve Avrupa Veri Koruma Kurulu'ndan bu konuda acil bir görüş ya da bağlayıcı bir karar istenebilir (GDPR §62/7).

V.D.2.İstikrar Mekanizması

Tüzük'te 63 ila 65 inci maddeler arasında düzenlenen istikrar mekanizması, denetim kurumlarının birbirleriyle ve Komisyon ile işbirliği yapmasının yanı sıra, özellikle AB genelinde etkili olabilecek önlemleri ve Tüzük'ün bir somut olayda ne şekilde uygulanması gerektiğine yönelik uyuşmazlıklar hakkında Avrupa Veri Koruma Kurulu'na başvurmasını öngören bir sistemdir. AB kişisel verilerin

korunması hukukunun yeknesaklaştırılmasında kilit rol oynayan[272] istikrar mekanizması, Tüzük taslak halindeyken Komisyon'a tanınan geniş yetkiler nedeniyle denetim kurumlarının bağımsızlığı ile çeliştiği[273] yönünde eleştirilere maruz kalmıştır. Daha sonra yapılan değişikliklerle, bu kez de bürokrasinin arttığı gerekçesiyle eleştirilmesine karşın, bu konudaki tartışmalı hususlar Tüzük'ten kaldırılmıştır.[274]

Tüzük'ün 64 üncü maddesi uyarınca; veri koruma etki değerlendirmesi gerektiren hallerin belirlenmesi ve listesinin çıkarılmasında, davranış kuralları (GDPR §40) ya da sertifikasyona (GDPR §41 vd.) ilişkin hususlarda, kişisel verilerin korunmasına yönelik standart hükümler belirlenmesinde ve üçüncü ülkelere uygun önlemlere tabi veri aktarımı hallerinde, buna yönelik sözleşme hükümleri ile idari anlaşmaları ve bağlayıcı kurumsal kuralların onaylanmasında, ilgili kararın taslağı Avrupa Veri Koruma Kurulu'na gönderilmeli ve Kurul, bu konuda halihazırda bir görüşü bulunmuyorsa, görüş bildirmelidir. Bunun için anılan maddenin üçüncü fıkrasında, altı haftalığına uzatılabilecek sekiz haftalık bir süre öngörülmüştür. Bu sürenin sona ermesinden önce denetim kurumu kararını uygulamaya koyamaz (GDPR §64/6). Kurul görüşünü açıkladıktan sonra iki hafta içinde, denetim kurumu, Kurul görüşünü azami ölçüde dikkate alarak, kararını, varsa görüş çerçevesinde yaptığı değişikliklerle birlikte, yeniden denetim kurumuna gönderir (GDPR §64/7). Eğer denetim kurumu, Kurul'a, görüşünü benimsemeyeceğini belirtilen süre içinde bildirirse, gerekli durumlarda, Kurul konuya ilişkin bağlayıcı bir karar verebilir (GDPR §64/8).

Tüzük'ün 65 inci maddesi, Tüzük'ün somut olaylar yönünden doğru ve istikrarlı bir şekilde uygulanabilmesi için, belirli durumlarda Kurul'un bağlayıcı kararlar verebileceğini öngörmüştür. Başka bir ifadeyle, Kurul, uyuşmazlık çözümü ile görevlendirilmiştir.[275] Buna göre, bir denetim kurumu, baş denetim kurumunun bir taslak kararına yerinde ve gerekçeli bir itirazda bulunmuşsa ya da bu itiraz baş

---

[272] **Lynskey**, *The Foundations*, s. 68.

[273] **Hornung**, s. 81.

[274] **Lynskey**, *The Foundations*, s. 69-70.

[275] **Develioğlu**, s. 142, dpn. 7.

denetim kurumu tarafından yerinde veya gerekçeli olmadığı için reddedilmişse, Kurul bu konuda bağlayıcı bir karar verebilir. Aynı şekilde, bir veri sorumlusunun ya da veri işleyenin ana işletmesi yönünden hangi denetim kurumunun yetkili olacağı yönünde görüş ayrılığı bulunuyorsa, Kurul bu hususu da karara bağlayacaktır. Nihayet, bir denetim kurumu, Kurul'un 64 üncü madde çerçevesinde görüş bildirmesini talep etmezse ya da bu kapsamdaki bir Kurul görüşüne uymazsa, ilgili denetim makamları ile Komisyon, bu durumu Kurul'a bildirebilir. Bu madde kapsamındaki kararlar başvurudan itibaren bir ay içinde ve üçte ikilik çoğunlukla alınır. Eşitlik halinde kararı Başkan verir. Kurul kararı haksız bir gecikme olmaksızın ilgili denetim kurumlarına bildirilir. Baş denetim kurumu ya da şikayette bulunulan denetim kurumu, haksız bir gecikme olmaksızın ve Kurul'un kararından itibaren en geç bir ay içinde ilgili konuda kararını verir.

Son olarak, Tüzük'ün 66 ncı maddesi uyarınca, olağanüstü hallerde, veri öznelerinin hak ve özgürlüklerinin korunabilmesi için acilen harekete geçilmesi gerekliyse, denetim kurumları, kendi yetkili oldukları Üye Devlet sınırları içinde hukuki sonuç doğuracak şekilde ve üç aydan uzun olmamak üzere belirli bir süre için geçerli önlemler alabilecektir. Denetim kurumları, Kurul'dan bu yönde acil olarak bir görüş bildirmesini veya bağlayıcı bir karar vermesini isteyebileceği gibi, böyle bir durumda denetim kurumlarının gerekli önlemleri almadığı hallerde de Kurul'a başvurulabilecektir. Aciliyet prosedürü kapsamındaki görüşler ve bağlayıcı kararlar, iki hafta içerisinde, basit çoğunlukla alınır.

V.E. Avrupa Veri Koruma Kurulu

V.E.1. Genel Olarak

Avrupa Veri Koruma Kurulu, Tüzük'ün 68 inci maddesi ile kurulan, görevleri ve işleyişine ilişkin esaslar Tüzük ile belirlenen, bağımsız ve tüzel kişiliği haiz bir AB organıdır. Anılan madde uyarınca Kurul, Kurul Başkanı tarafından temsil edilir ve Üye Devletlerin denetim kurumlarının başkanları[276] ile Avrupa Veri Koruma

[276] Eğer bir Üye Devlette birden fazla denetim kurumu görev yapıyorsa, o Üye Devlet hukuku çerçevesinde tüm denetim kurumları için ortak bir temsilci atanır (GDPR §68/4).

Denetçisi veya bunların temsilcilerinden oluşur. Komisyon, Kurul'un toplantılarına katılabilir ve faaliyetlerine dahil olabilir, ancak oy kullanma hakkı bulunmamaktadır. Kurul, görevlerini yerine getirirken ve yetkilerini kullanırken bağımsız hareket eder, kimseden talimat almaz ve isteyemez (GDPR §69).

Kurul, Tüzük'ün yürürlüğe girmesi ile faaliyeti sona eren Madde 29 Çalışma Grubu'nun yerini almıştır.[277]

V.E.2.Avrupa Veri Koruma Kurulu'nun Görevleri

Kurul'un en temel görevi, Tüzük'ün etkin ve istikrarlı bir şekilde uygulanmasını sağlamaktır. Bu çerçevede, Tüzük, 70 inci maddesinin birinci fıkrasında, Kurul'un kendi inisiyatifiyle ya da Komisyon talebi doğrultusunda özellikle yerine getirmesi gereken görevleri son derece geniş kapsamlı olarak saymıştır. Maddenin ifade tarzından, bu görevlerin sınırlı sayıda olmadığı ve tümünün Tüzük'ün istikrarlı bir şekilde uygulanması amacını gerçekleştirmeye yönelik olduğu anlaşılmaktadır. Bu görevler şu şekildedir:

- İstikrar mekanizması çerçevesinde Tüzük'ün doğru şekilde uygulanmasını denetlemek ve sağlamak (GDPR §70/1-a),
- Tüzük'te değişiklik teklifleri de dahil olmak üzere, Komisyon'a kişisel verilerin korunmasına ilişkin her türlü hususta tavsiyelerde bulunmak (GDPR §70/1-b),
- Komisyon'a; veri sorumluları, veri işleyenler ve denetim kurumları arasındaki veri aktarımlarına ilişkin bağlayıcı kurumsal kuralların formatı ve prosedürlerine ilişkin tavsiyelerde bulunmak (GDPR §70/1-c),
- Unutulma hakkı kapsamında kamuya açıklanan kişisel verilerin bağlantılarının ve kopyalarının silinmesi için en iyi uygulamalar ve prosedürlerin neler olduğuna ilişkin rehberler ve tavsiyeler yayımlamak (GDPR §70/1-d),
- Kendi inisiyatifiyle veya talep doğrultusunda Tüzük'ün istikrarlı bir şekilde uygulanmasına yönelik olarak Tüzük'ün çeşitli hükümlerinin hayata

[277] **Hornung**, s. 71; **Küzeci**, s. 161.

geçirilmesine yönelik en iyi uygulamalar ve prosedürlerin neler olduğuna ilişkin rehberler ve tavsiyeler yayımlamak (GDPR §70/1-e - m),

- Davranış kurallarının ve sertifikasyon, veri koruma mührü gibi uygulamaların benimsenmesini teşvik etmek ve bu uygulamalara ilişkin hususlarda Komisyon'a görüş bildirmek (GDPR §70/1-n - q),
- GDPR §12/7 uyarınca veri öznesine verilecek bilgiler standart semboller kullanılarak sunulacaksa, Komisyon'a bu konuda görüş bildirmek (GDPR §70/1-r),
- Üçüncü ülkelerin ya da uluslararası örgütlerin yeterlilik düzeyinin belirlenmesinde Komisyon'a görüş bildirmek (GDPR §70/1-s),
- İstikrar mekanizması çerçevesinde denetim kurumlarının taslak kararları hakkında görüş bildirmek ve aciliyet prosedürü kapsamındaki haller de dahil olmak üzere, uyuşmazlık çözüm mercii olarak bağlayıcı kararlar vermek (GDPR §70/1-t),
- Denetim kurumları arasında işbirliğini ve iki taraflı ya da çok taraflı bilgi paylaşımını teşvik etmek (GDPR §70/1-u),
- Denetim kurumları arasında ortak eğitim programları düzenlenmesini teşvik etmek ve personel değişimini kolaylaştırmak (GDPR §70/1-v),[278]
- Dünya genelindeki denetim kurumları ile kişisel verilerin korunması düzenlemeleri ve uygulamalarına yönelik bilgi alışverişinde bulunulmasını teşvik etmek (GDPR §70/1-w),
- Veri sorumlularının ya da veri işleyenlerin hazırladıkları davranış kuralları hakkında görüş bildirmek (GDPR §70/1-x),
- İstikrar mekanizması kapsamında ele alınan hususlara ilişkin olarak, denetim kurumları ya da mahkemeler tarafından verilen kararların kamunun erişimine açık, elektronik bir sicilini tutmak (GDPR §70/1-y).

Komisyon'un tavsiye istediği kimi hallerde, talep, olayın aciliyetine bağlı olarak bir süre sınırı içerebilir (GDPR §70/2). Kurul, görüşlerini, rehberlerini ve önerilerini; Komisyon'a ve Tüzük uyarınca Komisyon'a yardım etmekle görevli

[278] Bu düzenleme, mümkün olan hallerde üçüncü ülkelerin denetim kurumlarını ve uluslararası örgütleri de kapsamaktadır.

komiteye[279] bildirir ve bunları kamunun erişimine açar (GDPR §70/3). Ayrıca Kurul, görevlerini yerine getirirken mümkün olan hallerde ilgili taraflara da danışmalı ve makul bir süre içinde görüş bildirmelerine imkan tanımalıdır (GDPR §70/4).

Nihayet, Kurul, rehberlerinin ve önerilerinin uygulanmasına yönelik denetim sonuçlarının yanı sıra istikrar mekanizması çerçevesinde verdiği bağlayıcı kararları da içeren, gerçek kişilerin kişisel verilerinin işlenmesi karşısında korunmasına yönelik bir rapor hazırlar, bu raporu kamunun erişimine açar ve Komisyon'un yanı sıra Avrupa Parlamentosu ile Avrupa Birliği Konseyi'ne de iletir (GDPR §71).

V.E.3.Avrupa Veri Koruma Kurulu'nun Kurumsal Yapısı

Tüzük'ün 72 nci maddesi uyarınca, Kurul, Tüzük'te aksi belirtilmedikçe, basit çoğunlukla karar alır, ancak kendi izleyeceği prosedürlerin belirlenmesine yönelik kararlarda üçte ikilik nitelikli çoğunluk aranır.

Kurul'un bir Başkanı, iki başkan yardımcısı ve bir de Sekreterliği bulunur. Başkan ve yardımcıları, basit çoğunlukla seçilir ve görev süreleri 5 yıldır. Aynı kişiler yalnızca bir dönem daha yeniden seçilebilir (GDPR §73). Başkan ve yardımcıları, Kurul'u toplantıya çağırmakla, Kurul'un gündemini belirlemekle, istikrar mekanizması kapsamında verilen bağlayıcı kararları denetim kurumlarına bildirmekle ve istikrar mekanizması kapsamındakiler başta olmak üzere Kurul'un görevlerinin zamanında yerine getirilmesini sağlamakla görevlidir. Kurul, başkan ve yardımcıları arasında görev dağılımına ilişkin esasları kendisi belirler (GDPR §74).

Sekreterlik, Avrupa Veri Koruma Denetçisi tarafından oluşturulur ve yalnızca Kurul Başkanı'nın talimatı altında görev yapar. Avrupa Veri Koruma Denetçisi'nin Kurul Sekreterliği'nde görev alan personeli, Denetçi'nin olağan işlerinde görev alan personelinin aksine Kurul'a karşı sorumlu olur. Kurul'un günlük işleri, Kurul içi ve Kurul dışı iletişimin sağlanması ve bu doğrultuda elektronik yolların kullanılması, bilgilerin çevirisinin yapılması, Kurul toplantılarının hazırlığının ve takibinin yapılması ve görüşlerin, kararların ve Kurul tarafından kabul edilen diğer belgelerin yazılması ve yayımlanması Sekreterlik'in başlıca görevleridir (GDPR §75).

[279] Bkz. GDPR §93.

VI. ÖZEL VERİ İŞLEME HALLERİ

Kişisel verilerin korunması hakkı mutlak bir hak olmayıp, başka kişilerin hak ve özgürlüklerinin yanı sıra, bu kişilerin ya da kamunun menfaatlerinden kaynaklanan nedenlerle sınırlanabilmekte ya da istisnalara tabi olabilmektedir. Kişisel verilerin korunmasına ilişkin bütün belgelerde bu yönde düzenlemeler yer almaktadır.[280] Direktif de, özel yaşamın gizliliği hakkı ile ifade özgürlüğü arasında bir denge sağlanmasına ilişkin 9 uncu maddesinin yanı sıra, 13 üncü maddesinde kimi sınırlama halleri saymıştır. Tüzük'te de benzer bir düzenleme yer almakla birlikte,[281] özellikle kişisel verilerin korunması hakkının bazı yarışan haklarla bağdaştırılmasını sağlamak amacıyla, kimi veri işleme hallerinin ayrıca düzenlenmesine gerek görülmüştür.

Öncelikle, Direktif'in, Üye Devletler için getirdiği özel yaşamın gizliliği hakkı ile ifade özgürlüğü arasında bir denge sağlanması yönünde düzenlemeler yapma yükümlülüğü, Tüzük'ün 85 inci maddesinde, daha detaylı bir şekilde tekrarlanmıştır. Tüzük ile, Üye Devletlerin bu konuda kanun çıkarması öngörülmektedir. Bu kapsamda çıkarılan kanunlar ve bunlar üzerindeki her türlü değişiklik, gecikmeksizin Komisyon'a bildirilecektir.

Tüzük'ün 86 ncı maddesi uyarınca, bir kamu kurumunun ya da kamu yararına görev yerine getiren bir özel kurumun elindeki resmi belgelerde yer alan kişisel veriler, AB ya da ilgili kurumun tabi olduğu Üye Devlet hukuku kapsamında, resmi belgelerin kamuya açıklığı ile kişisel verilerin korunması hakkı arasında bir denge sağlanabilmesi için kamuya açıklanabilecektir.

Tüzük'ün 87 nci maddesi kapsamında, Üye Devletler, ulusal kimlik numaralarının işlenmesine yönelik özel koşullar öngörebilir. Bu durumda ulusal kimlik numaraları, ancak Tüzük'e uygun olarak, veri öznelerinin haklarının ve özgürlüklerinin korunmasına ilişkin uygun güvenlik önlemlerinin alınmış olması koşuluyla işlenebilir.

---

[280] **Küzeci**, s. 267.

[281] Tüzük'te sınırlama hallerinin düzenlenişi için bkz. yuk. s. 87-88.

Tüzük'ün 88 inci maddesi kapsamında, Üye Devletler, işçilerin hak ve özgürlüklerini güvence altına almak için, iş ilişkisi çerçevesinde işçilerin kişisel verilerinin işlenmesine yönelik özel kurallar belirleyebilir. Bu kurallar, veri öznesinin onuru, meşru menfaatleri ve temel haklarını korumaya yönelik uygun ve spesifik güvenlik önlemlerini içermelidir.

Tüzük'ün 89 uncu maddesi uyarınca, kamu yararı için arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla yürütülen işleme faaliyetleri, Tüzük hükümlerine uygun olarak, veri öznelerinin hak ve özgürlüklerinin güvence altına alınması için uygun güvenlik önlemlerine tabi olmalıdır. Özellikle veri minimizasyonu ilkesine uygunluğun sağlanması için gerekli teknik ve kurumsal önlemler alınmış olmalıdır. Üye Devlet hukukunda, bu amaçlara ulaşmak için gerekli olduğu hallerde, veri öznelerinin erişim, düzeltme, silme, veri taşınabilirliği, itiraz gibi haklarının kullanılmasına ilişkin istisnalar öngörülebilir. Ancak bu hakların kullanımının, belirtilen amaçlara ulaşılmasını imkansız hale getirecek ya da önemli ölçüde güçleştirecek olması gerekmektedir.

Tüzük'ün 90 ıncı maddesi kapsamında, Üye Devletler, kişisel verilerin korunması hakkı ile gizlilik yükümlülüğünün çatıştığı hallerde, denetim kurumunun görevleri doğrultusunda veri sorumlularının ya da veri işleyenlerin elindeki kişisel verilere ve bunların işyerlerine erişim yetkilerine yönelik düzenlemeler öngörebilir.

Son olarak, Tüzük'ün 91 inci maddesi, Tüzük'ün yürürlük tarihinde, kiliselerin ve diğer dini kurumların işleme faaliyetlerine karşı gerçek kişilerin korunmasına yönelik kapsamlı düzenlemeler uygulamakta olduğu Üye Devletlerde, bu düzenlemelerin Tüzük'e uygun hale getirilmek koşuluyla uygulanmaya devam etmesine izin vermiştir. Bu işleme faaliyetleri, bağımsız bir denetim kurumunun denetimine tabi olacaktır. İlgili denetim kurumunun ayrıca belirlenmesi mümkündür.

BEŞİNCİ BÖLÜM
SONUÇ

Kişisel veriler, her çeşit bilgi gibi, tarih boyunca kayda değer bir önem arz etmiştir. Kişisel verilerin önemi, bir bireye doğrudan ilişkin olması ve bu özelliği nedeniyle söz konusu bireyin belirlenmesi ve bu birey hakkında kararlar alınmasında kullanılabilmesinden kaynaklanmaktadır. Bu tür verilerin önemi ve değeri, teknolojik gelişmelerin veri işlemeyi çok daha kolay ve hızlı hale getirmesi, aynı zamanda bunun bir sonucu olarak verilere daha fazla ihtiyaç duyulmaya başlaması nedeniyle çok yakın geçmişte katlanarak artmıştır. Bu ortamda, bir hak olarak kişisel verilerin korunması ön plana çıkmış, bu hak ile kamu sektörü ile özel sektörün kişisel verilerin işlenmesini gerektiren meşru menfaatleri arasında bir denge kurulması gereği ve kişisel verilerin işlenmesi yönünden mevcut ve olası risklere yönelik endişeler, kişisel verilerin korunmasının bir hukuk dalı olarak gelişimine zemin hazırlamıştır.

Avrupa'da ulusal düzeyde başlayan kişisel verilerin korunmasına ilişkin esasların kanunlaştırılması hareketi, öncelikle kişisel verileri işleyen kişiler ve kurumların, verilerin ilişkin olduğu veri özneleri karşısında orantısız bir güce erişmesini önleme amacına yönelmiş olup, daha sonra kişisel verilerin korunması, insan hakları bağlamında ele alınmaya başlanmış ve nihayet OECD, BM gibi örgütlerin çalışmaları ile uluslararası bir boyut kazanmıştır. Dünya genelinde kişisel verilerin korunmasına yönelik bir farkındalık oluşmasına ve bu alanda çalışmaların yaygınlaşmasına rağmen, Avrupa, kişisel verilerin korunması hukukunun gelişimindeki öncü konumunu yitirmemiştir. 1981 tarihinde yürürlüğe giren ETS 108 ile 1995 yılında yürürlüğe giren 95/46/AT sayılı Direktif, dönemlerinin kişisel verilerin korunması alanına yönelik en kapsamlı düzenlemeleri olup, Türkiye dahil olmak üzere, dünyanın geri kalanındaki ulusal ve uluslararası çalışmaları etkilemiştir. Nitekim ülkemizde, 2010 yılında kişisel verilerin korunması hakkına Anayasal dayanak kazandırılmış, 2016 yılında da hazırlanmasında Direktif'ten yararlanılan Kişisel Verilerin Korunması Kanunu kabul edilerek yürürlüğe girmiştir.

Zaman içinde, Direktif, internetin ortaya çıkışı ve yaygınlaşması başta olmak üzere, teknolojik gelişmeler karşısında yetersiz kalmaya başlamıştır. Ayrıca Direktif'in, Üye Devletlerin Direktif esaslarını iç hukukuna aktarmadaki yorum ve

yöntem farklılıkları nedeniyle, AB düzeyinde kişisel verilerin korunması hukukunun yeknesaklığını sağlama amacını da etkili bir şekilde yerine getiremediği görülmüştür. Tüm bu gelişmeler sonucunda, Avrupa Komisyonu, bir veri koruma reformuna duyulan ihtiyacı belirtmesi ve bir reform paketi önerisi sunması üzerine başlayan çalışmalar, (AB) 2016/679 sayılı AB Genel Veri Koruma Tüzüğü ile (AB) 2016/680 sayılı Direktif'in 27 Nisan 2016 tarihinde kabul edilmesiyle son bulmuştur. 25 Mayıs 2018 itibariyle yürürlükte olan Tüzük, Direktif'teki birtakım düzenlemelere daha kapsamlı ve detaylı bir şekilde, birtakım değişikliklerle yeniden yer vermiştir. Örneğin Direktif'in AB dışına kişisel veri aktarımı için Komisyon'un yeterlilik kararı bulunmasını gerektiren düzenlemesi, üçüncü ülkelerin yanı sıra uluslararası örgütleri de kapsayacak şekilde ve bu tarz bir kararın bulunmadığı hallerde aktarımın nasıl yapılacağına ilişkin düzenlemelerle birlikte Tüzük'te de yer almıştır. Bunların yanı sıra Tüzük, unutulma hakkı, tasarımsal koruma, denetim kurumları arasında yardımlaşma ve istikrar mekanizması gibi yenilikler de getirmektedir. Tüzük, veri öznelerinin kişisel verileri üzerindeki kontrolünü ön plana almakta, veri sorumluları ve veri işleyenler yönünden işleme faaliyetlerinin güvenliğine yönelik yüksek standartlar getirmekte, hükümlerine aykırılık halinde ciddi yaptırımlar öngörmektedir. AB hukukunda tüzüklerin, tüm Üye Devletler yönünden, herhangi bir işleme gerek kalmaksızın bağlayıcı olduğu göz önüne alındığında, Tüzük'ün, AB genelinde yeknesaklığın sağlanması yönünden de etkili olacağı anlaşılmaktadır.

Tüzük uyarınca kişisel verilerin işlenmesi, ancak kişisel verilerin korunmasını temel ilkelerine uygun olduğu ölçüde ve veri öznesinin rızası başta olmak üzere bir hukuka uygunluk sebebine dayandığı ölçüde hukuka uygun olacaktır. Ayrıca, veri öznelerinin kişisel verilerinin geleceğini belirleme haklarını etkin bir şekilde kullanabilmeleri için, veri öznelerine birtakım haklar tanınmıştır. Buna göre veri özneleri, kişisel verilerinin işlenip işlenmediğini öğrenme ve işlendiği takdirde işleme sürecine ilişkin bilgi edinme, kişisel verilerinin düzeltilmesini, silinmesini ya da işlenmesinin kısıtlanmasını talep etme, verilerini bir veri sorumlusundan diğerine aktarma, verilerinin işlenmesine itiraz etme, otomatik bireysel karar alma uygulamalarına konu olmama gibi haklara sahiptir. Özellikle silme ya da unutulma hakkı bu çerçevede ön plana çıkmaktadır. Veri öznesinin, saklanmasına ya da farklı

bir şekilde işlenmesine artık ihtiyaç duyulmayan kişisel verilerinin silinmesini talep etme hakkını ifade eden unutulma hakkı, özellikle ABAD'ın Google Spain kararının da etkisiyle hukuk çevrelerinin gündemini oldukça meşgul etmiştir. Bunların yanı sıra, Tüzük'e aykırı işleme faaliyetlerinden zarar gördüğü takdirde, hukuki çarelere başvurma imkanı bulunmaktadır. Bu kapsamda veri sorumluları ve veri işleyenler yönünden, özellikle işleme sürecinde kişisel verilerin güvenliğinin sağlanmasına yönelik ciddi yükümlülükler öngörülmüş olup, bu kişiler yükümlülüklerini tamamen ya da kısmen yerine getirmedikleri takdirde veri öznelerinin bundan dolayı uğradığı zararları tazmin etmek zorunda kalacakları gibi, birtakım idari yaptırımlarla da karşılaşabileceklerdir.

Tüzük'ün önemli düzenlemelerinden bir diğeri, denetim kurumları yönünden öngörülmüş işbirliği ve istikrar mekanizmalarıdır. Buna göre, tüm Üye Devletlerin bağımsız denetim kurumları, Tüzük'ün AB genelinde doğru ve istikrarlı bir şekilde uygulanmasını sağlamak adına, birbirleri, Komisyon ve Tüzük ile kurulan Avrupa Veri Koruma Kurulu ile işbirliği halinde olacaktır. Kurul, denetim kurumu kararları hakkında görüş bildirir ve uyuşmazlık çözüm mercii olarak görev yapar.

Tüzük, AB kişisel verilerin korunması hukukuna köklü yenilikler getirmiştir. Gerek kişisel verilerin korunması hukukunun gelişiminde neredeyse tüm dünyanın Avrupa'yı örnek alınması ve Avrupa'dan etkilenmesi, gerekse Tüzük'ün dünyanın neresinde olursa olsun AB sınırları içerisindeki veri öznelerine yönelik işleme faaliyetleri gerçekleştiren kişiler yönünden uygulanabilen yapısı nedeniyle, söz konusu değişimin Avrupa dışında da karşılık bulacağı rahatlıkla öngörülebilir. Türkiye'nin AB ile ilişkileri, AB sınırları içerisindeki Türk vatandaşlarının Tüzük çerçevesinde birer veri öznesi oldukları ve AB sınırları içerisinde bir kuruluşu bulunsun bulunmasın AB sınırları içerisindeki veri öznelerini hedef alan pazarlama ve izleme faaliyetleri yönünden Türk veri sorumlularının ve veri işleyenlerinin Tüzük'e tabi oldukları göz önüne alındığında, Tüzük'ün kişisel verilerin korunması hukukunda yarattığı değişimin iyi anlaşılmasının ve gelecekteki olası etkilerinin iyi analiz edilmesinin, oluşturmaya başlamakta oldukça geç kaldığımız veri koruma kültürümüze büyük katkıları olacaktır.

KAYNAKÇA

ABAD, Bodil Lindqvist v Åklagarkammaren i Jönköping, C-101/01, 6 Kasım 2003. - http://curia.europa.eu/juris/liste.jsf?num=C-101/01 (Erişim tarihi: 7/5/2019)

ABAD, 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 and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others, Joined Cases C-293/12 and C-594/12, 8 Nisan 2014. - http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3596495 (Erişim tarihi: 9/3/2019)

ABAD, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, 13 Mayıs 2014. - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (Erişim tarihi: 17/4/2019)

ABAD, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 Ekim 2015. - http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2863454 (Erişim tarihi: 17/4/2019)

ABAD, Maximilian Schrems v Data Protection Commissioner, C-362/14, 6 Ekim 2015. - http://curia.europa.eu/juris/document/document.jsf?text=&docid=172254&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4466488 (Erişim tarihi: 10/5/2019)

ACKOFF R. L. (1999), "From Data to Wisdom", Ackoff's Best, John Wiley & Sons, New York, s. 170-172.

AİHM, Amann v Switzerland, 27798/95, 16 Şubat 2000. - http://hudoc.echr.coe.int/eng?i=001-58497 (Erişim tarihi: 4/2/2019)

AİHM, Rotaru v Romania, 28351/95, 4 Mayıs 2000. - http://hudoc.echr.coe.int/eng?i=001-58586 (Erişim tarihi: 4/2/2019)

AİHM, Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland, 931/13, 27 Haziran 2017. - http://hudoc.echr.coe.int/eng?i=001-175121 (Erişim tarihi: 4/2/2019)

AKGÜL Aydın (2013), Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi (Yayımlanmamış Doktora Tezi), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli.

AKINCI Ayşe Nur (2017), Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, T.C. Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, Ankara.

AKSOY Hüseyin Can **(**2010), Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak, Ankara.

APEC Mission Statement - https://www.apec.org/About-Us/About-APEC/Mission-Statement (Erişim tarihi: 9/3/2019)

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 Haziran 2007.

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 Şubat 2010.

Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173, 13 Temmuz 2010.

Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP 187, 13 Temmuz 2011.

Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 Nisan 2014.

Avrupa Konseyi 108 sayılı Avrupa Konseyi Sözleşmesi Türkçe tam metni - http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/ak/turkce/108_tur.pdf (Erişim tarihi: 28/3/2019)

BAŞALP Nilgün (2015), "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 21, S. 1, s. 77-105.

BAYRAM Mehmet Hanifi (2011), Avrupa Birliği ve İnternet Hukuku, Seçkin, Ankara.

BOSTANCI BOZBAYINDIR Gülşah (2018), "Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, S. 2018/2, s. 51 - 103.

BOZKURT Enver; **KÖKTAŞ** Arif (2018), Avrupa Birliği Hukuku, 7. Baskı, Legem, Ankara.

BOZKURT YÜKSEL Armağan Ebru (2016), "İnternet ve Unutulma Hakkı", 4.Uluslararası Bilişim Hukuku Kurultayı 2016 Bildiriler Kitabı, İzmir, s. 23 - 43.

BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83.

BYGRAVE Lee A. (2004), "Privacy Protection in a Global Context - A Comparative Overview", Scandinavian Law Studies, C. 47, s. 319 - 348.

Cambridge Advanced Learner's Dictionary & Thesaurus © Cambridge University Press - https://dictionary.cambridge.org/dictionary/english/ (Erişim tarihi: 5/12/2018)

CAVOUKIAN Ann (2010), "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D", Identity in the Information Society, C. 3, S. 2, s. 247 - 251.

Chart of signatures and ratifications of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=B16DdX3Y (Erişim tarihi: 28/3/2019)

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union (COM(2010) 609). - https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF (Erişim tarihi: 9/3/2019)

COOPER Ellyce R.; **RAUL** Alan Charles (2017), "APEC Overview", **RAUL** Alan Charles (ed.), The Privacy, Data Protection and Cybersecurity Law Review, 4. Baskı, Law Business Research Ltd, Londra, s. 26 - 38.

ÇEKİN Mesut Serdar (2018), Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha, İstanbul.

DEVELİOĞLU Hüseyin Murat (2017), Avrupa Birliği Genel Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha, İstanbul.

DURAL Mustafa; **ÖĞÜZ** Tufan (2018), Türk Özel Hukuku, Cilt: II, Kişiler Hukuku, 19. Baskı, Filiz, İstanbul.

EU Member State GDPR Implementation Laws and Drafts - https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/ (Erişim tarihi: 8/3/2019)

European Court of Human Rights Factsheet on Personal Data Protection, Şubat 2019. - https://www.echr.coe.int/Documents/FS_Data_ENG.pdf (Erişim tarihi: 4/2/2019)

European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the data protection reform package. - http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf (Erişim tarihi: 20/4/2019)

Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. - https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 (Erişim tarihi: 3/12/2018)

FALLON Rebecca (2015), "Celebgate: Two Methodological Approaches to the 2014 Celebrity Photo Hacks", **TRIOPANIS** Thanassis; **VAKALI** Athena; **SARTORI** Laura; **BURNAP** Pete (eds.), Internet Science: Second International Conference, INSCI 2015, Brussels, Belgium, May 27-29, 2015, Proceedings, s. 49 - 60.

Forecast of smartphone user numbers in Turkey from 2015 to 2022 (in million users) - https://www.statista.com/statistics/566218/predicted-number-of-smartphone-users-in-turkey/ (Erişim tarihi: 2/12/2018)

FRICKÉ Martin (2018), "Knowledge pyramid: the DIKW hierarchy", International Society for Knowledge Organization (ISKO) Encyclopedia of Knowledge Organization (IEKO). - http://www.isko.org/cyclo/dikw#3.2 (Erişim tarihi: 8/12/2018)

Full list of Council of Europe treaties signed by Turkey - https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/TUR?p_auth=dyD32ldD (Erişim tarihi: 12/3/2019)

Full text of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 (Erişim tarihi: 28/3/2019)

Full text of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim tarihi: 27/3/2019)

Full text of the revised OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Erişim tarihi: 28/3/2019)

Full text of the United Nation Guidelines for the Regulation of Computerised Personal Data Files - https://www.refworld.org/pdfid/3ddcafaac.pdf (Erişim tarihi: 28/3/2019)

Handbook on European Data Protection Law (2018). - http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law (Erişim tarihi: 24/10/2018)

HARBINJA Edina (2013), "Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?", SCRIPTed, C. 10, S. 1, s. 19-38. - http://script-ed.org/?p=843 (Erişim tarihi: 15/12/2018)

HERNÁNDEZ SÁNCHEZ Claudia Andrea (2005), The Meaning of the Information Society Services in the E-Commerce Directive, Oslo. - https://www.duo.uio.no/handle/10852/20433 (Erişim tarihi: 1/5/2019)

Hootsuite & We are Social, Digital in 2018 in Western Asia, slayt 180 vd. - https://www.slideshare.net/wearesocial/digital-in-2018-in-western-asia-part-1-northwest-86865983 (Erişim tarihi: 2/12/2018)

HORNUNG Gerrit (2012), "A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012", SCRIPTed, C. 9, S. 1, s. 64 - 81. - http://script-ed.org/?p=406 (Erişim tarihi: 19/10/2018)

HORNUNG Gerrit; **SCHNABEL** Christoph (2009), "Data Protection in Germany I: The population census decision and the right to informational self-determination", Computer Law & Security Report, C. 25, S. 1, s. 84-88. - https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Hornung/Hornung___Schnabel__Data_protection_in_Germany_I__CLSR_2009__84.pdf (Erişim tarihi: 8/3/2019)

HUSTINX Peter (2013), "EU Data Protection Law - Current State and Future Perspectives", High Level Conference: "Ethical Dimensions of Data Protection and Privacy", Centre for Ethics, University of Tartu/Data Protection Inspectorate, Tallinn. - https://edps.europa.eu/sites/edp/files/publication/13-01-09_speech_tallinn_en.pdf (Erişim tarihi: 8/5/2019)

Internet Users by Country (2016) - http://www.internetlivestats.com/internet-users-by-country/ (Erişim tarihi: 2/12/2018)

İŞEVİ A. Semih; **ÇELME** Burçin (2002), "Bilgi Çağında Yeni Hazine: Entelektüel Sermaye ile Rekabeti Yakalamak", I. ÜNAK Genel Konferansı (ÜNAK2002) 19 Mayıs Üniversitesi Samsun 10-12 Ekim 2002, Araştırma ve Teknoloji Genel Müdür Yardımcılığı, 2002 Ulusal ve Uluslararası Bildiriler. Şişecam, İstanbul. - http://eprints.rclis.org/7194/1/bilgidunyasiES.pdf (Erişim tarihi: 15/12/2018)

KERR Julia (2016), "What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What It Means for the Future of the Right to Be Forgotten", Chicago Journal of International Law, C. 17, S. 1, s. 217 - 243.

KORKMAZ Ali (2014), "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması", Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi, C. 16, Özel Sayı 1, s. 99 - 103. - http://dergi.kmu.edu.tr/userfiles/file/Mayis20141/14m.pdf (Erişim tarihi: 4/2/2019)

KOTLER Philip; **ARMSTRONG** Gary (2011), Principles of Marketing, 14. Baskı, Pearson.

KUCHEWSKY Monica (2013), What does the revision of the OECD Privacy Guidelines mean for businesses?, MLex Ab Extra. - https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf (Erişim tarihi: 28/3/2019)

KURT Levent (2005), Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin, Ankara.

KÜZECİ Elif (2010), Kişisel Verilerin Korunması, 2. Baskı, Turhan, Ankara.

LAMBERT Paul (2017), Understanding the New European Data Protection Rules, Taylor & Francis.

LYNSKEY Orla (2015), The Foundations of EU Data Privacy Law, Oxford University Press. **(Lynskey, The Foundations)**

LYNSKEY Orla (2015), "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja González", The Modern Law Review, C. 78, S. 3, s. 522 - 534. **(Lynskey, Control over Personal Data)**

MARQUES João (2016), ""And [they] built a crooked h[arbour]" – the Schrems ruling and what it means for the future of data transfers between the EU and US", UNIO - EU Law Journal, C. 2, S. 2, s. 54 - 70.

Mobile cellular subscriptions (per 100 people) - https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2017&locations=TR&start=2000 (Erişim tarihi: 2/12/2018)

MONTGOMERY Kathryn C.; **CHESTER** Jeff; **MILOSEVIC** Tijana (2017), "Children's Privacy in the Big Data Era: Research Opportunities", Pediatrics, C. 140, S. Supplement 2, s. 117 - 121. - https://doi.org/10.1542/peds.2016-1758O (Erişim tarihi: 2/12/2018)

OĞUZMAN M. Kemal; **BARLAS** Nami (2013), Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar), 19. Baskı, Vedat, İstanbul.

OĞUZMAN M. Kemal; **SELİÇİ** Özer; **OKTAY-ÖZDEMİR** Saibe (2012), Kişiler Hukuku, 12. Baskı, Filiz, İstanbul.

ÖNÜT Lale Burcu (2017), Avrupa Birliği Hukukunun Üye Devletlerde Uygulanması, Seçkin, Ankara.

PlayStation data breach deemed in 'top 5 ever' - https://www.cbc.ca/news/technology/playstation-data-breach-deemed-in-top-5-ever-1.1059548 (Erişim tarihi: 5/2/2019)

REGAN Priscilla M. (2003), "Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows", Journal of Social Issues, C. 59, S. 2, s. 263 - 282.

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach - https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (Erişim tarihi: 5/2/2019)

Revealed: how US and UK spy agencies defeat internet privacy and security - https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Erişim tarihi: 10/5/2019)

SOLOVE Daniel J. (2004), The Digital Person: Technology and Privacy in the Information Age, New York University Press.

TAMÒ-LARRIEUX Aurelia (2018), Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, Springer.

T.C. Avrupa Birliği Bakanlığı, 27. RİG Toplantısı Basın Bildirisi, Bursa, 11 Kasım 2012. - https://www.ab.gov.tr/files/sib/rig/27__rig_basin_bildirisi.pdf (Erişim tarihi: 12/3/2019)

Template data retention policy - https://www.privacy-advocaat.nl/public/documents/246/template-data-retention-policy.pdf (Erişim tarihi: 23/4/2019)

The Cambridge Analytica scandal affected nearly 40 million more people than we thought - https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/ (Erişim tarihi: 5/2/2019)

Turkish authorities 'probing huge ID data leak' - https://www.bbc.com/news/technology-35978216 (Erişim tarihi: 12/3/2019)

United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (Erişim tarihi: 27/3/2019)

UYGUN Murat (2010), Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması (Yayımlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

VOSS W. Gregory (2012), "Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments", Business Law Today.

WONG Stephen Kai-yi; **ZHU** Guobin (eds.) (2016), Personal Data (Privacy) Law in Hong Kong - A Practical Guide to Compliance, City University of Hong Kong Press, Hong Kong.

YÜCEDAĞ Nafiye (2017), "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 75, S. 2, s. 765-789.

YÜKSEL CİVELEK Dilek (2011), Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi), T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı Yayınları, Ankara.