T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ ANABİLİM DALI
AVRUPA ÇALIŞMALARI PROGRAMI
DOKTORA TEZİ

AVRUPA DİJİTAL TEK PAZARINDA KİŞİSEL VERİLERİN KORUNMASI

İpek ÇİMEN BULUT

Danışman

Doç. Dr. İbrahim Alper ARISOY

İZMİR – 2020

TEZ ONAY SAYFASI

YEMİN METNİ

Doktora tezi olarak sunduğum "Avrupa Dijital Tek Pazarında Kişisel Verilerin Korunması" adlı çalışmanın, tarafımdan, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin bibliyografyada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

12.12.2019

İpek ÇİMEN BULUT

ÖZET

Doktora tezi

Avrupa Dijital Tek Pazarında Kişisel Verilerini Korunması

İpek ÇİMEN BULUT

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Avrupa Birliği Anabilim Dalı

Avrupa Çalışmaları Programı

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler ve artan internet kullanımının sonucu, dijital teknolojiler, hayatımızın ekonomik, sosyal, kültürel ve siyasi alanlarına erişerek, bunları değiştirip, adeta yeniden düzenlemiştir. İnsan hayatının çeşitli alanlarında gerçekleşen bu geridönülemez nitelikteki gelişmeler neticesinde, bankacılık işlemlerinden, sağlık hizmetlerine, sosyal medya kullanımından, ticaret işlemlerine kadar pek çok işlem, dijital ağlar üzerinden kolaylıkla yapılabilir hale gelmiştir. Özellikle e-ticaret alanında gerçekleşen gelişmeler, dijital pazarların dünya ekonomisindeki payını gün geçtikçe artırmaktadır. Ancak ortaya çıkan küresel çaplı dijital pazarlar ve diğer her türlü çevirimiçi işlem, insanların hayatlarını kolaylaştırarak, zaman ve paradan tasarruf edilebilmesi gibi yararlar sağlarken, aynı zamanda da veri güvenliğine ilişkin bir takım tehditleri de beraberinde getirmiştir. Nitekim, çok çeşitlenerek yaygınlaşan dijital işlemler sırasında kayıt altına alınan kişisel verilerin sayı ve çeşitliliği ile veri hareketliliğinin artması, bu verilere üçüncü kişiler tarafından erişilerek, verilerin farklı amaçlarla çeşitli şekillerde işlenebilme kapasitelerini de artırmıştır. Bu durum, veri süjesinin, temel hak ve özgürlükler bağlamında korunan kişisel verileri üzerindeki kontrolünü zorlaştırarak, bir takım temel hak ihlalleri ve dolayısıyla da maddi-manevi kayıplara sebep olabilmektedir. Bu olumsuzluklara rağmen, Avrupa Birliği'nin dijital dünyadan, özellikle de ortaya çıkan dijital ekonomiden alabileceği payı bir kenara bırakamayacağı açıktır. Zira dijital dünyada var olamayan devlet, kurum ve kuruluşların gelecekte ekonomik varlıklarını parlak bir şekilde

devam ettirebilmeleri olası gözükmemektedir. Tüm bunların bilinciyle, kişisel verilerin daha iyi nasıl korunması gerektiği hususu, 2000'li yıllardan itibaren Avrupa Birliği'nin gündeminden neredeyse hiç düşmemiştir.

Avrupa Birliği, hem Birlik'in manevi köklerinin dayandığı temel hak ve özgürlükleri gelişen teknolojiler karşısında güncel ve Birlik genelinde uyumlu yasalar kapsamında koruyabilmek, hem de Avrupa dijital tek pazarının oluşumunu tamamlayarak, her geçen gün gelişerek toplam ticaret içindeki payını artıran dijital ekonomiden hak ettiği payı alıp, küresel rakipleri karşısında rekabet avantajını yitirmemek amacı ile kişisel verilerin korunmasına ilişkin çeşitli yasal düzenlemeler yapmaktadır. 2018 yılında yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü de bu yolda atılmış önemli bir adımdır. Bu çalışmada, dijital devrim sonucu ortaya çıkan yeni dünya düzeninde kişisel verilerin korunmasının önemi ve bu bağlamda yapılan yasal düzenlemelerin Avrupa dijital tek pazarının oluşumuna katkıları incelenmeye çalışılacaktır.

Anahtar Kelimeler: Kişisel verilerin korunması, Avrupa Birliği Genel Veri Koruma Tüzüğü, pandemi, Lizbon Stratejisi, Avrupa 2020 Stratejisi, dijital ekonomi, Dijital Gündem, dijital pazar, Avrupa dijital tek pazarı, küreselleşme.

ABSTRACT

Doctoral Thesis

Protection of Personal Data in European Digital Single Market

İpek ÇİMEN BULUT

Dokuz Eylül University

Graduate School of Social Sciences

Department of European Union

European Studies Doctoral Programme

As a result of developments in information and communication technologies and the increasing use of internet, digital technologies have reached, changed and rearrenged our economic, social, cultural and political areas of our lives. Because of these irreversible developments that occured in various areas of human life, many transaction, such as banking to health services, social media usage, commercial transactions, have become possible through digital networks. Developments especially in e-commerce increase the share of digital markets in the world economy day after day. However, emerging global digital markets and all kind of online transactions have benefits like easing people's lives by saving time and Money, but also have brought treats to the data security. Thus, the increase in the number and diversity of personal data and data mobility recorded during the digital transactions, also increased the capacity of these data to be accessed and processed by third parties in different ways and purposes. This could make it difficult for the data subject to control its personal data that protected in the context of fundamental Rights and freedoms, and as a result might cause Fundamental Rights violations as well as material and moral losses. Despite these adversities, European Union could not set aside the share that it could get from the digital world, especially from the emerging digital economy. The governments, institutions and organizations that could not exists in the digital World, would also not be able to survive economically in the future. By the conscious of these,

the idea of better protection of personal data has not fallen from the European Union's agenda since the 2000's.

With the aim of protecting the Fundamental Rights and freedoms, which the moral roots of the European Union are based on, against the developing technologies, within the current and harmonized Union laws; and also with the aim of gaining the share that it deserves from the digital economy, which increases its own share in total trade day by day; and maintaining its competitive advantage over its competitors; and completing the establishment of the European digital single market, European Union makes various legal arrangements regarding personal data protection. The European Union General Data Protection Regulation that came into force in 2018, is an important step forward in this direction. The importance of the personal data protection in the new world order that results from the digital revolution and the contribution of the legal arrangements regarding data protection to the establishment of the European digital single market would be examined in this study.

Keywords: Personal data protection, European Union General Data Protection Regulation, pandemic, Lisbon Strategy, Europe 2020 Strategy, digital economy, Digital Agenda, digital market, European digital single market, globalization.

AVRUPA DİJİTAL TEK PAZARINDA KİŞİSEL VERİLERİN KORUNMASI

İÇİNDEKİLER

İKİNCİ BÖLÜM
AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

ÜÇÜNCÜ BÖLÜM
AVRUPA DİJİTAL TEK PAZARININ GELİŞİMİNDE GENEL VERİ KORUMA TÜZÜĞÜNÜN ROLÜ

KISALTMALAR

ABAD	Avrupa Birliği Adalet Divanı
ABD	(USA) Amerika Birleşik Devletleri
ABTHŞ	Avrupa Birliği Temel Haklar Şartı
AİHS	Avrupa İnsan Hakları Sözleşmesi
Ar-Ge	Araştırma-geliştirme
AÜHFD	Ankara Üniversitesi Hukuk Fakültesi Dergisi
BİT	Bilgi ve İletişim Teknolojileri
Bkz.	Bakınız
BVerfG	(Bundesverfassungsgericht) Federal Alman Anayasa Mahkemesi
CCPA	(California Consumer Privacy Act) Kaliforniya Tüketici Mahremiyeti Kanunu
CNIL	(Commission Nationale Informatique & Libertes) Fransız Veri Koruma Makamı
Cod.	Code
COM	European Commission
ENISA	(The European Union Agency for Network and Information Security) Avrupa Ağ ve Bilgi Güvenliği Ajansı
EC	(European Council) Konsey
ECHR	(European Court of Human Rights) Avrupa İnsan Hakları Mahkemesi
ECJ	(European Court of Justice) Avrupa Adalet Divanı
Ed.	Edited
EFTA	Avrupa Serbest Ticaret Birliği
EU	(European Union) Avrupa Birliği
Eurojust	European Judicial Cooperation Unit
Europol	(European Police Office) Avrupa Polis Teşkilatı
GDPR	General Data Protection Regulation
GL	Guidelines
GSYH	Gayri Safi Yurtiçi Hasıla

HRW	Human Rights Watch
ICO	Information Commissioner's Office, UK
İİBF	İktisadi İdari Bilimler Fakültesi
İKV	İktisadi Kalkınma Vakfı
IP	İnternet Protokol Adresi
JCMS	Journal of Common Market Studies
KDV	(VAT) Katma değer vergisi
LSE	London School of Economics
No	Numara
NYU	New York University
OAPEC	Petrol İhraç Eden Arap Ülkeleri Teşkilatı
OECD	Ekonomik Kalkınma ve İşbirliği Örgütü
OLAF	**(**European Anti-Fraud Office) Avrupa Yolsuzlukla Mücadele Ofisi
Parag.	Paragraf
S.	Sayfa
SBF	Sosyal Bilimler Fakültesi
SSRN	Social Science Research Network
TBB İHAUM	Türkiye Barolar Birliği İnsan Hakları Araştırma ve Uygulama Merkezi
T.C.	Türkiye Cumhuriyeti
TILT	Tilburg Institute of Law, Technology and Society
Trh.	Tarihi
UK	United Kingdom
v.	Versus
v.b.	ve benzeri

TABLOLAR LİSTESİ

GİRİŞ

Bilgi ve iletişim teknolojilerinde yaşanan devrim niteliğindeki gelişmeler ve internet kullanımındaki önlenemez artış, ticaretten, siyasi ve sosyal hayata kadar tüm yaşam alanlarını dijitalleştirerek dönüştürmüştür. Ekonomik hayat da bu değişimden payını doğal olarak aldığından, bilgi ve iletişim teknolojileri temelli bir ekonomi sistemi olan "*dijital ekonomi*" küresel pazarlarda kendine hatırı sayılır bir yer edinerek, genel ekonomi sistemi içerisindeki payını her geçen gün biraz daha artırmış ve artırmaya da devam etmektedir. Büyüyen dijital ekonomi pastasından payını almak isteyen küresel aktörler de davranış biçimlerini, alışkanlıklarını, pazarlama tekniklerini değiştirerek, dijitalleşen dünyada değişen tüketici profili ve tüketim alışkanlıklarını anlayarak, yeni ekonomiye uyum sağlamaya çalışmaktadırlar.

Yeni dijital dünya düzeninde, değişen tüketici profil ve eğilimleri ile dijital ekonominin küresel ekonominin geri kalanından daha hızlı büyüdüğü gerçeği de göz önüne alındığında, Avrupa Birliği'nin bu sistemin dışında kalması düşünülemez. Bu sebeplerle, Birlik, geliştirdiği çeşitli stratejiler ve bu bağlamda yaptığı ve yapacağı yasal ve teknik alt yapı çalışmaları vasıtasıyla, uzun vadede Avrupa Birliği'nin hızla dijitalleşen yeni dünya düzeni içindeki öncü rolünü, güvenilirliğini, pazar payını ve rekabet gücünü artırarak, küresel kural koyucu olma niteliğini yeniden ve eskisinden daha güçlü bir şekilde geri kazanabilmeyi hedeflenmektedir. Bu hedeflere ulaşılabilmesi için Birlik'in ortaya koyduğu en önemli stratejilerden biri de "*Avrupa Dijital Tek Pazar Stratejisi*"dir.

Avrupa Dijital Tek Pazar Stratejisi doğrultusunda Birlik genelinde yapılacak uyumlaştırılmış yasal ve teknik düzenlemeler ile, herkesin, kişisel verilerin korunmasının sağlandığı güvenli bir ortamda bilgiye, teknolojiye, hızlı ve ucuz internete erişimlerinin sağlanarak, yekpare bir "*Avrupa Dijital Tek Pazarı*"nın oluşturulması amaçlanmaktadır. Ancak yapılan tüm çalışmalara rağmen üye devletlerin bir türlü tam olarak uyumlaştırılamayan ulusal yasal düzenleme ve uygulamaları sebebiyle tamamlanmaya çalışılan Avrupa dijital tek pazarının, parçalı görünümünden bir türlü kurtulamadığı görülmektedir. Bu parçalı görünüm, Avrupa Birliği'nin, iç ve dış pazara hitap etmek üzere oluşturmaya çalıştığı dijital tek pazardan beklediği verimi almasını engellemekte ve Birlik'in özellikle ekonomi

alanında öncü olma konusundaki hedefleri açısından da önemli bir tehdit oluşturmaktadır.

Parçalı pazar yapısından kurtulabilmek amacıyla, Birlik'in atacağı en önemli adımlardan biri, Birlik genelinde yasaların uyumlaştırılarak, hukuki anlamda yeknesaklığın sağlanmasıdır. Bu yasal uyumlaştırma çalışmalarının yardımıyla, aynı zamanda da Avrupa dijital tek pazarındaki uygulama ve işlemlerde hukuki öngörülebilirliğin gerçekleştirilerek, güvenilirliğin tesisi, hedeflenmektedir.

Tam da bu noktada kişisel verilerin korunmasının önemi ortaya çıkmaktadır. Zira bilgi ve iletişim teknolojilerindeki gelişmeler ve artan veri akışı sebebiyle, dijital ortamda, ileri teknoloji ürünü bilişim ağ ve işletim sistemleri, özellikle de bulut teknolojiler vasıtasıyla, kişisel veriler, her geçen gün daha fazla artan şekil ve oranlarda toplanıp, depolanarak çeşitli şekillerde işlenmektedirler. Diğer bir ifade ile, son dönemde kimlik bilgilerinden, banka ve kredi kartı bilgileri gibi ekonomik verilere, parmak izinden, retina izine kadar çeşitlenebilen kişisel verilerin, kontrolü çok zor olan internet ortamında pek çok iz bırakmaları ve depolanmaları, bu verilerin bireylerin kontrolleri dışına taşınarak işlenebilmeleri sonucunu ortaya koyabilmektedir. Ayrıca kişisel verilerin özel sektörde olduğu gibi kamusal alanda da dijital ortamda toplanarak, depolanmaları ve çeşitli şekillerde işlenerek kullanılmaları sebebiyle ortaya çıkabilecek, olası tehdit ve ihlallerin artması, kişisel verilerin korunması adına Birlik hukuku kapsamında yapılacak yeni düzenleme ve reformlara duyulan ihtiyacı perçinlemiştir. Böyle yoğun veri akışının bulunduğu bir ortamda, kişisel verilerin birbiriyle Birlik düzeyinde uyumlu yasalarla korunması, Avrupa dijital tek pazarında işlem yapan birey ve şirketler açısından, hukuki öngörülebilirliği artıracağı gibi, güven ortamının oluşturulmasını da kolaylaştırmaktadır. Oluşturulmaya çalışılan bu güven ortamı ise, dijital ekonomi kapsamında işlem hacmini artırmasının yanı sıra, işlemlerin sürdürülebilirliğinin sağlanmasına da katkıda bulunacaktır. Sonuç olarak Birlik, yapmış olduğu kişisel verilerin korunması reformu vasıtasıyla, hem Avrupa dijital tek pazarını parçalı görünümünden kurtararak, dijital ekonomi alanında atılım yapıp, küresel bir aktör olarak dijital alandaki rekabet edebilirliğini güçlendirerek sürdürülebilir kılmayı; hem de internet ve bilişim teknolojileri sebebiyle kişisel verilerin kamu ve özel sektör tarafından kontrolsüz ve yasa dışı kullanılması sonucu, Avrupa Birliği'nin

temel taşlarından biri olan temel hak ve özgürlüklerin ihlal edilmesinin önüne geçmeyi amaçlamaktadır. Aynı zamanda Avrupa Birliği, kuruluşundan itibaren sahip olduğu Avrupalılık kimliğinin kökenlerinde yattığını iddia ettiği, temel hak ve özgürlüklerin korunmasına dair etik değerlerinin de, kişisel verilerin korunması ve üçüncü ülkelere aktarılmaları hususlarında yapmış ve yapacak olduğu yasal düzenlemeler vasıtasıyla, Birlik dışındaki ülkeler için de bir referans noktası oluşturarak, bu üçüncü ülkelerdeki yasal düzenlemeleri olumlu etkilemeyi hedeflemektedir. Böylece Avrupa Birliği, kişisel verilerin korunmasında uluslararası standart ve yasaların oluşturularak benimsenmesinde, kural ihraç eder hale gelerek, öncü role de sahip olmayı amaçlamaktadır.

Bu tez çalışmasında, öncelikle Avrupa Dijital Tek Pazar Stratejisi'nin geliştirilmesine hangi sebeplerle ihtiyaç duyulduğu ile bu stratejinin ulaşmaya çalıştığı temel hedeflerin neler olduğu incelenecektir. Ayrıca Birlik hukuku kapsamında kişisel verilerin korunmasının temelleri, önemi ve boyutları ile birlikte, bugüne kadar Birlik hukukunda kişisel verilerin korunmasına ilişkin olarak yapılan yasal düzenlemelerin neler olduğu ortaya konulmaya çalışılacaktır.

Tez çalışmasının ilerleyen bölümlerinde ise Avrupa Dijital Tek Pazar Stratejisi ile ortaya konan hedeflerin gerçekleştirilmesi sürecinde, kişisel verilerin korunmasının hangi açılardan önemli olduğu sorusuna da yanıt verilmeye çalışılarak, bu süreçte "*Kişisel Verilerin Korunması Reformu*"nun bel kemiğini oluşturarak, 25 Mayıs 2018'den itibaren tüm Avrupa Birliği genelinde doğrudan uygulanmaya başlanan "*Avrupa Birliği Genel Veri Koruma Tüzüğü*"'ne neden ihtiyaç duyulduğu; Tüzüğün getirdiği önemli değişiklikler detaylı olarak incelenecektir.

Genel Veri Koruma Tüzüğü'nün getirdiği bu değişikliklerin, kişisel verilerin korunarak, Birlik içi ve dışı güvenli dolaşımlarının teminiyle, Avrupa Birliği'nin yapı taşlarından biri olan temel hak ve özgürlüklerin korunmasına ve özellikle de Avrupa dijital tek pazarının gelişimine ve dolayısıyla da Birlik'in dijital ekonomiden faydalanma oranına yapabileceği olası katkıların neler olacağı aktarılmaya çalışılacaktır. Ayrıca Avrupa Birliği'nin kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bağlamında yapmış olduğu yasal düzenlemelerin, Birlik'in bu konularda küresel anlamda kural ihraç ederek öncü olma hedefinin gerçekleştirilmesine katkısı bulunup bulunmadığı ortaya konmaya gayret edilecektir.

Tüm bu incelemeler yapılırken, Avrupa Birliği'nin Kurucu Antlaşmaları, Temel Haklar Şartı da dahil Birlik hukukunun birincil kaynaklarından; ilgili tüzükler, direktifler ile Birlik kurumlarının ortaya koyduğu çeşitli strateji, tavsiye, görüş ve kararlar gibi Birlik hukukunun ikincil kaynaklarından; Avrupa Birliği Adalet Divanı ve Avrupa İnsan Hakları Mahkemesi kararları gibi emsal belgeler ile bilimsel makalelerden yararlanılacaktır. Sonuç olarak da kişisel verilerin korunarak, Avrupa dijital tek pazarının kamu, tüketiciler ve şirketler açısından daha güvenilir olmasına yönelik olarak yapılan bu düzenlemelerin yeterli olup olmadığı ile gelecekte bu konuda başka neler yapılabileceği tartışılarak, bu konulara ilişkin çeşitli çözüm önerileri getirilmeye çalışılacaktır.

BİRİNCİ BÖLÜM
DİJİTALLEŞME VE AVRUPA DİJİTAL TEK PAZARI

Tez çalışmasının Birinci Bölüm'ünde öncelikle küreselleşme hareketlerinin dijitalleşmesi sürecine kısaca değinildikten sonra, Avrupa Birliği'nin dijital küreselleşmeye uyum süreci ve bu süreçte ortaya koyduğu çeşitli belge ve stratejiler incelenmeye çalışılacaktır. Birinci Bölüm'ün sonunda ise, bu süreç içerisinde kişisel verilerin korunmasının neden önemli olduğu çeşitli boyutlar altında irdelenecektir.

1.1. KÜRESELLEŞMENİN DİJİTALLEŞMESİ SÜRECİ

Küreselleşme yeni bir kavram değildir. Gerek bireysel, gerekse de kurumsal anlamda küresel çaplı karşılıklı etkileşim on yıllardır devam etmektedir. Küreselleşme sürecinin henüz başında, ulus devletlerin ve bu süreç içerisinde ortaya çıkan çok uluslu şirketlerin, küreselleşme akımından kaynaklanan ekonomik fırsatlardan yararlanmak istemeleri neticesinde seçtikleri daha liberal ticaret politikaları sayesinde, dünya ticareti ve finans piyasaları, her geçen gün biraz daha serbestleşmiştir. Yaşanan serbestleşme neticesinde de sermaye ve özellikle ölçek ekonomisine dayanan doğrudan yatırımlar, küresel anlamda yer değiştirmiştir. Bu yer değiştirmelerle birlikte iyiden iyiye liberalleşen ticaret politikaları, uluslararası karşılıklı ticari bağları artırmış, ticari bariyerleri yıkıp sınırları aşarak, uluslarüstü nitelik kazanan çok uluslu şirketler ve örgütlerin dünya piyasalarında daha fazla söz sahibi olmalarına yol açmıştır[1]. Nitekim seksenli yıllardan sonra iyiden iyiye etkilerini göstermeye başlayan ve dünya çapında bir dizi karmaşık süreçten oluşan modern dönem küreselleşme hareketleri[2], ekonomik, sosyal ve siyasal anlamda dünya üzerindeki devlet ve toplulukları karşılıklı etkileştirip, bütünleştirerek birbirine hem bağımlı, hem de benzer hale getirmiştir. Diğer bir ifade ile, küreselleşme hareketleri, yaşanan teknik gelişmeler sebebiyle azalan ulaşım ve

[1] Martin Khor, **Rethinking Globalization: Critical Issues and Policy Choices**, Zed Books, UK, 2001, ss.1-2, 7-8.

[2] Richard E. Baldwin, Philippe Martin, "Two Waves of Globalization: Superficial Similarities, Fundamental Differences", **Working Paper: 6904**, 1999, http://www.nber.org/papers/w6904.pdf , ss. (02.06.2020)*, ss. 5-17

*İşbu tez çalışmasındaki internet kaynakları, 02.06.2020 itibarı ile tekrar kontrol edilerek, erişilebilirlik tarihleri güncellenmiştir.

iletişim süre ve maliyetleri sonucunda, ülke sınırlarının belirsizleşip mesafelerin kısalması nedeniyle, dünya ülkeleri arasında gittikçe artan sosyal, kültürel ve ekonomik ilişkiler oluşmasına yol açmıştır. Bu da rekabeti, mal, hizmet ve sermayenin küresel dolaşım hızını artırmıştır. Ancak bu hızlı ve önlenemez artış, aynı zamanda ülkeler ve bölgeler arası eşitsizlikleri de tetiklemiştir. Tetiklenen bu eşitsizlikler, zengin ve fakir arasındaki aralığın açılmasına, çeşitli çevre problemlerinin ortaya çıkmasına, yerel kültürlerin benzeşerek çoğunlukla Batı kökenli olan homojen ve global nitelikli bir kültüre evrilmelerine, dolayısı ile kültürel çeşitliliğin azalmasına ve kimi ülke ve bölgelerin hızla zenginleşmesine karşılık, bazılarınınsa yoksullaşmalarına yol açmıştır[3]. Bu bağlamdaki klasik küreselleşmenin gerçekleşmesinde rol oynayan temel unsurlar, mal ticareti ve sermaye hareketleri iken; içinde bulunduğumuz yeni dönemde, bilgi, iletişim ve ulaşım teknolojilerinde gerçekleşen devrim niteliğindeki ilerlemeler, küreselleşmenin temellerini bilgi ve iletişim teknolojileri alanındaki gelişmelere odaklayarak, küreselleşme sürecini dijitalleştirmiştir. Bu dijitalleşme ve yaygınlaşan internet uygulamalarının etkisi ile tüm sektörler çevirim içi ağ üzerinden çalışabilir hale gelmiştir. Bu da sınır ötesi veri ve bilgi akışını artırmıştır. Böylelikle, bilgi ve iletişim teknolojileri temelli sistemlerdeki önlenemez ilerlemenin ortaya koyduğu veri ve veri ekonomisi kavramları da dijital küreselleşme kavramının kapsamına dahil olmuşlardır[4].

Ürün ve hizmetlerin dijitalleştiği, pazar ve kurumların ağ sistemleri içerisinde de işleyen elektronik sistemler haline geldiği günümüzde yaşanan onca bilgi ve teknoloji yoğun gelişmeye rağmen, dijital küreselleşme bağlamında henüz yolun başında olunduğunu söylemek yanlış olmayacaktır. Zira küreselleşme canlı bir evrim sürecidir. Dijital değişim robotik, yapay zeka, internet uygulamaları, 3D baskı ve

[3] David Dollar, "Globalization, Poverty and Inequality since 1980", **World Bank Policy Research Working Paper 3333**, 2004, https://openknowledge.worldbank.org/bitstream/handle/10986/14128/wps3333.pdf?sequence=1 (02.06.2020), ss.1-6;
Frederick P. Stutz, Barney Warf, "Economic Geography: An Introduction", **The World Economy Geography, Business, Development**, (Ed. Stutz & Warf), 6.Baskı, Pearson New International Edition, UK, 2014 s.24;
Deniz Ülke Arıboğan, **Globalleşme Senaryosunun Aktörleri-Uluslararası İlişkilerde Güç Mücadelesi**, 2. Baskı, Der Yayınları, İstanbul, 1997, ss.13-16.

[4] European Commission, "Reflection Paper on Harnessing Globalisation", **COM (2017) 240**, 10.05.2017, https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1544609950797&uri=CELEX:52017DC0240 (02.06.2020), ss.6-9; Don Tapscott, **Dijital Ekonomi, Ağ Üzerindeki Akıl Çağında Umut ve Tehlike**, 1.Baskı, Koç Sistem Yayınları, İstanbul, 1998, ss.5-8.

otomasyon, yenilenebilir enerji ve benzeri alanlarda devam eden bilgi birikimi, veri akışı ve teknik gelişim, üretim, tüketim, çalışma tercih ve koşullarını etkilemeye devam ederek dijital küreselleşme sürecini hali hazırda değiştirmeye devam etmektedir[5].

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler sonucu ortaya çıkan yoğun dijitalleşme neticesinde artık ticari bir değer olduğu genel kabul gören verilerin, sınır ötesi dolaşımlarını da kapsayarak, hayatın her alanını etkileyip, dönüştüren dijital küreselleşme, kaçınılmaz olarak dünya üzerindeki tüm ülke ve aktörleri etkisi altına almıştır. Etkileri kaçınılmaz olan dijital küreselleşme, birey, devlet ve şirketler açısından pek çok fırsatın yanı sıra ve çeşitli tehditleri de beraberinde getirmiştir[6]. Nitekim dijital küreselleşme kapsamında dünya çapında artan veri akışı, bir yandan bu bağlamda ortaya çıkan veri ekonomisini besleyip, dijital devrimi gerçekleştirerek dijital küreselleşmeye dahil olabilen tüm aktörlerin bu ekonomiden yararlanabilmeleri için kapıyı aralarken, diğer yandan da verilerin çevirim içi ağlar üzerinden sınır ötesi artan dolaşımları neticesinde kişisel verilerin korunmasının zorluğu gibi güvenlik zaafları ve temel hak ihlallerini içerebilen olumsuzlukların baş göstermesine de sebep olabilmektedir.

1.1.1. Avrupa Birliği'nde Küreselleşme Çabaları ve Lizbon Stratejisi

İkinci Dünya Savaşı'ndan sonra ekonomik anlamda yaralarını sararak toparlanmaya başlayan Avrupa Topluluğu'na üye devletler, özellikle seksenli yıllarda, ekonomik ve sosyal alanda atılım yaparak fark edilebilir bir büyüme oranı yakalamışlardır. Yaşanan ekonomik büyümeye bağlı olarak da Avrupa'da refah seviyesi artmış ve işsizlik de oldukça düşük seviyelere gerilemiştir. Petrol tüketicisi durumunda bulunan Avrupa Ekonomik Topluluğu'na üye devletler, bu yükselme döneminde, ekonomik anlamdaki ilk tökezlemeyi, 1973 Petrol Krizi ile

[5] European Commission, "Reflection Paper on Harnessing Globalisation", ss.10-11; Don Tapscott, ss.10.

[6] David Held, Anthony McGrew, David Goldblatt, Jonathan Perraton, "Global Transformations: Politics, Economics and Culture", **Politics at the Edge**, (Ed. Chris Pierson, Simon Tormey), Political Studies Association Yearbook Series, Palgrave Macmillan, London, 2000, ss. 14-15;
Wade Jacoby, Sophie Meunier, "Europe and the Management of Globalization: Responding to Globalization Pressures", **Working Paper**, https://www.researchgate.net/publication/2-42547663_Europe_and_the_Management_of_Globalization (02.06.2020), ss.1-4.

yaşamışlardır. Zira Arap-İsrail Savaşlarının devamında gerçekleşen 1973 yılındaki çatışmadan sonra, petrol üreten Arap ülkelerinin, siyasi amaçlarla[7], petrol arzını kısarak, petrolün varil fiyatını yükseltmeleri sonucu, küresel çapta bir Petrol Krizi tetiklenmiştir. Bu kriz küreselleşmenin de etkisiyle, tüm dünyaya olduğu gibi Avrupa Topluluğu'na üye devletlere de olumsuz olarak yansımıştır.

Serbest ticaret ilkesinin hemen hemen tüm dünyada benimsenmesiyle, malların, hizmetlerin, işgücünün ve sermayenin küresel çapta hareketliliğinin artarak, dünya ekonomilerinin her geçen gün birbirleri ile daha fazla bütünleşmesi olarak tanımlanabilen küreselleşmenin [8] etkilerinin, kuvvetli bir şekilde hissedilmeye başlandığı seksenli ve doksanlı yıllara gelindiğinde ise, Avrupa Topluluğu'nun, tek pazarda serbest dolaşımı, "*mallar*" açısından büyük oranda gerçekleştirebildiği görülmüştür. Buna karşın hizmet sektörü ve işgücü piyasası bakımlarından serbest dolaşımın önündeki dolaylı dolaysız pek çok engelin kaldırılamadığı, yasal düzenlemeler bakımından da tam bir uyumun yakalanamadığı anlaşılmaktadır. Bu da gerek üye devletler arasında, gerekse de küresel çapta gerçekleşen ticaret bakımından tek pazarda parçalı bir yapıya neden olmuş ve Topluluk açısından, tek pazardan beklenen verimin alınamamasına yol açmıştır[9]. Birlik, ayrıca küreselleşmenin ivme kazandığı bu yıllarda, özellikle emek yoğun üretim yapan Çin, Hindistan ve Güney Kore gibi yükselen ekonomileri olduğu kadar, teknoloji alanındaki eski rakipleri olan ABD ve Japonya'yı da yakalamakta güçlük çekmiş, bu ülkelerle rekabet

[7] Petrol İhraç Eden Arap Ülkeleri Teşkilatı (OAPEC) olarak bir araya gelen Arap ülkeleri, İsrail'in kuruluşuyla başlayan uyuşmazlıklar ve Arap-İsrail Savaşları olarak anılan çatışmalar sırasında, İsrail'e destek veren ve kendilerinden petrol satın alan başta Amerika Birleşik Devletleri olmak üzere, diğer batılı ülkelere karşı -siyasi saiklerle- petrol arzını kısıp fiyatları yükselterek, 1973 yılında küresel bir petrol krizinin doğmasını tetiklemişlerdir. Bu dönemde özellikle petrol tüketicisi konumunda bulunan Avrupa Ekonomik Topluluğu ülkelerinin artan ihtiyaçlarının karşılanması ve dolayısı ile de enerji güvenliği, kısıtlı arz sebebi ile tehlikeye düşmüş, küresel piyasalardaki fiyat istikrarı da bozulmuştur. Petrol fiyatlarında yaşanan bu yükselme, istikrarsızlığa ve güven ortamının bozulmasına, üretimde azalmaya, neticede ise enflasyonun ve işsizliğin artmasına sebebiyet vermiştir. Daha fazla bilgi için bkz. Sefer Yılmaz, Duhan K. Kalkan, "Enerji Güvenliği Kavramı: 1973 Petrol Krizi Işığında Bir Tartışma", **Uluslararası Kriz ve Siyaset Araştırmaları Dergisi**, Cilt.1 Sayı.3, 2017, ss. 181-187.

[8] Council of Europe, "Realising Both Economic Growth and Social Protection in Europe in an Era of Globalisation", **Resolution 1573**, 2007, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17580&lang=en , (02.06.2020).

[9] Communication from the Commission to the European Parliament and Council, "The Impact and Effectiveness of the Single Market", **COM(96) 520**, 1996, http://ec.europa.eu/internal_market/economic-reports/docs/single_en.pdf , (02.06.2020), ss.4-6.

edebilmek için kendisinden beklenen bilgi birikimine dayalı teknolojik atılımları ve yenilikleri yapmakta da gecikmiştir[10].

Küreselleşmenin Topluluk ekonomisine yaptığı yukarıda anılan olumsuz etkilerin yanı sıra, yine seksenli yıllarda Yunanistan, İspanya, Portekiz gibi görece daha zayıf ekonomilere sahip Güney Avrupalı devletler ile 2004 ve 2007 yıllarında, yapısal anlamda zayıf ekonomilere sahip Orta ve Doğu Avrupa ülkelerinin üye kabul edildiği genişleme hareketleri [11] neticesinde de işsizlik ve yoksulluk oranları yükselmiştir. Bu olumsuzluklar, Birlik'in, bilgi ve teknolojiye dayalı sıçramaları yapmasını sağlayacak Ar-Ge çalışmalarına yeterli yatırım yapamayarak, bu dönemde küresel yarıştaki yerini korumakta zorlanmasına yol açmıştır. Böyle bir ortamda Mart 2000'de ortaya konulan Lizbon Stratejisi ile, 2010'a kadar Avrupa Birliği'nin rekabet edebilirlik ve sosyal kapsayıcılık boyutlarıyla perçinlenen, ekonomik ve sosyal reformları gerçekleştirip, temelleri araştırma-geliştirmeye, yeniliğe ve dijitalleşmeye dayanan "*dünyanın en rekabetçi ve dinamik bilgi temelli ekonomisi*" haline gelerek, sürdürülebilir ekonomik büyümenin, tam istihdamın, sosyal uyum ve refahın sağlanması hedeflenmiş idi[12]. Bu hedeflerin içerisinde büyüme hedefinin tutturulması, Avrupa Birliği bölgeselleşme modelinin sürdürülebilirliğinin sağlanabilmesi, diğer bir ifade ile, Birlik'in dünya üzerinde küreselleşme ile meydana gelen değişimlere ayak uydurarak, ekonomi, bilim ve teknoloji alanlarında üstünlüğünü koruyabilmesi ve rekabet gücünü artırabilmesi bakımlarından hayati bir öneme sahipti. Lizbon Stratejisi'nin uygulanmaya çalışıldığı bu dönemde Birlik, ekonomik anlamdaki ikinci darbeyi, 2008'de Amerika Birleşik Devletleri'nde başlayarak, daha sonra tüm dünyayı saran ve küreselleşme süreci neticesinde birbirine bağımlı haline gelen piyasalar nedeniyle, Avrupa Birliği'ni de etkisi altına alan ekonomik krizden kaynaklı olarak almıştır. Nitekim ABD'de başlayarak

[10] Baldwin ve Martin, s. 17;
Selen Akses, "Avrupa 2020 Stratejisi", **İktisadi Kalkınma Vakfı (İKV) Yayın No.269**, 2014, https://www.ikv.org.tr/images/files/2020stratejisi.pdf , (02.06.2020), ss.19-36;
Sema Gençay Çapanoğlu, "Geçmişten Günümüze Lizbon Stratejisi ve 2020 için Yeni Bir Vizyon Işığında "AB 2020" Stratejisi", **İKV Değerlendirme Notu**, 2010, https://www.ikv.org.tr/images/upload/data/files/gecmisten_gunumuze_lizbon_stratejisi_ve_2020_icin_yeni_bir_vizyon_isiginda_ab_2020_stratejisi.pdf (02.06.2020), ss.1, 2.

[11] 1981'de Yunanistan, 1986'da İspanya ve Portekiz, 2004'te Macaristan, Polonya, Çekya, Slovakya, Slovenya, Letonya, Litvanya, Estonya, Malta, Güney Kıbrıs Rum Yönetimi, 2007'de Bulgaristan ve Romanya.

[12]European Parliament, "Lisbon European Council 23 and 24 March 2000 Precidency Conclusions", **Summits**, 2000, http://www.europarl.europa.eu/summits/lis1_en.htm , (02.06.2020).

2010'da tüm Avro bölgesini etkisi altına alan ve "*Avro Krizi*[13]" olarak da adlandırılan ekonomik kriz, küreselleşme neticesinde, global çapta ekonomi ve finans piyasalarının karşılıklı olarak birbirlerine ne kadar entegre, bağlı ve kırılgan hale geldiğini göstermesi bakımlarından önemlidir. Neticede 2010 yılına gelindiğinde, Lizbon Stratejisi'nin başarısız olduğu teyid edilmiştir. Strateji'nin başarısız olmasının pek çok nedeni bulunmakla birlikte, bunların en önemlileri; Strateji hazırlanırken üye devletler arasındaki ekonomik, sosyal ve yapısal farklılıkların göz önüne alınmaması; üye devletlerin Stratejiyi yeterince sahiplenmemesi ve aralarında koordinasyon eksikliklerinin olması; belirlenen hedeflerin fazlalığı ve bu hedeflere ulaşılabilmesi için gerekli yapısal reformların yapılamaması; bilgi ve iletişim teknolojilerine yatırım yapılmasına rağmen bu yatırımların Birlik'in geneline yaygınlaştırılamaması; mevzuat alanındaki uyumlaştırma faaliyetlerinin yeterli olmaması şeklinde özetlenebilir. Bu gibi eksiklikler nedeniyle, Birlik, parçalı görünümünden kurtulmuş uyumlu yapıda bir tek pazar oluşturma hedefine ulaşamadığı gibi, bilgi ve iletişim teknolojilerindeki ilerleme sonucu ortaya çıkan veri ekonomisinden beklenen payı da alamamıştır. 2000-2010 yılları arasında ortaya koyduğu büyüme oranının yetersizliği bile tek başına, Birlik'in Lizbon Stratejisi'yle hedeflediği özellikle bilgi ve iletişim teknolojilerine ve yeniliğe dayalı durmadan büyüyen bir ekonomi haline dönüşüm amacının gerçekleşmediğinin kanıtı niteliğindedir. Avrupa Birliği'nde büyüme hedefinin sürdürülebilirliğinin, bugün bile, bilgi birikimi, dijitalleşme ve teknolojik ilerlemede yaşanan aksaklıklar ile birlikte, dijital ekonomiye ve dolayısı ile veri ekonomisine katılımın yetersizliğinin yarattığı olumsuz etkiler sebebiyle, tehdit altında olduğu söylenebilir[14]. Tüm bu olumsuzluklar sebebiyle, Lizbon Stratejisi

[13] Küresel ekonomik bağlar ve iç içe geçmiş finansal piyasalar sebebi ile, ABD'den Avrupa Birliği'ne sirayet ederek, Avro bölgesine ulaşan kriz, öncelikle -yüksek kamu borçları ve işsizlik seviyeleri, bankacılık sistemlerindeki yüksek riskler, etkili olmayan ekonomi politikaları gibi yapısal nitelikli sorunları olan- Yunanistan, İspanya, İtalya, Portekiz ve İrlanda'da gibi görece daha zayıf üye devlet ekonomilerinde etkili olmuştur. Bu kriz, devletler arasındaki küresel bağların ne derece güçlü olduğunu ortaya koyması bakımından önemlidir. Yaşanan kriz sonrasında, üye devletlerin realitede "*Kopenhag Ekonomi Kriterlerini*" sağlayıp sağlayamadıkları ve üye devletlerin ekonomi politikaları arasındaki koordinasyon eksiklikleri konuları ile bir sonraki muhtemel küresel ekonomik krizi atlatabilmek için ne gibi tedbirler alınacağı, Birlik tarafından yeniden yüksek sesle tartışılmaya başlanmıştır. Daha fazla bilgi için bkz. Matthias Ruffert, "The European Debt Crisis and European Union Law", **Common Market Law Review**, Cilt. 48, Sayı 6, 2011.

[14] Birlik içerisinde büyüme hedeflerinin tutturulamamasının sebepleri arasında, nüfus artış hızının azalması ve dolayısıyla nüfusun yaşlanması gibi demografik değişikliklerin yanı sıra yaşlı nüfus

kapsamında geçen on yıllık dönem, Birlik tarihinde, ekonomik büyüme ve refaha ulaşabilmek için harcanan yetersiz çabaları sembolize eden, boşa harcanan kayıp zaman olarak anılacaktır[15].

1.1.2. Avrupa 2020 Stratejisi

Yenilik yaratma, teknolojik ilerleme ve dijital uyum ekonomik, sosyal kalkınma ve refahın temel taşlarını oluşturmaktadır. Başka bir ifade ile, içinde bulunduğumuz dijitalleşme çağında, küresel rekabette öncü olabilmenin yolu, bilgi ve iletişim teknolojilerine, yeniliğe kaynak ayırmaktan geçmektedir. Bu öngörü ile hazırlanmasına rağmen Lizbon Stratejisi'nin, kimi üye devletlerdeki işsizlik oranlarının görece düşmesi dışında, belirlenen hedeflere ulaşmada ve dijital devrimi gerçekleştirmede yetersiz kaldığı görülmüştür[16]. Zira 2008 yılında başlayan küresel finansal kriz, Birlik içerisindeki ve özellikle de Avro alanındaki yapısal zayıflıkları daha belirgin hale getirmiştir. Bu zayıflıkların yanı sıra üye devletlerin birbirlerinden farklı ekonomik, siyasi, sosyal yapıları, gelenekleri ve farklı yasal-teknik alt yapı ve gelişmişlik düzeyleri sebebiyle, genişleme ile birlikte yürütülen derinleşme hareketleri de Lizbon Strateji'nin başarısız addedilmesinde etkili olmuştur.

Üye devletlerin ulusal mevzuatlarının birbiriyle uyumlu olmaması sebebiyle, Birlik içinde yasal ve idari eş güdümün sağlanamaması, birlikte hareket etme konusunda güçlükler ortaya koymaktaydı. Bunların yanısıra, tarife dışı engellerin tam olarak kaldırılamaması; Ar-Ge yatırımlarının yetersizliği ve üye devletler arasındaki eşitsiz dağılımı sebebiyle de, bilgi ve iletişim teknolojileri alanlarında beklenen atılımlar gerçekleştirilememiş, dijital dönüşüm tamamlanamamış ve tek

---

nedeniyle sosyal güvenlik sistemi üzerinde her geçen gün daha fazla hissedilen bir baskının oluşması da sayılabilir.

İbrahim Hakkı Öztürk, "Dünyanın en dinamik ve en rekabetçi bilgi ekonomisi olmak ya da olamamak: Avrupa Birliği Lizbon Stratejisi ve Eğitim Boyutu", **Ankara Avrupa Çalışmaları Dergisi,** Cilt.7, Sayı.2, 2008, ss.14-17;

Report of an Independent High-Level Study Group Established on the Initiative of the President of the European Commission, "An Agenda for a Growing Europe, Making the EU Economic System Deliver", 2003, https://artnet.unescap.org/tid/artnet/mtg/gmscb_growingeurope.pdf (02.06.2020), ss. i, ii;

Selen Akses, ss.20, 23-32.

[15] Paul Copeland, "Conclusion: The Lisbon Strategy Evaluating Success and Understanding Failure", **The EU's Lisbon Strategy** (Ed. Paul Copeland, Dimitris Papadimitriou), Palgrave Macmillan, London, 2012, ss.235-236.

[16] Sema Gençay Çapanoğlu, ss.1-2.

pazar parçalı görünümünden kurtarılamamıştır. Bu durum, Birlik'in ekonomik ve sosyal gelişiminin önünde önemli bir engel teşkil etmekteydi. Tüm bu olumsuzluklara ek olarak, temelleri bilgi ve iletişim teknolojileri kullanılarak küresel veri akışından ekonomik fayda üretilmesine dayanan ve tüm dünyada yükselen bir değer olan veri ekonomisine tam bir adaptasyon sağlanamayarak, bu ekonomiden beklenen verimin alınamaması da, hızla değişen bir dünyada dijitalleşen küreselleşme süreci sonucunda ortaya çıkan uzun dönemli tehditlerle Birlik genelinde topyekün mücadele edilmesini zorlaştırmıştır. Böyle büyük ve çeşitli sorunlarla yüzleşmek zorunda kalan Avrupa Birliği'nin, krizlerden kaynaklanan güçlükleri avantaja çevirmek ve yeni dijital küreselleşme sürecine topyekün uyumu sağlamak adına daha pro-aktif ve güçlü yaklaşımlar ortaya koyması zorunluluğu doğmuştur. Mart 2010'da, dijitalleşen küresel yarıştaki yerini kaybetmek istemeyen Birlik tarafından, Lizbon Stratejisi'nin başarısız olma sebepleri arasında sayılan üye devletlerin farklı yapıları ve ihtiyaçları da göz önüne alınarak hazırlanan, yeni ve daha güçlendirilmiş bir Strateji olan, "*Avrupa 2020 Stratejisi*" yayınlamıştır. Bu yeni Strateji, her üye devletin kendi yapısal özelliklerine ve ulusal ihtiyaçlarına uygun başlangıçlar yapıp, eksikliklerini gidererek büyümelerini sağlayacak ve bu uğurda her bir üye devletin münhasır yol haritasının hazırlamasına imkan verecek bir ana gündem niteliğindedir.

Üye devletlerin kendilerine has farklılık ve eksikliklerini göz önünde tutarak hazırlanan Avrupa 2020 Stratejisi, yeni dijital dünya düzeninde hem Birlik'in yeni teknolojiler alanındaki eksikliklerini giderebilmek, hem de Avrupa sosyal pazar ekonomisini gerçekleştirebilmek adına, tüm üye devletlere yol gösterici nitelikte olan üç temel öncelik belirlemiştir. Bu öncelikler[17]:

- Bilgiye dayanan ve yenilik odaklı bir ekonomi anlayışı geliştirmeyi hedefleyen, ***Akıllı Büyüme,***
- Kaynakların etkin kullanımını, daha yeşil ve daha rekabetçi bir ekonomik sistem oluşturulmasını teşvik eden, ***Sürdürülebilir Büyüme,***
- Yüksek istihdama ulaşmayı sağlayarak, sosyal ve bölgesel bütünleşmeyi hızlandıracak olan, ***Kapsayıcı Büyüme***'dir.

[17] Communication from the Commission, "Europe 2020, A Strategy for Smart, Sustainable and Inclusive Growth", **COM (2010), 2020 final**, 3.3.2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF (02.06.2020), ss.3-14.

2020 yılında Avrupa Birliği'nin, kendisini nerede görmek istediği de yine bu öncelikler kapsamında tanımlandığından, Komisyon, bu önceliklere ulaşılabilmesi için gerekli ana hedefleri de ayrıca belirlemiştir. Strateji kapsamında, her üye devletin kendi ulusal ihtiyaç ve eksikliklerini yansıtan reel koşulları doğrultusunda hazırlanacak eylem planlarıyla bu hedeflere ulaşılmaya çalışılacaktır. Burada bir parantez açarak, Komisyon tarafından belirlenen hedeflerin, sınırlayıcı değil, örnekleyici olduğunu belirtmekte fayda vardır. Diğer bir ifade ile, Avrupa 2020 Stratejisi'nin temel önceliklerini gerçekleştirmeye yönelik olarak belirlenen hedefler, bu uğurda hareket eden üye devletleri sınırlandırıcı ya da zorlayıcı değil, yol gösterici olarak yorumlanmalıdır. Bu bağlamda her üye devletin kendi ulusal koşullarına uygun olarak üzerine düşeni yapmasıyla bu hedeflere Birlik genelinde ulaşılması beklenmektedir. Avrupa 2020 Stratejisi ile Komisyon tarafından öngörülerek belirlenen ana hedefleri de kısaca inceleyecek olursak[18]:

- "20-64 yaş arası nüfusun %75'inin istihdam edilmesinin,
- Birlik'in GSYİH'nın %3'ünün Ar-Ge harcamalarına ayrılmasının,
- Birlik'in sera gazı salınımının 1990 yılı seviyesinden %20 aşağıya çekilmesi; enerji ihtiyacının %20'sinin yenilenebilir enerji kaynaklarından karşılanması; ve son olarak da enerji verimliliğinin %20 oranında artırılması olarak belirlenen, 20/20/20 iklim ve enerji hedeflerinin tutturulmasının[19],
- Okullaşma oranının artırılarak, okulu erken terk oranının %10'nun altına çekilmesi ve genç nüfusun en az %40'ının yüksek öğrenim görmesinin sağlanmasının,
- Ulusal yoksulluk sınırlarının altında yaşayan Avrupalıların sayısının %25 azaltılarak, yirmi milyon kişinin yoksulluktan kurtarılmasının", hedeflendiği görülmektedir.

Komisyon ayrıca belirlenen öncelikler doğrultusunda koyulan hedeflere ulaşılmasını kolaylaştıracak yedi öncü girişim de belirlemiştir[20]:

[18] Communication from the Commission, Europe 2020, A Strategy for Smart, Sustainable and Inclusive Growth, 2010, ss. 3-9.
[19] European Commission, "Analysis of options beyond 20% GHG emission reductions: Member State Results", **Commission Staff Working Paper,** 1.2.2012, https://ec.europa.eu/clima/sites/clim-a/files/strategies/2020/docs/swd_2012_5_en.pdf (02.06.2020), s.4.
[20] Communication from the Commission, Europe 2020, A Strategy for Smart, Sustainable and Inclusive Growth, 2010, ss.3, 4.

- "Yenilikçi icat ve fikirlerin ticari ürün ve hizmetlere dönüştürülerek, büyümeye ve yeni iş alanları ortaya koymasına katkı yapmasını sağlamak amacıyla, Ar-Ge'ye daha çok kaynak ayıran "*Yenilikçi*" bir Birlik haline dönüşümü destekleyen girişimler,
- Eğitim sistemlerinin performansını yükselterek, gençlerin işgücü piyasasına girişlerini kolaylaştırmayı amaçlayan ve "*Hareket Halindeki Gençlik*" adı altında toplanan girişimler,
- Düşük karbon salınımı oranının yakalanmasını, yenilenebilir enerji kullanımının artırılmasını, enerji kullanımında etkinliğin desteklenmesini ve bu bağlamda Avrupa Birliği içerisindeki ulaşım ve taşımacılık sektörlerinin de yeniden yapılandırılmasını destekleyerek büyümeye katkı sağlayacağı düşünülen girişimler,
- İş hayatında özellikle küçük ve orta ölçekli işletmelerin güçlendirilerek, küresel dünyada rekabet edebilecek güçlü ve sürdürülebilir sanayinin oluşturulması ve sanayi politikalarının da küreselleşme çağına uyum sağlayacak şekilde güncellemesine yönelik girişimler,
- İşgücü piyasasının küresel gelişmelere ayak uyduracak şekilde yenilenip, kişilerin serbest dolaşımı önündeki her türlü engelin kaldırılarak, çalışanların yetkinliklerini ve işgücüne katılım oranlarını artıracak girişimler,
- Büyümenin nimetlerinden ve ortaya çıkan yeni iş olanaklarından yararlanmayı tüm Avrupa vatandaşları için imkanlı hale getirerek sosyal ve bölgesel bütünleşmeyi artırıp, yoksullukla mücadele imkanlarını geliştirmeye yönelik girişimler,
- Hızla dijitalleşen bir dünyada yaşanan gelişmeleri yakalamak ve veri ekonomisinden kendine düşecek payı artırabilmek adına bilim ve teknoloji alanlarına gerekli Ar-Ge yatırımlarını yapıp, teknolojiye, özellikle de bilgi ve iletişim teknolojilerine ve bunlara dayalı yeniliklere kapılarını açıp, yüksek hızlı internete erişimi artırıp, yasal düzenlemeleri uyumlaştırarak, hem kamunun, hem özel sektörün, hem de hane halkının "*Avrupa Dijital Tek Pazarı*"nın nimetlerinden faydalanmasını öngören ve "***Avrupa için Dijital Gündem***" başlığı altında toplanan çeşitli girişimler".

1.2. DİJİTAL GÜNDEM

Avrupa Birliği'ne üye devletlerin ekonomileri ve finansal piyasaları, küreselleşme akımlarının etkisiyle, hem üçüncü ülkelerle, hem de kendi aralarında karşılıklı olarak yüksek oranda bağımlıdırlar. Bu bağımlılık, özellikle ortak para biriminin kullanıldığı Avro alanında oldukça derindir. Ortaya çıkan bu derinlik, Avrupa tek pazarında, ekonomik krizlere ilişkin duyarlılığı ve kırılganlığı artırmaktadır. Anılan sebeplerle, bir üye devlette başlayan ekonomik, finansal ve sosyal krizler, "*yayılma (spill-over)*" etkisi ile kısa sürede tüm Birlik genelinde hissedilebilmektedir. Yayılma etkisi, 2008'de Amerika Birleşik Devletleri (ABD)'nde başlayarak, 2009'da önce Yunanistan'a, 2010'da ise Avro bölgesine ulaşıp derinleşerek, artçı sarsıntılarının uzun süre hissedildiği ekonomik ve mali kriz sırasında da oldukça yoğun hissedilmiştir. Avro krizi, Avrupa bankalarında yoğun likidite sıkıntısına yol açtığı gibi, Birlik ekonomisine ve sosyal hayatına da ağır darbe vurmuştur. Birlik üyelerinin ekonomik ve mali yapılarındaki zayıflıkları da gün yüzüne çıkaran bu kriz, Birlik'in yıllar içinde gerçekleştirmeye çalıştığı ekonomik ve sosyal refaha ulaşma yolunda yapmış olduğu ilerlemeleri de sekteye uğratmıştır[21].

Tüm bu olumsuzlukların yanında, üye devletlerin ekonomilerinin birbirleriyle yüksek oranda entegre olmasının, bazı avantajları da bulunmaktadır. Bu avantajlardan biri de, tüm yapısal eksikliklerine rağmen, içeride ve dışarıda yüksek ticari potansiyeli olan Avrupa tek pazarına sahip olunmasıdır. Avrupa tek pazarı, sadece Birlik içi ticarette dahi, Eurostat verilerine göre, 500 milyondan fazla kişiye[22]

---

[21] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A Digital Agenda for Europe", **COM 245**, 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF (02.06.2020), s.3;
Costas Lapavitsas, A.Kaltenbrunner, D.Lindo, J.Michell, J.P.Painceira, E.Pires, J.Powell, A.Stenfors, N.Teles, "Eurozone Crisis: Beggar Thyself and Thy Neighbour, Research on Money and Finance", **Journal of Balkan and Near Eastern Studies**, Cilt.12, Sayı 4, 2010, ss. 321-324;
Will Bartlett, Ivana Prica, "Interdependence between Core and Peripheries of the European Economy: Secular Stagnation and Growth in the Western Balkans", **LSE "Europe in Question" Discussion Paper Series No. 104**, 2016, http://www.lse.ac.uk/european-institute/Assets/Documents/LEQS-Discussion-Papers/LEQSPaper104.pdf, (02.06.2020), ss.1-12.

[22] Eurostat Statistics, "Demographic Balance", 2018, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Demographic_balance,_2018_(thousands).png, (02.06.2020). İlgili bağlantıdan da anlaşılabileceği gibi, Eurostat verilerine göre, 28 üye devletin 01.Ocak.2019 tarihi itibarı ile toplam nüfusu, 513.481,7 kişiye ulaşmıştır.

ulaşabilme kapasitesi ile dünyanın en büyük yekpare pazarlarından biridir. Bu büyük tek pazar, doğru politikalar uygulanması halinde Avrupa Birliği'ne ticari etkinlik açısından büyük bir rekabet avantajı sağlayabilecek kapasitededir.

Birlik, işte bu tek pazarda dijitalleşmeye uyumun yasal ve teknik anlamda gerçekleştirilmesi sayesinde hızlı bir büyüme oranı yakalamayı amaçlamaktadır. Dijital ekonomiye uyumun sağlanmasının akabinde Birlik, dijital küreselleşme yarışında liderliği de ele geçirerek, akıllı büyümenin yanısıra, Avrupalılık değerlerini ve serbest pazar ekonomisi sistemini üçüncü ülkelere empoze ederek, Avrupa sosyal modelini yaygınlaştırmayı da hedeflemektedir[23]. Büyüme potansiyeli yüksek olan tek pazarı, dijitalleştirip uyumlaştırarak bu pazarı küresel anlamda bir rekabet avantajına dönüştürüp, yaşanan ekonomik krizlerin etkilerini azaltmak amacıyla, Avrupa Birliği bugüne kadar pek çok yasal düzenleme ve stratejiye imza atmıştır. Ancak 21. yüzyıla şekil veren dijital devrim sebebiyle, Birlik'in hedeflerini sürdürülebilir bir şekilde gerçekleştirebilmesinin, temelleri bilgi ve iletişim teknolojilerine dayanan "*akıllı büyüme*"nin kilit noktalarının yakalanmasına bağlı olduğu söylenebilir. Akıllı büyümenin anahtarı ise, dijital teknolojilere yapılacak yatırımlarla yenilik üretmede ve bunlara paralel olarak beşeri sermayeye aktarılacak eğitim destekleriyle bireylerin hem teknoloji üretme, hem de yasal ve sistemsel güvenliği sağlanmış dijital ortamda bu teknolojileri kullanma kapasitelerinin artırılmasında yatmaktadır. Bu konulara yapılacak yatırımlar sonucunda, bilim ve teknoloji alanında halihazırda lider olan diğer ülkelerle, Birlik arasındaki makasın kapatılıp, sıçramalar yapılarak bu alanlarda öne geçilmesi hedeflenmektedir. "*Dijital Gündem*", dönüşüm sürecinde bulunan küresel yarışta Birlik'in, dijital teknolojilere yönelik teknik ve yasal alt yapı düzenlemelerini tamamlayıp, veri ekonomisinden, kendine düşen payı alarak, ekonomik ve sosyal manada, akıllı, kapsayıcı ve sürdürülebilir büyümede öncü hale gelmesini hedefleyen en önemli öncü girişimlerden biridir[24]. Dijital gündem kapsamında yapılacak uyumlaştırma çalışmaları ile, yasal, teknik ve operasyonel

[23] Sophie Meunier, "Managing Globalization? The EU In International Trade Negotiations", **Journal of Common Market Studies (JCMS)**, Cilt 45, Sayı. 4, 2007, ss. 914-915;
DigitalEurope, "A Transformational Agenda For The Digital Age: Digital Europe's Vision 2020", **WhitePaper,** 2009, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=157&language=enUS&PortalId=0&TabId=353 (02.06.2020) ss. 5-7.

[24] European Commission, A Digital Agenda for Europe, **COM 245**, 2010, ss.3-4, 34;
Phil Cooke, Lisa De Propris, "A Policy Agenda for EU Smarth Growth: The Role of Creative and Cultural Industries", **Policy Studies Journal**, Cilt.32, Sayı.4, 2011, s.372.

yeknesaklığı sağlanan Avrupa dijital tek pazarında bölünmüş yapıya son verilerek, temelleri, sınır ötesi hızlı internet bağlantıları ile standartlara tabi ve uyumlu bir şekilde birlikte çalışabilirliği sağlanmış ağlara dayanan veri ekonomisinden, beklenen sürdürülebilir ekonomik ve sosyal kazanımların elde edilmesi amaçlanmaktadır. Zira, verilerin, malların, hizmetlerin, pazarların, tüketicilerin ve hatta sosyal hayatın dijital bir nitelik kazanarak çevirim içi ağlar üzerinden sınır ötesi hareket, erişim ve işlem kabiliyeti kazandığı 21. yüzyılda ortaya çıkan ve kökeni bilgi ve iletişim teknolojilerine dayanan yeni küresel dijital ekonomik sistem[25], Barroso[26]'nun da çeşitli seferlerde belirttiği gibi; tüm dünya için olduğu gibi Avrupa Birliği için de bir dönüm noktasıdır. Dönüştürücü bir nitelik taşıyan dijital gündem, oldukça zorlu olan bu virajı alıp, dijitalleşmeye entegre olarak Birlik ilkeleri doğrultusunda küresel arenada kural koyucu olabilmek adına Birlik için önemlidir[27].

Küresel dijital süreç ve veri ekonomisi de dahil yeni nesil ekonomi sistemleri, bilgi birikimi ile yüksek teknolojinin ortaya koyduğu dijitalleşmeye dayanan ve verimliliğin artırılmasına büyük katkı sağlayan Bilgi ve İletişim Teknolojilerini (BİT) temel alarak gelişimlerini sürdürmekte ve geleceği şekillendirmektedir. Bu bağlamda bilgi ve veri paylaşımını; bunların yenilik yaratmada kullanılmasını ve bu alanlardaki birikimlerin sanayiye aktarılıp, katma değerli yenilikçi ürünler yaratılarak; sanayinin üretkenliğinin ve rekabet edebilirliğinin artırılmasını hedefleyen veri ekonomisinden beklenen payı alabilmesi için Avrupa Birliği'nin, dijital gündemi sıkı sıkıya takip etmesi gerekmektedir[28]. Dijital gündemin bu şekilde uygulanmasıyla, Birlik, yeni dijital teknolojilerin geliştirilmesini ve bunların dönüştürücü gücünün yeni pazarlara açılma, ekonomik büyüme ve sosyal gelişim

[25] Don Tapscott, ss.10, 23-24.
[26] José Manuel Barroso, Portekizli siyasetçi, 2004-2014 Avrupa Komisyonu Başkanı.
[27] European Commission, "European Commission President Jose Manuel Barrosso Proposes a Partnership for Progress and Ambition to the European Parliament", **Press Release Data Base, IP/09/1272**, 2009, http://europa.eu/rapid/press-release_IP-09-1272_en.htm (02.06.2020);
Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Proccessing of Personal Data and on Free Movement of Such Data (General Data Protection Regulation), **11 Final, 2012/0011 (COD),** 25.01.2012, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52012PC0011 , 27/04.2016 tarihinde yürürlükten kalkmıştır (02.06.2020) ss. 1-2.
[28] World Economic Forum, "The Europe 2020 Competitiveness Report, Building a More Competitive Europe", 2014, http://www3.weforum.org/docs/WEF_Europe2020_CompetitivenessReport_2014.pdf (02.06.2020) s. 9.

için kullanılmasını da sağlayabilecektir[29]. Nitekim BİT'lere kaynak ayırıp bu alana yatırım yaparak elde edilen bilgiyi, teknolojileri ve yenilikleri, tüm üretim süreçlerine entegre ederek, BİT'lerin dönüştürücü gücünden yararlanmayı başarabilen pro-aktif şirketlere sahip ülkelerin verimliliklerinin, bunu başaramayan ülkelere kıyasla daha yüksek olduğu da görülmektedir. Dijital küreselleşme düzeninde yüksek verimliliğin ve rekabet edebilirliğin yakalanabilmesi için tüm Birlik kurumları, gerçek ve tüzel kişiler ile üye devlet hükümetleri tarafından BİT'lerin benimsenerek, her alanda uygulanması gerekmektedir. Bu bağlamda bir örnek vermek gerekirse, Avrupa Birliği ve ABD arasındaki işgücü verimliliği farkının Avrupa Birliği aleyhine çok yüksek olması, Avrupa Birliği'nde BİT alanına yapılan yatırımların ve BİT kullanımının ABD'ye kıyasla düşük olmasıyla açıklanabilmektedir[30].

Özetlemek gerekirse, dijital gündem kapsamında dijitalleşen küresel ekonomiye entegrasyonun sağlanabilmesi için, BİT'lere gerekli yatırımların yapılarak, her türlü ticari bariyerden arındırılmış ve uyumlaştırılmış yasalar çerçevesinde işleyen engelsiz ve yekpare bir Avrupa dijital tek pazarının oluşturulması gereklidir. Dijital tek pazarın tamamlanabilmesi için de Birlik'in her yerinde yüksek hızlı ve güvenli internete erişim imkanlarının artırılarak, Birlik içindeki dijital bölünmüşlüğün önlenmesi; Birlik'in tamamındaki sanayi ve ticaret ile insan kaynaklarının, dijital teknoloji ve buna ilişkin ömür boyu eğitim uygulamaları ile güçlendirilerek, dijital entegrasyon ve okur-yazarlığın artırılması gereklidir. Yaşanan bu yoğun dijitalleşme ortamında, tüm bunların yanı sıra, insan onurunun, temel hak ve özgürlüklerin, hukukun üstünlüğünün, demokrasinin korunması temelinde özellikle vurgulanması gereken bir diğer husus da, gittikçe artan oranlarda dijital ortama aktarılan kişisel verilerin korunmasının önemlidir. Kişisel verilerin, uyumlu Birlik yasaları ile korunması, çevirim içi işlemlere olan güveni artıracağından, dijital işlem hacminin de yükselmesine sebep olacaktır. Zira kişisel

[29] Digital Europe, "A Transformational Agenda For The Digital Age: Digital Europe's Vision 2020", **White Paper**, ss.5, 6, 7;
Don Tapscott, ss. 40-46.
[30] World Economic Forum, "The Europe 2020 Competitiveness Report, Building a More Competitive Europe", 2014, s.9;
European Policy Center, "The Economic Impact of a European Digital Single Market, Final Report", **Copenhagen Economics,** 2010, https://www.copenhageneconomics.com-/dyn/resources/Publication-/publicationPDF/5/305/1435823773/study_by_copenhagen.pdf (02.06.2020) ss.16-18.

verilerin yeknesak uygulamalar ve uyumlu yasal mevzuat kapsamında korunamaması, Birlik genelinde, kullanıcılar tarafından dijital teknolojiye dayanan çevirimiçi sistemlerin benimsenerek kullanılması oranını düşürmekte ve dolayısı ile de Birlik'in dijital ekonomiden beklediği kazanımları elde etmesi sürecini baltalamaktadır[31].

1.3. AVRUPA DİJİTAL TEK PAZARI

Avrupa Birliği, 1980'li yıllardan itibaren başta Jacques Delors[32] olmak üzere Birlik teknokratlarının özellikle 1985 yılında hazırlanan "*İç Pazarın Tamamlanmasına ilişkin Beyaz Belge (White Paper: Completing the Internal Market)*[33]" ve hemen akabinde yayınlanan "*Tek Avrupa Senedi (The Single European Act)*[34] *"* gibi çeşitli belge ve çalışmalar kapsamında ortaya koyduğu "*tek pazar*" idealini gerçekleştirebilmek için yoğun çaba harcamıştır[35]. Aynı doğrultuda Dijital Gündem ile, teknoloji temelli yenilik çalışmaları teşvik edilerek bilgi ve iletişim teknolojilerinde atılım yapılması ve gerek bireylerin, gerekse de şirketlerin hızlı, erişimi kolay ve güvenli internet hizmetlerine ulaşmalarının kolaylaştırılması neticesinde oluşturulacak, "*Avrupa Dijital Tek Pazarı*" ile de, ekonomide dijital bir patlama yaratılması hedeflenmiştir. Birlik için "*Dijital Tek Pazar*", kişilerin, malların, hizmetlerin, sermayenin, verilerin serbest dolaşımı ile adil ve serbest rekabet koşullarının sağlandığı, uyumlu yasalarla regüle edilerek, tüketici hakları ile kişisel verilerin korunması da dahil temel hak ve özgürlüklerin garanti altına alındığı

---

[31] Digital Europe, "A Transformational Agenda For The Digital Age: Digital Europe's Vision", 2020, ss.5-7, 14, 72, 73; European Commission, A Digital Agenda for Europe, **COM 245**, 2010, ss. 3-8; European Commission, "The European Union Explained Digital Agenda for Europe", 2014, https://eige.europa.eu/resources/digital_agenda_en.pdf , (02.06.2020) s.3;
Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Proccessing of Personal Data and on Free Movement of Such Data (General Data Protection Regulation), **11 Final, 2012/0011 (COD)**, 25.01.2012, ss. 1-2.

[32] Jacques Delors, 1985-1995 yılları arasında Avrupa Komisyonu Başkanlığını yürüten Fransız siyasetçi.

[33] European Commission, "Completing the Internal Market", **White Paper,** Milan, 28-29.06.1985, https://op.europa.eu/en/publication-detail//publication/4ff490f3dbb64331a2eaa3ca59f974a8/language-en (02.06.2020).

[34] Single European Act, **Official Journal L 169**, 29.6.1987, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:11986U/TXT (02.06.2020), ss. 1-28,

[35] Nicolas Jabko, **Playing the Market: A Political Strategy for Uniting Europe, 1985-2005**, 1.Edition, Cornell University Press, Ithaca, London, 2006, ss.14-16;
Sophie Meunier (JCMS), s.910.

yekpare bir pazarı ifade etmektedir. Bu yolda yapılacak yasal ve teknik düzenlemeler sayesinde, Avrupa dijital tek pazarında, uyruklarına ve ikamet yerlerine bakılmaksızın Birlik içindeki tüm birey, kurum ve kuruluşların çevirim içi işlem ve faaliyetlerini sorunsuz bir şekilde gerçekleştirebilmeleri amaçlanmaktadır. Komisyon, ortaya koyduğu pek çok çalışmada, "*Avrupa dijital tek pazarı*"nın gerçekleştirilmesinde, sözleşmesel haklar, tüketici güvenliği, fikri mülkiyet ve telif hakların korunması ile bireylerin veri güvenliğine ilişkin yaşadıkları sıkıntı ve ön yargıların giderilmesinin öneminin altını çizmiştir. Kişisel verilerin ve işlem güvenliğinin Birlik içinde uyumlu yasalarla, en üst düzeyde sağlandığı bir ortamda, birey ve şirketlerin, dijital teknolojileri kullanma ve dijital sistem üzerinden işlem yapmaya ikna edilebilmelerinin kolaylaşacağına şüphe yoktur. Bu sebeplerle, BİT'ler konusundaki yatırımların artırılarak, uyumlaştırılmış yasal düzenlemeler kapsamında alınacak tedbirlerle, dijital tek pazarda işlem ve veri güvenliğinin sağlanıp, pazarın fiziksel olmayan bölünmüşlüğünün ve tarife dışı ticaret engellerinin ortadan kaldırarak pazarın birlikte işlerliğinin gerçekleştirilmesinin, hem Avrupa dijital tek pazarının parçalı yapısının ortadan kaldırılmasının, hem de sürdürülebilir, akıllı ve kapsayıcı büyümenin ve sosyal refahın anahtarı niteliğinde olduğu söylenebilir [36]. Bu noktada kişisel verilerin haiz oldukları nitelikleri gereği korunmalarının dijital tek pazarın tamamlanması ve işlem hacminin artırılması açısından özel önem arz ettiğinin altını bir kere daha çizmek gerekmektedir. Zira dijital ekonomi kapsamında kolaylıkla, güven içinde ve makul fiyatlarla faaliyet gösteren tüm gerçek kişilerin kişisel verilerinin birbiri ile uyumlu yasalar kapsamında korunduğu, tam entegre olmayı başarmış güvenilir bir Avrupa dijital tek

[36] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A Digital Single Market Strategy for Europe", (**COM 192) Final**, 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, (02.06.2020) s. 3;
European Parliament, "The Ubiquitous Digital Single Market, Fact Sheet on the European Union", 2018, http://www.europarl.europa.eu/ftu/pdf/en/FTU_2.1.7.pdf , (02.06.2020), ss.1-2;
H.Banu Yılmaz, "Lizbon Sonrası AB 2020 Stratejisi", **TOBB, Ekonomik Forum**, 2010, https://www.tobb.org.tr/AvrupaBirligiDairesi/Dokumanlar/Raporlar/AB%202020%20Stratejisi.pdf (02.06.2020), s.35;
European Commission, "Digital Agenda for Europe, Rebooting Europe's Economy", **EU Publications**, 2014, https://op.europa.eu/en/publication-detail/-/publication/27a0545e-03bf-425f-8b09-7cef6f0870af (02.06.2020), s.3;
Max Heermann, Political Contestation in the Digital Single Market: Exploring Party Politics in the EU's Digital Policy, (Yayınlanmamış Yüksek Lisans Tezi) **Utrecht Faculty of Law, Economics and Governance Theses**, 2016, https://dspace.library.uu.nl/handle/1874/344610 (02.06.2020) s.9.

pazarının, Birlik ekonomisine yılda tahmini 415 milyar Avro katkı ve Avrupa vatandaşlarına yeni iş imkanları sağlayabileceği öngörülmektedir. Bu katkıların da, Avrupa için büyüme ve refahı beraberinde getireceğine şüphe yoktur[37].

1.3.1. Avrupa Dijital Tek Pazar Stratejisi

Birlik, önceki bölümlerde bahsedilen hedeflerine ulaşabilmek için, yaptığı ve yapacağı yasal ve teknik alt yapı uyumlaştırma çalışmaları ve bu çalışmalar kapsamında oluşturacağı denetim ve yaptırım mekanizmaları ile öncelikle Avrupa dijital tek pazarını parçalı yapısından kurtarmaya çalışmaktadır. Parçalı yapısından kurtularak bireyler ve teşebbüsler için güvenli, öngörülebilir, istikrarlı ve adil bir rekabet ortamının sağlandığı, müşteri memnuniyetinin tesis edildiği bir dijital tek pazarda işlem hacminin artacağından ise şüphe yoktur[38]. Birlik, "*Avrupa 2020 Stratejisi*[39]"nin ortaya koyduğu hedeflere ulaşılıp ulaşılmadığını irdelemek ve hedeflerin gerçekleştirilmesinin hızlandırılabilmesi için güncel bir yol haritası belirlemek amacıyla, Mayıs 2015'de, bir ara dönem değerlendirme çıktısı olarak da nitelendirilebilen "*Avrupa için Dijital Tek Pazar Stratejisi*[40]"ni ortaya koymuştur. Birlik'in temel önceliklerinden birisi olarak açıklanan bu Strateji, toplamda on altı inisiyatifi kapsayan "*üç sütun*" üzerine tesis edilmiştir[41]. Avrupa dijital tek pazarının tamamlanabilmesi amacıyla 2015 öncesi ve sonrasında yapılan yasal ve teknik alt yapı çalışmaları, bu Stratejide belirtildiği şekilde, "*üç sütun*" çerçevesinde aşağıda açıklanmaya çalışılmıştır.

---

[37] European Commission, "The EU and The Digital Single Market", **EU Publications**, 2017, http://publications.europa.eu/webpub/com/factsheets/digital/en/ (02.06.2020).
[38] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.3-5, 9,12-13.
[39] European Commission, "Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth", **Com (2010) 2020 Final,** 3.3.2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF (02.06.2020).
[40] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, 2015.
[41] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss. 3-4, 6; European Commission, "A Digital Single Market for Europe: Commission Sets Out 16 Initiatives to Make it Happen", **Press Release**, 6.5.2015, http://europa.eu/rapid/press-release_IP-15-4919_en.htm, (02.06.2020), s.1.

1.3.1.1. Sütun I: Çevirimiçi İşlem ve Uygulamalara Daha İyi Erişim

"*Avrupa için Dijital Tek Pazar Stratejisi*"nin dayandığı sütunlardan ilki, Birlik içerisindeki tüm gerçek ve tüzel kişilere, çevirimiçi işlem ve uygulamalara daha iyi erişim imkanlarının sunulmasıdır. Birlik'in her yerinden daha iyi erişim sağlanması hedefini gerçekleştirebilmek adına, bugüne kadar yapılmış çalışmalardan bir kısmına bu bölümde kısaca değinilmeye çalışılacaktır.

2005 yılında kabul edilen ve halen yürürlükte bulunan, tüketiciye yönelen haksız ticari uygulamaların önlenmesine ilişkin "*2005/29 sayılı Direktif*[42]", Birlik genelinde, tüketicinin mümkün olan en iyi şekilde korunarak, tek pazara olan güveninin artırılmasının sağlanması hususunda atılmış önemli bir adımdır. Avrupa Birliği Hukuku kapsamında "*Direktif*[43]" şeklinde yapılan işbu düzenleme, doğrudan dijital tek pazara ilişkin olmasa da, özellikle aldatıcı, adil olmayan ve agresif nitelik taşıyan ticari uygulamalar ile yanıltıcı reklamların önlenmesi[44] ve mesafeli satışlar[45] gibi konularda getirdiği hükümlerle, tüketici güveninin güçlendirilmesinde oynadığı roller açısından oluşturulmaya çalışılan dijital tek pazar bakımından da önemlidir[46]. Ticari uygulamaların Birlik çapında uyumlaştırılması çalışmaları çerçevesinde kabul edilen bu Direktif'in kapsamındaki, "*Azami Koruma Prensibi*" ile haksız işlemler karşısında tüketici menfaatlerinin en üst düzeyde korunması gerekliliğine odaklanılmıştır. Özellikle 2004 genişlemesinden sonra Birlik'e dahil olan eski demir perde ülkelerindeki düşük koruma seviyelerini yükseltebilmek amacıyla kabul edilen 2005/29 sayılı işbu Direktif, tüketicilerin haksız ticari uygulamalara ve yanıltıcı reklamlara karşı, azami seviyede korunabilmelerini sağlamak adına çeşitli hükümler

[42] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No.2006/2004 of the European Parliament and of the Council ("Unfair Commercial Practices"), **Official Journal, L 149**, 11.6.2005, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1540545283496&uri=CELEX:32005L0029 (02.06.2020).

[43] Avrupa Birliği Hukukunun ikincil nitelikteki kaynaklarından biri olan ve Türkiye Cumhuriyeti Avrupa Birliği Genel Sekreterliği'nin yayınlamış olduğu "*Avrupa Birliği Terimler Sözlüğü*" kapsamında, Türkçe'ye "*Direktif veya Yönerge*" olarak tercüme edilebileceği belirtilen "*Directive*" terimi, işbu tez çalışması kapsamında, "*Direktif*" olarak kullanılmıştır. Türkiye Cumhuriyeti, Avrupa Birliği Genel Sekreterliği, **Avrupa Birliği Terimler Sözlüğü**, Ankara, 2009, https://www.ab.gov.tr/files/Sozluk/glossary_for_the_european_union.pdf (02.06.2020).

[44] Direktif 2005/29/EC parag. (6,14), madde5, 6, 8, 14.

[45] Direktif 2005/29/EC, madde 15.

[46] Direktif 2005/29/EC parag. (1,3,10).

içerir. Bu hükümlerin, doğrudan üye devletlerin kendi ulusal yasalarına aktarılması suretiyle, bu alanda tek tip kural ve yasaklar getirilmeye çalışılarak, güçlü bir uyumlaştırma yapılması amaçlanmıştır. Böylelikle tek pazarda ticaretin güven içinde gerçekleştirilmesi ve tüketicinin ekonomik yararının korunması hususlarının pekiştirilmesi hedeflenmiştir. Bu düzenlemenin, tüketici hak ve menfaatlerinin korunması bağlamında, Avrupa dijital tek pazarının güçlendirilmesine de önemli katkılarda bulunduğuna şüphe yoktur[47].

Üye devlet sınırlarını aşan bir bütünleşmeyi simgeleyen dijital tek pazarın geliştirilmesine ilişkin yapılan önemli düzenlemelerden biri de "*2000/31 sayılı Elektronik Ticaret Direktifi (E-Ticaret Direktifi)*[48]"dir. Bu Direktif ile, elektronik ticaret konusunda üye devlet mevzuatları arasındaki farklılıkların, bilgi toplumu hizmetlerinin serbest dolaşımına ve tek pazarın işleyişine zarar verdiğinin altı çizilerek, yasaların uyumlaştırılmasının gerekliliği bir kez daha vurgulanmıştır. Ayrıca bu Direktif kapsamında, elektronik ticaretin ana hatlarına ilişkin çerçeve niteliğindeki kural ve ilkeler de belirlenmiştir. Hazırlanan bu çerçeve aracılığıyla da üye devletler arasındaki yasal farklılıkların ortadan kaldırılarak, bu farklılıkların uygulamaya olumsuz yansımalarının engellemesi ile bilgi ve iletişim toplumu hizmetlerinin üye devletler arasındaki serbest dolaşımlarının sağlanması hedeflenmiştir. Ayrıca, 2000/31 sayılı E-Ticaret Direktifi ile, elektronik ticaret işlemleri kapsamında kişisel verilerin korunmasının ve verilerin serbest dolaşımlarının sağlanmasının önemi de vurgulanmıştır[49]. 2000/31 sayılı işbu Direktif ile kişisel verilerin korunması hususundaki 95/46 sayılı Direktif'in Birlik genelinde mümkün olduğunca uyumlaştırılmış yasalar kapsamında uygulanmasının sağlanması ile, Birlik'in dijital küreselleşme sürecinde elektronik ticaretten en yüksek seviyede yararlanarak ekonomik büyümeye ilişkin atılım yapabileceği de öngörülmüştür.

Avrupa için Dijital Tek Pazar Stratejisi ile, çevirim içi işlem ve uygulamalara daha iyi erişimin sağlanmasına yönelik teknik alt yapı düzenlemeleri ile sözleşme

---

[47] Mehmet Ali Aksoy, "2005/29/AT Haksız Ticari Uygulamalar Direktifinde Düzenlenen Haksız Rekabet Halleri ve Uygulama Örnekleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXXIII, Sayı: 1, 2015, ss.280-282.

[48] 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"), **Official Journal**, **L 178**, 17.7.2000, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1540545333940&uri=CELEX:32000L0031 (02.06.2020).

[49] Direktif 2000/31/EC, Beyanlar (3,5,7,8,14,40), madde 1,4.

hukuku, tüketicilerin koruması, garanti kapsam ve süreleri, gümrük uygulamaları, katma değer vergisi (KDV) dahil vergilendirmeye ilişkin hükümler, fikri mülkiyet ve telif hakları, etiketleme, paketleme gibi standartlar ile kişisel verilerin korunması gibi yasal düzenlemelerin, tüketici güvenini artırarak, çevirim içi işlem hacmini yükseltecek şekilde uyumlaştırılmasının önemi sıkça vurgulanmıştır. Uyumlaştırma faaliyetleri ile, üye devlet ve bölgeler arasındaki her türlü farklılık ve ayrımcılığın sona erdirilip, tarife dışı ticaret engelleri de kaldırılarak, sınırlar arası çevirim içi mal ve hizmetlerin serbest dolaşımlarının aksamadan sağlanması ve neticede de gerçek ve tüzel kişilere daha iyi erişim imkanları sunularak, dijital tek pazardan faydalanma oranlarının artırılması hedeflenmektedir. Bunlara ek olarak, çevirim içi satın almalar ve hizmetlerden yararlanma konusunda, Birlik içerisindeki tüketicilere ulusal sınırlara dayalı olarak farklı fiyat ve koşulların dayatılması anlamına gelen ve "*coğrafi engelleme*[50]" olarak adlandırılan tarife dışı ticaret engeli niteliğindeki tedarik kısıtlamalarının kaldırılması da dijital tek pazarın gelişimi açısından önemlidir. Böylelikle, hem müşteriler arasında ayrımcı uygulamalar yapılmasının, hem de serbest ve adil rekabet ortamının bozularak, şirketlerin pazar paylaşımı ve dikey anlaşmalar yolu ile rekabet kurallarını aşmalarının önüne de geçilebilecektir. Coğrafi engellemelerin kaldırılması, parçalı görünümünden kurtulması yönünde Avrupa dijital tek pazarına, olumlu etkide bulunacaktır.

E-ticaret işlemlerinin, olmazsa olmaz tamamlayıcı unsurlarından biri olan ve tüm üye devletleri kapsayarak birlikte çalışabilirliğe izin verir nitelikteki, makul fiyat

[50] Birlik içerisinde, vatandaşlığa, ikamet yerine ya da şirketin tek pazar kapsamındaki kuruluş yerine ilişkin olarak yapılan haksız coğrafi engellemeler yoluyla, dijital tek pazarda işlem yapan tüketicilerin, merkezi başka bir üye devlette bulunan web sitelerinde bulunan bir ürüne ve/veya hizmete erişmelerini, bunları satın almalarını engelleyen veyahut tüketicileri otomatik olarak yerel web sitesine yönlendiren haksız ticari uygulamalar "*coğrafi engelleme*" olarak adlandırılmaktadır. Bu gibi haksız ticari uygulamalarla ilgili Tüzük şeklinde yeni bir düzenleme kabul edilerek, 02.03.2018 tarihinde, 2018/302 sayı ile resmi gazetede yayınlanmıştır. Buna ilişkin detaylı bilgiye aşağıdaki linkten ulaşılabilir. Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (Text with EEA relevance), **Official Journal L 60I**, 2.3.2018, ss.1-15, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2018.060.01.0001.01.ENG&toc=OJ:L:2018:060I:TOC(02.06.2020), (02.06.2020)Council of the EU, "Geo-blocking: Council adopts regulation to remove barriers to e-commerce", **Press Release 95/18,** 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/02/27/geo-blocking-council-adopts-regulation-to-remove-barriers-to-e-commerce/pdf (02.06.2020)Agapi Patsa, Aliki Benmayor, "Competition and Antitrust in the Digital Age", **Baker McKenzie**, 20.07.2017, https://www.bakermckenzie.com//media/files/insight/publications/2017/10/ar_antitrust_digitalage_oct17.pdf?la=en (02.06.2020), s.3.

ve süreli, şeffaflık prensibi doğrultusunda işleyen kaliteli koli (paket) taşıma hizmetlerinin tüketicilere sunulması[51] da tüketici güveninin tesis edilerek, çevirimiçi mal ve hizmet hareketliliğinin artırılıp, dijital tek pazarın desteklemesi bakımından önemlidir.

E-ticarete ilişkin işlemlerde üye devletler arasında ticaret bariyeri oluşturabilen, birbirlerinden farklı KDV oranları gibi uyumlu olmayan vergi uygulamalarının azaltılmasına ilişkin olarak işbu Strateji kapsamında yapılacak çalışmalar da dijital tek pazarın yekpare bir görünüm kazanarak gelişmesi bakımından önemlidir[52].

İçinde bulunduğumuz dijitalleşme çağında yoğun internet kullanımı ve buna bağlı olarak bilgisayar, cep telefonu, tablet gibi mobil iletişim cihazları, oyun konsülleri, veri bankaları, sosyal medya platformları gibi araçlar, "*klasik medya*"nın anlamını değişen koşullarla yoğurup, dönüştürerek, "*dijital medya*" kavramını ortaya koymuştur. Dijital medya, kişisel veriler de dahil, çok miktarda veri ve eserin, çevirim içi yollarla, hızlı bir şekilde bir yerden bir yere aktarılmasıyla, bu veri ve eserlere zaman ve mekandan bağımsız olarak pek çok kullanıcı tarafından aynı anda ulaşılabilmesini mümkün kılmıştır. Bu hızlı dijital aktarım, veri ve eserlerin ulaşabilecekleri sınırları genişletmekte, buna paralel olarak da hak sahiplerinin bunlar üzerindeki kontrol imkanlarını zayıflatmaktadır. Bir başka ifade ile, entelektüel birikimlerin eşsiz çıktıları olan bilimsel ve edebi eserler, güzel sanat eserleri, müzik, müzikal, tiyatro ve sinema yapıtları, fotoğraflar, bilgisayar program ve oyunları, markalar, patentler, endüstriyel tasarımlar ve benzeri her türlü fikir ürününün dijital medya aracılığıyla, sınırlar ötesi dolaşıma girerek yayılabilmesi, eser sahiplerinin eserleri üzerindeki kontrollerini azaltmaktadır. Eserleri üzerindeki mülkiyetlerinin korunması bu bağlamda zorlaşan, eser sahiplerinin uğrayabilecekleri

[51] Birlik içinde sınırlar arası koli (paket) taşıma hizmetlerinin düzenlenmesine ilişkin olarak 2016 yılında sunulan teklif üzerine, Aralık 2017 tarihinde bu düzenlemeye ilişkin olarak bir anlaşmaya varılmıştır. Ancak varılan anlaşma üzerine hazırlanan düzenleme metni henüz olaylanmamıştır. Bu metine onaylanmamış haliyle aşağıdaki linkten ulaşılabilir. Proposal for a Regulation of the European Parliament and of the Council on cross border parcel delivery services, 2016/0149 (COD), **Pre-Cons 69/17**, http://data.consilium.europa.eu/doc/document/PE-69-2017-INIT/en/pdf (02.06.2020).

[52] Birlik genelinde tek KDV sistemi uygulamasını hayata geçirebilmek adına Komisyon, 2016 yılında bir eylem planı ortaya koymuştur. İlgili eylem planına aşağıdaki linkten ulaşılabilir. European Commission, "Communication on an Action Plan on VAT Towards a Single EU VAT Area-Time to Decide", **148 final,** 7.4.2016, https://ec.europa.eu/taxation_customs/sites/taxation/files/com_2016_148_en.pdf, (02.06.2020).

maddi-manevi zararların engellenmesi adına, uluslarüstü yasal düzenlemeler yapılması dijital çağda artık bir zorunluluk haline gelmiştir[53].

Dijital medyanın çevirimiçi mecrada sınırları ortadan kaldırması, veri ve eserlere üçüncü kişilerin erişimini de kolaylaştırmıştır. Tüm bu sebeplerle ortaya çıkan olumsuzluklar ve özellikle de kişisel verilerin korunması kapsamındaki hak ihlalleri ile mücadelede üye devletlerin farklı yasal düzenlemelere sahip olmalarından kaynaklanan, farklı uygulama ve yaptırımlar, büyük belirsizlikler yaratmaktadır. Bu belirsizliklerin engellenmesi ise, ancak Birlik genelinde uyumlaştırılacak fikri mülkiyet ve telif hakları ile kişisel verilerin korunmasına ilişkin yasal düzenlemeler ile mümkün olabilecektir. Dolayısı ile, dijital yaratıcılığın ön plana çıkarılarak, görsel-işitsel medya alanındaki çalışmaların[54] artarak devam etmesine ve eserlere daha güvenli bir çevirim içi-sınır ötesi erişimin sağlanmasına yönelik olarak yapılacak çalışmalar da dijital tek pazarın gelişimi için bu Strateji kapsamında belirlenen öncelikli konulardandır[55]. Bu doğrultuda, Birlik içinde özellikle eğitim, araştırma ve kültürel mirasın korunması hususlarında yeni düzenlemeler içeren ve telif haklarının korunmasına ilişkin çağın ihtiyaçlarına cevap verebileceği düşünülen bir "*Dijital Tek Pazarda Telif Hakları Direktifi*[56]" tasarısı hazırlamıştır. Ancak bu taslak henüz yasalaşmamıştır[57].

---

[53] Burak Medin, "Dijitalleşen Dünyada Fikri Haklar Sorunu", **Kırıkkale Üniversitesi Sosyal Bilimler Dergisi**, Cilt 7, Sayı 2, 2017, ss. 54-57.

[54] Telif hakları konusunda Komisyon tarafından 2015 yılında bir iletişim metni yayınlanmıştır. Bu metne aşağıdaki linkten ulaşılabilir. European Commission, "Communication Towards a Modern, More European Copyright Framework", **626 final**, 9.12.2015, https://ec.europa.eu/digital-single-market/en/policies/copyright , (02.06.2020).

[55] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, s. 3-8; European Commission, "A Comprehensive Approach to Stimulating Cross-border E-Commerce for Europe's Citizens and Businesses", **320 Final**, 25.5.2016, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-320-EN-F1-1.PDF ss.2-12;
European Commission, "Communication on the Mid-Term Review on the Implementation of the Digital Single Market Strategy, A Connected Digital Single Market for All", **228 final**, 10.5.2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0228 (02.06.2020), ss. 4, 6-7,11;
Paul-Jasper Dittrich, "Balancing Ambition and Pragmatism for the Digital Dingle Market", **Berlin Jacques Delors Institut Policy Paper 204**, 7.9.2017, https://institutdelors.eu/wp-content/uploads/2018/01/balancingambitionandpragmatismforthedigitalsinglemarket-dittrich-jdib-sept2017.pdf (02.06.2020), ss.4-5.

[56] European Council, "Proposal for a Directive of the European Parliament and the Council on copyright in the Digital Single Market", **COM/2016/0553 final – 2016/0280 (COD),** 14.9.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0593 (02.06.2020).

[57] European Parliament, "Legislative Train Schedule Connected Digital Single Market, JD-Modernisation of European Copyright Rules: Directive on Copyright in the Digital Single Market",

"*Taşınabilirlik Tüzüğü (Portability Regulation)*[58]" olarak anılan 2017/1128 sayılı Tüzük[59] ise, Birlik içerisinde seyahat eden kişilerin, film, müzik, video oyunları, spor etkinlikleri, e-kitap gibi kendi ülkelerinde sahip oldukları çevirimiçi hizmet ve aboneliklere, Birlik içerisindeki seyahatleri esnasında da, adil kullanım ilkesi (fair use policy)[60] çerçevesinde tıpkı kendi evlerinde olduğu gibi, ulaşabilirliklerinin sağlanması amacıyla kabul edilmiştir[61]. 2017/1128 sayılı bu Taşınabilirlik Tüzüğü ile, hem fikri mülkiyet haklarının izinsiz kullanımının önlenmesi, hem de çevirimiçi hizmetlere Birlik içi kesintisiz erişimin sağlanarak, yekpareliğin sağlandığı bir Avrupa dijital tek pazarında tüketici yararının korunması hedeflenmiştir.

1.3.1.2. Sütun II: Koşulların İyileştirilmesi

Avrupa için Dijital Tek Pazar Stratejisi ile belirlenen ikinci sütun, dijital ağ ve hizmetlerin gelişimi açısından gerekli koşulların, bu pazarda faaliyet gösteren bireysel ve kurumsal kullanıcılar bakımından iyileştirilmesidir. İyileştirme çabaları, Birlik genelinde hızlı ve makul fiyatlı internet erişimi yoluyla kolaylıkla işlem yapılabilecek dijital ağ bağlantılarının oluşturulması ve sistem güvenliğinin sağlanması amacıyla gerekli yasal ve teknik alt yapı koşullarının gözden geçirilerek güncellenmesi temeline oturtulmuştur. Böylelikle, başta Birlik vatandaşları olmak üzere Avrupa dijital tek pazarında işlem yapacak tüketiciler, girişimciler, yatırımcılar, kamu kuruluşları ve özel şirketler de dahil olmak üzere, tüm gerçek ve tüzel kişilerin dijital ekonomi sistemine duydukları güvenin artırılması ve tesis

---

2019, http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-directive-on-copyright-in-the-digital-single-market (02.06.2020).

[58] Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on crossborder portability of online content services in the internal market, (Portability Regulation), **Official Journal**, **L 168/1**, 30.06.2017, https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2017.168.01.0001.01.ENG (02.06.2020).

[59] Avrupa Birliği Hukukunun ikincil nitelikteki kaynaklarından biri olan ve Türkiye Cumhuriyeti Avrupa Birliği Genel Sekreterliği'nin yayınlamış olduğu "*Avrupa Birliği Terimler Sözlüğü*" kapsamında, Türkçe'ye "*Tüzük*" olarak tercüme edilebileceği belirtilen "*Regulation*" terimi, işbu tez çalışması kapsamında da bu açıklamaya uygun olarak "*Tüzük*" şeklinde kullanılmıştır. Türkiye Cumhuriyeti, Avrupa Birliği Genel Sekreterliği, **Avrupa Birliği Terimler Sözlüğü**, Ankara, 2009.

[60] "Adil Kullanım" a ilişkin hususlar, bu çalışmanın 1.3.1.2. sayılı bölümünde II. Sütuna ilişkin açıklamalar kapsamında detaylı olarak ele alınmıştır.

[61] European Commission and its Priorities, "Cross-border Portability of Online Content Services", 2019, https://ec.europa.eu/digital-single-market/en/cross-border-portability-online-content-services, (02.06.2020).

edilecek bu güven ortamı sayesinde de dijital pazardan beklenen yüksek verimliliğin alınması hedeflenmektedir. Bu hedef doğrultusunda bir yandan bilgi ve teknoloji temelli yenilik ve yatırımlar teşvik edilirken, diğer yandan da özellikle dijital ekonominin bel kemiğini oluşturan rekabet, telekomünikasyon, tüketici hakları, kişisel verilerin korunması alanlarında uyumlu yasalar oluşturularak, güvenilir, şeffaf ve yekpare Avrupa dijital tek pazarının oluşumunun tamamlanması amaçlanmaktadır[62].

Temelleri bilgi ve iletişim teknolojilerindeki hızlı değişime dayanan Avrupa dijital tek pazarının, sağlıklı gelişimi ve parçalı pazar görünümünden kurtarılarak, yekpare işlevselliğinin, güvenilirliğinin ve birlikte çalışabilirliğinin sağlanması önemlidir. Dijital tek pazarın sağlıklı gelişimi adına, telekomünikasyona ilişkin mevzuatın, dijital çağdaki teknolojik gelişmeler karşısında ortaya çıkan yeni koşullara uyum sağlayacak şekilde güncellenerek, uyumlaştırılması gereklidir. Elektronik iletişime yönelik Birlik müktesebatının son güncellemesi, halen yürürlükte olan "*2009/140/EC sayılı Direktif*[63]" ile gerçekleştirilmiştir. 2016 yılında, yüksek teknoloji ve hızlı internete ilişkin yatırımları cesaretlendirmeyi, iletişim sektöründeki rekabeti artırmayı, birlikte çalışabilirliğin tesisini, hizmet kalitesinin yükseltilmesini, ağ ve veri güvenliğinin artırılmasını temel alan "*2016/590 sayılı Avrupa Elektronik Telekomünikasyon Yasa Teklifi*[64]" Komisyon tarafından hazırlanıp sunulduysa da, bu tasarı henüz yürürlüğe girmemiştir[65]. Son olarak, Avrupa Parlamentosu ve Konsey, elektronik iletişim yasalarının yüksek teknolojik gelişmeler

[62] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss. 3-4,9-11.

[63] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services, **Official Journal**, **L337/37,** 18.12.2009, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0140 (02.06.2020).

[64] European Parliament, "Proposal for a Directive of the European Parliament and of the Council Establishing the European Electronic Communications Code", **COM (2016), 590**, 2016, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN (02.06.2020).

[65] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on the Mid-term, Review on the Implementation of the Digital Single Market Strategy, A Connected Digital Single Market for All", **(COM 228) final**, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A228%3AFIN, s.5;
European Commission, "State of the Union 2016: Commission Paves the Way for More and Better Internet Connectivity for all Citizens and Businesses", **Press Release**, 14.09.2016, http://europa.eu/rapid/press-release_IP-16-3008_en.htm (02.06.2020).

doğrultusunda güncellenmesi konusunda siyasi bir uzlaşmaya vararak, bunu 6.6.2018 tarihli Basın Açıklaması ile de ilan etmişlerdir[66]. Atılacak bu adımlar, teknolojik gelişmelerle uyumun yakalanması ve veri güvenliğinin sağlanarak, Avrupa dijital tek pazarından beklenen verimin artırılması bakımlarından gerekli yasal alt yapı çalışmalarının tamamlanabilmesi için önemlidir. Birlik'in elektronik iletişime ilişkin anılan hedefleri, aynı zamanda 2025'e kadar gerçekleştirmeyi planladığı ve Birlik genelinde –görece az gelişmiş bölgelerde bulunanlar da dahil- tüm gerçek ve tüzel kişilerin, "*kablosuz 4G ve 5G ağları*" üzerinden kesintisiz, hızlı, hesaplı ve güvenilir internete erişimlerinin sağlanabilmesi için yapılacak altyapı yatırımlarının tamamlaması ve bir "*Gigabit Topluluğu (Gigabit Society)*" oluşturulması hedefleri ile de örtüşmektedir[67].

Elektronik iletişim bağlamında atılan somut adımlardan biri de, "*dolaşım (roaming)*" konusunda kabul edilen "*2016/2286 sayılı Tüzük*[68]"tür. Dolaşıma ilişkin 2016/2286 sayılı bu Tüzük sayesinde, 2017 yılından bu yana, telekomünikasyon hizmeti sağlayıcıları, hangi üye devletin vatandaşı olurlarsa olsunlar, Birlik dahilinde seyahat eden kullanıcıların almış oldukları hizmetlere, ilgili kişilerin aboneliklerinin bulunduğu üye devlette ödedikleri perakende hizmet bedellerini uygulama ve bu bedellere ek herhangi bir servis ücreti yansıtmama yükümü altına girmişlerdir[69].

---

[66] European Commission, "Digital Single Market: EU Negotiators Reach a Political Agreement to Update the EU's Telecoms Rules", **Press Release**, 2018, http://europa.eu/rapid/press-release_IP-18-4070_en.htm , (02.06.2020).

[67] European Commission, "A Digital Single Market for Europe: Commission Sets Out 16 Initiatives to Make it Happen", **Press Release**, 2015, s.2; European Commission, "Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society", **COM 300 final**, 14.9.2016, https://ec.europa.eu/digital-single-market/en/news/communication-connectivity-competitive-digital-single-market-towards-european-gigabit-society (02.06.2020), ss.2-3, 5,15;
European Commission, "State of the Union 2016: Commission paves the way for more and better internet connectivity for all citizens and businesses", **Press Release**, 14.09.2016, http://europa.eu/rapid/press-release_IP-16-3008_en.htm (02.06.2020).

[68] "Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment", **Official Journal of the European Union**, **L 344/46,** 17.12.2016, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32016R2286

[69] 2016/2286 sayılı Avrupa Birliği Tüzüğü, parag.(1); Madde 1; European Commission, "End of Roaming Charges in the EU in 2017: Commission Agrees on New Approach to Make it Work for All Europeans", **Press Release**, 21.09.2016, http://europa.eu/rapid/press-release_IP-16-3111_en.htm (02.06.2020);
European Commission, "Completing a Trusted Digital Single Market for All", The European Commission's contribution to the Informal EU Leaders' Meeting on Data Protection and the Digital Single Market in Sofia on 16 May 2018, **COM 320 Final**, 2018

Ancak servis sağlayıcılarına getirilen bu yükümlülük, kullanıcıların bir başka üye devlet sınırları içinde "*adil kullanım ilkesi (fair use policy)*" ile sınırlı olarak yapacakları geçici kullanımları kapsamaktadır. Adil kullanım, 2016/2286 sayılı Tüzük'ün 4/4. maddesi kapsamında dört ay olarak belirlenmiştir. 2016/2286 sayılı Tüzük ayrıca servis sağlayıcıya, kötüye kullanımın engellenerek pazarda rekabetin bozulmaması amacıyla, hizmet kullanımının yasal sınırlar dahilinde yapılmasının kontrolü kapsamında orantılılık ilkesine uygun ve makul usullerle önlem alabilme yetkisi de tanınmıştır. Ancak servis sağlayıcı bu önlemleri alırken kişisel veriler de dahil tüm temel hak ve özgürlüklerin korunmalarına ilişkin yasal düzenlemeleri azami surette dikkate almakla yükümlüdür. Geçici nitelikte seyahat kapsamını aşarak, kalıcı nitelik kazanan kullanımlar ise, pazarda özellikle yerel fiyatlar üzerinde baskı yaratmak suretiyle rekabet ihlallerine yol açabileceğinden, 2016/2286 sayılı Tüzük, bu gibi uzun süreli kullanımlara uygulanmamaktadır[70]. Telekomünikasyon hizmetlerinin dolaşımına ilişkin yapılan bu düzenleme, hem tüketici menfaatlerinin ve güvenliğinin artırılmasına, hem de telekomünikasyon hizmetleri açısından, dijital tek pazarın parçalı görünümünden kurtarılmasına ilişkin atılmış önemli bir somut adımdır.

Tüketici haklarının korunmasına ilişkin olarak üye devletler arasındaki işbirliğinin artırılması hususunda 2017/2394 sayılı Tüzük[71] hazırlanıp, 17 Ocak 2020 tarihi itibarı ile yürürlüğe girerek, aynı hususta kendinden önceki 2006/2004 sayılı Tüzük [72] 'ün yerini almıştır. 2017/2394 sayılı bu Tüzük, sınırötesi işlemler kapsamında tüketici haklarının daha iyi korunması amacıyla, üye devletler arasında

---

https://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1&year=2018&number=320&language=EN s.6;
Wolfgang Kerber, Heike Schweitzer, "Interoperability in the Digital Economy", **Joint Discussion Paper Series in Economics by MAGKS, No. 12**, 2017, https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2017/12-2017_kerber.pdf (02.06.2020). ss.15-16.

[70] 2016/2286 sayılı Avrupa Birliği Tüzüğü, Beyanlar (6,40), (15); Madde 4.

[71] European Union, "Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No.2006/2004", **Official Journal of the European Union**, **L345/1**, 27.12.2017 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF-/?uri=CELEX:32017R2394&from=EN (02.06.2020).

[72] European Union, "Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation)", **Official Journal L 364**, 9.12.2004, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32004R2006 (02.06.2020).

Birlik çapında uyumlaştırılmış yasa hükümleri ile, etkili işbirliği ağları oluşturmayı hedeflemektedir. Her geçen gün daha fazla tüketiciye ulaşan Avrupa dijital tek pazarında tüketicilere yönelen tehditlerin nitelik ve nicelik olarak artmasının, bu hususlarda üye devletler arasında daha sıkı işbirliği oluşturulmasına ilişkin çabaların ivme kazanmasına yol açarak, neticede 2017/2394 sayılı Tüzük'ün kabulüne sebep olduğu da söylenebilir.

2015 tarihli Avrupa için Dijital Tek Pazar Stratejisi'nin altını çizdiği bir diğer husus da, yeni iş imkanları yaratarak büyümeye katkı sağlama potansiyeline sahip olan, pek çok açıdan yaratıcılığı tetikleyen ve her geçen an, günlük hayatımızda daha fazla yer kaplayan görsel ve işitsel "*dijital medya*" hizmetlerinin dijital ekonomideki önemidir. Dijital medya kavramı, internet üzerinden erişilen, filmleri, edebi eserleri, TV yayınlarını, video paylaşımlarını, tiyatro gösterilerini, konserleri, klipleri, bilgisayar oyunlarını, uzaktan eğitim programlarını ve benzeri çevirimiçi paylaşımları kapsamaktadır. Görsel ve işitsel medya hizmetlerine ilişkin halen yürürlükle bulunan "*2010/13/EC sayılı Direktif'in*[73]" artan ihtiyacı karşılayacak şekilde güncellenmesi çalışmaları devam etmektedir. Güncelleme çalışmaları dahilinde uyumlaştırılacak yasalar vasıtasıyla, Birlik genelinde, telif ve fikri mülkiyet hakları daha iyi korunurken, aynı zamanda dijital medya açısından da tek pazarın sekteye uğramadan işlemesinin de önü açılacaktır. Dolaşımı (Roaming) düzenleyen 2016/2286 sayılı Tüzük, Birlik vatandaşlarının görsel ve işitsel medya içeriklerine Birlik sınırları içinde kolaylıkla erişim imkanı da sağladığından, 2016/2286 sayılı işbu Tüzük'ün aynı zamanda medya hizmetlerinin de taşınabilirliğini artırarak, görsel-işitsel medya kullanımının yaygınlaşmasına katkıda bulunduğu da söylenebilir. Ayrıca Dolaşıma ilişkin 2016/2286 sayılı Tüzük'ün kabulü ile, dijital medya hizmetlerinin taşınabilirliğinin artması, bu konuda Birlik genelinde serbest ve adil rekabet ortamının sağlanmasını ve hizmet kalitesinin

[73] European Union, "Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of Audiovisual Media Services, (Audiovisual Media Services Directive)", **Official Journal, L 95/1,** 15.4.2010, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013 (02.06.2020).

artırılmasını da beraberinde getirerek, Avrupa dijital tek pazarının aksamadan işleyişine katkıda bulunmaktadır [74].

1.3.1.2.1. Big Data ve Kişisel Verilerin Korunması

"*Big Data (Büyük Veri)*", hızla gelişen ve yaygınlaşan çevirimiçi sistemler ve internet uygulamaları sayesinde, sosyal medya, e-ticaret, e-bankacılık işlemleri gibi dijital teknolojilerin sıklıkla kullanılması sonucu, çevirim içi ortamda kalan dijital izlerden ve değişik dijital kaynaklardan elde edilerek depolanıp işlenebilen çeşitli tipteki büyük hacimli veri yığınlarını ifade eder. Big data, pek çok kaynakta "3Vs-*hacim, çeşitlilik ve hız (3Vs- volume, variety, velocity)*" üçlemesi şeklinde ifade edilerek, diğer veri türlerinden nitelik ve niceliksel farklılığı ortaya konulmaya çalışılmaktadır. Günümüzde, hacmi, hızı ve gerek kaynak, gerekse de veri çeşitliliği inanılmaz boyutlara ulaşan bu büyük veri yığınının, gelişmiş bilgi ve iletişim teknolojileri kullanılarak, değişik şekillerde analiz edilip, anlamlı hale getirilmesi ve neticede de önceden bilinmeyen gizli bilgilere ulaşılarak, bu bilgilerden ekonomik fayda elde edilmesinde kullanılmasına yaygın olarak rastlanmaktadır. Gelişmiş teknolojilerle big datanın işlenmesine dayanan ve devrim niteliğinde kabul edilen bu yeni sistem, veri temelli yeni ekonomik değerler ortaya koymaktadır. Bu değerleri, ticari anlamda kullanabilen teşebbüs, birey ve hatta hükümetlerin, rakipleri karşısında öne geçerek, küresel pazarları değiştirip yeniden şekillendirebilecekleri düşünülmektedir[75]. Diğer bir ifade ile, Google, Yahoo, Yandex, Broadreader, Bing ve benzeri arama motorları; Facebook, Twitter, Linkedin, MySpace gibi sosyal medya platformları; Instagram, Flicker, YouTube ve sair fotoğraf ve video paylaşım

---

[74] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.10-11; European Commission, "Completing a Trusted Digital Single Market for All", **COM 320 Final**, 2018, s.6; Statista, "Statistics and Market Data on Media and Advertising", https://www.statista.com/markets/417/media-advertising/ ; Statista, "Digital Media Report", 2018, https://www.statista.com/study/44526/digital-media-report/ (02.06.2020).

[75] Chaowei Yang, Qunying Huang, Zhenlong Li, Kai Liu, Fei Hu, "Big Data and Cloud Computing: Innovation Opportunities and Challenges", **International Journal of Digital Earth**, Cilt. 10, Sayı.1, 2017, ss. 13-15;
Korcan Doğan, Sacit Arslantekin, "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum", **Ankara Üniversitesi Dil ve Tarih Coğrafya Fakültesi Dergisi**, Cilt.56, S.1, 2016, ss. 15, 21-25;
Viktor Mayer-Schönberger, Kenneth Cukier, **Big Data A Revolution that Will Transform How We Live, Work and Think**, Houghton Mifflin Harcourt Publishing, USA, 2013, ss.6-7;
Stephan J.Mooney, Daniel J. Westreich, Abdulrahman M. El-Sayed, "Epidemiology in the Era of Big Data", **Department of Health and Human Services**, 2015, https://www.ncbi.nlm.nih.gov/p-mc/articles/PMC4385465/pdf/nihms659322.pdf (02.06.2020) ss.1-3.

siteleri; e-ticaret, e-devlet sistemleri; uygulama satış mağazaları (App-stores), e-posta servisleri; Shopzilla, Trivago, PriceGrabber gibi fiyat karşılaştırma siteleri, internet bankacılığı, akıllı telefonlar, entegre kameralar ve benzeri çeşitli uygulamaların kullanılmasıyla, çevirim içi ortamda bırakılan pek çok dijital iz, big datada depolanmaktadır. Bu izlerin, klasik veri işleme yöntemlerinden farklı, yüksek teknolojik ve hatırı sayılır bir şekilde hızlı sistemler tarafından analiz edilip yorumlanmasıyla küresel ticareti şekillendirebilecek ekonomik değeri olan yeni çıktı ve bilgiler ortaya konulabilmektedir. Her gün katlanarak büyüyen big datanın müşterilerin hizmetlere ulaşmalarına, iş sahiplerinin de müşteri tercih, ihtiyaç ve davranışlarını anlamlandırarak yeni müşteriler bulmalarına, yeni pazarlara açılmalarına, iş stratejileri geliştirmelerine ve çevirim içi reklamcılık faaliyetlerine katkı sağlayıp, katma değerler ortaya koyabildiği görülmektedir. Ortaya konan bu katma değerlerin, dijital ekonomi çağında ekonomik ve sosyal hayatın gelişimine ivme kazandırıp yön verdiğini söylemek de yanlış olmayacaktır. Ancak, çeşitli analiz teknikleri kullanılarak yapılan "*veri madenciliği (data mining)*" yöntemleri ile, *big data* içinde barınan verilerin harmanlanması sonucu, gizli kalmış ve önceden tahmin edilemeyen yeni ve kullanılabilir bilgi ve verilere ulaşılmasının, hakim durumun kötüye kullanılması yoluyla rekabete [76], genel veri kontrol ve güvenliğine, mahremiyete ve kişisel verilerin korunmasına ilişkin çeşitli tehditleri de beraberinde getireceği söylenebilir[77]. Bu tehditlerin bertaraf edilebilmesi için dijital tek pazarı şekillendirme gücüne sahip bulunan çevirim içi platform ve sistemlerin, big data kapsamındaki faaliyet ve uygulamalarının denetlenmesini sağlamak üzere birbiriyle uyumlu yasal ve teknik alt yapı çalışmalarının tamamlanması önemlidir[78].

[76] Big data verilerine gerek hakim durumda bulunmaları, gerekse de daha iyi teknik ve ekonomik imkanlara sahip olmaları bakımından daha kolay erişebilir durumda bulunan şirket, çevirim içi platform ve aracılar, pazardaki adil rekabet ortamını bozarak pazarı şekillendirebilir. Daha fazla bilgi için bkz. Vicente Bagnoli, "The Big Data Relevent Market", **Concorrenza e Mercato**, Cilt. 23, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064792 (02.06.2020).

[77] Ira S. Rubinstein, "Big Data: The End of Privacy or a New Beginning?", **NYU School of Law, Public Law Research Paper, No.12-56**, 2012, International Data Privacy Law, "Forthcoming: 2013", 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659 (02.06.2020) s.1-4;
Pwint Phyu Khine, Wang Zhao Shun, "Big Data For Organizations: A Review", **Journal of Computer and Communications**, Cilt.5, 2017, ss. 41-43.

[78] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, s.11;
Martin Hilbert, "Big Data for Development: From Information to Knowledge Society", **Pre-published version**, 2013, http://ssrn.com/abstract=2205145 (02.06.2020), ss.3-5;
Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, The Challenge of

Big datanın özellikle kişisel verilerin korunması bağlamında oluşturduğu risklerin farkında olan Birlik, bu verilerin güvenliğinin korunması konusunda yapmış olduğu çalışmalar neticesinde, sonraki bölümlerde daha detaylı olarak incelenecek olan, "*2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü*[79]"nü kabul etmiştir. Bu Tüzük'ün kabulü ile, hem kişisel verilerin korunması, hem de belirli yasal sınırlar çerçevesinde bu verilerin serbest dolaşımlarının sağlanması hususlarında önemli bir adım atılmıştır. Genel Veri Koruma Tüzüğü ile aynı gün resmi gazetede yayınlanan "*2016/680 sayılı Direktif*[80]*"* ile de temel bir hak olarak korunması gerektiği Lizbon Antlaşması ile kabul ve taahhüt edilen kişisel verilerin[81], yetkili merciler tarafından suçun önlenmesi, soruşturulması, tespiti, kovuşturulması, cezaların infazı, kamu güvenliğinin korunması gibi amaçlarla dahi olsa, işlenmelerine yönelik kurallar getirilip, sınırlar belirlenerek, bu doğrultudaki ilke ve prensipler net bir şekilde ortaya konulmuştur.

1.3.1.2.2. Güven Tesisinin Önemi

Dijital ekonomiye hem bireysel, hem de tüzel kişiler bağlamında katılımın artırılarak, bu ekonomiden en üst seviyede yararlanılmasının ve Avrupa dijital tek

---

"big data" for data protection, **International Data Privacy Law**, Editorial, 2012, Cilt. 2, Sayı.2, s.47.

[79] European Union, "Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)", **Official Journal of the European Union, L 119,** 4.5.2016, https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1540463136351&uri=CELEX:32016R0679, (02.06.2020)K işisel verilerin korunmasına ilişkin 2016/679 sayılı Tüzük, 25 Mayıs 2016 tarihi itibarı ile yürürlüğe girmiştir. Bu çalışmada, "*Kişisel verilerin korunmasına ilişkin 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü*", "*2016/679 sayılı Tüzük*", "*Genel Veri Koruma Tüzüğü*", "*Tüzük*" veya "*GDPR*" olarak da adlandırılabilecektir.

[80] European Union, "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA", **Official Journal of the European Union, L 11989**, 4.5.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELE-X:32016L0680&qid=1540463803208&from=EN (02.06.2020), *Avrupa Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/680 sayılı, Konsey'in 2008/977/JHA Çerçeve Kararını Yürürlükten kaldıran, yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına ilişkin Direktif*.

[81] European Union, **Treaty of Lisbon, amending the Treaty on European Union and the Treaty Establishing the European Community**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT , (02.06.2020). Madde 6;
2016/680 sayılı Avrupa Birliği Direktifi Beyanlar (1).

pazarının sekteye uğramadan devamlılığının sağlanabilmesi için, dijital hizmetlere ve bunların sağlayıcılarına ilişkin güvenin artırılması önemlidir. Bu güvenin oluşturulmasında ise, her gün katlanan oranlarda toplanıp, çeşitli şekillerde işlenerek kullanılmaya devam eden verilerin sistemsel ve yasal güvenliklerinin tam olarak sağlanmasının payı yadsınamaz. Çevirim içi bankacılık ve finans işlemlerine yönelik ekonomik saldırılar, dolandırıcılık faaliyetleri, tüketici haklarının suiistimali, veri korsanlığı, kişisel verilerin çeşitli şekillerde ihlali ve bu verilere istenmeyen erişim gibi çok çeşitli unsur[82], dijital ekonomi çarkında kendine önemli bir yer edinerek, ticari bir tedavül değeri olduğu kabul edilen verilerin güvenliğini tehdit eden olumsuzluklar arasında sayılabilir. Dijital tek pazara duyulan güveni kırıcı nitelikteki bu tehditlere karşı verilerin korunmasının sağlanması, dijital ekonominin tetikleyicisi haline geldiği kabul edilen güvenin tesisi bakımından kilit niteliği taşımaktadır. Gönüllü olarak çevirim içi ortama aktardığımız verilerin yanı sıra, kamusal kayıtlar; akıllı cihaz, arama motoru ve internet kullanımları; navigasyon, sosyal medya, e-ticaret uygulamalarını kullanmamız nedeniyle çoğu zaman farkında olmadan arkamızda bıraktığımız veri ve dijital ayak izlerinin hacminin ne derece büyük olduğu artık herkes tarafından bilinmektedir. Arkada bırakılan bu iz ve verilerin yasal bir dayanağı olmadan kayıt dışı toplanıp, analiz edilerek kullanılabilmeleri sonucunda oluşan tehditlere karşı, Birlik'in, etkili ve şeffaf önemler alarak uyumlaştırılmış yasal ve teknik düzenlemeler yapması, dijital tek pazara duyulan güvenin artırılması bakımından önemlidir. Bu sebeple, Avrupa dijital tek pazarına güvenin artırılmasına yönelik olarak, şeffaflığı ve uyumu sağlayan, ifade özgürlüğüne zarar vermeyen nitelikteki uyumlu yasal ve teknik düzenlemeler

[82] Burada sayılan güven kırıcı unsurlara ek olarak, casus Truva Atları gibi virüsler yardımıyla yapılan siber saldırılar, siber-terör faaliyetleri; çevirim içi ağlar üzerinden yapılan şiddet içerikli söylemler ile nefret söylemleri, çocuk istismarı ile pornosu, yasadışı kumar hizmetleri, sahte ilaç temini de dahil yasadışı mal ve hizmet tedariki gibi siber suçlar, marka, telif hakkı ve fikri mülkiyet hakkı ihlalleri, mahremiyete yönelen çeşitli saldırılar, kimlik ve ticari sır hırsızlıklarını da kapsayan çeşitli kişisel veri ihlallerini içeren yasa dışı ve zarar verici içerik ve kullanım, istenmeyen erişime veya erişimin engellenmesine yönelik illegal faaliyetler de sayılabilir.

vasıtasıyla, Birlik, siber suç ve tehditlere[83] karşı hızlı ve etkili bir şekilde mücadele ederek, veri güvenliğini en üst noktaya taşıyacak önlemler almaya çalışmaktadır[84].

1.3.1.2.3. Güvenliğe İlişkin Altyapı Çalışmaları

Gerçek ve tüzel kişilerin, hatta devletlerin, bilgi ve iletişim teknolojilerine olan bağımlılığı, maaşların ödenmelerinden, muhasebe işlemlerine, envanter ve satış takiplerinden, bankacılık ve finans işlemleri ile eğitim, sağlık, milli savunma, lojistik ve taşımacılık sektörlerine kadar sınırları zorlayan nitelikte geniş bir yelpazeyi kapsamaktadır [85] . Dolayısıyla, bilgi ve iletişim teknolojileri ile internet uygulamalarının sağladığı kesintisiz ve açık imkanlardan yararlanarak, ekonomik, sosyal ve ticari ilişkilerimizi, sağlıklı bir şekilde sürdürebilmemiz, bu teknoloji ve sistemler vasıtasıyla işlenecek verilerin korunması ve veri ihlallerinin önlenmesine önemli ölçüde bağlıdır[86].

Soğuk Savaş döneminin tanklı tüfekli geleneksel tehditleri, içinde bulunduğumuz dijital çağda, biçim değiştirerek, bireyler, devletler, ekonomi ve çevre gibi kilit unsurları hedef alabilen ve nereden, kimden geldiği belli olmayan, sanal tehditlere dönüşmüştür[87]. Pazarların birbirlerine karşılıklı bağımlı olduğu küresel

---

[83] Yasa dışı içerikler; hackerlar, teröristler ya da suç şebekelerinden, üye devletlerin haber alma teşkilatları gibi kamusal aktörlerden gelebilecek çeşitli yasadışı müdahaleler; kimlik ve ticari sır hırsızlığı; veri akışının ve serbest dolaşımının yasayışı yollarla engellenmesi; online işlemler vasıtasıyla yapılan dolandırıcılıklar gibi hususlar siber suç ve tehditlere örnek olarak sayılabilir.

[84] Rob van der Dam, The Trust Factor in the Digital Economy: Why Privacy and Security is Fundamental for Successful Ecosystems, 14th International Telecommunications Society (ITS) Asia-Pacific Regional Conference: "Mapping ICT into Transformation for the Next Information Society", Kyoto, 2017, **ECONSTOR,** https://www.econstor.eu/bitstream/10419/168536/1/Rob-van-den-Dam.pdf (02.06.2020). ss. 1-5;
European Commission, "Directorate General Internal Market and Services, Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries", **Summary of Responses,** 4.7./12.9.2012, https://ec.europa.eu/digital-single-market/en/news/archive-e-commerce-directive-what-happened-and-its-adoption, (02.06.2020) s. 2;
The National Academies of Sciences, "Engineering, Medicine, At the Nexus of Cyber Security and Public Policy: Some Basic Concepts and Issues", 2014, https://www.nap.edu/download/18749 ss.vii, ix, 1, 13;
European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.12-13.

[85] The National Academies of Sciences, ss. 1-15.

[86] European Union, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", **JOIN**, **2013, 1, Final,** https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN (02.06.2020), s.2.

[87] 2007 yılında Estonya'nın kamusal çevirimiçi sistemlerine aynı anda, nereden geldiği belli olmayan bir şekilde yapılan çok sayıda siber saldırılar neticesinde, sistemler kilitlenmiş ve bir süre hizmet verilememiştir. Aynı şekilde 2011 yılında Sony ve Adidas firmalarına yapılan siber saldırılar

dünyada, dijitalleşmenin hayatın her alanına değen geniş bir işlem yelpazesine yayılması sebebiyle, küresel dijital sistemin bir yerinde ortaya çıkan sanal tehditler, sistemin genelini etkiler hale gelmişlerdir. Bu hassas denge, Birlik'i, çevirimiçi işlemlerin ve verilerin güvenliğinin artırılması hususunda, Siber Güvenlik Politikalarını hukukun üstünlüğüne, demokrasiye, temel hak ve özgürlüklere saygı, şeffaflık, hesap verebilirlik, kişisel verilerin korunması prensipleri çerçevesinde güncelleyerek, asgari güvenlik standartlarının belirlendiği yeni stratejileri benimsemeye zorlamaktadır. Böylelikle kişisel verilerin korunmasını da kapsayan temel hak ve özgürlükler ile güvenlik arasındaki hassas dengenin gözetilerek, doğası gereği sınırlar ötesi bir nitelik taşıyan siber suç ve tehditlerle başa çıkılmaya çalışılmaktadır. Zira internetin, çevirim içi işlemlerin ve kişisel verilerin güvenliğinin sağlanması, bir bütün olarak demokrasinin, temel hak ve özgürlüklerin ve özellikle de bilginin geleceğini kişinin kendisinin tayin etmesi hakkının, korunabilmesi bakımlarından elzem niteliktedir[88].

"*2000/31 sayılı E-Ticaret Direktifi*[89]", dijital tek pazarın gelişimi ve parçalı görünümünden kurtulabilmesi için bilgi teknolojilerinin desteklenmesinin yanı sıra, mal ve hizmetlerin serbest dolaşımlarının ve teşebbüsler bakımından Birlik içerisinde istenilen yerde kuruluş serbestisinin sağlanarak, Birlik'i ve vatandaşlarını bu anlamda bölen tüm ticaret engellerinin kaldırılmasının gerekliliğini vurgulamaktadır[90]. Böylelikle E-Ticaret Direktifi ile, dijital tek pazarın bir anlamda yasal çerçevesi oluşturularak, pazarda faaliyet gösterecek işletme ve tüketiciler bakımından hukuki anlamda açıklık ve kesinlik sağlanması amaçlanmıştır. Söz konusu E-Ticaret Direktifi, aynı zamanda, artan siber suç, ihlal ve saldırılar

---

sonucunda da ilgili şirketlerin çevirim içi sistemleri hasar görmüş ve müşteri verileri tehlikeye düşmüştür. Daha fazla bilgi için bkz. Annegret Bendiek, "European Cyber Security Policy", **Research Paper 13,** Berlin 2012, Stiftung Wissenschaft und Politik-SWP- Deutsches Institut für Internationale Politik und Sicherheit (Ed.), ss. 9-10; BBC, "Adidas websites go offline after hacking cyber-attack", **BBC Technology News**, 2011, https://www.bbc.com/news/technology-15614590 (02.06.2020); Beatrix Toth, "Estonia under Cyber Attack", **Hun-CERT,** https://www.cert.hu/sites/default/files/Estonia_attack2.pdf (02.06.2020);
James G.McGann, "2015 Global Go To Think Tank Index Report", TTCSP Global Go To Think Tank Index Reports, **University of Pennsylvania**, Paper 10, https://repository.upenn.edu/cgi-/viewcontent.cgi?referer=&httpsredir=1&article=1009&context=think_tanks (02.06.2020), s.166.

[88] Annegret Bendiek, ss.5-6, 19.

[89] European Union, "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)", **Official Journal L 178**, 17.7.2000, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031 (02.06.2020), ss.1-16.

[90] 2000/31/EC sayılı Direktif, Beyanlar (1), Madde 1.

karşısında e-ticaretin gelişimini desteklemeyi de amaçlamaktadır. Bu bağlamda aracı durumundaki bilgi toplumu hizmet sağlayıcılarını tüm Birlik çapında koruyarak, bunların faaliyetlerini, siber tehditler karşısında aksamadan sürdürebilmelerini sağlamak üzere özel bir düzenleme getirmektedir. Bu düzenlemeye göre, aracı durumundaki bilgi toplumu hizmet sağlayıcısı, iletimi kendisinin başlatmaması, iletimin alıcı tarafını veya içeriğinde yer alan bilgileri seçmemesi ya da değiştirmemesi kaydı ile, yalnızca iletimden ya da iletişim ağına erişime izin verilmesinden ibaret işlemler sırasında gerçekleşebilecek ihlallerden sorumlu tutulmayacaktır. Bu düzenlemenin amacı, hizmet sağlayıcılarının üzerinde gereğinden fazla baskı kurarak, onların hizmet sağlamaya ilişkin şevklerinin kırılmasının engellenmesidir. Böylece güvenlik ve e-ticaret arasındaki hassas denge de korunmaya çalışılmıştır. Ancak her halde aracı bilgi toplumu hizmet sağlayıcıları, yetkili mahkeme yahut idari makamların, ihlalin önlenmesi veya sona erdirilmesine yönelik kararlarının, işin gerektirdiği makul şekil ve sürede yerine getirilmesinden sorumludurlar. Ayrıca böyle bir ihlalin tespiti durumunda ilgili hizmet sağlayıcılarının, gerekli tedbirlerin alınabilmesi amacıyla, vakit kaybetmeden yetkili makamları haberdar etme yükümlülükleri de bulunmaktadır. E-Ticaret Direktif'inin anılan maddeleri, dijital güvenliğin tesis edilerek, Avrupa dijital tek pazarının gelişimine katkı sağlayacak önemli adımlardan birinin daha atılmasını temin etmesi bakımından önemlidir[91].

2004 yılında, Avrupa Birliği'nde siber güvenlik konusunda bir uzmanlık merkezi olarak faaliyette bulunması planlanan "*Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Union Agency for Network and Information Security-ENISA)"* kurulmuştur. ENISA'nın üye devletler ile kamu sektörü ve/veya özel sektördeki gerçek ve tüzel kişiler de dahil tüm aktörlerle, işbirliği halinde düzenleyeceği eğitimler, oluşturacağı politikalar vasıtasıyla, ağ, veri ve bilgi güvenliği konularında Birlik genelinde bir kültür ve farkındalık yaratarak, Avrupa dijital tek pazarının siber tehditler karşısında aksamadan işlemesine yardımcı olması beklenmektedir[92].

[91] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.12-13;
2000/31/EC sayılı Direktif, parag. (40,42), Bölüm 4, Servis Sağlayıcıların Sorumluluğu, madde 12, 13, 14, 15.
[92] Bu konuda daha fazla bilgi için bkz. ENISA, https://www.enisa.europa.eu/about-enisa (02.06.2020);

Ağ ve bilgi sistemlerinde güvenliğin artırılması hususunun önemi, Nisan 2007'de Estonya'ya sistematik olarak düzenlenen siber saldırılar sonucunda oluşan farkındalıkla daha da artmıştır. Bu siber saldırılar, özellikle Microsoft Outlook tabanlı kamusal sistemler ile bankacılık sistemlerine erişimi, büyük oranda engellemiştir. Bu engelleme neticesinde, e-iletişim işlemleri ile ağ üzerinden yürütülen diğer resmi ve ticari işlemler durma noktasına gelerek, büyük zararlara sebep olmuştur. 2007'de gerçekleşen bu siber saldırılar, başta Estonya olmak üzere tüm Birlik genelinde ağ ve bilgi sistemlerinin güvenliğinin sağlanması konusunda topyekün bir politika değişikliği ihtiyacını ortaya koyması bakımından önemlidir[93].

Yapılacak düzenlemelerle çevirim içi işlemlerde güvenliğin sağlanarak, sisteme duyulan güveninin artırılması, dijital tek pazardan beklenen verimliliğin sağlanabilmesi bakımından kilit rol oynamaktadır. Zira Avrupa Birliği, çevirim içi işlem ve veri güvenliğin sağlanması halinde tüm dünyada yükselen bir trend olan dijital ekonomiden alacağı payın artacağının, GSYH (Gayri safi yurtiçi hasılası)'nın da yıllık 500 milyar Avro'ya ulaşabileceğinin bilincindedir. Ancak Eurobarometre'nin 2013 yılı anket sonuçlarına göre, Birlik vatandaşlarının neredeyse üçte biri internet üzerinden yapılan bankacılık ve e-ticaret işlemlerini, hem ödemelerin güvenliği, hem de kişisel verilerin korunması açısından yeterince güvenilir bulmamaktadır. Bu da Avrupa dijital tek pazarının gelişimini engelleyebilecek boyutta önemli bir güven sorunu ve dolayısı ile de pazarın gelişmesini önleyen bir engel oluşturmaktadır[94].

Siber güvenlik konusunda yasal ve teknik alt yapı çalışmaları yapmaya devam eden Birlik, bugün halen güncel olan ve vatandaşlarının haklarını koruyarak, interneti daha güvenli hale getirmeyi amaçlayan "*Siber Güvenlik Stratejisi*"ni[95] Şubat 2013'de ilan etmiştir. Birlik'in siber güvenlik vizyonunu ana hatlarıyla ortaya koyan

---

ENISA, "The European Cyber Security Challenge: Lessons Learned", **ENISA Report**, 2017, https://www.enisa.europa.eu/publications/the-european-cyber-security-challenge-lessons-learned-report (02.06.2020).

[93] Camille Marie Jackson, "Estonian Cyber Policy after the 2007 Attacks: Driven of Change and Factors for Success, New Voices in Public Policy", **George Mason University, School of Public Policy,** Cilt.7, Sayı.1, 2013, ss. 2-3, 7-10.

[94] Bu konuda daha fazla bilgi için bkz. European Policy Center, ss.4, 35; European Commission, Special Eurobarometer, "**Cyber Security Report",** 404, 2013, http://ec.europa.eu/commfrontoffice/publicopinion-/archives/ebs/ebs_404_en.pdf s.4 (02.06.2020).

[95] European Union, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", **JOIN 2013, 1 Final**.

bu Siber Güvenlik Stratejisi, ifade özgürlüğünün, mahremiyetin ve kişisel verilerin korunması gibi Birlik'in temellerinde yatan ve Avrupa Temel Haklar Şartı ile garanti edilen değerlerin[96], siber alana da uygulanması gerektiğinin altını kuvvetli bir şekilde çizmektedir. Bu Strateji ile, ayrıca, Birlik genelinde teknik alt yapı anlamında yeterli ve güvenli ağ bağlantılarının oluşturularak, bunların birlikte işlerliğinin gerçekleştirilmesinin, hızlı ve kolay erişilebilir internet bağlantısının yaygınlaştırılmasının da dijital tek pazarda kullanıcı güveninin artırılması bakımından önemli olduğu ortaya konmuştur. Strateji aynı zamanda, siber güvenliğe ilişkin alınacak topyekün tedbirler vasıtasıyla, siber tehditlere ilişkin tüm seviyelerde farkındalık yaratma ve basit korunma önlemleri alabilme konularında kullanıcılara yetkinlik kazandırma hususlarında kamu ve özel sektör temsilcileri de dahil her bir paydaşın ortak sorumluluğunun bulunduğunu da teyit etmiştir. Siber Güvenlik Stratejisi, ayrıca sınır ötesi nitelik taşıyan siber suç oranını azaltmak, ağ ve veri güvenliğini en üst seviyeye taşımak amacıyla, uyumlaştırılmış yasalarla tedbir alınmasının ve suçla etkili mücadelenin sağlanması için uluslararası seviyede koordinasyon ve işbirliğinin önemini de vurgulamaktadır[97].

Siber Güvenlik Stratejisi'nin ilanından hemen sonra Ağustos 2013'de, özellikle terörizm veya siyasi saiklerle, bilgi sistemlerine yapılan saldırılara ilişkin olarak suçların tanımlanarak yaptırımların uygulanmasına yönelik asgari standartların belirlenmesi ve Eurojust[98], Europol[99], ENISA gibi yetkili kurumlarla

---

[96] Lizbon Antlaşması möööööööö54ile, Avrupa Birliği Temel Haklar Şartı, atıf yoluyla, istisnasız bir bütün olarak tanınarak, hüküm altına alınmıştır. Böylelikle 2000 yılında gerçekleşen Nice Zirvesinde bir katalog olarak kabul edilen Temel Haklar Şartı, Lizbon Antlaşması'na yapılan atıf ile Birlik'in Kurucu Antlaşmalarıyla aynı hukuki değere sahip olarak bağlayıcı hale getirilmiştir. Bu yolla, Avrupa Temel Haklar Şartı'nın 8. maddesi kapsamında bir temel hak olarak tanınan "kişisel veriler" de Lizbon Antlaşması ile korunma imkanı bulmuştur.

[97] European Union, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", **JOIN 2013, 1**, **Final,** ss. 2-4, 7-9, 19-20;
European Commission, "E-commerce Action Plan 2012-2015, State of Play 2013", **SWD 2013, 153 final,** http://ec.europa.eu/information_society/newsroom/image/document/2017-4/130423_report-ecommerce-action-plan_en_42073.pdf (02.06.2020), s.20.

[98] Eurojust (European Union's Judical Cooperation Unit), birden fazla üye devleti kapsayan, sınır ötesi organize suç şebekeleri ve terörizmle mücadele konusunda üye devletlerin ulusal yetkili mercilerinin yüksek düzeyde adli koordinasyon ve işbirliği yapmalarına yardımcı olan ve merkezi Hague'da bulunan Avrupa Birliği Adalet ve İşbirliği Birimidir. Daha fazla bilgi için bkz. Eurojust, http://eurojust.europa.eu/Pages/home.aspx . (02.06.2020).

[99] Europol, Avrupa Birliği'nin kolluk kuvvetidir. Merkezi Hague'da bulunan Europol, üye devletler ve Birlik'le işbirliği halinde bulunan üçüncü ülkelerle birlikte- uyuşturucu trafiği ve para aklama, dolandırıcılık, kalpazanlık, silah kaçakçılığı, insan ticareti, çocuk pornosu gibi- sınırötesi organize suçlar, siber suçlar ve terörizm gibi ciddi konularla mücadele edilmesini destekler. Daha fazla bilgi için bkz. Europol, https://www.europol.europa.eu/about-europol . (02.06.2020).

işbirliğinin artırılmasına ilişkin "*2013/40 sayılı Direktif*[100]" kabul edilmiştir. *2013/40 sayılı* bu Direktif ile, üye devletler, daha aktif bir role bürünerek, bilgi sistemlerine yönelebilecek siber saldırılara karşı gerekli tedbirleri alma yükümü altına girmişlerdir.

Özetlemek gerekirse, gün geçtikçe artan ve çeşitlenen çevirimiçi ağ ve bilgi sistemlerine yönelik güvenlik ihlal ve tehditlerinin çokluğu, kullanıcıların güvenlik algılarını ve dolayısı ile de ticari faaliyetleri, olumsuz etkilemektedir. Dijital ekonomi sistemine ilişkin bu olumsuz algı, ekonomik faaliyetleri sekteye uğratarak maddi zararlara yol açmaktadır. Birlik içinde, üye devletlerin bu ihlal ve tehditlerle teknik ve yasal anlamda başa çıkabilme yetenek ve kapasiteleri ise farklılık göstermektedir. Yasal ve teknik anlamdaki bu farklılıklar, Avrupa dijital tek pazarındaki parçalı görünümü perçinlemektedir. Bu sebeple, çevirim içi ağ ve bilgi sistemleri ile verilerin güvenliğinin, tüm üye devletlerde uyumlu yasalar ve teknik standartlar çerçevesinde sağlanması, dijital dünyadaki her türlü ekonomik ve sosyal aktivitenin devamı, veri, mal, sermaye, hizmet ve kişilerin serbest dolaşımının sağlanması ve nihayetinde de Avrupa dijital tek pazarının aksamadan işleyebilmesi bakımlarından hayati önem arz etmektedir. Bu doğrultuda, olumsuzluklarla mücadele edip, mümkün olan en yüksek seviyede veri ve işlem güvenliğini sağlayabilmek için, Birlik tarafından belirlenecek ortak siber güvenlik politikaları ve Birlik düzeyinde uyumlaştırılmış yasalar ışığında, tüm üye devletlerin asgari güvenlik standartlarını sağlayarak, bu bağlamda bireyleri ve iş sahiplerini güvence altına alması önemlidir. Bunun bilinci ile, 2016 yılında, Birlik genelinde ağ, veri ve bilgi sistemlerinin yüksek düzeyde güvenliğinin sağlanması amacıyla, gerekli standartların belirlenerek, üye devletlerin bu bağlamdaki kapasitelerini artırıp, bu sistemler için ortak güvenlik önlemleri alınmasına ilişkin "*2016/1148 sayılı Direktif*[101]" kabul edilmiştir[102]. 2016/1148 sayılı bu Direktif'in pek çok bölümünde özel hayatın, iletişimin gizliliğinin, mahremiyetin ve kişisel verilerin korunmasının siber güvenliğin

[100] European Union, "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA", **OJ L 218**, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&rid=11 (02.06.2020).

[101] European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union", **OJ L 194,** 19.7.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1539674899977&uri=CELEX:32016L1148 (02.06.2020).

[102] 2016/1148 sayılı Direktif, Beyanlar (1-5), madde. 1,2.

sağlanması bağlamındaki öneminin altı açıkça çizilmiştir[103]. Konunun, dijital ekonomi ve neticede de Birlik'in nihai amacı olan akıllı, kapsayıcı ve sürdürülebilir büyümenin gerçekleştirilebilmesi bakımlarından önemi artık tartışmasız olarak kabul edildiğinden, çevirim içi ağ ve sistemlerde güvenliğin artırılmasına ve verilerin korunmasına yönelik çalışmaların yapılmasına bugün bile aralıksız olarak devam edilmektedir.

1.3.1.3. Sütun III: Dijital Ekonominin Büyüme Potansiyelini Artırma

Yakın gelecekte dijital ekonominin genel ekonomi içindeki payının en üst düzeye çıkacağının öngörülmesi sebebiyle, "*Avrupa için Dijital Tek Pazar Stratejisi*" ile, bireyselden tüzele, kamudan özel sektöre her alanda dijitalleşmeye ve dijital dünyaya uyuma ilişkin reformlar yapılmasına, eğitim ve farkındalık programları hazırlanılmasına odaklanılmıştır. Yapılacak reformların sağlayacağı ivmeyle, Birlik'in küresel düzeyde dijital dünyaya tam entegrasyonunun sağlanması hedeflenmektedir. Bu entegrasyonun tamamlanması neticesinde, hem Birlik vatandaşlarının, hem de özel teşebbüslerin, her geçen gün büyüyerek kapsamını genişleten dijital ekonomiden en üst seviyede ve kesintisiz olarak yararlanması sağlanabileceği öngörülmektedir[104].

Birlik'in genel anlamda dijital ekonomiye entegrasyon seviyesine bakıldığında, üye devletlerin ve Birlik içinde faaliyet gösteren teşebbüslerin farklı seviyelerde entegre oldukları görülmektedir. Örneğin, ticaretin dijitalleşmesi ve işletmelerin uyumu bağlamında, dijital ekonomiye en yüksek entegrasyonun Danimarka, Finlandiya, İrlanda, Belçika ve Hollanda'da gerçekleştiği görülmektedir. Romanya, Polonya ve Bulgaristan'da ise entegrasyon seviyesi oldukça düşüktür. Ayrıca 28 üye devlet bünyesinde faaliyet gösteren teşebbüslerin, sadece beşte biri yüksek dijitalleşme oranına sahipken, bu oran, Danimarka ve Hollanda'da yüzde kırka çıkmakta, Bulgaristan ve Romanya'da ise onda bir oranına kadar gerilemektedir[105]. Üye devletlerin ve Birlik içinde faaliyette bulunan özel

[103] 2016/1148 sayılı Direktif, Beyanlar (63,72,75) madde. 2,15/4.
[104] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.13-14.
[105] European Commission, "Integration of Digital Technology, Digital Economy and Society Index Report", 2018, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/4_desi_r-

teşebbüslerin, dijitalleşme sürecine uyum konusunda sahip oldukları farklı seviyeler göz önüne alındığında, Avrupa dijital tek pazarının parçalı görünümünün giderilerek, Birlik'in dijital ekonomiden alacağı payın artırılması için önünde uzun bir yol olduğu iyiden iyiye su yüzüne çıkmaktadır.

Birlik genelinde yasaların uyumlaştırılması ve teknik alt yapının tamamlanması çalışmalarıyla Avrupa dijital tek pazarının parçalı yapısına son verilerek pazarın büyüme potansiyelinin artırılması amaçlanmaktadır. Tüm bu çalışmaların yanında, dijital ekonomiye entegrasyonun sağlanması amacıyla, kamu ve özel sektör çalışanlarını kapsayan işgücü, araştırmacılar ve bilim insanları, özel sektör temsilcileri, tüketiciler ile öğrenciler de dahil tüm Birlik vatandaşlarının dijital okur yazarlığını ve dijital becerilerini artırabilmek de önemlidir. Beşeri sermayenin dijital ekonomiye entegrasyonu hedefi doğrultusunda oluşturulacak eğitim-öğretim programları sayesinde, bireylerin sadece eğitimleri süresince değil, mezuniyetlerinden sonra da dijital beceriler edinmeleri sağlanabilecektir. Böylelikle bireylerin dijital tek pazardan yararlanabilme ve bu sisteme entegre olabilme yetkinlikleri de artırılacaktır[106].

1.3.1.3.1. Avrupa Dijital Tek Pazarı ve Kişisel Olmayan Veriler

Küresel dijitalleşme sürecinde, veri, ekonomik büyüme, sosyal değişim, rekabet edebilirlik, yenilik (inovasyon) ve yeni iş fırsatları ortaya koyma hususlarında önemli bir kilit ekonomik değer haline gelmiştir. Bu yeni ekonomik değer, ticaret, finans, sigortacılık, reklam hizmetleri gibi geleneksel sektörler üzerinde olduğu kadar, sosyal ilişkilerimiz ve günlük hayatlarımızda da dönüştürücü bir etkiye sahiptir. Bu güçlü etki dolayısı ile, küresel veri ekonomisinin aktörü olma hedefi, Avrupa için Dijital Tek Pazar Stratejisi'nin önemli bir parçasıdır. Ancak Avrupa Birliği'nin henüz içinde barındırdığı veri potansiyelinden tam anlamıyla

---

eport_integration_of_digital_technology_B61BEB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf (02.06.2020), ss. 2-6.

[106] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.15-17;
European Commission, "Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A New Skills Agenda for Europe, Working together to strengthen human capital, employability and competitiveness", **COM (2016) 381 final,** 10.06.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0381 (02.06.2020).

yararlanabildiğini söylemek de doğru değildir. Bu durumun en önemli nedenlerinden biri, özellikle kamu tüzel kişileri, akademik çalışanlar ve araştırmacılar tarafından toplanan "*kişisel olmayan veriler*"in paylaşımının öneminin bu aktörler tarafından henüz anlaşılamamış olmasıdır. Özellikle kamu sektöründe çalışanların, kişisel olmayan verilerin etkin kullanımına ilişkin bilgi eksikliklerinin bulunması, elde bulunan bu gibi verilerin aktif kullanımını kısıtlar niteliktedir. Konuyu özel sektör açısından incelediğimizde ise, özellikle KOBİ'ler tarafından toplanan veya üretilen kişisel olmayan verilerin, bu işletmeler tarafından korunmaları gereken ticari bir varlık olarak görülmeleri sebebi ile, bu veriler üçüncü kişilerle paylaşılamamakta ve dolayısı ile de aktif olarak kullanılamamaktadırlar. Veri potansiyelinden yararlanılmasının önündeki tüm bu engellerin yanı sıra, kişisel olmayan verilerin, disiplinler ve sektörler arası paylaşımına ilişkin Birlik genelindeki teknik ve yasal alt yapı eksiklikleri de sistemin birlikte çalışabilirliğini etkilediğinden toplanan bu verilerden istenilen seviyede yararlanılamamaktadır. Üye devletler arasında da kişisel olmayan verilerin serbest dolaşımını engelleyici nitelikteki çeşitli bariyerler bulunmaktadır. Bu bariyerler sebebi ile de, tek pazarın bölünmüşlüğü perçinlenmekte ve bu parçalı yapı özellikle veri güdümlü bilimsel ve teknolojik gelişimi baltalamaktadır. Oysa ki, yasal sınırlar çerçevesinde toplanan, depolanan, paylaşılan ve analiz edilen "*kişisel olmayan verilerin (non-personal data)*" yeniden düzenlenip, yorumlanmasıyla yeni ve anlamlı veri ve bilgiler ortaya koyularak, yeni ürün ve hizmetler geliştirilmesi, Birlik'in veri ekonomisine entegrasyonu bakımından önemlidir. Birlik'in kişisel olmayan verilerden ekonomik değer elde etme hedefi kapsamında, "*big data, bulut bilişim, nesnelerin interneti (Internet of Things), yapay zeka (artificial intelligence) ve yüksek performanslı bilişim (high performance – technical- computing)*" gibi dijital kökenli teknolojilere teknik yatırımlar yapması, Birlik'in ekonomik geleceği için son derece hayatidir. Üye devletler tarafından, ekonomik bir değer olan bu verilerin hareketliliğinin önüne getirilen ve "*veri konum kısıtlamaları* (*data localisation restrictions*)" olarak adlandırılan coğrafi kısıtlamaların kaldırılarak, tıpkı diğer mal ve hizmetlerde olduğu gibi verilerin de Birlik içinde serbest dolaşımlarının sağlanması gerekmektedir. Zira bu kısıtlamalar şirketler, üniversiteler ve benzeri diğer araştırma enstitüleri arasında bilgi alışverişini engelleyerek, araştırma geliştirme faaliyetlerinin kısıtlamasına da neden

olabilmektedirler[107]. Örneğin, kişisel olmayan verilerin sınır ötesi hareketliliği sırasında bu verilere yapılabilecek olumsuz ve yetkisiz müdahale ihtimalinden doğan güven eksikliği, üye devletlerin, kendi vatandaşlarına ait kişisel olmayan verilerin, kendi sınırları içinde tutulmasına ilişkin olarak "veri konum kısıtlamaları" getirmelerine sebep olmaktadır. Bu saikle hareket eden üye devletlerin yaptıkları farklı nitelikteki veri konum kısıtlamaları, kişisel olmayan verilerin Birlik içerisindeki serbest dolaşımını engellemektedir. Ayrıca bu kısıtlamalar, hizmet sağlayıcıların verilerin saklanması ve işlenmelerine yönelik olarak, her üye devlette ayrı ayrı yapılanmalarını da zorunlu kılmıştır. Bu da hem maliyetleri artırarak, üye devletler bazında farklı maliyetlerin oluşmasına sebep olmakta, hem de bir ekonomik değer olan, kişisel olmayan verilerin Birlik içerisindeki serbest dolaşımlarını baltalayarak veri kökenli büyüme ve yeniliği engellemektedir. Tüm bu sebeplerle kamu güvenliğinin gerektirdiği durumlar hariç olmak üzere, kişisel olmayan verilerin hareketliliği önünde bariz bir engel oluşturan her türlü veri konum kısıtlamalarının kaldırılması, Birlik'in veri ekonomisine tam uyumunun sağlanarak kazanımlarının artırılabilmesi bakımından öncelikli konulardandır[108].

Kişisel olmayan veri hareketliliğini artırarak, bu veriler ile birlikte, özellikle Birlik destekli bilimsel araştırmalardan elde edilen çıktılardan en üst seviyede yararlanılmasının temini amacıyla Birlik tarafından uygulanmaya çalışılan "Açık

---

[107] "Kişisel olmayan veriler"den ayrı olarak "Kişisel veriler"in ise toplanması, depolanması, işlenmesi ve benzeri hususlar, bu çalışmanın ilerleyen kısımlarında detaylı açıklanacak özel yasal düzenlemelere tabidir. European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, s.14;
European Union, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "European Cloud Initiative – Building a Competitive Data and Knowledge Economy in Europe", **COM (2016) 178 final,** 19.4.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC-0178&from=en (02.06.2020) ss.3-5;
European Commission, "Shaping Europe's Digital Future, a European Strategy for Data", **Policy**, https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy (02.06.2020);
European Parliament, "Free Flow of Non-Personal Data in the European Union", **Briefing EU Legislation in Process,** https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614628/EPRS_BRI%282017%29614628_EN.pdf (02.06.2020);
European Union, "Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union", **Official Journal of the EU L 303/59,** 28.11.2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1544179728555&uri=CELEX:32018R1807 (02.06.2020), parag.1.

[108] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, s.14; European Union, "Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union", **Official Journal of the EU L 303/59**, parag.2-6, 13,18, 24.

Erişim Politikası (Open Access Policy)", kişisel olmayan verilere kolay ve ücretsiz bir şekilde ulaşılmasını öngörür. Açık Erişim Politikası, bu yolla, bilimsel araştırmaların ve ortaya konan sonuçlarının etkilerinin maksimize edilip, kişisel olmayan verilerin bilimsel amaçlarla yeniden kullanılarak, teknik ve bilimsel gelişmenin yüreklendirilip desteklemesini amaç edinmiştir. Bu politikayla paralel olarak oluşturulan "*Avrupa Birliği Açık Veri Portalı (European Union Open Data Portal)*" da, Birlik enstitü ve organları tarafından ortaya konan kişisel olmayan verilere, açık ve kolay erişim ile bu verilerin ücretsiz olarak yeniden kullanımının sağlanmasını hedeflemektedir [109] . Kişisel olmayan verilerin Avrupa dijital tek pazarında herhangi bir bariyerle karşılaşmadan serbest dolaşımlarının garanti edilmesinin akabinde, "*Açık Erişim Politikası (Open Access Policy)*" çerçevesinde, yeniden kullanımlarının sağlanmasıyla, bu verilerden yeni ekonomik değerler üretilerek, ekonomik büyümeye daha fazla katkıda bulunulacağına şüphe yoktur[110].

Kişisel olmayan verilerin serbest dolaşımlarının sağlanabilmesi bağlamında "*2018/1807 sayılı bir Tüzük[111]*" yürürlüğe girmiştir. 2018/1807 sayılı bu Tüzük, şeffaflık ve birlikte çalışabilirlik prensiplerini, Birlik düzeyinde uyumlu yasal düzenleme ve standartları içeren daha rekabetçi bir veri ekonomisine ulaşma hedefi doğrultusunda Birlik'in konuya yaklaşımını ortaya koyması bakımından önem arz etmektedir[112].

Verileri depolayan ve yöneten altyapı sistemleri ile verileri bir yerden başka bir yere taşıyan yüksek kapasiteye sahip ağlar ve verilerin işlenmelerinde kullanılan ileri teknolojiye sahip bilgisayar sistemlerinin birleşiminden meydana gelen "*bulut (cloud)*", verilerin sınırlar arası dolaşımını ve paylaşılarak yeniden kullanımını mümkün kılmaktadır. Bu bağlamda Avrupa için Dijital Tek Pazar Stratejisi'nin gerçekleştirilmesine yönelik önde gelen inisiyatiflerden biri de "*Bulut Bilişim İnisiyatifi (Cloud Initiative)*"dir. Bu İnsiyatif, kişisel olmayan veri akışının ve

[109] Avrupa Birliği Açık Veri Portalı'na ilişkin daha fazla bilgi için bkz. European Open Data Portal, http://data.europa.eu/euodp/en/home .

[110] European Commission, "Shaping Europe's Digital Future, Open Science", **Policy,** https://ec.europa.eu/digital-single-market/en/open-science (02.06.2020); European Commission, Directorate-General for Research & Innovation, "H2020 Programme, Guidelines to the rules on Open Access to the Scientific Publications and Open Access to Research Data in Horizon 2020", **H2020 Programme,** Version 3,2, 21.03.2017, https://ec.europa.eu/research/participants/data/ref/h2-020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf (02.06.2020), ss. 3-5.

[111] European Union, "Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union", **Official Journal of the EU L 303/59.**

[112] 2018/1807 sayılı Avrupa Birliği Tüzüğü, Madde 6.

paylaşımının artırılıp, veri ekonomisinin canlandırılması, açık erişim sistemi ile bu verilerin paylaşım ve yeniden kullanım oranlarının artırılarak, bilimsel ve teknik ilerlemenin sağlanabilmesi bakımlarından önemlidir[113].

Anılan çalışmalar ve politika uygulamaları neticesinde kişisel olmayan verilerin, menşeilerine bakılmaksızın üye devletler arası serbest dolaşımlarının ve yeniden kullanımlarının sağlanması, hem veri ekonomisinin canlanması, hem de Avrupa dijital tek pazarının parçalı görünümünden kurtularak aksamadan birlikte işlerliğinin ve ekonomik büyümenin gerçekleştirilmesi için gereklidir. Nitekim, Avrupa Parlamentosu'nun yayınladığı 2019 tarihli bir rapor kapsamında, Birlik düzeyinde tam olarak uygulanması halinde "Kişisel Olmayan Verilerin, Avrupa Birliği içerisindeki Serbest Dolaşımlarına ilişkin 2018/1807 sayılı Tüzük (*Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*)"ün Birlik ekonomisine getireceği faydanın yıllık 4.3 milyar Avro kadar olabileceği tahmin edilmektedir[114].

1.3.2. Avrupa Birliği'nde Kişisel Verilerin Korunmasının Önemi ve Boyutları

Avrupa Birliği'nde kişisel verilerin korunmasının öneminin hangi temellerden kaynaklandığı hususu çok boyutludur. Bu boyutlar, "*Dijital Teknoloji Boyutu*"; "*Veri Ekonomisi ile Dijital Tek Pazar Boyutları*"nı içeren "*Dijital Ekonomi Boyutu*"; ve son olarak da "*Demokrasi ve İnsan Hakları Boyutları*" olarak sıralanabilir. Birbirleriyle her anlamda çok sıkı ilişkiler içerisinde bulunan bu boyutların her biri Birlik için ayrı ayrı önemlidir.

[113] European Union, "European Cloud Initiative – Building a Competitive Data and Knowledge Economy in Europe", **COM (2016) 178 final**, ss.2-3.

[114] European Parliament, "Contribution to Growth: The European Digital Single Market, Delivering Economic Benefits for Citizens and Businesses", Policy Department for Economic, Scientific and Quality of Life Policies, by authors: J.Scott Marcus, Dr.Gerorgios Petropoulos, Dr.Timothy Yeung, **Study,** January 2019, Table 1, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/631044/IPOL_STU(2019)631044_EN.pdf (02.06.2020) s.10.

Tablo 1: Kişisel Verilerin Korunmasının Öneminin Boyutları

	KİŞİSEL VERİLERİN KORUNMASININ ÖNEMİNİN BOYUTLARI
A.	Dijital Teknoloji Boyutu
B.	Dijital Ekonomi Boyutu
B.1.	Veri Ekonomisi Boyutu
B.2.	Dijital Tek Pazar Boyutu
C.	Demokrasi ve İnsan Hakları Boyutu

Kişisel verilerin korunmasının önemine ilişkin olarak yukarıdaki 1 numaralı Tablo'da belirtilen boyutlar, işbu tez çalışmasının genelinde detaylı olarak ele alınmakla birlikte, ilgili boyutları bir kere de bu bölümde kısaca açıklayarak konuya giriş yapmakta fayda vardır.

Bilgi ve iletişim teknolojilerindeki gelişmeler, hem dünyayı birbirine çok daha fazla bağlı ve birbirinden haberdar hale getirmiş, hem de küreselleşme akımlarının dijitale evrilmesine sebep olmuştur. Bu dijital devrim, küresel ekonomik yarışın da klasik mal-hizmet ticareti ve sermaye hareketliliğinden ziyade, bilgi ve iletişim teknolojisi temelli, katma değerli ve inovatif ürünlere doğru kaymasına yol açmıştır. Bu gelişmelere paralel olarak da küresel ekonomik savaş, dijital alana taşınıp sertleşmiştir. 20. yüzyılın ikinci yarısından itibaren ise, hayatın kamusal ve özel tüm alanlarında hızla artan dijitalleşme, ortaya çıkan bu dijital ortamda çeşitli tipte kişisel verilere tahminlerin çok ötesinde bir kolaylıkla erişilerek, bunların toplanma, işlenme ve depolanmalarına ilişkin devrim niteliğindeki gelişmeleri de beraberinde getirmiştir. Bilgi ve iletişim teknolojilerinde yaşanan gelişmelerin genel olarak insan hayatının her alanına yaptığı bu gibi dönüştürücü etkilerin yanı sıra, yaygınlaşan internet uygulamalarının da etkisi ile sınır ötesi veri ve bilgi akışı da artarak, bu veri ve bilgilerin yayılımı kolaylaşmış, bu bağlamda bir temel hak olan kişisel verilerin korunması da aynı oranda zorlaşmıştır. Kişisel verilerin korunmasının önemi ve konunun temelleri çok eskilere dayanmakla birlikte, her alanda yaşanan dijitalleşmenin ortaya koyduğu risklerin farkında olan Avrupa Birliği için, kişisel verilerin korunması hususu, bilgi ve iletişim teknolojileri ile internet

kullanımında yaşanmakta olan gelişmeler sebebiyle "*Dijital Teknoloji Boyutu*" kapsamında daha da öncelikli hale gelmiştir.

Bilgi ve iletişim teknolojileri ile internet kullanımında yaşanan bu gelişmeler, kişisel verilerin korunmasının önemini artıran "*Dijital Ekonomi Boyutu*" nu da ön plana çıkarmıştır. Diğer bir ifade ile, dünyayı her geçen gün biraz daha sıkı sarmalayan ve ülkeleri, bölgeleri, toplumları, insanları birbirlerine daha çok bağlı ve birbirinden haberdar hale getiren dijital ağlar, küreselleşme hareketlerini de yaşanan bu gelişmelerle uyumlu olarak dijitalleştirmektedir. Dijital küreselleşme de, son zamanlarda adını daha sık duymaya başladığımız bilgi ve teknoloji temelli bir ekonomi sistemi olan "*veri ekonomisi*"ne dönüşüm sürecini tetiklemiştir. Veri ekonomisinin temelleri, ekonomik bir değer olduğu günümüzde artık genel kabul gören verilerin toplanıp, işlenip, depolanarak, ekonomik, siyasi ve sosyal pek çok faaliyet kapsamında kullanılıp, bunlardan ekonomik fayda sağlanmaya çalışılmasına dayanmaktadır. Veri ekonomisinin hammaddesi haline gelmesi sebebiyle de günümüzde verilerin ekonomik değeri her geçen gün artmaktadır.

Kişisel verilerin korunması hususu, Dijital Teknoloji Boyutu ile Dijital Ekonomi Boyutu birlikte göz önüne alınarak daha detaylı incelenecek olursa, tüm dünyanın 7/24 kesintisiz veri akışı sağlayan çevirim içi ağ örgüsü tarafından çepeçevre sarıldığı söylenebilir. Sarmal haline gelen bu çevirimiçi ağ örgüsü, daha önce hiç olmadığı kadar fazla artan hacim ve çeşitlilikte verinin, sınırlar ötesi hareketliliğine imkan verebilmektedir. Bu ağlar üzerinden işlem yapan kullanıcılar ise her an çevirimiçi sisteme kişisel ve kişisel olmayan verilerini içeren dijital ayak izlerini bırakmaktadırlar. Bırakılan bu izlerin, yüksek teknolojik sistemler ve yapay zekalar tarafından işlenmesiyle, veri ekonomisi kapsamında ekonomik değeri olan yeni veri ve bilgi kümeleri ortaya çıkmaktadır[115].

Ekonomik değer üretmede kullanılan verilerin miktarı artıkça üretilen çıktıların miktar ve kalitesi de artmaktadır. Bu sebeple, veri toplama, işleme ve depolama süreçlerini ve verilerin çıktılarını elinde tutarak, kontrol edebilen kişi, kurum, kuruluş ve ülkeler, dünya üzerindeki ekonomik, sosyal ve siyasal gücü de

[115] McKinsey Global Institute, "Digital Globalization: The New Era of Global Flows", March 2016, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx, (02.06.2020.) s.8.

yönetebilmektedirler. Gelişmiş ülkeler ve çok uluslu şirketler dijital küreselleşmenin nimetlerinden yararlanma konusunda günümüzde de başı çekmektedirler. Ancak, küreselleşmenin dijitalleşmesi ve veri ekonomisi sayesinde, yükselen ekonomiler ile birlikte az gelişmiş bölgeler de dahil dünyanın herhangi bir yerinde bulunan yeni kurulmuş küçük işletmeler ile bireysel girişimlerin dahi, bu küresel akış ağına katılarak, gelişmiş ülkelerle rekabet edebilme şansları bulunmaktadır. Diğer bir deyişle, bilgi ve iletişim teknolojilerine yaptığı yatırımlarla dijital dönüşümü gerçekleştirerek, dijital teknolojileri ve bunlar vasıtasıyla toplanan verileri hedefleri doğrultusunda etkin kullanabilen ve böylelikle bilgi toplumuna dönüşümü ve veri ekonomisine adaptasyonu sağlayabilen her ülke, kurum, kuruluş ve bireyin, dijital küresel akışa katılarak, bu akıştan faydalanma ve rekabet edebilme imkanı vardır. Ayrıca, içinde bulunduğumuz dijital çağda, veri, potansiyel müşteri eğilimlerinin belirlenerek, kişiselleştirilmiş ürün/hizmet ortaya konulması; düşük maliyetli ve en avantajlı üretim yerinin ve hammaddenin nereden, ne kadara tedarik edilebileceği gibi rekabet edebilirliğin ve pazar payının artırılması ile yeni pazarlara ulaşılması için önemli olan hususlarda da belirleyici bir unsur haline gelmiştir. Dijitalleşmeye ve veri ekonomisine uyumun sağlayacağı ekonomik avantajlara bir diğer örnek olarak da, kişiye özel yenilikçi hizmet ve ürünlerin ortaya konulması, doğrudan kullanıcıların ilgi alanlarını hedefleyen dijital reklamcılık[116] faaliyetlerinin mümkün hale gelmesi, üçüncü şahıslara istatistiksel olarak anlam ifade edebilecek verilere erişim olanağı vermesi sayılabilir[117].

Her geçen gün derinleşen, genişleyen ve etkilerini artıran küreselleşmenin bu dijital formunun ve veri ekonomisinin, küreselleşme sürecinin bundan sonraki liderlerinin kimler olacağından, ticari rekabetin hangi ürün ve hizmetler kapsamında yapılacağına, işlem maliyetlerine ve neticede de dijital küreselleşme sonucu ortaya

[116] Klasik reklamcılık modeline, hatırı sayılır bir şekilde, ölçülebilirlik ve doğrudan hedefleme niteliklerini kattığı söylenebilen dijital reklamcılık, günümüzde pek çok farklı yöntem kullanılarak gelişmeye devam etmektedir. Bu yöntemlerden en önemlilerinden biri de çevirim içi davranışsal reklamcılıktır. İnternet ve akıllı cihazların kullanımı sonucu dijital ortamda bırakılan ayak izleri ve diğer veriler analiz edilerek elde edilen bilgiler doğrultusunda reklamcılık faaliyetlerinin kişiselleştirilerek iletilmesi anlamına gelen çevirim içi reklamcılık faaliyetleri hakkında daha fazla bilgi için bkz. Leyla Keser Berber, **Çevirimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması**, XII Levha Yayınları, 2014, I. Baskı.

[117] Rob van der Dam, ss. 1-2; Baker & McKenzie, "Ghosts in the Machine Revisited the State of Artificial Intelligence, Risks and Regulation in Financial Services", http://www.euromoneythoughtleadership.com/ghosts2/, s.3.

çıkan faydalardan en çok kimlerin yararlanacağına kadar pek çok konuyu yeniden şekillendirdiği söylenebilir[118]. Tüm bu anılan noktalar bir arada incelendiğinde, ortaya dijital sisteme giren verilerin, kişisel ve kişisel olmayan veriler şeklinde ayrımının yasalar kapsamında doğru bir şekilde yapılarak, veri ekonomisinin ortaya koyduğu süreçlerde, verilerden ekonomik fayda elde edilmesi kapsamında kişisel verilerin korunmasının önemi ortaya çıkmaktadır.

Kişisel verilerin korunmasının önemini ortaya koyan Dijital Ekonomi Boyutunun bir diğer alt boyutu da "*Dijital Tek Pazar Boyutu*"dur. Bir ekonomik entegrasyon modeli olarak yola çıkan Avrupa Birliği'nin en önemli kuruluş motivasyonlarından biri tek pazarın oluşturularak, yasal ve teknik yapılanmasının tamamlanmasıdır. Tamamlanmış bir Avrupa tek pazarının sadece Birlik içi ticarette dahi 500 milyon kişiye[119] ulaşabilme kapasitesi ile dünyanın en büyük yekpare pazarlarından biri olacağı unutulmamalıdır. Tek pazarın niteliği gereği içinde barındırdığı bu büyük ticari potansiyel sebebiyle, dijitalleşme sürecine ve veri ekonomisine uyum sağlayarak Avrupa dijital tek pazarının da oluşumunu tamamlamak, Birlik için atılması gereken önemli adımlardan biridir. Zira Birlik, dijital tek pazarın tamamlanmasına ilişkin hedeflerini, bugüne kadar yayınlamış olduğu çeşitli strateji belgeleri kapsamında da pek çok defa ortaya koymuştur.

Yasal ve teknik alt yapı çalışmalarının tamamlanmasıyla oluşturulacak yekpare bir Avrupa dijital tek pazarının, Birlik ekonomisine yılda tahmini 415 milyar Avro katkıda bulunarak, Avrupa vatandaşlarına da bu bağlamda yeni iş imkanları sağlayarak ekonomik büyümeye katkıda bulunacağı öngörülmektedir[120]. Bu noktada, veri ve işlem güvenliğinin sağlanarak, oluşumu tamamlanacak güvenilir ve güvenli bir Avrupa dijital tek pazarında, tüketici ve şirketlerin, işlem yapmaya ikna edilmesi önemlidir. Kişisel verilerin güvenliği ile işlem güvenliğinin Birlik içinde uyumlu yasa ve teknik düzenlemelerle, en üst düzeyde sağlandığı bir ortamda ise birey ve şirketlerin, dijital teknolojileri kullanarak dijital tek pazar üzerinden işlem yapmaya ikna edilebilmelerinin kolaylaşacağına şüphe yoktur. Bu sebeplerle, BİT'ler konusundaki yatırımların artırılarak, uyumlaştırılmış yasal düzenlemeler kapsamında

[118] McKinsey Global Institute, 2016, ss. Preface, In Brief, 2, 5, 8-9, 23, 28; James G.McGann, s.15.
[119] Eurostat Statistics, "Demographic Balance", 2018, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Demographic_balance,_2018_(thousands).png, (02.06.2020).
[120] European Commission, "The EU and The Digital Single Market", **EU Publications.**

alınacak tedbirlerle, dijital tek pazarda güvenliğin sağlanmasının, pazarın fiziksel olmayan bölünmüşlüğünün ve tarife dışı ticaret engellerinin ortadan kaldırarak, pazarın birlikte işlerliğinin gerçekleştirilmesinin, hem Avrupa dijital tek pazarının parçalı yapısının ortadan kaldırılmasının, hem de sürdürülebilir, akıllı ve kapsayıcı büyümenin ve sosyal refahın anahtarı niteliğinde olduğu söylenebilir[121]. Bu noktada kişisel verilerin haiz oldukları nitelikleri gereği korunmalarının, Dijital Tek Pazar Boyutu kapsamında, pazarın tamamlanması, tüketici güveninin yükseltilerek, işlem hacminin artırılması açılarından özel önem arz ettiğinin altını bir kere daha çizmek gerekmektedir. Bu durum tek başına dahi, dijitalleşmeye uyum sağlanarak, Birlik düzeyinde yapılacak yasal ve teknik düzenlemeler neticesinde Avrupa dijital tek pazarının tamamlanmasının önemini gösterir niteliktedir.

Tüm bu kazanım beklentilerine karşın, kişisel verilerin, sosyal medya platformlarından alışverişe ve vergi işlemlerine kadar benzeri pek çok alanda kullanılması yoluyla, ağ üzerinden dijital sisteme girmeleri, pek çok riski de beraberinde getirmiştir. Bu risklere örnek olarak, gün geçtikçe daha fazla gelişen, bilgi ve iletişim teknolojileri sebebiyle, ağda toplanan verilerin hacim ve çeşitliliğinin tahminlerin çok ötesinde artarak, kişisel ve kişisel olmayan nitelikteki bu verilere üçüncü kişiler tarafından erişilebilirliğin ve bu verilerin üçüncü ülkelere aktarım oranlarının yükselmesi gösterilebilir. Bu durum, Birlik hukukunda temel haklar kapsamında korunan kişisel verilerin, yetkisiz erişim, aktarım ve ihlallere, siber saldırılara, veri korsanlığına maruz kalmalarını kolaylaştırarak, neticede mahremiyet ve temel hak ihlalleri sebebiyle de veri süjelerinin zarar görmelerine sebep olabilmektedir[122].

Tüm bu avantaj ve risklerin farkında olan Avrupa Birliği de, dijital dönüşümünü tamamlayarak oluşturacağı yekpare bir Avrupa dijital tek pazarı vasıtası ile, küresel rakipleriyle daha iyi rekabet ederek dijital ekonomiden alacağı

---

[121] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, s. 3;
European Parliament, "The Ubiquitous Digital Single Market, Fact Sheet on the European Union", ss.1-2;
H.Banu Yılmaz, s.35;
European Commission, "Digital Agenda for Europe, Rebooting Europe's Economy", **EU Publications**, s.3;
Max Heermann, s.9.

[122] Rob van der Dam, ss. 1-2; Baker & McKenzie, "Ghosts in the Machine Revisited the State of Artificial Intelligence, Risks and Regulation in Financial Services", s.3.

payı artırmayı hedeflerken, aynı zamanda da, Birlik'in etik temellerini oluşturan temel hak ve özgürlüklerin dijitalleşme sonucu ortaya çıkan bu yeni riskler karşısında daha iyi korunabilmesinin de yollarını aramaktadır. Zira Avrupa Birliği, ekonomik fayda elde etme saikinin, hiç bir zaman temel hak ve özgürlüklerin korunması hedefinin önüne geçmemesi gerektiği gerçeğinin farkında olarak yoluna devam ederek bu uğurda gereken tedbirleri de almaya çabalamaktadır. Bu çabaların da kişisel verilerin korunmasının öneminin bir diğer boyutu olan "*Demokrasi ve İnsan Hakları Boyutu*"nu oluşturduğu söylenebilir.

BİT'lerdeki önlenemeyen gelişmeler ile Avrupa Birliği'nin dijitalleşme ve veri ekonomisi bağlamındaki küresel rekabetin dışında kalamayacağı hususları ile birlikte kişisel verilerin korunmasının içerdiği özel önem tüm boyutları ile birlikte göz önüne alındığında, kişisel verilere erişimin, üye devletler düzeyinde yapılacak ulusal yasal düzenlemelerle etkili bir şekilde durdurulamayacağı Birlik tarafından anlaşılmıştır. İşte tam da bu noktada kişisel verilerin güçlü ve uyumlu Birlik yasaları dahilinde korunmasının önemi ortaya çıkmaktadır. Bu bağlamda, Birlik'in etik değerlerinin dayanağını oluşturan temel hak ve özgürlükler, ilke ve değerler dikkate alındığında, kişisel verilerin etkili bir şekilde korunabilmesi için gereken yasal ve teknik önlemlerin alınarak, Birlik genelinde uyumlaştırılmış yasal düzenlemeler yapılmasının, Avrupa Birliği için öncelik arz ettiği yadsınamaz.

Avrupa Birliği, tüm bunların bilinciyle veri ekonomisine adapte olarak Avrupa dijital tek pazarının oluşumunu tamamlamaya çalışırken, aynı zamanda da, Avrupa'yı Avrupa yapan insan onurunun, temel hak ve özgürlüklerin, demokrasi ve hukukun üstünlüğünün her ne pahasına olursa olsun korunması ilkelerine bağlı kalma ve dolayısıyla da kişisel verilerin korunmasına dair kararlılığını koruyarak, bu uğurda çeşitli yasal düzenlemeler yapmaya çalışmaktadır[123]. Bu nedenlerle gelecekte

[123] Küreselleşme hareketlerinin oluşturduğu akış ağı içerisindeki yüz otuz bir ülkenin birbirleriyle ticari mal, hizmet ve veri entegrasyonu ile finansal ve sosyal entegrasyon seviyelerini ölçen "Bağlantı Endeksi"ne göre, miktar ve çeşitlilik bağlamında küresel akış oranının yukarı seviyelere doğru ivme kazanması, ülkelerin GSYİH'nı artırarak, refah seviyelerinin yükselmesine katkıda bulunmaktadır. Bu araştırma, ülkelerin küresel akışa ne kadar çok entegre olup, katılım sağlayabilirlerse, küreselleşmenin nimetlerinden o kadar fazla yararlanarak, ekonomik ve sosyal gelişim gösterebildiklerini ortaya koyması bakımından incelenmeye değerdir. Daha fazla bilgi için bkz. McKinsey Global Institute, "Global Flows in a Digital Age: How Trade, Finance, People and Data connect the World Economy", April 2014, https://www.mckinsey.com/~/media/mckinsey/-featured%20insights/Globalization/Global%20flows%20in%20a%20digital%20age/MGI%20Global%20flows%20in%20a%20digial%20age%20Executive%20summary.ashx (02.06.2020), ss.2-6; James G.McGann, ss.10, 13-16.; Baker & McKenzie, "Ghosts in the Machine Revisited the State of

de kişisel verilerin Birlik düzeyinde uyumlu yasalar dahilinde yüksek standartlarda korunup, dijital küreselleşmeye ve veri ekonomisine adaptasyon ve katılımı en üst düzeyde sağlayarak, fırsatlardan yararlanabilmek için, Birlik'in bu bağlamdaki eksikliklerini tespit ederek, bunların giderilmesi doğrultusunda, gerekli teknik ve yasal alt yapı çalışmalarını yapmaya devam etmesi gereklidir. Alt yapı çalışmaları, kısa dönemde zor ve masraflı gibi gözükse de, dijital küreselleşme sürecinde, veri ekonomisinin nimetlerinden yararlanarak rekabet edebilirliği artırmak adına, Birlik için uzun dönemde başarının anahtarı niteliğindedir[124]. Diğer bir ifade ile, yasal ve teknik düzenlemelerin tamamlanması, Birlik'in küresel ekonominin dijitalleşerek yeniden tanımlandığı veri ekonomisi döneminde, pek çok alanda rakipleri ile rekabet ederek, küresel "*oyun kurucu*" olma iddiasını sürdürebilmesi ve tamamlanmaya çalışılan Avrupa dijital tek pazarının parçalı görünümünden kurtulabilmesi için de önemli ve belirleyicidir. Kişisel verilerin uyumlu yasalar doğrultusunda korunacağı bu yasal ve teknik düzenlemeler, Birlik genelinde, yeknesak uygulamalar kapsamında şeffaflığı, hukuki öngürülebilirliği, istikrarı ve güvenilirliği artıracaktır. Böylelikle de Avrupa dijital tek pazarının yekpareliği perçinleneceğinden, ticaret hacmi yükselecek bu da neticede ekonomik ve sosyal büyümenin önünü açacaktır. Bu sebeplerle, kişisel verilerin korunması hususu, Avrupa 2020 Stratejisi ile Avrupa için Dijital Tek Pazar Stratejisi'nin ana merkezinde yer alan hususlardan biridir[125].

Tüm bu unsurlar birlikte değerlendirildiğinde, kişisel verilerin korunması bağlamında, üst düzey teknolojiler ve uyumlu yasalarla Birlik genelinde kişisel veri güvenliğinin tüm boyutlar kapsamında sağlandığı yekpare bir çevirim içi alana sahip olmanın, Birlik açısından, Avrupa dijital tek pazarının ve dolayısı ile de veri ekonomisinin gelişimi için gerekli bir ön koşul niteliğinde olduğu bir kere daha

---

Artificial Intelligence, Risks and Regulation in Financial Services", ss. 5-6; McKinsey Global Institute, 2016, ss. Preface, In Brief, 2, 5, 8-9, 23, 28; ; T.C. Kalkınma Bakanlığı, **2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı**, Yayın No.2939, 2015, ISBN NO. 978-605-904153-9, https://abdigm.meb.gov.tr/projeler/ois/004.pdf , ss.10,16.

[124] Baker & McKenzie, "A Changing World: New Trends in Emerging Market Infrastructure Finance", https://www.bakermckenzie.com/en/insight/publications/2018/12/emerging-market-infrastructure-finance (02.06.2020), ss.3-6, 9; Rob van der Dam, ss. 1-2; Baker & McKenzie, "Ghosts in the Machine Revisited the State of Artificial Intelligence, Risks and Regulation in Financial Services", s.3.

[125] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.12-13; Baker & McKenzie, "A Changing World: New Trends in Emerging Market Infrastructure Finance", ss.3-6, 9.

anlaşılmaktadır[126]. Ancak yapılan araştırmalara göre, Birlik içerisinde dijital ağ üzerinden işlem yapan yahut yapabilecek kapasitede olan pek çok kullanıcı, çevirim içi işlemleri yeterince güvenli bulmamaktadır. Veri ekonomisinden yüksek bir pay alabilmek için kişisel veri güvenliğini sağlayarak, Avrupa dijital tek pazarında işlem yapan kullanıcılar gözünde tek pazarın güvenilirliğini artırması gerektiği gerçeğinin farkında olan Birlik, kişisel verilerin korunmasına ilişkin mevzuatın Birlik genelinde uyumlaştırılmasına yönelik pek çok düzenleme yapmış ve yapmaya da devam etmektedir[127].

[126] Digital Europe, "A Transformational Agenda For The Digital Age: Digital Europe's Vision 2020", **White Paper**, ss. 18-19, 63, 67.
[127] Baker & McKenzie, "Ghosts in the Machine Revisited the State of Artificial Intelligence, Risks and Regulation in Financial Services", ss.17-18; European Union, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", **JOIN 2013, 1 Final,** ss.2-3.

İKİNCİ BÖLÜM
AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

İşbu tez çalışmasının İkinci Bölüm'ü başlığı altında kişisel verilerin korunmasının hangi temellere dayandığı, kişisel veri kavramı ve sınırları ile kişisel verileri korumanın Avrupa kıtasındaki tarihsel yolculuğu incelendikten sonra, 2018 yılında yürürlüğe giren 2016/679 sayılı Genel Veri Koruma Tüzüğü'ne gelene kadar, Birlik hukukunda kişisel verilerin korunmasına ilişkin yasal mevzuata yer verilmeye çalışılacaktır.

2.1. KİŞİSEL VERİLERİN KORUNMASININ TEMELLERİ

Tez çalışmasının ana temalarından birini oluşturan kişisel verilerin korunması konusunun temelleri, kişilik hakkına kadar uzanmaktadır. Bu sebeple kişisel verilerin korunması kavramının detaylarına geçmeden önce, kişilik hakkının tanımlanarak kapsamının belirlenmeye çalışılması önemlidir.

Kişilik hakkı, kişinin sadece "*var olması*" sebebiyle doğal olarak, vazgeçilemez, devredilemez ve zamanaşımına tabi olmayacak bir şekilde sahip olduğu, şahsa sıkı sıkıya bağlı, tekelci (inhisari) bir mutlak haktır. Mutlak hak olması dolayısı ile herkese karşı ileri sürülebilen kişilik hakkı, bireyin ölümüyle sona ereceğinden, hakkın kendisi, miras bırakılamayıp, parayla ölçülemeyeceği gibi icra takiplerine de konu olamaz. Bu hak, bireyi, maddi ve manevi anlamda çok yönlü bir varlık olarak kabul eder. Bu bağlamda da, kişilik hakkı, bir bütün olarak bireyin kendi özünden kaynaklanarak kişiliğini oluşturan yaşam hakkı, onuru, saygınlığı, beden bütünlüğü/sağlığı, özel hayatı, mahremiyeti, konut dokunulmazlığı, ekonomik özgürlüğü gibi kişilik değerlerini koruyarak, kişiliğini serbestçe geliştirmesini sağlayan hakların bütünü olarak da tanımlanabilmektedir. Bu tanımdan da anlaşılabileceği gibi, kişisel veriler kapsamında korunan değerler, kişilik hakkının korunması kapsamında değerlendirilen şeref ve onur, özel hayat ve benzeri kişilik değerlerinin korunması ile doğrudan ilgili ve bağlantılıdır[128].

[128] Aydın Zevkliler, Mehmet Beşir Acabey ve K.Emre Gökyayla, **Medeni Hukuk, Giriş, Başlangıç Hükümleri, Kişiler Hukuku**, **Aile Hukuku**, 6.Baskı, Seçkin Yayınevi, Ankara, 2000, ss. 399-400;

Yasa koyucular, tıpkı kişisel veri kavramını tanımlarken olduğu gibi, kişilik hakkını tanımlarken de sınırlayıcı olmaktan kaçınarak, bu hakkın kapsamında korunan hak ve değerleri tahdidi bir şekilde saymayı tercih etmemişlerdir. Bunun yerine, bireyin kişisel değerlerine ilişkin olan kişilik hakkının kapsamını geniş yorumlayıp, bu hakkı, kişinin toplum içindeki varlığını ve saygınlığını korumasına, kişiliğini serbestçe geliştirmesine imkan veren her türlü konuyu kapsayacak şekilde koruma altına almayı tercih etmişlerdir. Bu sebeple de somut olayın özelliklerine göre, kişinin onur, saygınlık gibi değerlerine zarar verecek ve/veya bunları ortadan kaldıracak nitelikteki her türlü maddi-manevi saldırılar, kişilik hakkına saldırı niteliğinde kabul edilerek, yasaların sağladığı korumadan yararlanabilmektedir. Böylelikle, herhangi bir eksik tanımın, kısıtlayıcı etkisinden uzak olarak, kişilik ve onu oluşturan tüm değerlerin bir bütün olarak, kendiliğinden kişilik hakkına sağlanan yasal korumadan yararlanması sağlanmıştır. Kişilik hakkına hukuka aykırı bir şekilde saldırıda bulunulduğunu iddia eden kişi, yargı yoluna giderek, hukuka aykırı ve kişilik hakkına saldırı niteliğinde olduğunu iddia ettiği herhangi bir eyleme karşı korunma talebinde bulunabilir[129].

Kişilik hakkının kapsamı, literatürde genelde maddi, manevi değerler ile manevi ekonomik değerler başlıkları altında incelenmektedir. Burada sayılanlarla sınırlı olmamak kaydı ile, kişinin yaşamı, beden bütünlüğü, bedensel ya da ruhsal sağlığı *maddi nitelikteki değerler*ine; insan onuru ve saygınlığı, özgürlük ve güvenlik alanı, aile ve özel hayatı, kişinin adı-soyadı, resim ve sesi, giz alanı, his dünyası *manevi değerler*ine; ekonomik özgürlüğü ve varlığı, ticari ve mesleki saygınlığı,

---

Fikret İlkiz, Barış Günaydın, "Kişilik Hakları, Medyada Etik ve Yargı Kararları", **Küresel İletişim Dergisi**, Sayı.2, 2006, s.2; Muhammet Sabır Fırat, Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu, **Hacettepe Hukuk Fakültesi Dergisi**, Cilt: 5, Sayı: 2, 2015, ss.107,108; Kemal Atasoy, "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası", **Marmara Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof.Dr. Cevdet Yavuz'a Armağan, Cilt 22, Sayı 3, 2016, ss.271-272, 275-276; Johann Neethling, "Personality Rights: A Comparative Overview", **The Comparative and International Law Journal of Southern Africa**, Cilt.38, Sayı.2, 2005, ss. 210-213.

[129] Çiğdem Ayözger, **Kişisel Verilerin Korunması-Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, 1. Baskı, Beta Yayınları, 2016, İstanbul, ss.45-46;
Semih Güner, Sır Saklama Yükümlülüğü, **Ankara Barosu Dergisi**, Sayı. 3, 2000, ss.43,44.
Pınar Bahar Doğan, "Çatışan İki Değer: Haber Verme Hakkı ve Kişilik Hakkı", **Ankara Barosu Dergisi**, Sayı.4, ss.481-482;
Fikret İlkiz, Barış Günaydın, s. 2.

mesleki ve ticari sırları ise *manevi ekonomik değerleri*ne örnek olarak gösterilebilir[130].

2.1.1. Kamu Hukukunda Kişilik Hakkı ve Kişisel Verilerin Korunması

Kişilik hakkı, kamu hukukuna insan hak ve özgürlükleri olarak yansıyarak, bu kapsamda korunma altına alınmaktadır. Bu bağlamda kendisi de bir temel hak olan kişisel veriler de kamu hukukunda, insan hak ve özgürlükleri kapsamında tanımlanarak koruma altına alınmıştır[131].

Demokratik bir hukuk devletinde, kişilik hakkı ve insan hak ve özgürlükleri bağlamında kişisel verilerin, daha güçlü olan kamu otoritesine karşı korunması sureti ile, bireyler, kişiliklerini serbestçe geliştirip, benliklerini koruyarak, kendi hayatlarına ve kişiliklerine kendileri yön verebilmektedirler. Kişisel verilerin kamu hukuku kapsamında korunması ise ancak, bu verilerin hukuka aykırı ve sınırsız bir şekilde toplanıp, saklanarak işlenmesi ve kullanılmasının engellenerek, bu hususlarda, devlet egemenliğinin yasalar çerçevesinde sınırlandırılması ile mümkün olabilir. Birlik hukukuna baktığımızda, kişisel verilerin kamu hukuku çerçevesinde korunmasının kaynağının da, İnsan Hakları Evrensel Beyannamesi, Avrupa İnsan Hakları Sözleşmesi, Avrupa Birliği Temel Haklar Şartı ve insan hakları alanında temel ilkelerin belirlenerek aktarıldığı Kurucu Antlaşmalar ile üye devletlerin anayasaları ve anayasal haklara paralel olarak getirilen ulusal mevzuatları olduğu anlaşılmaktadır. Zira insan hak ve özgürlükleri, Birlik'in temellerini oluşturarak Kurucu Antlaşmalarla koruma altına alındığı gibi, bizzat üye devletlerin kendi ulusal mevzuatlarıyla da korunmaktadır. İçinde bulunduğumuz dijital küreselleşme sürecinde, kişisel verilerin toplanıp işlenmelerinin kolaylaştığı da göz önüne alındığında, uyumlu Birlik yasaları dahilinde bu verilerin korunmasının önemi daha da fazla ortaya çıkmaktadır[132].

---

[130] Aydın Zevkliler, Mehmet Beşir Acabey, K.Emre Gökyayla, ss. 402-406, 407-416 ,423-425.
[131] Johann Neethling, s.211.
[132] Pınar Bahar Doğan, ss. 481-484;
Human Rights Watch (HRW), "The EU General Data Protection Regulation", **HRW Questions and Answers**, 06.06.2018, https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation (02.06.2020); Lee A. Bygrave, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, **International Journal of Law and Information Technology**, Cilt.6, Sayı.3, ss. 247-249; Fred H. Cate, "The EU Data Protection Directive, Information, Privacy and the Public Interest",

2.1.1.1. İnsan Hakları Temelinde Kişisel Verilerin Korunması

İnsan hakları, kökenleri insan onuru ve saygınlığına dayanan, tüm insanların doğuştan sahip oldukları ve ideal olarak her bireye ayrım gözetmeksizin, eşit olarak tanınması gereken haklar bütünüdür. Nitelikleri itibarı ile bu haklar, devlet erkinin ve egemenliğinin sınırlandırılmasını gerektirir ve hukukun üstünlüğü ilkesi kapsamında korunurlar[133].

İnsanlık tarihinde, yasalar önünde eşitlik ve demokrasi kavramlarının kökleri çok eskilere kadar uzanmaktadır. Zira bu kavramlar, Konfüçyüs öğretisi etkisi altındaki Çin'de, Moğol yönetimindeki Hindistan'da, Endülüs dönemi Arap medeniyetlerinde ve Antik Yunan'da önemli çıkışlar yapmışlardır[134]. Daha sonra ise, Roma dönemi boyunca geliştirilip, yazıya dökülerek yasalarla korunmaya çalışılmışlardır. Tarihte insan hak ve özgürlüklerinin gelişimi konusundaki en önemli sıçramalar, 18. yüzyılda ABD'de yaşanan gelişmeler ve bu gelişmelerin akabinde kabul edilen Bildirgeler[135] ile yaşanmıştır. Yayınlanan bu Bildirgelerle, bütün insanların eşit doğarak, varoluşlarından kaynaklanan vazgeçilemez ve devredilemez haklara sahip oldukları kabul edilmiştir. İnsan hakları kavramının uluslararası genel kabul görerek, evrensel boyuta ulaşmasında ise, 1789 Fransız Devrimi'nin ardından gelen "*Fransız İnsan ve Vatandaş Hakları Bildirgesi*"nin önemi büyüktür[136].

Modern çağda yaşanan iki büyük dünya savaşı sırasında ise, insan hakları kavramının gelişimi büyük sekteye uğramıştır. Özellikle İkinci Dünya Savaşı'nda

---

Articles by Maurer School of Law: Indiana University, Paper 646, 1995, ss. 431-432, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1647&context=facpub (02.06.2020); Spiros Smitis, "Reviewing Privacy in an Information Society", **University of Pennsylvania Law Review**, Cilt 135, 1987, ss.708-709, 730, 746.

[133] United Nations, General Assembly, **Universal Declaration of Human Rights**, 1948, http://www.verklaringwarenatuur.org/Downloads_files/Universal%20Declaration%20of%20Human%20Rights.pdf ; Bahri Savcı, "İnsan Hakları Üzerine Uluslararası Alanda, Norm İlkeler ve Türk İç Hukuku", **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Cilt.35, Sayı 1, 1980, , s.8; Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması (Unutulma Hakkı ve Biyometrik Veriler İlaveli)**, 2.Baskı, Beta Yayınları, İstanbul, 2016, s.79.

[134] Daha fazla bilgi için bkz. Micheline R. Ishay, **The History of Human Rights: From Ancient Times to the Globalization Era**, 2.Baskı, University of California Press, 2008, ss.64-68.

[135] Daha fazla bilgi için Bkz. Virginia Haklar Bildirgesi, 1776, https://tr.wikisource.org/wiki/Virginia_İnsan_Hakları_Bildirgesi (02.06.2020) ve Amerikan Bağımsızlık Bildirgesi, 1778, https://tr.wikisource.org/wiki/Amerikan_Bağımsızlık_Bildirgesi (02.06.2020)

[136] Hilal Sanioğlu, "Avrupa Birliği Hukukunda İnsan Hakları", **Türkiye Barolar Birliği Dergisi**, Sayı.74, 2008, ss.77-111, s.78.

yaşanan savaş suçları ve soykırım sebebiyle, insan onuru büyük darbe yemiştir. Bu sebeple, insan onurunu gelecekte meydana gelebilecek muhtemel zararlardan koruyabilmek adına, dünya devletleri, Birleşmiş Milletler çatısı altında bir araya gelerek, 10 Aralık 1948 tarihinde gerçekleşen Genel Kurul'da, "*İnsan Hakları Evrensel Beyannamesi (Universal Declaration of Human Rights)* [137] "ni ilan etmişlerdir. Böylece, herhangi bir ayrım yapmadan tüm bireylerin insan olmalarından kaynaklanan, vazgeçilemez ve devredilemez nitelikteki hak ve özgürlüklerinin varlığı ve bu hakların üçüncü kişilere karşın korunmasının gerekliliği kabul edilerek, hüküm altına alınmıştır. Bu Beyanname'nin önemi, felsefi temelli düşünce tarihinde yüzyıllardır insanın salt insan olması sebebiyle, doğası gereği ve istisnasız olarak doğuştan sahip olduğuna inanılan, doğal bir hak olan insan hak ve özgürlüklerinin, dünya üzerindeki tüm insanlar ve uluslar için geçerli olacak ortak değerler ile ideal ölçütler kapsamında derlenip ilk kez bir uluslararası metin ile ortaya konulmasından gelmektedir [138] . Ancak bu Beyanname, hukuki anlamda "tavsiye" niteliğinde olduğundan, hukuken bağlayıcılığı yoktur. Buna paralel olarak da beraberinde herhangi bir yaptırım mekanizması da getirmemiştir[139]. Tüm bunlara rağmen, "*İnsan Hakları Evrensel Beyannamesi*", insan hakları kavramının küresel anlamda gelişimi bakımından çok önemli bir adım niteliğindedir. Nitekim, o tarihten bu yana, uluslararası toplumu temsilen Birleşmiş Milletler Genel Kurulu tarafından kabul edilen bu değer ve ölçütlerin, tüm dünyada benimsenip uygulanmalarını sağlamak amacıyla, ulusal ve uluslararası düzeyde çok çeşitli yasa, mekanizma ve uygulamalar ortaya konulmaya çalışılmaktadır[140].

İnsan Hakları Evrensel Beyannamesi'nin kabulü her ne kadar bağlayıcı nitelik taşımasa da, Beyanname ile ilan edilen ilke ve idealler, özellikle Avrupa ülkeleri

---

[137] Birleşmiş Milletler, Genel Kurulu, **İnsan Hakları Evrensel Beyannamesi**, 1948, https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf (02.06.2020).

[138] Jack Donnelly, Human Rights as Natural Rights, Human Rights Quarterly, **Johns Hopkins University Press,** Cilt. 4, Sayı.3, 1982, ss. 391, 395, 398, 401;
Laura-Cristiana Spataru-Negura, Cornelia Lazar, "Lifting the Veil of the GPPR to Data Subjects", Challenges of the Knowledge Society, Public Law, **Nicolae Titulescu University**, 2018, ss. 658, http://cks.univnt.ro/articles/12.html (02.06.2020).
Sanioğlu, s.78.

[139] Rona Aybay, "Açıklamalı İnsan Hakları Evrensel Bildirisi", **Türkiye Barolar Birliği Yayınları**, No. 113, Türkiye Barolar Birliği İnsan Haklan Araştırma ve Uygulama Merkezi dizisi: 7, Ankara, 2006, http://tbbyayinlari.barobirlik.org.tr/TBBBooks/iheb.pdf (02.06.2020), s.6.

[140] United Nations, **Universal Declaration of Human Rights**, (Illustrations by Yacine Ait Kaci), 2015, http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf , (02.06.2020).

arasında büyük kabul görmüştür. Bu ilkelerin kabulünü takiben dünyada barış ve adaletin tesisi ile hukukun üstünlüğünü hakim kılmak amacıyla, 1949'da kurulmuş hükümetlerarası bir kuruluş olan Avrupa Konseyi'ne üye devletler, daha ayrıntılı ve bağlayıcı bir metnin hazırlanması için harekete geçmişlerdir. İnsan hak ve özgürlüklerinin tanınıp korunarak geliştirilmesi ve kurulacak yaptırım mekanizmaları ile korunması fikrinden hareketle, Avrupa Konseyi tarafından hazırlanan "*Avrupa İnsan Hakları Sözleşmesi (European Convention on Human Rights)* [141]" 20 Mart 1950 tarihinde imzalanmıştır. Bu Sözleşme'nin kabulünün akabinde de, uygulanmasını garanti altına almak amacıyla, 1959 yılında Avrupa Konseyi'ne bağlı uluslararası bir mahkeme olan ve merkezi Strazburg'da bulunan, "*Avrupa İnsan Hakları Mahkemesi (European Court of Human Rights)*" kurulmuştur.

"İnsan Hakları Evrensel Beyannamesi" ve "*Avrupa İnsan Hakları Sözleşmesi"* metinleri incelendiğinde ise, bu metinlerde kişisel verilerin korunmasına dair özel bir düzenlemenin bulunmadığı görülmektedir. Bu metinler kapsamında kişisel veriler, genel anlamda insan onuru ve saygınlığının, mahremiyetin, özel hayatın ve aile hayatının, haberleşmenin korunması ilkeleri bağlamında değerlendirilerek korunmaktadırlar. Zira bu haklar, aynı kökenden kaynaklanmakta ve neticede insan onurunun ve bireyin özel alanının korunarak, mahremiyetinin güvence altına alınmasını, böylelikle de kişiliğini ve düşüncelerini serbestçe geliştirebilmesini sağlamayı hedeflemektedirler [142] . Avrupa İnsan Hakları Mahkemesi'nin kişisel verilerin korunması hususunda verdiği pek çok karar, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde düzenlenen "*Özel Hayatın ve Aile Hayatının Korunması*" ilkesine dayandırılmıştır[143].

---

[141] Council of Europe, **European Convention on Human Rights**, 1950, https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c (02.06.2020);
Avrupa İnsan Hakları Sözleşmesi 18.Mart.1954 tarihinde Türkiye Cumhuriyeti tarafından da onaylanmıştır.

[142] İnsan Hakları Evrensel Beyannamesi, madde 12, "Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz kalamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır.";
Avrupa İnsan Hakları Sözleşmesi, Özel Hayatın ve Aile Hayatının Korunması başlıklı, madde 8/1, "Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir."
European Union Agency for Fundamental Rights, **Handbook on European Data Protection Law**, Luxembourg, 2018, https://www.echr.coe.int/Documents/Handb-ook_data_protection_02ENG.pdf (02.06.2020), ss.18-19.

[143] T.C. Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü, İnsan Hakları Dairesi Başkanlığı, Basın Birimi, **Kişisel Verilerin Korunması-Tematik Bilgi Notu**, 2015, http://inhak.adalet.gov.tr/inhak_bilgi_bankasi/tematik_bilginotu/bilgi/Protection%20of%20personal%

2.1.1.2. Avrupa Birliği'nde Temel Haklar ve Kişisel Verilerin Korunması

Üye devletler, 1950'li yıllardan itibaren Avrupa Konseyi üyelikleri sebebi ile, münferiden Avrupa İnsan Hakları Sözleşmesi'ni kabul etmek suretiyle, devlet gelenekleri, uygulamaları ve ulusal yasaları aracılığıyla insan haklarına saygıyı büyük oranda prensip edinmişlerdir. Ancak Avrupa Topluluğu'nun kuruluşuna temel olan ve Topluluk çatısı altında öncelikle ekonomik bütünleşmeyi hedefleyen Kurucu Antlaşmalardan, ne Avrupa Kömür Çelik Topluluğu Anlaşması'nda, ne de Roma Antlaşması ile Avrupa Atom Enerjisi Antlaşması'nda temel haklara ilişkin açık ve özel bir düzenlemeye yer verilmemiştir. Üye devletler, öncelikli bulunan ekonomik bütünleşme hedef ve kaygıları sebebiyle olsa gerek, siyasal ve kültürel bir temeli olan insan hak ve özgürlüklerinin, Topluluk müktesebatında bizzat yer alması fikrinden, Topluluğun kuruluşunun ilk dönemlerinde uzak kalmışlardır. Yasal düzenlemelerdeki bu eksikliklere rağmen, özellikle 60'lı yıllardan itibaren, insan hakları ihlallerine yönelik davalar, Avrupa Adalet Divanı'nın gündeminden hiç düşmemiştir. Topluluk düzeyinde insan haklarının korunmasının önemi, Adalet Divanı'nın, bu konuda yazılı Birlik müktesebatındaki eksiklik sebebi ile, başlarda takındığı çekimser tavırlarına rağmen, zaman içinde aldığı çeşitli kararlar aracılığıyla, vurgulanarak kabul edilmiştir. Adalet Divanı'nın aldığı bu kararlar neticesinde de, temel hakların tanınarak korunmasının, Topluluk hukukundaki yeri sağlamlaşmıştır. Adalet Divanı'nın insan hak ve özgürlüklerine ilişkin olarak aldığı çeşitli kararların ise, ileriki yıllarda Avrupa Temel Haklar Şartı'nın oluşturulmasına zemin hazırladığı söylenebilir. 2000'li yıllara gelene kadar bu konuda Topluluk müktesebatında görülen eksikliğe rağmen, insan haklarının üye devletlerin kendi ulusal uygulamaları, yasa ve anayasaları ile devlet anlayışlarındaki yeri ve öneminin, yok farzedilemeyeceğinin ise altını çizmek önemlidir[144].

20data%20(kişisel%20verilerin%20korunması).pdf (02.06.2020); European Union Agency for Fundamental Rights, **Handbook on European Data Protection Law,** 2018, ss.15-17, 23.

[144] Didem Saygın, "Avrupa Birliği'nde Temel Haklar: ABAD İçtihatları Üzerinden Bir Değerlendirme", **International Conference on Awareness**, Poland, 2017, https://www.researchgate.net/publication/3-22952247_AVRUPA_BIRLIGI'NDE_TEMEL_HAKLAR_ABAD_ICTIHATLARI_UZERINDEN_BIR_DEGERLENDIRME (02.06.2020) ss. 42-44,48;
Işıl Karakaş, "Ulusalüstü Anayasada Temel Haklar Problematiği: Teorik ve Pratik Sorunlar", **Anayasa Yargısı Dergisi**, Cilt.22, 2005, s.292;

Topluluğun sadece bir ekonomik bütünleşmeden ibaret olmadığının ve kökenleri Avrupa kültür mirasına temel teşkil eden eski Yunan ve Roma İmparatorluğu'na dek uzanan ortak değer ve kültürel bağlardan oluşan bir "*Avrupalılık kültür ve idealinin*" etrafında birleşildiğinin ispatı niteliğindeki Avrupalılık kimliğinin oluşumunda da insan hak ve özgürlüklerinin etkisi büyüktür. Avrupalılık kimliğinin temellerini oluşturan Avrupa ortak kültürel mirasının önemi, 1992 tarihli Maastricht Antlaşması ile yapılan düzenleme kapsamında da açıkça ortaya konmuştur[145]. Ayrıca Maastricht Antlaşması (Avrupa Birliği Antlaşması) madde 6[146]'da özgürlüğe, demokrasiye, insan hakları ve temel özgürlüklerle hukukun üstünlüğüne saygının, Birlik hukukunun temel ilkeleri olduğunun da altı çizilmiştir. Bu gelişmelerden hemen sonra kabul edilen, 1993 tarihli Kopenhag Siyasi Kriterleri vasıtası ile de Avrupa Birliği, sadece ekonomik bir birleşme değil, aynı zamanda siyasi, sosyal ve kültürel temel ve amaçları olan bir bütünleşme olduğunu adeta ilan etmiştir. Bu Kriterlerle, "*demokrasiye, hukukun üstünlüğüne, insan hakları ve azınlık haklarına saygının*" Avrupalılık kültürünün ve dolayısı ile de kimliğinin bir parçası olarak, Birlik'in "*sine qua non (olmazsa olmaz)*" ortak değerlerini oluşturduğunun altı önemle çizilmiştir. Böylelikle Birlik'in gerek iç, gerekse de dış ilişkilerinde, demokrasiye, hukukun üstünlüğüne ve insan haklarına bağlılığın, esaslı koşul teşkil ettiği açıkça benimsenerek kabul edilmiştir. Avrupalılık kültürünü yansıtan ortak değerlerin Kopenhag kriterleri kapsamındaki ilanının ardından, 1997 Amsterdam Antlaşması ile de üyelik koşulları değiştirilmiştir. Bu değişiklik ile eklenen "*...demokrasiye, insan haklarına saygılı...*" her Avrupa devleti üyelik için başvurabilir ibaresiyle de "*demokratik koşulluluk ilkesi*" getirilerek, Avrupalılık kültürüne, kimliğine, insan haklarına ve ortak değerlere vurgu yapılmıştır[147].

Tüm bu gelişmeler neticesinde, üye devletler, Birlik'in ortak etik değerlerini yansıttığı fikrinden hareketle, Avrupa İnsan Hakları Sözleşmesi ile tanınan temel hak

---

Hakan Taşdemir ve Arif Bağbaşlıoğlu, "Avrupa Birliği Hukuk Düzenindeki İnsan Hakları Anlayışına Avrupa Birliği Temel Haklar Şartının Getirdikleri", **Gazi Üniversitesi İİBF Dergisi**, Cilt.9, Sayı.3, 2007, ss. 22,23.

[145] Monica Sassatelli, "Imagined Europe: The Shaping of a European Cultural Identity Through EU Cultural Policy", **European Journal of Social Theory,** Cilt.5, Sayı. 4, 2002, ss. 435-440.

[146] European Union, **Treaty on European Union**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT (02.06.2020).

[147] Frank Schimmelfenning, Stephan Engert, Heiko Knobel, "Costs, Commitment and Compliance: The Impact of EU Democratic Conditionality on Latvia, Slovakia and Turkey", **Journal of Common Market Studies**, Cilt. 41, Sayı.3, 2003, ss. 495-498, 501.

ve özgürlükleri, kapsamlı bir metin altında toplayıp geliştirerek, Birlik hukuku kapsamında da güvence altına alma ihtiyacı duymuşlardır. Bunun için atılan en önemli adım, hazırlanan "*Avrupa Temel Haklar Şartı (Charter of Fundamental Rights of European Union)* [148] "nın 2000 yılında Fransa'da gerçekleşen Nice Zirvesi'nde bir katalog olarak ilanıdır. İlk ilan edildiği dönemde hukuken bağlayıcı olmayan bu Katalog, daha sonra 01 Aralık 2009 tarihinde yürürlüğe giren Lizbon Antlaşması kapsamında yapılan atıfla bağlayıcılık kazanmıştır. Bu atıfla, Avrupa Temel Haklar Şartı, tıpkı Birlik'in Kurucu Antlaşmaları gibi, Avrupa Birliği hukukunun birincil kaynakları arasına girmiştir. Ayrıca Avrupa Adalet Divanı'nın insan haklarının korunması hususundaki içtihatlarının, bugünkü gelişmişlik düzeyine ulaşmasında, Temel Haklar Şartı'nın Birlik düzeyinde kabulünün de etkili olduğu söylenebilir[149].

Kişisel verilerin korunması hususu, Temel Haklar Şartı'nın 8.maddesi ile ilk kez, ayrıca ve açıkça bir temel hak ve özgürlük olarak düzenlenerek koruma altına alınmıştır. Böylece Birlik hukukunda, önceleri Avrupa İnsan Hakları Sözleşmesi'nin "*Özel Hayatın ve Aile Hayatının Korunması*" başlıklı 8. Maddesi ile özel hayatın gizliliği temelinde korunan kişisel veriler, Avrupa Temel Haklar Şartı'nın kabulü ile bu Şart'ın "*Kişisel Verilerin Korunması*" başlıklı 8. maddesi[150] kapsamında özel olarak düzenlenerek korunmaya başlanmıştır.

Kişisel verilerin korunması hususu, Avrupa Birliğinin İşleyişine Dair Antlaşma'nın 16. maddesi kapsamında da, özel bir başlık altında ayrıca düzenlenmiştir[151]. Hem Avrupa Temel Haklar Şartı, hem de Avrupa Birliğinin İşleyişine Dair Antlaşma'daki bu düzenlemeler, Birlik hukukunda kişisel verilerin korunmasına verilen değeri vurgulamaları açısından önemlidirler.

---

[148] European Union, **Charter of Fundamental Rights of European Union**, 2000/C, 364/01,18.12.2000, http://www.europarl.europa.eu/charter/pdf/text_en.pdf (02.06.2020).

[149] T.C. Avrupa Birliği Bakanlığı, **Avrupa Birliği Müzakere Sürecinde Yargı ve Temel Haklar Faslı**, Avukatlar için Yargı ve Temel Haklar Projesi**,** 013, Ankara, ss.32-37.

[150] Avrupa Temel Haklar Şartı, Kişisel Verilerin Korunması, madde 8, " *1.Herkes kendisine ilişkin kişisel verilerin korunmasını isteme hakkına sahiptir.*

2. Bu tür veriler belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes kendisi hakkında toplanmış olan verilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.

3. Bu kurallara uyulması bağımsız bir makam tarafından denetlenecektir."

[151] European Union, **Consolidated Version of The Treaty on the Functioning of the European Union**, OJ 2010/C, 83/01, 30.03.2010, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2010:083:FULL&from=EN (10.08.2020).

2.1.1.2.1. Avrupa Birliği'nde Temel Hak ve Özgürlüklerin Teorik Kökenleri

Avrupa Birliği'nde temel hak ve özgürlüklerin tarihsel gelişiminin ardından, konunun teorik kökenlerine de değinmekte fayda vardır. Avrupa bütünleşme sürecini, Wiener ve Diez'in de dediği gibi tek bir büyük teori ile açıklayabilmek mümkün değildir. Bu yazarların görüşleri kapsamında, bütünleşme süreci bir mozaiğe benzetilecek olursa, her bir teori, mozaiğin ancak bir parçasını açıklayarak bütünü oluşturabilir [152] . Aynı doğrultuda, Avrupa Birliği'nde temel hak ve özgürlüklerin gelişimini ve bütünleşme sürecindeki yolculuğunu da tek bir teori üzerinden açıklayabilmek mümkün değildir. Tıpkı bütünleşmenin kendisi gibi, Avrupa Birliği'nde kişisel verilerin korunmasının da dahil olduğu temel hak ve özgürlüklerin gelişim sürecini de farklı teorilerle açıklamak mümkündür.

Ekonomik bir hareket olarak başlayan Avrupa bütünleşmesinin zaman içinde siyasal alana yayılıp, politik konuları da kapsayıp dönüştürmeye başlamasında olduğu gibi, temel hak ve özgürlüklerin Birlik genelinde her alanda gün geçtikçe biraz daha fazla özümsenerek korunması da Ernest Haas'ın öncülüğünde gelişen "*neo-fonksiyonalizm*" kapsamındaki "*fonksiyonel yayılma etkisi*" ile açıklanabilir. Nitekim Birlik'in temellerinin dayandığı Avrupalılık kültürü ile etik değer ve ilkelerden kaynaklanan temel hak ve özgürlükler, zamanla etkilerini artırıp yayılarak, Birlik'in gelenek ve tutumları ile kurum ve kararlarını da dönüştürmüşlerdir[153].

Kurucu Antlaşmalarda, temel hak ve özgürlüklere ilişkin henüz açık bir düzenlemenin olmadığı erken dönemlerde dahi, Adalet Divanı'nın temel hak ve özgürlüklerin korunmasına ilişkin olarak almış olduğu kararlar doğrultusunda, Birlik kurumlarının ve üye devletlerin tavır, tutum, uygulama ve davranışlarını değiştirdikleri görülmüştür. Adalet Divanı tarafından verilen kararlar kendi aleyhlerine dahi olsa Birlik kurumlarının ve üye devletlerin bu kararlarla uyumlu davranış geliştirmeleri de "*Rasyonel Tercihli Kurumsalcılığa*" göre açıklanabilir. Zira buna göre, Birlik düzeyinde üye devletlerin rasyonel iradelerini kullanmaları

[152] Antje Wiener, Thomas Diez, "Introducing the Mosaic of Integration Theory", **European Integration Theory**, (Ed. Antje Wiener, Thomas Diez**)** 2.baskı, Oxford University Press, 2009, ss.19-20.

[153] Arne Niemann, Philippe C.Schmitter, "Neofunctionalism", **European Integration Theory** (Ed. Antje Wiener, Thomas Diez), 2.baskı, Oxford University Press, 2009, s.47.

neticesinde kabul edilen normlar ve oluşturulan kurumlar, zaman içinde devletlerin beklenti, tutum ve davranışlarını kısıtlamak suretiyle değiştirebilmektedirler[154]. Ayrıca bir önceki bölümde de belirtildiği gibi 1997 Amsterdam Antlaşması ile, Birlik'e yeni üye alımına ilişkin olarak, demokratik koşulluluk ilkesi getirilmiştir. Demokrasiye, hukukun üstünlüğüne, insan hak ve özgürlüklerine bağlılığın, yeni üye alımına ilişkin temel stratejilerden biri olarak Topluluk tarafından vurgulanması ile getirilen bu koşulluluk ilkesinin, aday ülkeler üzerindeki dönüştürücü etkileri de "*Rasyonel Tercihli Kurumsalcılık*" kapsamında değerlendirilebilinir[155].

İçinde bulunduğumuz sosyal çevre, bizim kim olduğumuzu belirlemede büyük oranda etkilidir. İşte bu noktadan hareket eden, "*sosyal inşaa*", üye devletlerin özgür iradeleri ile yetki devri yapmalarıyla ortaya çıkan kurumlar ile oluşturulan normların ve üye devletler arasında kurulan sosyal ilişkiler sebebiyle oluşan etkileşimin, sosyal inşaa süreci kapsamında, devletlerin tutum, davranış ve bağlılıklarını şekillendirerek değiştirdiğini iddia eder. Avrupa bütünleşme sürecinde sosyal inşaanın etkilerinin en net görüldüğü alanlardan biri, Avrupalılık ideali ve dolayısı ile de Avrupalılık kimliği çerçevesinde demokrasiye, hukukun üstünlüğüne ve insan hak ve özgürlüklerine bağlılığın, üye ve aday devletler tarafından benimsenmesi sürecidir. Diğer bir ifade ile, sosyal inşaa, Avrupa bütünleşme sürecini açıklarken ortaya koyduğu gibi, ajan ve yapılar arasında ortaya çıkan sosyal öğrenme, üye ve aday devletler tarafından, Avrupalılık kimliğinin ayrılmaz parçaları olan demokrasiye, hukukun üstünlüğüne ve insan haklarına bağlılık ilkelerinin özümsenerek benimsenmesi sonucunu doğurmaktadır[156]. Oluşan bu bağlılıkların da Avrupa Temel Haklar Şartı'nın oluşturularak, atıf yoluyla Lizbon Antlaşması'na dahil edilmesi ve bu yolla Avrupa Birliği Kurucu Antlaşmaları bünyesine girip, Birlik için olmazsa olmaz bir nitelik kazanmasındaki katkısı yadsınamaz. Bu durum, Birlik'in, kişisel verilerin korunmasının da dahil olduğu temel hak ve özgürlüklere bağlılığının

---

[154] Mark A.Pollack, "The New Institutionalisms and European Integration", **European Integration Theory** (Ed. Antje Wiener, Thomas Diez), 2.baskı, Oxford University Press, 2009, ss. 134-135;
Sinem Akgül Açıkmeşe, "Uluslararası İlişkiler Teorileri Işığında Avrupa Bütünleşmesi", **Uluslararası İlişkiler Dergisi**, Cilt. 1, Sayı.1, 2004, ss. 20-22.

[155] Ulrich Sedelmeier, "Europeanisation in New Member and Candidate States", **Living Reviews in European Governance**, Cilt. 6, Sayı. 1, 2011, ss.14-15;
Mark A.Pollack, s.136.

[156] Thomas Risse, "Social Constructivism and European Integration", **European Integration Theory** (Ed. Antje Wiener, Thomas Diez), 2.baskı, Oxford University Press, 2009, ss.145-148, 151-152;
Ulrich Sedelmeier, s. 11;
Sinem Akgül Açıkmeşe, ss.24-27.

güçlenerek, bu hak ve özgürlüklerin zamanla Avrupalılık kimliğinin ve etik değerlerinin ayrılmaz bir parçası haline gelmesinde sosyal inşaacı yaklaşımın ne denli önemli olduğunu gözler önüne sermektedir.

Avrupa Birliği hukuku, Birlik'in kuruluşundan itibaren temellerini dayadığı yapı taşlarını oluşturan demokrasi, hukukun üstünlüğü, ahde vefa, insan haklarına saygı gibi temel değerler ve bu temel değerlerden Adalet Divanı tarafından türetilen ilkeler ile, bu ilke ve değerler doğrultusunda alınan Divan kararları üzerine inşa edilmiştir. Birlik hukuku, niteliği gereği, Avrupa Birliği'nin sahip olduğu uluslar üstü kurumlar ve bağımsız karakterdeki yargı organı Adalet Divanı sebebiyle, uluslararası hukuktan farklı, kendine özgü (*sui generis*) bir yapıya sahiptir. Bu özgün yapı gereği, Adalet Divanı'nın vermiş olduğu bağımsız kararlarla, bu kararlar bağlamında zamanla ortaya koyduğu ilkelerin, üye devletler ve üye devlet mahkemeleri tarafından benimsendiği gözlemlenmektedir. Özellikle üye devlet mahkemelerinin Adalet Divanı kararlarına göndermeler yaparak, bu kararlar doğrultusunda hareket ettikleri görülmektedir. Bu sebeple, Birlik hukuku zamanla Birlik'in en istikrarlı yapılarından biri haline gelerek, Avrupa bütünleşmesi sürecine önemli katkılarda bulunmuştur. En başından itibaren Birlik tarafından benimsenen etik değerlerden biri olan, "*İnsan hak ve özgürlüklerine saygı ilkesi*" de, Adalet Divanı'nın 1969 tarihli Stauder kararı ile Birlik Hukukunun ayrılmaz bir parçası olarak nitelendirilmiştir. Alınan bu karar kapsamında, Komisyon da dahil tüm Birlik kurumlarının insan hak ve özgürlüklerine saygı çerçevesinde hareket etmelerinin gereği açık bir şekilde ortaya konmuştur[157]. Diğer bir ifade ile, üye devletlerin sahip oldukları farklı ulusal çıkarlara rağmen, üye devlet mahkemeleri Adalet Divanı kararları doğrultusunda hareket ederek, Avrupa Birliği hukukunun en önemli yapı taşlarından biri olarak kabul edilen insan hak ve özgürlüklerinin vazgeçilmez nitelikte olduğunu kabul ederek, Temel Haklar Şartı'nın, atıf yoluyla Lizbon Antlaşmasına dahil edilmesinden önceki dönemlerde dahi, bu yöndeki Adalet Divanı kararlarına uygun hareket etmişlerdir. Tüm bu hususlar bir arada değerlendirildiğinde, temel hak ve özgürlüklerin, Birlik'in Adalet Divanı kararları ve yasal düzenlemeleri vasıtasıyla, hukuk yoluyla bütünleşmesinin en önemli ayaklarından birini oluşturmaktadır. Özetle, Adalet Divanı'nın temel haklara saygılı

[157] Gülören Tekinalp ve Ünal Tekinalp, **Avrupa Birliği Hukuku**, 2.Baskı, Beta Yayınları, İstanbul, 2000, s. 755.

bir hukuk düzeni kurma çabaları kapsamında aldığı çeşitli kararları ile ortaya koyduğu insan hak ve özgürlüklerinin korunması ilkesinin, bu bağlamda Avrupa Birliği bütünleşmesinin asli unsurlarından birini oluşturduğu ve Hukuk Yoluyla Bütünleşmenin de temellerinden biri olduğu söylenebilir[158].

2.1.2. Özel Hukuk Alanında Kişilik Hakkı ve Kişisel Verilerin Korunması

Kişilik hakkının korunmasının çıkış noktası, birey karşısında açık ara daha kuvvetli bulunan devletin, kişiye zarar vermesini engelleyecek şekil ve oranda, iktidarının sınırlandırılarak, kişinin devlet karşısında saygınlığını koruyup, benliğini geliştirebilme özgürlüğünü elde edebilmesidir. Bu sebeple, kişilik hakkı ilk etapta devlete karşı kamu hukuku kapsamında korunmuştur[159]. Ancak zamanla kişinin toplum içinde etkileşimde bulunduğu üçüncü kişilerin sayısının artarak, karşılıklı olarak kurulan sosyal ilişkilerin çeşitlilik kazanması neticesinde, üçüncü kişilerden kaynaklanan hak ihlallerinin çoğalması, bireylerin üçüncü kişilere karşı da korunması ihtiyacını ortaya çıkarmıştır. Bu ihtiyaç, özellikle İkinci Dünya Savaşı sonrasında arttığından, kişilik hakkının korunması konusu, kamu hukukunun yanı sıra özel hukuk alanının da kapsamına girmiştir[160]. Kişilik hakkının özel hukuk alanına yansıması da yine insan hak ve özgürlüklerinin korunması temelinde ortaya çıktığından, Birlik hukukunda bir temel hak olarak kabul edilen kişisel verilerin korunmasında, kamu hukukunda olduğu gibi özel hukuk alanında da insan hak ve özgürlüklerinin korunmasına yönelik yasa hükümlerinden yararlanılır[161].

---

[158] Ulrich Haltern, "Integration Through Law", **European Integration Theory** (Ed. By Antje Wiener, Thomas Diez)", 2. Baskı, Oxford University Press, 2009, ss. 177-179, 181-185;
Andreas Vosskuhle, "European Integration Through Law, the Contribution of the Federal Constitutional Court", **European Journal of Sociology**, Cilt.58, Sayı.1, 2017, ss. 146-149;
Ahmet Burak Bilgin, "Avrupa Birliği Hukukunda Hukukun Genel İlkeleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXXIV, Sayı: 1, 2016, ss. 78-79, 85-91;
İlhan Aras, "Avrupa Birliği Hukukunun Önceliği İlkesi", **Sayıştay Dergisi**, Cilt. 99, Ekim-Aralık 2015, ss. 6-10.

[159] Pınar Bahar Doğan, ss. 481-484.

[160] Monica Hinteregger, "The Protection of Personality Rights in Private Law: Remedies", **The Legal Protection of Personality Rights: Chinese and European Perspectives**, (Ed.Ken Oliphant, Zhang Pinghua, Chen Lei, Brill Nijhoff), Brill/Nijhoff, Leiden, 2018, ss.71-73;
Aydın Akgül, s.54.

[161] Çiğdem Ayözger, s.46.

2.1.3. Birlik Hukukunda Kişilik Hakkı ve Kişisel Verilerin Korunması

Kişisel verilerin korunması kavramının kökleri, Birlik hukukunda da kişilik hakkı temelindeki insan hak ve özgürlüklerinin, devletin ve üçüncü şahısların olası müdahaleleri karşısında korunarak, güvence altına alınması gerekliliğine dayanır. Küresel dünyada ve Birlik içinde devam eden dijital değişim sürecine bakıldığında, artan teknolojik gelişmelerin, bireylerin yaşamlarını her geçen gün biraz daha fazla şeffaflaştırarak etkilediği görülmektedir. Önlenemeyen bu şeffaflaşma, istenmeyen etki ve ihlalleri de beraberinde getirdiğinden, kişilik hakkının bir yansıması olan insan haklarının korunması temeline dayanan kişisel verilerin korunması hususunun önemini artırmaktadır.

Birlik hukukunda kişisel verilerin korunmasına ilişkin henüz özel yasal düzenlemelerin olmadığı erken dönemde dahi, bu veriler, özel hayatın ve aile hayatının korunması temelinde Avrupa İnsan Hakları Sözleşmesi madde 8 ile 108 No'lu Avrupa Konseyi Sözleşmesi kapsamında korunmuşlardır. Birlik hukukunda kişisel verilerin korunması hususu, özel başlık altında ayrıca ve açıkça ilk kez Avrupa Temel Haklar Şartı'nın 8.maddesi ile düzenlenmiştir. Atıf yoluyla Lizbon Antlaşmasına eklenmesiyle bu Şart, Kurucu Antlaşmalarla eşdeğer bağlayıcılığa sahip hale gelmiştir. Günümüzde kişisel veriler, bu Şart'ın kişisel verilerin korunması başlıklı 8.[162] maddesi ve 7.maddesi[163] kapsamındaki özel hayat ve aile hayatına saygı, konut ve haberleşme dokunulmazlığı ilkeleri ile mahremiyet hakkı dahilindeki diğer maddeleri çerçevesinde korunmaktadırlar[164]. Bu sebeple, Birlik hukuku kapsamında kişisel verilerin korunması bağlamında verilen kararlarda, insan

[162] ABTHŞ, Madde 8. "1.Herkes, kendisine ilişkin kişisel bilgilerin korunmasını isteme hakkına sahiptir.
2. Bu tür bilgiler belirtilen amaçlar için ve ilgili kişinin muvafakatine ya da yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes kendisi hakkında toplanmış bulunan bilgilere erişme ve bunlarda düzeltme yapma hakkına sahiptir.
3. Bu kurallara uyulması bağımsız bir makam tarafından denetlenecektir."

[163] European Union, **Charter of Fundamental Rights of European Union**.
Avrupa Birliği Temel Haklar Şartı (ABTHŞ), Madde 7. "Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir."

[164] European Union Agency for Fundamental Rights, **Handbook on European Data Protection Law**, Belgium, 2014, https://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition ss. 14-20; Ernst Karner, "Human Rights and the Protection of Personality Rights in Europe: Comparative Reflections", **The Legal Protection off Personality Rights, Chinese and European Perspectives**, (Ed. Ken Oliphant, Zhang Pinghua, Chen Lei), Brill Nijhoff, Leiden, 2018, ss. 93-94.

onuru ve saygınlığı, özel hayatın ve aile hayatının gizliliğinin korunması, düşünce ve ifade özgürlüğü, haberleşme özgürlüğü, bilgi edinme hakkı, din, vicdan ve inanç özgürlüğü gibi temel haklara her zaman atıfta bulunulabilmektedir[165].

2.1.3.1. İnsan Onuru ve Saygınlığı Bağlamında Kişisel Veriler

İnsan, akıl ve düşünme yetisi sebebi ile sahip olduğu, yalnız kendi varlığından kaynaklanan maneviyatla, kişiliğini geliştirip kendi kaderini kendisi tayin edebilirken, aynı zamanda da çevresine etki edip, onu değiştirebilme gücüne sahiptir. Bu öz yeti nedeniyle, "*insan onuru ve saygınlığı*", tüm temel hakların çıkış noktası olarak kabul edilmektedir. Genel anlamda insan onuru ve saygınlığı, insanın hangi koşul ve durumda bulunursa bulunsun sadece insan olmasından kaynaklanan, vazgeçilemeyen ve hiç bir şart altında dokunulamayacak olan değer ve saygının kendisine tanınması olarak açıklanabilir. Bu sebeple, temel hak ve özgürlüklere yönelik bir ihlal olup olmadığının değerlendirilmesinde, öncelikle, tüm diğer insan haklarının temeli ve evrensellik sebebi sayılan insan onurunun korunması hakkına müdahale edilip edilmediğinin tespiti önemlidir. Bu tespit yapılırken literatürde, Tübingen Üniversitesi'nin Kamu Hukuku alanında çalışmış ünlü profesörlerinden biri olan Günter Dürig'in anayasaya ilişkin çalışmalarından faydalanılmaktadır. Dürig çalışmalarında, Kant'tan esinlenerek insanı, aklıyla doğa kanunlarının dışına çıkarak, çevresini yeniden şekillendirebilen, kendi varlığının bilincinde olan ve kendi kendini tanımlayabilen bilinçli bir varlık olarak nitelendirir. Bu tanıma göre, insan sadece araç değil, aynı zamanda amaçtır. İnsanın sadece araç olarak görülmesi durumunda ise insan onuru zedelenebilecektir[166].

---

[165] European Union Agency for Fundamental Rights, 2014, ss. 67, 148; Elif Küzeci, **Kişisel Verilerin Korunması**, 2. Baskı, Turhan Kitapevi, Ankara, , 2018, ss. 68-70.

[166] Günter Dürig, "Die Menschenauffassung des Grundgesetzes", 1952, s.259 ile "Der Grundrechtssatz von der Menschenwürde: Entwurf eines praktikablen Wertsystems der Grundrechte aus Art.1 Abs. I in verbindung mit Art.19 Abs. II des Grundgesetzes", **Archiv des Öffentlichen Rechts**, Cilt. 81, (N.F.42), Sayı. 2, 1956, ss. 117,127, Aktaran Matthias Mahlmann, "Human Dignity and Authonomy in Modern Constitutional Orders", **The Oxford Handbook of Comparative Constitutional Law** (Ed. Michel Rosenfeld, Andras Sajo), Oxford University Press, 2012, https://www.jura.uni-hamburg.de/media/ueber-die-fakultaet/personen/albers-marion/seoul-national-university/course-outline/mahlmann-2013-human-dignity-and-autonomy-in-modern-constitutional-orders.pdf , ss. 371-378, 379 (02.06.2020)
Henk Botha, "Human Dignity in Comparative Perspective", **STELL LR**, Cilt.2, 2009, s.183;
Erdal Yerdelen, "Klonlamanın (Kopyalama) Ceza Hukukundaki Yeri", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 63, Sayı: 3, 2014, s. 660.

İnsan hak ve özgürlüklerinin temelini oluşturan insan onuru ve saygınlığının korunması hususu her ne kadar Avrupa İnsan Hakları Sözleşmesi'nin ana metninde açıkça yer almasa da[167], bu konuda atılan en önemli adımlardan biri de, AİHS'ne ek olarak imza altına alınan 1983 ve 2002 tarihli 6 ve 13 numaralı Protokollerdir. Bu Protokoller vasıtası ile, ölüm cezasının kaldırılması hüküm altına alınmıştır. Uluslararası hukuk kapsamında önemli bir atılım olan bu Protokoller ile, yaşam hakkını, insan onuru ve saygınlığını hiçe saydığı, günümüzde gelişmiş demokrasilerde kabul edilen, idam cezasının kaldırılması, insan hak ve özgürlüklerinin korunması yönünde atılmış önemli bir adım niteliğindedir. İdam cezasının kaldırılmasının, insan onurunun layıkıyla korunması hususunu, pek çok bakımdan güçlendirdiğinin altı, Avrupa Birliği tarafından 10 Ekim 2019 tarihinde yayınlanan Bildiri ile de bir kere daha çizilmiştir[168].

Bireyler, ancak ve ancak insan onuru ve saygınlığının tanımlanarak, yasal güvence altına alındığı hallerde, kişiliklerini serbestçe geliştirip, temel hak ve özgürlüklerini kullarak, yaşamlarını bağımsız bir şekilde sürdürebilme imkanına sahip olabilirler. Bu bilinçle, insanın insan olmaktan kaynaklanan özsaygısını, itibarını ifade eden insan onurunun dokunulmazlığına saygı duyularak, mutlak koruma altına alınmasının gerekliliği, Avrupa Temel Haklar Şartı'nın birinci maddesinde açıkça hüküm altına alınmıştır[169].

Tüm diğer temel haklarda olduğu gibi, Avrupa Temel Haklar Şartı madde 8'de ayrıca ve açıkça düzenlenen kişisel verilerin korunması hakkının da çıkış noktası, insan onuru ve saygınlığının korunması ana ilkesidir. Nitekim, kökleri, insan onurunun mutlak bir şekilde korunması gerekliliğinden kaynaklanan kişisel verilerin

---

[167] Christopher McCrudden, "Human Dignity and Judicial Interpretation of Human Rights", **The European Journal of International Law**, Cilt.19, Sayı. 4, 2008, ss.670-671;
Elisabeth Wicks, "The Meaning of Life: Dignity and the Right to Life in International Human Rights Treaties", **Human Rights Law Review**, Cilt.12, Sayı.2, 2012, s. 206.

[168] Joint Declaration by the High Representative for Foreign Affairs and Security Policy on behalf of the European Union and the Secretary General of the Council of Europe on the occasion of the European and World Day against the Death Penalty, **Joint Declaration**, 10 October 2019, https://rm.coe.int/2019-joint-declaration-final-003-/16809818b6 (02.06.2020).
Türkiye de, 2003 yılında imza altına aldığı 6 numaralı Protokol ve 2004'te imzaladığı 13 numaralı Protokol ile ölüm cezasını kaldırmıştır. Daha fazla bilgi için bkz. M.Balkan Demirdal, "Uluslararası İnsan Hakları Hukukunda Ölüm Cezasının Kaldırılması ve Türkiye'deki Süreç", **Politik Ekonomik Kuram**, Cilt.2, Sayı.1, 2018, ss.64-66.

[169] European Union, **Charter of Fundamental Rights of European Union**, madde 1; European Data Protection Supervisor, "Towards a New Digital Ethics: Data, Dignity and Technology", **Opinion 4/2015,** https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf (02.06.2020) s. 4.

korunması hakkı, insanın insan olmaktan ötürü sahip olduğu maddi ve manevi değerlerinin, saygın olma ve kendini değerli hissetme duygusunun korunması, böylelikle de bireyin kendisini, iç dünyasında ve toplum içinde saygın bir yerde konumlandırarak, kişiliğini özgürce koruyup geliştirmesi noktasında ortaya çıkmaktadır. Buradaki temel kural, veri süjesinin kendi kişisel verileri üzerindeki kontrolü elinde bulundurmasıdır. Kişisel verilerinin üzerindeki kontrolünü kaybeden bir birey, artık hayatının özel ve giz (sır) alanları da dahil hangi noktasındaki, hangi kişisel verinin, kimlerin erişim ve kullanımına açık olduğuna ilişkin kontrolünü de yitirecektir. Bu kontrol kaybının yaratacağı maddi-manevi riskler ve kayıplar sebebiyle birey, insan onurunu ve saygınlığını koruyup toplum içinde dik durarak kişiliğini serbestçe geliştirmekte güçlük çekecektir. Böyle bir durumda serbest irade de zarar görebileceğinden, toplumsal demokrasinin de bu bağlamda kan kaybedeceği açıktır[170].

Teknoloji ve internet kullanımının veri güvenliğine ilişkin getirdiği tehdit ve riskler, hak süjesi olan bireylerin kişisel verilerinin ve mahremiyetlerinin korunmasını zorlaştırarak, bu hakların temelinde yatan insan onuru ve saygınlığının da zedelenmesine sebep olabilmektedir. Sanal tehdit ve saldırıların boyutu, yaşanan teknik ilerlemelere paralel olarak her geçen gün artarak, bireyi ve sahip olduğu kişisel verilerini, üçüncü kişilerin çeşitli amaçlarına hizmet etmekte kullanılabilecek bir meta haline getirebilmektedir. Bu durum, insan onuru ve saygınlığı temelindeki tüm insan hak ve özgürlüklerinin korunmasını tehlikeye düşürmektedir. Bu sebeplerle, hazırlanacak kapsamlı yasalarla temel hak ve özgürlüklerin korunması hususu, dijital çağda her zamankinden daha önemli bir öncelik olarak karşımıza çıkmaktadır[171].

---

[170] Gerrit Hornung, Christoph Schnabel, "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination", **Computer Law & Security Report**, Cilt.25, Sayı 1, 2009, s. 87;
Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2008, ss.111,128-132; Edward J. Eberle, "The German Idea of Freedom", **Oregon Revıew of Int'l Law**, Cilt.10, 2008, http://docenti.unimc.it/benedett-a.barbisan/teaching/2014/12694/files/thirteenth-and-fourteenth-class-10-11-november/human-dignity-in-the-german-basic-law-2 , ss. 23-24 (02.06.2020).
[171] European Data Protection Supervisor, **Opinion 4/2015**, s. 12; Gerrit Hornung, Christoph Schnabel, I-2009, s. 87.

2.1.3.2. Mahremiyet Hakkı Bağlamında Kişisel Veriler

Modern dünyada, özellikle son dönemde yaşanan teknolojik gelişmeler ve buna bağlı dijitalleşmeden kaynaklanarak, hızla artan saydamlaşma nedeniyle, bireylerin öz benliklerini ve yaşam alanlarının mahremiyetlerini, kamuya ve diğer gerçek ve tüzel kişilere karşı koruyabilmelerine imkan veren "*mahremiyet hakkı"* büyük önem kazanmıştır[172].

Avrupa İnsan Hakları Sözleşmesi'nin kabul edilmesi ile, kişisel verilerin korunması kavramının temellerinde yatan haklardan biri olan mahremiyet hakkı (*Right to privacy*), önemli ve bağlayıcı bir hukuki metin kapsamında zikredilerek, bu Sözleşme'nin 8. maddesinde [173] düzenlenip, "*Özel Hayatın ve Aile Hayatının Korunması*" çerçevesinde koruma altına alınmıştır. Avrupa Konseyi, Parlamenterler Asamblesi'nin 428 sayılı Deklarasyonu madde 16'da ise "*mahremiyet hakkı, esas olarak kişinin kendi hayatını en az müdahale ile yaşayabilme hakkı*" olarak tanımlanmıştır. Bu bağlamda mahremiyet hakkının, insan onuru ve saygınlığı, özel ve aile hayatı, düşünce, ifade ve haberleşme özgürlüğü, din, vicdan ve inanç özgürlüğü, bilgi edinme hakkı ve kişisel verilerin korunması gibi temel hakların kilit taşını oluşturduğu söylenebilir[174].

Bireyin kendisinin başlı başına bir değer olduğunun kabul edilerek, bireysel özgürlük alanının ve haklarının yasal olarak tanınıp, korunduğu modern dönemde büyük önem kazanan, "*mahremiyet hakkı",* bireyin, yaşam alanlarına gerek kamudan, gerekse de diğer bireyler ile özel kuruluş ve oluşumlardan gelebilecek

---

[172] Adam Carlyle Breckenridge, **The Right to Privacy**, University of Nebraska Press, Lincoln, 1970, s. 14, Aktaran Mehmet Yüksel "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", **Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi**, Cilt.58, Sayı. 1, 2003, s.183.

[173] Avrupa Konseyi, Avrupa İnsan Hakları Sözleşmesi (11 ve 14. Protokollerle değiştirilen metin-Ek Protokol ile Protokol 4, 6,7,12 ve 13 eklenmiştir), http://www.echr.coe.int/Documents/Convention_T-UR.pdf , (02.06.2020)

Avrupa İnsan Hakları Sözleşmesi (AİS), madde 8. "*Özel ve Aile Hayatına Saygı Hakkı 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın ve ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

[174] Council of Europe, Parliamentary Assembly, "Declaration on Mass Communication Media and Human Rights", **Resolution 428(1970),** Article 15-16, http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNTg0MiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE1ODQy (02.06.2020).

müdahalelere karşı koyabilme ve bu alanları koruyabilme hak ve özgürlüğü olarak da tanımlanabilir. Mahremiyet hakkı, bireye, yalnız kalarak, diğer gerçek ve tüzel kişiler ile devletin müdahalesinden koruyabileceği, yalnızca kendi kontrolünde olan ve sadece kendisinin belirleyeceği kişilere açmakta serbest olduğu yaşam alanında, kişiliğini serbestçe geliştirerek, koruyabilmesi bağlamında hizmet etmektedir[175]. Burada mahremiyet hakkına ilişkin üç önemli özellik dikkati çekmektedir. Bunlardan ilki "*bağımsızlık*" tır. Mahremiyet hakkı kapsamında bağımsızlık, bireylerin kendi yaşam alanlarındaki seçim, tutum ve davranışlarında özgür olmalarını ifade eder. İkinci özellik ise, kişilerin kimilerine yaşam alanlarını açıp, kimilerini de dışarıda bırakarak, giz ve özel alanlarını belirleyip, kendi sınırlarını özgürce çizmeleri bağlamında ortaya çıkan "*gizlilik*" kavramıdır. Üçüncü özellik, bireylerin kendi yaşam alanlarının gizliliğini ihlal edebilecek nitelikte olan girişim, tehdit ve ihlallere karşı "*önleme ve korunma tedbirlerini alabilme ve/veya bunları talep edebilme hak ve imkanı*" na sahip olmalarıdır. Mahremiyet hakkının korunması bağlamında genel kabul gören bir diğer konu da, "*bireysel yaşam alanı*"nın üç temel bölüme ayrılmasıdır: Bireyin sadece kendisine sakladığı veya çok sınırlı sayıda seçtiği yakınlarına açtığı ve bunlar haricinde dışarıdan gelebilecek her türlü müdahaleye kesin bir şekilde kapalı olan "*giz (sır) alanı*"; bireyin yine kendi seçtiği ancak giz alanını açtığına kıyasla daha fazla sayıda hısım, eş, dost ve arkadaşlarına açtığı "*özel alanı*"; ile son olarak da bireyin toplumsal hayatının olağan akışı içerisinde, rahatsız edilmeden ve kişilik hakkına zarar gelmeden kamu yaşamına katıldığı "*ortak yaşam alanı*"[176].

Mahremiyetin, özellikle de giz (sır) alanının ve bu kapsamda kişisel verilerin, korunması hakkındaki düzenlemeler, her ne kadar, teknoloji ve internet kullanımının her alanda yaygınlaştığı, modern dönemde popüler hale geldiyse de, mahremiyet hakkının ve bu kapsamda kişisel verilerin korunmasının kökenleri, çok eski dönemlere kadar uzanmaktadır. Nitekim Hippocrates'ın öğretileri doğrultusunda hazırlandığına inanılan "*Hipokrat yemini*"; hekimlere, mesleki yetkilerinin kötüye

[175] Gerrit Hornung, Christoph Schnabel, I-2009, ss. 86-87;
Aydın Aksoy, s.75;
Oğuz Şimşek, ss. 132-133-135-136.
[176] Aydın Zevkliler, Mehmet Beşir Acabey, K.Emre Gökyayla, ss. 416-419;
Adam Carlyle Breckenridge, ss.122, 123, Aktaran Mehmet Yüksel, 2003, ss.182-183-187-188-189;
Mine Kaya, "Telekomünikasyon Alanında Kişilik Haklarının Korunması", **Ankara Barosu Dergisi**, Sayı.4, 2010, ss.285,286.

kullanılmaması, dürüstlük, insanlığa hizmet, ayrımcılık yapmama, insan hayatına saygı gibi ahlaki temelli "*mesleki sırların korunması yükümlülükleri*"nin yanı sıra, kişisel verilerin korunması ve mahremiyet hakları kapsamında zikredilen hastaların sır alanlarının, kimliklerinin ve sağlık verilerinin korunması yükümlülüklerini de getirmektedir. Görüldüğü üzere, mahremiyetin ve kişisel verilerin korunmasına ilişkin düşünce ve çalışmalar, özellikle 20.yüzyılın sonundan itibaren bilgi ve iletişim teknolojileri alanında meydana gelen devrim niteliğindeki gelişmelere paralel olarak, büyük ivme kazanmışsa da, aslında bu konuların felsefi kökenleri, Eski Yunan'a kadar uzanmaktadır[177].

Kişisel verilerin korunması hakkının en önemli çıkış noktalarından biri olan mahremiyet hakkı, çok anlamlı ve geniş kapsamlı bir kavram olduğundan, sınırlarının net olarak çizilerek, bu hakkın korunması, somut olay bağlamında oldukça karmaşık bir durum arz eder[178]. Zira, ihlalin gerçekleştiği iddia edilen durumun, hangi yaşam alanının kapsamında olduğu ve ne ölçüde mahremiyet hakkının sağladığı korumadan yararlanabileceği hususunu, açık ve doğru bir şekilde belirleyebilmek oldukça zordur. Bu sebeple, böyle bir ihlal iddiasını içeren somut olayın özelliklerine göre hakkaniyete uygun bir yoruma gidilerek, ihlalin gerçekleşip gerçekleşmediğinin belirlenmesi önemlidir. Örneğin, kişinin, kamusal bir alanda gerçekleştirdiği ve aslında genel toplumsal davranış kuralları çerçevesinde değerlendirildiğinde toplum tarafından kabul görmeyecek, ifşası halinde ise kişinin saygınlığına zarar vererek, onu rencide edebilecek nitelikteki bir davranışını ele alalım. Bu davranışın, kamusal alan dahilinde de olsa gizlice kayıt altına alınarak, kişinin bilgi ve onayı haricinde yayınlanması durumu, somut olay, her ne kadar kamuya açık bir alanda meydana gelse de mahremiyet hakkının ihlali kapsamında değerlendirilebilinir. Bu örnekten de açıkça anlaşılacağı gibi, olay, halka açık bir kamu alanında gerçekleşse dahi münferit olayın özelliklerine bakılarak, kimi hallerde, kişinin, mahremiyetinin ihlal edildiği sonucuna varılabilmektedir.

---

[177] Oğuz Şimşek, ss.5-10;
Hatice Sarıtaş, **Hasta Hakları Açısından Hekim Sorumluluğu**, Bilge Yayınevi, Ankara, 2005, s.5;
Enis Karaarslan, Ali Murat Ergin, Nalin Turğut, Özgür Kılıç, "Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti", **İNET-TR 2015,** https://www.researchgate.net/profile/Enis_Karaarslan/publication/287975276_Elektronik_Saglik_Kayitlarinin_Gizlilik_ve_Mahremiyeti/links/576cc6ff08ae9bd709961314/Elektronik-Saglik-Kayitlarinin-Gizlilik-ve-Mahremiyeti.pdf , (02.06.2020). s.2.

[178] Mehmet Yüksel, "Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar", **Ankara Üniversitesi SBF Dergisi**, Cilt. 64, Sayı.1, 2007, s.277.

Mahremiyet hakkının sınırlarının çizilmesindeki güçlük, özellikle halka mal olmuş kişilerin mahremiyetlerinin ve kişisel verilerinin, hangi sınırlar dahilinde korunacağının belirlenmesi kapsamında ortaya çıkmıştır. Yaşanan teknolojik gelişmelerin de etkisiyle, tanınmış kişilerin mahremiyetlerinin nerede başlayıp nerede biteceği, bir diğer ifade ile "*özel hayat nerede biter ve kamuya açık hayat nerede başlar*" sorunu günden güne daha fazla tartışılır hale gelmiştir[179].

Prenses Caroline'nın Avrupa İnsan Hakları Mahkemesi'nde Almanya'ya karşı açtığı "*Von Hannover Davası*"[180], tanınmış kişilerin özel hayatının sınırlarının nasıl çizilmesi gerektiği konusunda önemli bir örnek teşkil eder. Bu dava kapsamında 2004 yılında verilen kararda, somut olayın, halka açık bir alan olan Monte Carlo Beach Kulüpte, Prensesin, yanında çocukları ve bir arkadaşı varken, izinsiz fotoğraflarının çekilmesi şeklinde gerçekleştiği tespit edilmiştir. Bununla birlikte, Prensesin rızası dışında çekilen bu fotoğrafların, hem yanında reşit olmayan çocuklarının da bulunduğu bir zamanda, hem de prenses tatilde iken çekilmesi ve kamuya mal olmuş bir kişi olsa dahi fotoğrafların Prensesin resmi görevleriyle ilgisinin bulunmaması sebepleriyle, somut olayda, halka açık alanın dar yorumlanması gerektiğine hükmedilmiştir. Buradaki somut olayın özellikleri incelendiğinde, kişisel veri niteliğindeki fotoğrafların, tamamen aile ve özel hayatın korunması kapsamında kaldığı, bunların gazetede yayınlanarak açıklanmasında bir kamu yararının da bulunmadığı anlaşılmaktadır. Bu durum, ilgili bireylerin özel hayat ve aile hayatı dokunulmazlıklarına zarar verecek nitelikte olduğundan, somut olayda mahremiyet hakkının öncelikli olarak korunması önemlidir. Nitekim, bu davada, temel hak ve özgürlüklerin korunması kapsamında "*ifade ve basın-yayın özgürlüğü*" ile "*mahremiyet hakkı, dolayısı ile de özel hayatın ve aile hayatının, kişisel verilerin"* korunması hakları karşılıklı olarak yarışsa da, ikinci gruptaki haklara, somut olayın özellikleri gereği verilen öncelik sebebi ile, bu haklar, ifade ve basın-yayın özgürlüğünün korunması haklarının önüne geçerek öncelikli olarak korunmuştur[181].

---

[179] Council of Europe, Parliamentary Assembly, **Resolution 428(1970)**, Madde 17-18-19-20.

[180] Judgment by the European Court of Human Rights, Case of von Hannover v. Germany, **ECHR Application No. 59320/00**, 24.06.2004, https://www.juridice.ro/wp-content/uploads/2016/07/von-Hannover-v-Germany-ECHR-24-June-2004.pdf (02.06.2020).

[181] Dirk Voorhoof, "European Court of Human Rights, Case of Von Hannover v. Germany", **IRIS Merlin 2004-8:2/2**, http://merlin.obs.coe.int/article/3137 , (02.06.2020);

İçinde bulunduğumuz dijital çağda, veri kullanımına dayanan dijital teknolojiler ve internetin, bireylerin günlük yaşamlarının her alanına dokunmaya başlamasıyla birlikte, kişilerin mahremiyetlerinin ve bu bağlamda da kişisel verilerinin korunması, her geçen gün daha zorlu bir iş haline gelmiştir. Nitekim, yaşanan bu teknolojik gelişmelere paralel olarak artan "*Facebook, Twitter, Instagram*" gibi sosyal medya platformları ile *"Yahoo, G-mail, Hotmail*" gibi e-posta hizmetlerinin, çeşitli sunucuların (server), Google gibi arama motorlarının kullanılması; e-ticaretin ve e-kamu işlemlerinin artması gibi sebeplerle, kişisel veriler çevirimiçi ağ sistemlerine yoğun olarak aktarılmıştır. Dijital sistemlerde depolanarak işlenen bu kişisel veriler ise, veri süjesinin kontrol alanı dışına çıkarak, herkes tarafından kolaylıkla erişilebilir hale gelmişlerdir. Bu durum da mahremiyete ve kişisel verilere yönelen tehditlerin artması sonucunu ortaya çıkarmıştır[182].

2.1.3.3. Özel Hayatın Korunması Bağlamında Kişisel Veriler

Özel hayata ve aile hayatına saygı gösterilmesi hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8.maddesi ile Avrupa Birliği Temel Haklar Şartı'nın 7.maddesinde açıkça düzenlenerek kamu otoritesi de dahil olmak üzere tüm üçüncü kişilere karşı koruma altına alınmıştır.

Özel hayatın sınırlarını belirleyen net bir tanımın yapılmaya çalışılmasına yönelik gelenekselci tutum, 70'li yıllarda değişerek, bireyin her türlü tutum, davranış ya da ilişkilerinin, kamusal alanda gerçekleşse dahi, somut olayın özelliklerine göre, özel hayatın sınırları dahilinde değerlendirilerek korunabileceği anlayışı benimsenmiştir. Bu doğrultuda, Avrupa Konseyi ve Avrupa İnsan Hakları Mahkemesi de özel hayatın kapsamını sınırlandırıcı nitelikte net bir tanım yapmaktan kaçınarak, özel hayatın kapsamını mümkün mertebe geniş yorumlama yoluna gitmişlerdir[183].

Ivana Roagna, **Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması**, Avrupa Konseyi İnsan Hakları El Kitapları Serisi, Strazburg, 2012, s.65.

[182] Özgür Uçkan, "Internet, Mahremiyet ve Kişisel Verilerin Korunması", https://www.evrensel.net/haber/67935/internet-mahremiyet-ve-kisisel-verilerin-korunmasi, Evrensel Haber, 2013, (02.06.2020).

[183] Loukes G. Loukaides, "Essays on the Developing Law of Human Rights"**, International Studies in Human Rights**, Kluwer Academic Publishers, Boston, 1995, ss.85-87.

Avrupa İnsan Hakları Mahkemesi'nin 1992 yılında verdiği "*Niemietz v. Germany Kararı*"nın 29. paragrafında bu hususun altı özel olarak çizilerek, özel hayatın kapsamına ilişkin etraflı ve net bir tanım getirilmesinin mümkün ve gerekli olmadığı belirtilmiştir. Zira özel hayatın sadece "*içsel bir alandan (Inner circle)*" ibaret olduğunun kabul edilmesi oldukça sınırlandırıcı bir yaklaşım olacaktır. Bu sebeple, özel hayata saygının, somut olayın özelliklerine göre, bireyin üçüncü kişilerle belli dereceye kadar kurmuş ve geliştirmiş olduğu her türlü sosyal ilişkinin de gizliliğini ve dokunulmazlığını kapsayabileceği dikkate alınmalıdır. Yine Niemietz v. Germany Kararının 30. ve 31. paragraflarında, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde belirtilen "*ev (Home (İngilizce metin), Domicile (Fransızca metin))*" ibaresinin dar yorumlanarak, kişilerin kimi özel ilişkilerini yönetebilecekleri işyeri veya ticari tesisleri bu kavramın dışında tutmanın, özel hayatın korunması hakkının kapsam ve içeriğine uygun olmadığının altı çizilmiştir. Bu durumda olay, bireyin giz (sır) ve özel alanlarında veya kamuya açık alanda dahi gerçekleşmiş olsa, özel hayatın gizliliğinin ihlal edilip edilmediğine, somut olayın özelliklerine bakılarak karar verilmesi yerinde olacaktır[184].

Kişisel veriler ile özel hayatın gizliliğinin korunması hakkı arasında kendiliğinden doğan organik bir bağ vardır. Zira bireyin gerçek kimliği ile ilintili bulunan kişisel verilerinin kontrolünü elinde bulundurması ve bu verilere kamudan ya da üçüncü kişilerden gelebilecek, herhangi bir yasal dayanağı da bulunmayan müdahalelerin engellenmesi, aynı zamanda özel hayatın korunması hakkıyla da sıkı sıkıya ilişkilidir.

Günümüzde teknoloji ve internet kullanımı kapsam ve oranının hızla artması, özel hayatın ve aile hayatının gizliliğinin korunması hususlarını da içerebilen kişisel verilerin, veri süjeleri tarafından kontrolünü her geçen gün daha da zorlaştırmaktadır. Bu sebeple, yoğun teknoloji kullanımı sonucu, internet ortamına aktarılan kişisel verilerin, gerek birey karşısında asimetrik olarak açık ara daha kuvvetli bulunan devlete, gerekse de internet sayesinde bu verilere ulaşmaları kolaylaşan diğer gerçek ve tüzel üçüncü kişilere karşı korunması, özel hayata ve aile hayatına saygının

[184] Judgment by European Court of Human Rights, Case of Niemietz v. Germany, **ECHR Application no. 13710/88**, 16.12.1992, Strasbourg, https://hudoc.echr.coe.int/eng#{"itemid":["001-57887"]} (02.06.2020); Ursula Kilkelly, "The Right to Respect for Private and Family Life, A Guide to the Implementation of Article 8 of the European Convention on Human Rights", **Council of Europe, Human Rights Handbooks,** No.1, Strasbourg, 2001, ss.10,11,12,19.

korunması bakımından da büyük önem taşır. Böylece özel ve aile hayatına da ilişkin olabilen kişisel verilerin korunması yoluyla, bireyin kendiyle veya seçmiş olduğu yakınlarıyla baş başa kalabilmesi ve en az müdahale ile kişiliğinin tüm unsurlarını serbestçe geliştirebilmesi sağlanarak, bireyin eşsiz özerkliği de korunabilecektir[185].

2.1.3.4. Düşünce ve İfade Özgürlüğü Bağlamında Kişisel Veriler

Düşünce ve ifade özgürlüğü, bireyin düşüncesini, kanaatlerini serbest bir şekilde oluşturup, ifade ederek diğerlerine aktarabilme hakkı şeklinde tanımlanabilir. Bu hak, demokrasi ve hukukun üstünlüğü gibi medeni hak ve özgürlüklerin, temel ilkeler olarak benimsendiği tüm gelişmiş toplumlarda her bireyin sahip olduğu vazgeçilmez insan haklarından biridir. Düşünce ve ifade özgürlüğünün toplum tarafından özümsenerek korunması ve geliştirilmesi bağlamında özgür, bağımsız ve tarafsız basın-yayın kuruluşlarının varlığı büyük önem taşımaktadır. Zira bilgi, düşünce ve söylemlerin yasalarla korunarak, yasal sınırlar dahilinde, kamu müdahalesi olmadan özgürce ortaya konularak, serbest dolaşımlarının sağlandığı bir ortamda, aynı zamanda da şeffaflığın ve hesap verebilirliğin hakim olduğu medya kuruluşlarına sahip olma, demokratik bir toplumda düşünce ve ifade özgürlüğünün anahtarı niteliğindedir. Düşünce ve ifade özgürlüğü, kişilik hakkı bakımından da büyük önem taşır. Nitekim ancak ve ancak bireysel düşünce ve ifade özgürlüklerinin sağlam temeller üzerine oturtulduğu toplumlarda, kişisel gelişimini tamamlayabilen, kişilik hakkının anlam ve önemini özümsemiş özerk ve özgür bireylerden bahsedilebilinir[186].

Özgür düşünebilen ve düşüncelerini serbestçe ifade edebilen bireylerden oluşan toplumlarda demokrasi varlığını sürdürerek kendini geliştirebilir. İsveçli ünlü düşünür Peter Forsskal'ın "*Medeni Özgürlük Üzerine Düşünceler (Thoughts on Civil*

---

[185] Ursula Kilkelly, s.11; Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 61, Sayı: 3, 2012, ss. 1098-1099 ;
Ergun Özbudun, "Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği", **Ankara Hukuk Fakültesi Ellinci Yıl Armağanı**, Cilt 1, 1977, https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/10322 (02.06.2020) ss.265, 267;
Çiğdem Ayözger, s.38.

[186] Çiğdem Ayözger, s.42; European Union Agency for Fundamental Rights, 2018, ss.22-26; Council of the European Union, **EU Human Rights Guidelines on Freedom of Expression Online and Offline**, Foreign Affairs Council Meeting, Brussels, 2014, https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf , s.1 (02.06.2020).

Liberty)[187]" adlı ünlü eserinde açıklamaya çalıştığı gibi, toplumların demokratik gelişimi ile düşünce, ifade ve bilgi edinme özgürlükleri, birbirlerine karşılıklı olarak sıkı sıkıya bağlıdırlar ve birbirlerinin gelişimlerini tahminlerin çok ötesinde etkilerler. Forsskal'ın 1759'da yayınlanan bu eserinde tanzim ederek açıkladığı temel hakların neredeyse tamamı, otuz yıl sonra Fransız İnsan ve Yurttaş Hakları Bildirgesi'ne girerek, genel kabul görmüştür. Bu bağlamda, düşünce ve ifade özgürlüğü de, Fransız İnsan ve Yurttaş Hakları Bildirgesi'nde yerini alarak, yönetim şekli olarak demokrasiyi benimseyen devletler tarafından, ulusal yasalarına aktarılarak, temel haklar bağlamında korunan en önemli haklardan biri haline gelmiştir[188].

Düşünce ve ifade özgürlüğü, Avrupa İnsan Hakları Sözleşmesi'nin "Düşünce, Vicdan ve Din Özgürlüğü" başlıklı 9. maddesi ve "İfade Özgürlüğü" başlıklı 10. maddesi kapsamında düzenlenmiştir. Bu haklar, ayrıca Avrupa Birliği'nin kuruluşundan itibaren ortak temel değerlerden biri olarak benimsenip, Avrupa Birliği Antlaşması'nın ilgili maddeleri[189] ve Avrupa Birliği Temel Haklar Şartı'nın 10. ve 11. maddeleri ile düzenlenerek, Birlik hukukunun birincil kaynakları kapsamında da ayrıca yasal koruma altına alınmışlardır[190].

Modern hukukta, düşünce ve ifadelerin, bireyin kendi iç dünyasında oluştukları ve içeriklerinde bireye ait öznel değer, kanaat, bilgi ve verileri barındırdıkları kabul edilir. Bu sebeple, düşünce ve ifadeler, prensip olarak ait oldukları kişinin kontrolünde bulunarak, üçüncü kişilerden gelebilecek müdahale ve tehditlere karşı yasal düzenlemelerle korunmaları gereken kişisel veriler kapsamında sayılırlar. Bu bakımdan düşünce ve ifade özgürlüğü anlamında kişisel verilerin korunması kavramı, düşüncenin birey tarafından serbestçe oluşturularak, yalnızca

---

[187] Peter Forsskal'ın "*Medeni Özgürlük Üzerine Düşünceler*" başlığı ile Türkçeye çevrilen eserinin orjinal adı "*Tankar om borgerliga friheten*" olup eserin başlığının birebir çevirisi "*Burjuva Özgürlüğü Üzerine Düşünceler*"dir. Daha fazla bilgi için bkz. İlke Dağlı, Derviş Erel, Medeni Özgürlük Üzerine Düşünceler (revised by Prof.Esin Orucu), http://www.peterforsskal.com/thetext-tu.html , (02.06.2020).

[188] Ulla Carlsson, "Freedom of Expression and the Media in a Time of Uncertainty, A Brief Introduction", **Freedom of Expression and Media in Transition, Studies and Reflections in the Digital Age**, (Ed. Ulla Carlsson), Nordicom, 2016, s.10.
Ahmet Çelik, Yaşar Tonta, "Düşünce Özgürlüğü, Bilgi Edinme Özgürlüğü ve Bilgi Hizmetleri", ***Bilgi Edinme Özgürlüğü***, (Ed.Yaşar Tonta, Ahmet Çelik), Türk Kütüphaneciler Derneği Genel Merkezi Yayınları No.21, Ankara, 1996, ss.1,2.

[189] European Union, **Treaty on European Union**, Madde 2, 6, 21, 49.

[190] Council of the European Union, **EU Human Rights Guidelines on Freedom of Expression Online and Offline**, parag.7.

bireyin kendisinin belirleyeceği ortamda ve dilediği muhataplara açıklanmasını kapsar[191]. Dijital çağda, her alanda bireysel teknoloji ve internet kullanımının artması nedeniyle, bireyin özgürce yaşayıp düşünerek kişiliğini serbestçe geliştirmesinin anahtarlarından biri olan, düşünce ve ifade özgürlüğünün, çevirim dışı korunmasının yanı sıra dijital ortama aktarılan kişisel veriler bağlamında çevrim içi olarak da korunması hususu önem kazanmıştır[192]. Zira çevirim içi ortamda kullanılan çeşitli dijital platformlar ve kitle iletişim araçları vasıtasıyla, bireylerin kişisel verilerini içeren düşüncelerini ifade ederek, bunları üçüncü kişilere ulaştırma ve üçüncü kişilerle karşılıklı etkileşim biçimleri de, tıpkı daha önce radyo ve televizyonun hayatımıza girdiğinde olduğu gibi, radikal bir biçimde değişmiştir. Devrim niteliğindeki bu değişim, çevirim içi araçları kullanan bireylere, düşüncelerini daha katılımcı bir ortamda, daha geniş kitlelere ulaştırma, karşılıklı etkileşim sonucu kendi benliğini yeniden tanımlayarak geliştirme gibi imkanlar sunmaktadır. Ancak dijital değişim, imkanların yanı sıra aynı zamanda bazı olumsuzluklar da ortaya çıkarmıştır. Nitekim dijital devrim, düşünce ve ifadeler, bir kez bireyin kontrolünden çıkarak, dijital ortama girdikten sonra, bunların içerdiği kişisel verilerin nasıl korunması gerektiği sorunsalını da beraberinde getirmiştir [193].

Düşünce ve ifade özgürlüğünün günlük hayattaki en önemli yansımalarından biri de basın-yayın özgürlüğüdür. Bilgi, düşünce ve haberlerin, basın-yayın özgürlüğü vasıtasıyla kamuya aktarılması da, halkın haber alma, bilgi edinme özgürlüklerini kullanabilmesi bakımından demokratik toplumlarda kilit niteliği taşır. Ancak tüm özgürlükler gibi düşünce ve ifade özgürlüğünün, basın-yayın özgürlüğünün, haber alma ve bilgi edinme özgürlüklerinin kullanımlarının da meşru sınırlar dahilinde ve özellikle de kişisel verilerin korunması hakkı gözetilerek yapılması gerekmektedir. Zira, farklı menfaatleri gözeten düşünce ve ifade, basın-yayın, haber alma ve bilgi edinme özgürlükleri ile kişisel verilerin korunması hakkı arasında hassas bir denge bulunmaktadır. Bu hassasiyet, özellikle kişisel verilerin

[191] Çiğdem Ayözger, ss.42-43;
Aydın Akgül, ss. 96-97.
[192] Council of the European Union, **EU Human Rights Guidelines on Freedom of Expression Online and Offline**, parag.6 (02.06.2020).
[193] Jack M.Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", **New York University Law Review**, Cilt 79, Sayı 1, 2004, ss.1-4, 30-32;
Council of the European Union, **EU Human Rights Guidelines on Freedom of Expression Online and Offline**, ss.2,4,10-11.

korunmasına yönelik özel yasa düzenlemelerinin yapılmasıyla daha da artmıştır. Diğer bir ifade ile, düşünce ve ifade özgürlüğünün, haber alma-bilgi edinme hakkı ile basın yayın özgürlüğünün en çok kişisel verilerin korunması hakkı ile çeliştiği söylenebilir. Bu sebeplerle, hak ve özgürlükler kullanılırken, aradaki hassas dengenin korunarak, herhangi bir ihlale sebebiyet verilmemesinin gerektiği unutulmamalıdır[194].

Avrupa Adalet Divanı'nda karara bağlanan "*İspanya Google Davası*[195]", kişisel verilerin korunması ile ifade özgürlüğü ve basın-yayın özgürlüğünün kesişme noktasında bulunmasından dolayı, bu hakların uzlaştırılarak, aralarındaki dengenin nasıl korunması gerektiği hususlarında belirleyici olmuştur.

Somut olayda Costeja Gonzalez tarafından yapılan başvuruda, hakkındaki 1998 tarihli haciz kararına ilişkin haberin, bahsedilen konu tamamen ortadan kalkmasına rağmen, ilgili gazetenin internet sitesinde halen yayınlanması sebebiyle, Google arama motoru sayfalarında kendi ismiyle arama yapıldığında gözüktüğü belirtilmiştir. Bu durum sebebiyle kişisel verilerinin ihlal edildiğini iddia eden Gonzales, bu iddia ile öncelikle 2009 yılında La Vanguardia Gazetesi'ne başvurarak, kişisel verilerine zarar verdiğini iddia ettiği haberin yayından kaldırılmasını talep etmiştir. Ancak gazete haberin resmi kaynaklara dayandığı gerekçesi ile, bu talebe olumsuz yanıt vermiştir. Bunun üzerine Gonzalez, 2010 yılında Google Spain'e başvurarak, kendi ismiyle Google'da yapılan aramaların ilgili gazetenin haberine yaptığı referansın kaldırılmasını talep etmiştir. Bu talebin olumlu karşılanmaması üzerine, konu, İspanya Veri Koruma Kurulu'nun önüne gelmiştir. Kurul, Gonzales'in talebini, La Vanguardia Gazetesi açısından, hem haberin resmi kaynaklara dayanması, hem de basın-yayın ve ifade özgürlüğünün korunması bakımından reddetmiştir. Kurul'un bu kararı ile, kişisel verilerin korunması ile basın-yayın ve ifade özgürlükleri arasındaki ince çizgiyi geçmeyerek, dengeyi korumaya çalıştığı görülmektedir. Ancak çekişme, kişisel verilerin korunmasına ve mahremiyete ilişkin

[194] Magdalena Jozwiak, "Balancing the Rights to Data Protection and Freedom of Expression and Information in the EU: The Vulnerability of Rights in an Online Context", **SSRN**, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3138296 (02.06.2020), ss.1-2, 9-11.
Aydın Akgül, ss.96-99.

[195] Judgment of the Court of Justice of the European Union (Grand Chamber), EUR-Lex, Reports of Cases, **ECJ Case C-131/12**, 13.05.2014, Google Spain SL, Google Inc. V. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 , (02.06.2020).

yasalarla bağlı olmalarından dolayı, arama motorlarının somut olayın özelliklerine göre, veriyi yayından kaldırma yükümlülüklerinin bulunabilmesi sebebiyle, Google açısından devam etmiştir. Konu İspanyol Üst Mahkemesi'ne taşınmıştır. Üst Mahkeme ise, 95/46 sayılı Kişisel Verilerin Korunması Direktifi[196] kapsamında; (1) üçüncü kişilerce yayınlanan verilerin, arama motoru operatörleri tarafından internet kullanıcıları için düzenlenerek kullanıma ve erişime hazır hale getirilmesinin, kişisel verilerin işlenmesi sayılıp sayılmadığı hususu ile; (2) üçüncü kişilerce yasal olarak elde edilip derlenerek internette yayınlanan, kişisel verilerin, sırf arama motorlarında gözükmeleri sebebiyle, kaldırılması ve silinmesi işlemlerinden, arama motoru operatörlerinin, sorumlu ve yükümlü olup olmadığı hususunu karara bağlanması için ön karar prosedürü bağlamında Avrupa Birliği Adalet Divanı'na başvurmuştur. Divan ön karar prosedürü kapsamında verdiği kararında, en önemli kişisel verilerden biri sayılan, bireyin ismi ile yapılan aramalar bakımından, arama motorlarının da kişisel verilerin korunmasına ilişkin yasalarla bağlı olduğunun altını çizmiştir. Divan, verdiği karar kapsamında ayrıca, bilgiye erişim hakkı ile mahremiyet ve kişisel verilerin korunması hakları aradaki dengenin korunması gerektiğini de ifade etmiştir. Temel haklar arasında denge kurulurken, kişisel verinin bireyin özel hayatı bakımından hassasiyet derecesinin ve kamunun bu bilginin açığa çıkarılmasındaki yararının birlikte değerlendirilmesinin gerektiğinin de altı çizilmiştir[197]. Divan tarafından verilen kararda, kişinin isminin bir kişisel veri olduğu ve bu isimle yapılacak aramaların da dolayısı ile kişisel verilerin korunması kapsamında değerlendirilmesi gerektiği kabul edilmiştir. Bu sebeple, somut olayda hak süjesi

[196] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, **Official Journal L 281**, 23/11/1995 P.0031 – 0050, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (02.06.2020);
Yukarıda belirtilen Avrupa Birliği'nin mülga "*95/46 sayılı Direktifi*", kimi Türkçe kaynaklarda "*Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Direktif*" olarak tercüme edilmektedir. İlgili Direktif, işbu tez çalışması kapsamında, "*95/46 sayılı Kişisel Verilerin Korunması Direktifi*" ya da "*95/46 sayılı Direktif*" şeklinde ifade edilmiştir.

[197] Columbia University, Global Freedom of Expression, "Google Spain SL V. Agencia Espanola de Proteccion de Patos" , **Case Analysis**, https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/ , (02.06.2020);
The London School of Economics and Political Science (LSE), "Media Policy Project Block, European Court Rules Against Google in Favour of Right to be Forgotten", http://blogs.lse.ac.uk/mediapolicyproject/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten/ ; Stefan Kulk, Frederick Zuiderveen Borgesius, "Privacy, Freedom of Expression and the Right to be Forgotten in Europe", **Cambridge Handbook of Consumer Privacy** (Ed. Jules Polonetsky, Omer Tene, Evan Selinger), Cambridge University Press, 2017, ss.17-21.

olan Gonzales'in, veri kontrolörü olan Google'dan ismiyle yapılan arama sonuçlarında gözüken ilgili bilginin bloke edilerek, kaldırılmasını talep etmeye ilişkin pozitif bir hakkının olduğu teyid edilmiştir. Bu karar, yarışan temel haklar arasındaki dengenin ne şekilde korunması gerektiğini göstermesi bakımından önem arz etmektedir. İlgili kararın yorumlanmasından, yarışan bu haklara ilişkin karar alınırken, kişisel verilerin korunması hakkına, somut olayın özellikleri gereği öncelik verildiği sonucu da çıkartılabilir[198].

2016/679 sayılı Genel Veri Koruma Tüzüğü 85.maddesinde bu durum, "*Kişisel Verilerin İşlenmesi ve İfade ve Bilgi Edinme Özgürlüğü (Processing and Freedom of Expression and Information)*" başlığı altında özel olarak düzenlenmiştir. Buna göre, kişisel verilerin, gazetecilik yapma amacıyla ve akademik, sanatsal veya edebi amaçlar da dahil, ifade ve bilgi edinme özgürlüğü çerçevesinde işlenmeleri durumunda, üye devletler yapacakları yasal düzenlemelerle, ifade ve bilgi edinme özgürlüğü ile kişisel verilerin korunması hakkını uzlaştırarak bu temel hakları dengeleyici önlemleri almakla yükümlüdürler.

2.1.3.5. Haberleşme Özgürlüğü Bağlamında Kişisel Veriler

Haberleşmenin tanım ve içeriğinin ortaya konulabilmesine ilişkin literatürde uzun yıllardır, çeşitli çalışmalar yapılmaktadır. Bu çalışmalar kapsamında, "*haberleşme*", bireylerin değişik amaç ve araçlarla yazılı-sözlü, bireysel-kitlesel, yüz yüze yahut mesafeli (uzaktan) bir şekilde kurdukları iletişim vasıtasıyla, duygu, düşünce, tecrübe, tutum, gözlem, bilgi ve veri aktarımı yapmak suretiyle, karşılıklı olarak birbirlerinin zihinlerini etkileyip dönüştürdükleri, her türlü süreç ve eylem olarak tanımlanabilmektedir. İçinde bulunduğumuz dijital çağda ortaya çıkan teknolojik gelişmeler ve bilgi toplumuna dönüşüm süreci sebebiyle, iletişim ağ ve araçları, çeşitlenip çevirimiçi alanı da kapsayarak, sınırlar ötesi geniş kitlelerce kullanılır hale gelmiştir. Bu doğrultuda günümüzde haberleşme, telefon, telgraf, faks, televizyon, radyo gibi klasik haberleşme araçları ile yapılabileceği gibi, e-posta, internet üzerinden çalışan kablolu-kablosuz ağ sistemleri, WhatsApp, Facebook, Instagram ve benzeri sosyal ağ ve dijital platformlar gibi yeni nesil iletişim araçları

[198] Magdalena Jozwiak, ss.17-23.

yoluyla da yapılabilmektedir[199]. Ayrıca hemen belirtmek gerekir ki, haberleşmenin gizliliğinin korunmasının kapsamı, hiç durmadan gelişen dijital teknolojiler göz önüne alınarak geniş yorumlanma eğilimindedir. Bu korumanın kapsamına, e-postalar, e-mesajlaşma servisleri ile internet protokol adresleri (IP) üzerinden yapılan bilgisayar bazlı ses ve görüntü servisleri, e-devlet, e-sağlık, e-okul gibi kamusal ya da e-ticaret, sosyal medya kullanımı veya diğer e-platformlar gibi özel sektör web site ve uygulamaları da dahil bilgisayar, telefon ve diğer akıllı cihazlarla internet üzerinden gerçekleştirilen her türlü iletişim şekilleri ve içlerinde barındırdıkları kişisel verilerin korunması da girmektedir[200].

Geçmişte büyük oranda kamunun üstlendiği haberleşme hizmetleri, günümüzde özel sektör tarafından da sağlanmaktadır[201]. Ancak hizmet sağlayıcısının değişmesi, kamunun, haberleşme özgürlüğünün garanti edilerek, haberleşmeye gerek üçüncü kişilerden, gerekse de kamunun kendi kurumlarından gelebilecek müdahalelere karşı gerekli önlemleri alma yükümlülüğünü ortadan kaldırmamıştır. Haberleşme yoluyla yapılan duygu, düşünce ve bilgi paylaşımının insani bir ihtiyaç olmasının yanı sıra, bireyin kişiliğinin serbestçe gelişiminin garanti edilmesi açısından da son derece önemli olduğu unutulmamalıdır. Bu sebeple kökleri, kişilik hakkı ile insan haklarını koruma yükümlülüğüne kadar giden, haberleşmenin içeriğinde kişinin kendisine ait olan ve açıklanması yalnızca kişinin kendi kontrolünde olması gereken, çok özel bilgi, duygu ve düşüncelerin bulunması ve bunların bireyin kişiliğinin gelişiminde özel yer tutması sebepleriyle, kişisel veriler bağlamında da haberleşmenin gizliliği esastır. Bu nedenlerle, iletişimde bulunan tarafların her birinin ayrı ayrı açık rızası olmadan haberleşmenin gizliliğine

---

[199] Katherine Miller, **Communication Theories: Perspectives, Processes and Contexts**, 2.Baskı, McGraw Hill, Boston, 2005, ss. 3-4-5; Hayrunnisa Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Birinci Baskı, Seçkin Yayınevi, Ankara, 2009, ss.4,6-7; Aydın Akgül, ss.377-378.

[200] Oğuz Şimşek, ss. 148-149; Frederick J. Zuiderveen Borgesius, Wilfred Steenbruggen, "The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression and Trust", Working Draft, 31 August 2018, Forthcoming, **Theoretical Inquiries in Law**, **SSRN**, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3152014 (02.06.2020), ss.15-19;
Aydın Akgül, s.87; Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communicatios), **COM (2017) 10 Final,** 2017/0003 (COD), 10.1.2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1550836328519&uri=CELEX:52017PC0010(02.06.2020); (02.06.2020), ss.2,6-8.

[201] Hayrunnisa Özdemir, s.3.

müdahale edilmesi, kişisel verileri koruma yükümlülüğünü de kapsayan haberleşme özgürlüğü bakımından kabul edilemez niteliktedir. Haberleşmenin gizliliğine, ancak, kamu güvenliğinin sağlamasına, kargaşa ve suçun önlenmesine ilişkin olarak yasalarla açıkça düzenlenmiş istisnalar kapsamında ve yasal sınırlamalara uyulması, demokratik bir toplumda hukukun üstünlüğü gereği asgari korumanın garanti edilmesi şartlarıyla, kamu tarafından dokunulabilir[202].

Çevirim dışı ve özellikle 20. yüzyıldan itibaren de çevirim içi haberleşmenin, bireyler tarafından yoğun olarak tercih edilmesi, bu haberleşmelerin ve bunlar vasıtası ile aktarılan kişisel verilerin, aktif olarak korunması bağlamında yeni adımlar atılmasını zorunlu kılmıştır. Konuyu bir vaka ile açıklamak gerekirse; 1970'li yıllarda antikacı olarak çalışan Bay James Malone'a karşı, çalıntı malları dürüstlüğe aykırı olarak elinde bulundurduğu iddiasıyla dava açılmıştır. "*Malone Davası*", olarak da bilinen bu davada, İngiliz polisinin yapmış olduğu yasadışı telefon dinleme kayıtlarının delil olarak kullanılması suretiyle, hüküm verildiği gerekçesiyle yapılan şikayet üzerine, konu Avrupa İnsan Hakları Mahkemesi'ne taşınmıştır. Mahkeme, dava kapsamında aldığı kararla, İngiltere'yi, haberleşmenin gizliliğine ilişkin olarak Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin ikinci fıkrasının ihlal edilmesi sebebi ile mahkum etmiştir[203].

Malone davasında görev alan hakimlerden biri olan Pettiti'nin hükme ilişkin olarak kaleme aldığı görüşüne göre; gelişen teknolojinin yardımı ile, özellikle 80'li ve 90'lı yıllar arasında, kişilerin özel hayatlarına, kamu otoriteleri tarafından çeşitli şekillerde müdahale etme eğilimi artmıştır. Bu durum, teknolojik gelişimin, bireylerin mahremiyetleri ve kişisel verilerinin korunması aleyhine ortaya koyduğu tehditlerinden biri olarak sayılabilir. Özellikle de kamu otoriteleri tarafından, çeşitli

---

[202] Rolf Schmidt, Stephanie Seidel, Grundrechte, 2001, Bremen, s. 257 ile Wolfgang Schulz, Verfassungsrechtlicher Schutzauftrag in der Informationsgesellschaft, in: Die Verwaltung, 1999, s.140 Aktaran Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2008, ss.148-153;

[202] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning processing of personal data and the protection of privacy in the electronic communications sector (*Directive on Privacy and Electronic Communications*) **OJ L 201**, 31.7.2002, ss.37-47, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1550756322930&uri=CELEX:32002L0058 (02.06.2020), Madde 5, 1;

T.C. Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü, İnsan Hakları Dairesi Başkanlığı, Basın Birimi**, Kişisel Verilerin Korunması-Tematik Bilgi Notu**, 2015, ss.3-5.

[203] Judgment by the European Court of Human Rights, Case of Malone v. The United Kingdom, **ECHR Application No. 8691/79**, Strasbourg, 1984, https://hudoc.echr.coe.int/ENG#{"itemid":["001-57533 , ss. 2-4, 31 (02.06.2020).

araçlarla, telefonların dinlenmesi faaliyetlerinin yaygınlaşarak, kişisel veriler içeren tapelerin kayıt altına alınıp analiz edilmesi[204], haberleşme özgürlüğü bağlamında özel hayata yapılan müdahaleleri artırmıştır. Bireylerin temel haklarının kamu otoriteleri tarafından ucu açık bir şekilde müdahaleye uğrayarak, ihlal edilmesine ilişkin olayların artması, ilgili alanda yasal düzenlemeler yapılarak, kamu otoritesinin sınırlandırılması ihtiyacını doğurmuştur. Zira kamu otoritesi karşısında temel haklar düzeyinde bireyler, oldukça kırılgan ve korunmaya muhtaç durumdadırlar. Bu sebeple, bireyin haberleşmesinin, mahremiyetinin, "*yalnız bırakılma hakkının (Right to be left alone)*", kişisel verilerinin korunması hakkının ve kişilik hakkı bağlamındaki diğer temel hak ve özgürlüklerinin tanınarak, modern teknolojinin kullanılması suretiyle yapılabilecek ihlallere karşı da korunması önemlidir. Bireyin haberleşme özgürlüğünün yapılacak yasal düzenlemeler ile desteklenerek korunmasının, kişisel verilerin korunması kapsamında kişiliğin serbest gelişimi açısından da önemli olduğu unutulmamalıdır[205].

Haberleşme özgürlüğü, pek çok bağlamda özel hayatın ve aile hayatının korunması, düşünce ve ifade özgürlüğü, basın-yayın ve haber alma özgürlükleri, kişisel verilerin korunması hakları ile kesiştiğinden, bu hakların korunarak, doğru şekilde kullanılabilmelerine de vasıta olduğu söylenebilir. Bu kesişme sebebiyle, Birlik hukukunda, haberleşme özgürlüğü, Avrupa Birliği Temel Haklar Şartı'nın "*Özel ve Aile Yaşamına Saygı*" başlıklı 7.maddesi, "*Kişisel verilerin korunması*" başlıklı 8.maddesi ile "*İfade ve Haber Alma Özgürlüğü*" başlıklı 11.maddesi kapsamında da korunmaktadır.

Dijitalleşme sürecinde, her geçen gün, genel iletişim ağı içerisindeki payını hızla artıran elektronik haberleşme, haberleşmenin gizliliğinin ve niteliği gereği içinde barındırdığı kişisel verilerin korunması hususlarında yeni ihtiyaçların doğmasına sebep olmuştur. Bu ihtiyaçlar doğrultusunda kabul edilen, 2002/58 sayılı Direktif ile, elektronik haberleşmenin güvenliğinin artırılması yoluyla, hem haberleşmenin içinde barındırdığı kişisel verilerin daha iyi korunması, hem de

[204] O dönemde yapılan analizlerde yoğun olarak "mozaik tekniği" kullanılmıştır. Kullanılan bu teknik vasıtası ile ortaya vatandaşın hayat tarzına ilişkin tam bir resim konulabilmesi mümkün olabiliyordu.
[205] Judgment by the European Court of Human Rights, Case of Malone v. The United Kingdom, **ECHR Application No. 8691/79,** ss. 38-44.

Avrupa dijital tek pazarında dijital hizmetlere ilişkin güvenin artırılarak, işlem hacminin yükseltilmesi hedeflenmektedir[206].

2.2. KİŞİSEL VERİ KAVRAMI VE SINIRLARI

Tez çalışmasının işbu alt başlığı kapsamında, kişisel verilerin kapsamlı bir tanımı yapılarak, hassas kişisel verilerin diğer kişisel verilerden ayrımı ve kişisel verilerin işlenmesi hususları örnekleriyle ortaya konmaya çalışılacaktır.

2.2.1. Kişisel Veri Tanımı

Kişisel verinin hangi kapsam ve sınırlar dahilinde, ne şekilde korunması gerektiğine ilişkin tartışmalar, hızla ilerleyen teknolojik gelişmelere ve artan internet kullanımına paralel olarak her geçen gün biraz daha alevlense de, kişisel verinin tanımı, 1980'li yıllardan beri çok büyük bir değişikliğe uğramamıştır. "*Kişisel Verilerin Korunmasına ve Sınır Ötesi Dolaşımına İlişkin Temel İlkeler*[207]" adlı Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) belgesinin 1/b Bölümü ile Avrupa Konseyi'nin imzaladığı "*Avrupa Antlaşmaları Serisi 108 numaralı Uzlaşı Belgesi*[208]" madde 2'de yer alan kişisel veri tanımı, "*Avrupa Birliği Genel Veri Koruma Tüzüğü* [209] " madde 4 kapsamında hâlihazırda kabul edilen tanımlama ile karşılaştırıldığında, bu tanımlamaların ana hatları ile aynı oldukları görülebilmektedir. Şöyle ki, yukarıda anılan 80'li yıllara ait erken dönem metinlerinde "*kişisel veri, halihazırda belirli ya da belirlenebilir bir bireye (veri*

[206] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning processing of personal data and the protection of privacy in the electronic communications sector (*Directive on Privacy and Electronic Communications*) Beyanlar 5-6, Madde 1,5;
Frederick J. Zuiderveen Borgesius, Wilfred Steenbruggen, ss.3,5-8, 15-17.

[207] OECD, Guidelines On the Protection of Privacy and Transborder Flows of Personal Data, Part 1/b, **OECD GL,** 1980, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyand-transborderflowsofpersonaldata.htm#part1 , (02.06.2020).

[208] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, **European Treaty Series Sayı. 108**, 1981, https://rm.coe.int/1680078b37 , (02.06.2020).

[209] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 29.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation "GDPR"), **Official Journal of the European Union, L 119/1**, 4.5.2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj (02.06.2020).

süjesine) ait bulunan her türlü bilgi" şeklinde tanımlanmıştır. Buradaki en önemli nokta, verinin ilgili olduğu kişinin kim olduğunun, kısmen veya tamamen işbu veri ya da elde bulunan başka veri ve bilgilerin kullanılması vasıtası ile belirlenebilir nitelikte olmasıdır.

Avrupa Birliği'nin mülga 95/46 sayılı Direktifi'nin 2. maddesinde ise erken dönemde yapılan bu tanıma ek olarak, "*kişinin kim olduğunun, doğrudan ya da dolaylı olarak bir kimlik numarasına ya da fiziksel, psikolojik, zihinsel, mali, kültürel veya sosyal kimliklerinden bir veya birkaçına atıf yapma yoluyla, belirlenebilir olmasının, ilgili verilerin kişisel veri olarak sınıflandırılmasına yol açacağının*" altı çizilmiştir[210].

25 Mayıs 2018 tarihi itibarı ile yürürlüğe girerek, 95/46/EC sayılı Direktif'in yerini alan Avrupa Birliği Genel Veri Koruma Tüzüğü madde 4/1'e göre ise, "*kişisel veri, belirli ya da belirlenebilir bir gerçek kişiye (Veri Süjesi) ilişkin her türlü bilgidir. Belirlenebilir kişi ise, bir ada, kimlik numarasına, konum verisine, çevirim içi tanımlayıcıya ya da bireyin fiziksel, fizyolojik, genetik, zihinsel, mali, kültürel veya sosyal kimliklerinden bir veya daha fazlasına, atıf yapılarak doğrudan ya da dolaylı olarak kişinin kimliğinin belirlenebilir olmasını ifade eder*".

Günümüzde kişinin kimliğinin doğrudan ya da dolaylı olarak tespitinde kullanılabilecek verilerden olan ve teknoloji ve internet kullanımının yaygınlaşması ile çeşitleri hızla artarak, her geçen gün çevirim içi ağlar üzerinden üçüncü kişilerce daha kolay erişilebilir hale gelen, "*kişiye özel sağlık verileri, kimlik, adli sicil ve sosyal güvenlik kayıtları, mali kayıtlar, vergi ve tapu kayıtları, istihdama ilişkin tutulan kayıtlar, telefon görüşmeleri, adres defterleri, IP adresleri, sms'ler, e-postalar ve sosyal medya üzerinden gerçekleşenler de dahil olmak üzere yazılı, sesli ve görüntülü olmak üzere haberleşmeye ilişkin tüm kayıtlar, fotoğraflar, konum (yer) verileri, kredi kartları ve diğer kredi işlemleri gibi çeşitli bankacılık işlemleri, banka müşteri ve hesap kayıtları ile sigortacılık işlemleri, dijital pazarda bırakılan kişiye özel izler, e-imza, DNA ve benzeri genetik özellikler, parmak izi, yüz tarama, ses ve görüntü kayıtları, retina izi uygulamaları gibi eşsiz bir şekilde kişiye özel olan biyometrik veriler, çeşitli kamu kurumları ya da özel kurumlar tarafından tutulan*

[210] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing Personal Data and on the Free Movement of Such Data, **Official Journal L 281**, 23/11/1995 ss.0031 – 0050, Madde 2.

kişiye ilişkin tüm kayıt ve arşivler" gibi benzeri pek çok veri, kişisel veri kapsamında kabul edilerek, yasalarla koruma altına alınmıştır.

Avrupa Adalet Divanı, kişisel verilerin tanımlanmasına ve bu tanıma nelerin dahil olabileceğine ilişkin vermiş olduğu pek çok kararında, sınırlayıcı davranmaktan kaçınarak konuyu geniş yorumlamıştır. Bu bağlamda Divan, nelerin kişisel veri kapsamına dahil olabileceğini, somut olayın özelliklerine göre, yorum yoluyla genişleterek, kişilerin ilgili veriler vasıtası ile, dolaylı yollardan da olsa belirlenebilir olmasını ve zarar görebilme risklerinin bulunmasını, o verinin kişisel veri sayılabilmesi için yeterli görmüştür[211]. Adalet Divanı'nın 20 Aralık 2017 tarihli "*Peter Nowak*[212]" kararı bu doğrultuda örnek gösterilebilir. Bu karara göre, 95/46 sayılı Direktif'te yer alan kişisel veri tanımında kullanılan "*herhangi bir bilgi (any information)*" ibaresi, yasa koyucunun konuyu geniş yorumlamak istediğinin açık bir ifadesini oluşturur. Bu karar kapsamında, Adalet Divanı, sınava giren adayın verdiği yanıtları, bu yanıtlar –özellikle adayın el yazısını ve entellektüel birikimini de barındırdığından- doğrudan veri süjesiyle birebir ilişkili bulunarak, kişisel veri kapsamında kabul edilmiştir[213].

Adalet Divanı'nın "*Schwarz*[214]" *kararında*, parmak izlerinin; "*Bavarian Lager*[215]" kararında, kişilerin ad ve soyadlarının yanı sıra bir toplantıya katılanların listesinin; "*Worten*[216]" kararında, çalışanların mesai saatlerini dolayısı ile de günlük çalışma ve dinlenme saatlerini içeren belgenin; "*Scarlet*[217]" kararında, internet servis

---

[211] W.Kuan Hon, Christopher Millard, Ian Walden, "The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated?- the Cloud of Unknowing", part 1, Queen Mary University of London, **Legal Studies Research Paper No.75/2011**, ss. 16-17, 40-45.

[212] Judgment of the Court of Justice of the European Union, (Second Chamber), EUR-Lex, Reports of Cases, **ECJ C-434/16**, Peter Nowak v. Data Protection Commissioner, 20.12.2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0434 (02.06.2020).

[213] Judgment of the Court of Justice of the European Union (Second Chamber), EUR-Lex, Reports of Cases, **ECJ C-434/16**, Peter Nowak v. Data Protection Commissioner, parag. 34, 36, 37, 63.

[214] Judgment of the Court of Justice of the European Union (Fourth Chamber), EUR-Lex, Reports of Cases, **ECJ C-291/12**, Schwarz v. Bochum, 17.10.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0291&rid=3 (02.06.2020).

[215] Judgment of the Court of Justice of the European Union (Grand Chamber), EUR-Lex, Reports of Cases, **ECJ C-28/08**, Commission v. Bavarian Lager Co., 29.6.2010, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0028 (02.06.2020).

[216] Judgment of the Court of Justice of the European Union (Third Chamber), EUR-Lex, Reports of Cases, **ECJ C-342-12**, Worten-Equipamentos Para o Lar SA v. Autoridade para as Condiçoes de Trabalho (ACT) (Authority for Working Conditions), 30.5.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1551084733669&uri=CELEX:62012CJ0342 (02.06.2020).

[217] Judgment of the Court of Justice of the European Union (Third Chamber), EUR-Lex, Reports of Cases, **ECJ C-70/10**, Scarlet Extended SA v. Societe Belge Des Auteurs, Compositeurs et Editeurs

sağlayıcısı (Internet Service Provider-ISP) adreslerinin; "*Englebert*[218]" kararında ise özel dedektifler tarafından toplanan verilerin, kişisel veri kapsamında değerlendirileceğini hükme bağlanmıştır. Nitekim anılan somut olaylar incelendiğinde, bu veriler kullanılarak kişilerin gerçek kimliklerinin tespit edilebilmesinin mümkün olduğu görülmüştür[219].

2.2.1.1. Hassas Kişisel Veriler

Bazı kişisel veriler, kötüye kullanımları halinde, veri süjesinin, özellikle mahremiyetinin korunmasına veya ayrımcılık yasağına ilişkin temel haklarına daha fazla zarar gelmesi ihtimalinin bulunması sebebiyle, "*hassas kişisel veriler*" olarak adlandırılırlar. Hassas kişisel veriler, diğer kişisel verilerden bu bağlamda ayrılarak, onlara nazaran daha üst bir korumadan yararlandırılırlar. Nitekim, hassas kişisel veriler, yalnızca yasalar kapsamında yetkilendirilen özel kurum ya da kamu kurumları tarafından, istisnai hallerde, sınırları çizilerek belirlenmiş amaçlarla, özel koşullar altında, işlenebilmektedirler. Birlik hukukunda, hassas kişisel verilere ilişkin, ilk açık düzenleme, mülga 95/46 sayılı Kişisel Verilerin Korunması Direktifi'nin "*Özel Kategorilerin İşlenmesi*" başlığı altındaki III. Kısım madde 8'de yapılmıştır. Bu madde ile, üye devletlerin hassas kişisel verilerin, istisnalar dışında işlenmelerini yasaklamaları gerektiğinin altı çizilerek, bu verilerin işlenebilmelerinin, ancak ve ancak veri süjesinin hiçbir tereddüte yer bırakmayan açık rızasının bulunması durumunda mümkün olabileceği belirtilmiştir. Mülga 95/46 sayılı Direktif'in kapsamından ise "*ırksal veya etnik kökene, siyasi fikirlere, dini veya felsefi inançlara, ticaret birliği üyelikleri de dahil olmak üzere, dernek, vakıf, sendika üyeliği gibi iş ilişkilerine, adli ya da cezai soruşturma ve kovuşturmaya veyahut mahkumiyete, idari yaptırımlara, işyeri performansına, siyasi parti üyeliğine, ekonomik duruma, fiziksel ya da psikolojik sağlık durumuna, biyometrik ve*

SCRL (SABAM), 24.11.2011, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=155108483381-6&uri=CELEX:62010CJ0070 (02.06.2020).

[218] Judgment of the Court of Justice of the European Union (Third Chamber), EUR-Lex, Reports of Cases, **ECJ C-473/12**, Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and others,7.11.2013, https://eurlex.europa.eu/search.ht-ml?qid=155108-4899834&text=IPI%20v.%20Englebert&scope=EURLEX&type=quick&lang=en (02.06.2020).

[219] Laraine Laudati, "Summaries of EU Court Decisions Relating to Data Protection 2000-2015", European Anti-Fraud Office **(OLAF)**, 2016, https://ec.europa.eu/anti-fraud/sites/antifraud-/files/caselaw_2001_2015_en.pdf (02.06.2020), ss. 11-12, 14-15, 21-22, 24, 25, 38.

genetik bilgilere, cinsel hayata ilişkin verilerin" hassas kişisel veriler olarak kategorize edildiği anlaşılmaktadır[220].

2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü[221]'nde ise, mülga Direktif'te yapılan tanımlama daha da geliştirilerek burada sayılanlara ek olarak "*bireyin kimliğinin belirlenmesinde kullanılabilen, eşsiz nitelikteki genetik ve biyometrik verileri ile konuma ve harekete ilişkin veriler, kişinin cinsel tercih ve eğilimleri*" de hassas kişisel veriler kapsamına alınmıştır[222].

"*Bodil Lindqvist Davası*"nda bir kilise çalışanı olan Bayan Lindqvist'in, İsveç Protestan Kilisesi'nde gönüllü olarak çalışan kişilere ilişkin kişisel verileri, veri süjelerinden rıza almadan kilisenin internet sayfasına yüklemesinin, kişisel verileri ihlal anlamına gelip gelmediği incelenmiştir. Adalet Divanı'nın bu dava kapsamında verdiği karar ile, yapılan eylem sebebiyle, ilgili veri süjelerinin kişisel verilerinin korunması kapsamındaki haklarının ihlal edildiği sonucuna varılmıştır. Zira bu veriler, kilisenin internet sayfasında yayınlanmaları suretiyle, sayısı belli olmayan internet kullanıcısının erişimine ve çeşitli serverlar aracılığı ile de otomatik veri işleme eylemlerine açık hale gelmişlerdir. Ayrıca yine aynı kararda, Bayan Lindqvist'in bir gönüllü çalışanın sağlık durumuna ilişkin aynı internet sitesi üzerinden yapmış olduğu yayının da ilgili kişinin hassas kişisel verilerinin ihlali anlamına geldiğinin altı çizilmiştir. Nitekim burada veri süjesinin, açık izni alınmadan- ayağını incittiği ve sağlık durumunda meydana gelen bu değişiklik sebebi ile yarım gün çalıştığı belirtilmiştir[223]. Adalet Divanı'nın Lindqvist Kararı, 95/46 sayılı Direktif'in 8 (1). maddesine göre[224], kişinin hem fiziki, hem de mental sağlık durumuna ilişkin verilerin, hassas kişisel verilerin korunması kapsamında olduğunu

---

[220] Article 29 Data Protection Working Party, "Advice Paper on Special Categories of Data *("Sensitive Data"*)", **Ref.Ares (2011)444105** – 20.04.2011, https://www.pdpjournals-.com/docs/88417.pdf (02.06.2020), ss.3-8.

[221] General Data Protection Regulation (GDPR).

[222] 2016/679 sayılı Genel Veri Koruma Tüzüğü kapsamında, hassas kişisel verilerin düzenlemesi konusu, işbu tez çalışmasının "*3.4.2.4. Hassas Kişisel Verilerin İşlenme Koşulları*" başlıklı bölümünde daha detaylı olarak ele alınmıştır.
GDPR, Beyanlar 10, 35, 51,56, 71, 75, Madde 4/13, 9, 14, 15.

[223] Judgment of the Court of Justice of the European Union, **ECJ Case C-101/01**, Criminal Proceedings
Against Bodil Lindqvist, 6.11.2003, http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130de32c334f6a84d4d948303f434d25f29fc.e34KaxiLc3eQc40LaxqMbN4Pb30Oe0?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=385015 , (02.06.2020).

[224] Hassas kişisel veriler, Avrupa Birliği Genel Veri Koruma Tüzüğü madde 9 kapsamında düzenlenmiştir.

ve sağlığa ilişkin verilerin bu bağlamda geniş yorumlanması gerektiğini ortaya koyması bakımlarından önemlidir[225].

2.2.2. Kişisel Verilerin İşlenmesi

"*Kişisel verilerin işlenmesi*", mülga 95/46 sayılı Direktifin 2 (b) maddesi ile onun yerini alan 2016/679 sayılı Tüzük'ün 4 (2) maddesinde tanımlanmıştır. Bu tanımlara göre, "*belirli ya da belirlenebilir veri süjesiyle ilgili her türlü kişisel verinin, otomatik olarak yahut başka herhangi bir şekilde, toplanıp kaydedilerek, düzenlenmesi, depolanması, dönüştürülüp uyarlanması, değiştirilmesi, yeniden yapılandırılması, geri alınması, bu veriye danışılmak suretiyle farklı şekillerde kullanılması, çeşitli iletişim kanalları aracılığıyla ifşa edilerek, açıklanıp yayılması ya da başkaca herhangi bir şekilde erişilebilir hale getirilmesi, değişik şekillerde hizalanıp kombine edilerek farklı amaçlarla kullanıma hazır hale getirilmesi, erişiminin engellenerek bloke edilmesi, silinmesi veya imha edilmesi ve benzeri işlemler, Birlik hukuku kapsamında kişisel verilerin işlenmesi*" olarak değerlendirilir.

Kişisel verilerin işlenmesine ilişkin hem mülga 95/46 sayılı Direktif'teki, hem de 2016/679 sayılı Tüzük'teki tanımların lafzından, bu verilerin işlenme şekillerinin ilgili maddelerde sayılanlarla sınırlı olmadığı anlaşılmaktadır. Bilgi ve iletişim teknolojileriyle internet kullanımının çeşitlenerek, yaygınlaşması sebebi ile, yasa kapsamında açıkça yazılı olmayan şekillerde de kişisel verilerin işlenebilmesi mümkün hale gelmiştir. Bu nedenle, yasada sayılanların dışında dahi olsa, kişisel verilerin, türlü şekillerde işlenmesi, 2016/679 sayılı Tüzük'ün gözetim, denetim ve sınırlamalarına tabidir[226].

Birlik hukukunda kişisel verilerin işlenmesi, bazı temel ilke ve koşullara bağlanmıştır. Bunlara 95/46 sayılı mülga Direktif'in 5. ve 6. maddeleri kapsamında değinilerek, üye devletlerin, kişisel verilerin işlenmesinin yasalar çerçevesinde ve adaletli bir şekilde yapılmasını garanti altına almaları gerektiği vurgulanmıştır. Bu

[225] Laraine Laudati, s. 40.

[226] Nilgün Başalp, "Avrupa Birliği Veri Koruma Genel Regulasyonu'nun Temel Yenilikleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (MÜHF HAD)**, 2015, Cilt.21, Sayı.1, s.85; Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Yetkin, Ankara, 2004, ss.32-33; Armağan Ebru Bozkurt Yüksel, **Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing)**, Yetkin, Ankara, 2016, s.94.

düzenlemeler ile, işlenecek kişisel verilerin, doğru ve güncel olmaları, yanlış ve eksik olanların silinmeleri veya düzeltilmeleri, toplanma amaçları sona erdiğinde ise silinmeleri, hususlarında gereken her türlü tedbiri alma konusunda da üye devletlere sorumluluk yüklenmiştir. Ayrıca kişisel verilerin işlenmesinin ancak ve ancak özel olarak açıkça belirlenerek sınırları çizilmiş, meşru amaçlar doğrultusunda yapılabileceği, toplanması sırasında belirtilen amaç ve bu amaca uygun süre dışında ise bu verilerin işlenemeyeceklerinin de altı çizilmiştir. Kişisel verilerin toplanma amaçları kapsamında tarihsel, istatistiksel ya da bilimsel amaçlarla daha uzun bir süre arşivlenebileceği özel durumlarda ise üye devletlerin bu verilerin korunmasına ilişkin olarak uygun güvenlik önlemlerini almaları gerektiği vurgulanmıştır.

Avrupa Birliği Genel Veri Koruma Tüzüğü 5.maddesinde de, mülga 95/46 sayılı Direktif'te sayılan, kişisel verilerin işlenmesinde göz önüne alınması gereken ilkeler, pekiştirilip eklemeler yapılarak sıralanmıştır. Tüzük madde 5/1 (a) ile, kişisel verilerin yasal düzenlemeler çerçevesinde ve adil bir şekilde işlenmesi gerektiğine ilişkin "*adil ve yasal işleme (Lawfulness & Fairness)*" ilkesine ek olarak, ilgili mülga 95/46 sayılı Direktif'in giriş kısmında bahsedilmekle birlikte, madde kapsamında yer almayan "*şeffaflık (Transparency)*" ilkesi de getirilmiştir[227]. Şeffaflık ilkesine göre, kişisel verilerin işlenmesine ilişkin yapılacak her türlü bildirim ve iletişimin herhangi bir yanlış anlaşılmaya izin vermeyecek şekilde açık, sade ve kolay anlaşılır bir dille yapılması gerekmektedir[228].

Tüzük madde 5/1 (b) kapsamında ise, "*amaç ile sınırlılık (Purpose limitation)*" ilkesi düzenlenmiştir. Bu ilke, kişisel verilerin, sadece, açık ve belirli, meşru amaçlarla toplanarak, bu ilk toplanma amaçları doğrultusunda işlenebilmelerini ifade eder. Kişisel verilerin işlendikten sonra arşivlenerek, daha sonra yeniden işlenebilmeleri ise, ancak ilk toplama amaçları kapsamında, tarihsel, istatistiksel, bilimsel amaçlarla veya kamu yararının gerektirdiği hallerde yapılabilmektedir. Tüzük ile getirilen bu değişiklik ile, kişisel verilerin arşivlenerek ilk toplanma amaçları kapsamında daha sonra da işlenebilecekleri haller olarak

[227] Article 29 Data Protection Working Party, "Guidelines on Transparency under Regulation 2016/679", **WP260**, adopted on 29.11.2017, as last revised and adopted on 11.04.2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (02.06.2020), s.5.
[228] GDPR, Beyanlar (39).

mülga 95/46 sayılı Direktif'te sayılan tarihsel, istatistiksel ya da bilimsel amaçlara, kamu yararının gerektirdiği hallerin de eklendiği görülmektedir.

Tüzük madde 5/1 (c) bendinde ise, işlenecek kişisel verilerin toplanma amaçları dışında tutulamayacağı ve sadece bu toplanma amaçları ile sınırlı olarak ve bu amaçla ilgili hususlarda, yeteri kadar verinin, yine yeteri kadar işlenebileceğini ifade eden "*veri minimizasyonu (Data minimisation)*" ilkesi açıklanmıştır.

Tüzük madde 5/1 (d) ile açıklanan, işlenecek kişisel verilere ilişkin "*doğruluk ve güncellik (Accuracy)*" ilkesi, mülga 95/46 sayılı Direktif'teki şekliyle aynen tekrar edilerek, bu verilerin toplanma amaçları dikkate alındığında doğru ve güncel olmadıklarının tespiti halinde silinmeleri veya düzeltilmeleri için her türlü adımın gecikmeksizin atılmasının gerektiği hususu tekrarlanmıştır.

2016/679 sayılı Tüzük kapsamında "*kişisel verilerin toplanma amacı*" sık sık vurgulanmıştır. Zira kişisel veriler bir kere toplandıktan sonra, toplanma amacını ve bu amacın gerektirdiği süreyi aşarak uzun bir zaman saklanmaları, veri süjesinin bu veriler üzerindeki kontrolünü zayıflatarak, kişisel verilerin korunmalarını zorlaştıracak niteliktedir. Kişisel verileri üzerindeki kontrolünü kaybederek, bu verilerin üçüncü kişiler tarafından bir daha ne zaman işleneceği hakkında bilgi ve öngörüsü kalmayan veri süjesinin, kişiliğini serbestçe geliştirerek, benliğini, maddi ve manevi bütünlüğünü koruyabilmesi ise mümkün olamayabilecektir. Bu sebeplerle, veri süjesinin, temel hak ve özgürlüklerinin korunması esası çerçevesinde, Tüzük'ün 5/1 (e) bendi ile, kişisel verilerin, toplanma amaçlarının gerektirdiğinden daha uzun süre saklanamayacağı anlamına gelen "*süreyle sınırlı saklama (Storage limitation)*" ilkesi düzenlenmiştir[229].

Tüzük madde 5/1 (f) bendinde ise, kişisel verilerin, "*bütünlük ve gizlilik (integrity and confidentiality)*" ilkesi gereği, yetkisiz veya yasa dışı erişim ve işleme ya da kaza sonucu oluşabilecek kayıp, tahrip, imha veya hasara karşı korunmaları gerektiği belirtilmiştir. Bu bağlamda kişisel verilerin gizliliğinin ve bütünlüğünün bozulmamasını garanti edebilecek nitelikteki teknik veya kurumsal önlemlerin alınıp, makul seviyede güvenlik koşullarının sağlanarak işlenmeleri önemlidir.

Kişisel verilerin korunması hakkının, Avrupa Temel Haklar Şartı kapsamında korunan haklardan biri olması sebebiyle, Tüzük'ün 5. maddesinin 2.fıkrası

[229] Elif Küzeci, ss.221-222.

kapsamında, veri kontrolörü [230], kişisel verilerin işlenmesinin yürütülmesinden "*hesap verebilirlik (Accountability)"* ilkesi çerçevesinde sorumlu tutulmuştur.

Tüzük'ün giriş kısmının (4). paragrafında da belirtildiği gibi, kişisel verilerin işlenmesi eyleminin, insanlığa hizmet edecek şekilde düzenlenmesi önemlidir. Bu bağlamda kişisel verilerin korunması hakkının da sınırsız bir hak olmadığının unutulmaması ve bu hak kullanılırken, toplum içindeki hassas dengelerin gözetilerek, "*orantılılık (Proportionality)"* ilkesi doğrultusunda, diğer bireylerin de temel haklarının sınırlarının korunmasına özen gösterilmesi gerekir.

Tüzük madde 6 kapsamında ise, kişisel verilerin hukuka uygun bir şekilde işlenme koşulları düzenlenmiştir. Buna göre, işlemenin hukuka uygun sayılabilmesi için madde kapsamında anılan koşullardan en az bir tanesinin somut olay bakımından gerçekleşmesi gerekmektedir. Bu koşulların en önemlilerinden biri de, veri süjesinin göstereceği rızadır. Rıza gösterilmesi öncesinde veri süjesinin işleme amaç, kapsam ve süresi ile ilgili net bir şekilde açıkça ve özel olarak bilgilendirilmesi gerekir. Ayrıca rızanın, bilgilendirmede belirtilen tüm işleme faaliyetlerini, tereddüte yer bırakmayacak bir şekilde kapsar nitelikte ve açık olması, irade beyanının da serbestçe yapılması gerekmektedir. Veri süjesinin rızası, başka hususları da içeren yazılı bir bilgilendirme yazısı ile talep edilmiş ise, kişisel verilerin işlenmesine ilişkin rıza talebinin diğer hususlardan kolayca ayrılarak anlaşılabilir bir şekilde yazılması, sade bir dil kullanılması, herhangi bir yanlış anlaşılmaya yer bırakmayacak şekilde açık ve net olması da gerekmektedir. Veri süjesi, verdiği bu rızayı, izleyeceği kolay bir prosedür aracılığıyla da her zaman geri alabilmelidir[231].

Kişisel verilerin işlenmesinin veri süjesinin açık rızasına bağlı olmadığı bazı istisnai durumlarda da kişisel veriler yasallık ilkesi çerçevesinde işlenebilmektedirler. Şöyle ki, Tüzük madde 6/1 (b)'ye göre, veri süjesinin taraf olduğu bir akdin ifası veya veri süjesinin kendi talebi ile, taraf olacağı bir akdin yapılmasından önce işlemenin gerekli olduğu hallerde; Tüzük madde 6/1 (c)'ye göre, veri kontrolörünün yasal bir yükümlülüğünü yerine getirebilmesi için işlemenin

[230] Veri kontrolörü, Tüzük'ün 4/7. maddesinde kişisel verilerin işlenme amaç ve araçlarını tek başına veya diğerleriyle birlikte belirleyen, gerçek veya tüzel kişi(ler), kamu otoriteleri ya da başka herhangi bir kurum şeklinde tanımlanmıştır.
[231] GDPR Beyanlar (32), Madde 4/11, 6, 7.

gerektiği durumlarda; Tüzük madde 6/1 (d)'ye göre, işleme faaliyetinin veri süjesinin ya da diğer bir gerçek kişinin hayati menfaatlerinin korunması için gerekli olduğu durumlarda; Tüzük madde 6/1 (e)'ye göre ise, işlemenin kamu yararına ilişkin bir görevin yerine getirilebilmesi ya da veri kontrolörüne verilen resmi yetkinin kullanılabilmesi için gerekli olduğu taktirde, istisnai olarak açık rıza olmadan da kişisel veriler yasallık ilkesi çerçevesinde işlenebilir. Ayrıca 2016/679 sayılı Tüzük'ün 6/1 f maddesine göre, veri süjesinin –özellikle de veri süjesi bir çocuksa, çocuğun korunmasına ilişkin özel hükümler saklı kalmak kaydı ile- temel hak ve özgürlüklerinin üstün olması sebebiyle öncelikli olarak korunması gerektiği haller saklı olmak üzere, veri kontrolörü tarafından gözetilen meşru çıkarların veya üçüncü kişilerin meşru çıkarlarının korunmasının gerekli kıldığı hallerde de kişisel veriler yasallık ilkesi kapsamında işlenebilecektir.

95/46 sayılı mülga Direktif'in ilgili maddeleri [232] ile onun yerine geçen Tüzük'ün 23. maddesi kapsamında temel hakların esasına dokunmamak ve toplumsal demokrasi anlayışını bozmayacak şekilde orantılı olmak kaydı ile, üye devletlerin, kişisel verilerin korunmalarına ilişkin yasa maddelerinden muaf tutulabilecekleri, istisnai haller, düzenlenmiştir. Aşağıda sayılan istisnai haller kapsamında, yasal sınırlamalara uymak şartıyla, üye devletlere muafiyet tanınabilir: "*Ulusal güvenliğin veya savunmanın gerektirdiği hallerde; ceza hukuku alanına giren suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması, kamu güvenliğinin korunmasına ilişkin tedbirlerin alınarak tehditlerin önlenmesi, adli ya da cezai yaptırımların ifası durumlarında; mali, vergi ve bütçe kaynaklı hususlar ile kamu sağlığı, sosyal güvenlik gibi konularda üye devletlerin ya da Birlik'in ekonomik veya finansal menfaatleri ve benzeri kamu yararının korumasını gerektiren hallerde; yargı bağımsızlığının korunması amacıyla; yasalarla düzenlenmiş meslek gruplarının etik kuralları ihlallerinin önlenebilmesi için, bu gibi durumların soruşturulması, tespit edilmesi veya kovuşturulmasının gerektirdiği hallerde; veri süjesinin veya diğerlerinin temel hak ve özgürlüklerinin korunmasının için gereken durumlarda; medeni hukuka ilişkin hakların icra edilmesinin gerekli kıldığı hallerde".*

[232] Mülga 95/46 sayılı Direktif madde 2/h, 3,13.

Kişisel verilerin işlenmesinin kanuni sınırlamalar dahilinde yapılarak, kişisel veri güvenliğinin ihlal edilmesini önleyecek her türlü tedbirin alınması önemlidir. Zira kişisel veri güvenliğinin ihlal edilerek, bu verilerin işlenmesinin yasal sınırlar dışına çıkması durumunda veri süjesi, kişisel verilerinin üzerindeki kontrolünü kaybedeceğinden, bu durum aynı zamanda; bireyin en önemli temel haklarından sayılan insan onurunu, kişiliğini serbestçe geliştirme hakkını, mahremiyetini, itibarını kaybetmesine; kişilerin ayrımcılığa, kimlik hırsızlığına veya dolandırıcılığa maruz kalmalarına; ekonomik kayba uğramalarına; mesleki gizlilik kapsamında korunan sırlarını yitirmelerine; rumuz sahiplerinin gerçek kimliklerinin açığa çıkmasına, veri süjesinin çeşitli düzeylerde ekonomik ya da sosyal dezavantajlarla karşılaşarak, kimi hak ve özgürlüklerini kullanamamasına yol açabilmektedir. Bu da kişisel verileri ihlal edilen bireylerin fiziksel, maddi ve manevi zarara uğramasını da beraberinde getirebilir[233]. Yine 95/46 sayılı mülga Direktif'in ilgili maddeleri[234] ile Tüzük'ün 82. maddesi kapsamında bu gibi zararların ortaya çıkması halinde veri süjesinin tazminat hakkı olduğu zikredilmiştir.

2.3. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN YASAL DÜZENLEMELER

Tez çalışmasının bu alt başlığında ise, Avrupa kıtasında kişisel verilerin korunmasının tarihsel temellerine değinildikten sonra, Avrupa hukuku kapsamında 2018 yılına gelene kadar kişisel verilerin korunmasına ilişkin yasal mevzuatın gelişimi detaylandırılarak aktarılmaya çalışılacaktır.

2.3.1. Kişisel Verilerin Korunmasının Avrupa Kıtasındaki Tarihsel Kökenleri

Avrupa'da kişisel verilerin korunmasının kökenleri, teorik olmaktan çok, yaşanan travmatik toplumsal olaylara dayanır. İkinci Dünya Savaşı öncesinde ve savaş sırasında, özelikle azınlıklardan "*ulusal güvenliği koruma*" bahanesi ile toplanan kişisel verilerin kötüye kullanımlarından kaynaklanan ciddi insan hakları

[233] GDPR Beyanlar (75).
[234] Mülga 95/46 sayılı Direktif madde 23.

ihlalleri yaşanmıştır. Nitekim o dönemde, kamu otoritesi kullanılarak toplanan kimliğe, etnik kökene, milliyete, dine dayanan veya beden ve ruh sağlığı ile politik tutum ve anlayışları konu alan kişisel veriler, bizzat devletler tarafından, kendi vatandaşlarının ayrıştırılıp, gruplaştırılmalarında kullanılmıştır. Bu gruplar, ayrımcılığa maruz kalıp, devlet eliyle toplum dışına itilerek dışlanmışlardır. Toplumun genelinden izole edilerek yaşamaya zorlanan bu kişiler, daha sonra toplama kamplarına yönlendirilerek, soykırıma kadar varan insanlık dışı muamelelere maruz bırakılmışlardır. Özellikle Musevilerin, çingenelerin, fiziksel ve ruhsal engellilerin bu dönemde maruz bırakıldıkları insan onuru ile hiç bir koşul altında bağdaşmayan muamelelerin, toplumların dimağında bıraktığı yaralar, insan hak ve özgürlüklerinin korunması fikrinin, uluslararası toplumda benimsenmesine yol açmıştır. Kişisel verilerin korunması fikrinin temelleri de insanlığın bu karanlık döneminde yaşananlar sebebiyle daha da güçlenen, insan onurunu ve mahremiyetini koruma esasından kaynaklanmaktadır. Bir başka deyişle, kişilerin kendi eşsiz kişiliklerini oluşturarak birey olabilmeleri yolunda gerekli olan insan hak ve özgürlüklerinin korunması fikrinin temellerinde yatan insan onurunun ve mahremiyetin korunması, esasen kişisel verilerin korunması fikrinin de çıkış noktasını oluşturmaktadır[235].

Avrupa'da temel hakların gelişimine ilişkin kaynaklara bakıldığında, kişisel verilerin korunması kapsamındaki erken dönem ilk yasal düzenlemenin, Federal Almanya'nın Hessen eyaletinde 1970 yılında yapıldığı görülmektedir. "*Datenschutz* [236] " olarak da anılan bu düzenleme, Hessen eyaletinde tutulan, vatandaşlara ait veri kayıtlarının, kamu kurum ve kuruluşları tarafından, depolanması, otomatik olarak işlenmesi ve bu verilerden çeşitli sonuçlar elde edilmesi faaliyetlerinin, veri sahipleri açısından yasal güvenceler çerçevesinde yapılmasının sağlanmasını ve bunlara yetkisiz erişimin engellenmesini

[235] Michael Kirby, The History, "Achievement and Future of the 1980 OECD Guidelines on Privacy", **International Data Privacy Law**, Cilt.1, Sayı.1, 2011, ss.7-8;
Cansu Çakan, "Kişilik Hakkı Kapsamında Korunan Bir Değer Olarak Kişisel Veriler", **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.12, Sayı. 2, 2013, ss.187-222; Ireland Data Protection Commissioner, "Privacy as a Human Right, Section Two", https://www.dataprotection.-ie/documents/teens/cspe%20resource%20booklet/Section_2_-_Privacy_as_a_Human_Right.pdf , ss.20-24, (02.06.2020).

[236] "*Hessisches Datenschutzgestz*", 7 Ekim 1970. Dilimize "Veri Koruma Kanunu" olarak da tercüme edilebilen kişisel verilerin korunmasına ilişkin bu yasa, verilerin sınır ötesi hareketlerine yönelik herhangi bir hüküm içermemekteydi.

hedeflemekteydi. Sadece kamu tarafından tutulan verilere ilişkin olarak Hessen eyaletinde kabul edilen bu yasa ayrıca, ilgili verinin yanlış olduğunun ileri sürülmesi halinde, veri süjesinin, verinin düzeltilmesine ilişkin talep hakkı olduğunu da hüküm altına almıştır. Ancak kişisel verilerin korunmasına ilişkin bu yasa, verilerin sınır ötesi hareketlerine yönelik herhangi bir hüküm içermemekteydi. Hessen'i takiben 1973'te, veri bankalarında tutulan kişisel verilere gereksiz müdahalelerin önlenerek, veri süjelerinin kişilik hakkının ve mahremiyetlerinin koruması amacıyla, İsveç'te kabul edilen "*Datalagen"* verilerin korunmasına ilişkin olarak yapılan ilk ulusal nitelikli yasal düzenlemedir. 1978'de ise Fransa'da yaşanan uzun ve hararetli tartışmaların ardından, bilgisayarların, bireylerin kimlikleri, özel hayat ve mahremiyetleri, bireysel ve kamusal hak ve özgürlüklerinin kullanımı açısından tehdit teşkil etmeyerek, sadece vatandaşlara hizmet etmeleri gerektiği fikirlerinden hareketle, "*Loi No 78-17 du 6 Janvier 1978 Relative a L'Informatique, aux Fichiers et aux Libertés (Law on Computers, Files and Freedoms of 6 January 1978)"* isimli veri koruma yasası kabul edilmiştir. Birbiri ardına yapılan bu düzenlemelerin, Avrupa kıtasında, kişisel verilerin korunması bağlamında farkındalık yaratarak, Birlik hukukunda kişisel verilerin korunmasına ilişkin temellerin atılmasına ön ayak olduğu söylenebilir[237].

Dijital teknolojiler ve internet kullanımı konusunda özellikle son yıllarda küresel çapta her alanda yaşanan gelişmeler, bilgisayar ağları ve internet vasıtası ile kişisel verilerin toplanıp, depolanarak, otomatik işlemeye tabi tutulmasını da kolaylaştırmıştır. Bilgi ve iletişim teknolojilerindeki bu gelişmeler de Avrupa'da kişisel verilerin korunmasının önemini yeniden ve her zamankinden daha güçlü bir şekilde gündeme getirmiş ve buna ilişkin tartışmaları kolay kolay sönmeyecek şekilde tetiklemiştir.

[237] Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", TILT (Tilburg Institute for Law, Technology and Society) **Law and Technology Working Paper Series**, No. 016/2010, http://ssrn.com/abstract=1689483 (02.06.2020), ss.5, 15-16, 61; Jan Freese, "The Swedish Data Act, Swedish Institute", **Current Sweden**, Swedish Institute, No.178, 1977, s. 1, https://www.ncjrs.gov/pdffiles1/Digitization/49670NCJRS.pdf (02.06.2020).

2.3.1.1. Kişisel Verilerin Korunmasında OECD Rehber İlkeleri

Küreselleşmenin yarattığı ekonomik, sosyal ve çevresel tehditlerle mücadele konusunda hükümetlerarası işbirliği platformu olarak kurulan OECD, kişisel verilerin öneminin anlaşılmasıyla, bunların küresel anlamda korunmasında da öncü bir rol oynayarak, 1980 yılında "*Kişisel Verilerin Mahremiyetinin ve Sınır Ötesi Hareketlerinin Korunmasına ilişkin Rehber İlkeleri (Rehber İlkeler - The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data)*" ortaya koymuştur. Bugün dahi geçerliliğini koruyan bu Rehber İlkeler, kişisel verilerin korunması alanında bağlayıcılığı olmasa da yol gösterici niteliğinde olan uluslararası ilk düzenleme olması bakımından önemlidir. Ayrıca bu Rehber İlkeler, küresel ekonomi alanında kişisel verilerin korunmaları gerektiğinin uluslararası toplumda kabul edildiğini belgelemesi ve ulusal veri koruma yasalarının oluşturulmasında etkili olması açılarından da önemlidir[238].

OECD tarafından ortaya konan Rehber İlkeler incelendiğinde ilk sırayı "*Kişisel Verilerin Toplanmasında Sınırlılık (Collection Limitation Principle)"* ilkesinin aldığını görmekteyiz. Bu ilkeye göre, kişisel verilerin toplanmasında önceden belirlenip sınırları çizilen amaca bağlı kalınması, toplama işleminin yasal sınırlamalara uyularak, adil bir şekilde ve veri süjesinin bilgisi dahilinde yapılması gereklidir. Aynı doğrultudaki "*Amacın Belirliliği (Purpose Specification Principle)"* ilkesi kapsamında da, kişisel verilerin ne amaçla toplandıkları, veri toplama işlemi öncesinde nitelendirilip sınırlandırılarak belirlenmiş olmalıdır. Veri süjesinin rızasının bulunması veya yasal zorunluluk sebeplerine dayanan istisnai haller dışında, "*Kullanımın Sınırlılığı (Use Limitation)"* ilkesi gereği, kişisel veriler özel olarak tanımlanıp, önceden belirlenen toplanma amaçları dışında kullanılamaz, açıklanamaz ve başka herhangi bir şekilde erişime açılamaz. "*Veri Kalitesi (Data Quality)*" ilkesine göre ise, kişisel veriler, kullanılacakları amaçlara uygun ve bu amaçların gerçekleştirilebilmesi için gerekli olmalı, doğru, eksiksiz ve güncel durumda bulunmalıdırlar. "*Güvenlik Önlemleri (Security Safeguards)" ilkesi*

[238] OECD, **Thirty Years After the OECD Privacy Guidelines**, 2011, http://www.oecd.org/sti/ieconomy/49710223.pdf , (02.06.2020) ss.3, 6, 11;
OECD, **The OECD Privacy Framework**, 2013, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf , (02.06.2020) s.19.

bağlamında da, kişisel veriler kayıp, yetkisiz erişim ve kullanım, imha, değişiklik veya ifşa gibi risk unsurlarına karşı makul güvenlik tedbirleri alınmak sureti ile korunmalıdırlar. "*Açıklık (Openness)*" ilkesi ise kişisel verilere ilişkin gelişmeler, uygulamalar ve politikalara yönelik genel bir şeffaflık politikasının bulunmasının gerekliliğini ifade eder. "*Bireysel Katılım (Individual Participation)*" ilkesi uyarınca ise, veri süjesinin, veri kontrolöründen ya da başka bir yetkili kişiden, ellerinde kendisine ait veri bulunup bulunmadığının teyidini isteme; kendi kişisel verilerine ilişkin haberleşmenin, makul sürede ve -eğer gerekli ise- makul bir ücret karşılığında, kolayca anlaşılır bir formda yapılmasını talep etme; veri süjesinin kişisel verilerine ilişkin taleplerinin reddedilmesi durumunda red gerekçelerinin bildirilmesini isteme ve bu gerekçelere itiraz edebilme; kendi kişisel verilerinin aksini iddia edebilme ve bu iddiasında haklı ise ilgili verileri sildirme, düzelttirme, tamamlatma ya da tadil edilmesini isteme hakları bulunmaktadır. Bireysel Katılım İlkesi, kişisel verilerin korunması sürecine veri süjesinin pro-aktif olarak katılımına imkan vermesi bakımından önemlidir. "*Hesap Verebilirlik (Accountability)*" ilkesi ise, veri kontrolörünün kişisel verilerin korunmasına ilişkin Rehber İlkeler doğrultusunda gerekli tedbirleri alarak, bu tedbirlere ve Rehber İlkelere uygun hareket etmekle yükümlü olmasını ve yaptığı eylemlerden sorumlu tutulabileceğini ifade etmektedir[239].

Rehber ilkeler, günümüze kadar güncelliğini korusa da, teknolojik gelişmelere paralel bir şekilde her alanda artan dijitalleşme ve değişen pazarlar ve tüketici davranışları gibi sebeplerle, 2013 yılında yeniden gözden geçirilerek güncellenmiştir. Zira dijital çağda, işlenen kişisel verilerin miktarının, veri toplayan aktörlerin sayısının ve bu aktörlerin verileri işleme çeşitlerinin artması, verilere erişimin kolaylaşması ile birlikte mahremiyet ihlal ve tehdit oranlarının yükselmesi, kişisel verilerin sosyal ve ekonomik değerlerinin anlaşılması gibi sebeplerle, kişisel verilerin değişen bu koşullarla birlikte ortaya çıkan yeni tehdit ve ihtiyaçlara yönelik olarak korunmasının önemi de artmıştır[240]. Kişisel verilerin korunması alanında ortaya çıkan yeni gereksinimler karşısında, OECD üç alanda daha yeni ilkeler ortaya

[239] OECD 2011, ss. 21-22; OECD 2013, ss. 14-16; Marit Hansen, Ari Schwartz, Alissa Cooper, Identity Management, "Privacy and Identity Management", **IEEE Computer Society**, 2008, https://cdt.org/files/privacy/2008schwartzcooper.pdf , (02.06.2020) s.39.
[240] OECD 2013, ss.3-4.

koymuştur: "*Veri Güvenliği İhlal Bildirimi* (*Data Security Breach Notification)*; *Gizlilik Yönetimi Programları* (*Privacy Management Programme)*; *Gizlilik İcra Makamları* (*Privacy Enforcement Authorities*)*"*.

"Gizlilik Yönetimi Programları İlkesi", önemi gittikçe artan Hesap Verebilirlik İlkesi ile bağlantılıdır. Bu ilkeye göre, ulusal hukuk kuralları vasıtasıyla kişisel veri mahremiyetinin korunması amacıyla, çeşitli gizlilik yönetimi programları oluşturularak, kamusal ve özel veri kontrolörlerinin hesap verebilirliğini artırmak önemlidir. Bu programlar vasıtasıyla ortaya koyularak aktif hale getirilecek, yeni mekanizmalar yardımıyla, mahremiyetin korunması amacıyla kurumsal sorumluluk oluşturulmaya çalışılmaktadır. Veri kontrolörlerinin ve gizlilik hükümlerini uygulamaya yetkili tüm diğer kişilerin, şeffaflık yükümlülüklerine uygun davranmalarının teminine yönelik faaliyetler ile veri kontrolörünün kişisel verilerin işlenmesine ilişkin makul güvenlik tedbirlerini almasının sağlanmasına yönelik faaliyetler, "*Gizlilik Yönetimi Programları İlkesi"*nin iki önemli örneğini oluşturur[241].

Kaybolma, yetkisiz erişim ve kullanım, imha, değiştirme veya ifşa gibi tehditlere ilişkin olarak, kişisel verilerin, makul güvenlik tedbirleri vasıtasıyla korunması da önemlidir. Ancak alınan tedbirlere rağmen hackerlar, dikkatsiz ve eğitimsiz çalışanlar, taşınabilir cihazları çalan adi hırsızlar v.b. sebeplerle veri güvenliğinin ihlal edilmesi halinde, veri süjeleri önemli kayıplarla karşı karşıya kalabilirler. Bu nedenle böyle bir ihlalin gerçekleşmesi durumunda, *"Veri Güvenliği İhlal Bildirimi İlkesi"* gereğince, veri kontrolörü, vakit kaybetmeksizin veri süjesi ve diğer yetkilileri ihlalden haberdar etmekle yükümlüdür[242].

2013 yılına gelinceye kadar, ne 1980 tarihli Rehber İlkelerde, ne de 2007 yılında ortaya konan tavsiye nitelikli kararlarda "*Gizlilik İcra Makamları"* oluşturulmasına ilişkin açık bir hüküm bulunmamaktaydı. Ancak uluslararası veri hareketliliğinin hacim, çeşitlilik bakımlarından artması, güvenlik ihlallerinin boyutlarının da büyümesine sebep olduğundan, 2013 yılında yapılan revizyon ile uygulamada esneklik sağlayarak güvenliği artıracağı öngörülen bu makamların kurulmasının gerekliliği açıkça belirtilmiştir. Bu bağlamda, Kişisel Verilerin Mahremiyetinin ve Sınır Ötesi Hareketlerinin Korunmasına ilişkin Rehber İlkelerle

[241] OECD 2013, ss.23-25.
[242] OECD 2013, ss.26-27.

İlgili Konsey'in Tavsiye Kararı'nın 5.bölümde[243], üye devletlere de, gerekli kaynak ve teknik bilgiye sahip, her türlü baskıdan uzak, bağımsız ve tarafsız olarak görevini ifa ederek objektif kararlar alabilecek nitelikteki "*Gizlilik İcra Makamlarının*" oluşturulması çağrısı yapılmıştır[244].

OECD tarafından ortaya konan tüm bu Rehber İlkelere ilişkin olarak şunu da belirtmek gerekir ki; bu İlkeler, ekonomik ve ticari amaçlarla işlenen kişisel veriler için geçerlidir. Kolluk kuvvetleri ya da haber alma teşkilatları tarafından işlenen kişisel veriler ise OECD ilkelerinin kapsama alanı dışında kalmaktadırlar[245].

2.3.1.2. 108 No'lu Avrupa Konseyi Sözleşmesi

80'li yıllarda artan teknolojik gelişmeler ve internet kullanımı, ticaret hayatında köklü değişikliklere yol açarak, kişisel verilerin sınır ötesi hareketliliğini de artırmıştır. Bu artışın bir gereği olarak, kişisel verilerin uluslararası düzeyde korunmasının önemi, uluslararası arenada masaya yatırılmış ve Avrupa Konseyi kişisel verilerin otomatik işlenmesi karşısında, gerçek kişilerin temel hak ve özgürlüklerinin ne şekilde korunabileceğine ilişkin yasal alt yapı çalışmalarına başlamıştır. Bu çalışmalar sonucu Avrupa Konseyi tarafından düzenlenerek ortaya konan ve "*108 No'lu Sözleşme*" olarak da anılan "*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (Convention for the Protection of Individuals with Regard to Authomatic Processing of Personal Data)*", 1981 yılında imzaya açılmıştır[246]. 108 No'lu Sözleşme, uyruklarına bakılmaksızın, taraf devletlerde ikamet eden tüm gerçek kişilerin, kişisel verilerinin, kamuda veya özel sektörde otomatik olarak işlenmesi karşısında, temel hak ve özgürlüklerinin güvence altına alınmasının sağlanması amacını taşır. 108 No'lu bu Sözleşme, Avrupa kıtasında bölgesel düzeyde yürürlüğe giren, bağlayıcı niteliğe sahip ilk çok

[243] OECD, Recommendation of the Council concerning OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, **OECD/Legal/0188,** https://legalinstruments.oecd.org/public/doc/114/114.en.pdf , s.17, (02.06.2020).
[244] OECD 2013, ss.28-29.
[245] Christina Blasi Casagran, **Global Data Protection in the field of Law Enforcement: An EU Perspective, Routledge**, 1. Baskı, Oxon & New York, 2017, ss.214-215.
[246] Türkiye bu Sözleşmeyi 28 Ocak 1981 tarihinde imza altına almışsa da Sözleşme ancak 18 Şubat 2016 tarihinde uygun bulunarak 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazetede yayımlanarak iç hukukumuz açısında bağlayıcı hale gelmiştir.

uluslu düzenleme olması bakımından önemlidir [247] . Ayrıca bu Sözleşmenin, bireylerin kişisel veriler üzerindeki hak sahipliğini ve bu verilerin neden ve ne şekilde korunması gerektiğini ortaya koyarak, hem Birlik hukukuna, hem de ulusal düzenlemelere aktarımının sağlanması bakımından öncü nitelikte olduğu da unutulmamalıdır[248]. Zira 108 No'lu Sözleşme'nin hazırlanmasında, Komisyon, aktif bir rol oynayarak, kişisel verilerin korunmasına ilişkin kendi bakış açısını bu Sözleşme'nin içeriğine de yansıtmıştır. Bu sebeple, 108 No'lu Sözleşme'nin Avrupa Birliği'nin kişisel verilerin korunmasına ilişkin yapmış olduğu yasal düzenlemelerin tabanını oluşturduğu da söylenebilir[249].

2.3.1.3. Bilginin Geleceğini Belirleme Hakkı ve Nüfus Sayımı Kararı

1983 yılında Federal Alman hükümeti, istatistiki amaçlarla bilgi toplamak ve planlama yapmak için kişisel hayat, iş ve çalışma hayatı ile yaşam koşullarına ilişkin 160 soruluk bir anketin Alman vatandaşları tarafından cevaplanmasını da içeren nüfus sayımı kararını almıştır. Ancak Alman tarihinin en karanlık sayfalarını oluşturan İkinci Dünya Savaşı döneminde toplanan kişisel veriler, kötüye kullanılarak, Alman vatandaşlarının ayrıştırılıp katledilmesine kadar varan insan hakları ihlallerine sebebiyet verdiğinden, bu karanlık dönemde yaşanan ve bugün dahi izleri devam eden travmalar, Alman halkında, mahremiyetin ve kişisel verilerin korunmasının ne denli önemli olduğuna dair farkındalığın, erken oluşmasına yol açmıştır[250]. Alınan bu kararla toplanacak kişisel verilerin, ileriki yıllarda bireylerin kontrolü dışında çeşitli şekillerde işlenebileceği ve neticede de temel hak ihlallerine sebep olabileceği ihtimalinden hareketle, nüfus sayımı kararı, Alman kamuoyunda büyük rahatsızlıklara, tartışma ve protestolara neden olmuştur. Kamuoyundaki bu rahatsızlık, aynı yıllarda etkileri hissedilmeye başlayan dijitalleşme sonucu bilgilerin

[247] Avrupa Konseyi, 108 No'lu Sözleşme Metni, https://rm.coe.int/1680078b37 (02.06.2020) Madde 3 "Kapsam"; Christopher Kuner, 2010, s. 5; Armağan Bozkurt Yüksel, 2016, s.62; İstanbul Bilgi Üniversitesi, İnsan Hakları Hukuku Uygulama ve Araştırma Merkezi, **Duyurular**, https://insanhaklarimerkezi.bilgi.edu.tr/tr/news/none-kisisel-verilere-dair-sozlesme-bakanlar-kurul/ , (02.06.2020).
[248] Nilgün Başalp, 2015, s.79.
[249] Christina Blasi Casagran, ss.225-227.
[250] Alvar C.H. Freude, Trixy Freude, "Echos of History: Understanding German Data Protection", Bertelsmann Foundation, **Newpolitik**, https://www.bfna.org/wp-content/uploads/2017/04-/Echoes_of_history_Understanding_German_Data_Protection_Freude.pdf (02.06.2020), ss.1-2, 6.

sanal ortamdaki izlerinin sonsuza kadar var olarak, bunlara herkes tarafından erişilebileceği gerçeğiyle de birleşince daha da şiddetlenmiştir. Sonuçta, konu muhalif kesim tarafından anayasaya aykırılık iddiası ile Federal Alman Anayasa Mahkemesi *(Bundesverfassungsgericht)*'nin önüne getirilmiştir. Konuyla ilgili olarak yaptığı incelemeler sonucu, Anayasa Mahkemesi, o yıllarda Almanya'da kişisel verilerin korunmasına ilişkin özel bir yasal düzenlemenin olmadığı hususunu da göz önünde tutarak, "*15 Aralık 1983 tarihli Nüfus Sayımı Kararını (Census Act, BVerfGE 65, 1, Population Census Decision of the German Federal Constitutional Court)*" almıştır[251].

Nüfus Sayımı Kararı ile Anayasa Mahkemesi, Alman Anayasa Hukuku kapsamında kişisel verilerin korunması bakımından büyük bir adım atarak, ortaya iki önemli sonuç koymuştur: Bunlardan birincisi "*Bilginin Geleceğini Belirleme Hakkı (Informational Self-determination)"*nın tanımlanıp sınırlarının çizilerek kabul edilmesi; bir diğeri ise kişisel verilerin korunmasına ilişkin bazı temel ilkelerin açıklığa kavuşturulmasıdır[252].

"*Bilginin Geleceğini Belirleme Hakkı*"nı öncelikle inceleyecek olursak, bu hakkın, Alman hukukunda kişisel verilerin korunması hakkının temel çıkış noktasını teşkil ettiği söylenebilir. Bireylerin kendi kişisel verilerinin geleceğini, kendilerinin tayin etmesi olarak da tanımlanabilen bu hak, Federal Alman Anayasa Mahkemesi tarafından bireyin onur ve saygınlığının korunması hakkı ile kişiliğini serbestçe geliştirme hakkına dayandırılmıştır[253].

Yaşanan teknolojik gelişmeler sayesinde, dijital alanda toplanarak depolanan kişisel verilerin, analiz edilip birleştirilerek, aralarında çeşitli bağlantılar kurulması yoluyla, veri süjelerine ilişkin pek çok özel çıkarım ve saptamalar yapılmasına imkan verdiğine şüphe yoktur. İnternet ortamında, verilerin, toplanma, depolanma, kullanılma ve aktarılma gibi sonsuz ve sınırsız işlenme kapasitelerinin olduğu artık apaçık ortadadır. Bu sınırsızlık karşısında bireylerin onur ve saygınlıkları temelinde

---

[251] Census Act, "English Translation of Essential Parts of the German "Volkszahlungsurteil" from 15 December 1983, which established in Germany the Basic Right on Informational Self-Determination", **BVerfGE 65,1**, https://freiheitsfoo.de/census-act/ , (02.06.2020), s.2;
Gerrit Hornung, Christoph Schnabel, I-2009, ss.84-85.

[252] Oğuz Şimşek, ss.114-117.

[253] Joseph A. Cannataci, "Lex Personalitatis & Technology-driven Law", **Scripted**, Cilt.5, Sayı.1, 2008, https://www.um.edu.mt/library/oar/bitstream/123456789/17704/1/OA%20%20%20%20-Lex%20Personalitatis%20%26%20Technology-driven%20Law.pdf (02.06.2020) s.2.

kişilik hakkının ve mahremiyetlerinin korunması için özel bir çaba gösterilmesi gerektiği, şüphe götürmemektedir. Zira yaşanan bu gelişmeler neticesinde kişisel verilerin nasıl, ne şekilde ve hangi zaman diliminde toplanacağı ve işleneceği hususlarında bireyler neredeyse savunmasız kalmışlardır. Kişisel verilerin işlenip analiz edilmesiyle, her türlü bilgiye ulaşılmasının kolaylığı, bireylerin kamusal ve sosyal ortamlarda ve hatta kendi özel alanlarında dahi, fişlenme, alenileşme ve sınıflandırılarak, ayrımcılığa uğrama çekincesi sebebi ile, baskı altında hissederek, kendilerini doğru ve açık bir şekilde ifade etmekten kaçınmalarına yol açabilmektedir. Kendini herhangi bir baskı altında kalmadan ve tehdit hissetmeden, açık ve doğru bir şekilde, ifade edemeyen bir bireyin demokrasinin temel ilkelerinden olan kişiliğini serbestçe geliştirebilme imkanına sahip olduğundan bahsedebilmek de mümkün olamayacaktır. Bu da temel hakların ilk çıkış noktasını oluşturan insan onurunun ve saygınlığının korunması ilkesi ile kesinlikle bağdaşmamaktadır. Bu noktalardan hareketle, Federal Alman Anayasa Mahkemesi konuyu, kişilik hakkı çerçevesinde ele alıp, insan onurunun korunması ile de doğrudan bağlantı kurarak, kişisel verilerin korunmasının, bireylerin kişiliklerini serbestçe geliştirebilmelerinin anahtarı olduğunu belirtmiştir. Mahkeme, ayrıca, bireylerin kişisel verilerinin hangilerini, ne kapsamda, hangi zaman dilimi içinde ve sürede, ne amaçla paylaşacaklarını kendilerinin belirlemelerinin demokratik bir toplum için vazgeçilmez nitelikte olduğunu da belirterek, bilginin geleceğini belirleme hakkının bireyin kendisine bırakılması gerektiğinin altını almış olduğu Nüfus Sayımı Kararı ile net bir şekilde çizmiştir. Bu karar ile insan onurunun korunması ile doğrudan bağlantı kurulan bilginin geleceğini belirleme hakkı, anayasal korunma altına alınarak, bireylere bir "*anayasal temel hak*" olarak tanınmıştır[254].

Nüfus Sayımı Kararı ile mahkeme, her ne kadar kişisel verilere kamu yararına meşru müdahale imkanının olduğunu belirtse de, kişisel verilerin

[254] Census Act, **BVerfGE 65,1**, ss.2-4, 6-8;
Nikola Werry, Benjamin Kirschbaum, Jens-Marwin Koch, "Germany", **The Privacy, Data Protection and Cybersecurity Law Review** (Ed. Alan Charles Raul), 4.Baskı, The Law Reviews, UK, 2017, s. 131;
Gerrit Hornung, Christoph Schnabel, I-2009, ss.85-87; Anoek Baars, The Value of Personal Data in a Competitive Information Age, **Master Thesis,** University of Oslo, Faculty of Law https://www.duo.uio.no/bitstream/han-dle/10852/51383/8011_ICTLTHESIS.pdf?sequence=1 (02.06.2020) ss.9-10.

mahremiyetlerine dokunabilecek nitelikteki kamusal faaliyet ve müdahalelerin dahi anayasal sınırlamalara uygun yapılması gerektiğini önemle vurgulamıştır[255]. Kararda ayrıca kişisel verilerin, kamu yararına ilişkin meşru müdahale istisnasının dışında, veri süjesinin konuya ilişkin bilgilendirilmesine müteakip serbestçe vereceği rızası olmaksızın işlenmesinin mümkün olmadığı da belirtilmiştir[256].

Nüfus Sayımı Kararı ile, kişisel verilerin korunması hususunda, gelecekte Avrupa Birliği hukukunda da temel alınacak, bazı bilindik ilkeler bir kez daha ortaya konulmuştur. Buna göre, kişisel verilere yapılacak her türlü müdahalenin, açıkça yasal temellere dayandırılması ve veriler işlenirken yasal düzenlemelerden kaynaklanan sınırlamalar dahilinde hareket edilmesi gerekmektedir. Kararda ayrıca, kişisel verilerin belirli, sınırlı ve açık bir amaç için işlenmesinin esas olduğu, önceden belirlenen işleme amacının dışına çıkılmaması gerektiği ve orantılılık ilkesi çerçevesinde hareket edilmesinin önemi de vurgulanmıştır[257].

2.3.2. Avrupa Birliği'nde Kişisel Verilerin Korunmasına İlişkin Yasal Mevzuat

Tez çalışmasının bu bölümünde Avrupa Birliği'nde 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün kabulüne kadar geçen sürede kişisel verilerin korunmasına ilişkin olarak yapılan çeşitli yasal düzenlemeler incelenecektir.

---

[255] Gerrit Hornung, Christoph Schnabel, "Data Protection in Germany II: Recent Decisions on Online-searching of Computers, Automatic Number Plate Recognition and Data Retention", **Computer Law & Security Review**, Cilt.25, Sayı.2, 2009, s. 118;
Census Act, **BVerfGE 65,1**, s. 8.

[256] Census Act, **BVerfGE 65,1**, s. 2;
Oğuz Şimşek, s. 116.; Anoek Baars, s.10.

[257] Census Act, **BVerfGE 65,1,** ss. 2-3, 9-11; Gerrit Hornung, Christoph Schnabel, I-2009, s. 87; Gerrit Hornung, Christoph Schnabel, II-2009, ss. 118,121,122;
Wayne Madsen, **Handbook of Personal Data Protection**, 1.Baskı, Palgrave Macmillan, UK, 1992, s.36.

2.3.2.1. 95/46 Sayılı Kişisel Verilerin Korunması Direktifi[258]

Dijitalleşmenin ve internet kullanımının artmasıyla, web siteleri ve mobil uygulamalar üzerinden bilgisayarlar ve akıllı cihazlarla yapılan satın alma, ödeme, araç kiralama, otel rezervasyonları gibi günlük hayatımızda gerçekleştirdiğimiz sıradan işlemler neticesinde, alışveriş sıklığı ve tercihlerimiz; seyahat planlarımız gibi, çeşitli ihtiyaç, eylem ve eğilimlerimize ilişkin kişisel verilerimizi de içeren kalıcı izler, çevirimiçi ağa aktarılmaktadır. İşlemlerimizin ağ ortamıyla her karşılaşmasında bırakılan bu izlerin, çoğalarak, tüm ağ boyunca küresel düzeyde yayılması, depolanması ve üçüncü kişilerin erişimine açık hale gelerek işlenmesi ile, veri süjelerine ilişkin çeşitli analiz ve çıkarımlar yapılabilmesi imkanı da doğmuştur. Önceden tahmin dahi edilemeyen hacim ve boyutlara ulaşan dijital ortamdaki bu verilere ulaşmanın kolaylığı, en temel insan haklarından sayılan mahremiyetin ve kişisel verilerin korunmasının ne denli zorlaştığı gerçeğini su yüzüne çıkararak, bu konudaki ihlalleri de artmıştır. Bu ortamda, Birlik içindeki bazı üye devletlerin vatandaşlarının kişisel verilerinin korunmasına ilişkin farkındalıklarının, diğer üye devletlerden görece daha fazla olması sebebiyle, bu devletler, ulusal sınırları dışına veri transferi yapılması konusunda diğerlerine nazaran daha hassas davranma yolunu seçmişlerdir. Bu hassasiyet sonucu, kimi üye devletler tarafından yapılan düzenlemeler ile, Birlik dışına olduğu gibi, Birlik içi veri transferlerine de bazı sınırlamalar getirilmiştir. Ancak bu sınırlamalar sebebiyle, ticari bir değere haiz mal olduğu kabul edilen verilerin, Birlik içi sınırlar arası akışının bozulması, malların serbest dolaşımı esasına dayanan tek pazar dinamiklerini olumsuz etkileyerek, Avrupa tek pazarının işleyişinin de aksaması sorununu ortaya çıkarmıştır. Bu bilinçle, Birlik tarafından verilerin kişisel olmayan veriler[259] ve kişisel veriler

[258] 95/46 sayılı Kişisel Verilerin Korunması Direktifi, 25.05.2018 tarihinde yürürlükten kaldırılarak, yerini 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'ne bırakmıştır.
Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, **OJ L 281**, 23/11/1995 ss.0031-0050, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (02.06.2020).

[259] İşbu tez çalışmasının önceki bölümlerinde detaylı olarak işlenen kişisel olmayan verilerin, serbest dolaşımına ilişkin olarak kabul edilen 2018/1807 sayılı Birlik Tüzüğü'ne aşağıdaki linkten ulaşılabilir: European Union, "Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union", 28.11.2018 **Official Journal of the EU L 303/59**, https://eurlex.europa.eu/legalcontent/EN/TXT-/?qid=1544179728555&uri=CELEX:32018R1807 (02.06.2020).

şeklinde ayrımı yapılarak, üye devletlerin kişisel verilerin korumasına ilişkin olarak hazırlayacakları ulusal yasalarının oluşturulmasında temel teşkil edecek asgari ilke, koşul ve sınırlamaları içeren, çerçeve niteliğindeki "*95/46 sayılı Kişisel Verilerin Korunması Direktifi*", 24 Mayıs 2018 tarihine kadar geçerli olacak şekilde kabul edilmişti[260]. Bu çerçeve düzenlemeyle, temel haklara saygılı, daha öngörülebilir ve istikrarlı ticari bağları olan ve getirilen çerçeve hükümler kapsamında kişisel verilerin makul seviyelerde korunduğu, daha fazla bütünleşmiş bir tek pazar oluşturma yolunda, önemli bir adım daha atılması hedeflenmişti[261]. 25 Mayıs 2018 itibarı ile 95/46 sayılı Direktifin yerini alan ve tez çalışmasının Üçüncü Bölümünde incelenecek olan, 2016/679 sayılı Tüzük'ün mantığının daha iyi anlaşılabilmesi için, mülga 95/46 sayılı Direktif'in kişisel verilerin korunması kapsamında getirdiği düzenlemeleri ana hatlarıyla incelemekte fayda vardır.

Mülga 95/46 sayılı Direktifin ikinci maddesinde, "*kişisel veri, kişisel verilerin işlenmesi, kişisel veri dosyalama sistemi*, *kontrolör, işleyici, üçüncü kişi, alıcı, veri süjesinin rızası*" gibi temel kavramların açık tanımlamalarına yer verilerek, bu terimlerin her bir üye devlette aynı anlam ve içeriğe kavuşması amaçlanmıştır. Böylelikle de Birlik genelinde kişisel verilerin korunması hususunda anlam kargaşası yaşanmasının önüne geçilmeye çalışılmıştır.

Madde 3/1 incelendiğinde mülga 95/46 sayılı Direktif'in kapsamının, kısmen veya tamamen otomatik işlenmeye tabi tutulan kişisel veriler ile otomatik olarak işlenmese dahi dosyalanarak depolanan veya daha sonra depolanabilecek nitelikte olan kişisel verilerin işlenmelerine ilişkin faaliyetleri kapsadığı görülmektedir. Aynı maddenin ikinci fıkrasında ise, işbu Direktif'in uygulanmasına istisna teşkil eden durumlar sayılmıştır. Buna göre, Birlik hukukunun kapsamı dışında kalan faaliyetler

---

[260] Avrupa Parlamentosu ve Konseyinin, 24 Ekim 1995 tarihli ve 95/46 sayılı Kişisel Verilerin İşlenmesine İlişkin Olarak Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımlarının Sağlanmasına Yönelik Direktifi,
EUR-Lex, 31995L0046, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046, (02.06.2020);
Julia M. Fromholz, "The European Union Data Privacy Directive", **Berkeley Technology Law Journal**, Cilt. 15, Sayı.1, 2000, ss.461-463, 467-468; Peter P. Swire, Robert E. Litan, "None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive", **Harvard Journal of Law & Technology**, Cilt.12, Sayı. 3, 1999, ss. 483-484;
W. Scott Blackmer, GDPR: Getting Ready for the New EU General Data Protection Regulation, **Info Law Group**, 2016, https://www.infolawgroup.com/insights/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation , ss.1-2, (02.06.2020).

[261] Mülga 95/46 sayılı Direktif Beyanlar (1,3);
Mülga 95/46 sayılı Direktif, madde 1.

ile her şekilde kamu güvenliğine, savunmasına, devlet güvenliğine, yapılan işlemler devletin güvenliğini ilgilendirdiği sürece devletin ekonomik refahına ilişkin işlemler ile; devletin ceza hukuku alanındaki faaliyetleri; sadece kişisel amaçlarla veya hane içi faaliyetler dahilinde bireyler tarafından gerçekleştirilen işlemeler, istisna kabul edilerek, işbu Direktif'in uygulanma kapsamı dışında tutulmuştur.

Mülga 95/46 sayılı Direktif'in 11.paragrafında Avrupa Konseyi'nin 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne doğrudan atıf yapılarak, 108 No'lu işbu Sözleşme'de vurgulandığı gibi, kişisel verilerin, temel hak ve özgürlükler kapsamında güçlü bir şekilde korunması gerektiğinin altı çizilmiştir.

Üye devletlerin veri işleme faaliyetlerini yasallık ilkesi çerçevesinde yapabilmeleri ve veri kalitesini koruyabilmeleri için hangi ilkeler doğrultusunda hareket etmeleri gerektiği, mülga 95/46 sayılı Direktifin 5. ve 6.maddeleri kapsamında "*Amaç ile Sınırlılık*" ve "*Adil ve Yasal İşleme*" ilkeleri dahilinde açıklanmıştır. Bu ilkeler, açıkça sınırlanarak tanımlanan meşru amaçlar için toplanan kişisel verilerin, yalnızca bu toplanma amaçları doğrultusunda, adil bir şekilde ve yasal sınırlamalar kapsamında işlenmelerinin, üye devletler tarafından yapılacak yasal düzenlemelerle garanti altına alınmasının gereğini ifade eder. Ancak 6. maddede bir parantez açılarak, üye devletlerin uygun güvenlik tedbirlerini almaları koşulu ile, kişisel verilerin tarihsel, istatistiksel ve bilimsel amaçlarla daha uzun süre işlenebilmeleri için arşivlenmelerinin, verilerin amacın gerektirdiğinden daha uzun süre tutulamaması ilkesine aykırılık teşkil etmeyeceğinin de altı çizilmiştir. Yine 6.maddede yer alan "*Doğruluk ve Güncellik*" ilkesi ile de kişisel verilerin, toplanma amaçlarının gerçekleştirilebilmesi bakımından uygun, yeterli, doğru ve güncel nitelikte olmalarının gerektiği, ayrıca toplanma amacının gerçekleştirilmesine ilişkin kriterlere uymayan aşırı, hatalı ve eksik verilerin ise silinmesi veya düzeltilmesi için gerekli adımların atılmasının önemi vurgulanmıştır. "*İlgililik ve Orantılılık*" ilkesi doğrultusunda da kişisel verilerin sınırları belli toplanma amaçlarıyla ilgili ve orantılı bir şekilde işlenmeleri gerektiği hususunun altı çizilmiştir. Veri süjelerinin kimliklerinin tespitine imkan verebileceğinden, "*Süreyle Sınırlılık*" ilkesi doğrultusunda, verilerin toplanma amaçlarına uygun olandan daha uzun sürelerde

saklanmalarına -tarihsel, istatistiksel veya bilimsel amaçlarla gerçekleşebilecek istisnalar hariç olmak üzere- izin verilmemiştir.

"*Gizlilik*" ilkesine ilişkin olan 16. maddede ise, veri kontrolörünün veya *işleyicinin* kendisinin ya da yetkisi altında hareket eden ve kişisel verilere erişim hakkı bulunan diğer kişilerin, yasayla özel olarak yetkilendirilmedikleri sürece, veri kontrolörünün talimatları dışında işleme yapamayacakları hüküm altına alınmıştır.

Mülga 95/46 sayılı Direktifin 17.maddesiyle ise, kazaen ya da yasa dışı imha, kayıp, değiştirme, yetkisiz ifşa gibi her türlü yasa dışı işleme faaliyetlerine karşı, kişisel verilerin güvenliğinin sağlanması amacıyla veri kontrolörü ve işleyicisinin, işleme faaliyetinin ve verinin doğasına uygun, gerekli ve yeterli teknik ve kurumsal tedbirleri almasının temini sorumluluğu, üye devletlere yüklenmiştir. Kişisel verilerin işlenmesinin bir işleyici aracılığıyla gerçekleştirileceği durumlarda, işleyicinin, yalnızca veri kontrolörünün talimatları doğrultusunda hareket edebileceğini ve madde 17/1'de belirtilen hususlardan da sorumlu olacağını içeren bir sözleşme ile, veri kontrolörüne bağlanması gerektiği yine 17/3.maddede hüküm altına alınmıştır. Kontrolör ve işleyici arasındaki yasal ilişkiyi düzenleyen sözleşmelerin, delil teşkil edebilmeleri bakımından, yazılı yapılmaları gerektiği de madde 17/4'te belirtilmiştir. 17. madde kapsamı bir bütün olarak incelendiğinde, bu maddenin kişisel verilerin işlenmesinde "*Güvenlik*" ilkesine uyulmasının önemini vurguladığı anlaşılmaktadır.

Mülga 95/46 sayılı Direktif'in 7/a. maddesinde kişisel verilerin hukuka uygun işlenebilmeleri, öncelikle veri süjesinin açık onayına bağlanmıştır. İlgili 7.maddenin devamında ise kişisel verilerin işlenmesini meşru kılan diğer hukuka uygunluk sebepleri sayılmıştır. Buna göre, veri süjesinin taraf olduğu bir sözleşmenin ifası ya da veri süjesinin talebi üzerine, veri süjesinin taraf olacağı bir sözleşmenin akdi için (*madde 7 b*); veri kontrolörünün tabi olduğu yasal yükümlülüklerin yerine getirilebilmeleri için (*madde 7 c*); veri süjesinin hayati çıkarlarının korunması için (*madde 7 d*); kamu yararına yerine getirilecek bir görev veya veri kontrolörüne ya da verinin açıklandığı üçüncü kişiye verilen resmi yetkinin kullanılması kapsamında (*madde 7 e*); -veri süjesinin temel hak ve özgürlüklerinin korunmasının bu amaçlara üstün gelmemesi kaydı ile- veri kontrolörünün ya da verinin açıklandığı üçüncü kişi veya kişilerin, takip ettiği meşru amaçlar kapsamında (*madde 7 f*) , gerekli olduğu

takdirde kişisel verilerin işlenmesi meşruiyet kazanabilir. Ancak mülga 95/46 sayılı Direktifin 14/a maddesi ile de, üye devletlere, yapacakları yasal düzenlemelerle, veri süjesine, madde 7 (e) ve (f) fıkralarında belirtilen kapsamda kişisel verilerin işlenmelerine, meşru gerekçelerle itiraz edebilme hakkı verme yükümlülüğü de getirilmiştir. İtirazın, haklı gerekçelerle ve usulüne uygun olarak yapıldığının anlaşılması halinde de itiraz konusu ilgili veriler, işlenme kapsamından çıkarılmalıdırlar. Madde 14/b'de ise, kişisel verilerin doğrudan pazarlama amacıyla kullanılması veya kullanılmak üzere üçüncü şahıslara ifşa edilmesi durumunda veri süjesinin, derhal durumdan haberdar edilmesi ve kendisine hem ifşa, hem de kullanılmaya ilişkin olarak, herhangi bir ücrete tabi olmadan, itiraz edebilme hakkı tanınması gerektiği düzenlenmiştir.

Mülga 95/46 sayılı Direktifin 8/1.maddesinde, ırk, etnik köken, siyasi görüşler, dini ve felsefi inançlar, sendika üyeliği, sağlık ve cinsel hayata ilişkin verileri kapsayan, hassas kişisel verilerin işlenmelerinin üye devletler tarafından yasaklanmasının gereği hüküm altına alınmıştır. Aynı 8.maddenin diğer fıkralarında ise hassas kişisel verilerin hangi istisnai hallerde işlenebilecekleri düzenlenmiştir. Buna göre, veri süjesinin tereddütte yer vermeyen açık ve yasal rızasının bulunması halinde; iş hukukunun veri kontrolörünü yasal olarak yetkili kıldığı hallerde; veri süjesinin rızasını gösteremediği istisnai durumlarda kendisinin ya da üçüncü bir kişinin hayati çıkarlarının korunması amacıyla; bizzat veri süjesinin kendisi tarafından kamuya açıklanan veriler hakkında; yasal savunma kurulması, sağlık hizmetlerinin yerine getirilmesi, suçla mücadele, idari ve cezai yaptırımlar veya kamu güvenliği tedbirlerine ilişkin hallerle, kamu yararı gereği benzeri durumlarda istisnai olarak hassas kişisel veriler işlenebilmektedirler.

Mülga 95/46 sayılı Direktifin 9. maddesinde ise, kişisel verilerin korunması ile ifade özgürlüğü arasında hassas ve adil bir dengenin muhafazası amacıyla, salt gazetecilik, sanatsal veya edebi maksatlarla ifade özgürlüğü sınırları dahilinde ortaya konan işlem ve ifadelerin, üye devletler tarafından kişisel verilerin işlenmesi yasağından istisna tutulabileceği belirtilmiştir. Avrupa Adalet Divanı da verdiği pek çok karar kapsamında, somut olayın özelliklerine göre, kişisel verilerin ve mahremiyetin korunması ile ifade özgürlüğü arasındaki adil dengenin korunmasının gereğine vurgu yapmıştır. Bu tez çalışmasının "*2.1.3.4. Düşünce ve İfade Özgürlüğü*

Bağlamında Kişisel Veriler", başlıklı bölümünde detaylı olarak incelenen "*İspanya Google Davası*[262]" adil denge vurgusunun kuvvetli bir şekilde yapıldığı Divan kararlarına örnek olarak gösterilebilir[263].

Madde 10'da, kişisel verilerin doğrudan veri süjesinden toplanması durumunda, veri kontrolörüne veya temsilcisine, çeşitli hususlarda veri süjesinin bilgilendirilmesine ilişkin bazı yükümlülükler getirilmiştir. Buna göre, veri kontrolörü, kendi kimliğine, işlemenin amacına, verilerin iletileceği alıcılara, verilerin toplanması sırasında sorulan sorulara cevap verilmesinin zorunlu olup olmadığına, cevap verilmemesi halinde hangi olası sonuçlarla karşılaşılabileceğine, veri süjesinin ilgili verilere erişim ve düzeltme hakkına ilişkin bilgiler ile verilerin adil işlenmesinin sağlanması için gerekli olabilecek diğer her türlü bilgiyi, veri süjesine bildirmekle yükümlüdür.

Mülga 95/46 sayılı Direktifin 11.maddesinde ise, doğrudan veri süjesinden elde edilmeyen kişisel verilerin, kaydedilmesi veya üçüncü kişilere ifşası halinde, veri kontrolörüne veya temsilcisine, kontrolörün veya temsilcisinin kimliğine, alıcıların kimler olduğuna, işlemenin amacına, verilerin kategorilerine, verilere erişim ve düzeltme hakkına ilişkin olarak veri süjesini makul bir süre içerisinde bilgilendirme yükümlülüğü getirmiştir.

Mülga 95/46 sayılı Direktif'in 12.maddesi ile de veri kontrolörlerine, makul aralıklarla ve herhangi bir gecikmeye veya masraf yapılmasına sebebiyet vermeksizin, veri süjesini, kişisel verisinin işlenip işlenmediğine ve işlendi ise işlenme amaç ve kategorisine, verilerin açıklandığı alıcılara ilişkin bilgilendirme yapma; ve, veri süjesiyle otomatik olarak yapılan veri işlemeleri de dahil olmak üzere, devam eden işlemelere ilişkin olarak iletişim kurma; yükümlülüğü getirilmiştir.

Madde 13'te ise kişisel verilerin korunmasına ilişkin getirilen genel istisna ve sınırlama sebepleri sıralanmıştır. Buna göre, ulusal güvenlik; savunma; kamu güvenliği; suçun önlenmesi; yasalarla belirlenmiş bazı meslek grupları için etik ihlali halleri; cezai soruşturma ve kovuşturma; üye devletin veya Birlik'in önemli

[262] Judgment of the Court of Justice of the European Union (Grand Chamber), EUR-Lex, Reports of Cases, **ECJ Case C-131/12**, 13.05.2014 Google Spain SL, Google Inc. V. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez.

[263] Stefan Kulk, Frederick Zuiderveen Borgesius, ss.17-21; European Union Agency for Fundamental Rights, 2018, ss. 23-24.

ekonomik ve mali çıkarlarının korunması; veri süjesinin veya diğer kişilerin temel hak ve özgürlüklerinin korunması için zorunlu olan hallerde kişisel verilerin korunmasına istisnai olarak yasal sınırlamalar getirilebilir.

Kişisel verilerin salt otomatik işlenmesi sonucunda, veri süjesinin iş performansı, kredibilitesi, güvenilirliği gibi, ilgili bireyi belirgin olarak ve önemli ölçüde etkileyebilecek nitelikteki konularda çıkarımlarda bulunularak alınacak kararlara, tabi olmama hakkı, mülga 95/46 sayılı Direktifin 15/1. maddesi kapsamında tüm bireylere tanınmıştır. Aynı maddenin ikinci fıkrasında ise tabi olmama hakkının istisnaları sayılmıştır. Buna göre, veri süjesinin kendi talebi ile bir sözleşmenin akdi veya ifasının gerçekleşmesi sırasında; veri süjesinin meşru menfaatlerini korunması kapsamında gerekli olması veya veri süjesinin meşru menfaatlerinin korunması için yasal olarak düzenlenen güvenlik tedbirlerine dayanması durumlarında, veri süjesinin 15/1 kapsamındaki kararlara tabi olmama hakkı, ilgili üye devlet tarafından yapılacak yasal düzenlemeler kapsamında kaldırılabilir.

Mülga 95/46 sayılı Direktifin 28/1. maddesine göre, her üye devlet, işbu Direktif'ten kaynaklanan hükümlerin kendi ulusal sınırları içerisinde uygulanmasının izlenerek, kontrol edilmesinden sorumlu olacak, bağımsız hareket edebilme yeteneğine sahip, bir ya da daha fazla, "*denetim makamının (supervisory authority)*" kurulmasını sağlamakla yükümlüdür. 28/2.maddeye göre ise, üye devletler, ayrıca, kişisel verilerin işlenmesi sırasında temel hak ve özgürlüklerin korunabilmesi için gerekli idari tedbirlerin alınması veya yasal düzenlemelerin yapılmasına ilişkin olarak bu denetim makamlarına danışılmasını sağlamalıdırlar.

Mülga 95/46 sayılı Direktifin 28/3.maddesi kapsamında, oluşturulacak denetim makamlarının, denetim görevlerini yerine getirebilmeleri için hangi yetkilere sahip olmaları gerektiği sayılmıştır. Bu maddeye göre, denetim makamları, veri işleme faaliyetinin konusunu oluşturan kişisel verilere "*erişim yetkisi*" ile gerekli tüm bilgileri toplama yetkisi gibi "*araştırma yetkileri*"ne sahip olmalıdırlar. Denetim makamları, ayrıca, veri işleme faaliyetleri yapılmadan önce, işbu Direktif'in 20. maddesi ile uyumlu bir şekilde görüş beyan edilmesi ve kişisel verilerin engellenmesi, silinmesi, imha edilmesi ile işlemenin geçici ya da kalıcı bir şekilde yasaklanması, kontrolörün uyarılması, veyahut konunun ulusal parlamentolara ya da

siyasi kurumlara taşınabilmesine ilişkin görüşlerinin uygun şekillerde yayınlanmasını da içerebilen "*etkili müdahale yetkileri*ne" de haizdirler. Denetim makamları, kişisel verilerin korunmasına yönelik işbu mülga 95/46 sayılı Direktif doğrultusunda hazırlanacak ulusal yasaların ihlali halinde bu "*ihlalleri yargıya taşıma yetkileri*" ile de donatılmalıdırlar. Ancak işbu denetim makamlarının vermiş oldukları kararlar da yargı denetimine açık olacaktır.

Mülga 95/46 sayılı Direktifin 28/4. maddesi kapsamında ayrıca, kişisel verilerin işlenmesinde hak ve özgürlüklerin korunması talebiyle kişinin kendisinin veya o kişiyi temsilen bir dernek ya da kuruluşun da denetim makamlarına başvurma hakkı olduğu ve bu kapsamda yapılacak başvurunun sonucuna ilişkin olarak ilgili kişiye, bilgi verilmesi gerektiği de hüküm altına alınmıştır. Denetim makamları, verilerin işlenmesi sırasında, özellikle işbu Direktifin 13.maddesinde belirtilen genel istisna ve sınırlama sebepleri ile, diğer hususların hukuka uygunluğunun kontrolüne ilişkin bireysel başvuruları da kabul eder ve bu başvurular üzerine yapılan kontrollerle ilgili geri bildirimlerde bulunur.

Mülga 95/46 sayılı Direktifin 28/5.maddesine göre, denetim makamları, faaliyetlerine ilişkin düzenli olarak hazırlayacakları raporları sunmakla yükümlüdürler ve bu raporlar kamuya açıktırlar. Madde 28/6'ya göre, her bir üye devletin denetim makamları, diğer üye devletin denetim makamları tarafından görevini yapmaya davet edilebilirler. Üye devletlerin her birinin denetim makamları görevlerini, bilgi paylaşımı yapmak da dahil olmak üzere, birbirleriyle koordineli bir şekilde yerine getirirler. Madde 28/7'de de, üye devletlerin, kendi denetim makamlarında çalışanların, görevleri sona erdiğinde dahi, görevleri sırasında öğrendikleri gizli bilgilerin korunması bağlamında, mesleki gizlilik yükümlülüğü altında olmalarını temin etmekle yükümlü olduklarının altı çizilmiştir.

Mülga 95/46 sayılı Direktifin 18.maddesi kapsamında denetim makamına bildirimde bulunma yükümlülükleri düzenlenmiştir. Buna göre, üye devletler, bir ya da daha fazla amaç için tamamen veya kısmen otomatik olarak yapılacak kişisel verilerin işlenmesi faaliyet(ler)inden önce, veri kontrolörü ya da varsa temsilcisi tarafından, denetim makamına, bildirimde bulunulmasını sağlayacak önlemleri almakla yükümlüdürler. Üye devletler, işlenecek kişisel veriler göz önüne alındığında, yapılacak işlemin veri süjesinin hak ve özgürlüklerini olumsuz yönde

etkilemeyecek nitelikte olması gibi, madde 18/2 kapsamında sayılan durumlarda, veri kontrolörlerine getirilen bildirim yükümlülüğü koşullarını azaltabilir ya da onları bu yükümlülükten muaf tutabilirler. Madde 18/3'e göre, üye devletler, tüm amacı yasalar kapsamında genel olarak, kamunun ya da meşru amaçlarla bireylerin danışmasına açık olacak şekilde kamuya bilgi temini olan sicil kaydı tutulması faaliyetlerine, 18/1. fıkranın uygulanmamasını sağlayabilirler. Mülga 95/46 sayılı Direktif'in 18/4.maddesinde ise, yine aynı Direktifin 8/2 (d) fıkrasına göre siyasi, felsefi, dini ya da ticari birliğe ilişkin amaçlarla faaliyet gösteren bir vakıf, dernek veya diğer bir kar amacı gütmeyen kuruluş tarafından, sadece kendi mensuplarının ya da kendileriyle kuruluş amaçları doğrultusunda bağlantıda bulunan kişilerin hassas kişisel verilerinin, makul garantiler kapsamında işlenmeleri durumunda, bu verilerin veri süjesinin izni olmadan üçüncü kişilere açıklanmamaları şartıyla, üye devletler, yapacakları düzenlemelerle, bu kuruluşlara denetim makamlarına bildirim yapma yükümlülüklerinden muafiyet sağlayabilecekleri hüküm altına alınmıştır. Madde 18/5'te ise, üye devletlerin otomatik olmayan kişisel verileri işleme faaliyetlerinin tamamı veya bir kısmı için bildirim yükümlülüğünün basitleştirilmesini ya da kaldırılmasını düzenleyebilecekleri ifade edilmiştir.

Mülga 95/46 sayılı mülga Direktifin 19.maddesinde, 18. madde kapsamında yapılacak bildirimlerin içeriğinin neleri kapsaması gerektiği düzenlenmiştir. Buna göre bu bildirimler, kontrolörün ve varsa temsilcisinin ad ve adresine; işleme amacına; veri süjesine ve kişisel verilerin kategorilerine; bu verilerin açıklanacağı alıcıların kimlik bilgilerine; veri transferi yapılması planlanan üçüncü ülkelere ve işbu Direktif'in 17. maddesi uyarınca veri işleme güvenliğinin sağlanması için alınacak tedbirlere ilişkin genel bir açıklamayı içermelidir.

Üye devletlerin, veri süjelerinin hak ve özgürlüklerine zarar verebilecek nitelikte olan işleme faaliyetlerini belirleyerek, bu faaliyetlere başlanmasından önce, gerekli ön kontrolleri yapma yükümlülükleri mülga 95/46 sayılı Direktifin 20.maddesi kapsamında düzenlenmiştir. Ön kontroller, denetim makamları tarafından, kendilerine veri kontrolörü veya veri koruma yetkilisi tarafından bildirim yapılmasını takiben derhal gerçekleştirilmelidir. Takip eden 21.maddede ise, üye devletlerin, kişisel verilerin işlenmesi faaliyetlerinin kamuya duyurulması kapsamında gerekli tedbirleri alma yükümlülükleri düzenlenmiştir. İdari çözüm

yoluna gidilebilmesi hakkına halel gelmemek kaydıyla, kişisel verilerinin işlenmesi yoluyla hakları ihlal edilen bireylerin yargı yoluna başvurma hakkının üye devletler tarafından garanti altına alınması gereği ise mülga 95/46 sayılı Direktifin 22.maddesinde belirtilmiştir.

Yasadışı bir işleme faaliyetinden ya da işbu Direktif'e uygun olarak hazırlanarak kabul edilen ulusal yasalara aykırı bir işlemden kaynaklanan zararın karşılanması için zarara uğrayan bireyin, veri kontrolöründen tazminat isteme hakkının, üye devletler tarafından garanti altına alınması hususu, mülga 95/46 sayılı Direktifin 23.maddesi kapsamında düzenlenmiştir. Bu maddeye göre, kontrolör, ancak, ilgili zarara sebep olan olayın doğmasından sorumlu olmadığını ispat ettiği takdirde, sorumluluktan kısmen veya tamamen kurtulabilir. Üye devletlerin, mülga 95/46 sayılı Direktif'in ve işbu Direktif'e uygun olarak kabul edilen hükümlerin uygulanmasının sağlanması için gerekli tedbirleri alma ve bazı somut yaptırımları ortaya koyma yükümlülükleri ise madde 24 kapsamında düzenlenmiştir.

Mülga 95/46 sayılı Direktif'in 4. Bölüm, 25. maddesi kapsamında, üçüncü ülkelere kişisel veri transferine ilişkin ilkeler düzenlenmiştir. Buna göre, işbu Direktif doğrultusunda kabul edilen ulusal yasa hükümlerine halel gelmeksizin, üye devletler, kişisel verileri, ancak ve ancak, bu veriler için uygun ve yeterli bir koruma düzeyini garanti eden üçüncü ülkelere aktarabilirler. Aktarım yapılacak üçüncü ülkenin sağladığı koruma düzeyinin uygunluk ve yeterliliği, kişisel verilerin aktarımına ilişkin somut olayın tüm koşulları birlikte göz önüne alınarak değerlendirilmelidir. Bu hususta değerlendirme, özellikle, işlemenin süresi ve amacı; kişisel verinin türü; menşei ve nihai varış ülkesi; ilgili üçüncü ülke sınırları içinde yürürlükte olan genel ve sektörel bazdaki hukuk kuralları, mesleki kurallar ve güvenlik önlemleri dikkate alınarak yapılmalıdır. Üye devletler ve Komisyon, veri transferi yapılması planlanan üçüncü ülkenin uygun ve yeterli koruma düzeyini sağlayamadığını düşündükleri hallerde, birbirlerini bu durumdan haberdar etmekle yükümlüdürler. Komisyon, üçüncü bir ülkenin, kişisel verilerin korunması bağlamında yeterli koruma düzeyini sağlayamadığını tespit ettiği taktirde, üye devletlerin, Komisyonun konuya ilişkin kararı doğrultusunda tedbirler alarak bu üçüncü ülkeye kişisel veri transferi yapılmasını engellemeleri gerekir.

Mülga 95/46 sayılı Direktifin 26.maddesi kapsamında, madde 25'te sayılan koşulları sağlayamayan üçüncü ülkelere kişisel veri transferinin yapılabileceği istisnai haller sayılmıştır. Madde 26/1 (a) (b) ve (c)'ye göre, uygun ve yeterli tedbirleri almayan bir üçüncü ülkeye, kişisel verilerin aktarımı, veri süjesinin herhangi bir şüpheye yer bırakmayan açık rızası varsa; veri süjesi ile kontrolör arasındaki sözleşmenin ifası veya veri süjesinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için gerekliyse; veri süjesinin çıkarlarını korumak üzere, kontrolör ve üçüncü kişi arasında akdedilen veya ifa edilecek olan bir sözleşme için gerekli olduğu takdirde, istisnai olarak yapılabilir. Madde 26/1 (d) ve (e)'de ise, önemli bir kamu menfaatinin gerçekleşmesi ya da kanuni hakların tesisi, icrası veya savunulması için gerekli ya da yasal olarak zorunlu ise ve veri süjesinin hayati menfaatlerinin korunması için gerekli ise üçüncü ülke madde 25'te sayılan koşulları sağlayamasa da yine istisnai olarak kişisel veri aktarımının yapılabileceği düzenlenmiştir.

Mülga 95/46 sayılı Direktif'in 26/1 (f) maddesi kapsamındaki, üye devletlerin yedlerinde bulunan ve kamuya ya da meşru menfaati olan üçüncü kişilere bilgi sağlanması amacıyla açık olan kayıtlar içerisinden, üçüncü ülkelere yapılan kişisel veri transferleri de üçüncü ülkeye aktarıma ilişkin yasağın istisnaları arasında sayılır. İstisnai hallerde üye devletler, mülga 95/46 sayılı Direktif'in 25/2. maddesi kapsamında uygun ve yeterli sayılan genel koruma düzeyini garanti edemeyen üçüncü ülkelere de, bireylerin mahremiyetleri ile temel hak ve özgürlüklerinin korunması hususunda özel güvenceler vermeleri koşuluyla, kişisel veri transferi yapılmasına izin verebilirler. Bu durumda izni veren üye devlet, madde 26/3 kapsamında, Komisyon ve diğer üye devletleri bu durumdan haberdar etmelidir. Madde 26/4'e göre ise, Komisyon üye devletin bu kararına haklı sebeplerle karşı çıkarak, somut olaya ilişkin bir karar verdiği takdirde, üye devlet bu karar doğrultusunda uygun tedbirleri almakla yükümlüdür.

Kişisel verilerin işlenmesine ilişkin olarak bireylerin korunması konusunda faaliyet göstermek üzere, mülga 95/46 sayılı Direktifin 29. maddesi uyarınca, bağımsız bir danışma kurulu olarak her üye devletin temsilcileri ile Birlik kurum ve kuruluşlarının temsilcilerinden oluşan "*Madde 29 Çalışma Grubu*" oluşturulmuştur. Madde 29 Çalışma Grubu'nun görevleri ise, 30.maddede sıralanmıştır. 30.maddeye

göre, Madde 29 Çalışma Grubu, mülga 95/46 sayılı Direktif kapsamında alınan tedbirlerin, üye devletlerde birbirleriyle uyumlu bir şekilde uygulanmalarını denetlediği gibi; üçüncü ülkelerdeki koruma seviyelerinin uygunluğu konusunda görüş bildirmeye de yetkilidir. Madde 29 Çalışma Grubu, ayrıca, mülga 95/46 sayılı Direktif'in tadiline, kişisel verilerin işlenmesi hususunda gerçek kişilerin hak ve özgürlüklerinin korunmasına yönelik ek tedbirlerin alınmasına ve Birlik düzeyinde davranış kurallarına ilişkin olarak Komisyon'a görüş bildirmeye de yetkilidir. Ulusal yasa farklılıklarının, Birlik genelinde gerçek kişilere eşit korumanın sağlanması hususunu olumsuz etkilediğinin tespiti halinde, Madde 29 Çalışma Grubu, Komisyon'a bu konuda bilgi vermekle de yükümlüdür. Kişisel verilerin işlenmesi hususunda bireylerin hak ve özgürlüklerinin korunmasına ilişkin görüş ve tavsiyelerini Komisyon'a ileten Madde 29 Çalışma Grubu, bu konuda hazırlanacak raporu Konsey ve Avrupa Parlamentosu'na da sunmakla yükümlüdür.

Mülga 95/46 sayılı Direktif madde 32 ile, üye devletlere, kabulünden itibaren en geç üç yıl içerisinde, işbu Direktif'le belirlenen asgari koşul ve ilkelere uygun ulusal yasa, yönetmelik ve idari hükümlerin oluşturularak tamamlanması yükümlülüğü getirilmiştir.

2.3.2.1.1. Avrupa Dijital Tek Pazarı Çerçevesinde Mülga 95/46 Sayılı Direktif'e İlişkin Kısa Bir Değerlendirme

Birlik hukuku kapsamında öncül bir düzenleme niteliğinde sayılabilen mülga 95/46 sayılı bu Direktif, kişisel verilerin korunması hususunda, çerçeve hükümler getirerek Birlik içinde ve üye devletler arasında, ilk etapta asgari bir koruma seviyesi ve farkındalık oluşturmayı hedeflemişti. Ancak işbu Direktif kapsamında yapılan tüm uyumlaştırma çabalarına rağmen, özellikle kişisel verilerin korunması konusunda üye devletler arasında mevcut bulunan anlayış ve gelişmişlik farklılıkları sebebiyle, ortaya çıkan ulusal yasa ve uygulama farklılıklarının bir türlü tam olarak sona erdirilememesi sebebiyle, bu konudaki aksaklıkların devam ettikleri görülmüştür.

Üye devletlerin kimi zaman bir diğer üye devletin kişisel verilerin korunması hususundaki ulusal yasa ve uygulamalarını yetersiz bularak, kendi vatandaşlarının

kişisel verilerini o üye devlete aktarmaktan kaçınması hali dahi, tek başına, tek pazarda bu bağlamda yaşanan aksaklıklara önemli bir örnek teşkil eder. Ayrıca kimi üye ülkelerde kişisel verilerin daha güçlü ulusal yasa ve uygulamalar kapsamında korunması, Birlik içerisinde dahi, e-ticaret kapsamında işlem yapacak tüketicileri bu üye ülkelerde yer alan şirketlere yöneltmesi de, hem yine tamamlanmaya çalışılan Avrupa dijital tek pazarının parçalı yapısını perçinlemekte, hem de Birlik'i bölgesel gelişmişlik farklılıklarının ortadan kaldırılmasına yönelik olarak uzun yıllardır vermekte olduğu mücadelede geri bırakmaktaydı. Bu ve benzeri aksaklıklar ise, dijital tek pazarın parçalı görünümünden kurtarılması çalışmalarını baltalar nitelikteydi.

Yaşanan dijital devrim kapsamında ortaya çıkan dönüşüm, tüm bu aksaklıklarla birleşince, mülga 95/46 sayılı Direktif ile getirilen sade sistem, özellikle tamamlanmaya çalışılan Avrupa dijital tek pazarında, kişisel verilerin korunması hususunda ortaya çıkan yeni tehdit ve ihtiyaçlarla başa çıkma konusunda yetersiz kalmış ve doğal olarak da daha etkili koruma ve yaptırım mekanizmaları ihtiyacı doğmuştu. Bu sebeplerle, Birlik kişisel verilerin korunması konusundaki gayretlerini bir üst seviyeye taşıyarak, dijital ekonomiye daha iyi uyum sağlayabilmek, gelişen teknolojinin ortaya koyduğu yeni tehditlerle başa çıkabilmek ve temel hak ve özgürlükleri daha etkili koruyabilmek amacıyla, Birlik düzeyinde, doğrudan uygulanabilir yasa hükümleri çerçevesinde yapılacak kişisel verilerin korunması reformuna ilişkin çalışma başlatmıştır.

"*Avrupa Birliği Veri Koruma Reform*" çalışmaları sonucunda, mülga 95/46 sayılı Direktif yürürlükten kaldırılarak, yerini 25.05.2018 tarihi itibarı ile, "*Genel Veri Koruma Tüzüğü*[264]"ne bırakmıştır. Böylelikle, Birlik düzeyinde doğrudan uygulanabilir hükümlerden oluşan işbu Tüzük kapsamında tamamen uyumlaştırılan düzenlemelerle, kişisel verilerin daha sıkı bir şekilde kontrol altında tutmaları sağlanarak, ihlallerin önüne geçilmesi, ticari işletmelerin ve tüketicilerin daha güvenilir, uyumlu ve bütünleşik bir tek pazarda faaliyette bulunabilmeleri, nihayetinde de Avrupa dijital tek pazarında güvenirliğin ve buna bağlı olarak da

[264] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Official Journal of the European Union, L 119/1**, 4.5.2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj (02.06.2020).

ticaret hacminin artırılarak, ekonomik büyümeye ivme kazandırılması amaçlanmaktadır. Sonuç olarak Genel Veri Koruma Tüzüğü'nün, mülga 95/46 sayılı Direktifin yerini alması ile, Avrupa Temel Haklar Şartı kapsamında Birlik hukukunda bir temel hak olarak tanınarak, koruma altına alınan kişisel verilerin, Direktif gibi üye devletler arasında farklı uygulamalara neden olabilecek bir hukuki enstrüman yerine, Birlik düzeyinde yeknesak bir şekilde uygulanacak bir Tüzük kapsamında korunmasının sağlanmasının, konunun önemi göz önüne alındığında en doğru yol olduğu söylenebilir[265].

2.3.2.2. 2002/58 Sayılı E-Mahremiyet Direktifi

Avrupa Birliği Veri Koruma Reformu kapsamında kabul edilen, Genel Veri Koruma Tüzüğü kapsam ve içeriğine geçmeden önce, elektronik iletişim konusunda hem kişisel verilerin, hem de mahremiyetin korunması hususlarında Avrupa dijital tek pazarının gelişimine önemli katkılarda bulunan ve halen yürürlükte olan "*2002/58 sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunmasına İlişkin Direktifi (E-Mahremiyet Direktifi)* [266] "ni incelemekte fayda vardır.

Akıllı cihazlar, bilgisayarlar ve cep telefonları, e-posta hizmetleri, sosyal medya ve diğer dijital platformlar aracılığıyla çevirim içi ağ üzerinden yapılabilen ses ve görüntü aktarımı, yazışma, mesajlaşma, konum uygulamaları ve benzeri diğer iletişim şekil ve teknikleri vasıtası ile, elektronik iletişimin günden güne yaygınlaşmasıyla birlikte, bu kapsamda işlenen ve transfer edilen kişisel veri, hacim ve çeşitliliği de artmıştır. Birlik, elektronik iletişim sektörüne özel bu durumu göz önüne alıp, temel hak ve özgürlüklerin korunması temel prensibinden yola çıkarak, 95/46 sayılı Kişisel Verilerin Korunması Direktifini tamamlayıcı nitelikte olan

[265] European Commission, "Communication from the Commission to the European Parliament and the Council, Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018", 24.01.2018, **COM (2018) 43 Final**, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0043&from=EN (02.06.2020), ss.1-3.

[266] 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), **Official Journal L 201**, 31.07.2002, https://eur lex.europa.eu/legal content/EN/TXT/?qid=1552477714766&uri=CELEX: 32002L0058 (02.06.2020).

"*2002/58 sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunmasına İlişkin Direktifi (E-Mahremiyet Direktifi)"ni* kabul etmiştir.

95/46 sayılı Direktif ile getirilen yasal düzenleme, sınırlama ve ilkeler çerçevesinde hazırlanan 2002/58 sayılı E-Mahremiyet Direktifi ile, elektronik iletişim kapsamındaki mahremiyetin, kişisel verilerin ve dolayısı ile de özel hayatın korunmasına özel düzenlemeler ortaya konmuştur. 2009 yılında gözden geçirilerek tadil edilen 2002/58 sayılı bu Direktifin de Veri Koruma Reformu kapsamında, doğrudan uygulanabilir kurallar çerçevesinde değiştirilmesi adına, 2017 yılında tüzük şeklinde düzenlenmiş bir "*Yasa Teklifi*[267]" hazırlanmıştır. Ancak bu Yasa Teklifi, henüz yasalaşmadığından, elektronik haberleşme alanında 2002/58 sayılı E-Mahremiyet Direktifi halen geçerliliğini korumaktadır.

95/46 sayılı Direktifi tamamlayıcı nitelikte olduğu, 2002/58 sayılı E-Mahremiyet Direktifi'nin 1. maddesinin 2. fıkrasında açıkça belirtilmiştir. Bu bağlamda, 2002/58 sayılı E-Mahremiyet Direktifi, halkın erişimine açık elektronik iletişim hizmetleri alanında işlenen kişisel verilerin, temel hak ve özgürlükler bağlamında, üye devletler tarafından kabul edilebilir ve eşit seviyelerde korunarak, bu verilerin mahremiyetlerinin ve serbest dolaşımlarının garanti edilmesi amacıyla, kabul edilen yasal düzenleme ve sınırlamaları içerir. 2002/58 sayılı Direktifin 1.maddesi ile giriş 12.paragrafında, işbu E-Mahremiyet Direktifinin, elektronik iletişim kapsamında gerçek kişi abonelerin yanı sıra -95/46 sayılı Direktifin aksine- tüzel kişilerden oluşan abonelerin de meşru çıkarlarının korunmasında kullanılacağının altı çizilmiştir. Diğer taraftan, 2002/58 sayılı E-Mahremiyet Direktifinin içeriği incelendiğinde, tanımlamalar da dahil pek çok konuda, 95/46 sayılı Direktife doğrudan ya da dolaylı atıflar yapılarak, buradaki tanım, ilke ve kuralların, elektronik iletişim sektörüne de uygulanabilir hale getirildiği görülmektedir[268].

[267] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017, **COM (2017) 10 Final**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 (02.06.2020).
[268] Gloria Gonzales Fuster, **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, Law, Governance and Technology Series 16, Springer, Heidelberg, 2014, ss.216-217;

2002/58 sayılı E-Mahremiyet Direktifi ile, temel hak ve özgürlüklere saygı ilkesi doğrultusunda, elektronik iletişim sektöründe işlenen kişisel verilerin ve dolayısıyla da mahremiyetin korunması ve bu verilerin serbest dolaşımlarının sağlanması adına, üye devletlere yasal düzenlemeler yapma sorumluluğu yüklenmiştir. Aşağıda sayılan hususlar, E-Mahremiyet Direktifi kapsamında, üye devletlerin yapmaları gereken düzenlemelere örnek olarak verilebilir[269]: E-iletişim hizmetlerinin güvenliğinin etkili teknik, yasal ve kurumsal alt yapı düzenlemeleri yapılarak sağlanması; Güvenlik ihlali risklerinin olması halinde kullanıcıların risklerin içeriği ve bunlara ilişkin alınacak tedbirler konusunda bilgilendirilmeleri (*2002/58 sayılı Direktif madde 4*); İstisnai haller dışında, verilerin işlenmeleri konusunda elektronik iletişimin gizliliğini temin edecek her türlü tedbirin alınması (*2002/58 sayılı Direktif madde 5*); İletişim hizmetleri verilirken abone veya kullanıcıların bıraktıkları izlerden yola çıkarak ağda depolanan verilerin işlenmesi prensibine dayanan, "*çerez (cookies)" ve "casus yazılımlar (spyware)*" olarak adlandırılan yazılımlar kullanılarak, kişisel verilere yapılabilecek her türlü müdahalenin, ancak ve ancak abone veya kullanıcı, 95/46 sayılı Direktif doğrultusunda, açık ve anlaşılır bir şekilde bu müdahalenin içeriğine ilişkin bilgilendirildiği taktirde yapılabilmesinin sağlanması (*2002/58 sayılı Direktif madde 5/3*); Doğrudan insan müdahalesi olmadan gerçekleşen otomatik aramalar, faks, e-posta v.b. ile yapılan doğrudan pazarlama yöntemleri, işbu Direktif kapsamında "*istenmeyen iletişim (unsolicited communications)*" olarak nitelendirilerek, bu tip iletişimin önceden veri süjesinin izni alınmadan yapılmamasının sağlanması *(2002/58 sayılı Direktif madde 13)*; Abone veya kullanıcılara ait konum bilgilerinin ancak veri süjelerinin rıza göstermesi ya da bu verilerin anonim hale getirilmesi durumunda işlenebilmelerinin sağlanması *(2002/58 sayılı Direktif madde 9)*.

Özetlemek gerekirse, 2002/58 sayılı E-Mahremiyet Direktifi, elektronik iletişim kapsamında kişisel verilerin işlenmesine ilişkin çeşitli sınırlama ve çerçeve ilke ve kurallar getirerek, veri mahremiyetinin korunması; veri trafiğinin işleyişinin düzenlenmesi; verilere spam, istenmeyen iletişim, casus yazılımlar ve çerezler v.b.

Mario Viola de Azevedo Cunha, **Market Integration Through Data Protection, An Analysis of the Insurance and Financial Industries in the EU**, Law, Governance and Technology Series 9, Springer, Heidelberg, 2013, s.190.

[269] Elif Küzeci, ss. 193-195.

uygulamalar vasıtasıyla müdahale edilmesi hususlarında düzenlemeler yapılmasına imkan vermiştir. 2002/58 sayılı bu Direktif ile, elektronik iletişim sektöründe, kişisel verilerin korunması ile verilerin serbest dolaşımlarının önemi vurgulanarak, abone ve kullanıcıların mahremiyet hakları bağlamında farkındalıklarının artırılması, hakların içeriğinin ve uygulama koşullarının daha iyi anlaşılması, böylelikle de tüketici haklarının daha belirgin hale getirilerek, yasal düzenlemelerin özele indirgenerek, sektörel bazda da yaygınlaşıp uygulanmalarının sağlaması hedeflenmiştir.

Hem 2015 yılında açıklanan Avrupa Dijital Tek Pazar Stratejisi kapsamında, hem de 2016/679 sayılı Genel Veri Koruma Tüzüğü 173.paragrafı dahilinde, kişisel verilerin korunmasına ilişkin genel düzenlemelerin yapılmasını takiben, 2002/58 sayılı E-Mahremiyet Direktifinin de güncellenmesi gerektiğinin altı önemle çizilmiştir[270]. Zira Birlik'in içinde bulunduğumuz küresel dijital çağda her geçen gün pazar payını biraz daha artıran dijital ekonomiden beklediği verimi alabilmesi için, kişisel verilerin her alanda olduğu gibi elektronik iletişim sektöründe de Birlik düzeyinde uyumlaştırılmış, güncel nitelikli yasalar dahilinde korunması önemlidir. Böylelikle, Avrupa dijital tek pazarının, parçalı görünümünden kurtarılarak, birbiriyle uyumlu güçlü yasalar dahilinde regüle edilen, yekpare bir tek pazar haline getirilmesi hedefi doğrultusunda atılması gereken adımlardan biri daha gerçekleştirilmiş olacaktır.

2016/679 sayılı Genel Veri Koruma Tüzüğü'nün 95.maddesi kapsamında da işbu Tüzük'ün, 2002/58 sayılı E-Mahremiyet Direktifi ile birlikte ne şekilde uygulanabileceği hususuna açıklama getirilmeye çalışılmıştır. Buna göre, 2002/58 sayılı Direktif ile özel olarak düzenlenen konular kapsamında, bu maddelere halihazırda tabi olan gerçek ve tüzel kişilere, 2016/679 sayılı Tüzük ile aynı kapsamda ek yükümlülükler getirilemeyeceğinin altı çizilmiştir. Bu hüküm bile tek başına, 2002/58 sayılı Direktifin bir an önce güncellenmesinin gereğini hatırlatır niteliktedir.

[270] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, s. 13.

ÜÇÜNCÜ BÖLÜM
AVRUPA DİJİTAL TEK PAZARININ GELİŞİMİNDE GENEL VERİ KORUMA TÜZÜĞÜNÜN ROLÜ

İşbu tez çalışmasının üçüncü ve son bölümünde, öncelikle Avrupa Birliği Veri Koruma Reformu'nun teorik kökenleri ile işbu reformun yapılmasını gerekli kılan temel sebepler ve reform çalışmalarında Komisyon'un rolü üzerinde durulacaktır. Akabinde 2016/679 sayılı Genel Veri Koruma Tüzüğü ve bu Tüzük kapsamında getirilen önemli değişiklikler irdelenerek, bu değişikliklerin Avrupa Dijital Tek Pazarının gelişimine katkılarının neler olabileceği aktarılmaya çalışılacaktır.

3.1. VERİ KORUMA REFORMUNUN TEORİK KÖKENLERİ

Avrupa Birliği, küresel dijital devrim tarafından tetiklenerek, her geçen gün genel ekonomideki payını artıran dijital ekonomiden mümkün olan en büyük payı almak istemektedir. Birlik bu amaçla hazırladığı Avrupa Dijital Tek Pazar Stratejisi kapsamındaki hedeflerine ulaşabilmek için öncelikle hem yasal mevzuat, hem de idari uygulamalar kapsamında parçalı pazar görünümünden kurtulmalıdır. Bu bağlamda da, dijital ekonomi içerisinde artık ticari bir değer olduğu tartışma götürmeyen verilerin korunmalarının ve serbest dolaşımlarının, Birlik düzeyinde uyumlu yasal düzenlemeler oluşturularak sağlanması, Birlik için olduğu kadar, ayrı ayrı üye devletler için de elzemdir. Bu yolla dijital tek pazara duyulan güvenin artırılmasıyla, dijital ekonomiden alınacak payın yükseltilerek, ekonomik ve sosyal büyümeye ivme kazandırılması, Birlik'in en önemli stratejik hedeflerindendir. Bu hedeflerin gerçekleştirilebilmesi için de, Avrupa Birliği Temel Haklar Şartı kapsamında temel haklardan biri olarak tanınarak, Lizbon Antlaşması'nın kabulü ile de Kurucu Antlaşmalar düzeyinde yasal koruma kazanan, kişisel verilerin, Birlik düzeyinde uyumlu yasalarla korunması bağlamında Veri Koruma Reformu ihtiyacı ortaya çıkmıştır.

Reform ihtiyacını ortaya koyan itici güçlere bakıldığında, bunların Avrupa bütünleşmesi kapsamında pek çok teori ile dirsek temasında olduğu

görülebilmektedir. Bu teoriler içinde en çok göze çarpanlardan biri de pek çok araştırmacı tarafından Avrupa Birliği bütünleşmesini en iyi şekilde açıklayan teorilerden biri olarak kabul edilen "*Kurumsalcılık (Institutionalism) Teorisi*"dir.

Siyasette kurumların ve normların dönüştürücü etkilerinin önemine işaret eden Kurumsalcılık Teorisi, özellikle de bu teorinin alt kategorilerinden biri olan "*Rasyonel Tercihli Kurumsalcılık*", Veri Koruma Reformunun itici güçlerinin açıklanmasında önemli bir yere sahiptir. Rasyonel tercihli kurumsalcılığa göre, devletler kendi çıkarlarını en üst düzeyde gerçekleştirerek, işlerini kolaylaştırmak adına yaptıkları rasyonel seçimlerle kuracakları kurumlara yetki devri yapıp, supranasyonel nitelikteki normlar oluşturarak, karşılıklı ilişkilerinde bu normlar dahilinde ve kurumlar aracılığıyla hareket ederler. Kurumlar da kendilerine devredilen bu yetkiler çerçevesinde gündem belirleyici bir role bürünebilmektedirler. Çıkarlarını maksimize ederek dijital ekonomiden büyük pay alma konusunda rasyonel seçimlerini yapan üye devletler, bu konuda Birlik düzeyinde ve doğrudan uygulanabilir nitelikte yasal düzenlemeler yapma ve bu düzenlemeler çerçevesinde yargı yetkisini kullanma konularında, Birlik kurumlarına, özellikle de Komisyon'a ve Avrupa Birliği Adalet Divanı'na yetki devri yapmışlardır. Devredilen yetkiler dahilinde bu kurumlar tarafından oluşturulan gündem ve belirlenen öncelikler kapsamında hazırlanan Genel Veri Koruma Tüzüğü ve uygulamada veri koruma hususunda verilen Adalet Divanı kararları ise, dijital pazarı ve bu pazardaki aktörleri regüle ettiği gibi, tıpkı Rasyonel Tercihli Kurumsalcılıkta savunulduğu gibi, üye devletlerin davranışlarını da sınırlandırarak şekillendirmektedir[271].

Mülga 95/46 sayılı Direktif, kişisel verilerin korunması hususunda temel çerçeveyi oluşturup, yasal sınırları çizerek bu konuda ulusal düzenlemelerin yapılmasını ise federalist kökenlere sahip Subsidiarity İlkesi gereği, üye devletlere bırakmıştı [272] . Bu Direktif, Veri Koruma Reformu kapsamında yürürlükten kaldırılarak, yerini doğrudan uygulanabilir nitelikteki Genel Veri Koruma Tüzüğü'ne bırakmıştır. Böylece, kişisel verilerin korunması hususu, üye devletlerin egemenlik hakları dahilinde yapacağı ulusal yasal düzenlemeler kapsamından çıkarılarak, Birlik düzeyinde doğrudan uygulanabilir hükümlerle regüle edilmeye başlanmıştır. Bu değişiklik, üye devletlerin rasyonel tercihleri sonucu kurulan Birlik kurum ve

[271] Mark A.Pollack, ss.126-128, 134; Sinem Akgül Açıkmeşe, ss. 20-22.
[272] Sinem Akgül Açıkmeşe, s. 30.

normlarının güç kazanıp, üye devletlerin tutum ve davranışları üzerinde etkili olarak, onları her geçen gün biraz daha sınırlandırdığının göstergesi niteliğindedir.

Veri Koruma Reformu ihtiyacının ortaya çıkmasında etkili bir diğer itici güç de "*Sosyal İnşaa (Social Constructivism) Yaklaşımı*"dır. Bu yaklaşım, devletlerin ortaya koyduğu norm ve kurumların, kendilerini oluşturan devletlerle girmiş oldukları karşılıklı sosyal etkileşimlerin, birey ve devletlerin tercihleri, çıkarları, kültür ve kimlikleri üzerinde dönüştürücü etkiler yaptıkları temeline dayanır. Diğer bir ifade ile, Sosyal İnşaa'ya göre, içinde bulunduğumuz sosyal çevre ve bu çevreyi oluşturan sosyal unsurlar, bizim kim olduğumuzu belirlemektedirler[273] .

Kuruluşundan itibaren Avrupalılık kültürünün ve dolayısı ile de Birlik'in etik temellerini oluşturduğu kabul edilen ve nihayetinde Avrupa Birliği Temel Haklar Şartı kapsamında derlenerek tanınan, temel hak ve özgürlükler de, Avrupalılık kimlik ve kültürünün olmazsa olmaz unsurlarından biridir. Bu sebeple, Avrupa'yı Avrupa yapan Avrupalılık kimliğinin ve kültürel değerlerinin en önemli parçalarından birini oluşturan temel hak ve özgürlüklerin korunması bağlamında kişisel verilerin, Birlik düzeyinde doğrudan uygulanabilir yasalar kapsamında, yeknesak uygulamalarla korunması ihtiyacı, kapsamlı bir Veri Koruma Reformu yapılması adına, üye devletler üzerinde yoğun bir baskı oluşturmuştur. Bu perspektiften bakıldığından, reform çalışmaları neticesinde hazırlanan Genel Veri Koruma Tüzüğü'nün Avrupalılık kimliğinin tamamlayıcı unsurlarından biri olduğunu söylemek de yanlış olmayacaktır.

Kişisel veriler, Birlik hukukunda, Birlik'in kuruluşundan bu yana benimsenerek, korunmaya çalışılan en önemli etik değerlerden biri olan temel hak ve özgürlükler kapsamında ele alınmaktadırlar. Dolayısıyla zaman içinde gelişen bilgi ve iletişim teknolojileri ile artan internet kullanımının olumsuz etkileri de dikkate alındığında, temel haklar kapsamında kabul edilen kişisel verilerin, üye devletler bazında farklı uygulamalara yol açabilen 95/46 sayılı Direktif ile korunmasının yetersiz kaldığı daha iyi anlaşılmıştır. Bu farkındalık, Avrupa Birliği'ni, kişisel verileri, doğrudan uygulanabilir yasal düzenlemeler kapsamında tüm Birlik düzeyinde aynı şekil ve yeterlilik düzeyinde koruyabilmek adına yasal düzenlemeler yapmaya yöneltmiştir. Bu çabalar sonucu ortaya konan, veri koruma reformu

[273] Thomas Risse, ss. 145-149; Sinem Akgül Açıkmeşe, ss. 24-25.

kapsamında hazırlanarak kabul edilen doğrudan uygulanabilir nitelikteki Genel Veri Koruma Tüzüğü, kişisel verilere Birlik genelinde aynı şekil ve düzeyde sağladığı koruma ile Birlik'in hukuk yoluyla bütünleşme çabalarının önemli bir çıktısı sayılabilir. Dolayısı ile, işbu Tüzük çerçevesinde verilecek Adalet Divanı kararlarının da, Avrupa dijital tek pazarının gelişimine ve yekpareliğine önemli katkılarda bulunarak, Birlik'i hem hukuk yoluyla bütünleşmeye, hem de bu yolla oluşturulacak tek parça dijital tek pazar vasıtasıyla da ekonomik bütünleşmeye bir adım daha yaklaştıracağı söylenebilir[274].

3.2. VERİ KORUMA REFORMUNU GEREKLİ KILAN TEMEL SEBEPLER

95/46 sayılı Kişisel Verileri Koruma Direktifi, Avrupalılık kültür ve kimliğinin en önemli unsurlarından biri olarak görülen temel hak ve özgürlüklerin güvence altına alınması kapsamında, kişisel verilerin korunması temelinde oluşturulmuştur. Bu Direktif ile, kişisel veri güvenliğinin sağlandığı bir ortamda, kişilerin, malların, hizmetlerin, sermayenin olduğu kadar verilerin de serbest dolaşımlarının sağlanarak, uyumlu yasalarla regüle edilen bir Avrupa tek pazarının oluşturulması hedefine doğru bir adım daha atılmaya çalışılmıştır. Ancak Direktif, özellikle 21. yüzyılda büyük hız kazanan devrim niteliğindeki teknolojik gelişmeler ve onu takip eden dijital küreselleşme hareketleri karşısında kişisel verilerin korunmasına ilişkin ortaya çıkan yeni sorun ve tehditlerle başa çıkabilme konusunda yetersiz kalmıştır. Kişisel verilerin korunmasına ilişkin reform ihtiyacının, pek çok farklı sebebi olmakla birlikte ortaya çıkan bu yetersizliğin, kişisel verilerin korunması kapsamında bir reform yapılması ihtiyacının en önemli sebeplerinden biri olduğu söylenebilir[275].

Konuyu biraz daha detaylandırmak gerekirse, küresel anlamda yaşanan dijital devrim ile birlikte özellikle e-ticaret, e-devlet uygulamaları gibi çevirim içi işlemlerin yükselişe geçmesi, sosyal medya da dahil dijital platformlara bireysel

[274] Ulrich Haltern, ss.180-181, 184-185; Andreas Vosskuhle, ss. 146-149.
[275] European Commission, 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 final**, 4.11.2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF (02.06.2020) s.2.

katılımın artması ile birlikte büyük miktar ve çeşitlilikte kişisel veri, çevirim içi ağ akışına dahil olarak kolaylıkla erişilebilir hale gelmiştir. Dijitalleşme alanında yaşanan bu gelişmeler sebebi ile, bilgi, bilişim ve iletişim alanlarında yaşanan büyük değişim ve ilerlemelerle, veri akışının artmasının, ekonomiye yansıması olarak da tanımlanabilen ve günümüzde ekonomik büyüme ve sosyal değişimin anahtarı niteliğinde olan dijital ekonominin[276], küresel pazardaki payı da her geçen gün artmaktadır[277]. Dijital ekonomi kapsamında internet kullanımının da artmasına bağlı olarak alışılmış tüketici profili, tüketim alışkanlıkları, kurum ve kuruluşların iş yapma ve pazarlama şekil ve koşulları da büyük değişime uğramıştır. Sosyal hayatta, kamu sektöründe ve özel sektörde yaşanan bu değişim rüzgarları, internetin ve dolayısı ile de verilerin ticarileşmesine yol açmıştır. Nitekim internetin hızla ticarileşmesiyle, kişisel veriler de dahil verilerin, daha önce akla gelmedik şekillerde toplanarak, ticari amaçlarla işlenme hacim ve çeşitliliği de artmıştır. Bu hızlı dijital değişim sürecinde, özellikle çok uluslu şirketlerin küresel ticaretteki ağırlıklarının artması, hem kişisel verilerin sınır ötesi hareketliliğini, hem de bu verilerin küresel çapta toplanarak özellikle de tüketici davranışlarının değerlendirilerek, yeni pazarlama stratejilerinin belirlenmesi gibi ticari amaçlarla kullanılması oranını daha da artırmıştır. İnternetin ticari faaliyetlerdeki durdurulamaz yükselişi ve artan sınır ötesi hareketlilik pek çok başka sorunla birlikte, kişisel verilere ve mahremiyete yönelen tehdit ve ihlalleri artırarak, bu konularda Birlik hukuku kapsamında bir reform yapılması ihtiyacını doğurmuştur[278].

Artan teknolojik gelişmeler ve internetin ticarileşmesinin beraberinde getirdiği kişisel verilerin toplanarak, depolanmaları ve işlenmelerine yönelik yeni teknik ve iş modelleri sebebiyle, işletmeler, artık her zamankinden daha fazla kişisel

---

[276] Erik Brynjolfsson, Brian Kahin, **Understanding the Digital Economy: Data, Tools and Research**, MIT Press, UK, 2002, s. 1.

[277] European Commision, **Digital Agenda for Europe**, 2014, http://eige.europa.eu/resources/-digital_agenda_en.pdf , ss.3-4.

[278] Ayşe Nur Akıncı, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", T.C. Kalkınma Bakanlığı, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, **Çalışma Raporu,** No. 6, Yayın No.2968, Haziran 2017, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf (02.06.2020) ss.10-11; European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union", **COM (2010)**, **609 final,** ss.2-5

[278] European Commission, **Press Release**, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to cut Costs for Businesses", Brussels, 2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm (02.06.2020).

veriye ulaşabilmektedirler. Gelişen tekniklerle, bu veriler üzerindeki hakimiyetlerini günden güne artırarak, kişisel veriler üzerindeki kontrolü ele geçiren bu işletmeler, verileri kendi ticari çıkarları doğrultusunda kullanmaktadırlar. Gelişmiş bilgisayarlar ve akıllı cihazlar ile yapay zeka ve veri madenciliği teknik ve uygulamaları, istatistiksel modeller, GPS gibi konum uygulamaları, big data, bulut bilişim v.b. sayısız teknolojik imkanlarla yapılan veri analizi yöntemleri, neredeyse görünmez bir boyuta geçerek, bireyler tarafından artık daha az fark edilebilir hale gelmişler ve dolayısı ile de veri süjelerinin, kendi kişisel verileri üzerindeki hakimiyetlerinin aşınmasına yol açmışlardır. Bireylerce algılanma oranı düşen bu gelişmiş teknikler sonucu ortaya konan şaşırtıcı sonuç ve korelasyonlar ise kısa vadede bireylere fayda sağlıyor gibi görünse de uzun vadede bireyler aleyhine ciddi mahremiyet sorunları ortaya koymaktadırlar. Neticede bu gelişmeler, az önce de belirtildiği gibi, kaçınılmaz olarak, bireylerin kişisel verileri üzerindeki kontrollerini kaybetmelerine de yol açarak, temel haklardan biri olan kişisel verilerin korunmasını neredeyse imkansız hale getirmişlerdir[279]. 95/46 sayılı Direktif ise, kişisel verilerin toplanma, depolanma ve işlenme şekillerinin daha tanımlanabilir, öngörülebilir ve izlenebilir; niceliklerinin de nispeten daha az olduğu bir dönem için tasarlandığından, özellikle 21. yüzyıldan itibaren kişisel verilerin toplanarak işlenmesi kapsamında ortaya çıkan bu yeni teknik ve mekanizmalarla sayı ve içerik bağlamında başa çıkmakta zorlanarak, neredeyse çağ dışı kalmıştır[280].

Reform ihtiyacının doğmasının bir başka önemli sebebi de, Lizbon Antlaşması ile temel bir hak olarak Kurucu Antlaşmalar düzeyinde tanınarak, korunur hale gelen kişisel verilerin, Birlik hukuku kapsamında doğrudan uygulanabilir olmayan Direktif ile korunarak, serbest dolaşımlarının sağlanmaya çalışılması yönteminin, yaşanan devrim niteliğindeki teknolojik değişimler karşısında yeterlilik ve güvenilirliğini yitirmesidir. Zira çerçeve nitelikli hükümler içeren Direktif'te belirlenen koşul ve sınırlamalar kapsamında, üye devletlerin her birinin ayrı ayrı yaptıkları ulusal düzenlemelerle, kişisel verilerin Birlik içinde

[279] Ira S.Rubinstein, ss.1-2;
European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union", **COM (2010), 609 final,** s.2.
[280] Paul De Hert, Vagelis Papakonstantinou, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", **Computer Law & Security Review**, Cilt.28, Sayı.2, 2012, ss. 131, 138-141.

birbirinden farklı seviyelerde korunarak, serbest dolaşımlarının sağlanmaya çalışılması, kaçınılmaz olarak farklı uygulamaların ortaya çıkmasına da yol açmıştır. Bu durum, Birlik içindeki farklı uygulamalara uyum sağlayarak, üye devletlerde ticari faaliyetlerde bulunmaya çalışan tüzel kişilerin, katlanmak zorunda oldukları idari yükün de ağırlaşmasına yol açmakta idi. Neticede ortaya çıkan bu durum, Birlik'in parçalı yapısını perçinleyerek, tamamen uyumlaştırılmış yasal düzenlemeler çerçevesinde tamamlamaya çalıştığı yekpare bir Avrupa dijital tek pazarı oluşturma nihai hedefine ulaşmasını da baltalamaktaydı. Ayrıca kişisel verilerin korunmasına ilişkin farklı yasal düzenlemelerin varlığı, Birlik genelinde ve veri transferinin yapıldığı üçüncü ülkelerde, yeterli korumanın sağlanıp sağlanamadığı konusunda şüpheleri artırarak, dijital tek pazara ilişkin güvenilirlik algısını zayıflatmaktaydı[281].

Reform ihtiyacını doğuran bir diğer sebep de, 95/46 sayılı Direktifin kişisel verilerin işlenmesi faaliyetlerinin meşruiyetinin sağlanması bağlamında temellerini dayadığı, madde 7/a kapsamındaki düzenlemedir. Bu düzenlemeye göre, kişisel verilerin işlenmesinin meşru sayılabilmesi için, veri süjesinin işleme faaliyetine ilişkin kesin bir şekilde rıza vermesi gerekmekteydi. Ancak hem rızanın bulunması hali, hem de veri süjesinin işleme faaliyetinden önce bilgilendirilmesini ifade eden ilgili Direktifin 10, 11, 12 ve 14.maddeleri, kişisel verilerinin işlenmesine ilişkin olarak bireylerin korunması hususunda, ortaya çıkan küresel dijital gelişmeler karşısında yetersiz kalmıştır. Zira kimi somut olaylar kapsamında, 7/a'da düzenlenen kesin rızanın verilmesiyle ilgili düzenleme, kişisel verilerin korunmasına ilişkin pek çok yasal korumadan bireyler aleyhine feragat edilebileceği şeklinde yanlış yorumlamalara sebep olabilmiştir. Bu da, Direktif kapsamında korunmaya çalışılan temel hak ve özgürlükler bağlamında kabul edilebilir bir durum değildir. Ayrıca küresel çaptaki şirket ve kurumların, mahremiyetin ve kişisel verilerin korunmasına ilişkin veri süjesini bilgilendirme konusundaki politika ve kuralları da, gerek bu kuralların yeterince açık ve detaylı bir dil kullanılmadan kaleme alınmaları ve ilgili

[281] European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union", **COM (2010), 609 final**, s.3.
Paul De Hert, Vagelis Papakonstantinou, s.131; Efrén Diaz Diaz, "The New European Union General Regulation on Data Protection and the Legal Consequences for Institutions", **Church, Communication and Culture**, Cilt.1, Sayı.1, 2016, ss.208; Stephen A. Oxman, "Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?"; **Boston College International and Comparative Law Review**, Cilt.24, Sayı.1, 2000, ss. 192-193, 203;
Max Heermann, ss. 6,34-35.

şirket ve kurumlar tarafından tek taraflı olarak kolaylıkla güncellenebilmeleri, gerek bireylerin bu kural ve politikalara ilişkin metin ve formları okuma ve anlamada gönülsüz davranmaları, gerekse de küresel işlemler bağlamında bireyler aleyhine oluşan dil bariyeri sebepleri ile, kişisel verilerin korunmasının sağlanmasında yetersiz kalmışlardır. Tüm bu noktalar birlikte değerlendirildiğinde, kişisel verilerin korunmasında veri süjesinin rızası temeline dayanan 95/46 sayılı Direktifin, veri süjesinin rızasının alınmasına ilişkin pek çok detayı düzenlemediği de göz önüne alındığında çağın gerisinde kaldığı sonucu ortaya çıkmaktadır. 95/46 sayılı Direktifin ayrıca, kişisel verilerin korunması hususundaki kurallara uyulmasını denetlemeye; ihlalleri izleme ve önlemeye ilişkin etkili denetim ve yaptırım mekanizmaları getiremediği de gözlemlenmiştir[282].

Neticede tüm bu sebeplerle, kişisel verilerin etkili korunmasında yetersiz kaldığı belirlenen, 95/46 sayılı Direktifin yerine, yetkiyi merkeze alan, doğrudan uygulanabilir ve güncel ihtiyaç ve sorunlara daha net ve doyurucu yanıtlar verebilecek nitelikte olan Genel Veri Koruma Tüzüğü kabul edilmiştir. Böylece Avrupa dijital tek pazarında kişisel verilerin korunarak, serbest dolaşımlarının sağlanması bağlamında önemli bir adım daha atılmıştır. 25 Mayıs 2018 tarihi itibarı ile yürürlüğe giren bu Tüzük, kişisel verilerin korunması bağlamında Avrupa Birliği tarafından düzenlenerek uygulamaya konan en geniş kapsamlı yasal düzenlemelerden biri olması bakımından önemlidir. Bu düzenlemenin bir başka ilgi çekici yanı da, üye devletler tarafından uygulanması, ulusal hukuka uyarlama işlemine tabi olan "*direktif*" şeklinde yapılmayarak, yürürlüğe girdiği tarihten itibaren tüm üye devletler nezdinde, başkaca herhangi bir işleme gerek kalmaksızın, doğrudan etki ilkesi çerçevesinde, bağlayıcı hale gelerek, hak ve yükümlülükler doğuran "*tüzük*" şeklinde yapılmış olmasıdır.

[282] Fred H.Cate, "The Failure of Fair Information Practice Principle", **Consumer Protection in the Age of the Information Economy** (Ed. Jane K.Winn), Burlington, Ashgate, 2006, ss.351, 357, 360-365; Ira S.Rubinstein, s.2; European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union", **COM (2010) 609 final**, ss.4, 7-10.

3.3. KOMİSYON'UN REFORM ÇALIŞMALARINDAKİ ROLÜ VE GÖRÜŞLERİ

Birlik hukukunda kişisel verilerin korunması reform çalışmaları kapsamında en etkin rolü, supranasyonel bir Birlik kurumu olarak Birlik'in çıkarlarını koruyup, hedeflerini gerçekleştirmesi için çalışan "Komisyon" oynamıştır[283]. Komisyon'un, 4.11.2010 tarihinde yayınlamış olduğu belgede, kişisel verilerin korunmasında, 95/46 sayılı Direktifin küresel çapta meydana gelen dijital teknolojik gelişme ve değişimler karşısında neden yetersiz kaldığı, yeni yasal düzenlemelerin hangi hedefler doğrultusunda yapılması gerektiği kapsamlı şekilde açıklanarak, bu konudaki reform ihtiyacı net bir şekilde ortaya konmuştur[284].

4.11.2010 tarihli işbu belgede, öncelikle yeni dijital teknolojilerin kişilik hakkına, mahremiyete ve dolayısı ile kişisel verilerin korunmasına ve bu verilerin serbest dolaşımlarına yönelik olumsuz etkileri üzerinde durulmuştur. Bu olumsuzlukların giderilmesi için yapılacak reform çalışmaları sonucunda oluşturulacak uyumlu yeni yasalarla, esasen hedeflenen hususun, kişisel verilere, Birlik genelinde aynı seviyede, makul korumanın sağlanması ve verilerin serbest dolaşımlarının tesisi olduğunun da altı çizilmiştir. Komisyon, yine aynı belgede, hazırlanacak yeni yasal düzenlemeler kapsamında kişisel verilerin Birlik genelinde etkin korunabilmeleri ve serbest dolaşımlarının temini için yapılacaklar ile bu konuda ulaşılması gereken hedefleri de sıralamıştır. Buna göre; Komisyon, ilgili belgede, kişisel verilerin etkin korunabilmesinin esaslı şartlarından birinin, bu verilerin işlenmesinde şeffaflık ilkesinin net olarak uygulanması olduğunu belirtmiştir. Bu bağlamda da şeffaflık ilkesi doğrultusunda, özellikle de kişisel verilere ilişkin ihlal hallerinde, veri süjesinin, açık ve kolay anlaşılabilir bir dille bilgilendirilmesinin önemi vurgulanmıştır. Veri kontrolörlerinin kişisel verilerin işlenmesi bakımından, verilerin toplanma amaçlarıyla bağlı ve sınırlı olmaları gerektiği de Komisyonun işbu belgesi kapsamında belirtilerek, bireylerin kendi

[283] Roger Goebel, "Supranational? Federal? Intergovernmental? The Governmental Structure of the European Union After the Treaty of Lisbon", **Columbia Journal of European Law**, Cilt.20, Sayı.1, 2013, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1576&context=faculty_scholarship (02.06.2020), ss. 86-87.
[284] European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union", **COM (2010) 609 final**.

kişisel verileri üzerindeki kontrollerinin güçlendirilmesinin hedeflenmesi gerektiğinin altı çizilmiştir. Yeni hazırlanacak reform paketi kapsamında kamuoyunda, özellikle de interneti aktif olarak kullanan genç insanlar ve özellikle de çocuklar arasında, kişisel verilerin işlenmesine yönelik risklere ilişkin farkındalık yaratma ile yine bu kişisel verilerin işlenmesi öncesinde verilecek rızaya ilişkin kuralların güçlendirilmesi hedeflerine yönelik çalışmalar yapılması gerektiği üzerinde durulmuştur. Hassas kişisel verilere ilişkin düzenlemelerin, ortaya çıkan yeni bilimsel ve teknolojik değişiklikler karşısında gözden geçirilerek, "*genetik*" gibi yeni hassas veri çeşitlerinin de koruma altına alınması gereği önemle vurgulanmıştır. Yeni düzenlemeyle birlikte kişisel verilerin korunmasına ilişkin kuralların uygulanabilirliğini artırabilmek adına, etkili çözüm ve yaptırım mekanizmalarının getirilmesinin elzem olduğunun altı da Komisyon tarafından çizilmiştir. Ayrıca 2010 tarihli bu Komisyon belgesi kapsamında, kişisel verilerin korunmasının temelinde, özellikle de kişisel verilerin serbest dolaşımlarının sağlanması bağlamında, güçlü bir tek pazar stratejisi boyutunun yattığı da ifade edilmiştir. Bu boyut sebebiyle, kişisel verilere ilişkin yasaların asgari koşullarda uyumlaştırılmasının yeterli olmadığı, bu konuda Birlik düzeyinde tam uyumlu yasalara ihtiyaç duyulduğu ısrarla belirtilmiştir. Bu da kişisel verilerin korunmasına ilişkin yeni düzenlemenin, bir "*tüzük*" kapsamında yapılacağının önemli sinyallerden biri sayılırdı. Birlik düzeyinde tam uyumlu veri koruma yasasının hazırlanmasıyla, Komisyon tarafından hedeflenenler arasında; Farklı ulusal uygulamalardan kaynaklanan idari yükün azaltılması; Çok taraflı vakalarda hangi üye devlete ait ulusal veri koruma yasasının uygulanacağına ilişkin karışıklıkların önlenmesi; Üye devlet ve veri kontrolörlerinin görev ve sorumluluklarının daha açık bir şekilde tanımlanması; Uluslararası veri transferlerinin ne kapsamda ve hangi kurallara bağlı olarak yapılabileceğinin açıklığa kavuşturulması ve neticede de Birlik içerisinde kişisel verilerin korunmasına ilişkin daha güçlü ve uyumlu bir yasal alt yapıya kavuşularak, Birlik'in bu konuda kural ihraç edebilecek noktaya gelip, küresel anlamda öncü bir kural koyucu kuvvet haline getirilmesi sayılabilir[285].

Komisyon, kişisel verilerin korunmasına ilişkin yapılması gereken reform çalışmalarıyla ilgili olarak 2010 yılında ortaya koyduğu bu hedefler doğrultusunda,

[285] European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union", **COM (2010), 609 final,** ss.5-18.

25 Ocak 2012 tarihinde bir basın açıklaması da yapmıştır. Komisyon bu açıklamasıyla, özellikle bireylerin kendi kişisel verileri üzerindeki kontrollerinin artırılması ve farklı ulusal uygulamalar neticesinde kurum ve kuruluşlara yansıyan maliyetlerin azaltılması ile küresel dijital çağda ortaya çıkan yeni sorunlarla daha rahat başa çıkılabilmesi hedefleri kapsamındaki güncel reform önerisini bir kere daha açıkça dile getirmiştir. Zira, bireylerin kişisel verilerinin toplanması, depolanması ve çeşitli şekillerde işlenmesi, teknolojik gelişmelerin ve internet kullanımı ile birlikte küreselleşmenin etkilerinin insan hayatının her bir noktasına yoğun olarak tesir ettiği içinde bulunduğumuz dijital çağın doğal bir sonucudur. Ancak bu yapılırken, Birlik'in temel yapı taşlarından biri olan ve Avrupa Birliği Temel Haklar Şartı'nda da açıkça bir temel hak olarak koruma altına alınan kişisel verilerin korunması hususunun, azami surette göz önünde alınması gerekmektedir. Bu sebeplerle, kişisel verilerin, güncellenerek güçlendirilmiş doğrudan uygulanabilir Birlik yasalarıyla regüle edilip korunması ve böylelikle meşru olmayan kullanımlarının engellenebilmesi için kapsamlı bir reforma ihtiyaç duyulduğu, Komisyon tarafından pek çok kere açıkça dile getirilmiştir[286]. Komisyon, nihayet 25 Ocak 2012 tarihinde, tüm bu hedefleri göz önüne alarak, kişisel verilerin korunması ve serbest dolaşımlarının sağlanmasına ilişkin tüzük şeklinde hazırlanılan Yasa Taslağını[287] ortaya koyarak bu hususta önemli bir adım daha atmıştı.

Her alanda olduğu gibi kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bağlamında da Birlik içerisindeki yasal düzenlemelerin parçalı görünümlerinden kurtularak, tam uyumlu hale getirilmesi, Avrupa Birliği'nin dijital çağa entegre olmasının ve Avrupa dijital tek pazarından beklenen verimin alınabilmesinin anahtarı niteliğindedir. Durumun öneminin günden güne daha fazla anlaşılmasıyla birlikte, Birlik içerisinde bu konudaki çalışmalar da artmıştır.

Bu çalışmaları neticesinde, kişisel verilerin Birlik içerisinde nerede olursa olsun aynı seviyede korunması ve serbest dolaşımlarının sağlanması için yapılacak

---

[286] European Commission, **Press Release**, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses", Brussels, 25.01.2012.

[287] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)", Brussels, **COM (2012), 11 Final,** 25.1.2012, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF (02.06.2020).

yasal değişikliklerle ilgili olan Avrupa Veri Koruma Reformu'nun kapsamına ve temel noktalarına ilişkin Komisyon, Konsey ve Parlamento arasındaki üçlü görüşmeler meyvesini vermiş ve 2015 yılında bir anlaşmaya varılmıştır. Bu anlaşmanın detaylarına ilişkin Komisyon tarafından yapılan basın açıklamasına göre ise, Veri Koruma Reformu iki önemli yasal düzenlemeyi kapsayacaktır. Bunlardan birincisi bu tez çalışması kapsamında incelenecek olan "*2016/679 sayılı Genel Veri Koruma Tüzüğü*"dür. İkincisi de işbu Tüzük'ü tamamlayıcı nitelikte olan ve kişisel verilerin, suçun önlenmesi, soruşturulması, kovuşturulması veya hükmün infazı, koruyucu faaliyetler ile kamuyu ve ulusal güvenliği tehlikeye düşüren hallerin önlenmesi gibi istisnai hallerde işlenebilmesinin kapsam ve sınırlarının düzenlendiği "*2016/680 sayılı Önleyici ve Adli Faaliyetlerde Kişisel Verilerin Korunması Direktifi*[288]"dir. 2015 yılında yayınlanan bu açıklamayla, yasa taslaklarının son haliyle 2016 yılında Parlamento ve Konsey'in onayına sunularak, kabul edilecek metinlerin, iki yıllık bir geçiş dönemi sonunda yürürlüğe gireceği ve Komisyon'un ilgili yasal düzenlemelerin Birlik genelinde bir bütün olarak ve kesintisiz uygulanabilmesi için gerekli her türlü çalışmayı yapacağı da belirtilmiştir[289]. Tüm bu çalışmalar incelendiğinde, Komisyon'un, dijital çağa uyum ve temel hak ve özgürlüklerin korunması bağlamında ortaya koyduğu öncü nitelikteki görüşleri ve hazırladığı belgeler vasıtasıyla, kişisel verilerin korunmasının önemi bağlamında, Birlik düzeyinde ve üye devletler nezdinde bir aydınlanma oluşturup, bu konularda insiyatif alarak yasal düzenlemelerin yapılmasında aktif rol oynadığı rahatlıkla söylenebilir.

2016/679 sayılı Tüzük, kişisel verilerin korunması hususunda, üçüncü ülke ve uluslararası organizasyonlardaki yasa, kural ve uygulamaları değerlendirerek, verilerin buralara aktarımına ilişkin yeterlilik kararı alabilmesi, aldığı bu kararı belli aralıklarla kontrol ederek yenileyebilmesi ya da iptal edebilmesi de dahil pek çok konuda Komisyon'a takdir yetkisi tanıması sebebiyle, literatürde kimi araştırmacılar

[288] European Union, "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (02.06.2020).

[289] European Commission, **Press Release**, "Agreement on Commission's EU Data Protection Reform will Boost Digital Single Market", Brussels, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm (02.06.2020).

tarafından eleştirilmektedir. Komisyon'a tanınan takdir yetkilerinin, Komisyon'un işbu Tüzük'ün hazırlanmasında oynadığı öncü rolün bir göstergesi olduğu da söylenebilir. Bu perspektiften kimi araştırmacılar tarafından, Komisyon, kişisel verilerin korunması hususunda yapılan yasal düzenlemelere ilişkin kural koyucu (*rule setter*) bir role sahip olarak nitelendirilirken, üçüncü ülkeler de kural alıcı (*rule taker*) olarak nitelendirilmişlerdir. Hatta Brexit sonrası Avrupa Birliği'nden ayrılarak yasal anlamda üçüncü ülke durumuna gelecek olan İngiltere'nin, kişisel verilerin serbest dolaşımını sağlayarak, bu serbest dolaşımın ekonomik nimetlerinden faydalanabilmek için bir yeterlilik kararına ihtiyaç duyacağı açıktır. Bu sebeple İngiltere, 2016/679 sayılı Tüzük hükümlerine uygun bir yasal düzenlemeye gitmeyi tercih eder ise Brexit sonrası İngiltere'nin de kural alıcı bir ülke haline geleceği ileri sürülebilir[290].

3.4. 2016/679 SAYILI GENEL VERİ KORUMA TÜZÜĞÜ

27 Nisan 2016 tarihinde kabul edilip, resmi gazetede yayınlanarak[291], 25 Mayıs 2018 tarihinde yürürlüğe giren, Avrupa Birliği'nin 2016/679 sayılı Genel Veri Koruma Tüzüğü (GDPR)'nün 94. maddesinde de açıkça belirtildiği gibi, 95/46 sayılı Kişisel Verilerin Korunması Direktifi, işbu Tüzük kapsamında yürürlükten kaldırılmıştır. Tüzük'ün 94. maddesinde ayrıca, daha önce 95/46 sayılı Direktife ve Madde 29 Çalışma Grubu'na yapılan tüm atıfların, işbu Tüzük'ün yürürlük tarihinden itibaren, 2016/679 sayılı Tüzük'e ve Avrupa Veri Koruma Kurulu'na yapılmış sayılacağı kabul edilmiştir.

Yapılan bu değişiklik ile, Avrupa Birliği hukukunda, 25 Mayıs 2018'den itibaren gerçek kişilerin kişisel verilerinin korunması ve serbest dolaşımlarının sağlanması bağlamında, 2016/679 sayılı Genel Veri Koruma Tüzüğü geçerli hale gelmiştir. Giriş, kapsam ve içeriği incelendiğinde, işbu Tüzük'ün kişisel verilerin

[290] W.Gregory Voss, "Preparing for the Proposed EU General Data Protection Regulation: With or Without Amendments", **Business Law Today** Cilt.1, 2012, https://www.academia.edu/11847219/Preparing_for_the_Proposed_EU_General_Data_Protection_Regulation_With_or_without_Amendments (02.06.2020), s. 2;
Oliver Patel, Nathan Lea, "EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?" **UCL European Institute, Brexit Insights**, 2019, https://www.ucl.ac.uk/european-institute/sites/european-institute/files/eu-uk_data_flows_brexit_and_no-deal.pdf (02.06.2020) ss.5-6, 13-14.

[291] 2016/679 sayılı Genel Veri Koruma Tüzüğü, 27 Nisan 2016'da kabul edilmesini takiben Avrupa Birliği'nin 4.5.2016 tarih ve L119/86 sayılı Resmi Gazetesinde yayınlanmıştır.

korunmasının garanti altına alınarak, dijital tek pazarda işlem yapan gerçek kişiler açısından oluşturulacak güven ortamında, temel hak ve özgürlüklerin korunması ilkesi çerçevesinde, Avrupa dijital tek pazarının yeknesak kurallar dahilinde aksamadan işlemesinin sağlanarak, dijital ekonomiden de alınan payın artırılması nihai hedefi ile birlikte, oluşturulduğu anlaşılabilmektedir. Bu nihai hedefler doğrultusunda Tüzük ile, hangi üye devletin vatandaşı olduklarına veya Birlik sınırları dahilinde nerede ikamet ettiklerine bakılmaksızın, gerçek kişilere ait kişisel verilerin, kısmen veya tamamen, otomatik olarak ya da bir dosyalama sisteminin parçasını oluşturan araçlar vasıtasıyla, işlenmelerine karşı korunarak, verilerin serbest dolaşımlarının sağlanması amacıyla Birlik düzeyinde kurallar getirildiği görülmektedir[292].

3.4.1. Genel Veri Koruma Tüzüğü'ne Hakim Olan Temel İlkeler

Kişisel verilerin korunmasına ve serbest dolaşımlarına ilişkin olarak ortaya konan Veri Koruma Reform paketi, özü itibarı ile, tıpkı kendinden önceki yasal düzenlemelerde olduğu gibi, veri kontrolörleri ve işleyicileri ile veri süjeleri arasında, kontrolör ve işleyiciler lehine var olan asimetrik gücün dengelenebilmesini amaç edinmiştir. Bu amaçla, reform paketinde, dengeyi sağlayarak, kişisel verilerin daha etkili korunabilmeleri hususunda veri süjelerinin ellerini güçlendirip, birbirlerine kaynaklık ederek tamamlayacak nitelikteki temel ilkeler [293] ortaya konmuştur[294]. Önceden kişisel verilerin işlenmesine ilişkin olarak mülga 95/46 sayılı Direktif'te de genel olarak sayılan bu temel ilkeler, Veri Koruma Reformu kapsamında yapılan yeni yasal düzenlemelerin hazırlanmasında da önemlerini korumuşlardır. Nitekim, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bağlamında 2016/679 sayılı Tüzük uygulanırken ya da somut olay kapsamında yorumlanırken mutlaka göz önünde bulundurulması gereken bu temel ilkeler, gözden geçirilip, Tüzük'ün "*II. Bölümü*" kapsamında yerlerini almışlardır.

[292] GDPR Beyanlar 1,2,7,123, Madde 1-2.
[293] Bu tez çalışmasının "*2.2.2. Kişisel Verilerin İşlenmesi*" başlıklı bölümü altında kişisel verilerin işlenmesinde göz önüne alınması gereken temel ilkelerin detaylı açıklamaları bulunmaktadır.
[294] Damian Clifford, Jef Ausloos, Data Protection and the Role of Fairness, KU Leuven, Center for IT & IP Law, **Working Paper Series 29/2017**, https://ssrn.com/abstract=3013139 (02.06.2020), s.7; Elif Küzeci, s. 205.

2016/679 sayılı Tüzük madde 5 incelendiğinde, mülga 95/46 sayılı Direktif ile kabul edilen, "*Adil ve Yasal İşleme (Lawfulness & fairness)*[295]", "*Amaç ile Sınırlılık (Purpose Limitation)*[296]", "*Veri Minimizasyonu (Data Minimisation)*[297]", "*Doğruluk ve Güncellik (Accuracy)*[298]", "*Süreyle Sınırlı Saklama (Storage Limitation)*[299]" ile "*Bütünlük ve Gizlilik (Integrity & Confidentiality)*[300]" ilkelerinin, Tüzük kapsamında da geçerlilik ve içeriklerini korudukları görülebilmektedir. Mülga 95/46 sayılı Direktif'ten farklı olarak, "*Hesap verebilirlik (Accountability)*" ilkesi, ilk kez Tüzük'ün 5/2.maddesi kapsamında zikredilerek yürürlüğe girmiştir. Hesap verebilirlik ilkesi gereği, veri kontrolörü, kişisel verilerin işlenmesine ilişkin olarak 5.madde kapsamında ortaya konan ilkelerin uygulanmasından sorumlu tutulmuştur. Yine ilk kez Tüzük maddeleri kapsamında kabul edilen "*şeffaflık ilkesi (Transparency)* [301]*"* ise, içinde veri kontrolörleri açısından bir yükümlülük, veri sujleri açısından da bir hak barındırması bakımından önem arz eden bir ilkedir. Açıklamak gerekirse, şeffaflık ilkesi, hem veri kontrolörlerinin, veri süjelerini kişisel verilerinin işlenmelerine ilişkin olarak kısa, kolay anlaşılır ve şeffaf bir şekilde bilgilendirmelerine ilişkin yükümlülüklerini, hem de veri süjelerinin kişisel verilerine ve bu verilerin hangi amaç ve kapsamla işlendiklerine ilişkin bilgilendirmeye kolaylıkla erişebilme haklarını, ifade eder[302].

Tüzük madde 23/1'de sayılan istisnai hallerde kamu yararının korunmasının gereği olarak;

a) Hakkın özüne dokunulmaması, ve,

b) Meşru bir amaca hizmet etmek için gerekli olması,

c) Demokratik toplumla bağdaşabilecek düzeyde orantılı tedbirler alınması, ile,

d) Yasal düzenlemeler aracılığıyla yapılması kaydıyla,

---

[295] GDPR Madde 5/1 (a); mülga 95/46 sayılı Direktif Madde 6/1 (a).
[296] GDPR Madde 5/1 (b); mülga 95/46 sayılı Direktif Madde 6/1 (b).
[297] GDPR Madde 5/1 (c); mülga 95/46 sayılı Direktif Madde 6/1 (c).
[298] GDPR Madde 5/1 (d); mülga 95/46 sayılı Direktif Madde 6/1 (d).
[299] GDPR Madde 5/1 (e); mülga 95/46 sayılı Direktif Madde 6/1 (e).
[300] GDPR Madde 5/1 (f); mülga 95/46 sayılı Direktif Madde 16-17.
[301] GDPR Madde 5/1 (a); mülga 95/46 sayılı Direktif Beyanlar (63).
[302] GDPR Beyanlar (58);
Bird & Bird, **Guide to the General Data Protection Regulation**, ss.5, 7-8; European Union Agency for Fundamental Rights, 2018, ss.116-120.

kişisel verilerin işlenmelerine ilişkin Tüzük madde 5'te sayılan temel ilkelerin uygulanmalarına kısıtlama getirilebilir. Bu gibi istisnai hallerin neler olduğu ilgili Tüzük'ün 23.maddesinde sayılmıştır.

23.maddeye göre; "*Ulusal güvenliğin veya savunmanın gerektirdiği hallerde; ceza hukuku alanına giren suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması, kamu güvenliğinin korunmasına ilişkin tedbirlerin alınarak tehditlerin önlenmesi, adli ya da cezai yaptırımların ifası durumlarında; mali, vergi ve bütçe kaynaklı hususlar ile kamu sağlığı, sosyal güvenlik gibi konularda üye devletlerin ya da Birlik'in ekonomik veya finansal menfaatleri ve benzeri kamu yararının korumasını gerektiren hallerde; yargı bağımsızlığının korunması amacıyla; yasalarla düzenlenmiş meslek gruplarının etik kuralları ihlallerinin önlenebilmesi için, bu gibi durumların soruşturulması, tespit edilmesi veya kovuşturulmasının gerektirdiği hallerde; veri süjesinin veya diğerlerinin temel hak ve özgürlüklerinin korunmasının için gereken durumlarda; medeni hukuka ilişkin hakların icra edilmesinin gerekli kıldığı hallerde"* istisnai olarak kişisel verilerin işlenmesinde temel ilkelerin uygulanmalarına ilişkin bazı kısıtlamalara gidilebilir. Ancak madde 23/1 kapsamında yapılacak bu kısıtlamaların meşru kabul edilebilmesi için yukarıda hakkın özüne dokunulmaması, meşru bir amaca hizmet edebilmek için gerekli olması, demokratik toplum düzeni ile bağdaşacak şekilde orantılı olması ve bir yasal düzenleme vasıtasıyla yapılması, şeklinde sayılan koşulların, somut olay kapsamında bir arada sağlanması gerektiği de unutulmamalıdır[303].

Avrupa Adalet Divanı'nda görülen "*Schwarz v. Stadt Bochum*" davasında, hassas kişisel verilerden biri olan parmak izi verisi olmadan Bay Schwarz'a pasaport verilmemesinin, kişisel verilerin korunması bağlamında istisnai hallere girerek, işleme yasağından muafiyet tanınmasının söz konusu olup olamayacağı hususu incelenmiştir. Dava sonucu verilen kararda, üye devletlerin, hassas kişisel verilerin – somut olayda parmak izlerinin korunmasını, en üst düzeyde garanti altına almaları kaydıyla- pasaport ile veri süjesi arasındaki bağı en doğru ve güvenilir şekilde kurabilmeyi sağlayıp, kimlik tespitinin hataya yer bırakmayacak şekilde yapılarak, kamu güvenliğinin sağlanabilmesi amacıyla, pasaport verilmesini, parmak izi şartına bağlayabilecekleri hüküm altına alınmıştır. Diğer bir ifade ile, Schwarz kararında,

[303] European Union Agency for Fundamental Rights, 2018, ss. 49-51.

Birlik sınırlarının güvenliğinin sağlanabilmesi amacıyla, kimlik tespitinin yapılmasının öneminin altı çizilerek, bu bağlamda pasaportların parmak izi verilmesi şartına bağlanması, meşru amaç sayılarak, alınan tedbir, orantılı olarak değerlendirilmiştir. Bu tedbirin alınması için gerekli düzenlemelerin de, hazırlanan yasalar dahilinde yapıldığı belirtilmiştir. Güvenlik amacıyla yasa kapsamında alınan bu tedbirin ise Avrupa Temel Haklar Şartı'nın 7. ve 8.maddeleri kapsamında korunan hakların özüne dokunduğuna ilişkin bir tespit de yapılamadığından somut olay kapsamında istisna uygulanmasında sakınca bulunmadığı belirtilmiştir. Bu karar kapsamında ayrıca, istisnanın uygulanabilmesi için ilgili kişisel verilerin bütünlük, güvenilirlik ve gizliliklerinin, güvence altına alınabilmeleri amacıyla, gerekli her türlü tedbirin üye devletler tarafından alınmasının gerekliliğinin altı da kuvvetli bir şekilde çizilmiştir [304] . Somut olaya ilişkin tüm gerekçeler bir arada değerlendirildiğinde, Adalet Divanı'nın Schwarz Kararının, kişisel verilerin işlenme yasağı istisnalarının, temel ilkelerin ışığı altında, somut olay kapsamında nasıl uygulanması gerektiğine ilişkin güzel bir referans oluşturduğu söylenebilir.

3.4.1.1. Kişisel Verilerin Adil, Yasal ve Şeffaf İşlenmesi

Tüzük'ün içeriğinde "*adil işleme*"nin nasıl olması gerektiğine ilişkin açık bir tanım yapılmamıştır. Buna rağmen bu ilkenin de, genel olarak yasal koruma sağlanması bağlamında birbiriyle yarışır nitelikte olan ve aralarında hiyerarşik bir ilişki de bulunmayan temel hak ve özgürlükler ile diğer meşru menfaatler arasında, "*hakkın özünün korunması ve orantılılık ilkeleri*" de göz önüne alınarak, adil bir dengenin kurulmasına hizmet ettiği söylenebilir. Bu ilke, özellikle aralarında veri kontrolörü lehine asimetrik bir güç bulunan, veri süjesi ile veri kontrolörü arasındaki hassas ilişkinin nasıl yönetilmesi gerektiğine ilişkindir. Veri kontrolörü ve veri süjesi arasındaki bu ilişki kapsamında veri süjesinin, kişisel verilerinin yasal sınırlamalar dahilinde hangi kapsamda, ne amaçla, kimler tarafından, ne sürede işlenebileceği, verilerin kimlerin erişimine açık olacağı ve bu işlemeden kaynaklanan olası risklerin neler olduğu hakkında veri kontrolörü tarafından açık bir şekilde bilgilendirilmesi

[304] Judgment of the Court of Justice of the European Union (Fourth Chamber), 17.10.2013, **ECJ Case C291/12**, Michael Schwarz v. Stadt Bochum, http://curia.europa.eu/juris/liste.jsf?num=C-291/12 (02.06.2020).

gereklidir. Bu bilgilendirme neticesinde, veri süjesi karşısında, kontrolör lehine olan asimetrik gücün dengelenerek, kişisel verilerin işlenmesinin adil işleme ilkesi çerçevesinde gerçekleştirilmesi sağlanabilir. Kişisel verilerin adil işlenmesi ilkesi bağlamında veri süjesinin açıkça bilgilendirilmesinin gerekliliği noktasında ise, veri kontrolörüne sorumluluk yükleyen "*şeffaflık ilkesi*" ortaya çıkmaktadır. Şeffaflık ilkesi, bilgilendirme, iletişime açık olma ve hesap verebilirlik kapsamında değerlendirilmesi gereken, Birlik hukukunun temel değerlerindendir. Kişisel verilerin korunması hususunda şeffaflık ilkesinin ise, işleme kapsam, süre ve çeşitleri çerçevesinde kişisel verilere kimler tarafından, hangi yollarla, hangi süreler kapsamında, ne dereceye kadar erişimin sağlanacağına ilişkin bilgilendirmenin, veri süjesine açıkça ve uygun şekillerde yapılması gerek ve sorumluluğunu, bir diğer ifade ile verilerin adil işlenmesi sorumluluğunu, veri kontrolörüne yüklediği söylenebilir[305].

Kişisel verilerin işlenmesinde hukuka uygunluğu, bir başka ifade ile, işlemenin ancak ve ancak yasal düzenlemeler kapsamında ve bunlarla sınırlı olarak yapılabilmesini, temsil eden "*yasal işleme*" ilkesine ilişkin koşullar ise, Tüzük madde 6 (1)'de özel olarak sayılmıştır. Buna göre, kişisel verilerin işlenmesinin yasal işleme ilkesi çerçevesinde gerçekleştirilebilmesi için, sayılan altı gerekçeden ilki, açıkça belirlenen bir veya daha fazla amaç çerçevesinde kişisel verilerinin işlenmesi hususunda veri süjesinin usulüne uygun verilmiş "*rızası*"nın bulunmasıdır.

Tüzük madde 6/1'de sayılan kişisel verilerin işlenebilmesine ilişkin diğer hukuka uygunluk sebepleri ise, "*veri işlemenin, 1. Kişisel verilerin işlenmesinin veri süjesinin halihazırda taraf olduğu veya taraf olmaya hazırlandığı bir akdin hayata geçirilebilmesi için gerekli olması hali; 2. Veri kontrolörünün tabi olduğu bir yasal yükümlülüğün, orantılılık ilkesi de göz önüne alınarak, yerine getirilmesi için gerekli olması hali; 3. Veri süjesinin ya da bir diğer gerçek kişinin hayati nitelikteki menfaatlerinin korunması için mutlaka gerekli olması hali; 4. Kamu yararına olan yasal bir görevin ifası veya veri kontrolörüne ait resmi bir yetkinin kullanılması için,*

[305] European Union Agency for Fundamental Rights, 2018, ss.117-120; Anoeska Wilhelmina Geertruida Johanna Buijze, "The Principle of Transparency in EU Law", **Thesis,** 2013, Uitgeverij BOX Press, 's-Hertogenbosch, ISBN 978-90-8891-579-6, ss.28-30, 243-244;
William B.T. Mock, "On The Centrality of Information Law: A Rational Choice Discussion of Information Law and Transparency", **John Marshall Journal of Computer & Information Law**, Cilt.17, 1999, ss. 1080-1082; Damian Clifford, Jef Ausloos, ss. 11-15.

yine orantılılık ilkesi dahilinde yapılması koşuluyla, gerekli olması hali", şeklinde sıralanabilir.

Tüzük madde 6/1 (f) kapsamında ise, bir başka hukuka uygunluk sebebi olarak, veri kontrolörü ya da üçüncü kişiler tarafından gözetilen meşru menfaatler bakımından kişisel verilerin işlenmesinin gerekli olması hali sayılmıştır. Ancak (f) bendi kapsamında belirtilen bu hukuka uygunluk sebebinin geçerli olabilmesi için, özellikle çocukların kişisel verilerinin korunmasına ilişkin özel hükümler saklı kalmak kaydı ile, veri süjesinin, kişisel veriler bağlamında korunan çıkarlarının veya temel hak ve özgürlüklerinin, (f) bendi kapsamında bahsedilen işbu meşru menfaatlere baskın gelmemesi gerekmektedir. Kamu kuruluşlarının görevlerini yerine getirirken işlemek zorunda kaldıkları kişisel verilere ise, Tüzük madde 6/1 (f) bendinin uygulanmayacağı madde 6/1 kapsamında ayrıca belirtilmiştir.

Madde 6'nın 4.fıkrasında da, kişisel verilerin, toplanma amacı dışında bir amaca ilişkin olarak işlenebilmesinin koşulları düzenlenmiştir. Bu maddeye göre, yeni amaca ilişkin veri süjesinin rızası yoksa veya bu yeni amacın Tüzük madde 23/1'de sayılan istisnai haller çerçevesinde alınacak, demokratik toplumla bağdaşabilecek düzeyde orantılı tedbirler kapsamında sayılabilmesini sağlayacak Birlik ya da üye devlet yasası da bulunmuyorsa; veri kontrolörü, yeni amaç doğrultusunda yapılacak veri işleme faaliyetinin, verilerin asıl toplanma amacıyla uyumlu olup olmadığını değerlendirmelidir. Veri kontrolörünün bu değerlendirmeyi yapabilmesi için de, aşağıdaki hususları inter alia dikkate alması gerekir:

a. Verilerin ilk toplanma amacı ile, işleme yapılması düşünülen yeni amaç arasında herhangi bir bağ olup olmadığı (*Tüzük Madde 6/4 a*);

b. Veri süjesi ve veri kontrolörü arasındaki ilişkinin kapsamı başta olmak üzere, kişisel verilerin toplanma kapsamının ne olduğu (*Tüzük Madde 6/4 b*);

c. Madde 9 kapsamına uygun şekilde işlenen özel kategorideki kişisel veriler ile madde 10 kapsamında işlenen *mahkumiyet* kararları ve adli suçlara ilişkin kişisel veriler başta olmak üzere, işlenecek kişisel verilerin niteliklerinin ne olduğu (*Tüzük Madde 6/4 c*);

d. Daha sonra yapılması planlanan işleme faaliyetlerinin veri süjesine olası etkilerinin neler olacağı (*Tüzük Madde 6/4 d*);

e. "*Şifreleme (encryption)*" ya da "*takma ad (pseudonymisation)"* kullanma da dahil, uygun önlemlerin alınıp alınmadığı (*Tüzük Madde 6/4 e*).

Tez çalışmasının bu bölümünde ele alınan tüm hususlar birlikte değerlendirildiğinde, kişisel verilerin adil, yasal ve şeffaf işlenme ilkelerinin, birbirlerini tamamlayıcı nitelikte ilkeler oldukları ve işleme falliyetlerinin yapılabilmesi için bir arada aranmaları gerektiği söylenebilir[306].

Avrupa Birliği, Avrupa Dijital Tek Pazarının tamamlanmasına yönelik olarak yaptığı pek çok çalışma ve bu çalışmalar sonucu ortaya koyduğu belgelerde, dijital tek pazarın geliştirilmesi hususunda yapılacak şeffaflığı, hukuki öngörülebilirliği ve dolayısı ile güveni artırıcı nitelikteki her türlü uygulamada, Genel Veri Koruma Tüzüğü'ne de hakim olan ve Tüzük'ün 5.maddesi kapsamında sayılan bu temel ilkelerin uygulanmasının önemini vurgulamaktadır[307].

3.5. GENEL VERİ KORUMA TÜZÜĞÜ KAPSAMINDA GETİRİLEN ÖNEMLİ DEĞİŞİKLİKLER

25 Mayıs 2018 tarihinde, Avrupa Birliği'ne üye tüm devletlerde aynı anda, doğrudan etkili olacak şekilde yürürlüğe giren, Genel Veri Koruma Tüzüğü, yasal düzenlemelerin Birlik düzeyinde uyumlaştırılması sebebiyle, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması anlamında atılmış devrim niteliğinde bir adımdır. Tüzük'ün önemi, sadece yaşanan dijital devrime uygun olarak, kişisel verilerin korunması hususunda getirdiği esaslı değişikliklerden değil, üye devletlerle birlikte, Avrupa Birliği ile iş yapmak isteyen ve Birlik içinde bulunan gerçek kişilerin verilerini bir şekilde işleyen dünya üzerindeki tüm kişi, kurum ve kuruluşları bağlamasından da kaynaklanmaktadır. Bu sebeple, ister Avrupa Birliği içinde kurulu olsun ister olmasın, dünya üzerindeki en büyük tek parça pazar niteliğindeki Avrupa tek pazarında, iş yapmak isteyen tüm şirketler, Tüzük'ün kişisel verilerin korunması bağlamında getirdiği koşul, değer ve standartlara uyarak, "*veri*

[306] European Union Agency for Fundamental Rights, 2018, s.119; Damian Clifford, Jef Ausloos, ss. 9,22.

[307] European Commission, "Completing a Trusted Digital Single Market for All", **COM 320 Final**, 2018;
European Commission, **Press Release**, "Digital Single Market: EU Negotiators agree to set up new European rules to improve fairness of online platforms' trading practices", Strasbourg, 14.02.2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168 (02.06.2020).

koruma dostu ürün ve hizmetler (data protection friendly products and services)" geliştirmek zorundadırlar. Tüm bunları başarabilenlerin, pazarın geri kalanından hızlı büyüyen Avrupa dijital tek pazarının sunduğu nimetlerden daha fazla yararlanabileceğine de şüphe yoktur. Genel Veri Koruma Tüzüğü, zaman zaman özellikle ABD kökenli kaynaklar tarafından, Avrupa dijital tek pazarını, aşılması zor bir dijital kale haline getirdiği şeklinde eleştirilse de, kişisel verilerin korunması hususunda getirdiği yüksek standartlar vasıtasıyla, 2016/679 sayılı Tüzük'ün dünya genelinde mahremiyetin ve temel hak ve özgürlüklerin korunması bağlamında da bir referans noktası oluşturduğu ve bu konuda güvenilir bir dijital pazar oluşturulması için uluslararası standartların ortaya konmasına öncülük ettiği söylenebilir[308]. Ayrıca 2016/679 sayılı Tüzük ile getirilen hükümlerin ve yaptırımların, Birlik dışında olduğu kadar, Birlik içinde de oldukça sıkı uygulandığı göz önüne alındığında, dijital kale benzetmesinin gerçek durumu yansıtmadığı görülebilmektedir. Bu bölümde Avrupa Birliği'nin kabul ettiği Genel Veri Koruma Tüzüğü kapsamında getirilen önemli değişiklikler incelenerek, bu değişikliklerin Avrupa Dijital tek pazarının gelişimine olan katkıları incelenmeye çalışılacaktır.

3.5.1. Genel Veri Koruma Tüzüğü'nün Bölgesel ve Maddi Kapsamı

Mülga 95/46 sayılı Direktif ile karşılaştırıldığında, 2016/679 sayılı Genel Veri Koruma Tüzüğü ile, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması kapsamında bazı önemli değişiklikler yapıldığı anlaşılmaktadır. Tüzük'ün getirdiği bu önemli değişikliklerden biri de, Tüzük hükümlerinin uygulanacağı "*Bölgesel Kapsamın*" genişletilmesidir.

Tüzük'ün "*Bölgesel Kapsam (Territorial Scope)*" başlıklı 3.maddesi kapsamında, işbu Tüzük'ün bölgesel anlamda hangi sınırlar dahilinde uygulanabileceği iki temel faktör göz önüne alınarak belirtilmiştir. Bu faktörlerden ilki, veri kontrolörü veya işleyicisinin "*ikamet yeri*"dir. Buna göre, ikamet yeri, Birlik sınırları içerisinde bulunan veri kontrolörünün veya işleyicisinin, Birlik içinde ya da dışında yapmış olduğu kişisel verilerin işlenmesine ilişkin tüm faaliyetlerinin, bu faaliyetlerin nerede gerçekleştiklerine bakılmaksızın, işbu Tüzük'ün uygulama

[308] Jan Philipp Albrecht, "How the GDPR Will Change the World", **European Data Protection Law Review**, Cilt.2, Sayı.3, 2016, ss. 287-289.

kapsamında kalacağı belirtilmiştir. Bu bağlamda Tüzük madde 3/1 ile mülga 95/46 sayılı Direktifin 4/1 (a) maddeleri karşılaştırıldığında, ikamet yeri anlamında bölgesel kapsamın sınırlarının belirlenmesinde esaslı bir değişiklik olmadığı anlaşılmaktadır[309].

Tüzük'ün bölgesel kapsamının sınırlarının belirlenmesinde kullanılan ikinci faktör ise, Birlik vatandaşı olup olmadığına bakılmaksızın, veri işleme faaliyetlerinin, "*Birlik içinde bulunan gerçek kişileri hedef alması*"dır. Burada gerçek kişilerin hedef alınmasından kasıt, bu kişilere –ücretli ya da ücretsiz olarak- bir mal veya hizmet sunulması yahut bu kişilerin Birlik içerisindeki davranışlarının izlenmesidir[310].

Tüzük madde 3/2 (a) incelendiğinde, işbu Tüzük hükümlerinin, Birlik vatandaşı olan yahut vatandaş olmamakla birlikte Birlik içerisinde bulunan, gerçek kişilere ait kişisel verilerin, Avrupa Birliği içerisinde kurulu olmayan veri kontrolörü veya işleyicisi tarafından, veri süjesine ücretli ya da ücretsiz mal veya hizmet sunulması ile ilgili olarak işlenmesi halinde de uygulanabileceği görülmektedir. Bu madde kapsamından verilen hizmetin ücretsiz olmasının dahi, Birlik dışında yerleşik bulunan veri kontrolörü ya da işleyicisinin veri işleme faaliyetlerine, işbu Tüzük hükümlerinin uygulanmasını engelleyemeyeceği anlaşılmaktadır. Tüzük madde 3/2 (b)'de de yine, Birlik vatandaşı olan yahut vatandaş olmamakla birlikte Birlik içerisinde bulunan gerçek kişilerin, ağ üzerinde bıraktıkları izlerin, Avrupa Birliği içerisinde kurulu olmayan veri kontrolörü veya işleyicisi tarafından izlenip, bu yolla veri süjesinin davranışlarının veya tutumlarının analiz edilmesi hallerinde de Tüzük hükümlerinin somut olaya uygulanabileceği ifade edilmektedir. Bu bağlamda Birlik vatandaşı olsun olmasın, Birlik içerisinde bulunan gerçek kişilerin kişisel verilerine ilişkin işleme faaliyetleri yapıldığı taktirde, bu faaliyetleri gerçekleştiren ve Birlik içinde ve/veya dışında yerleşik olan veri kontrolörleri ya da işleyicilerinin yönetim ve sorumluluğunda bulunan, çerez (*cookies*) uygulamaları, web siteleri, arama motorları, sosyal medya platformları, casus yazılımlar v.b. uygulama ve araçlar

[309] Paul de Hert, Michal Czerniawski, "Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context", **International Data Privacy Law**, Cilt.6, Sayı 3, 2016, ss. 236-238.
[310] Paul de Hert, Michal Czerniawski, ss. 236-239, 242-243.

üzerinden yapılan inceleme ve analizler de, madde 3/2 (b) kapsamında kabul edilerek, 2016/679 sayılı Tüzük'ün uygulama alanına girebilmektedirler[311].

Tüzük madde 3 kapsamı incelendiğinde, kişisel verilerin korunması hususundaki Tüzük'ün uygulama alanının bölgesel anlamda genişletilerek, Birlik ile ekonomik, sosyal, siyasi herhangi bir bağ kurarak, Birlik vatandaşlarının ya da Birlik içinde bulunan gerçek kişilerin, kişisel verilerini işleme veya izleme ihtimali bulunan dünyanın neresinde kurulu olursa olsun Birlik dışı veri kontrolörü veya işleyicisinin de Tüzük ile bağlı olacağı hükmünün getirildiği anlaşılmaktadır. Diğer bir ifadeyle, madde 3 ile, Tüzük'ün uygulama alanı bölgesel kapsamda genişletildiğinden, kişisel verilerin korunması hususunda getirilen bu yeni hüküm ve sınırlandırmalar hakkında Birlik ile iş yapan ya da yapacak olan Birlik dışı veri kontrolörü veya işleyicilerinin de bilgi sahibi olmaları, işlerin aksamadan yürütülebilmesi ve hak kayıplarının önlenebilmesi için önemli ve gereklidir[312].

2016/679 sayılı Tüzük'ün hangi kapsamda uygulanabileceği hususu Tüzük'ün "*Maddi Kapsam (Material Scope)*" başlıklı 2.maddesinin 1.fıkrası kapsamında açıklanmaya çalışılmıştır. Bu maddeye göre, ilgili Tüzük, gerçek kişilere ait kişisel verilerin teknolojik araçlar kullanılarak, kısmen ya da tamamen otomatik olarak işlenmesi faaliyetlerine ve otomatik işleme olmamakla birlikte kişisel verilerin bir dosyalama sisteminin parçasını oluşturacağı veya gelecekte oluşturabileceği nitelikte yapılan manuel işleme faaliyetlerine de, uygulanabilecektir. 2/1.maddenin içeriği incelendiğinde, 2016/679 sayılı Tüzük'ün hangi işlemlere uygulanabileceği hususunun geniş yorumlanması gerektiği anlaşılmaktadır. Bu bağlamda Tüzük'ün uygulamasının, kişisel verilerin işlendiği her türlü faaliyet alanını kapsadığı söylenebilir[313].

Adalet Divanı da, vermiş olduğu pek çok karar kapsamında, kişisel verilerin korunmasına ve serbest dolaşımlarına ilişkin yasa hükümlerinin kapsamlarının geniş yorumlanması gerektiğine işaret etmiştir. "*Lindqvist Kararı*" da yasa kapsamının

---

[311] Paul Voigt, Axel von dem Bussche, **The EU General Data Protection Regulation (GDPR), A Practical Guide**, Springer, 2017, ss.21-22, 26-28;
Mira Burri, Rahel Schar, "The Reform of the EU Data Protection Framework, Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", **Journal of Information Policy**, Cilt.6, 2016, ss.495-496.

[312] Bird & Bird, **Guide to the General Data Protection Regulation**, 2017, https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en (02.06.2020) s.1.

[313] Paul Voigt, Axel von dem Bussche, ss.9-10.

geniş yorumlanması gerektiğine ilişkin verilen kararlara örnek gösterilebilir. Bu kararda, yasa hükümleri geniş yorumlanarak, işleme faaliyeti, tamamen hayırseverlik ve gönüllülük esasına göre yapılmış olsa da, kişisel verilerin bir web sitesine yüklenmesi faaliyeti dahi tek başına kişisel verilerin otomatik olarak işlenmesi kapsamında kabul edilerek, bu durumda yasada belirtilen istisnalardan faydalanılamayacağına hükmedilmiştir[314].

Kişisel verilerin korunmasına ve serbest dolaşımlarının sağlanmasına yönelik olarak Tüzük de, tıpkı kendisinden önceki mülga 95/46 sayılı Direktif gibi, orantılılık ilkesi çerçevesinde korunmaları hedeflenen diğer temel haklarla, kişisel verilerin korunması arasındaki hassas ve adil dengenin bozulmamasının gerekliliği bağlamında, Tüzük'ün uygulanabilirliği bakımından bazı istisnalar getirmiştir[315]. Bu istisnalar, Tüzük'ün "*Maddi kapsam (Material Scope)*" başlıklı, madde 2/2 (a) (b) ve (d) kapsamında açıklanmaya çalışılmıştır. Buna göre, işbu Tüzük hükümleri, yetkili otoriteler tarafından kamu güvenliğine yönelik tehditlerle mücadele edilmesi, kamu güvenliğinin korunması, suçun önlenmesi, soruşturulması, tespit edilmesi, kovuşturulması, cezaların infazı, yargı bağımsızlığı ve adli süreçlerin korunması gibi üye devletlerin egemenlik alanında kalan ve Birlik hukuku kapsamına girmeyen konular ile, Birlik'in ortak dış ve güvenlik politikaları kapsamındaki veri işlemelerine uygulanmayacaktır[316]. Bu istisnaların yanı sıra, Birlik'in ya da üye devletlerin önemli ekonomik ya da mali çıkarlarının, sosyal güvenlik sistemlerinin, mesleki etik kurallarının korunması amacıyla; Bütçe veya vergilendirmeye ilişkin konular ile; Veri sahibinin ya da bir başkasının temel hak ve özgürlüklerinin korunması gereğinin zorunlu kıldığı hallerde; Medeni hukuktan kaynaklanan kararların icrasının gerekli kıldığı durumlarda, üye devletlerin, Tüzük madde 23 kapsamında kişisel verilere ilişkin yapacakları yasal düzenlemelerle, bu konularda istisnai kısıtlamalar getirebilecekleri de hüküm altına alınmıştır. Ancak hemen şunu da belirtmek gerekir ki, bu kısıtlamalar, temel bir hak olan kişisel verilerin

[314] Lindqvist kararı, bu tez çalışmasının "*2.2.1.1. Hassas Kişisel Veriler*" başlıklı kısmında daha detaylı olarak ele alınmıştır.
Judgment of the Court of Justice of the European Union, **ECJ C-101/01**, Criminal Proceedings Against Bodil Lindqvist;
Laraine Laudati, s.6.
[315] Bird & Bird, **Guide to the General Data Protection Regulation**, s.3.
[316] GDPR Beyanlar 16, 19.

korunması hakkının özüne dokunmayacak ve verilerin serbest dolaşımlarını aksatmayacak bir şekilde, yine orantılılık ilkesi çerçevesinde yapılmalıdırlar.

Tüzük madde 2/2 (c) kapsamında da Tüzük'ün, ayrıca kişisel verilerin gerçek bir kişi tarafından mesleki veya ticari bir faaliyetle herhangi bir bağı olmayacak şekilde, tamamen kişisel ya da hane halkına ilişkin olarak işlenmesi durumlarında da uygulanmayacağı belirtilmiştir[317].

Madde 2/2 (c)'deki "*kişisel ve hane halkına ilişkin olma*" ibaresi, sınırlı sayıda kişinin erişebileceği nitelikteki, yazışmalar ile adres defterlerini içerebildiği gibi, somut olayın özelliklerine göre ticari bir anlam taşımayan ve sosyalleşme amacıyla, yapılan sosyal medya aktiviteleri ile diğer çevirimiçi faaliyetleri de kapsayabilmektedir. Tüzük'ün 2/2 (c) maddesinin yanı sıra, mülga 95/46 sayılı Direktif madde 3/2'de de düzenlenen "*Kişisel ve hane halkına ilişkin olma*" ibaresinin, ilgili madde hükmünün kastını aşmayacak şekilde dar yorumlanmasının gereği, Avrupa Adalet Divanı tarafından verilen pek çok karar kapsamında belirtilmiştir.

Somut olayda, kişisel ve hane halkına ilişkin olma kavramının yorumlanması açısından, "*Rynes v. Urad*[318]" vakası kapsamında verilen karar önemlidir. Bu vakada, bir kaç kere saldırıya uğrayarak, konut dokunulmazlığı ihlal edilen evinin güvenliğinin, hane halkının sağlığının ve hayatının korunmasının sağlanması amacıyla, Bay Rynes tarafından, evinin dışında kalan girişinin, giriş yolunun ve komşusunun evinin girişinin bulunduğu yöndeki kamuya açık alanları da görecek şekilde güvenlik kameraları döşenmiş olduğu anlaşılmıştır. Ekim 2007 tarihinde Bay Rynes'in konutuna yapılan bir başka saldırı sırasında bu kameraların yaptığı kayıtların polis tarafından incelenmesiyle de Bay Rynes'ın evine saldıran kişilerin kimlik tespitleri yapılmış ve bu kişiler yakalanmıştır. Kimliği tespit edilen bu kişilerden birinin kişisel verilerinin ihlal edildiğine ilişkin şikayeti üzerine, Çek Cumhuriyeti Kişisel Verileri Koruma Ofisi, izinsiz yapılan kaydı, 95/46 sayılı Direktif kapsamında yasadışı bularak, Bay Rynes'e ceza vermiştir. Verilen bu ceza üzerine Bay Rynes, döşemiş olduğu güvenlik kameraları vasıtasıyla, ilgili kişilerin

[317] GDPR Beyanlar (18).
[318] Judgment of the Court of Justice (Fourth Chamber), Rynes v. Urad Case, 11 December 2014, **ECJ C-212/13**, http://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=EN (02.06.2020).

kişisel verilerinin ihlal edilip edilmediğinin ve bu görüntülerin –o dönemde yürürlükte bulunan- 95/46 sayılı Direktifin 3. maddesinin 2.fıkrasında geçen "*Kişisel ve hane halkına ilişkin olma*" istisnasının kapsamına dahil olup olmadığının tespiti amacıyla, üst mahkemeye başvurmuştur. Üst mahkeme tarafından bu durum ön karar prosedürü ile Adalet Divanı'na taşınmıştır. Adalet Divanı, konuya ilişkin verdiği kararında, güvenlik kameralarının, evin dışarısında kalan kamusal alanların görüntülerini sürekli olarak kaydederek otomatik bir şekilde depoladıklarını tespit etmiştir. Kamusal alana ilişkin depolanan bu görüntülerin ise, 95/46 sayılı Kişisel Verilerin Korunması Direktifinin koruma alanına girdiği belirtilmiştir. Bu sebeple, kamusal alanları da içeren görüntülerin, madde 3/2'deki muafiyetin kapsamına girmediğinin ve *"Kişisel ve hane halkına ilişkin olma"* ibaresinin de dar yorumlanması gerektiğinin altı Adalet Divanı tarafından bu kararla net bir şekilde çizilmiştir[319].

Tüm bu düzenlemelerin yanı sıra, Tüzük'ün maddi kapsamının sınırlarına ilişkin son bir noktanın daha altını çizmekte fayda vardır. Giriş 26.paragrafında da belirtildiği gibi, işbu Tüzük hükümleri belirli ya da belirlenebilir bir veri süjesine ait olmayan veriler ile yapılan anonimleştirme işlemi sebebiyle artık ilgili veri süjesinin belirlenebilmesi imkanı kalmayan anonimleştirilmiş bilgilere uygulanamayacaktır[320].

3.5.2. Kişisel Verilerin İşlenmesine Yönelik Yeni Teknik ve Yöntemler

2016/679 sayılı Tüzük, mahremiyetin ve veri güvenliğinin tarihte belki de hiç olmadığı kadar kırılgan hale geldiği içinde bulunduğumuz dijital çağda, kişisel verilerin en üst seviyede korunabilmesi amacıyla bazı yeni teknik ve yöntemler ortaya koymuştur. Bunlardan en önemlilerinden biri de ilgili Tüzük madde 25 kapsamında açıklanan "*Tasarımla Veri Koruma*" ve "*Varsayılan Ayarlarla Veri Koruma*" şeklinde dilimize kazandırılmış olan "*Privacy by Design*" ile "*Privacy by Default*" ilkeleridir[321].

[319] Judgment of the Court of Justice (Fourth Chamber), Rynes v. Urad Case, **ECJ C-212/13.**
[320] Gerald Spindler, Philipp Schmechel, "Personal Data and Encryption in the European General Data Protection Regulation", **Journal of Intellectual Property, Information Technology and E-Commerce Law**, Cilt.7, Sayı.2, 2016, s.170.
[321] Nilgün Başalp, 2015, s.92.

Tasarımla Veri Koruma İlkesi (Privacy by design), iş yapma süreçleri ve işletim sistemleri içerisindeki veri işleme faaliyetleri kapsamında, kişisel verilerin, etkin ve etkili bir şekilde korunabilmelerinin sağlanması amacıyla, bu sistem ve süreçler henüz tasarım aşamasındayken, öngörülebilir risklere karşı, mahremiyeti güçlendirici teknik ve idari tedbirlerin alınmasını ifade eder. Teknolojik ilerlemelerle birlikte kişisel veri güvenliğine ilişkin tehdit ve ihlallerin artması sebebiyle, siber güvenliği sağlamanın gereğinin her geçen gün daha fazla hissedildiği günümüz dünyasında, tasarımla veri koruma (Privacy by design) ilkesi de gün geçtikçe daha önemli hale gelmektedir. Başka bir deyişle, yaşanan teknik ilerlemelere ve internet kullanımının artmasına paralel olarak popülerliği artan privacy by design ilkesi, kişisel verilerin korunması bağlamında oluşturulacak sistemsel bütünlük içerisinde ve bu sistem henüz tasarım aşamasındayken, reaktif değil, proaktif davranarak, olası risklerin ve güvenlik ihlallerinin gerçekleşmesinden önce bunların tahmin edilerek önlemler alınmasını ifade eden önleyici nitelikteki teknik ve idari tedbirler bütünü olarak da tanımlanabilir[322].

Varsayılan Ayarlarla Veri Koruma İlkesi (Privacy by default) ise, tasarlanan iş yapma süreçleri kapsamında yapılacak veri işleme faaliyetlerinin, yalnızca ilk başta belirlenerek veri süjesine bildirilen toplanma amacıyla sınırlı olarak yapılmasını sağlayacak nitelikteki mahremiyet dostu teknik mekanizmaların oluşturularak, bu uğurda gereken önlemlerin alınmasını ifade eder. Varsayılan Ayarlarla Veri Koruma (Privacy by default) ilkesinin, kişisel verilerin korunmasında göz önüne alınması gereken "*Veri Minimizasyonu*" ve "*Amaç ile Sınırlılık*" temel ilkeleri ile doğrudan bağlantılı olduğundan ve bu bağlamda da kişisel veriler üzerinde veri süjesinin kontrolünün artırılmasına katkıda bulunduğundan şüphe yoktur[323].

---

[322] Ann Cavoukian, "Privacy by Design, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf (02.06.2020), ss. 2-4; Ann Cavoukian, "Privacy by Design: the Definitive Workshop. A Foreword by Ann Cavoukian", **Identity in the Information Society (IDIS) 3**, 2010, ss.247-249; European Data Protection Supervisor, "Dissemination and Use of Intrusive Surveillance Technologies", **Opinion 8/2015**, https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf (02.06.2020), ss.9-10.

[323] Amaya Noain Sanchez, "'Privacy by default' and active 'informed consent' by layers: Essential measures to protect ICT users' privacy", **Journal of Information, Communication and Ethics in Society**, Cilt. 14, Sayı. 2, 2016, ss. 124, 129-130; Information Commissioner's Office, UK **(ICO),** "Data Protection by Design and Default", https://ico.org.uk/for-organisations/guide-to-data-

2016/679 sayılı Tüzük ile getirilen Tasarımla Veri Koruma (privacy by design) ve Varsayılan Ayarlarla Veri Koruma (privacy by default) ilkelerinin özümsenmesi yoluyla geliştirilecek mahremiyet dostu teknik çözümler, iş yapma süreçleri, işletim sistemleri, iş modelleri ve şirket yapılanmaları vasıtasıyla, ortaya "*veri koruma dostu ürün ve hizmetler*" koyularak, dijital tek pazardan yararlanabilme oranının artırılabilecektir[324].

2016/679 sayılı Tüzük'ün 25.maddesi kapsamında, gerek Tasarımla Veri Koruma, gerekse de Varsayılan Ayarlarla Veri Koruma ilkeleri ile, veri kontrolörlerine kişisel verilerin korunması bağlamında oluşturacakları mekanizmalar ve kullanacakları yöntemler açısından önemli görev ve sorumluluklar yüklenmiştir. Bu ilkeler vasıtasıyla, kişisel verilerin, hem tasarım aşamasından itibaren alınacak önleyici tedbirler kapsamında oluşturulacak sistemler aracılığıyla güven içinde işlenmesi, hem de amaçla sınırlı olma hususunda gereken hassasiyetin gösterilmesi garanti altına alınmaya çalışılmıştır. Alınacak bu tedbirlerle de Avrupa dijital tek pazarına duyulan güvenin yükseltilip, dijital işlemler bağlamındaki güvensizlik bariyerinin kaldırılarak, yapılacak işlem sayı ve çeşitliliğinin artırılması ve dijital ekonominin güçlendirilmesine katkı sağlanması hedeflenmiştir[325].

Kişisel verilerin korunmasında kullanılan bir diğer yöntem de, Tüzük'ün getirdiği önemli değişikliklerden biri olan "*Rumuz*" yahut "*takma ad kullanımı*" olarak da isimlendirilen "*pseudonymisation*"dur. Takma ad kullanımı (pseudonymisation), Tüzük'ün 4/5.maddesinde tanımlanmıştır. Buna göre, "*takma ad kullanımı (pseudonymisation)*", kişisel verilerin, ayrı tutulan ve özel teknik ve örgütsel tedbirlerle korunan ek bilgiler olmadan, veri süjesinin kim olduğunun tespit edilemeyeceği şekilde işlenmesi anlamına gelir. Bu yöntemde, veri süjesinin kimliğinin tespitinde kullanılabilecek nitelikteki veriler, işlenen verilerden ayrı bir

---

protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (02.06.2020).

[324] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, "Europa Union, Privacy and Data Protection by Design from Policy to Engineering", **ENISA**, December 2014, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (02.06.2020), ss.iii, iv, 55-58.

[325] Sandra Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR", **Computer Law and Security Review**, Cilt.34, Sayı.3, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083554&download=yes (02.06.2020) ss. 17-21.

yerde tutulup, bunların yerlerine çeşitli kod ve sayılar kullanılır. Böylelikle, işlenen kişisel verilerin gerçekte kime ait olduğunun tespiti engellenerek, mahremiyetin korunması garanti altına alınmaya çalışılmaktadır. Takma ad kullanımı (pseudonymisation) yöntemiyle işlenen veriler, kişisel veri olma özelliklerini yitirmeseler de, ayrı bir yerde saklanarak özel tekniklerle korunan ek bilgiler olmadan bu verilerin ait oldukları veri süjelerinin kimler oldukları tespit edilememektedir[326].

Tüzük kapsamında işlenecek kişisel verilerin güvenliğinin, özellikle bulut bilişim gibi ileri teknoloji sistemleri dahilinde gerçekleşebilecek güvenlik ihlal ve zaafları karşısında, en üst seviyede sağlanarak, korunabilmesi için kullanılabilecek teknik uygulamalardan bir diğeri de "*Şifreleme (Encryption)*" yöntemidir. Bir veri güvenliği yöntemi olan şifreleme ile, kişisel verilerin kime ait olduğuna ilişkin belirleyici olabilecek veri ve bilgilerin, gizli bir algoritma, kod veya kripto anahtarı kullanılarak gizlenmesi yoluna gidilerek, erişime yetkili olmayan herhangi bir kimsenin anlayamayacağı hale getirilen verilerin, mahremiyetlerinin korunması hedeflenmektedir. 2016/679 sayılı Tüzük, şifreleme (encryption) yöntemine ilişkin açık bir tanımlama getirmemekle birlikte, veri güvenliğinin ve işlemenin yasallığının sağlanabilmesi bağlamında, çeşitli maddeler kapsamında bu yöntemin kullanılmasının gereğini işaret etmektedir[327]. Şifreleme yöntemi de, kişisel verilere yetkisiz erişimin engellemesi bağlamında, veri güvenliğinin artırılmasına katkı sağlayacağından, tüketici güvenini artırarak, Avrupa dijital tek pazarının gelişimine katkıda bulunması beklenmektedir.

3.5.3. Veri Süjesinin Rızası

2016/679 sayılı Genel Veri Koruma Tüzüğü'ne göre, veri süjesinin rızasının bulunmasının, kişisel verilerin meşru bir şekilde işlenebilmesi için gerekli hukuka uygunluk sebeplerinden biri olduğundan daha önceki bölümlerde bahsedilmişti.

[326] Samson Yoseph Esayas, "The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the 'All or Nothing' " **Approach, European Journal of Law and Technology**, Cilt.6, Sayı.2, 2015, (02.06.2020), ss.4, 8.
[327] GDPR Beyanlar (83); Gerald Spindler, Philipp Schmechel, ss.169-171; Steve Mansfield-Devine, "Meeting the Needs of GDPR with Encryption", **Computer Fraud and Security**, Cilt.2017, Sayı 9, https://www.sciencedirect.com/science/article/pii/S136-1372317301008 (02.06.2020), ss. 18-19.

Kişisel verilerin korunmasına ilişkin olan mülga 95/46 sayılı Direktif ile karşılaştırıldığında, işbu Tüzük ile veri süjesinin rızasının usulüne uygun olarak alınmasına ilişkin olarak daha fazla koşul getirildiği görülmektedir[328].

Rızanın alınması ve kullanılmasına ilişkin bu koşul ve kısıtlamalara geçmeden önce, veri süjesinin rızasının Tüzük kapsamındaki tanımına göz atmakta fayda vardır. "*Rıza*" tanımı, ilgili Tüzük'ün 4/11.maddesi kapsamında yapılmıştır. Bu tanıma göre, öncelikle veri süjesinin, belirli bir amaçla yapılacak işleme faaliyetine ilişkin, bu amaç ve kapsamı net bir şekilde ortaya koyan, açık, sade ve anlaşılır bir dille bilgilendirilmesi gerekmektedir. Bu bilgilendirmeye müteakip, veri süjesi, hiçbir baskı altında kalmadan serbest iradesi ile; bu belirgin amaca yönelik özel olarak ve kesin bir dille vereceği, bir beyan ya da tereddütte yer vermeyecek şekilde açık ve olumlu bir eylem vasıtası ile kişisel verilerinin işlenmesine ilişkin onay verebilir. Bu veri süjesinin serbest iradesini yansıtan, "*beyan veya onay eylemi*", Tüzük kapsamında "*rıza*" olarak tanımlanmıştır.

Veri süjesinin rızasının, işleme faaliyetine geçmeden önce, veri süjesinin, işbu işlemenin amaç, kapsam ve niteliğine ilişkin bilgilendirilmesine müteakip, alınması gerektiği unutulmamalıdır. Zira veri süjesinin bilgilendirilmesi hususu, 2016/679 sayılı Tüzük'e göre, rızanın usulüne uygun verilebilmesinin esaslı unsuru niteliğindedir. Diğer bir ifade ile, rızanın, veri süjesinin serbest iradesini yansıtabilmesinin bir koşulu da, veri süjesinin kişisel verilerinin hangi amaç ve kapsamda işleneceği ve bu işlemeye ilişkin haklarının neler olduğuyla ilgili bilgilendirilmesidir. Ayrıca rızanın geçerli sayılabilmesi için de bilgilendirmenin, en azından, "*veri kontrolörünün kimlik bilgileri; işlemenin ne amaçla yapılacağı; veri süjesine ilişkin olarak ne çeşit verilerin toplanıp kullanılacağı; veri süjesinin rızasını geri çekme hakkının bulunduğu; ilgili verilerin ne çeşit otomatik karar verme işlemlerinde kullanılacağı; yapılacak veri transferi faaliyetlerine ilişkin olası risklerin neler olduğu*" bilgilerini içermesi gerekmektedir. Tüzük'ün Giriş (32) sayılı paragrafına göre, kişisel verilerin işlenmesine ilişkin gerekli bilgilendirmeler yapıldıktan sonra ve fakat veri işleme faaliyetinden önce talep edilmesi gereken rıza,

[328] Fatema, Kaniz, Ensar Hadziselimovic, Harshvardhan Pandit, Christophe Debruyne, Dave Lewis, Declan O'Sullivan, "Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model", Adapt Center, Trinity College, Dublin, http://www.tara.tcd.ie/bitstream/handle/2262/82659/88248c5b669175f267069c3319d9ac2d3e84.pdf?sequence=1 (02.06.2020), ss.1-2.

yazılı şekilde verilebileceği gibi, sözlü olarak da verilebilmektedir. Ancak yazılı beyanın ispat kolaylığı sağlayacağı da unutulmaması gereken bir husustur. Rıza, ayrıca, "*bir web sitesi ziyareti sırasında onay kutucuğunun işaretlenmesi*" veya "*bir bilgi toplumu hizmeti sunulması esnasında teknik ayarların kullanılması*" şeklinde de yapılabilen açık ve olumlu bir eylemde bulunulması vasıtasıyla elektronik ortamda da verilebilir. Ancak veri süjesinin, bu bağlamda sessiz ya da hareketsiz kalmasının ya da önceden işaretlenmiş kutucukların bulunmasının, işbu Tüzük dahilinde hiçbir şekilde rıza beyanı olarak kabul edilemeyeceğinin de altı yine Tüzük'ün 32.paragrafı kapsamında çizilmiştir. Özellikle elektronik ortamda veri süjesine yönlendirilen rıza talebinin açık olması, kısa ve öz bilgiler içermesi ve kullanılacak hizmet bağlamında veri süjesini gereksiz yere rahatsız ederek, zorlayacak nitelikte bulunmaması da gerekmektedir. Yine rızanın, yapılması planlanan işleme faaliyetlerine ilişkin tüm amaçları açık bir şekilde kapsar nitelikte olması da önemlidir[329].

Rızanın 2016/679 sayılı Tüzük kapsamında geçerli kabul edilebilmesi için, veri işleme faaliyetinin başlamasından önce, açık, kesin ve olumlu bir beyan ya da eylem vasıtasıyla verilmesi gerektiğinden, veri süjesinin rızasını vermekten vazgeçme eyleminin herhangi bir şekilde geçersiz sayılması sureti ile rızanın alınmış varsayılması da mümkün değildir[330].

Avrupa Adalet Divanı da, 1 Ekim 2019 tarihli bir kararında, kişisel verilerin korunması bağlamında, veri süjesinin rızasının, önceden işaretlenmiş kutucuklarla alınmasının, 2016/679 sayılı Tüzük kapsamında yasal kabul edilemeyeceğinin altını net bir şekilde çizmiştir. Bu olay, bir çevirimiçi bahis şirketi olan Planet49 ile Alman Tüketici Dernekleri Federasyonu arasındaki bir dava kapsamında önkarar verilmesine ilişkin olarak Adalet Divanı'nın önüne gelmiştir. Davanın konusu, Planet49 Şirketi'nin, yapmış olduğu çevirimiçi bir çekilişe katılabilmeleri için kullanıcıların, kişisel verilerinin, –sayıları elliyi aşkın bulunan- partner ve sponsorlarına transferlerine; bu verilerin depolanmalarına; ve, kullanıcıların laptop, cep telefonu gibi kişisel cihazlarında depolanan bu verilere erişime ilişkin rızalarının

[329] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679, Adopted on 28.11.2017", **WP259rev.01**, as last revised and adopted on 10.04.2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (02.06.2020), ss.12-15.
[330] Eugenia Politou, Efthimios Alepis, Constantinos Patsakis, "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions", **Journal of Cyber Security**, Cilt.4, Sayı.1, 2018, ss.6-7.

alınmasıyla ilgilidir. Açıklamak gerekirse, bu çekilişe katılabilmeleri için kullanıcıların önüne, Planet49 tarafından, iki farklı onay kutucuğu çıkarılmıştır. Bu kutucuklardan ilki, kullanıcıların kendilerine, Planet49'un partner ve sponsorlarından, posta, telefon, kısa mesaj ya da e-posta yoluyla, reklam gönderilmesine, kullanıcıların rıza göstermesine ilişkindir. Bu ilk kutucuk önceden işaretlenmemiştir ve verilecek bu rızanın herhangi bir zamanda geri alınabileceği ifadesini de içermektedir. İkinci kutucuk ise, çevirimiçi hareketlerinin izlenmesine ilişkin olarak bazı analiz tekniklerinin kullanılmasına, verilerinin saklanmasına ya da üçüncü kişilerin işbu verilere erişimine izni verilmesine kullanıcıların, önceden işaretlenmiş kutucuk vasıtasıyla, rıza göstermesine ilişkindir. Yapılan yargılama sonucu, Avrupa Adalet Divanı, vermiş olduğu kararında, önceden işaretlenmiş kutucuklar vasıtasıyla alınan kullanıcı rızalarının, kişisel verilerin işlenmesi kapsamında geçerli kabul edilemeyeceğine hükmetmiştir[331]. Aynı dava kapsamında, Hakim Szpunar, 2016/679 sayılı Tüzük'te geçen kullanıcı rızasının nasıl yorumlanması gerektiğine ilişkin görüşünü de açıklamıştır. Bu görüşe göre, Tüzük, mülga 95/46 sayılı Direktif ile kıyaslandığında, kişisel verilerin işlenmesi ve veri transferine ilişkin olarak veri süjesinden alınması gereken rızaya ilişkin koşulları sertleştirmiştir. Ayrıca Hakim Szpunar, önceden işaretlenmiş kutucukların veya kullanıcının sessiz ve hareketsiz kalması da dahil diğer her türlü pasif davranışlarının, veri süjesinin kişisel verilerinin işlenmesine ilişkin rıza gösterdiği şeklinde yorumlanamayacağının da altını çizmiştir[332].

Tüzük'ün Giriş (42) sayılı paragrafında, kişisel verilerin işlenmesinin veri süjesinin rızasına bağlı olduğu hallerde, rızanın bulunduğunu ispat yükünün, veri kontrolörüne ait olduğu belirtilmiştir. Aynı paragraf kapsamında, veri kontrolörü tarafından önceden hazırlanmış rıza beyanlarının, açık, sade ve kolay anlaşılır bir dille kaleme alınması; adil olmayan koşullar içermemesi ve bu beyanlara veri süjesi tarafından kolay erişilebilmesinin gerekli olduğu da belirtilmiştir. Ayrıca, yine

---

[331] Judgement of the Court of Justice of the European Union (Grand Chamber), **ECJ C-801**, 1.10.2019, German Federation of Consumer Organisations v. Planet49 GmbH, http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8867771 (02.06.2020).

[332] Opinion of Advocate General Szpunar delivered on 21 March 2019, **Case c-673/17**, Planet49 GmbH v. German Federation of Consumer Organisations, http://curia.europa.eu/juris/document/-document.jsf?text=&docid=212023&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8867771 (02.06.2020).

paragraf 42'ye göre, veri süjesinin rızası, hür iradesiyle yaptığı bir seçime dayanmıyorsa ya da bir zarara uğramadan rıza vermeyi reddetme veya rızasını geri çekme hakkı bulunmuyorsa, bir başka ifade ile, rıza vermenin reddedilmesi ya da rızanın geri çekilmesi halinde hizmet alınamaması veya aynı kapsam ve kalitede hizmete erişilememesi durumu ortaya çıkıyorsa, bu hallerde de rıza serbest irade ile verilmiş sayılamayacaktır.

Rıza, veri süjesinin bireysel özgürlüğünün ve bilginin geleceğini belirleyebilme hakkının bir dışa vurumu olarak da nitelendirilebilir. Tüzük'ün Giriş (43) sayılı paragrafında, somut olay kapsamında, veri süjesi ile veri kontrolörü arasında, veri süjesi aleyhine açık bir güç dengesizliğinin bulunduğu hallerde, veri süjesinin bireysel özgürlüğünün baskı altında olabileceği hususu da göz önüne alınarak, verilecek rızanın niteliği açıklanmıştır. Buna göre, veri süjesi aleyhine açık bir güç dengesizliğinin bulunduğu ve özellikle de veri kontrolörünün bir kamu otoritesi olduğu hallerde, verilen rıza, somut olayın özelliklerine göre, kişisel verilerin yasal olarak işlenebilmesi için gereken geçerli rıza kapsamında addedilemeyebilecektir. Aynı paragrafta, birbirlerinden ayrı rızaya dayanması gereken, farklı kişisel veri işleme faaliyetlerine zorunlu olarak, tek seferde rıza verilmesi şeklinde düzenlenen işlemler neticesinde alınan rızanın da serbestçe verilmiş geçerli bir rıza sayılamayacağının da altı çizilmiştir[333].

Tüzük madde 7/1 kapsamında, geçerli bir rızaya dayanması gereken veri işleme faaliyetinin söz konusu olduğu durumlarda, veri süjesinin bu işlemeye ilişkin rızasının bulunduğunu ispat yükünün, veri kontrolörüne ait olduğunun altı net olarak bir kere daha çizilmiştir.

Tüzük madde 7/2 kapsamında, veri süjesinin rızasının, başka hususların da yer aldığı yazılı bir beyan kapsamında verildiği durumlarda, rıza talebinin, açık ve sade bir dil içeren, kolay erişilebilir bir formda ve diğer hususlardan açıkça ayırt edilebilir bir şekilde yazılması gerektiği hüküm altına alınmıştır. Böyle bir yazılı beyanın, Tüzük hükümlerini ihlal eden maddeler içermesi halinde ise, ihlal içeren bu kısımların bağlayıcı olmayacağının da altı önemle çizilmiştir.

Tüzük madde 7/3 kapsamında, veri süjesinin kişisel verilerinin işlenmesine ilişkin olarak verdiği rızasını her zaman geri çekme hakkına sahip olduğu

[333] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679, Adopted on 28.11.2017", **WP259rev.01**, as last revised and adopted on 10.04.2018, ss. 2, 5-6.

belirtilmiştir. Ayrıca aynı maddede, rızanın geri çekilmesinin, bu eylemden önce ilgilinin usulüne uygun olarak verilmiş rızası kapsamında halihazırda yapılmış olan veri işleme faaliyetlerinin yasallığını etkilemeyeceği de belirtilmiştir. Burada önemli olan husus, veri süjesinin rızasını vermesinden önce veri işleme faaliyetinin amaç ve kapsamına ilişkin usulüne uygun olarak bilgilendirilmiş olmasıdır. Ancak, rızanın geçerlilik koşullarına uygun alınmış sayılabilmesi için, verilmesi kadar geri çekilmesinin de kolaylıkla yapılabilir olması gerekmektedir. Veri süjesinin rızasını geri çekme hakkının yanı sıra, rızasının kapsamını herhangi bir zamanda güncelleyerek, içeriğini değiştirme hakkının da bulunduğunu söylemek yanlış olmayacaktır. Güncelleme veri süjesi tarafından kendiliğinden yapılabileceği gibi, işlemenin kapsam ve niteliğinin değişmesine müteakip, veri kontrolörü tarafından da talep edilebilir[334].

Tüzük madde 7/4'e göre, veri süjesinin rızasının serbestçe verilip verilmediğinin tespitinde, göz önüne alınması gereken bir diğer husus da, kişisel verilerin işlenmesine ilişkin alınan rızanın, veri süjesine bir hizmet sunulmasını da kapsayabilen bir sözleşmenin ifası bakımından alınırken, rıza alınan hangi işleme faaliyetlerinin bu sözleşmenin ifası için gerçekten gerekli, hangilerinin gereksiz olduğunun tespitidir. Zira ilgili sözleşmenin ifa edilebilmesi için gerekli olmayan bir veri işleme faaliyetine, sözleşme kapsamında alınan rıza, serbestçe verilmiş rıza kapsamından çıkabileceğinden, böyle bir rıza ile yapılan işleme faaliyeti de, somut olayın özelliklerine göre, meşruiyetini kaybederek, yasal işleme kapsamında sayılamayabilecektir. Tüzük madde 7/4 çerçevesinde engellenmeye çalışılan bu durum, literatürde kimi yazarlar tarafından "*paketleme (bundling)*" olarak ifade edilmektedir. Paketleme (bundling), bir sözleşme kapsamında kişisel verilerinin işlenmesi amacıyla veri süjesinin rızasının alınması için hazırlanan metne, bu sözleşmenin ifası için gerekli olmayan başka amaçların da eklenerek, bunlar açısından da veri süjesinin rızasını vermeye zorlanması olarak da tanımlanabilir[335]. Eğitim hizmeti alınmasına ilişkin imzalanan hizmet sözleşmesi kapsamında, veri süjesinin kişisel verilerinin aynı zamanda reklam faaliyetlerine ilişkin olarak da işlenmesini kapsayan rızasının alınması hali bu duruma örnek gösterilebilinir.

---

[334] Kaniz Fatema ve diğerleri, s.4.

[335] Bojana Kostic, Emmanuel Vargas Penagos, "The Freely Given Consent and the "Bundling" Provision under the GDPR", **Computerrecht,** Cilt.4, sayı.153, 2017 ss.217-218.

Kişisel verilerin işlenmesine ilişkin veri süjesinin rızasının geçerli bir şekilde alınabilmesini etkileyen anılan koşullara uyularak, gerektiğinde veri süjesi tarafından rızanın geri çekilebilmesi, güncellenebilmesi gibi değişikliklerin kolaylıkla yapılabildiği, veri süjesini bilgilendirme koşullarına uyulduğu, "*kullanıcı dostu bir sistem*" oluşturulması, Avrupa Birliği'nin Avrupa dijital tek pazarının geliştirilmesi hedefi doğrultusunda önemlidir. Ayrıca, işleme faaliyetleri kapsamında geçerli rızanın bulunması sürecinin sağlıklı bir şekilde yönetilmesi, aksi hallerde ortaya çıkabilecek ihlaller sebebi ile, herhangi bir yaptırıma uğranılmaması, maddi-manevi tazminat talepleri ile karşılaşılmaması, maliyetlerin düşürülmesi, tüketiciler gözünde ticari itibarın zedelenmemesi, işlerin aksamadan yürütülerek verimliliğin artırılması gibi hususlarda da özellikle işletmeler bakımından büyük önem taşımaktadır[336].

3.5.3.1. Çocuklara İlişkin Kişisel Verilerin İşlenme Koşulları

Çocukların bilgisayarlar, tablet, telefon gibi diğer akıllı cihazlar vasıtasıyla internet kullanım oranları, yapılan araştırmalara göre, Birlik genelinde ortalama %75 seviyelerine erişmiştir[337]. Teknoloji ilerledikçe, tüm dünyada olduğu gibi, Avrupa Birliği'nde de her geçen gün daha fazla çocuk, internetin hayatlarımızın ayrılmaz bir parçası haline getirdiği dijital dünyada daha fazla yer alarak, bilgiye erişme, öğrenme, oyun oynama, sosyalleşme, girişimcilik, çeşitli dijital platformlara katılma, yaratıcı olabilme, kendini ifade edebilme, çevirimiçi eğitim gibi imkanlardan yararlanmaktadır. Ancak çocukların dijital ortama katılımlarının artması, anılan imkanların yanı sıra kimi olumsuzluklara da sebebiyet verebilmektedir. Çocukları etkileyebilecek nitelikteki olumsuzluklara örnek olarak, "*Çocuğun kişisel verilerinin üçüncü kişilerin erişimine açık hale gelmesi; Ayrımcılığa ve maddi-manevi suistimale, akran zorbalığına uğrama; Kimlik hırsızlığı, dolandırıcılık, psikolojik ve davranışsal profilleme, konum takibi yapılabilmesi; Çeşitli temel hak ve özgürlükleri ile mahremiyetin ihlali; Gerçek hayattan koparak izole olabilme riski; Yasadışı*

[336] Kaniz Fatema, ve diğerleri, ss.1-2,5;
Eugenia Politou, ve diğerleri, ss. 4-6.
[337] Çocukların internet kullanımı kimi üye devletlerde Birlik ortalamasından daha yüksek oranlardadır. Daha fazla bilgi için bkz. Sonia Livingstone, Leslie Haddon, "EU Kids Online: Final Report, The London School of Economics and Political Science", **EC Safer Internet Plus Programme,** Deliverable D6.5, 2009, ss.1, 5-6.

içeriklere kolay erişim" sayılabilir. Günlük hayatın çok değişik alanlarını kapsayarak, derinleşip çeşitlenen, internet ve dijital teknoloji kullanımı sebebiyle, ortaya çıkan bu tehditler arasında en sık karşılaşılanlardan biri de hiç şüphesiz çocuklara ait kişisel verilerin yasa dışı kullanımı ve suistimalidir. Bu hassas durum, Birlik'i, üzerinde bulunduğumuz kaygan dijital zemin kapsamında, kişisel verilerinin yasadışı kullanımı ve suistimali konularında yetişkinlerden daha kırılgan ve korunmaya muhtaç olduğu şüphe götürmeyen çocuklara ait kişisel verilerin, daha özel tedbir, yasal düzenleme ve politikalar vasıtası ile korunması yükü altına sokmuştur. Bu bilinçle Avrupa Birliği, mülga 95/46 sayılı Direktif kapsamında düzenlenmeyen çocukların rızasının alınmasına ilişkin bu hususu, 2016/679 sayılı Tüzük madde 8 kapsamında ayrı bir başlık altında düzenlemiştir[338]. Diğer bir ifade ile, kişisel verilerin korunması bağlamında çocuklara verilen bu özel önem sebebiyle, yasal işleme ilkesi dahilinde, kişisel verilerinin çocuğa "*bilgi toplumu hizmetleri (Information society services)*" sunulması kapsamında işlenmesine ilişkin çocuğun rızasının geçerli kabul edilebilmesi için, Tüzük'ün 8.maddesi ile bazı özel koşullar getirilmiştir.

Tüzük madde 8'de düzenlenen bu koşullardan ilki, doğrudan çocuğun kendisine sunulan bilgi toplumu hizmetleri kapsamında, rızasının geçerli sayılarak, kişisel verilerinin işlenmesinin yasal işleme ilkesi çerçevesinde gerçekleştiğinin kabul edilebilmesi için, ilgili çocuğun "*en az on altı yaşında*" olması gerektiğidir. Çocuğun on altı yaşından küçük olduğu hallerde ise rızanın yasal ve geçerli sayılabilmesi için, velayet hakkı sahibi tarafından onaylanması veya doğrudan velayet hakkı sahibi tarafından verilmesi gerekmektedir. Ancak üye devletlerin, bu hususta kanunla düzenleme yaparak, on üç yaşından küçük olmamak kaydı ile, ilgili Tüzük'te belirtilenden daha küçük bir yaş haddi de belirleyebilecekleri de yine madde 8/1'de belirtilmiştir. Bu hüküm doğrultusunda, "*on üç yaş*"ın işbu Tüzük kapsamında çocuğun rızasının geçerliliği hususunda, alt eşik olduğu ve on üç yaşından küçük çocukların kişisel verilerinin bilgi toplumu hizmetleri kapsamında

[338] Milda Macenaite, Eleni Kosta, "Consent for Processing Children's Persona Data in the EU: Flowing in the US Footsteps?", **Information and Communication Technology Law**, Cilt.26, Sayı.2, 2017, ss. 146-147; European Commission, "Towards a Safer Use of Internet for Children in the European Union – A Parents' Perspective", Analytical Report, **Flash Eurobarometer Series** 248, The Gallup Organization, 2008, https://ec.europa.eu/commfrontoffice/publicopinion/flash/fl_248_en.pdf , (02.06.2020) ss.5, 30; Sonia Livingstone, Leslie Haddon, ss.1-3, 5-6, 23, 26; Bird & Bird, Guide to the General Data Protection Regulation, s.17.

işlenmesine ilişkin kendilerinin verecekleri rızalarının geçerli olmayacağı sonucuna varılabilmektedir[339]. Üye devletlere Tüzük madde 8/1 kapsamında sağlanan bu kısmi serbesti sebebiyle, çocuğun rızasının geçerli sayılabilmesine ilişkin Birlik düzeyinde, aşağıdaki 2 numaralı tabloda da izlenebilen farklı yaş uygulamalarının ortaya çıktığı görülmektedir. Çocukların kişisel verilerinin korunmasının oldukça hassas bir konu olduğu da göz önüne alındığında, üye devletlerdeki bu farklı uygulamaların, tamamlanmaya çalışılan Avrupa Dijital tek pazarının parçalı yapısını perçinleyerek, Avrupa Birliği'nin yasaların Birlik düzeyinde tamamen uyumlaştırılması hedefine zarar verdiği söylenebilir[340].

Tablo 2: Çocuğun Doğrudan Kendisine Sunulan Bilgi Toplumu Hizmetlerine İlişkin Olarak Vereceği Rızanın Geçerli Olabilmesi için Avrupa Birliği'ne Üye Devletlerin 2016/679 sayılı Tüzük'ü Dikkate Alarak Belirledikleri Yaş Sınırları

YAŞ SINIRLARI	AVRUPA BİRLİĞİ'NE ÜYE DEVLETLER
13	Belçika, Danimarka, Estonya, Finlandiya, Letonya, Malta, Portekiz, İsveç
14	Avusturya, Bulgaristan, İtalya, Litvanya, İspanya
15	Çek Cumhuriyeti, Fransa
16	Hırvatistan, Almanya, Yunanistan, Macaristan, İrlanda, Lüksemburg, Hollanda, Polonya, Romanya, Slovakya, Slovenya

İşbu TABLO 2, Ingrida Milkaite ve Eva Lievens'in kişisel verilerin işlenmesi bağlamında çocukların rızasının alınmasına ilişkin yapmış oldukları, aşağıda bahsi geçen 1.7.2019 tarihli çalışmadan uyarlanarak alıntılanmıştır[341].

[339] Bird & Bird, Guide to the General Data Protection Regulation, ss.5,15-16;
Center for Information Policy Leadership, Hunton & Williams LLP, **GDPR Implementation In Respect of Children's Data and Consent**, 6.03.2018, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf (02.06.2020) ss.4-7.

[340] Bu hususta daha fazla bilgi için bkz. Ingrida Milkaite, Eva Lievens, "The GDPR Child's Age of Consent for Data Processing Across the EU – One Year Later", **Ghent University**, 1.7.2019, https://biblio.ugent.be/publication/8621651/file/8621654.pdf (02.06.2020).

[341] Ingrida Milkaite, Eva Lievens Ingrida Milkaite, Eva Lievens, "The GDPR Child's Age of Consent for Data Processing Across the EU – One Year Later", **Ghent University**, 1.7.2019, https://biblio.ugent.be/publication/8621651/file/8621654.pdf (02.06.2020)

Tüzük madde 8/2'de, veri kontrolörlerinin, somut olayda, kullanılan teknolojiyi de göz önüne alarak, velayet hakkı sahibinin rızasının ya da onayının bulunup bulunmadığının belirlenmesine yönelik olarak makul çabayı göstermekle yükümlü olduklarının da altı çizilmiştir.

Tüzük'ün Giriş bölümünün (38).paragrafında da belirtildiği gibi, çocukların, kişisel verilerinin işlenmesine ilişkin sahip oldukları haklar ve karşı karşıya oldukları riskler ile kişisel verilerle ilgili çeşitli hareketlerinin olası sonuçları hakkında daha az bilgi, öngörü ve farkındalığa sahip oldukları varsayılmaktadır. Bu sebeple de, çocukların, kişisel verilerinin korunması bağlamında, özellikle de bu verilerin pazarlama, kişilik analizi ve kullanıcı profili oluşturma gibi sebeplerle işlenmeleri hallerinde ya da doğrudan çocuğa sunulacak hizmetler kapsamında toplanmaları durumunda, ortaya çıkabilecek çeşitli tehditlere karşı özel hükümlerle korunması önemlidir[342].

Dijital ortamda ortaya çıkabilecek riskler karşısında, çocukların kırılganlığının yetişkinlere kıyasla daha yüksek olduğunun bilinciyle Birlik, Tüzük madde 40/2 (g) kapsamında bir başka düzenlemeye daha yer vermiştir. Bu düzenlemeye göre, veri kontrolörleri, işleyicileri veya diğer ilgililer, çocukların kişisel verilerinin işlenmesi faaliyetlerine ilişkin olarak, gerekli bilgilendirmelerin yapılması ve korumanın sağlanması ile çocuklar üzerinde velayet hakkına sahip olan kişilerden rıza alınması hususlarıyla ilgili olarak, işbu Tüzük doğrultusunda ve Tüzük'ün uygulanmasına katkıda bulunacak şekilde özel "*davranış kuralları (codes of conduct)*" da oluşturabileceklerdir. Ayrıca madde 57/1 (b)'ye göre, Tüzük kapsamında yetkili kılınan kişi ve kurumların, çocukların kişisel verilerinin işlenme ve korunmalarına ilişkin tehditlerin, yasa hükümlerinin ve bu doğrultuda alınabilecek diğer önlemlerin neler olduğunun, toplum tarafından anlaşılmasına yardımcı olarak, farkındalık yaratılmasını sağlayacak tedbirleri almaları da önemlidir. Bu bağlamlarda Tüzük'ün (58).paragrafı kapsamında da belirtildiği gibi, çocuğa yönelik kişisel verilerin işlenmesi faaliyetlerine ilişkin bilgilendirme ve iletişim işlemlerinin, çocuğun kolaylıkla anlayabileceği bir şekilde, açık ve sade bir dille yapılması gerekli

[342] Article 29 Data Protection Working Party, s. 23.

ve önemlidir. Bu şekilde yapılmayan bilgilendirme işlemleri, "*bilgilendirilmeye dayanan rıza*" şeklinde yorumlanamayacaktır[343].

3.5.4. Hassas Kişisel Verilerin İşlenme Koşulları

Doğaları gereği "*hassas*" olarak nitelendirilen ve Tüzük kapsamında çeşitli maddeler altında tanımlanarak, kişisel verilerin özel bir kategorisi olarak kabul edilen "*ırka veya etnik kökene; siyasi fikirlere ve siyasi parti üyeliğine; dini veya felsefi inançlara; ticaret birliği üyelikleri de dahil olmak üzere, dernek, vakıf, sendika üyeliği gibi iş ilişkilerine; adli ya da cezai soruşturma ve kovuşturmaya veyahut mahkumiyete, idari yaptırımlara; işyeri performansına, ekonomik duruma; fiziksel ya da psikolojik sağlık durumuna; biyometrik ve genetik bilgilere ya da cinsel hayat, tercih ve eğilimlerine; konuma ve harekete"* ilişkin veriler, hassas kişisel veriler olarak sınıflandırılırlar[344].

2016/679 sayılı Tüzük'ün 9/1.maddesi kapsamında, hassas kişisel verilerin, nitelikleri gereği, daha özel ve yüksek bir yasal koruma altına alınarak, bu verilerin işlenmelerinin kural olarak yasaklandığının altı çizilmiştir. Kişisel verilerin bu özel kategorisine sağlanan hassas ve özel korumanın nedeni, bu verilerin veri süjesinin, bir ya da daha fazla belirli amaca yönelik olarak işlenebilmesi için vereceği "*açık rızası*" dışında yahut özel olarak verilen bu açık rızanın amacına aykırı olarak işlenerek kullanılmaları halinde, veri sahibinin "*ayrımcılığa uğrama"* ihtimalinin çok yüksek olmasıdır. Diğer bir ifade ile, Birlik hukuku kapsamında hassas kişisel verilere erişimin ve bunların işlenmesinin yasal düzenlemelerle, yasada sayılan istisnalar dışında yasaklanması vasıtasıyla, özellikle dini ve felsefi inanca, siyasi görüşe, ırk, cinsiyet, milliyet ve sağlık durumuna, cinsel eğilimlere ilişkin hassas kişisel verilerin kullanılması sonucu çeşitli şekillerde doğrudan ayrımcılık yapılması ihtimalinin önlenmesi amaçlanmaktadır. Bu sebeple de hassas kişisel verilerin ihlal edilmesinin önlenmesi babında daha yüksek bir koruma ve özen gösterilmesi gerektiği açıktır. Hassas kişisel verilerin kullanılmasıyla yapılan doğrudan ayrımcılığa örnek olarak sağlık verileri, medikal geçmiş ya da hastalık riski gibi verilerin kötüye kullanımı verilebilir. Şöyle ki, belli bir coğrafi bölgede yaşayan

[343] Article 29 Data Protection Working Party, s. 24.
[344] GDPR, Beyanlar 10, 35, 51, 56, 71, 75; Madde 4/13, 9, 14, 15.

insanlarda yüksek sağlık riski bulunması halinde, sigorta şirketlerinin bu bölgenin posta kodundan yola çıkarak burada yaşayan kişilere sigorta yapmamaları; bölgeyi ve bu muhitte yaşayan insanları kara listeye almaları; yahut, sigorta prim uygulamalarında aşırı fiyatlandırma yapmaları halleri, hassas kişisel veriler kullanılarak yapılan doğrudan ayrımcılığa açık örnek teşkil edebilmektedirler. Bu da hassas kişisel verilerin korunmasına özel önem verilmesi gerektiğini kanıtlar niteliktedir[345].

Hassas kişisel verilerin işlenme yasağının istisnaları, Avrupa Birliği Genel Veri Koruma Tüzüğü madde 9/2'de sayılmıştır. Bu madde incelendiğinde hassas kişisel verilerin işlenme yasağı istisnalarının, mülga 95/46 sayılı Direktif ile kıyaslandığında, daha katı bir şekilde düzenlendiği görülebilmektedir. Burada sayılan istisnai hallerden ilki, veri süjesinin hassas kişisel verilerinin işlenmesine ilişkin hiçbir şüpheye yer bırakmayacak şekilde açık ve belirgin rızasının bulunmasıdır. Tüzük madde 9/2 (a)'ya göre, hassas kişisel verilerin işlenmesi yasağının kaldırılamayacağına yönelik Birlik hukuku ya da üye devletlerin ulusal yasaları kapsamında özel bir düzenleme bulunmaması kaydı ile, veri süjesinin, belirli bir ya da daha fazla özel amaca yönelik olarak hassas kişisel verilerinin işlenmesine yönelik açık ve belirgin rızasının bulunması halinde, yalnızca belirlenen bu amaç(lar) doğrultusunda hassas kişisel verileri işlenebilecektir.

Madde 9/2'da belirtilen, hassas kişisel verilerin işlenebileceği diğer istisnai haller ise şunlardır: "*İşe alma, sosyal güvenlik veya iş hukukundan kaynaklanan zorunlu veri işleme faaliyetleri kapsamında; Veri işleme faaliyeti veri süjesinin veya bir diğer kişinin hayati çıkarlarının korunması amacıyla yapılıyorsa ve veri süjesi fiziksel ya da yasal olarak rıza gösterebilecek durumda değil ise; Veri işleme politik, felsefi, dini veya ticari amaçla kurulan bir dernek, vakıf veya kar amacı gütmeyen bir kuruluş tarafından, kendi meşru faaliyetleri kapsamında, üçüncü kişilere açıklanmaması ve işleme faaliyetinin yalnızca ilgili kuruluşun mevcut ve önceki üyelerine veya kuruluşun amaçlarıyla ilgili olarak ilişki kurduğu kişi ya da kişilere ait olması koşuluyla yapılıyorsa; Veri süjesi tarafından bizzat kamuya açık hale*

[345] Indre Zliobaite, Bart Custers, "Using Sensitive Personal Data May be Necessary for Avoiding Discrimination in Data-Driven Decision Modals", **Artificial Intelligence and Law**, Cilt. 24, Sayı 2, 2016, ss. 185,188-189; Tal Z.Zarsky, "Incompatible: The GDPR in the Age of Big Data", **Seton Hall Law Review**, Cilt.47, Sayı 4(2), 2017, ss. 1012-1013.

getirilen verilere ilişkinse; Mahkemelerin yetkileri dahilinde hareket etmeleri veya yasal taleplerin tesisi, uygulanması ya da savunulması durumlarında; İşlemenin, önleyici tıbbi tedbirlerin, teşhis ve tedavinin, sağlık çalışanlarının çalışma kapasitelerinin değerlendirilmesinin, sağlık hizmetlerinin mesleki ve idari anlamda yürütülerek sağlık bakım hizmetlerinin verilmesinin gerekli kıldığı hallerde yapılması durumlarında; Sınırlar ötesi ciddi bir tehditin hasıl olması durumunda, genel kamu sağlığının korunması bağlamında veya kamu sağlığına ilişkin standartları ve güvenliği yükselterek, hizmetlerin ve gerekli tıbbi cihazların aksamadan işlemesinin sağlanmasının gerekli kıldığı hallerde; Temel hakları garanti eden tedbirler alınıp, mesleki etik kurallarına uyulması koşulu ile, genel kamu yararının sağlanmasına, tarihi araştırma ve bilimsel ya da istatistiksel amaçlarla arşivleme yapılmasına yönelik olması halinde", orantılılık ilkesi ile temel hakların ve hakkın özünün korunması ilkelerine uyulması koşuluyla; hassas kişisel verilerin işlenmesi yasağı uygulanmayabilir. Yine 9. maddenin 4. fıkrasında üye devletlerin, yapacakları ulusal yasal düzenlemeler vasıtasıyla, genetik ve biyometrik verilerin ya da sağlık verileri gibi hassas kişisel verilerin işlenmelerine ilişkin olarak başka koşullar getirebileceklerinin altı da çizilmiştir.

Tüzük madde 10'da ise, mahkumiyet kararları ve ceza gerektiren suçlara ilişkin olarak ya da bunlarla ilgili güvenlik tedbirlerinin alınmasının gerekli olduğu hallerde, kişisel verilerin, Tüzük madde 6/1'de hüküm altına alınan yasal işleme koşullarına uygun işlenebilmelerine ilişkin özel bir düzenleme yapılmıştır. Bu düzenlemeye göre, kapsamlı bir şekilde, yalnızca resmi mercilerin denetimi altındaki bir sicilde kayıt altına alınabilen mahkumiyet kararlarına ve ceza gerektiren suçlara ilişkin hassas kişisel veriler, ancak ilgili resmi merciinin denetimi altında veya veri süjesinin hak ve özgürlüklerinin uygun yasal güvencelerle korunduğu hallerde Birlik ya da üye devlet hukuku kapsamında verilen onay dahilinde işlenebileceklerdir.

Hassas kişisel verilerin korunması konusunda unutulmaması gereken bir diğer husus da, kişisel verilerin gelişmiş metotlarla analiz edilmesi neticesinde elde edilebilecek bulgu ve sonuçların, hassas kişisel verilerin ortaya çıkarak bilinir olmasına sebep olabilmesidir. Her geçen gün daha fazla gelişen dijital teknolojilerin ve Big Data'nın kaçınılmaz bir sonucu olarak ortaya çıkan bu durum, kişisel verilerin hassasiyet çeşitlerine göre farklı şekillerde kategorize edilerek, korunmalarına ilişkin,

Birlik hukuku kapsamında, önce mülga 95/46 sayılı Direktif'le, daha sonra ise Tüzük ile, ortaya konulmaya çalışılan ayrımların muğlaklaşmasına sebep olabilmektedir. Bu da hassas kişisel verilerin korunmalarını zorlaştırırken, bu bağlamda veri kontrolörlerine düşen sorumluluğu da artırmaktadır. Anılan sebeplerle, özel kategori olarak zikredilen hassas kişisel verilerin toplanıp, depolanarak işlenmelerinin ya da bir yerden başka bir yere iletilmelerinin yasal düzenlemelere uygun olarak ve güven içinde gerçekleştirilebilmesi için, veri kontrolörlerinin ek koruma önlemleri almaları gerekli ve önemlidir. İnternet üzerinden yapılan alışveriş detaylarından, örneğin eczanelerde yapılan harcamalardan, bireylerin güncel sağlık sorunlarının ortaya çıkmasını sağlayabilecek nitelikteki verilerden olan ve hassas kişisel veri kategorisine giren sağlık verilerine ulaşılabilmesinin mümkün olması, ileri teknolojiler kullanılarak yapılan analiz yöntemleri sonucunda kişisel veri kategorileri arasında yaşanabilen muğlaklaşma sorununa ilişkin olarak gösterilebilecek önemli örneklerden biridir [346].

Yukarıdaki paragrafta bahsi geçen muğlaklaşma sebebi ile, hassas kişisel verilerin yetkisiz üçüncü kişilerin erişimine açık hale gelebilmesi hususu, tüm dünya için olduğu gibi, Avrupa Birliği için de aşılması gereken önemli bir sorundur. Bu sorunun, Avrupa Birliği tarafından yapılacak çeşitli yeni teknik ve yasal düzenlemelerle çözülmeye çalışılması, hassas kişisel verilerin korunması hususundaki tüketici güvenini yükselteceğinden, dolayısı ile, Avrupa dijital tek pazarının işlem hacminin artırılmasına da olumlu katkıda bulunacağına şüphe yoktur.

3.5.5. Veri Süjesinin Hakları

Avrupa Birliği Veri Koruma Reformu kapsamında yürürlüğe giren 2016/679 sayılı Tüzük'ün, altını belirgin bir şekilde çizdiği en önemli hususlardan biri de, kişisel verilerin korunması bağlamında veri süjesine tanınan haklardır. Tüzük ile yapılan yeni düzenlemeye göre, kişisel verilerin korunması kapsamında veri süjesinin bizzat kendisinin kullanabileceği "*erişim hakkı, düzeltme hakkı, işlemenin kısıtlanmasını talep hakkı, itiraz hakkı, profilleme de dahil tamamen otomatik olarak yapılan herhangi bir işleme faaliyetine dayalı olarak alınan karara tabi olmama*

[346] Tal Z.Zarsky, ss. 1013-1014.

hakkı, veri taşınabilirliği hakkı, unutulma (silme) hakkı" şeklinde sıralanan haklar ve bunların hangi istisnai koşullar altında kısıtlanabileceğiyle, yine veri süjesine tanınan işbu haklar kapsamında veri kontrolörlerine getirilen yükümlülükler, Tüzük'ün III. Bölümünde yer alan 12. ila 23.maddeler arasında düzenlenmiştir.

3.5.5.1. Veri Süjesinin Bizzat Kendisinin Kullanabileceği Haklar

2016/679 sayılı Tüzük, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bağlamında, veri süjesinin bizzat kendisinin kullanabileceği hakları da düzenlemektedir. Veri süjesine kişisel verilerine ilişkin olarak bahşedilen ve aşağıda detaylı şekilde ele alınacak olan bu haklar, "*erişim hakkı, düzeltme hakkı, işlemenin kısıtlanmasını talep hakkı, itiraz hakkı, profilleme de dahil tamamen otomatik olarak yapılan herhangi bir işleme faaliyetine dayalı olarak alınan karara tabi olmama hakkı, veri taşınabilirliği hakkı, unutulma (silme) hakkı"* şeklinde sıralanabilir. Veri süjelerine sağlanan bu haklar ile, bireylerin kendi kişisel verileri üzerindeki kontrollerinin artırılması hedeflenirken, bu yolla veri kontrolörlerinin ellerinde bulunan asimetrik gücün, veri süjeleri lehine çevrilerek güçler dengesinin kurulması amaçlanmaktadır[347]. Veri süjesine tanınan bu haklar ile, ayrıca, eksik, yanlış veya hatalı bir kişisel veriye dayanılarak işlem yapılmasının; yasal işleme ilkesi dışına çıkılarak kişisel verilerin işlenmesinin; ya da, yetkisiz kişilerce işleme yapılmasının önüne geçilerek; bu yolla veri süjesinin zarara uğramasının, bizzat veri süjesinin kendisi tarafından, birinci elden engellenebilmesi hedeflenmiştir.

Kişisel verilerinin korunması bağlamında veri süjesinin bizzat kendisinin kullanabileceği haklardan ilki, "*Erişim Hakkı (Right of Access by the Data Subject)*"dır. Erişim hakkı, Tüzük'ün 15.maddesi kapsamında düzenlenmiştir. Bu maddeye göre, veri süjesi, kendisine ait kişisel verilerin işlenip işlenmediğine ilişkin veri kontrolöründen teyid isteme hakkına sahiptir. Kişisel verilerinin işlendiği teyid edilen veri süjesi, kontrolörden işleme konusu olan kişisel verilerinin kapsam ve içeriğine erişim talep edebilecektir.

Erişim hakkı kapsamında veri süjesinin, kontrolörden, aşağıdaki bilgileri de talep edebilme hakkı bulunmaktadır: "*İşlemenin amacı (Madde 15/1 - a); Verilerin*

[347] Michelle Goddard, "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact", **International Journal of Market Research**, Cilt.59, Sayı.6, s. 705.

ne şekilde sınıflandırıldığı (Madde 15/1 - b); Üçüncü ülkelerdeki ve uluslararası organizasyonlardaki alıcılar da dahil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcıların kimler olduğu (Madde 15/1 - c); Mümkün olduğu taktirde, verilerin saklanacağı öngörülen süre, bu süre öngörülemediği taktirde ise, sürenin belirlenmesinde kullanılacak kriterlerin neler olduğu (Madde 15/1 - d); İşlemeye konu kişisel verilerin veri süjesinden elde edilmediği durumlarda, bu verilerin hangi kaynak ya da kaynaklardan elde edildiği (Madde 15/1 - g); işbu Tüzük'ün 22/1. ve 4.maddelerinde ifade edildiği şekilde, profilleme[348] *yapılması da dahil, otomatik karar verme mekanizmaları kapsamında işleme yapılması durumunda, işlemenin hangi mantıktan yola çıkılarak yapıldığına ilişkin bilgiler ve veri süjesi açısından kayda değer ve öngörülebilir sonuçlarının neler olduğu (Madde 15/1 - h)".* Aynı zamanda, Tüzük'ün 15/1 (f) maddesi kapsamında, veri süjesinin, erişim hakkı kapsamında işlemeye ilişkin olarak bir "*denetim makamına şikayette bulunabilme hakkı*" da bulunmaktadır.

"*Erişim hakkı*" çerçevesinde, Tüzük madde 15/3'e göre, kontrolör, işlenen kişisel verilerin neler olduğuna ilişkin bilgileri içeren bir belgeyi, veri süjesine sağlamakla yükümlüdür. Kontrolör bu belgenin hazırlanması sebebiyle, yapmış olduğu idari işlemlere ilişkin olarak veri süjesinden makul bir ücret talep edebilecektir. Veri süjesi, belge talebini, kontrolöre, elektronik ortamda ilettiği taktirde, veri süjesi tarafından özellikle başka şekilde iletilmesi istenmez ise, bilgilendirme yine elektronik ortamda yapılabilir. Ancak hemen belirtmek gerekir ki, işbu belge talebinin, üçüncü kişilerin hak ve özgürlüklerini hiçbir şekilde olumsuz yönde etkilememesi gerektiği hususunun altı, madde 15/4 ile açıkça çizilmiştir.

Veri süjesine tanınan erişim hakkının, kişisel verilerin aktarıldığı alıcıların kimliğine ve bu alıcılara hangi verilerin açıklandığına ilişkin bilgileri de kapsadığı anlaşılmaktadır. Ancak erişim hakkının, veri süjesi tarafından geçmişe dönük olarak bu bilgilerin talep edilmesine ilişkin kullanılması durumunda, veri kontrolörünün hangi zaman dilimi sınırları dahilinde, ne kadar geriye gidilerek, bu verilerin saklanmasından ve veri süjesine iletilmesinden sorumlu olduğu hususu uygulamada

[348] 2016/679 sayılı Tüzük'ün 4/4.maddesi kapsamında "*profilleme*" eylemi, kişisel verilerin otomatik işleme faaliyetleri kapsamında analiz edilip değerlendirilerek, kişinin iş performansı, ekonomik ve sağlık durumu, kişisel tercih ve eğilimleri, ilgi alanları, güvenilirliği, davranış kalıpları, konumu ve hareketleri gibi çeşitli bireysel özellikleri hususunda çıkarımlarda bulunulması şeklinde tanımlanmaktadır.

pek çok tartışmayı beraberinde getirmiştir. Bu hususta Adalet Divanı'nın vermiş olduğu "*Rijkeboer Kararı*" önemlidir.

Rijkeboer davası kapsamında, Bay Rijkeboer, College van burgemeester en wethouders van Rotterdam (*Bundan böyle "College" olarak adlandırılacaktır*)'dan geriye dönük olarak iki yıl boyunca hangi kişisel verilerinin, hangi üçüncü kişilere açıklandığına ilişkin bilgi talebinde bulunarak, bu verilere erişim hakkını kullanmak istediğini bildirmiştir. College ise, Bay Rijkeboer'in bu talebini kısmen reddederek, sadece son bir yıla ilişkin bilgilerin kendisine iletilebileceğini, bir yıldan daha eski bilgilerin ise otomatik olarak silinerek, sistemlerinde daha fazla saklanmadığını bildirmiştir. Bunun üzerine açılan davada yerel mahkeme konuyu Adalet Divanı'na taşımıştır. Adalet Divanı'nın bu hususta vermiş olduğu karara göre; veri süjesine tanınan erişim hakkı, kişisel verilerin iletildiği alıcıların kimliği ile bu alıcılara hangi verilerin iletildiği hususlarını da kapsamaktadır. Üye devletlere ise, -mülga 95/46 sayılı Direktif çerçevesinde- bu tür verilerin geçmişe dönük olarak hangi süreyle sınırlı olarak saklanacağına ilişkin düzenleme yapma yetkisi tanınmıştır (*Davanın görüldüğü Hollanda'da bu saklama süresi geriye dönük olarak bir yıldır*). Ancak aynı zamanda da, üye devletlere, bu süre kısıtına ilişkin düzenleme yaparken, veri süjesinin mahremiyetinin korunması konusundaki çıkarları ile veri kontrolörüne bu verilerin saklanmasına ilişkin olarak yüklenen maddi yükün ağırlığı arasında kurulması gereken adil dengenin bozulmaması gerektiğini göz önüne alma yükümlülüğü getirildiği de belirtilmiştir. Somut olayda, bu gibi verilerin saklanması hususunda veri kontrolörü üzerine gerçekten çok büyük bir yük bindiği sabit olmadıkça, ilgili kişisel verilerin kendisi halen depolanmakta iken bu verilerin hangi üçüncü kişilere aktarıldığı bilgisinin saklanmasının bir yıllık süreyle sınırlı tutulmasının adil dengenin korunması çerçevesinde değerlendirilemeyeceğinin de altı çizilmiştir[349]. Adalet Divanı'nın Rijkeboer kararı ile erişim hakkının kullanılması hususunda hakkaniyete ve orantılılık ilkesine uygun davranılması gerektiğine ilişkin önemli bir adım atarak, uygulamada verilerin hangi süreyle arşivlenmesi gerektiğine

[349] Judgment of the Court of Justice (Third Chamber), **ECJ C-553/07**, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 7 May 2009, http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1065929 (02.06.2020).

ilişkin olarak ortaya çıkan sorunları, bu ilkelere uygun olarak çözmeye çalıştığı söylenebilir.

Veri süjesinin, Tüzük kapsamında bizzat kendisinin kullanabileceği haklardan ikincisi, madde 16'da tanımlanan "*Düzeltme hakkı (Right to Rectification)*"dır. Bu maddeye göre, veri süjesi, kendisine ilişkin gerçeği yansıtmayan kişisel bir verinin vakit geçirilmeksizin düzeltilmesini veri kontrolöründen talep edebilir. Ayrıca veri süjesinin düzeltme hakkı kapsamında, işleme amaçları göz önüne alındığında eksik, yanlış veya hatalı olduğu anlaşılan kişisel verilerinin, yine kendisinin yapacağı ek beyan doğrultusunda tamamlanmasını talep etme hakkı da bulunmaktadır.

Tüzük'ün 18.maddesi ile de, bu maddede anılan koşullar altında, veri üjesine "*İşlemenin kısıtlanmasını talep hakkı (Right to restrictions of processing)*" tanınmıştır. Madde 18/1'e göre; "*kişisel verilerin doğruluğuna veri süjesi tarafından itiraz edildiği taktirde, verilerin doğruluğunun veri kontrolörü tarafından onaylanmasına kadar geçecek süre zarfında (Madde 18/1 a); Veri işleme faaliyetinin yasal olmadığı hallerde, veri süjesinin verilerin silinmelerine izin vermediği taktirde, bu verileri silmek yerine (Madde 18/1 b); İşleme amaçları kapsamında veri kontrolörünün ilgili kişisel verilere daha fazla ihtiyacının kalmamasına rağmen, veri süjesinin yasal bir hak talebi oluşturulması, hakkın icrası ya da savunmanın yerine getirilmesi bakımlarından bu verilere ihtiyacının olduğu hallerde (Madde 18/1 c); Veri süjesinin işbu Tüzük'ün 21/1.maddesi kapsamında kişisel verilerinin işlenmesine ilişkin olarak itiraz hakkını kullandığı durumlarda, veri kontrolörünün veri işlenmesine ilişkin meşru gerekçelerinin veri süjesinin itiraz gerekçelerine ağır basmadığının doğrulandığı hallerde (Madde 18/1 d)*", veri süjesi, kontrolörden kişisel verilerinin işlenmesi faaliyetlerinin kısıtlamasını talep etme hakkına sahiptir. Veri süjesinin yukarıda bahsedilen sebeplerle, kişisel verilerinin işlenmesinin kısıtlanmasını talep hakkını kullanmasıyla, artık bu veriler, veri süjesinin talebi doğrultusunda, somut olayın özelliklerine göre, gerekli tedbirler alınarak işlenmemek üzere dondurulacaklardır. Örneğin, bir kişinin almış olduğu hizmetle ilgili şikayetine ilişkin olarak, doldurmuş olduğu ve çeşitli kişisel verilerini de içeren şikayet formunun, daha sonra açacağı davaya delil teşkil etmesi amacıyla, ilgili şirketin kayıtlarında saklanmasıyla birlikte, bu kaydın başka amaçlarla işlenmesini önlemek

için, veri süjesi, veri kontrolöründen bu şikayet formundaki kişisel verilerinin işlenmelerinin kısıtlanması talebinde bulunabilecektir[350].

Tüzük madde 18/2'ye göre, işleme faaliyetinin veri süjesinin talebi ile yukarıda anılan sebeplerden biri ile kısıtlanması durumunda, ilgili kişisel veriler, saklama faaliyeti dışında, kural olarak işlenemez. Ayrıca kullanımı kısıtlanan kişisel veriler, ancak, veri süjesinin vereceği özel onay dahilinde; veya, üçüncü kişi konumundaki gerçek veya tüzel kişiye ilişkin bir hak talebinin oluşturulması, hakkın icrası veya savunmanın yerine getirilmesinin gerektirdiği; ya da, Birlik'e veya üye devlete ait önemli bir kamu yararının korunmasının gerekli kıldığı, istisnai hallerde işlenebilecektir. Madde 18/3 kapsamında da, veri süjesinin talebi üzerine işlenmesi kısıtlanan kişisel veriler üzerindeki bu kısıtın kaldırılmasından önce veri süjesinin, kontrolör tarafından bilgilendirilmesi gerektiği düzenlenmektedir.

Tüzük'ün 21. maddesi kapsamında kişisel verilerinin işlenmesine ilişkin veri süjesinin "*İtiraz hakkı (Right to object)*" düzenlenmiştir. Bu maddeye göre, kişisel verilerin işlenmesi, Tüzük'ün 6/1 (e) ve (f) fıkraları kapsamında belirtilen kamu yararına yönelik bir görevin ifası veya veri kontrolörüne bahşedilen resmi yetkinin kullanılması için gerekliyse; ya da, kişisel verilerin işlenmesi veri kontrolörünün veya üçüncü kişilerin meşru menfaatlerinin korunması doğrultusunda yapılıyorsa *(madde 21/1)*; veya, profilleme de dahil, doğrudan pazarlama hedefiyle gerçekleştiriliyorsa *(madde 21/2)*, bu amaçlarla yapılan işleme faaliyetlerine, veri süjesi her zaman itiraz edebilecektir.

Veri kontrolörünün veya üçüncü kişilerin meşru menfaatlerinin korunması amacıyla yapılan kişisel verilerin işlenmesi faaliyetlerinin, veri süjesi tarafından yapılan itiraza rağmen devam edebilmesi için ise, Tüzük madde 6/1 (f)'de de belirtildiği şekilde, veri kontrolörü veya üçüncü kişinin, kendi meşru menfaatlerinin, veri süjesinin kişisel verilerinin korunması hakkına üstün geldiğini ispat edebilmeleri gerekmektedir. Tüzük madde 21/3'e göre ise, doğrudan pazarlama amacıyla yapılan işleme faaliyetlerine, veri süjesi tarafından itiraz edilmesi halinde, artık ilgili kişisel veriler doğrudan pazarlamaya ilişkin amaçlarla hiçbir şekilde işlenemeyeceklerdir.

[350] Hüseyin Murat Develioğlu, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, 1.Baskı, Oniki Levha Yayınları, İstanbul, 2017, ss.93-94.

Tüzük'ün 21.maddesi ile, profilleme de dahil doğrudan pazarlama amacıyla yapılacak işleme faaliyetleri kapsamında, kişisel verilerin işlenmesine ilişkin olarak, veri süjesine tanınan itiraz hakkı ve bu hakkın herhangi bir zamanda veri süjesi tarafından kullanılmasıyla birlikte, artık işbu verilerin hiçbir şekilde işlenemeyecek olması hali, tamamlanmaya çalışılan Avrupa dijital tek pazarının, tüketiciler açısından daha güvenli hale gelmesine önemli katkıda bulunabilecek bir düzenlemedir. Zira veri süjesi, 21.maddede düzenlenen itiraz hakkını kullanması yoluyla, doğrudan pazarlama faaliyetlerinde kişisel verilerinin kullanılmasını doğrudan ve kesin bir şekilde engelleyebilmektedir.

Tüzük'ün 22.maddesi kapsamında ise veri süjesinin kendisi bakımında yasal etki ve sonuç doğurabilecek nitelikte bulunan ve insan müdahalesinden uzak bir şekilde "*Profilleme de dahil, tamamen otomatik olarak yapılan, herhangi bir işleme faaliyetine dayalı olarak alınan karara tabi olmama hakkı (Right not to be subject to a decision based solely on automated processing, including profiling)*" düzenlenmiştir. Salt otomatik işleme sonucu alınan bir karara tabi olmamaya ilişkin olarak veri süjesine tanınan bu hak, özellikle veri süjesine ilişkin bir takım yasal sonuçlar ortaya koyarak, onu önemli ölçüde etkileyebilecek nitelikteki, otomatik işleme faaliyetlerine karşı kullanılabilir. Veri süjesinin iş performansını, ekonomik durumunu, sağlık durumunu, kişisel tercihleri ve ilgi alanlarını, davranışlarını, konum ve hareketlerini içeren kişisel verilerinin tamamen otomatik bir şekilde işlenmesi halleri bu kapsamda örnek olarak sayılabilir. Bu gibi durumlarda kişisel verilerin yapay zekalar aracılığıyla otomatik işlenmesi neticesinde ortaya konulan işleme sonuçlarına, insan müdahalesi yapılarak, nihai yorumlamanın yetkili kişilerce gerçekleştirilmesi, veri süjesinin otomatik işleme sonucu katlanmak zorunda kalabileceği olumsuz etkilerin bertaraf edilebilmesi bakımından önem arz eder[351].

Bu hak literatürde, kapsam ve içerik olarak iyi tanımlanmadığı, özellikle de insan müdahalesinin hangi şekillerde yapıldığı takdirde alınan kararın salt otomatik olarak yapılan işleme faaliyeti kapsamından çıkabileceğine ilişkin hususları açıklamakta muğlak ve yetersiz kaldığı, bu sebeplerle de veri süjelerinin kendilerine tanınan bu haktan tam manasında yararlanmalarının mümkün olmadığı, hususlarından eleştirilmektedir. Gelişmiş teknoloji ürünü otomatik veri işleme teknik

[351] GDPR Beyanlar (71).

ve sistemlerinin, veri süjelerine ilişkin olarak beklenmeyen ve istenmeyen sonuçlar ortaya koyabileceği göz önüne alındığında Tüzük'e yöneltilen bu eleştirilerde bir haklılık payı olduğu anlaşılmaktadır[352]. İşleme sonuçlarına bu kapsamda yapılacak insan müdahalesinin ise somut olayın özelliklerine göre, yeterli miktarda olması ve kararın verilmesinden önceki bir dönemde yapılması, ilgili maddenin uygulanması kapsamında getirilen eleştirilere bir miktarda olsa yanıt verilebilmesi bakımından önemli ve gereklidir[353].

Tüzük'ün getirdiği önemli değişikliklerden bir diğeri de 20. madde kapsamında düzenlenmiştir. Bu maddeye göre, veri süjesinin bizzat kendisinin kullanabileceği haklardan biri de "*Veri Taşınabilirliği Hakkı (Right to Data Portability)*" dır. Bu hak kapsamında veri süjesi, bizzat kendisinin veri kontrolörüne aktardığı kişisel verilerini, yaygın bir şekilde kullanılan ve makinalar tarafından yeniden okunmaya elverişli olarak yapılandırılmış bir formatta hazırlanarak, bir başka veri kontrolörüne iletilmek üzere, kendisine teslim edilmesini yahut teknik anlamda mümkünse, elektronik ortamda, doğrudan veri süjesinin kendisinin belirlediği yeni kontrolöre gönderilmesini talep edebilir[354].

Veri taşınabilirliği hakkının, veri süjesinin kendi kişisel verileri üzerindeki kontrolünü artırma hedefine yönelik olarak atılmış önemli bir adım olduğunu söylemek yanlış olmayacaktır. Bu noktada veri kontrolörlerinin, veri taşınabilirliği hakkının kullanımını kolaylaştıracak nitelikte, birlikte çalışabilirliğin sağlandığı, kullanışlı formatlar geliştirme çalışmaları yapmaları teşvik edilmelidir[355]. Netice itibarı ile, veri taşınabilirliği hakkı içeriğinde, kişisel verilerin bir kopyasının veri kontrolöründen aktarıma uygun bir formatta alınması hakkı ile, bu verileri bir kontrolörden, diğerine aktarabilme hakkı şeklinde tanımlanabilen, veri süjesinin kullanabileceği iki önemli hak barındırarak, veri süjesinin bu bağlamda kendi verileri üzerindeki kontrolünü artırmaktadır. Bu hak, günlük hayatta, kişisel verilerin sadece

[352] Sandra Wachter, Brent Mittelstadt, "Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", **International Data Privacy Law**, Cilt.7, Sayı.2, 2017, ss.76-77, 92.
[353] Gianclaudio Malgieri, "Giovanni Comande, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", **International Data Privacy Law**, Cilt.7, Sayı 4, 2017, ss. 248-256.
[354] Aysem Diker Vanberg, Mehmet Bilal Ünver, "The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?", **European Journal of Law and Technology**, Cilt.8, Sayı.1, 2017, s.3.
[355] GDPR Beyanlar (68).

sosyal medya alanında değil, arama motorları, e-posta hizmetleri, çevirim içi alışveriş siteleri, bankalar, ilaç firmaları, enerji sağlayıcıları, iletişim sektörü, havayolu şirketleri, sağlık merkezleri gibi çok çeşitli sektörler kapsamında veri süjesi tarafından taşınabilirliklerinin sağlaması bakımından önemlidir[356].

Veri süjesi, Tüzük madde 20 kapsamında veri taşınabilirliği hakkını kullansa dahi, bu hakkın kullanılması, mevcut veri kontrolörünün sisteminde bulunan kişisel verilerinin otomatik olarak silinmesi sonucunu doğurmayacaktır. Bu sebeple veri süjesi bu hakkını kullansa dahi, mevcut veri kontrolöründen hizmet almaya da devam edebilecektir. Ayrıca veri süjesi tarafından veri taşınabilirliği hakkı ile birlikte, bir sonraki bölümde detaylı olarak anlatılacak olan unutulma (silme) hakkının da kullanılması durumu, mevcut veri kontrolörüne, somut olayda işbu veri taşınabilirliği hakkının kullanılmış olmasını ileri sürerek, kişisel verilerin silinmesini erteleme ya da silme işlemini reddetme hakkı da vermemektedir[357].

3.5.5.1.1. Unutulma Hakkı

2016/679 sayılı Tüzük'ün 17.maddesi kapsamında "*Silme Hakkı veya Unutulma hakkı (Right to Erasure or Right to be forgotten)*" düzenlenmiştir. Avrupa'daki tarihsel kökenleri çok eskilere dayanan unutulma hakkının[358] ve dolayısı ile de kişisel verilerin korunması hakkının Birlik hukuku kapsamındaki ilk çıkış noktası serbest dolaşımın temini bağlamında ekonomik temellidir. Dijitalleşmenin yoğunlaşmasıyla ortaya çıkan gelişmelerle birlikte, hem unutulma hakkı, hem de kişisel verilerin korunması hakkı, Birlik'in salt ekonomik çıkarlarının korunması perspektifinden kurtularak, kişilik hakkı çerçevesinde ele alınıp, korunmaları gereken anayasal haklar olarak önem kazanmaya başlayarak, evrilmişlerdir. Unutulma hakkının anayasal bir çerçevede ve kişilik hakkı bağlamında korunması gerektiğini kabul eden en önemli erken dönem kararlarından biri, İtalyan Yüksek Mahkemesi'nin 22 Haziran 1985 tarihli ve 3769 sayılı kararıdır.

[356] Aysem Diker Vanberg, Mehmet Bilal Ünver, s. 2;
Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, adopted on 13 December 2016 as last revised and adopted on 5 April 2017, **WP 242**, rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 (02.06.2020), ss.4-5.
[357] Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, s. 7.
[358] Avrupa'da unutulma hakkının gelişiminde İsviçre Federal Mahkemesi'nin kararları önemli bir yer tutar. Bu hususta derinlemesine bilgi için bkz. Nilgün Başalp, 2015, ss. 93-97.

Bu kararla mahkeme, bireyin kişiliğinin korunmaya değer esaslı parçaları olarak kabul edilen kültürel, siyasi, sosyal, dini veya iş hayatına ilişkin kişisel verilerinin, kamuoyuna yanlış aksettirilmelerine karşın, anayasal koruma altında olmaları gerektiği hususunu kabul etmiştir[359]. İtalyan Yüksek Mahkemesi'nin bu kararı ile, dijital çağda bireylerin temel hak ve özgürlüklerine fazlasıyla değmeye başlayan teknolojinin olası olumsuz etkilerine karşın bireyin kişiliğinin korunması perspektifinden yola çıkılarak, unutulma hakkı da temel hakların korunması çerçevesinde hüküm altına alınmıştır[360].

Unutulma hakkı, devam eden süreçte, özellikle 21.yüzyılda, sonsuz veri tarama ve saklama kapasitesine sahip teknoloji ve internet kullanımının geniş kapsam ve kitlelere yayılması sebebiyle, mahremiyete, kişilik hakkına, dolayısı ile de kişisel verilere ilişkin ihlallerin artması doğrultusunda, her geçen gün daha fazla önem kazanmıştır. Avrupa Birliği'nde de 21.yüzyıldaki teknolojik gelişmelere paralel olarak kişisel veriler ile mahremiyetin ve kişilik hakkının büyük risk altında olduğu tespit edilmiştir. Birlik'in bu öngörüsü sebebiyle, 2000'li yıllardan itibaren bireylerin kendi kişisel verileri üzerindeki kontrollerini ve bu bağlamdaki yasal korunma seviyelerini artırma amacı ile, unutulma hakkına yönelik çalışmalar hızlanmış ve bu yönde Birlik tarafında zaman zaman çeşitli tespit ve açıklamalar yapılmıştır[361]. 2012 yılının başında Komisyon, kişisel verilerin korunmasına ve verileri üzerinde veri süjelerinin kontrollerini artırmalarına yönelik kapsamlı bir reform önerisi getirmiştir. İlgili öneride, unutulma hakkının, özellikle çevirim içi ortamda bireylerin, kişisel verilerinin ihlaline ilişkin riskleri daha iyi yönetmelerine

[359] Marco Bassini, Oreste Pollicino, "Reconciling Right to be Forgotten and Freedom of Information in the Digital Age: Past and Future of Personal Data Protection in the European Union", **Diritto Pubblico Comparato ed Europeo**, Cilt.2014/2, https://www.academia.edu/19963974/Reconciling_right_to_be_forgotten_and_freedom_of_information_in_the_digital_age._Past_and_future_of_personal_data_protection_in_the_European_Union (02.06.2020) ss. 641-643.

[360] Eugenio Foco, "The Codification of the Right to be Forgotten in the Digital Era: From Directive 95/46/EC to the General Data Protection Regulation", 17.11.2016, http://www.medialaws.eu/the-codification-of-the-right-to-be-forgotten-in-the-digital-era-from-directive-9546ec-to-the-general-data-protection-regulation/ (02.06.2020).

[361] Bu açıklamalardan bazıları için bkz: European Commission, **Press Release Database**, "Data Protection Reform – Frequently asked Questions", 4.11.2010, http://europa.eu/rapid/press-release_MEMO-10-542_en.htm , (02.06.2020); Viviane Reding, "Privacy matters-Why the EU needs new Personal Data Protection Rules", European Commission, **Press Release Database**, 30.11.2010, http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm , (02.06.2020); Viviane Reding, "Independent Data Protection Authorities: Indispensable Watchdogs of the Digital Age European Commission", **Press Release Database**, 7.12.2011, http://europa.eu/rapid/press-release_SPEECH-11-863_en.htm , (02.06.2020).

ve kişisel verilerin işlenmesine ilişkin yasal sebepler ortadan kalktığında, bu verilerin veri süjesinin talebi ile ortadan kaldırılabilmesine yardımcı olabileceğinin altı çizilmiştir[362]. Böylece internet ortamında müdahale edilmediği takdirde, verilerin sonsuza kadar var olabileceği ve bireylerin bu bağlamda karşılaşabilecekleri zararlardan korunmaları gerektiği fikrinden hareketle, unutulma hakkı kapsamında yapılacak yasal düzenlemelerle, bireylerin kişisel verileri ve bu verilerin işlenmesi faaliyetleri üzerindeki kontrol ve etkilerinin artırılarak, oluşabilecek temel hak ihlallerinin önlenmesi hedeflenmiştir[363].

"*Unutulma hakkı*" başlığı altındaki ilk açık yasal düzenleme, her ne kadar Avrupa Birliği Genel Veri Koruma Tüzüğü madde 17 kapsamında yapılmışsa da, "*kişisel verilerin işlenmesine ilişkin meşru amaçlar ortadan kalktığında, bireylerin bu verilerin silinmesini talep edebilmesi*" şeklinde formüle edilebilen bu hakkın çıkış noktası, Avrupa Birliği'nin mülga 95/46 sayılı Direktifi'nin 6. maddesine uzanmaktadır. Mülga 95/46 sayılı Direktifin 6. maddesinde, üye devletlerin, toplanma amaçları sona erdikten sonra kişisel verilerin işlenmemelerini sağlamaları gerektiği belirtilmiştir. Yine aynı Direktif'in 12. maddesinde de veri süjelerinin kişisel verilerin silinmesini ya da bloke edilmesini talep haklarının bulunduğu açıklanmıştır[364].

"*Unutulma Hakkı*", Avrupa Birliği Genel Veri Koruma Tüzüğü madde 17 kapsamında ise ayrı bir başlık altında açıkça düzenlenmiştir. 17.madde kapsamına göre; "*Kişisel verinin toplanma ya da herhangi bir şekilde işlenme amaçları göz önüne alındığında, artık ilgili kişisel veriye ihtiyaç kalmaması (madde 17/1 a); Veri süjesinin ilgili kişisel verisinin işlenmesine yönelik iznini geri çekmesi ya da verinin işlenmesini gerektiren yasal zeminin ortadan kalkması (madde 17/1 b); Kişisel verinin işlenmesini haklı çıkaracak meşru zeminin olmaması sebebiyle, veri süjesinin kişisel verinin işlenmesine itiraz etmesi (madde 17/1 c); Kişisel verinin yasa dışı işlenmesi (madde 17/1 d); Veri kontrolörünün, Birlik ya da üye devletteki yasal bir zorunluluğa uyma yükümlülüğü doğrultusunda, verinin silinmesinin gerekmesi*

[362] European Commission, **Press Release**, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses", Brussels, 25.01.2012.
[363] Meg Leta Ambrose, "It's about time: Privacy, Information Life Cycles and the Right to be Forgotten", **Stanford Technology Law Review**, Cilt.16, Sayı.2, 2013, ss. 101, 120-122.
[364] Robert Kirk Walker, "The Right to be Forgotten", **Hasting Law Journal**, Cilt. 64, Sayı.1, 2012, s. 272.

(madde 17/1 e); Kişisel verinin bilgi toplumu hizmeti sunulması teklifi ile ilgili olarak çocuklara ilişkin toplanması gibi durumlarda (madde 17/1 f)", veri süjesinin, ilgili verilerin gecikmeksizin silinmesini, veri kontrolöründen talep etme hakkı bulunmaktadır. Veri kontrolörü de böyle bir talebin kendisine ulaşması durumunda, ilgili kişisel verileri gecikmeksizin silmekle yükümlüdür. Ayrıca yine aynı maddede, kendisine ulaşan bu silme talebini, ilgili kişisel verileri işleyen diğer üçüncü şahıslara iletme yükümlülüğünün de veri kontrolöründe olduğunun altı çizilmiştir. Madde 17'nin 3. fıkrasında ise unutulma hakkının uygulama kapsamı dışında kalacak istisnai haller sayılmıştır. Buna göre; Haber alma ve ifade özgürlüğünün korunması kapsamındaki; Kamu yararının, kamu sağlığının korunmasının gerektirdiği; Yasal iddiaların oluşturulması, uygulanması ve savunmanın gerekli kıldığı; Kamu yararı dolayısıyla gerçekleştirilen arşivleme çalışmaları ile bilimsel, istatistiksel veya tarihi araştırmalar amacıyla işleme yapılan, hallerde somut olayın özelliklerine göre, unutulma hakkı uygulanmayabilmektedir.

2016/679 sayılı Tüzük'ün Giriş 65.paragrafı kapsamında da, unutulma hakkının, özellikle çevirimiçi ortamda yapmış olduğu hareketlerinin ve çeşitli işlemlere vermiş olduğu rızasının getirebileceği riskleri, tam olarak idrak edemeyeceği kabul edilen çocuklar bakımından, titizlikle uygulanması gerektiğinin altı çizilmiştir.

Kamuoyunda "*İspanya Google Davası*[365]" olarak da bilinen "*Mario Costeja Gonzales Davası*", unutulma hakkının somut olaya nasıl uygulanması gerektiği hususunda önemli noktalara değinmesi bakımından burada anılmaya değer bir davadır. İspanya Google Davasında verilen karar ile, basın-yayın özgürlüğü kapsamında kamuya açık hale gelen kişisel verilerin, aradan geçen uzun zaman dikkate alındığında "*haber değerini yitirmesi ve artık internet ortamında bulunmasında kamu yararının kalmaması*"; bu verilerin silinmemesi durumunda, çevirim içi ortamda sonsuza dek kalarak, veri süjesi hakkında kamuoyunda önyargı oluşmasına neden olup, kişilik hakkına zarar verebilmeleri sebepleri ile, bu gibi

[365] İspanya Google Davası, işbu tez çalışmasının "*2.1.3.4. Düşünce ve İfade Özgürlüğü Bağlamında Kişisel Veriler*" başlıklı bölümünde detaylı olarak anlatılmıştır.

verilerin veri süjesinin unutulma hakkı kapsamında yapacağı başvuru üzerine internet ortamından kaldırılmaları gerektiği hususu açıkça ortaya konmuştur[366].

Avrupa Birliği Adalet Divanı'nın 2014 tarihli İspanya Google Kararı, hem Birlik topraklarında faaliyet gösteren yabancı bilişim şirketlerinin Birlik hukuku kapsamında ortaya çıkabilecek sorumluluklarını ortaya çıkarması; hem ticari bir işletmenin ekonomik çıkarlarının özellikle de bireyin özel yaşamının gizliliğinin korunmasına ilişkin temel hak ve özgürlüklerine üstün gelemeyeceğinin altını çizmesi[367]; hem de henüz Genel Veri Koruma Tüzüğü'nün kabul edilmesinden önce dahi unutulma hakkının, uygulamada, Birlik makamlarınca benimsenerek yargı kararlarına yansıdığını göstermesi, bakımlarından önemlidir.

Adalet Divanı tarafından verilen İspanya Google Kararının ertesinde, Google Şirketi de kişisel verilerin korunması ile basın yayın ve ifade özgürlüğü arasındaki hassas dengenin korunması hususunda, bu karar neticesinde kendi üzerine düşen sorumlulukları yerine getirebilmek adına bazı önemli adımlar atmıştır. Bu adımlardan ilki, unutulma hakkını kullanmak isteyen bireylerin, Google Şirketinin bu hususdaki yetkili birimlerine ulaşmalarını kolaylaştırmak üzere bizzat kendisinin hazırladığı dijital (çevirimiçi) başvuru formudur. Bu formun, Mayıs 2014 tarihinden bu yana, dokuzyüz bine yakın Google kullanıcısı tarafından doldurulduğu ve bu şekilde Google'a ulaşan silinme taleplerinin yarısına yakın kısmına da Google tarafından olumlu yanıt verilerek bu verilerin silindiği görülmüştür[368][369].

Google tarafından atılan ikinci önemli adım ise, kişisel verilerin korunması hususunda uzmanlardan oluşan bir danışma kurulu oluşturmasıdır. Bu kurulun hazırladığı rapor kapsamında, silinme taleplerinin Google tarafından karara bağlanması hakkında dört kriter belirlenmiştir. Bu kriterler, veri süjesinin kamusal bir rolünün bulunup bulunmadığının değerlendirilmesi; ilgili verinin niteliği ve türünün ne olduğunun belirlenmesi; ilgili verinin kaynağının tespit edilmesi; ve son

---

[366] Judgment of the Court of Justice of the European Union (Grand Chamber), **ECJ Case C-131/12**, 13.05.2014, Google Spain SL, Google Inc. V. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez.

[367] Elif Küzeci, ss. 230-233.

[368] Avrupa Birliği'nin 2014 yılında almış olduğu İspanya Google Kararına istinaden yapılan güncel silinme talebi ve silinen toplam URL sayısı hakkında daha fazla bilgi için bkz. Google, Transparency Reports, https://transparencyreport.google.com/eu-privacy/overview (02.06.2020).

[369] W.Gregory Voss, "After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change", **The Business Lawyer**, Cilt. 71, Sayı.1, Winter 2015-2016, s.282.

olarak da, ilgili verinin yayınlanmasının üzerinden ne kadar zaman geçtiğinin tespit edilmesidir. Aynı raporda bu dört kriterin hiçbirinin tek başına belirleyici olmadığı ve kriterler arasında herhangi bir hiyerarşinin de bulunmadığının altı çizilerek, somut olay kapsamında silinme kararının verilmesinde bu dört kriterin birlikte göz önüne alınması gerektiğinin altı önemle çizilmiştir[370].

"*Unutulma Hakkı*" başlıklı işbu bölüm ile yukarıda "*Veri Süjesinin Bizzat Kendisinin Kullanabileceği Haklar*" başlığı altında yer alan "*erişim, düzeltme, işlemenin kısıtlanmasını talep, itiraz, profilleme de dahil tamamen otomatik olarak yapılan herhangi bir işleme faaliyetine dayalı olarak alınan karara tabi olmama, veri taşınabilirliği, unutulma (silme)"* hakları ile, veri süjesinin, kişisel verileri üzerindeki kontrolünün artırılarak, mahremiyetinin daha sağlam bir şekilde korunması ve bilginin geleceğini kişinin kendisinin belirlemesi ilkesinin uygulanmasının kolaylaştırılması hedeflemektedir. Bu yolla, temel hak ve özgürlüklere sağlanan korumanın artırılarak, bireyler için oluşturulacak güven ortamında, Avrupa dijital tek pazarının gelişimine katkıda bulunulabileceği de unutulmamalıdır.

3.5.6. Veri Süjesinin Hakları Hususunda Bilgilendirme Yükümlülüğü

2016/679 sayılı Tüzük, kişisel verilerin korunması bağlamında, hem veri süjesinin bu Tüzük kapsamındaki haklarını gerektiği şekilde kullanabilmesinin sağlanarak, veri süjesinin kişisel verileri üzerindeki etkin kontrolünün artırılması, hem de şeffaflık ilkesinin gerektiği gibi uygulanmasının sağlaması bakımlarından, veri kontrolörüne, veri süjesinin bilgilendirilmesine ilişkin bazı yükümlülükler getirmiştir. Tüzük madde 12'de yer alan "*Bilgilendirme yükümlülüğüne*[371]" göre, veri kontrolörü, açık ve sade bir dille, kısa ve öz olarak hazırlanan, şeffaf, kolay anlaşılır, taşınabilir ve erişilebilir bir format kapsamında, veri süjesinin kişisel verilerinin işlenmesine ilişkin olarak, gecikmeksizin ve herhalikarda en geç bir ay içerisinde bilgilendirilmesine ve kendisi ile gerekli her türlü iletişimin sağlanmasına yönelik

[370] Google, "The Advisory Council to Google on the Right to be Forgotten", 6.2.2015, https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf (02.06.2020), p.7-14; W.Gregory Voss, Winter 2015-2016 ss. 282-283.

[371] Veri kontrolörünün "*Bilgilendirme yükümlülüğü*", kimi kaynaklarda veri süjesi perspektifinden ele alınarak "*Bilgilendirilmeyi talep hakkı*" olarak nitelendirilmiştir.

uygun tedbirleri almakla yükümlüdür. Bu bilgilendirme yazılı şekilde yapılabileceği gibi, anılan koşulları kapsayan başka herhangi bir şekilde de yapılabilir. Ancak uygulamada, ispat kolaylığı açısında, bu gibi bilgilendirmelerin yazılı olarak yapılmasının tercih edildiği görülmektedir. Veri süjesi ile bu bağlamda iletişime geçilmesi ve bilgilendirme yapılması prensip olarak ücretsiz olacaktır. Ancak veri süjesinin tekrarlayan, açıkça temelsiz ve aşırı sayılabilecek nitelikteki taleplerinin söz konusu olması durumunda, madde 12/5'te, somut olayın özelliklerine göre, veri kontrolörünün, idari masrafların karşılanabilmesi bakımından makul bir ücret talebinde bulunabileceği ya da ilgili talebi reddedebileceği de belirtilmiştir. Madde 12/6 kapsamında da, bilgi talebinde bulunan veri süjesinin kimliği konusunda makul şüphenin oluşması durumunda, veri kontrolörünün kimlik tespiti yapabilmek adına, veri süjesinden ek bilgi talep edebileceği hüküm altına alınmıştır. Veri süjesinin bilgilendirilmesine ilişkin olarak 12.madde kapsamında yapılan düzenlemenin uygulanması, özellikle de veri süjesinin çocuk olduğu durumlarda, temel hak ve özgürlüklerin korunması bağlamında büyük önem arz eder[372]. Tüzük kapsamında getirilen veri süjesinin bilgilendirilmesine ilişkin bu yükümlülük sayesinde, yapılacak bilgilendirmenin akabinde, veri süjesinin, hem hangi kişisel verilerinin, ne amaçlarla işlendiği hususundaki, hem de hangi verinin hangi mikroskobik parçasının kendisinden beklenmeyecek oranda kapsamlı bir veri analizine yol açabileceği hususundaki, farkındalığının artırılması hedeflenmektedir[373].

Tüzük'ün 13. ve 14.maddelerinde ise, kişisel verilerin doğrudan veri süjesinin kendisinden toplanıp toplanmaması dikkate alınarak, veri kontrolörüne adil ve şeffaf işleme faaliyetleri kapsamında getirilen bilgilendirme yükümlülüğünün içeriği ve diğer detaylar düzenlenmiştir.

Tüzük madde 13'e göre, kişisel verilerin doğrudan veri süjesinin kendisinden elde edildiği hallerde, veri süjesinin bilgilendirilmesi işbu verilerin toplanması esnasında yapılmalı ve şu hususları içermelidir: Kontrolörün ve varsa temsilcisinin kimliği ve iletişim detayları ile veri koruma görevlisinin irtibat bilgileri (*madde 13/1 a,b*); Yapılacak işleme faaliyetinin hedeflediği amaçlar ile dayandığı yasal temellerin

[372] GDPR Beyanlar 39, 58;
Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", **Computer Law and Security Review: The International Journal of Technology Law and Practice**, Cilt.34, Sayı.1, 2018, s. 139.
[373] Laura-Cristiana SPATARU-NEGURA, Cornelia Lazar s. 661.

neler olduğunu (*madde 13/1 c*); İşleme faaliyeti, kontrolörün ya da üçüncü kişilerin meşru menfaatlerinin korunması amacıyla yapıldığı taktirde, bu meşru amaçların neler olduğunu (*madde 13/1 d*); Kişisel verilerin tevdi edileceği alıcılar varsa, bu alıcıların kimler olduğunu (*madde 13/1 e*); Veriler üçüncü bir ülkeye veya uluslararası bir organizasyona transfer edilecekse, bu transfer işlemine ilişkin alınacak önlemlere ve transfer edilecek verilerin bir kopyasının veri süjesi tarafından nasıl elde edilebileceğine ilişkin bilgileri (*madde 13/1 f*).

Veri süjesine, saklama süresine ve bu sürenin belirlenmesinde kullanılacak kriterlere (*madde 13/2 a*); veri süjesinin erişim, düzeltme, silme, işlemenin kısıtlanmasını talep etme, itiraz etme ve veri taşınabilirliğini talep edebilme gibi haklarının bulunduğuna (*madde 13/2 b*); rızanın ne şekilde geri alınabileceğine (*madde 13/2 c*) ve bir denetim makamına şikayette bulunabilme hakkına (*madde 13/2 d*); veri süjesi için verileri sağlamanın yasal veya sözleşmesel bir zorunluluk olup olmadığına ve bu verileri sağlamamanın veri süjesi bakımından ortaya çıkarabileceği olası sonuçlara (*madde 13/2 e*); profilleme de dahil otomatik işleme yapılacağı hallerde, işlem mantığı ve veri süjesi açısından ortaya çıkabilecek olası sonuçlarına (*madde 13/2 f*), ilişkin gerektiğinde ek bilgilendirme de yapılabilecektir. Ayrıca Tüzük'ün 13/3.maddesine göre, toplama amacından başka bir amaçla verilerin işlenmesi hedeflendiğinde, kontrolörün veri süjesine, işleme faaliyetine başlamadan önce, bu yeni amaca ilişkin de bilgi verme yükümlülüğü bulunmaktadır.

2016/679 sayılı Tüzük'ün 14.maddesi kapsamında ise kişisel verilerin doğrudan veri süjesinden elde edilmediği hallerde, veri kontrolörünün veri süjesine yapacağı bilgilendirmenin hangi unsurları içermesi gerektiği sıralanmıştır. Bu madde incelendiğinde, veri süjesine yapılacak bu bilgilendirme metninin yukarıda anılanlara ek olarak, işlenecek kişisel verilerin kategorilerinin neler olduğu bilgisini de içermesi gerektiği anlaşılmaktadır (*madde 14/1 d*).

Tüm bu maddeler incelendiğinde, 2016/679 sayılı Tüzük madde 13 ve 14 ile, veri kontrolörüne getirilen bilgilendirme yükümlülüğünün nasıl yerine getirilmesi gerektiğine ilişkin kapsam ve koşulların, mülga 95/46 sayılı Direktif madde 10 ve 11 ile kıyaslandığından, şeffaflık ilkesinin etkili bir şekilde uygulanmasının gereği olarak, daha da detaylandırılarak güçlendirildiği anlaşılabilmektedir[374]. Kişisel

[374] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, ss. 139-140;

verilerin işlenmesinde bu yolla ulaşılmaya çalışılan adil, yasal ve şeffaf işleme hedeflerinin de doğal olarak Avrupa dijital tek pazarının, bu pazarda işlem yapacak tüketiciler için daha güvenilir olmasına katkıda bulunacağı öngörülmektedir.

3.5.7. Kişisel Verilerin İşlenmesinde İhlal Çeşitleri ve Güvenlik

Madde 29 Veri Koruma Çalışma Grubu, 2017 yılında, henüz 2016/679 sayılı Tüzük yürürlüğe girmeden önce, bu Tüzük çerçevesinde yapılacak veri ihlal bildirimlerine ilişkin bir rehber yayınlayarak, kişisel veri ihlal çeşitlerini üç kategori altında düzenlemiştir. Buna göre, kişisel verilere ilişkin olarak yetkisiz veya kazara yapılan her türlü ifşa yahut erişim "*gizlilik ihlali (confidentiality breach)*"; kişisel verilerin yetkisiz kişiler tarafından kazara imhası yahut kayıp edilmesi "*ulaşılabilirlik ihlali (availability breach)*"; kişisel verilerin yetkisiz kişilerce veya kazara değiştirilmesi faaliyeti ise "*bütünlük ihlali (integrity breach)*" olarak sınıflandırılmıştır[375].

2016/679 sayılı Tüzük'ün 32.maddesi kapsamında, kişisel verilerin işlenmesi sürecinde, ihlallerin önlenerek, makul ve kabul edilebilir bir seviyede veri güvenliğinin sağlanabilmesi için gerekli tedbirlerin alınmasına ilişkin, veri kontrolörü ve işleyicisine düşen sorumluluklar düzenlenmiştir[376]. 32.madde hükmü incelendiğinde, uygun teknik ve örgütsel tedbirleri alma yükümlülüğünün eskiye oranla genişletilerek, veri kontrolörünün yanı sıra işleyicinin de bu tedbirlerin alınmasından sorumlu olduğunun altının çizildiği görülmektedir. Buna göre; Takma ad kullanılması ve şifreleme yapılması (*madde 32/1 a*); Veri işlemeye ilişkin sistem ve hizmetlerin ihlal girişimlerine karşı, gizliliğinin, bütünlüğünün, kullanılabilirliğinin ve dayanıklılığının sürekliliğinin sağlanması (*madde 32/1 b*); Teknik veya fiziki bir müdahalenin gerçekleşmesi durumunda kişisel verilerin

---

Cedric Burton, Laura de Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot, Sara G.Hoffman "Privacy and Security Law Report, EU Regulation, The Final European Union General Data Protection Regulation", **Bloomberg BNA**, 2016, https://www.wsgr.com/images/content/2/7/v1/278/bloombergBNA-0116.pdf (02.06.2020), s.6.

[375] Article 29 Data Protection Working Party, Guidelines on Personal Data Breach Notification under Regulation 2016/679, 03.10.2017, **WP250 17/EN**, https://webcache.googleusercontent.com/search?q-=cache:X49fS0vPpRgJ:https://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D47741+&cd=1&hl=tr&ct=clnk&gl=tr&client=safari (02.06.2020), ss.6-8.

[376] Article 29 Data Protection Working Party, "Guidelines on Personal Data Breach Notification under Regulation 2016/679", s.5.

yeniden kullanılabilirliğinin ve erişilebilirliğinin sağlanması (*madde 32/1 c*); İşlem güvenliğinin devamlılığını sağlamak adına alınan tedbirlerin etkinliğinin düzenli aralıklarla kontrol edilerek değerlendirilmesi (*madde 32/1 d*), gibi uygulamalar, veri kontrolörü ve işleyicisinin, somut olayın özelliklerini, uygulama maliyetlerini, işleme faaliyetinin kapsam, içerik ve amaçlarını, olası riskleri birlikte göz önüne alarak, veri işleme sürecinin güvenliğinin sağlanması adına alabileceği, teknik ve örgütsel tedbirler kapsamında sayılabilirler.

Tüm bunların yanı sıra, Tüzük madde 32/4'e göre, veri kontrolörü ve işleyicileri, kişisel verilere erişim imkanı bulunan ve kendi yetki ve denetimleri altında çalışan kişilerin, kişisel verilerin işlenmesi hususunda, yalnızca kişisel verilerin korunmasına ilişkin yasa hükümlerine uygun şekilde verecekleri talimatlara göre işleme yapmalarını sağlamak adına gereken tedbirleri de almakla yükümlüdürler. Bu da veri kontrolör ve işleyicilerinin işbu Tüzük kapsamında sorumluluk ve yükümlülüklerinin artırıldığının bir başka somut kanıtı niteliğindedir [377].

2016/679 sayılı Tüzük madde 33 ile, kişisel verilerin işlenmesinde güvenliğin sağlanmasına yönelik olarak, veri kontrolörüne, ihlalin gerçekleştiğinin öğrenilmesini takiben, vakit geçirmeksizin ve herhalikarda ihlalin öğrenilmesinden itibaren 72 saat içerisinde, yetkili denetim makamının, bu durumdan haberdar edilmesi yükümlülüğü de getirilmiştir. Diğer bir ifade ile, veri kontrolörünün her türlü kişisel veri ihlalini, bu ihlalin etkilerini ve gerçekleşen ihlale karşılık alınan düzeltici önlemlerin neler olduğunu detayları ile birlikte kayıt altına alarak, ihlale ilişkin yetkili denetim makamını, bilgilendirme yükümlülüğü bulunmaktadır. En geç 72 saat içinde yapılması gereken bu bildirim ile, denetim makamının, hak kayıplarının önüne geçilmesi amacıyla, ihlale ilişkin gerekli ve yeterli tedbirlerin alınarak, yasal düzenlemelere uyulup uyulmadığının tespitine ilişkin, denetim görevini yerine getirebilmesi için uygun koşulların yaratılmasının da hedeflendiğini söylemek yanlış olmayacaktır. Kişisel veri ihlalinin, işleyici tarafından öğrenildiği durumlarda ise, işleyicinin de, veri kontrolörünü bu durumdan, gecikmeksizin haberdar etme yükümlülüğü bulunmaktadır. Yetkili denetim makamına, veri kontrolörü tarafından Tüzük madde 33 kapsamında yapılacak ihlal bildiriminin en

[377] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, s.143.

azından; "İhlal edilen, kişisel verilerin kategorileri, ihlale konu veri süjelerinin ve kişisel veri kayıtlarının kategorileri ile gerçekleşen ihlallerin -yaklaşık olarak- sayısı gibi unsurların tarifini (*madde 33/3 a*); Veri koruma görevlisinin veya daha fazla bilgi alınabilecek bir başka iletişim makamının adı ve iletişim bilgilerini (*madde 33/3 b*); İhlalin olası sonuçlarını (*madde 33/3 c*); Kontrolör tarafından ihlale ve olası etkilerine yönelik olarak halihazırda alınan ya da alınması önerilen tedbirlerin neler olduğu hususlarını (*madde 33/3 d*)", içermesi gerekmektedir[378].

Kişisel verilere yönelebilecek olası risklerin boyutları, işlenen kişisel verinin niteliği ile işlemenin kapsam ve niteliğine, kullanılan teknolojiye göre değişiklik gösterebilmektedir. Bu doğrultuda Tüzük ile, kişisel verilerin işlenmesi kapsamında gerçekleşen ihlalin, veri süjesinin temel hak ve özgürlüklerine ilişkin büyük risk oluşturduğu hallerde, salt madde 33 kapsamında veri kontrolörü tarafından denetim makamına ihlal bildiriminde bulunulmasının yeterli olmayacağı kabul edilmiştir. Bu sebeple, ihlalin veri süjesinin temel hak ve özgürlükleri bakımından yüksek risk içermesi durumunda, Tüzük'ün 34.maddesi kapsamında, veri süjesinin de bu ihlalin kapsam ve niteliğine, ihlalin önlenmesi için alınacak tedbirlere ilişkin olarak veri kontrolörü tarafından kolay anlaşılır şekilde, açık ve sade bir dille gecikmeksizin bilgilendirilmesi şartı getirilmiştir[379].

Tüzük'ün 34/3.maddesi kapsamında sayılan koşullardan herhangi birinin yerine getirilmesi durumunda ise veri kontrolörü, veri süjesini bilgilendirme yükümlülüğünden muaf tutulabilecektir. Muafiyet halleri 2016/679 sayılı Tüzük'ün madde 34/3 kapsamında sayılmıştır. Buna göre, "kontrolörün, kişisel verilerin veri süjesi ile bağını şifreleme gibi koruma tedbir ve yöntemleriyle kesmesi sebebiyle, ihlalin veri süjesinin kimliğini ortaya çıkaramadığı durumlar (*madde 34/3 a*); veri kontrolörünün ihlalin gerçekleşmesinden sonra aldığı tedbirler neticesinde temel hak ve özgürlükleri tehdit eden koşulların ortadan kalktığı durumlar (*madde 34/3 b*); veri süjelerinin halka açık genel bir bilgilendirme vasıtasıyla haberdar edilmesi durumu (*madde 34/3 c*)", muafiyet halleri kapsamında sayılmıştır.

---

[378] W.Gregory Voss, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting", **Business Lawyer**, Cilt.72, Sayı.1, Winter 2016-2017, s.229.

[379] GDPR Madde 34/1,2; European Union, European Union Agency for Fundamental Rights, 2018, s.179.

Kişisel verilerin yetkisiz, yasadışı ve kazara kullanım, imha, ifşa, kayıp ve tahrip edilmesi, erişilmesi, yayılması, saklanması ve değiştirilmesinin engellenmesi amacıyla 2016/679 sayılı Tüzük kapsamında yapılan anılan düzenlemeler, veri güvenliğinin sağlanması ve dolayısı ile de temel hak ve özgürlüklerin korunması bağlamında büyük önem taşımaktadırlar. Bunun bilinciyle, Tüzük kapsamında, hesap verebilirlik ilkesi doğrultusunda, risk yönetimi yapılarak, kişisel verilerin işlenmeleri sürecinde, ihlallerin önlenerek işlem ve veri güvenliğinin sağlanmasına yönelik uygun ve yeterli tedbirlerin alınmasına çalışılmıştır. Alınan bu tedbirlerin, veri güvenliğine olduğu kadar, tamamlanmaya çalışılan Avrupa dijital tek pazarında, işlem güvenliğinin sağlanmasına da olumlu etki ederek, neticede de işlem hacminin yükselmesinin sağlanacağı düşünülmektedir.

3.5.7.1. Veri Koruma Etki Değerlendirmesi

2017 yılında, Madde 29 Veri Koruma Çalışma Grubu, 2016/679 sayılı Tüzük'te düzenlenen veri koruma etki değerlendirmesinin tanım ve kapsamına ilişkin bir rehber yayınlamıştır. Bu rehbere göre, "*veri koruma etki değerlendirmesi*", kişisel verilerin işlenmesinde, işlemenin amacının, gerekliliğinin ve oranının belirlenerek, işleme sürecinin tanımlanmasına ve kişisel verilerin işlenmesinden kaynaklanabilecek ihlallerin öngörülüp, olası olumsuz etki ve sonuçlarının en aza indirilmesini sağlayacak tedbirlerin alınmasına, olanak verecek şekilde risk analizi ve yönetiminin hedeflendiği, değerlendirme, öngörü ve 2016/679 sayılı Tüzük'ün getirdiği hükümlere uygunluk oluşturma süreci olarak tanımlanabilir. Bu bağlamda veri koruma etki değerlendirmesi yapılmasının, hem kişisel verileri işlenen veri süjeleri, hem de bu işleme faaliyetini gerçekleştiren tüzel kişiler açısından bazı avantajları olduğu söylenebilir. Zira veri koruma etki değerlendirmesi yöntemi vasıtasıyla olası risklerin henüz gerçekleşmeden elenmesi yolu ile, hem veri süjeleri açısından temel hak ve özgürlüklerin daha iyi korunmasının sağlanmasının, hem de 2016/679 sayılı Tüzük'ün hükümlerine uyulmaması sebebiyle kesilecek idari para cezalarının engellenmeye çalışılmasının hedeflenmekte olduğu söylenebilir[380].

[380] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is '*Likely to result in a High Risk*' for the Purposes of

Teknolojik gelişmelere paralel olarak kapsamı, nitelik ve niceliği günden güne gelişerek artan otomatik veri işleme teknik ve süreçleri, ekonomik gayelerin gerçekleştirilmesine yönelerek, öncelikli olarak temel hak ve özgürlüklerin korunmasını hedeflemedikleri için, bu otomatik işlemelerden kaynaklanan kişisel veri ihlalleri de doğal olarak artmıştır. Bu gelişmeler, kişisel verilerin işlenmesine başlanmadan önce, amaçlanan işlemenin olası etki ve sonuçlarının incelenerek, risk analizi yapılmasının akabinde, ortaya çıkabilecek muhtemel ihlallere karşı alınacak tedbirlerin belirlenmesi bağlamında, Tüzük'ün 35.maddesi ile ortaya konan veri koruma etki değerlendirmesinin önemini bir kere daha ortaya koymaktadır. 2016/679 sayılı Tüzük'ün 35/1.maddesinden anlaşılacağı üzere, ileri teknoloji kullanılarak yapılan ve doğası, kapsamı, içeriği ve amaçları gereği, veri süjesinin hak ve özgürlüklerinin yüksek olasılıkla ihlali neticesini doğurabilecek nitelikteki, işleme faaliyetlerine başlanmasından önce, veri kontrolörü tarafından, veri koruma etki değerlendirmesinin yapılması zorunludur. Bu sayede önceden alınacak tedbirler vasıtasıyla, kişisel verilerin işlenmesi neticesinde ortaya çıkabilecek olumsuz sonuçların öngörülerek, engellenmesi yahut en aza indirilmesi hedeflenmektedir[381]. Ancak her ne kadar madde 35/1'in lafzından, veri koruma etki değerlendirmesinin veri kontrolörü tarafından işleme faaliyetine başlanmasından önce yapılması gerektiği anlaşılsa da, aslında veri koruma etki değerlendirmesinin sadece bir kereye mahsus yapılması gereken bir prosedür değil, riskin ortaya çıkma ihtimalinin olduğu herhangi bir zamanda da tekrarlanabilecek bir süreç olduğu unutulmamalıdır[382].

Tüzük'ün 35/3.maddesi kapsamında ise, veri koruma etki değerlendirmesinin mutlaka yapılması gereken özel durumlar sayılmıştır. Madde 35/3'e göre, "profilleme yapılması da dahil olmak üzere, kişilik özelliklerine dair kapsamlı

Regulation", 2016/679, 13.10.2017, **17/EN WP 248** rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (02.06.2020), s.4.

[381] European Union Agency for Fundamental Rights, 2018, ss.179-181;
Felix Bieker, Michael Fiedewald, Marit Hansen, Hannah Obersteller, Martin Rost, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation", **Privacy Technologies and Policy** (Ed. S.Schiffner et.al), Annual Privacy Forum, Springer International Publishing, Switzerland, 2016, ss.21-22, 24-25;
Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is '*Likely to result in a High Risk*' for the Purposes of Regulation 2016/679, s.8.

[382] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is '*Likely to result in a High Risk*' for the Purposes of Regulation 2016/679, **WP248REV.01**, s.14.

inceleme yapılmasına ilişkin olan otomatik işleme faaliyetleri ile, otomatik işleme faaliyetlerinin sonuçlarının veri süjesi hakkında yasal etkiler doğurabilecek nitelikteki önemli kararların alınmasında kullanılacak olması durumu (*madde 35/3 a*); Tüzük'ün 9/1.maddesinde ifade edilen hassas kişisel verilere ilişkin işleme faaliyetleri ile, yine Tüzük'ün 10.maddesinde belirtilen cezai hüküm ve suçlara ilişkin işleme faaliyetleri *(madde 35/3 b*); ve, halka açık alanların sistematik bir şekilde ve geniş ölçekte izlenmesine ilişkin işleme faaliyetleri (*madde 35/3 c*)", veri koruma etki değerlendirilmesinin mutlaka yapılmasının gerektiği özel durumlar kapsamında sayılmıştır. Yine 2016/679 sayılı Tüzük madde 35/4'e göre, hangi veri işleme faaliyetleri öncesinde mutlaka bir veri koruma etki değerlendirmesi yapılmasının gerektiği hususu, yetkili denetim makamınca özel olarak belirlenip, kamuoyuna açıklanarak, bu konuda Avrupa Veri Koruma Kurulu'nu da bilgilendirmelidir. Denetim makamının veri koruma etki değerlendirmesi yapılmasına gerek olmayan işleme faaliyetlerinin neler olduğuna ilişkin de bir liste oluşturarak kamuoyunu bilgilendirebileceği hususu da madde 35/5 kapsamında belirtilmiştir. Yapılan veri koruma etki değerlendirmesi neticesinde, işleme faaliyetinin önlem alınmaması halinde, veri süjesi açısından yüksek risk oluşturacağı sonucuna ulaşılması halinde, işleme faaliyetine başlanmadan önce, veri kontrolörünün, denetim makamını bu hususta bilgilendirerek, izlenecek yola ilişkin olarak denetim makamına danışması gerektiği hususunun altı da Tüzük madde 36 ile çizilmiştir[383].

3.5.8. Kişisel Verilerin Korunmasında Yetkili Makamlar

2016/679 sayılı Tüzük madde 4/7 kapsamında, "*veri kontrolörü (controller)*", kişisel verilerin işlenme amaç ve araçlarını tek başlarına veya diğerleriyle birlikte belirleyen, gerçek veya tüzel kişi(ler), kamu otoriteleri ya da başka herhangi bir kurum şeklinde tanımlanmıştır. 2016/679 sayılı Tüzük'ün 24.maddesi kapsamında kontrolörlerin sorumlulukları düzenlenmiştir. Buna göre, kontrolörler, kişisel

[383] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, s. 143;
Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is '*Likely to result in a High Risk*' for the Purposes of Regulation 2016/679, s.18.

verilerin işlenmesinde, işleme faaliyetinin niteliğini, kapsamını, içeriğini, hedeflediği amaçları ve temel hak ve özgürlükler açısından yaratabileceği olası riskleri göz önünde bulundurarak, 2016/679 sayılı Tüzük'ün getirdiği hükümler kapsamında, en uygun teknik ve örgütsel tedbirleri alarak, gerektiği taktirde bu tedbirleri gözden geçirerek güncellemekle yükümlüdürler.

"*İşleyici (processor)*", Tüzük'ün 4/8.maddesinde, kişisel verilerin korunması için gerekli ve yeterli teknik ve örgütsel tedbirleri almalarına ve böylelikle veri süjesinin hak ve özgürlüklerinin en iyi şekilde korunmalarını garanti etmelerine müteakip, veri kontrolörleriyle aralarında yapacakları sözleşme gereği, veri kontrolörü adına kişisel verileri işleyen, gerçek veya tüzel kişi(ler), kamu otoriteleri ya da başka herhangi bir kurum olarak tanımlanmaktadır. İşleyicinin, kontrolörün önceden verilmiş özel ve yazılı onayı olmadan bir başka işleyici ile çalışamayacağı hususu Tüzük'ün 28.maddesi kapsamında düzenlenmiştir. Bu düzenleme, kişisel verilerin işlenmesinde görevlendirilebilecek işleyicilerin, mutlaka kontrolör tarafından seçilerek onaylanmaları gerektiği hususunu ortaya koymaktadır. Ayrıca aynı madde kapsamında kontrolör ve işleyicinin aralarında yapacakları sözleşmenin Birlik hukuku ya da ilgili üye devlet hukuku kapsamında bağlayıcı nitelikte olmasının gerektiğinin de altı çizilmiştir. Kontrolör ve işleyicinin aralarında akdedecekleri işbu sözleşmede, işleme faaliyetine ilişkin işleme amacı ve süresi, hangi tip kişisel verilerin işlenebileceği, kontrolörün hak ve yükümlülükleri gibi her türlü detay belirlenebilecektir. Diğer bir ifade ile, işleyici, kişisel verileri, kontrolör adına, yalnızca kontrolörün işbu sözleşme çerçevesinde vereceği talimatlar doğrultusunda işlemekle yükümlüdür.

Bulut servis sağlayıcıları ile dijital ağ oluşturan ya da bilişim teknolojileri üreten diğer teknoloji sağlayıcıları ve veri merkezleri, veri işleyicilere örnek olarak verilebilir. Tüzük kapsamında yapılan tanımlar incelendiğinde, 2016/679 sayılı Tüzük ile, kontrolör ve işleyiciye ilişkin tanımlamaların değiştirilmediği ancak, bunların sorumluluklarının kapsam ve içeriklerinin genişletildiği görülmektedir. Nitekim, Tüzük ile, kişisel verilerin işlenmesinde, veri işleyicilerine de kontrolörler ile aynı seviyede sorumluluk yüklenmiş ve kişisel verilerin korunması hususunda,

Tüzük kapsamında ortaya çıkabilecek hukuka aykırılıklardan, kontrolör ve işleyici birlikte sorumlu tutulmuşlardır[384].

2016/679 sayılı Tüzük kapsamında, kişisel verilerin işlenmesi faaliyetlerinin gerçekleştiği kurum ya da kuruluşlara, hesap verebilirlik ilkesi çerçevesinde bu faaliyetlerin yasallığının ve Tüzük'e uygunluğunun garanti edilmesi için gerekli adımların atılarak, önlemlerin alınması amacıyla tavsiyelerde bulunmak üzere, kontrolör veya işleyici tarafından, "*veri koruma görevlisi (data protection officer)*" atanabileceği belirtilmiştir. Veri koruma görevlisi atanması hususu, ilk kez 2016/679 sayılı Tüzük ile, Birlik düzeyinde doğrudan uygulanabilir bir yasal düzenleme ile getirilmiş bir yeniliktir [385].

Tüzük'ün 37.maddesi kapsamında yapılan düzenleme ile kimi durumlarda veri kontrolörü ve işleyicisine, zorunlu olarak bir veri koruma görevlisi atamaları yükümlülüğü de getirilmiştir. Örneğin, büyük miktarlarda kişisel verinin depolandığı ve işlenerek profilleme, çevirimiçi davranışsal reklamcılık da dahil olmak üzere çeşitli şekillerde kullanıldığı Instagram, Facebook gibi sosyal medya platformları ile; hassas kişisel verilerden sayılan sağlık verileri ile genetik ve biyometrik verilerin depolanarak sistematik olarak işlendiği devlet hastaneleri gibi sağlık kuruluşlarına, Tüzük'ün 37/1.maddesi kapsamında getirilen yeni düzenleme gereği, veri kontrolörü ve işleyicisi tarafından, veri koruma görevlisi atanması zorunludur[386].

Tüzük'ün 37.maddesine göre; Yargılama yetkileri kapsamında hareket eden mahkemeler hariç olmak üzere, kişisel verilerin işlenmesinin bir kamu kurum ya da makamı tarafından gerçekleştirilmesi durumunda (*madde 37/1 a*); Veri kontrolörü veya işleyicinin esas faaliyet alanının, kişisel verilerin büyük ölçekte toplanarak,

---

[384] GDPR Beyanlar 13; Hazel Grant, Amy Lambert, Kate Pickering, "Data Protection Day-Data Processors and the GDPR", **LexisNexis,** 2016 https://www.lexology.com/library/detail.aspx?g=3477a69d-812f-45d2-93f4-49f60cf946ce (02.06.2020);
Ayşe Nur Akıncı, s.14; Jenna Lindqvist, "New Challenges to Personal Data Processing Agreements: is the GDPR Fit to Dealwith Contract, Accountability and Liability in a World of the Internet of Things", **International Journal of Law and Information Technology**, Cilt.26, Sayı 1, 2017, ss. 46-48.

[385] Veri koruma görevlisi kavramı, kimi üye devletler için Avrupa Birliği Genel Veri Koruma Tüzüğü ile ilk kez getirilen yeni bir uygulama ise de bu terimin 1977'deki çıkış noktasını oluşturan Almanya gibi diğer bazı üye devletler bu kavrama daha önceden aşinadır. Veri koruma görevlisi makamının, 2016/679 sayılı Tüzük'ten önceki dönemde, bazı üye devletlerdeki varlığına ilişkin daha fazla bilgi için bkz. Miguel Recio, "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability, Practitioner's Corner", **European Data Protection Law Review**, Cilt.3, Sayı.1, 2017, ss. 114-118.

[386] European Union Agency for Fundamental Rights, 2018, s.176.

düzenli ve sistematik olarak izlenip işlenmelerini gerektiren faaliyetleri kapsadığı hallerde (*madde 37/1 b*); Hassas veriler ile cezai suç ve mahkumiyetlere ilişkin kişisel verilerin büyük ölçekte işlenmeleri durumlarında (*madde 37/1 c*), veri kontrolörü veya işleyicisi tarafından yapılan işleme faaliyeti kapsamında bir veri koruma görevlisi atanması zorunluluk arz eder. Bu durum, ilk kez 2016/679 sayılı Tüzük madde 37/1 ile ortaya konan yasal bir zorunluluktur[387]. Madde 37/1'de sayılanların dışındaki başka işleme faaliyetleri kapsamında da, gerekli görüldüğü taktirde, üye devletler ya da Birlik tarafından zorunlu olarak bir veri koruma görevlisi atama yükümlülüğü getirilebileceğinin altı da madde 37/4 ile çizilmiştir.

Veri koruma görevlileri, aynı zamanda adlarına işlem yaptıkları kurum ve kuruluşlar ile denetim makamları ve veri süjeleri arasında arabuluculuk yaparak karşılıklı iletişimin sağlanmasına da katkıda bulunurlar[388]. Tüzük madde 37/5 ile, veri koruma görevlisinin hangi alanlarda uzman kişiler arasından seçilerek atanması gerektiğine ilişkin bir açıklama getirilmediği görülmektedir. Ancak, veri kontrolörü ve işleyicisi tarafından atanacak veri koruma görevlisinin, kişisel verilerin korunmasına ve özellikle de 2016/679 sayılı Tüzük'ün yorumlamasına ilişkin mesleki yeterliliğe sahip uzman kişiler arasından seçilmesinin uygun olacağı anlaşılmaktadır. Veri koruma görevlisinin, görevlerini yerine getirirken, kişisel verilerin işlenmesinden etkilenen veri süjesinin de görüşünü alması önemlidir[389]. Yine Tüzük'ün 37/7.maddesine göre, şeffaflık ve hesap verebilirlik ilkeleri doğrultusunda, veri koruma görevlisinin iletişim bilgilerinin yayınlanması ve bu bilgilerin denetim makamına da bildirilmesi gerekmektedir. İletişim bilgilerinin, gerektiğinde veri süjesi veya denetim makamının, veri koruma görevlisine rahatlıkla ulaşabilmelerini sağlayacak kapsam ve yeterlilikte bilgi içermesi önemlidir[390].

Kişisel verilerin korunması hususunda bir diğer yetkili makam ise Tüzük'ün 51 ila 63.maddeleri arasında yapılan düzenlenen "*denetim makamları (supervisory*

---

[387] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ("DPOs") Adopted on 13 December 2016, **16/EN WP 243**, https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A (02.06.2020) ss.4-5; Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, s.149.

[388] European Union Agency for Fundamental Rights, 2018, ss.175-176.

[389] Felix Bieker, Michael Fiedewald, Marit Hansen, Hannah Obersteller, Martin Rost, s. 31;
Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ("DPOs") Adopted on 13 December 2016, s.11.

[390] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ("DPOs") Adopted on 13 December 2016, s.12.

authorities)"dır. Denetim makamlarının üstlenecekleri yetki ve görevlerle, kişisel verilerin korunması bağlamında, Tüzük'ün uygulanmasını denetleyerek, temel hak ve özgürlüklerin korunmasına ve verilerin Birlik içerisindeki serbest dolaşımlarının sağlanmasına katkıda bulunmaları hedeflenmektedir. Bu hedeflerin gerçekleştirebilmesi amacıyla da, her bir üye devletin, kendi bünyesinde ulusal yasaları ile kuracağı ve hiçbir makamdan doğrudan ya da dolaylı bir şekilde talimat almamasının garanti edilerek, bağımsızlıkları, yetki ve yetkinlikleri bu yasalar kapsamında teyit edilip korunan, bir ya da daha fazla bağımsız denetim makamı oluşturma sorumlulukları bulunmaktadır. Denetim makamlarının bağımsız karakterinin niteliği, bu makamların görev ve sorumluluklarını yerine getirirken, herhangi bir siyasi ya da ticari kaynaktan gelebilecek doğrudan veya dolaylı her türlü baskı ve etkiden uzak kalarak, ulusal çıkarlardan da bağımsız hareket edebilmelerinin sağlanması olarak açıklanabilir. Üye devletler, bu hususta kendilerine düşen sorumlulukları yerine getirerek, denetim makamlarının oluşturulmasına ilişkin ulusal yasaları hazırlarken, bu makamların bağımsızlıklarının temini için gereken düzenlemeleri yapmakla da yükümlüdürler. Ayrıca, sorumlulukları bağlamında kişisel verilerin korunması sisteminin esaslı unsurlarından olan ve görevlerine ilişkin mesleki yetkinliğe sahip kişilerden oluşturulacak olan bu denetim makamları, üye devletler arasında koordineli çalışarak, Birlik çapında, kişisel verilerin Tüzük kapsamında etkili bir şekilde korunup korunmadığını denetlemekle yükümlüdürler[391]. Denetim makamlarının bağımsız karakterlerinin korunarak, hiçbir mevki ve makamdan emir ve talimat almayacak olmalarının altının her fırsatta çizilmesi, Avrupa Birliği'nin köklerinde yatan etik değerlerinden olan temel hak ve özgürlüklerin korunmasına verdiği önemi açıkça ortaya koyar niteliktedir.

Avrupa Adalet Divanı da vermiş olduğu C-518/07 sayılı ve 2010 tarihli kararında, kişisel verilerin korunarak özel hayatın gizliliğinin güvence altına alınması ile bu verilerin serbest dolaşımlarının sağlanması arasında adil bir dengenin kurulması doğrultusunda, denetim makamlarının üstlenmiş oldukları görev ve

[391] European Union Agency for Fundamental Rights, 2018, ss.188-189;
Damien Geradin, Nicolas Petit, "The Development of Agencies at EU and National Levels: Conceptual Analysis and Proposals for Reform", **Jean Monnet Working Paper**, 01/04, 2004, https://papers.ssrn.com-/sol3/papers.cfm?abstract_id=489722 (02.06.2020), ss.49-50.

sorumluluklarını hakkıyla yerine getirebilmeleri amacıyla bu makamların içeriden ya da dışarıdan gelebilecek, doğrudan ya da dolaylı her türlü siyasi baskı ile piyasa etkisinden uzakta tutularak, tam bağımsızlıklarının üye devletler tarafından yapılacak yasal düzenlemeler vasıtasıyla sağlanmasının gerek ve önemini vurgulamıştır[392]. Bu karar 95/46 sayılı mülga Direktifin yürürlükte olduğu dönemde alınmış eski bir karar olsa da denetim makamlarının bağımsızlıklarının sağlanmasının kişisel verilerin korunmasındaki önemini ortaya koyması bakımında oldukça önemlidir.

Denetim makamlarının tam bağımsızlığının temini ile, hem Birlik çapında yeni bir yasal düzenleme olan 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün üye devletler tarafından kabul, uyum seviyesinin yükseltilmesi, hem de kişisel verilerin korunması hususunda üye devletler arasında eşgüdümün artırılması sağlanarak, neticede de tek pazarın bütünleşmesinin teşvik edilmesinin amaçlandığı söylenebilir[393].

Denetim makamlarının, görevleri Tüzük madde 57 kapsamında sıralanmıştır. Buna göre, "denetim makamlarının, kişisel verilerin korunması hususunda, Tüzük'ün uygulanmasını izleme ve denetleme görevleri dışında başka bazı görevleri de bulunmaktadır. Çocuklara ilişkin veriler başta olmak üzere, kişisel verilerin işlenmesinde ortaya çıkabilecek riskler ile Tüzük'ün getirdiği hak ve özgürlükler konularında, kamuoyunun bilgi ve farkındalığının artırılmasına katkıda bulunma (*madde 57/1 b*); Ulusal parlamentolara, hükümetlere ya da diğer kurumlara işleme faaliyetleri sırasında veri süjelerinin hak ve özgürlüklerinin korunması için alınabilecek idari tedbirlere ilişkin tavsiyelerde bulunma (*madde 57/1 c*); Tüzük kapsamındaki yükümlülüklerine ilişkin olarak, veri kontrolörleri ile işleyicilerinin farkındalıklarını artırma (*madde 57/1 d*); Talepleri halinde kişisel verilerinin işlenmesi hususundaki haklarına ilişkin veri süjelerine bilgi sağlama (*madde 57/1 e*); Veri süjesi veya başka bir kuruluş tarafından yapılan şikayetleri ele alarak soruşturma ve bu soruşturmanın gidişatı ya da sonucu hakkında ilgilileri bilgilendirme (*madde 57/1 f*); Kişisel verilerin korunmasına etki edebilecek

[392] Judgment of the Court of Justice (Grand Chamber), **ECJ C-518/07**, 9 March 2010, European Commission supported by European Data Protection Supervisor v. Federal Republic of Germany, http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5404007 (02.06.2020);
Saskia Lavrijssen, Annetje Ottow, "Independent Supervisory Authorities: A Fragile Concept", **Legal Issues of European Integration**, Cilt.39, Sayı.4, 2012, ss. 434-437.
[393] Saskia Lavrijssen, Annetje Ottow, ss. 423-427.

teknolojik gelişmeleri ve ticari faaliyetleri takip etme (*madde 57/1 i*)", gibi hususlar, denetim makamlarının diğer görevleri arasında sayılabilir.

Denetim makamlarının, görevlerini yerine getirebilmek adına gerektiğinde kullanabilecekleri yetkileri ise, soruşturma yetkileri (*madde 58/1: investigative powers*), düzeltici yetkileri (*madde 58/2: corrective powers*) ile yetkilendirmede bulunabilme ve danışmanlık yapabilme yetkileri (*madde 58/3: authorisation and advisory powers*) olmak üzere üç başlık altında sınıflandırılarak Tüzük madde 58'de detaylı bir şekilde sayılmışlardır. "Veri kontrolörü ve işleyicisinden görevlerini yerine getirebilmek için gerekli her türlü bilgiyi talep edebilme (*madde 58/1 a*); Veri koruma denetimleri formunda yapılacak soruşturmaları yürütme (*madde 58/1 b*); Tüzük'ün ihlal edildiğine ilişkin iddiaları kontrolör veya işleyiciye bildirme (*madde 58/1 d*); Görevlerinin ifasına ilişkin her türlü bilgiyi kontrolör veya işleyiciden temin edebilme (*madde 58/1 e*); Kontrolör veya işleyicinin görev yaptıkları tesis ve buralardaki ekipmanlara yasalar dahilinde erişim sağlayabilme (*madde 58/1 f*); Kontrolör ve işleyiciyi, gerçekleştirecekleri veri işleme faaliyetinin, işbu Tüzük hükümlerini muhtemelen ihlal edebileceğine ilişkin uyarma (*madde 58/2 a*); Kontrolör veya işleyiciye, işleme faaliyetlerinin, belirtilen şekilde ve belirli bir süre içinde, Tüzük hükümlerine uygun hale getirilmesini emretme (*madde 58/2 d*), Kontrolöre, kişisel veri ihlaline ilişkin veri süjesiyle iletişime geçmesini emretme (*madde 58/2 e*); İşleme yasağı da dahil olmak üzere, kesin ya da geçici nitelikte sınırlamalar getirme (*madde 58/2 f*); Kişisel verilerin düzeltilmesini ya da silinmesini emretme (*madde 58/2 g*)", denetim makamlarının 58.madde kapsamında sayılan yetkilerine örnek olarak verilebilir.

2016/679 sayılı Tüzük'ün 59.maddesi kapsamında da, denetim makamlarının, ihlal bildirimleri ve alınan tedbirlerle ilgili bilgileri de kapsayan, tüm görev ve yetkilerine ilişkin, yıllık faaliyet raporları hazırlamakla yükümlü oldukları belirtilmiştir. 59.maddeye göre, bu raporlar, her bir denetim makamının kendi ulusal kuruluş yasasında belirtilen makamlara iletileceği gibi; kamunun, Komisyon'un ve Avrupa Veri Koruma Kurulu'nun erişimine de açık tutulacaklardır. Denetim makamlarının faaliyetlerine ilişkin olarak sunmak zorunda oldukları yıllık raporlar ile, 2016/679 sayılı Tüzük'ün uygulanmasında şeffaflık ve hesap verebilirlik ilkelerine uygun hareket edilmesinin sağlanmaya çalışıldığı anlaşılmaktadır.

Tüzük'ün getirdiği bir başka yenilik de, madde 68 kapsamında tüzel kişiliğe haiz bir Birlik organı olan "*Avrupa Veri Koruma Kurulu (European Data Protection Board)*"nun kurularak, "*Madde 29 Çalışma Grubu (Article 29 Working Group)*"nun yerini almasıdır[394]. Herhangi bir kurum veya makamdan emir ya da talimat almaksızın bağımsız bir şekilde Tüzük'te belirtilen görevlerini yerine getiren (*madde 69*), Avrupa Veri Koruma Kurulu, her üye devletin denetim makamlarının başkanı ile "*Avrupa Veri Koruma Baş Denetçisi (European Data Protection Supervisor)*" veya bunların temsilcilerinden oluşur (*madde 68/3*). Avrupa Veri Koruma Kurulu'nun faaliyet ve toplantılarına Komisyon da, oy hakkı olmayan bir temsilci vasıtasıyla katılabilecektir (*madde 68/5*).

Avrupa Veri Koruma Kurulu'nun yetki ve görevlerinin temelleri, 2016/679 sayılı Tüzük'ün Birlik genelinde tutarlı ve doğru bir şekilde yorumlanarak, yeknesak uygulanmasının sağlanması hedefi ile kişisel verilerin korunmasında denetim makamları arasında etkili işbirliğinin gerçekleştirilmesi hedefinde yatmaktadır[395]. Bunu temin için de, Avrupa Veri Koruma Kurulu, Tüzük'ün 70.maddesi kapsamında sayılan, çeşitli konularda Komisyon'a danışmanlık yapma; Tüzük'ün yorumlanıp uygulanmasına yönelik çeşitli rehber ve tavsiyeler yayınlama ile bunların uygulanmasını denetleme; Üye devletler arasında işbirliği ve bilgi paylaşımını teşvik etme; Denetim makamları ve mahkemeler tarafından tutarlılık mekanizmasına ilişkin olarak alınan kararlarla ilgili kamuya açık dijital sicil tutma, gibi çeşitli görevleri yerine getirmekle yükümlüdür. Madde 70/1 (t)' ye göre ise, Avrupa Veri Koruma Kurulu'nun, Tüzük'ün 65.maddesi kapsamında, bireysel vakalara ilişkin uyuşmazlıkların çözümüyle ilgili olarak aldığı kararlar ile; hak kayıplarının önüne geçilebilmesi amacıyla Tüzük madde 66 ile düzenlenen "*acil durum prosedürü (urgency procedure)*" kapsamında aldığı kararlar, bağlayıcıdır.

Tüzük'ün kabulünden önceki dönemde, kişisel verilerin sınırlar arası ihlallerine ilişkin, benzer konularla ilgili olarak farklı üye devletlerde verilen, farklı kararlar bulunmakta idi. Bu durum göz önüne alındığında, Tüzük'ün 63 ve 64. maddelerinde bahsedilen "*tutarlılık mekanizması (consistency mechanism)*"nın

[394] Andra Giurgiu, Gerard Lommel, "A New Approach to EU Data Protection, More Control Over Personal Data and Increased Responsibility", **Critical Quarterly for Legislation and Law**, Cilt. 97, Sayı. 1, 2014, s.26.
[395] GDPR Beyanlar 135.

önemli parçalarını oluşturan, denetim makamları ile Avrupa Veri Koruma Kurulu'nun, Birlik genelinde Tüzük'ün yeknesak bir şekilde uygulanması çabalarına, önemli katkılarda bulunacağı daha net bir şekilde anlaşılmaktadır. Zira Tüzük ile yapılan düzenleme ile, birden fazla üye devleti ilgilendiren sınır aşan sorunların çözümünde üye devletlerde bulunan denetim makamlarına, Avrupa Veri Koruma Kurulu'nun görüşünü bekleme yükümlülüğü getirilmiştir[396]. Bu güçlendirilmiş işbirliği formülü ile hesap verebilirlik ilkesi doğrultusunda, benzer konularda, birbiriyle tutarlı kararlar alınarak, kişisel verilerin yeknesak uygulamalarla korunması sağlanıp, tek pazarın güvenilirliğine katkıda bulunulması da hedeflenmektedir. Bu durumun uzun vadede, tüketici güvenini yükseltip, Avrupa dijital tek pazarındaki işlem hacmini artırarak, ekonomik büyümeye katkıda bulunacağı unutulmamalıdır[397].

3.5.9. Kişisel Verilerin Üçüncü Ülke ve Uluslararası Organizasyonlara Aktarımı

Bir ticari değer olduğu genel kabul gören verilerin serbest dolaşımlarının sağlanmasına ilişkin düzenlemeler, Birlik'in kuruluşundan itibaren ortaya konan temel değerler göz önüne alındığında şaşırtıcı değildir. Buna paralel olarak da, 2016/679 sayılı Tüzük, kişisel verilerin Birlik düzeyinde uyumlaştırılmış yasalar dahilinde en iyi şekilde korunarak, verilerin Avrupa Birliği sınırları içerisinde serbest dolaşımlarının teminini ilke edinmiştir. Küreselleşmenin etkileri ile uluslararası ticaret hacminin artması ve dijital teknolojilerin hızlı gelişimiyle birlikte, kişisel veriler, Birlik dışındaki üçüncü ülkelere ve uluslararası organizasyonlara her geçen gün daha da artan oranlarda aktarılarak, Birlik dışındaki çeşitli sunucular (*serverlar*) aracılığıyla, depolanıp işlenmeye başlanmışlardır. Engellenemeyen bir şekilde, yüksek miktarlara ulaşan bu veri aktarımları, beraberinde kişisel verilerin Birlik sınırları ötesinde de korunmalarının garanti altına alınması ihtiyacını ortaya çıkarmıştır. Ortaya çıkan bu ihtiyaç sebebiyle de, Tüzük kapsamında, veri aktarımı yapılacak üçüncü ülke veya uluslararası organizasyonlar tarafından, kişisel verilerin,

[396] Nilgün Başalp, 2015, ss. 86-87.
[397] Giovanni Buttarelli, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard", Guest Editorial, **International Data Privacy Law**, Cilt.6, Sayı.2, 2016, s.77.

Birlik düzeyinde korunmasının garanti edilmesi kaydıyla, buralara kişisel verilerin aktarımına, belli koşullar altında Komisyon tarafından izin verilebileceği düzenlenmiştir. Kişisel verilerin tıpkı Birlik içinde olduğu gibi, aynı seviyede korunmasının garanti altına alınarak Birlik dışına aktarılmalarına izin verilmesiyle, bu verilerin güvenli bir şekilde serbest dolaşımlarının sağlanması da ulaşılmaya çalışılan hedefler arasındadır[398]. Yapılan yasal düzenlemeler ve alınan tedbirlerle, Birlik dışındaki üçüncü ülkelere ya da uluslararası şirket ve diğer organizasyonlara, her ne şekilde olursa olsun, transfer edilen kişisel verilerin, Birlik içinde tutulanlarla aynı korumadan yararlanması hedeflenmektedir. Bu durum, Tüzük'ün getirdiği hüküm ve koşullar ile, bunların ortaya koyduğu korumanın, kişisel verilerle birlikte Birlik dışına taşınarak, -bir diğer ifade ile, kimi koşullar altında Tüzük'ün bölgesel kapsamı genişletilerek- aynı şekilde uygulanması olarak da ifade edilebilinir[399][400].

Tüzük'ün bölgesel kapsamına ilişkin olan 3/1.maddesi ile, Birlik içerisinde yerleşik veri kontrolörü veya işleyicisinin faaliyetleri kapsamında yapılacak olan veri işleme, ister Birlik içinde, isterse Birlik dışında gerçekleşsin, her şekilde bu işleme faaliyetlerinin kişisel verilerin korunması hususunda, Tüzük hükümlerine tabi olacağının altı çizilmiştir. Tüzük madde 3/3'e göre, işleme faaliyetini gerçekleştiren veri kontrolörü veya işleyicisi, Birlik içinde değil de, uluslararası kamu hukuku gereği, üye devletlerden birinin hukukunun uygulandığı yerlerden birinde yerleşik olduğu taktirde dahi, somut olaya, 2016/679 sayılı Tüzük hükümleri uygulanacaktır. Son olarak, Tüzük madde 3/2'ye göre, Birlik içerisinde yerleşik veri süjesinin kişisel verilerinin, Birlik dışından bir veri kontrolörü ya da işleyicisi tarafından, veri süjesinin bir ödeme yapıp yapmayacağına bakılmaksızın, veri süjesine bir mal ya da hizmet sunulması; ve, veri süjesinin Birlik içerisindeki davranışlarının izlenmesi, kapsamlarında işlenmeleri durumlarında da, ilgili işleme faaliyetlerine, 2016/679 sayılı Tüzük hükümleri uygulanacaktır. Madde 3'ün kapsamından da anlaşılacağı gibi, 2016/679 sayılı Tüzük hükümlerinin, Birlik içinde yerleşik veri süjesinin kişisel

[398] GDPR Beyanlar 3,6, 101; European Union Agency for Fundamental Rights, 2018, s.250.

[399] 2016/679 sayılı Tüzük'ün 3.maddesinde düzenlenen "*Bölgesel Kapsam*"a ilişkin detaylı açıklamalar, işbu tez çalışmasının "*2.3.2.3.1. Genel Veri Koruma Tüzüğü'nün Bölgesel ve Maddi Kapsamı*" başlığı altında yapılmıştır.

[400] European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, 10.1.2017, **COM (2017) 7 final**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN (02.06.2020).

verilerinin, hem Birlik içinde, hem de Birlik dışında işlenmesi faaliyetlerine uygulanması sureti ile, kişisel verilerin güvenliklerinin yanı sıra serbest dolaşımları da garanti edilmeye çalışılmıştır.

2016/679 sayılı Tüzük madde 44'ün lafzından, kişisel verilerin korunması bağlamında Tüzük'ün uygulama alanının Birlik dışına genişletilmesi ile, kişisel verilerin Birlik dışına çeşitli şekillerde aktarımı yoluyla, Birlik içinde sağlanan güvenlik seviyesinin, zayıflatılmasının önüne geçilmeye çalışıldığı anlaşılmaktadır.

Tüzük, kişisel verilerin üçüncü ülkelere veya uluslararası organizasyonlara aktarımı hususunda, üç temel yaklaşım ortaya koymaktadır: Bunlar, "*Bir yeterlilik kararına dayanan aktarımlar (Transfers on the basis of an adequacy decision)"*; "*Uygun önlemlerin alınmasına tabi olan aktarımlar (Transfers subject to appropriate safeguards)*"; ile, "*İstisnai hallerde yapılabilen aktarımlar (Derogations for specific situations)*"dır.

2016/679 sayılı Tüzük'ün 45.maddesine göre, üçüncü bir ülkenin, belli bir bölgenin, üçüncü ülke kapsamındaki belirli bir sektörün yahut bir uluslararası organizasyonun, kişisel verilere ilişkin Avrupa Birliği düzeyinde yeterli koruma sağladığına, Komisyon tarafından kanaat edildiği taktirde, Komisyon'un özel olarak alacağı ve Avrupa Birliği'nin resmi gazetesinde yayınlanacak bir "*yeterlilik kararı*[401]" kapsamında, işbu kararda anılan yerlere, bu yerler tıpkı Birlik içindeymiş gibi, başkaca herhangi bir koşul aranmaksızın, kişisel veri transferi yapılabilecektir. Madde 45 kapsamında yeterlilik kararının verilmesinden önce, Komisyon, özellikle ilgili üçüncü ülke veya uluslararası organizasyonda, hukukun üstünlüğüne, temel hak ve özgürlüklere saygı gösterilmesinin gereğinin yasal düzenlemeler ve bunların uygulanmaları bağlamında yerine getirilip getirilmediğini; veri süjelerinin haklarını korumaya yönelik etkili ve uygulanabilir yasa hükümleri ile yaptırım mekanizmalarının var olup olmadığını; veri süjelerinin haklarını kullanmasına etkin bir şekilde yardım edecek ve onlara yol gösterecek nitelikteki bağımsız denetim makamlarının varlığını, teyit etmelidir. Madde 45/3'e göre ise, bu koşulların korunup korunmadığı, en az dört yılda bir olmak üzere, dönemsel olarak kontrol edilmelidir.

[401] Kimi Türkçe kaynaklarda "*adequacy decision*" terimi, "*yeterlilik kararı*" yerine "*uygunluk kararı*" şeklinde Türkçe'ye aktarılmıştır.

Bu kontroller sonunda yeterli koruma seviyesinin yitirildiğinin tespiti halinde de, bu yerlere yapılan kişisel veri aktarımı yasaklanabilecektir[402].

Liechtenstein, Norveç, İsviçre ve İzlanda'dan oluşan "*Avrupa Serbest Ticaret Birliği (EFTA)*"ne üye ülkeler ile Andorra, Arjantin, Uruguay, Yeni Zelanda, İsrail, Kanada ve Japonya, Komisyon'un yeterlilik kararı verdiği üçüncü ülkelere örnek olarak gösterilebilinir[403].

Kişisel verilerin, alınacak bir yeterlilik yararı kapsamında üçüncü ülkelere veya uluslararası organizasyonlara aktarımı hususunda, 95/46 sayılı mülga Direktif ile onun yerini alan 2016/679 sayılı Genel Veri Koruma Tüzüğü karşılaştırıldığında, işbu mülga Direktif'in 25 ve 26.maddeleri ile üye devletlere tanınan bir yeterlilik kararı alarak aktarıma izin verebilme yetkisinin Tüzük ile kaldırılarak, bu hususta karar alabilme yetkisinin yalnızca Komisyon'a bırakıldığı görülmektedir [404].

Birlik dışına kişisel veri transferi yapılabilmesi için bir yeterlilik kararının bulunmadığı hallerde ise, Komisyon tarafından etkililiği kabul edilmiş, bağlayıcı ve uygulanabilir nitelikteki çeşitli yasal ve idari düzenleme, taahhüt, sözleşme hükümleri, kurumsal kurallar ve benzeri diğer belgeler vasıtasıyla, uygulanabilir veri süjesi haklarının ve etkili kanun yolları ile yaptırım mekanizmalarının garanti edildiği "*uygun önlemlerin (appropriate safeguards)*" alınmasına tabi olan kişisel veri aktarımlarının yapılabileceği durumlar ise, Tüzük'ün 46. ve 47.maddelerinde düzenlenmiştir.

Aktarılacak kişisel verilerin korunması hususunda, uygun önlemlerin alınıp alınmadığının tespitinden önce verilerin hangi üçüncü ülke ya da uluslararası organizasyona aktarılacağı ile aktarılacak verilerin kapsam ve niteliğinin belirlenmesi gerekmektedir. Ancak bu ön tespitlerin yapılmasından sonra, kişisel verilerin korunması hususunda, ilgili üçüncü ülke ya da uluslararası organizasyon tarafından yeterli ve uygun önlemlerin alınıp alınmadığının incelenmesi yerinde olacaktır[405].

---

[402] GDPR Beyanlar 103,104,107; Mira Burri, Rahel Schar, ss. 496-497.
[403] European Commission, **Adequacy Decisions**, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (02.06.2020).
[404] Hüseyin Murat Develioğlu, ss. 73-75.
[405] Mina Miri, Farbod h.Foomany, Nathanael Mohammed, "Complying with GDPR: An Agile Case Study", **ISACA Journal**, Cilt.2, 2018, s.6.

Kamu makam ve kurumları arasında yapılmış hukuken bağlayıcı ve uygulanabilir anlaşmaların bulunması (*madde 46/2 a*); madde 47'de belirtildiği şekilde bağlayıcı kurumsal kuralların bulunması (*madde 46/2 b*); standart veri koruma hükümlerinin varlığı (*madde 46/2 c, d*); Avrupa Veri Koruma Kurulu'nun da görüşü alınarak yetkili denetim makamları tarafından akredite edilen uzmanlar tarafından Genel Veri Koruma Tüzüğü madde 40 kapsamında hazırlanan ve Tüzük'ün ilgili sektör kapsamında nasıl uygulanması gerektiğinin belirlemesine yardımcı olan davranış kurallarının varlığı ile bu kurallara uygun davranılacağına ilişkin üçüncü ülkede bulunan ve uygun önlemleri alacak olan veri kontrolör veya işleyicisinin taahhütlerinin bulunması (*madde 46/2 e*); madde 42 kapsamında, yetkili sertifikasyon kurum ve kuruluşları ile denetim makamları tarafından, üçüncü ülke ve uluslararası organizasyonun gerçekleştireceği işleme faaliyetlerinin, Tüzük'e uygunluğunun onaylandığını belgelendiren – ve en fazla üç yıl süreyle verilerek, bu sürenin sonunda koşulların sağlanmaya devam etmesi kaydıyla yenilenebilen- sertifikanın bulunması ve kişisel verilerin korunması hususunda bu sertifika kapsamındaki koşulların sağlanacağına dair üçüncü ülkede bulunan ve uygun önlemleri alacak olan veri kontrolör veya işleyicisinin taahhütlerinin bulunması (*madde 46/2 f*), hallerinde ise somut olay kapsamında uygun önlemlerin alınması koşulunun gerçekleştiği kabul edilerek veri aktarımı yapılabilecektir[406].

Konu, Türkiye açısından incelendiğinde, ülkemiz hakkında henüz bir yeterlilik kararı verilmediği görülmektedir. Bununla birlikte, ülkemizde 24.03.2016 tarihinde kabul edilen "*6698 sayılı Kişisel Verilerin Korunması Kanunu*"nun Avrupa Birliği'nin mülga 95/46 sayılı Direktifi ile uyumlu olmasına rağmen, onun yerini alan 2016/679 sayılı Tüzük ile tam uyumu yakalayamaması sebebiyle, kişisel verilerin üçüncü ülke konumunda olan Türkiye'ye aktarımı hususunun Tüzük'ün 46.maddesindeki uygun önlemlerin alınmasına tabi olan aktarımlar kapsamında değerlendirilebileceği görülmektedir[407]. Bu bağlamda, Avrupa Birliği'nde yerleşik bir veri süjesinin kişisel verilerinin, Türkiye'ye aktarımının, ancak veri güvenliğinin sağlanması bağlamında madde 46'da belirtildiği şekilde uygun önlemlerin alındığının teyid edilmesi halinde yapılabileceği söylenebilir.

[406] Hüseyin Murat Develioğlu, ss. 75-78.
[407] European Parliament, Parliamentary Questions, 15 September 2016, **Ref. E-005636/2016**, http://www.europarl.europa.eu/doceo/document/E-8-2016-005636-ASW_EN.html (02.06.2020).

Tüzük'ün 49.maddesinde ise, üçüncü ülke ve uluslararası organizasyonlara, bir yeterlilik kararına ya da uygun önlemlerin alınmasına dayanmayan ve yalnızca bu madde kapsamında belirtilen istisnai durumlarda yapılabilen, kişisel veri aktarım halleri düzenlenmiştir. Bu istisnai durumlardan ilki, veri süjesinin rızasının bulunması halidir. Madde 49/1 (a)'ya göre, olası riskler konusunda bilgilendirilmesine müteakip, veri süjesinin, kişisel verilerinin Birlik dışına aktarımına ilişkin olarak vereceği hiçbir tereddüte yer bırakmayacak derecede açıkça ve ilgili aktarım işlem(ler)ine özel olarak verilmiş rızasına dayanarak, istisnai olarak, veri aktarımı gerçekleştirilebilecektir. Burada veri süjesinin rızasının alınması ile istisnai olarak yapılabilecek veri aktarımı işleminin kapsam, koşul ve amaçları hakkında veri süjesinin bilgilendirilmesi hususunda şeffaflık ilkesinin sağlanmasına büyük önem verildiği görülmektedir[408].

Veri süjesinin rızasının bulunması dışında madde 49'da sayılan diğer istisnai hallerde de üçüncü ülke ve uluslararası organizasyonlara bir yeterlilik kararına ya da uygun önlemlerin alınması şartına dayanmadan kişisel veri aktarımı yapılabilecektir. Madde 49'a göre; Veri süjesi ve kontrolör arasında aktedilen bir sözleşmenin ifası veya veri süjesinin talebi ile, sözleşme yapılmasının öncesinde bazı tedbirlerin alınabilmesi için veri aktarımının gerekli olduğu haller (*madde 49/1 b*); Veri süjesinin çıkarları doğrultusunda, veri kontrolörü ile bir gerçek veya tüzel kişi arasında gerçekleşecek bir sözleşmenin yapılması veya icrası kapsamında gerekli olduğu haller (*madde 49/1 c*); Kamu yararının gerektirdiği önemli sebeplerden ötürü aktarımın yapılmasının gerektiği durumlar (*madde 49/1 d*); Yasal iddia ve taleplerin tesisi, uygulanması veya savunmanın yapılması için aktarımın gerekli olduğu haller (*madde 49/1 e*); Fiziksel ya da yasal olarak rızasını veremeyecek durumda olması halinde, veri süjesinin veya bir üçüncü şahsın hayati menfaatlerinin korunmasının gerektirdiği durumlar (*madde 49/1 f*); Somut olayın özelliklerine göre, sicile başvuruya ilişkin yasal koşulların tamamlanması şartıyla, aktarımın, kamuya veya meşru menfaati olduğunu kanıtlayan kişilere açık bir sicilden yapılacağı haller (*madde 49/1 g*), Tüzük kapsamında bir yeterlilik kararına ya da uygun önlemlerin

[408] European Data Protection Board, "Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679", **Guidelines 2/2018,** 25.05.2018, https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2018/06/edpb_guidelines_2_2018_derogations_en.pdf (02.06.2020), ss.6-7.

alınması şartına dayanmayan, istisnai nitelikli kişisel veri aktarımı halleri arasında sayılmaktadırlar.

Madde 49/1 (b,c,d,e,f) kapsamındaki istisnaların uygulanabilmesi için, Avrupa Birliği içindeki veri ihracatçısı tarafından, bu istisnaların getirilmesinin temelinde yatan amaç ile, somut olayda, ilgili istisna kapsamında yapılması planlanan aktarım işleminin koşullarının uyumlu olup olmadığına ilişkin değerlendirme yapılmasının gerekli olduğu anlaşılmaktadır[409].

Madde 49/1'in son paragrafında ise, üçüncü ülkeye veya uluslararası bir organizasyona yapılması düşünülen kişisel veri aktarımının, Tüzük'ün 45.ve 46.maddeleri ile 49.maddede sayılan istisnai koşulların hiçbirini karşılamadığı hallerde izlenecek yol açıklanmıştır. İşbu maddelerde sayılan hiçbir koşulu karşılamayan aktarım, yalnızca bir kereye mahsus yapılacak olması; sınırlı sayıda veri süjesini ilgilendirmesi; veri süjesinin menfaatleri ile hak ve özgürlüklerine halel gelmemesi, kontrolörün korumak zorunda olduğu meşru menfaatler için gerekli olması; kontrolörün karşılaşılabilecek her türlü olumsuz koşulu göz önünde bulundurarak kişisel verilerin korunmasına ilişkin tüm tedbirleri alması, şartlarının birlikte yerine getirilmeleri kaydıyla gerçekleştirilebilecektir. Ancak, böyle bir aktarımın yapılmasına ilişkin olarak kontrolör, ilgili denetim makamını ve veri süjesini haberdar etmekle yükümlüdür.

Kişisel verilerin üçüncü ülke veya uluslararası organizasyonlara aktarımına ilişkin olan ve yukarıda açıklanan Tüzük'ün V.Bölümü kapsamındaki hiçbir hükmün, kişisel verilere işbu Tüzük kapsamında sağlanan yasal korumanın zayıflatılması ya da bertaraf edilmesi amacıyla kullanılamayacağının altı, Tüzük madde 44 ile belirgin olarak çizilmiştir. Tüzük'ün Giriş 111.paragrafı ile 49.maddesinin kapsamında geçen "*nadiren (occasional)*" ve "*tekrarlanmayan (not repetitive)*" ifadelerinden, 49.maddede belirtilen bu istisnaların, rastgele ve düzenli olmayan aralıklarla birden fazla kere uygulanabileceği anlamı çıkarılabilmekle birlikte, süreklilik arz edecek şekilde, kısa aralıklarla ve düzenli olarak uygulanabileceği şeklinde yorumlanmaması gerektiği anlaşılmaktadır[410].

[409] European Data Protection Board, **Guidelines 2/2018**, s.5.
[410] European Data Protection Board, **Guidelines 2/2018**, ss.3-5.

3.5.9.1. Kişisel Verilerin Amerika Birleşik Devletleri'ne Aktarımı

Kişisel verilerin korunması hususunda, Amerika Birleşik Devletleri'nde kabul edilen "*Güvenli Liman Gizlilik İlkelerinin (Safe Harbour Privacy Principles)*", mülga 95/46 sayılı Direktif kapsamında, üçüncü ülkelere kişisel veri aktarımı konusunda yeterli koruma sağladığı, Komisyon tarafından 2000 yılında alınan bir "*yeterlilik kararı*[411]" ile kabul edilmişti. "*Güvenli Liman (Safe Harbour)*" olarak da anılan işbu "*2000/520 sayılı Komisyon'un Yeterlilik Kararı*", neticesinde ABD Ticaret Bakanlığının yayınladığı Güvenli Liman İlkeleri kapsamında kişisel verilerin korunmasına ilişkin olarak, mülga 95/46 sayılı Direktif'e uygunluğunu, resmen sertifikalandırarak belgelendirebilen ABD şirketlerine, Avrupa Birliği'nden kişisel veri transferi yapılabilme hakkı verilmekteydi[412].

Güvenli Liman Kararı'nın verildiği 2000'li yılların ilk yarısı, artan teknolojik gelişmeler ve bu gelişmeler bağlamında hayatımızın her alanına giren internet kullanımı sebebiyle, aynı zamanda kişisel verilerin Avrupa Birliği dışına üçüncü ülkelere özellikle de ABD'ye aktarımının yaratacağı olası mahremiyet ve temel hak ihlallerinin kapsam ve sonuçlarının en çok tartışıldığı dönem olmuştur.

2000 yılında, Microsoft Iberica SRL'ye, İspanyol Veri Koruma Denetim Makamı tarafından kesilen idari para cezasının bu tartışmaların fitilini ateşlediği söylenebilir. Bu vaka kapsamında, İspanyol Veri Koruma Denetim Makamı tarafından yürütülen inceleme neticesinde, Microsoft Iberica'nın, İspanyol veri koruma yasalarına uymayarak, İspanyol vatandaşlarının kişisel verilerini, veri süjelerinin rızalarını almadan ve kendilerine aktarım hususunda gereken bilgilendirmeleri de yapmadan, üçüncü bir ülke olan ABD'deki veri tabanlarına aktardığı tespit edilmiştir. Vaka incelemesinde her ne kadar daha sonra bu verilerin İspanya'daki bir veri tabanına geri aktarıldığı tespit edilse de inceleme sonunda

[411] Commission Decision, 2000/520/EC (No longer in force) 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), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520, (02.06.2020).

[412] Nurullah Tekin, "Kişisel Verilerin Korunması ile ilgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", **Uyuşmazlık Mahkemesi Dergisi**, Cilt. 4, 2014, s.241

Microsoft Iberica'ya 10.000.000 İspanyol pesetası tutarında idari para cezası uygulanmıştır[413].

Güvenli Liman Kararının alınmasından sonra devam eden süreçte, İrlanda Facebook üzerinden ABD'ye aktarılan kişisel verilerine, Amerikan istihbarat kurumları tarafından kolaylıkla erişilerek, bu verilerin ihlal edilebileceğinin, Avusturya vatandaşı ve bir mahremiyet aktivisti olan Bay Schrems tarafından anlaşılmasından sonra[414], Bay Schrems, İrlanda Veri Koruma Denetim Makamına konunun incelenmesi adına başvuruda bulunmuştur. İrlanda Veri Koruma Denetim Makamı ise, kişisel verilerin ABD'ye aktarımı hususunda Komisyon'un aldığı 2000/520 sayılı Yeterlilik Kararı'nı ileri sürerek Bay Schrems'in ileri sürdüğü bu hususu incelemeyi reddetmiştir. İlgili red kararı üzerine konu İrlanda Yüksek Mahkemesi tarafından ön karar prosedürü ile ABAD'a taşınmıştır. ABAD tarafından verilen 6 Ekim 2015 tarihli karar sonucunda, İrlanda Veri Koruma Denetim Makamının, 2000/520 sayılı Komisyon'un Yeterlilik Kararının varlığına dayanarak, Bay Schrems'in inceleme talebine karşılık verdiği red kararının yerinde olmadığına hükmedilmiştir. Komisyon'un ilgili Yeterlilik Kararının varlığının, üye devletlerin denetim makamlarının kişilerin hak ve özgürlüklerinin korunması hususundaki yetkilerini ortadan kaldırmadığının altı da Schrems davası sonunda verilen karar ile çizilmiştir. Neticede Amerikan şirketlerinin tüketici mahremiyetinin korunması ve kişisel verilerin depolanması da dahil bu verilerin işlenmelerine ilişkin hususlarda, Güvenli Liman İlkelerine uygunluklarını belgelendirdikleri taktirde, 95/46 sayılı Direktif kapsamında, yeterli koruma sağladıklarına ve kişisel verilerin aktarımının uygun olduğuna ilişkin olarak alınan "*2000/520 sayılı bu Komisyon Kararı*", 2015

[413] Christopher Kuner, "Beyond Safe Harbour: European Data Protection Law and Electronic Commerce", **The International Lawyer**, Cilt.35, Sayı.1, 2001, s.84.

[414] Avrupa Birliği kamuoyunda kişisel veri güvenliğine devletlerin istihbarat kurumları tarafından yasadışı müdahalelerde bulunulabileceğine ilişkin hassasiyet, özellikle Snowden vakasının ardından daha da artmıştır. Zira bu vaka ile Amerikan Ulusal Gizli Servisi'nin Facebook, Google, Microsoft, Yahoo, Instagram, Apple gibi Amerikan kökenli internet araç ve hizmet sağlayıcılarının sahip oldukları sistemler üzerinden bireylerin kişisel verilerine eriştiği hususu net olarak kamuoyunun görüş alanına girmiştir. Özellikle ABD'nin istihbarat kurumlarıyla ilgili şüpheleri artıran Snowden vakasına ilişkin daha fazla bilgi için bkz. Serkan Bulut, "Söylemin Kapatılma ve Açımlama Savaşımında Edward Snowden", **Üsküdar Üniversitesi İletişim Fakültesi Akademik Dergisi**, Cilt.2, Sayı.3, 2019, ss. 128-140; Mira Burri, Rahel Schar, s. 482.

yılında, ABAD tarafından "*Schrems Davası*" kapsamında yeniden değerlendirilerek, iptal edilmiştir[415].

Schrems davasında alınan iptal kararından sonra, hem artan veri trafiği, hem de ulusal haber alma teşkilatlarının kişisel veriler üzerinde oluşturabileceği mahremiyet ve temel hak ihlalleri göz önüne alınarak, Birlik içerisinde yerleşik veri süjesinin kişisel verilerinin ticari amaçlarla ABD'ye aktarım koşullarının yeniden düzenlenmesine karar verilmiştir. Bunu üzerine veri süjesinin ABD'ye yapılacak aktarım bağlamındaki temel hak ve özgürlüklerinin korunmasını teminat altına almak üzere hazırlanan ve çerçeve ilke ve koşulları içeren, "*Gizlilik Kalkanı (Privacy Shield)*" olarak da anılan Komisyon'un "*2016/1250 sayılı Yeterlilik Kararı*[416]", 2016 yılında kabul edilerek yürürlüğe girmiştir. Gizlilik Kalkanı Yeterlilik Kararına göre, işbu karar ile getirilen çerçeve koşulları sağlayacağına ilişkin, Amerikan Ticaret Bakanlığı'na taahhütte bulunarak, yeterliliği onaylanan Amerikan şirketleri, Birlik üzerinden ABD'ye kişisel veri transferi yapabileceklerdir. İlgili şirketin yapacağı bu taahhüt üzerine, yeterlilik onayının alınabilmesi için, öncelikle ilgili Amerikan şirketinin, Temel Haklar Şartı'nda düzenlendiği şekliyle, özel hayatın ve kişisel verilerin korunmasına yönelik, etkili kural ve yaptırım mekanizmalarını oluşturması gerekmektedir. Amerikan şirketlerinin, oluşturacakları bu kural ve mekanizmalar vasıtasıyla, veri süjelerinin hak ve özgürlüklerinin korunmasına ilişkin olan Gizlilik Kalkanı çerçeve ilkelerine uygun, bir öz sertifikalandırma sistemi ortaya koymaları gerekmektedir. Bu koşulları sağlayarak, yeterlilikleri onaylanan şirket ya da kurumlar, Amerikan Ticaret Bakanlığı'nın hazırlayarak yayınladığı "*Gizlilik Kalkanı Listesine (Privacy Shield List)*" dahil edilirler. Bu listeye girebilen şirket ve kurumlardaki veri kontrolörleri ve işleyicileri, verdikleri taahhütle, Gizlilik Kalkanı

[415] Judgment of the Court of Justice of the European Union (Grand Chamber), EUR-Lex, Reports of Cases, **ECJ C-362/14**, Maximillian Schrems v. Data Protection Commissioner, 6.10.2015, Request for a preliminary ruling from the High Court (Ireland)— Transfer of personal data to the United States, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 (02.06.2020); Court of Justice, of the European Union, Research and Documentation Directorate, **ECJ Fact Sheet**, Protection of Personal Data, 2017, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf (02.06.2020), s. 17-18;
Alessandro El Khoury, "The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EY-USA Data Transfers?", **European Journal of Risk Regulation**, Cilt.6, Sayı.4, 2015, ss. 659-661.

[416] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-US Privacy Shield, **Official Journal L 207/1**, 01.8.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG (02.06.2020).

İlkelerine sözleşmesel olarak bağlı ve dolayısı ile de hukuki anlamda sorumlu hale gelmektedirler. Tüm bunların yanında, Birlik ve ABD, Gizlilik kalkanı ilke ve kurallarının, doğru uygulanıp uygulanmadığına ilişkin, yıllık olarak ortak incelemelerde de bulunacaklardır. Güvenli Liman ile kıyaslandığında Gizlilik Kalkanı'nın daha katı ve detaylı bir şekilde düzenlendiği anlaşılmaktadır. Zira Gizlilik Kalkanı ile getirilen güçlendirilmiş ilkelerle, kişisel verilerin toplanmasından depolanmasına kadar nasıl işleneceğine dair kuralların ve yükümlülüklerin daha açık ve belirgin hale getirilmesinin yanı sıra, veri süjeleri, kişisel verilerinin korunması bağlamında Güvenli Limana kıyasla daha güçlü şikayet hakları da elde etmişlerdir. Böylelikle, Gizlilik Kalkanı'nın getirdiği yeni sistemde, veri süjeleri, kişisel verilerinin ihlaline ilişkin şikayetlerini doğrudan ilgili Amerikan şirketine yapabilecekleri gibi, anlaşmazlıkların çözümü bağlamında bağımsız bir kuruma, üye devlet denetim makamına ya da ABD Federal Ticaret Komisyonunu da başvurabilecektir. Ayrıca sorunun çözümsüz kaldığı hallerde veri süjeleri, Gizlilik Kalkanı Yeterlilik Kararı doğrultusunda kurulan bir organ olan "*Gizlilik Kalkanı Paneli (Privacy Shield Panel)*"ne başvurarak bağlayıcı tahkim talep etme hakkına da sahiptir. Bu da sorunların vakit kaybetmeksizin kolaylıkla çözümünde, veri süjelerine seçim yapabilme hakkı tanımaktadır[417]. Ancak tüm düzenlemelere rağmen, Bay Schrems tarafından Gizlilik Kalkanı Yeterlilik Kararının iptaline ilişkin olarak açılan bir başka dava neticesinde, Gizlilik Kalkanı çerçevesinde getirilen yeni ilke ve koşulların dahi, Birlik vatandaşlarının ABD'ye aktarılan kişisel verilerine kamu güvenliği kapsamında ABD'nin ulusal haber alma teşkilatları tarafından erişilerek işlenmelerine engel olunamadığı anlaşılmıştır. Bu sebeplerle, Avrupa Birliği'nden ABD'ye aktarılan kişisel verilerin, Genel Veri Koruma Tüzüğü'ne uygun bir şekilde korunabilmelerinin mümkün olmadığı gerekçesi ile Adalet Divanı 16.07.2020 tarihinde Gizlilik Kalkanı Yeterlilik Kararı'nın da iptaline hükmetmiştir[418].

---

[417] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, **Official Journal L 207/1**, parag. (3) (6) (7) (14) (31);
Mira Burri, Rahel Schar, s. 504;
W.Gregory Voss, Winter 2016-2017, ss. 231-232.

[418] Judgment of the Court of Justice of the European Union (Grand Chamber), EUR-Lex, Reports of Cases, **ECJ C-311/18**, Data Protection Commissioner v. Maximillian Schrems & Facebook Ireland Ltd., 16.07.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:6201-8CJ0311&qid=1597766650136&from=EN (16.08.2020); Court of Justice, of the European Union, Research and Documentation Directorate, **ECJ Fact Sheet**, Protection of Personal Data, 2017

3.5.10. Kişisel Verilerin Korunmasında Yaptırım Mekanizmaları

Kişisel verilerin korunmasında uygulanacak yaptırım mekanizmaları ve para cezalarına ilişkin düzenlemeler, 2016/679 sayılı Tüzük'ün 77 ila 84.maddeleri arasında bulunmaktadır. Bu düzenlemeler birlikte değerlendirildiğinde, yaptırım mekanizmalarının tasarlanmasında, denetim makamlarından başlayarak üye devlet mahkemelerine kadar uzanan çok katmanlı bir yaklaşımın benimsendiği anlaşılmaktadır[419].

Yapılan bu yeni düzenlemeler, mülga 95/46 sayılı Direktif'teki düzenlemelerle karşılaştırıldığında, kişisel verilerin işlenmesinde hukuka aykırı davranılması durumunda, Tüzük ile, kontrolör ve işleyicilere yüklenen sorumluluğun da, birbirleriyle eşit düzeye getirilerek, genişletildiği görülmektedir[420]. Ayrıca yine Tüzük kapsamında kişisel verilerin korunması hususunda karşılaşılan sorunlara, daha elverişli çözüm mekanizmaları getirilmeye çalışıldığı da anlaşılmaktadır. Bu bağlamda, Tüzük'ün kabulüyle, kişisel verilerin hukuka aykırı işlenmeleri sonucu uygulanacak yaptırımların, Birlik düzeyinde uyumlu hale getirilerek, idari para cezası miktarları da dahil, yaptırımların kapsam ve içerikleri artırılmıştır. Denetim makamları Tüzük kapsamında getirilen yaptırımları uygularken her bir somut olayın özelliğini ayrı ayrı değerlendirerek karar vermekle yükümlüdürler. Bu yaptırımların etkili, orantılı ve caydırıcı nitelik taşımaları ve Birlik çapında aynı ya da benzer nitelikteki ihlallere eşdeğer yaptırımlar getirilerek uygulamada tutarlılığın sağlanması gerekmektedir. Yaptırımların uygulanmasında Birlik çapında uyumun yakalanabilmesi için ise, düzenli yapılacak atölye çalışmaları gibi çeşitli işbirliği mekanizmaları aracılığıyla denetim makamları arasında bilgi paylaşımı ve aktif katılımın sağlanması önemlidir[421]. Tüzük ile, yaptırımların, Birlik düzeyinde uyumlu hale getirilmesinin, Avrupa dijital tek pazarının parçalı görünümünden kurtularak uyumlu işleyebilmesi yönünde atılmış bir başka önemli adım olduğu söylenebilir.

---

[419] Laura-Cristiana Spataru-Negura, Cornelia Lazar, s. 664.

[420] Article 29 Data Protection Working Party, "Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation", 2016/679, **17/EN WP 253**, 3.10.2017, https://knowww.eu/search-tree?t=5ad7131ed39f5aa2bcbf0f34# (02.06.2020), Introduction.

[421] Article 29 Data Protection Working Party, Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679, **17/EN WP 253,** Principles; Irina Alexe, "Personal Data Protection, The Sanctioning Regime Provided by Regulation (EU) 20167679 on the Protection of Personal Data", **Law Review**, Cilt.VIII, Sayı.1, January-June 2018, ss.71, 73.

2016/679 sayılı Tüzük ile, siyasi baskı da dahil her türlü baskıdan uzak tutularak bağımsız niteliklerinin korunacağının altı çizilen denetim makamlarının, işbu Tüzük hükümlerinin etkili uygulanmasının sağlanmasına ilişkin önemli yetkilerle donatıldığı görülmektedir[422]. Zira Tüzük madde 77 kapsamında, kişisel verilerinin, yasal olmayan şekillerde işlendiğini düşünen veri süjesinin, ilgili denetim makamlarına başvurarak, şikayette bulunma hakkı düzenlenmiştir. Denetim makamı, veri süjesinin yapmış olduğu şikayeti değerlendirirken, bu şikayetin gidişatına ve sonucuna ilişkin süreçten veri süjesini bilgilendirerek haberdar etmekle yükümlüdür. Denetim makamı, yapılan bu şikayet başvurusunu cevapsız bırakır ya da şikayetin gidişatına veya sonucuna ilişkin veri süjesini üç ay içerisinde bilgilendirmez ise, veri süjesinin, Tüzük madde 78'e göre, denetim makamları karşı "*etkili hukuk yollarına başvuru hakkı (The Right to an Effective Judicial Remedy)*[423]" da bulunmaktadır. Etkili hukuk yollarına başvuru hakkı kapsamında, her gerçek ve tüzel kişinin, denetim makamlarının verdiği bağlayıcı nitelikteki kararlara karşı, ilgili denetim makamının yerleşik bulunduğu üye devlet mahkemelerinde yargı yoluna başvuru haklarının da bulunduğunun altı yine Tüzük'ün 78.maddesinde çizilmiştir. Denetim makamlarının bağlayıcı kararlarına karşı, veri süjeleri tarafından yetkili

---

[422] Article 29 Data Protection Working Party, Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679, **17/EN WP 253,** Introduction.

[423] 2016/679 sayılı Tüzük'ün 78.maddesinde düzenlenen "*Etkili Hukuk Yollarına Başvuru Hakkı*"nın kökenleri, Avrupa İnsan Hakları Sözleşmesinin (European Convention on Human Rights) 13.maddesi kapsamındaki "*Etkili Başvuru Hakkı (Right to an Effective Remedy)*"na dayanmaktadır. Bu hak, özellikle kamu kurum ve kuruluşları karşısından, bireylerin hak ve özgürlüklerinin korunması temel prensibine dayanır. Avrupa Temel Haklar Şartı (Charter of Fundamental Rights of European Union) madde 47'de düzenlenen "*Etkili Hukuki Bir Yola Başvurma ve Adil Yargılanma Hakkı*" da bu temelde düzenlenmiştir. Daha fazla bilgi için bkz. Herwig C.Hofmann, "The Right to an 'Effective Judicial Remedy' and the Changing Conditions of Implementing EU Law", Université du Luxembourg, Faculty of Law, Economics and Finance, **Law Working Paper Series**, Paper No. 2013-02, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2292542 (02.06.2020);
Avrupa Birliği Temel Haklar Şartı: madde 47 – "*Etkili Hukuki Bir Yola Başvurma ve Adil Yargılanma Hakkı: Birlik hukuku tarafından teminat altına alınmış olan hakları ve özgürlükleri ihlal edilen herkes, bu maddede belirtilen şartlara Uygun olarak bir mahkemede hukuki yola başvurma hakkına sahiptir.*
Herkes daha önceden yasa ile tesis edilmiş bağımsız ve tarafsız bir mahkemede makul bir sure içinde yapılacak adil ve kamuya açık bir duruşma yapılması hakkına sahiptir. Herkes kendisine bilgi verilmesi, savunulması ve temsil edilmesi fırsatına sahip olmalıdır.
Gerekli imkanlara sahip olmayan herkese, bu yardımın adalete etkin bir şekilde ulaşmasının sağlanması için gerekli olması koşulu ile hukuki yardım sağlanacaktır." İşbu 47.madde tercümesi Avrupa Birliği Türkiye Delegasyonu resmi web sitesinde bulunan Avrupa Birliği Temel Haklar Bildirgesi tercüme metninden aynen alıntılanmıştır. Bkz. Avrupa Birliği Türkiye Delegasyonu Resmi Sitesi, Avrupa Birliği Temel Haklar Bildirgesi Tercümesi, https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708 (02.06.2020).

mahkemelere başvurulması halinde, uyuşmazlıkların çözümü hususunda bu mahkemler tam yargı yetkilerini kullanarak her türlü hususu inceleyebileceklerdir[424].

Tüzük'ün 79.maddesinde de bu kerre, kontrolör veya işleyiciye karşı etkili hukuk yollarına başvuru hakkı düzenlenmiştir. Madde 79'a göre, Tüzük'te düzenlenen haklarının ihlal edildiğini iddia eden veri süjesi, 78.madde kapsamında bu hususta denetim makamlarına başvuru hakkına halel gelmeden, ilgili işleme faaliyetini gerçekleştiren veri kontrolörü veya işleyicisine karşı, bunların kurulu bulundukları üye devlet mahkemelerinde etkili hukuk yollarına başvurabileceklerdir.

Tüzük'ün 82.maddesinde de, kişisel verilerinin korunmasına ilişkin haklarının ihlali sebebiyle, maddi-manevi zarara uğrayan veri süjesinin, ilgili kontrolör ve işleyiciden tazminat isteme hakkı düzenlenmiştir. Madde 82'ye göre, kontrolör veya işleyicinin tazminat yükümlülüğünün doğabilmesi için, işbu Tüzük'le düzenlenen sorumluluklarını yerine getirmemeleri veya Tüzük'e aykırı talimat vermek sureti ile bu zararın oluşmasına sebep olmaları gerekmektedir. Birden fazla kontrolör veya işleyicinin zarara sebep olan işleme faaliyetine dahil olmaları durumunda ise, bunların her birinin, veri süjesinin katlanmak zorunda kaldığı zararın tamamen ve etkili bir şekilde tazmininden sorumlu olacakları da madde 82/4 kapsamında belirtilmiştir. Kontrolör veya işleyici, 82.maddedeki tazminat yükümlülüğünden, ancak ve ancak somut olaydaki zararın oluşmasında herhangi bir sorumluluklarının bulunmadığını ispatlamaları koşuluyla kurtulabilirler. Ancak kontrolör veya işleyicinin, zararın oluşmasında küçük de olsa bir sorumlulukları olduğu taktirde, madde 83 kapsamında tazminat yükümlülüğü doğmaktadır. Burada dikkat çekici bir diğer konu da mülga 95/46 sayılı Direktif ile mücbir sebep hallerinde kontrolörlere tanınan tazminat yükümlülüğünden kurtulabilmeye ilişkin istisnanın, 2016/679 sayılı Tüzük ile tanınmamasıdır[425].

Tüzük madde 80'e göre ise, veri süjesi, 77, 78, 79 ve 82.maddelerde düzenlenen haklarını, bizzat kendisi kullanabileceği gibi, yasalar dahilinde kurulmuş olan ve kişisel verilerin korunması hususunda aktif olarak kamu yararına çalışan, kar

[424] Paul Voight, Axel von dem Bussche, s. 214.
[425] Laura-Cristiana Spataru-Negura, Cornelia Lazar, s. 664;
Paul Voight, Axel von dem Bussche, ss. 205-208;
Mülga 95/46 sayılı Direktif Beyanlar (55).

amacı gütmeyen dernek, kuruluş veya birliği de bu konularda vekaleten yetkilendirebilme hakkına sahiptir.

Kişisel verilerin korunmasına ilişkin Tüzük hükümlerine aykırı davranılması sonucu denetim makamlarınca kesilebilen ve somut olayın özelliklerine göre etkili, orantılı ve caydırıcı olacak nitelikteki idari para cezaları, Tüzük'ün 83.maddesi kapsamında düzenlenmiştir. İdari para cezası kesilip kesilmeyeceği veya cezanın miktarı belirlenirken, 83/2.maddede yer alan aşağıdaki hususlar göz önüne alınmalıdır: "İşleme faaliyetinin doğası, kapsam ve amacı dikkate alındığında, somut olayda ortaya çıkan ihlalin kapsam ve niteliği ile süresi, ihlalden etkilenen veri süjelerinin sayısı ve etkilenme dereceleri (*madde 83/2 a*); İhlalin bir kasıt yahut ihmalden kaynaklı olup olmadığı (*madde 83/2 b*); Veri süjelerinin uğradıkları zararı hafifletmek adına kontrolör veya işleyici tarafından herhangi bir işlem yapılıp yapılmadığı (*madde 83/2 c*); Tüzük'ün 25.maddesinde düzenlenen Privacy by design ve by default ilkeleri ile 32.maddesi kapsamındaki kişisel verilerin güvenli bir şekilde işlenebilmesi için gerekli, uygun ve yeterli teknik ve idari tedbirlerin alınıp alınmadığı konularında kontrolör ve işleyicinin sorumluluk düzeyinin ne olduğu (*madde 83/2 d*); Kontrolör ve işleyicinin daha önceden benzer bir ihlal gerçekleştirip gerçekleştirmediği (*madde 83/2 e*); İhlalin giderilmesi ve olası olumsuz etkilerinin giderilmesi için denetim makamı ile işbirliği yapılıp yapılmadığı (*madde 83/2 f*); İhlalden etkilenen kişisel veri türlerinin neler olduğu (*madde 83/2 g*); İhlalin veri kontrolör veya işleyicisi tarafından denetim makamına bildirilip bildirilmediği, bildirildi ise ne kapsamda bildirim yapıldığı (*madde 83/2 h*); Veri kontrolör veya işleyicisinin, daha önceden, Tüzük'ün 58/2.maddesinde sayılan, denetim makamının düzeltici yetkileri kapsamındaki uyarı, kınama gibi yaptırımlara maruz kalıp kalmadığı (*madde 83/2 i*); Tüzük'ün 40.maddesi kapsamındaki onaylı davranış kurallarına veya 42.maddedeki onaylı belgelendirme mekanizmalarına uyulup uyulmadığı (*madde 83/2 j*); Somut olayda ihlal nedeniyle doğrudan ya da dolaylı olarak elde edilen maddi menfaatler yahut önüne geçilen kayıplar gibi ağırlaştırıcı veya hafifletici faktörlerin bulunup bulunmadığı (*madde 83/2 k*)", hususları somut olayda, idari para cezalarının uygulanıp uygulanmayacağı veya uygulanacak ise bu cezaların miktarlarının ne olacağının belirlenmesinde etkilidirler.

Kişisel verilerin ihlali halinde uygulanacak idari para cezalarının üst limitleri, söz konusu ihlalin kapsam ve niteliğine göre, Tüzük'ün 83/4 ve 83/5.maddelerinde iki kategori halinde düzenlenmişlerdir. 2016/679 sayılı Tüzük ile getirilen idari para cezalarının niteliklerine bakıldığında bu cezaların, Tüzük kapsamında doğrudan uygulanan en güçlü yaptırım mekanizmaları olduğu söylenebilir. 2016/679 sayılı Tüzük'ün 83/5.maddesi kapsamında düzenlenen ve ağır ihlaller olarak nitelendirilebilen durumlarda, sorumlulara, 20 milyon Avro'ya veya bir önceki mali yılın küresel cirosunun %4'üne kadar –hangisi daha fazla ise o uygulanacak şekilde- idari para cezası kesilebilmektedir. Tüzük madde 83/4'te ise, daha hafif ihlaller için, 10 milyon Avro'ya veya bir önceki mali yılın küresel cirosunun %2'sine kadar –hangisi daha fazla ise o uygulanacak şekilde- idari para cezası uygulanabileceği hüküm altına alınmıştır[426].

İlgili Tüzük'ün 84.maddesi kapsamında, üye devletlerin, Tüzük'ün 83.maddesi ile idari para cezası kesebilmeleri için belirlenen genel hükümlerin kapsamına dahil olmayan diğer ihlallere ilişkin cezaların miktar ve uygulama koşullarını, yapacakları etkili, orantılı ve caydırıcı nitelikteki yasal düzenlemelerle hüküm altına alabilecekleri düzenlenmiştir. Diğer bir ifade ile, Tüzük madde 84 ile, üye devletlere, Tüzük'ün 83.maddesi kapsamına girmeyen ihlallerin gerçekleşmesi halinde verilecek cezalara ilişkin olarak bir takdir yetkisi tanındığı görülmektedir.

Tüzük ile idari para cezalarının bu derece yüksek seviyelere yükseltilmesi ilk etapta büyük tartışmalara yol açmıştır. Ancak demokratik toplum yaşamının olmazsa olmazlarından olan temel hak ve özgürlükler bağlamında korunmaları gereken kişisel verilerin, uyumlu yasalar ve güçlü yaptırımlar kapsamında Birlik düzeyinde korunmaları, aynı zamanda oluşturulmaya çalışılan yekpare dijital tek pazarda, işlem ve tüketici güvenliğinin sağlanabilmesi için de hayati öneme sahiptir. Oluşturulacak bu güven ortamı, dijital tek pazarın işlem hacminin artırılmasına yardımcı olacağından, neticede de hem bu bağlamda ekonomik büyümeyi, hem de temel hakların korunmasının güçlendirilmesi bağlamında sosyal ve toplumsal gelişimi, hızlandıracağı da açıktır.

---

[426] Sebastian J.Golla, "Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR", **Journal of Intellectıal Property, Information Technology and E-Commerce Law**, Cilt.70, Sayı. 8 (1), 2017, s. 74.
Jan Philipp Albrecht, s. 287.

3.5.10.1. Fransız Veri Koruma Makamı ve Google Vakası

2016/679 sayılı Tüzük'ün yürürlüğe girmesiyle birlikte, Google ile Messenger, Instagram, WhatsApp gibi şirketlere de sahip olan Facebook gibi dünyanın en güçlü teknoloji firmaları da, Avrupa Birliği'nin -deyim yerindeyse- kapsama alanına girmiştir. Tüzük kapsamında ortaya çıkan ihlal iddiaları çerçevesinde, bu dev teknoloji şirketleri ile Birlik kurumları arasındaki ilk önemli karşılaşmalardan biri, Fransız Veri Koruma Makamı (CNIL) ile Google LLC ve Google France SARL arasında yaşanmıştır.

Fransız Veri Koruma Makamı, Google France SARL'nin, 2016 yılı itibarı ile Fransa'da toplam 27 milyon kullanıcıya ulaştığını tespit etmiştir. Aynı yıl Fransız Veri Koruma Makamı, Google France SARL'ın, 2016/679 sayılı Tüzük hükümlerine uymayarak, veri süjelerinin haklarını ihlal ettiği gerekçesi ile, "*None of Your Business Derneği*" ile "*La Quadrature du Net Derneği*" adlı iki farklı sivil toplum kuruluşundan, Tüzük madde 80 kapsamında, toplamda 9.974 kullanıcıyı temsilen, toplu şikayetler almıştır. Bu şikayetlerde, Android mobil terminal kullanıcılarının, "*Google Gizlilik Politikasını ve Google Hizmetleri Genel Kullanım Koşullarını*" kabul etmedikleri hallerde, bu terminalleri kullanmalarının, Google tarafından engellendiği belirtilmiştir. Ayrıca, Google'a ait hangi terminalin kullanıldığına bakılmaksızın, Google'ın davranışsal analiz ve hedefli reklamcılık amaçlarıyla kişisel verileri işleyebilmesi için gerekli ve geçerli yasal dayanaklara da sahip olmadığı, bu şikayetler kapsamında ileri sürülmüştür. Fransız Veri Koruma Makamı tarafından yapılan çeşitli incelemeler neticesinde, 2016/679 sayılı Tüzük kapsamındaki bilgilendirme yükümlülüklerine, işleme faaliyetlerinin şeffaflık ve yasal işleme ilkesi doğrultusunda yapılması gereklerine Google tarafından uyulmaması sebepleriyle, kişisel veri ihlallerinin gerçekleştiği tespit edilerek, hüküm altına alınmıştır. Ayrıca somut olay kapsamında tespit edilen bu ihlallerin uzun zaman devam etmeleri, ihlallerden etkilenen veri süjesi sayısının fazlalığı ve yasal olmayan işlemelerin, ticari kar elde edilmesi amaçlarıyla yapılmış olmaları,

ihlallerden doğan sorumluluğu artırdığından, Fransız Veri Koruma Makamı, Google LLC şirketini, 50 milyon Avro idari para cezası ödemeye mahkum etmiştir[427].

Fransa Google vakası olarak da anılabilen bu olay kapsamında verilen karar ve kesilen idari para cezası, Tüzük'ün bölgesel kapsamının genişlediğinin ve böylelikle de Tüzük hükümlerinin uygulama alan, etki ve yaptırımlarının Birlik dışı devlet ve şirketlere kadar ulaşabildiğinin göstergesi niteliğinde olması bakımlarında önemlidir. 2019 tarihli bu kararın akabinde, Birlik ile doğrudan ya da dolaylı herhangi bir ticari ilişki yürüterek, aynı zamanda yaptıkları bu ticari faaliyetlerin mahiyetleri gereği kişisel verileri işleyerek bunların Birlik dışına aktarımlarını gerçekleştiren, özellikle Google, Facebook, Apple v.b. uluslararası kuruluş ve/veya şirketler ile Birlik dışı ülkelerin, 2016/679 sayılı Tüzük ile kişisel verilerin korunması ve serbest dolaşımlarının sağlanmasına ilişkin getirilen yasa hükümlerinin, sadece Birlik'e üye devletlere mahsus olmadıklarını idrak ederek, bu hükümlerin doğru anlaşılarak Avrupa Birliği ile bundan sonraki ilişkilerin Tüzük çerçevesinde yürütülmesinin gereğini daha net olarak anladıkları söylenebilir.

[427] French Data Protection Authority, (CNIL - The Commission Nationale de L'Informatique et des Libertes), Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019, Pronouncing a Financial Sanction Against GOOGLE LLC, https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf (02.06.2020), ss. 2, 7, 19, 21, 26-27-28.

SONUÇ VE DEĞERLENDİRME

Bilgi ve iletişim teknolojileri ile internet kullanımında ortaya çıkan devrim niteliğindeki gelişmeler neticesinde, kamusal işlemlerden, ticarete, siyasi ve sosyal hayata kadar pek çok yaşam alanı etkilenerek, kalıcı şekilde değişime uğramıştır. Manuelden dijitale olarak da nitelendirilebilen bu değişiklikler, bir çok tehdit ve fırsatı da beraberinde getirmişlerdir.

Artan veri akışı ve bu verilere erişimin kolaylaşması sayesinde, bilim ve teknolojide daha fazla ilerleme imkanının ortaya çıkması ile kamu sektörü ve özel sektörde işlemlerin dijitalleşmesiyle birlikte işlem süre ve maliyetlerinin azalması, katma değerli, kişiselleştirilmiş ve yenilikçi mal ve hizmetler ortaya konulmasının kolaylaşması bilgi ve iletişim teknolojileri ile internet kullanımında yaşanan gelişmelerin ortaya koyduğu önemli fırsatlar arasında sayılabilirler. Bu konuda ortaya çıkan en önemli fırsatlardan bir diğeri de, küresel e-ticaret hacminin tahminlerin çok ötesinde artmasıdır. Zira bu gelişmeler, dünya üzerindeki tüm pazarların dijital bir alternatifini ortaya koyarak, bu dijital pazarları da adeta görünmez kilitler yardımıyla birbirlerine bağlamıştır. Ortaya çıkan bu dijital bağlar sebebiyle, nerede kurulu olursa olsun bir ticari işletme, dünyanın herhangi bir yerindeki bir diğer işletme ya da tüketiciyle karşılıklı etkileşime geçerek, dijital pazarlarda kolaylıkla mal ve hizmet alıp satarak, e-ticaret yapabilmektedir.

Yaygınlaşarak dünyayı çepeçevre saran çok çeşitli dijital sistem ve çevirimiçi ağlardan oluşan ve geleceğin iş modelleri olarak da tasvir edilerek, büyük bir hızla genel ekonomi içerisindeki payını artıran dijital ekonominin dışında kalmak ise dünya üzerindeki hiç bir aktör için kabul edilebilir bir durum değildir. Nitekim Avrupa Birliği de, dijital pazarların yarattığı büyük ekonomik potansiyeli görerek, Birlik'in dijital ekonomiye entegrasyonunun sağlanması bağlamında pek çok çalışma yaparak, bu konuda çeşitli stratejiler geliştirmeye çalışmaktadır. Avrupa Birliği'nin bu hususta ortaya koyduğu en önemli strateji belgelerinden biri de "*Avrupa için Dijital Tek Pazar Stratejisi*"dir. Avrupa Birliği, işbu Strateji kapsamında, her türlü ticaret engelinden arındırılarak, uyumlu Birlik yasaları dahilinde regüle edilip, parçalı pazar görünümünden kurtarılacak yekpare bir Avrupa dijital tek pazarının,

Birlik'in dijital ekonomiye entegrasyonunun sağlanması bakımından atılacak en önemli adımlardan biri olduğunun bilincindedir.

Avrupa Birliği, sadece iç pazarda dahi 500 milyondan fazla tüketiciye ulaşma potansiyeline sahip bulunan Avrupa dijital tek pazarının tamamlanması yoluyla, Birlik ekonomisine yılda yaklaşık 415 milyon Avro katkı sağlanabileceğinin de altını önemle çizmektedir. Bu sebeplerle, Birlik, dijital dönüşümü gerçekleştirerek, Avrupa dijital tek pazarının tamamlanması çalışmalarına büyük kaynak ve efor sarfetmektedir. Avrupa Birliği, bu yolla her geçen gün gelişerek, küresel anlamda genel ekonomi içerisindeki payını artıran dijital ekonomiden alacağı payı yükselterek, sürdürülebilir büyümeyi yakalayıp, rekabet edebilirlik ve istihdam oranlarını da artırarak, Avrupa Birliği'nde refah artışını desteklemeyi de hedeflemektedir[428] [429].

Avrupa Birliği, bilgi ve iletişim teknolojileri ile internet kullanımındaki gelişmelerin yol açtığı dijitalleşmenin getirdiği tüm bu fırsatların farkında olarak, bir yandan dijital ekonomiye entegrasyon çalışmalarını sürdürürken, bir yandan da, bu fırsatların yanı sıra, pek çok tehditin de var olduğunun bilincindedir. Özellikle sınırlar ötesi veri akışındaki artış ve çevirim içi ağda toplanan verilerin büyük hacmi ve işlenme çeşitliliği ile bu verilere üçüncü kişilerin erişim oranlarındaki yükseliş sebebiyle ortaya çıkan, veri güvenliği ihlalleri ve buna bağlı olarak artan siber suçlar ile mahremiyete ve temel haklara ilişkin ihlaller, bu bağlamda sayılabilecek en önemli tehdit gruplarını oluşturmaktadırlar. Zira yaşanan dijital devrim ile birlikte hayatın her alanında ortaya çıkan çevirimiçi dijital ağ sistemleri içerisinde bulunan büyük miktar ve çeşitlilikteki kişisel ve kişisel olmayan veriler, tabiri caiz ise ışık hızı ile, kütleler halinde, sınırlar arasında oradan oraya aktarılarak, farklı amaçlarla ve çok çeşitli şekillerde işlenebilmektedirler. Hızla gelişen dijital teknikler karşısında

[428] Mario Monti, "A New Strategy for the Single Market At the Service of Europe's Economy and Society, Report to the President of the European Commission Jose Manuel Barroso", **Report**, 2010, https://www.kfw.de/migration/Weiterleitung-zur-Startseite/Homepage/KfW-Group/Research/PDF-Files/Monti_Report.pdf (02.06.2020), s.12-13,44. European Commission, Directorate-General for Research and Innovation, "Digitalisation Research and Innovation – Transforming European Industry and Services", August 2017, https://ec.europa.eu/pro-grammes/horizon2020/sites/horizon-2020/files/dt_booklet.pdf (02.06.2020), s. 4.

[429] Mal ve hizmetlerin dijitalleştirilerek, Avrupa dijital tek pazarının uyumlu yasalar kapsamında tamamlanması sureti ile, Birlik'in verimliliğinin artırılması sağlanarak, sadece Avrupa Birliği sanayisine dahi yıllık 110 milyar Avro katkı sağlanabileceği tahmin edilmektedir. Daha fazla bilgi için bkz. European Commission, Directorate-General for Research and Innovation, Digitalisation Research and Innovation – Transforming European Industry and Services, 2017.

engellenemeyen bu veri akışının ve işleme faaliyetlerinin, Birlik yasaları ile denetim altına alınarak, kişisel ve kişisel olmayan veri ayrımının doğru yapılması bu noktada büyük önem arz etmektedir. Nitekim bu ayrımın yapılarak Birlik hukukunda temel hak ve özgürlükler kapsamında tanınıp, koruma altına alınan kişisel verilerin, ortaya konacak Birlik düzeyinde uyumlu yasalar ve yaptırım mekanizmaları ile korunmaları, hem Birlik'in olmazsa olmaz etik değerlerinden sayılan temel hak ve özgürlüklerin güvence altına alınmasına, hem de Avrupa dijital tek pazarının güvenilirliğinin sağlanıp, parçalı yapısından kurtarılarak dijital ekonomiden alınacak payın yükseltilmesine, göz ardı edilemeyecek seviyede önemli katkılarda bulunabilecektir. Avrupa Birliği, tüm bu hususları bir arada göz önünde bulundurarak hazırladığı "*Avrupa için Dijital Tek Pazar Stratejisi*" ile, Avrupa dijital tek pazarının oluşumunun tamamlanması hedefi doğrultusunda kapsamlı bir Veri Koruma Reformu yapılmasının gereğinin altını önemle çizmiştir[430]. Zira, Birlik, gerçekleştirmeye çalıştığı ekonomik hedefleri doğrultusunda Avrupa dijital tek pazarının oluşumunu tamamlamaya çalışırken, aynı zamanda köklerinin dayandığı temel değerler ile insan haklarına saygı ilkesinden de ödün vermeye niyetli değildir.

Veri Koruma Reformu ile ortaya konan 2016/679 sayılı Genel Veri Koruma Tüzüğü, gerek temel hak ve özgürlüklerin Birlik düzeyinde korunması, gerekse de uyumlu Birlik yasaları dahilinde Avrupa dijital tek pazarının oluşumunun tamamlanarak, parçalı pazar görünümünden kurtarılması hususlarında atılmış önemli bir adım niteliğindedir.

Avrupa Temel Haklar Şartı'nın, Lizbon Antlaşması'na atıf yoluyla dahil edilmesiyle, kişisel veriler, Birlik hukukunda Kurucu Antlaşmalar düzeyinde koruma sağlanan temel haklardan biri haline gelmiştir. Ancak Genel Veri Koruma Tüzüğü'nün kabulüne kadar geçen sürede, kişisel veriler, bu verilerin korunması ve serbest dolaşımlarının sağlanmasında çerçeve niteliğinde hükümler getirip, bu hususta yasal düzenleme yapma yetkisini ise üye devletlere bırakması sebebiyle, Birlik içinde farklı uygulamaların ortaya çıkmasına sebep olarak eleştirilerin hedefi haline gelen mülga 95/46 sayılı Direktif kapsamında korunmaya çalışılmıştır. Oysa bilgi ve iletişim teknolojilerinde yaşanan gelişmeler ve dijital çağın gerekleri göz önüne alındığında, temel haklardan biri olan kişisel verilerin, Birlik hukukunda bir

[430] European Commission, "A Digital Single Market Strategy for Europe", **COM (192) Final**, 2015, ss.2, 11-14.

direktif kapsamında korunmasının yeterli olmadığı, dijital çağın gereksinimlerine uygun, Birlik düzeyinde uyumlu olan ve güçlü yaptırım mekanizmaları ile desteklenen, doğrudan uygulanabilir yasa hükümlerine ihtiyaç olduğu zaman içinde Birlik tarafından daha net olarak anlaşılmıştır. Genel Veri koruma Tüzüğü'nün kabulü ile kişisel verilerin, Birlik düzeyinde doğrudan uygulanabilir ve uyumlu yasa hükümleri kapsamında koruma kazanmaları, dijitalleşme ile ortaya çıkan yeni tehditlerle baş edilerek, temel hak ve özgürlüklerin daha etkili bir şekilde korunmaları, hem Avrupa dijital tek pazarında hukuki öngörülebilirlik ve güvenin tesisi ile pazarda işlem hacminin artırılması yoluyla, Birlik'in küresel dijital ekonomi kapsamında ortaya çıkan fırsatlardan en iyi şekilde yararlanması, hem de Avrupa dijital tek pazarının parçalı görünümünden kurtulması yönünde atılmış dev bir adım niteliğindedir. Zira kişisel verilerin Birlik düzeyinde doğrudan uygulanabilir, uyumlu ve güçlü yasalarla korunması, tamamlanmaya çalışılan Avrupa dijital tek pazarında veri güvenliğinin yükseltilmesine katkıda bulunacağı gibi, kişisel verilerin korunmasında ve serbest dolaşımlarının sağlanmasında Birlik içindeki yasa ve uygulama farklılıklarından kaynaklanan eşitsizlikleri gidererek, hukuki öngörülebilirliği de artıracaktır. Bu durum, Avrupa dijital tek pazarında işlem yapan çok uluslu firmalar da dahil tüm tüzel kişilerin, farklı üye devletlerin ulusal yasalarına uyum sağlama zorunluluğu sebebiyle geçmişte üstlenmek zorunda kaldıkları idari yükten kurtularak, Avrupa dijital tek pazarındaki işlemlerini daha kolay gerçekleştirmelerini de sağlayabilecektir. Ayrıca, kişisel verilerin korunması hususundaki uyumlu yasalar dahilinde veri güvenliğinin ve hukuki öngörülebilirliğin sağlanması, neticede Birlik içindeki ve dışındaki tüketicilerin güveninin kazanılmasını da beraberinde getireceğinden, bu durumun, orta ve uzun vadede, Avrupa dijital tek pazarındaki işlem hacmini yükseltip, Birlik'in dijital ekonomiden alacağı payı artırarak, Avrupa Birliği'nin ana hedeflerinden biri olan sürdürülebilir ekonomik kalkınmayı da desteklemesi beklenmektedir.

Tüm bunların yanı sıra, Genel Veri Koruma Tüzüğü, kişisel verilerin korunması ve Birlik dışı üçüncü ülkelere veri aktarımı hususlarında, temel hakların korunması perspektifinden hareketle bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte ortaya çıkan tehditlerle gerektiği gibi başa çıkılarak, kişisel verilere hak ettikleri yüksek korumanın sağlanması hedefleri doğrultusunda, üçüncü ülkelerle

kıyaslandığında sert hükümler içermektedir. Genel Veri Koruma Tüzüğü, bu sebeple, Avrupa Birliği'ni aşılması zor bir dijital kaleye dönüştürdüğü gerekçesi ile eleştirilmiştir. Ancak Genel Veri Koruma Tüzüğü'nün kişisel verilere Birlik genelinde sağladığı yüksek standartlardaki korumanın, hukuki öngörülebilirliği tesis ederek, Avrupa dijital tek pazarında güvenilirliği artırması sebepleriyle, orta ve uzun vadede bu eleştirileri boşa çıkararak, tüketici ve şirketlerin işlemlerinde Avrupa dijital tek pazarını tercih etmelerine ve neticede de rakipleri karşısında küresel ticarette Birlik'e rekabet avantajı sağlayarak, Avrupa Birliği'nin rekabet edebilirliğinin yükselmesine yol açacağı düşünülmektedir[431].

Özellikle Türkiye gibi aday ülkelerde kişisel verilerin korunması hususunda Birlik'teki gelişmelere paralel olarak yapılan yasal düzenlemeler incelendiğinde, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü kapsamında yapmış olduğu yasal düzenlemelerin, bu hususlarda farkındalık yaratarak, Birlik'in küresel arenada öncü kural koyucu olma hedefine katkı sağladığı da anlaşılmaktadır.

Economist Dergisi'nde yayınlanan 21 Aralık 2019 tarihli makale de, Birlik'in kişisel verilerin korunması hususunda üçüncü ülkelere kural ihraç ederek, bu konularda öncü olma iddiasını destekler niteliktedir. Nitekim bu makale ile, Amerika Birleşik Devletleri'nin Kaliforniya Eyaleti'nin, yürürlüğe girdiği tarihten itibaren, küresel arenada faaliyet göstererek, pek çok konuda lider durumda bulunan dev dijital teknoloji firmalarını derinden sarsan, 2016/679 sayılı Genel Veri Koruma Tüzüğü ile uyumlu olan, "*Kaliforniya Tüketici Mahremiyeti Kanununu (California Consumer Privacy Act-CCPA)*", Ocak 2019 tarihi itibarı ile, ülkenin tamamının önüne geçerek, kabul ettiğinin altı çizilmektedir. Avrupa Birliği'nin 500 milyonu aşkın kullanıcıya sahip olan yekpare dijital tek pazarında faaliyetlerine devam etmekte istekli olan, Microsoft ve Apple gibi Amerikan teknoloji devleri de bu gelişmelere paralel olarak yaptıkları açıklamalarla, CCPA'nın sadece Kaliforniya'da değil, Birleşik Devletlerin tamamında uygulanmasını sağlayacak düzenlemeleri yapmayı planladıklarını beyan etmişlerdir. Bu beyanlardan hareketle, Genel Veri Koruma Tüzüğü'nün, lider teknoloji firmalarının dikkatlerini yoğun olarak çekerek, Amerika Birleşik Devletleri de dahil olmak üzere küresel dünyanın tamamını kişisel verilerin korunması hususlarında etkilediği ve Birlik tarafından ortaya konan bu

[431] Jan Philipp Albrecht, ss. 287-289.

hüküm ve ilkelerin, yayılarak evrensel hale gelmede her geçen gün bir adım daha ileri gittiğini söylemek yanlış olmayacaktır[432]. Aday ülkeler de dahil üçüncü ülkelerde ortaya çıkan bu gelişmeler, Genel Veri koruma Tüzüğü'nün Birlik'i dijital bir kale haline getirdiği eleştirilerinin büyük oranda çürütülmesine neden olurken, aynı zamanda Birlik'in kişisel verilerin korunmasında öncü hale gelerek, üçüncü ülkelere kural ihraç etme iddiasını da güçlendirmektedir.

Mart 2020 tarihinden itibaren küresel dünyada olduğu gibi Avrupa Birliği'nde de içinde bulunduğumuz Covid 19 salgınına ilişkin etkiler, dramatik bir şekilde hissedilmeye başlanmıştır. Bu pandemi süreci beraberinde Birlik'in e-ticaret hacminde artış gibi kimi fırsatlar getirse de, aynı zamanda mahremiyetin ve kişisel verilerin korunması gibi temel hak ve özgürlükler kapsamında bazı önemli tehditler de ortaya koymuştur. Nitekim, Genel Veri Koruma Tüzüğü ile hassas kişisel veriler kapsamında kabul edilerek korunmalarına ilişkin daha sıkı kurallar getirilen bireylerin sağlık ve konum verilerinin korunmalarına ilişkin hükümlerin, kamu sağlığı ve kamu yararının korunması istisnaları çerçevesinde, pandemi döneminde Avrupa Birliği'nde de gevşetildiği anlaşılmaktadır. Bu durum özellikle mobil uygulamalar aracılığıyla, hasta kişilerin yerlerinin belirlenerek, bu kişilerin hareketlerinin kontrol edilmeye çalışılması hususunda atılan adımlarla iyiden iyiye su yüzüne çıkmaktadır. Toplum sağlığını etkileyen bu ölçekteki bir salgının, kimi kısıtlamaları kaçınılmaz kıldığı yadsınamasa da kişisel verilerin korunmasına ilişkin istisnaların uygulanırken, Genel Veri Koruma Tüzüğü madde 23/1'de belirtildiği gibi hakkın özüne dokunmadan, meşru bir amaca hizmet etmek için gerekli olandan fazla olmamak kaydı ile ve toplumsal demokrasi anlayışına zarar gelmeden orantılılık ilkesi çerçevesinde yapılmasının gerekli ve önemli olduğu unutulmamalıdır.

Sonuç olarak söylemek gerekirse; Genel Veri Koruma Tüzüğü ile getirilen Birlik düzeyinde uyumlu yasal düzenlemelerin, temel hak ve özgürlüklerin korunarak, kişisel verilerin Avrupa dijital tek pazarında güvenli bir şekilde serbest dolaşımlarının sağlanması temel hedeflerinin gerçekleşmesine katkıda bulunduğu yadsınamaz. Ancak Genel Veri Koruma Tüzüğü ile Avrupa Birliği'nin kişisel verilerin korunması hususunda kat etmiş olduğu önemli mesafeye rağmen, gerek şirketlerin, gerek çalışanların, gerekse de hane halkının dijital kültürü benimseyerek

[432] **Ekonomist Dergisi**, 21 Aralık 2019 tarihli sayısı, Business Bölümü, "California's Data Sheriffs", s.91.

bu bağlamda gerekli teknik becerileri elde edebilmeleri noktasında, Avrupa Birlik'nin, ABD, Çin, Güney Kore gibi rakipleri ile karşılaştırıldığında hala biraz daha geride olduğu söylenebilir. Avrupa dijital tek pazarından alınacak verimin artırılabilmesi için Avrupa Birliği'nin birey ve şirketlerin, dijital becerilerini ve dijital atmosfere uyumlarını artırırken, aynı zamanda da temel hak ihlallerinin önüne geçebilecek şekilde gerekli teknik ve yasal tedbirler almaya ve bu uğurda güncellemeler yapmaya devam ederek, hem Avrupa dijital tek pazarına duyulan güveni artırırken, hem de dijital okur yazarlık ve teşebbüslerin dijitalleşmesi oranlarını yükseltmesi, aynı zamanda da kişisel verilerin korunması hususunda farkındalık yaratması önemlidir.

Bilgi ve iletişim teknolojileri ve internet alanında yaşanan gelişmeler büyük bir süratle devam ettiğinden, Avrupa Birliği'nin kişisel verilerin korunması bağlamında ortaya çıkabilecek yeni fırsat ve tehditlere ilişkin çalışmalarını sürdürmesinin ne kadar önemli olduğu bir kere daha ortaya çıkmaktadır. Bu sebeple, bu tez çalışması kapsamında yapılan incelemeler neticesinde, Avrupa dijital tek pazarının gelişimi bağlamında önümüzdeki süreçte de kişisel verilerin korunması konusunun önemini koruyacağının altı çizilirken, Birlik'in bu konudaki araştırma ve çalışmalarının da devam edeceği öngörülmektedir.

KAYNAKÇA

Akgül Açıkmeşe, Sinem. "Uluslararası İlişkiler Teorileri Işığında Avrupa Bütünleşmesi", **Uluslararası İlişkiler Dergisi**, Cilt. 1, Sayı.1, 2004, ss. 1-32

Akgül, Aydın. **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması (Unutulma Hakkı ve Biyometrik Veriler İlaveli)**, 2.Baskı, Beta Yayınları, İstanbul, 2016

Akıncı, Ayşe Nur. "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", T.C. Kalkınma Bakanlığı, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, **Çalışma Raporu,** No. 6, Yayın No.2968, Haziran 2017, http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf, (02.06.2020).

Akses, Selen. "Avrupa 2020 Stratejisi", **İktisadi Kalkınma Vakfı (İKV) Yayın No.269**, 2014, https://www.ikv.org.tr/images/files/2020stratejisi.pdf, (02.06.2020)

Aksoy, Mehmet Ali. "2005/29/AT Haksız Ticari Uygulamalar Direktifinde Düzenlenen Haksız Rekabet Halleri ve Uygulama Örnekleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXXIII, Sayı: 1, 2015, ss. 279-318

Albrecht, Jan Philipp. "How the GDPR Will Change the World", **European Data Protection Law Review**, Cilt.2, Sayı.3, 2016, ss. 287-289

Alexe, Irina. "Personal Data Protection, The Sanctioning Regime Provided by Regulation (EU) 20167679 on the Protection of Personal Data", **Law Review**, Cilt.VIII, Sayı.1, January-June 2018, ss. 60-70

Ambrose, Meg Leta. "It's about time: Privacy, Information Life Cycles and the Right to be Forgotten", **Stanford Technology Law Review**, Cilt.16, Sayı.2, 2013, ss. 101-154

Amerikan Bağımsızlık Bildirgesi, 1778, https://tr.wikisource.org/wiki-/Amerikan_Bağımsızlık_Bildirgesi, (02.06.2020).

Aras, İlhan. "Avrupa Birliği Hukukunun Önceliği İlkesi", **Sayıştay Dergisi**, Cilt. 99, Ekim-Aralık 2015, ss. 5-28

Arıboğan, Deniz Ülke. **Globalleşme Senaryosunun Aktörleri-Uluslararası İlişkilerde Güç Mücadelesi**, 2. Baskı, Der Yayınları, İstanbul, 1997

Armağan Ebru Bozkurt Yüksel, **Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing)**, Yetkin, Ankara, 2016

Article 29 Data Protection Working Party, "Advice Paper on Special Categories of Data *("Sensitive Data"*)", **Ref.Ares (2011)444105** – 20.04.2011, https://www.pdpjournals.com/docs/88417.pdf, (02.06.2020)

Article 29 Data Protection Working Party. "Guidelines on Consent under Regulation 2016/679, Adopted on 28.11.2017", **WP259rev.01**, as last revised and adopted on 10.04.2018, https://ec.europa.eu/newsroom/article29/ite-mdetail.cfm?item_id=623051 (02.06.2020)

Article 29 Data Protection Working Party. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is '*Likely to result in a High Risk*' for the Purposes of Regulation", 2016/679, 13.10.2017, **17/EN WP 248** rev.01, https://ec.europa.eu/newsroom/artic-le29/item-detail.cfm?item_id=611236, (02.06.2020)

Article 29 Data Protection Working Party. "Guidelines on Data Protection Officers ("DPOs")" Adopted on 13 December 2016, **16/EN WP 243**, https://ec.europa.eu/information_society/newsroom/image/document/201651/wp243_en_40855.pdf?wb48617274=CD63BD9A (02.06.2020)

Article 29 Data Protection Working Party. "Guidelines on Personal Data Breach Notification under Regulation 2016/679", 03.10.2017, **WP250 17/EN**, https://webcache.googleusercontent.com/search?q=cache:X49fS0vPpRgJ:https://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D47741+&cd=1&hl=tr&ct=clnk&gl=tr&client=safari, (02.06.2020)

Article 29 Data Protection Working Party. "Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation", 2016/679, **17/EN WP 253**, 3.10.2017, https://knowww.eu/search-tree?t=5ad7131ed39f5-aa2bcbf0f34#, (02.06.2020)

Article 29 Data Protection Working Party. "Guidelines on the Right to Data Portability", adopted on 13 December 2016 as last revised and adopted on 5 April 2017, **WP 242**, rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233, (02.06.2020)

Article 29 Data Protection Working Party. "Guidelines on Transparency under Regulation 2016/679", **WP260**, adopted on 29.11.2017, as last revised and adopted on 11.04.2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item-_id=622227, (02.06.2020)

Atasoy, Kemal. "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası", **Marmara Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof.Dr. Cevdet Yavuz'a Armağan, Cilt 22, Sayı 3, 2016, ss. 269-301

Avrupa Birliği Türkiye Delegasyonu Resmi Sitesi. Avrupa Birliği Temel Haklar Bildirgesi Tercümesi, https://www.avrupa.info.tr/tr/avrupabirligitemelhaklarbildirgesi708, (02.06.2020)

Avrupa Konseyi. 108 No'lu Sözleşme Metni, https://rm.coe.int/1680078b37 (02.06.2020)

Avrupa Konseyi. Avrupa İnsan Hakları Sözleşmesi (11 ve 14. Protokollerle değiştirilen metin-Ek Protokol ile Protokol 4, 6,7,12 ve 13 eklenmiştir), http://www.echr.coe.int/Documents/Convention_TUR.pdf, (02.06.2020)

Aybay, Rona. "Açıklamalı İnsan Hakları Evrensel Bildirisi", **Türkiye Barolar Birliği Yayınları,** No. 113, Türkiye Barolar Birliği İnsan Haklan Araştırma ve Uygulama Merkezi dizisi: 7, Ankara, 2006, http://tbbyayinlari.barobirlik.org.tr/TBBBooks/iheb.pdf (02.06.2020)

Ayözger, Çiğdem. **Kişisel Verilerin Korunması-Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, 1. Baskı, Beta Yayınları, İstanbul, 2016

Baars, Anoek. The Value of Personal Data in a Competitive Information Age, **Master Thesis,** University of Oslo, Faculty of Law https://www.duo.uio.no/bitstream/handle/10852/51383/8011_ICTLTHESIS.pdf?sequence=1, (02.06.2020)

Bagnoli, Vicente. "The Big Data Relevent Market", **Concorrenza e Mercato**, Cilt. 23, 2016, ss. 73-94

Baker & McKenzie. "A Changing World: New Trends in Emerging Market Infrastructure Finance", https://www.bakermckenzie.com/en/insight/publications/2018/12/emerging-market-infrastructure-finance, (02.06.2020)

Baker & McKenzie. "Ghosts in the Machine Revisited the State of Artificial Intelligence, Risks and Regulation in Financial Services", http://www.euromoneythou-ghtleadership.com/ghosts2/, (02.06.2020)

Baldwin, Richard E. ve Martin, Philippe. "Two Waves of Globalization: Superficial Similarities, Fundamental Differences", **Working Paper: 6904**, 1999, http://www.nber.org/papers/w6904.pdf , (02.06.2020)

Balkin, Jack M. "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", **New York University Law Review**, Cilt 79, Sayı 1, 2004, ss. 1-55

Bartlett, Will ve Prica, Ivana. "Interdependence between Core and Peripheries of the European Economy: Secular Stagnation and Growth in the Western Balkans", **LSE "Europe in Question" Discussion Paper Series No. 104**, 2016, http://www.lse.ac.-uk/europeaninstitute/Assets/Documents/LEQSDiscussionPapers/LEQSPaper104.pdf, (02.06.2020)

Bassini, Marco ve Pollicino, Oreste. "Reconciling Right to be Forgotten and Freedom of Information in the Digital Age: Past and Future of Personal Data Protection in the European Union", **Diritto Pubblico Comparato ed Europeo**, Cilt.2014/2, ss. 641-662,https://www.academia.edu/1-9963974/Reconciling_right_t_be_forgotten_and_freedom_of_information_in_the_digital_age._Past_and_future_of_personal_data_protection_in_the_European_Union, (02.06.2020)

Başalp, Nilgün. "Avrupa Birliği Veri Koruma Genel Regulasyonu'nun Temel Yenilikleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (MÜHF HAD)**, 2015, Cilt.21, Sayı.1, ss. 77-105

Başalp, Nilgün. **Kişisel Verilerin Korunması ve Saklanması**, Yetkin, Ankara, 2004

BBC. "Adidas websites go offline after hacking cyber-attack", **BBC Technology News**, 2011https://www.bbc.com/news/technology-15614590, (02.06.2020)

Bendiek, Annegret. "European Cyber Security Policy", **Research Paper 13,** Berlin 2012, Stiftung Wissenschaft und Politik-SWP- Deutsches Institut für Internationale Politik und Sicherheit (Ed.)

Bieker, Felix, Fiedewald, Michael, Hansen, Marit, Obersteller, Hannah ve Rost, Martin. "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation", **Privacy Technologies and Policy** (Ed. S.Schiffner et.al), Annual Privacy Forum, Springer International Publishing, Switzerland, 2016

Bilgin, Ahmet Burak. "Avrupa Birliği Hukukunda Hukukun Genel İlkeleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXXIV, Sayı: 1, 2016, ss. 73-94

Bird & Bird. **Guide to the General Data Protection Regulation**, 2017, https://www.twobirds.co-m/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en, (02.06.2020)

Birleşmiş Milletler, Genel Kurulu, **İnsan Hakları Evrensel Beyannamesi**, 1948, https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf, (02.06.2020)

Blackmer, W. Scott. "GDPR: Getting Ready for the New EU General Data Protection Regulation", **Info Law Group**, 2016, https://www.infolawgroup.com/insight-s/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation , (02.06.2020)

Borgesius, Frederick J. Zuiderveen, Steenbruggen, Wilfred. "The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression and Trust", Working Draft, 31 August 2018, Forthcoming, **Theoretical Inquiries in Law**, **SSRN**, https://papers.ssrn.com/sol3/papers.-cfm?abstract_id=3152014, (02.06.2020)

Botha, Henk. "Human Dignity in Comparative Perspective", **STELL LR**, Cilt.2, 2009, ss. 171-220

Breckenridge, Adam Carlyle. **The Right to Privacy**, University of Nebraska Press, Lincoln, 1970, s. 14, Aktaran Mehmet Yüksel "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", **Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi**, Cilt.58, Sayı. 1, 2003, ss. 181-213

Brynjolfsson, Erik ve Kahin, Brian. **Understanding the Digital Economy: Data, Tools and Research**, MIT Press, UK, 2002

Buijze, Anoeska Wilhelmina Geertruida Johanna. "The Principle of Transparency in EU Law", **Thesis,** 2013, Uitgeverij BOX Press, 's-Hertogenbosch, ISBN 978-90-8891-579-6

Bulut, Serkan. "Söylemin Kapatılma ve Açımlama Savaşımında Edward Snowden", **Üsküdar Üniversitesi İletişim Fakültesi Akademik Dergisi**, Cilt.2, Sayı.3, 2019, ss. 128-140

Burri, Mira ve Schar, Rahel. "The Reform of the EU Data Protection Framework, Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", **Journal of Information Policy**, Cilt.6, 2016, ss. 479-511

Burton, Cedric, Laura de Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot ve Sara G.Hoffman. "Privacy and Security Law Report, EU Regulation, The Final European Union General Data Protection Regulation", **Bloomberg BNA**, 2016, https://www.wsgr.com/images/content/2/7/v1/27-8/bloombergBNA-0116.pdf (02.06.2020)

Buttarelli, Giovanni. "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard", Guest Editorial. **International Data Privacy Law**, Cilt.6, Sayı.2, 2016, ss. 77-78

Bygrave, Lee A. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, **International Journal of Law and Information Technology**, Cilt.6, Sayı.3, ss. 247-284

Cannataci, Joseph A. "Lex Personalitatis & Technology-driven Law", **Scripted**, Cilt.5, Sayı.1, 2008, ss.16, https://www.um.edu.mt/library/oar/bitstream/123456789/17704/1/OA%20%20%20%20-Lex%20Personalitatis%20%26%20Technology-driven%20Law.pdf, (02.06.2020)

Carlsson, Ulla. "Freedom of Expression and the Media in a Time of Uncertainty, A Brief Introduction", **Freedom of Expression and Media in Transition, Studies and Reflections in the Digital Age**, (Ed. Ulla Carlsson), Nordicom, 2016

Casagran, Christina Blasi. Global Data Protection in the field of Law Enforcement: An EU Perspective, Routledge, 1. Baskı, Oxon & New York, 2017

Cate, Fred H. "The EU Data Protection Directive, Information, Privacy and the Public Interest", **Articles by Maurer School of Law: Indiana University**, Paper 646, 1995, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1647&context-=facpub, (02.06.2020)

Cate, Fred H. "The Failure of Fair Information Practice Principle", **Consumer Protection in the Age of the Information Economy** (Ed. Jane K.Winn), Burlington, Ashgate, 2006

Cavoukian, Ann. "Privacy by Design, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf, (02.06.2020)

Cavoukian, Ann. "Privacy by Design: the Definitive Workshop. A Foreword by Ann Cavoukian", **Identity in the Information Society (IDIS) 3**, 2010, ss. 247-251

Census Act. "English Translation of Essential Parts of the German "Volkszahlungsurteil" from 15 December 1983, which established in Germany the Basic Right on Informational Self-Determination", **BVerfGE 65,1**, https://freiheitsfoo.de/census-act/ (02.06.2020)

Center for Information Policy Leadership, Hunton & Williams LLP. **GDPR Implementation In Respect of Children's Data and Consent**, 6.03.2018, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf (02.06.2020)

Clifford, Damian. Jef Ausloos. Data Protection and the Role of Fairness, KU Leuven, Center for IT & IP Law, **Working Paper Series 29/2017**, https://ssrn.com/abstract=3013139, (02.06.2020)

Columbia University, Global Freedom of Expression, "Google Spain SL V. Agencia Espanola de Proteccion de Patos" , **Case Analysis**, https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/, (02.06.2020)

Commission. Implementing Regulation 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment", **Official Journal of the European Union**, **L 344/46,** 17.12.2016, https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32016R2286, (02.06.2020)

Commission. Implementing Decision 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-US Privacy Shield, **Official Journal L 207/1**, 01.8.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.-2016.207.01.0001.01.ENG, (02.06.2020)

Commission Decision. 2000/520/EC (No longer in force) 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), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A320-00D0520, (02.06.2020)

Communication from the Commission to the European Parliament and Council. "The Impact and Effectiveness of the Single Market", **COM(96) 520**, 1996, http://ec.europa.eu/internal_market/economic-reports/docs/single_en.pdf, (02.06.2020)

Cooke, Phil ve De Propris, Lisa. "A Policy Agenda for EU Smarth Growth: The Role of Creative and Cultural Industries", **Policy Studies Journal**, Cilt.32, Sayı.4, 2011, ss. 365-375

Copeland, Paul. "Conclusion: The Lisbon Strategy Evaluating Success and Understanding Failure", **The EU's Lisbon Strategy** (Ed. Paul Copeland, Dimitris Papadimitriou), Palgrave Macmillan, London, 2012

Council of Europe. "Realising Both Economic Growth and Social Protection in Europe in an Era of Globalisation", **Resolution 1573**, 2007, http://assembly.coe.int/nw/xml/XRef/XrefXML2HTMLen.asp?fileid=17580&lang=en, (02.06.2020)

Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, **European Treaty Series Sayı. 108**, 1981, https://rm.coe.int/1680078b37, (02.06.2020)

Council of Europe. **European Convention on Human Rights**, 1950, https://www.echr.coe.int/Pages/ho-me.aspx?p=basictexts&c, (02.06.2020)

Council of Europe. Parliamentary Assembly. "Declaration on Mass Communication Media and Human Rights", **Resolution 428(1970),** http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNTg0MiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE1ODQy, (02.06.2020)

Council of the EU. "Geo-blocking: Council adopts regulation to remove barriers to e-commerce", **Press Release 95/18,** 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/02/27/geo-blocking-council-adopts-regulation-to-remove-barriers-to-e-commerce/pdf , (02.06.2020)

Council of the European Union. **EU Human Rights Guidelines on Freedom of Expression Online and Offline,** Foreign Affairs Council Meeting, Brussels, 2014, https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf, (02.06.2020)

Court of Justice of the European Union. Research and Documentation Directorate, **ECJ Fact Sheet**, Protection of Personal Data, 2017, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf, (02.06.2020)

Cunha, Mario Viola de Azevedo. **Market Integration Through Data Protection, An Analysis of the Insurance and Financial Industries in the EU**, Law, Governance and Technology Series 9, Springer, Heidelberg, 2013

Çakan, Cansu. "Kişilik Hakkı Kapsamında Korunan Bir Değer Olarak Kişisel Veriler", **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.12, Sayı. 2, 2013, ss. 187-222

Çapanoğlu, Sema Gençay. "Geçmişten Günümüze Lizbon Stratejisi ve 2020 için Yeni Bir Vizyon Işığında "AB 2020" Stratejisi", **İKV Değerlendirme Notu**, 2010, https://www.ikv.org.tr/images/upload/data/files/gecmisten_gunumuze_lizbon_stratejisi_ve_2020_icin_yeni_bir_vizyon_isiginda_ab_2020_stratejisi.pdf, (02.06.2020)

Çelik, Ahmet ve Yaşar Tonta. "Düşünce Özgürlüğü, Bilgi Edinme Özgürlüğü ve Bilgi Hizmetleri", ***Bilgi Edinme Özgürlüğü***, (Ed.Yaşar Tonta, Ahmet Çelik), Türk Kütüphaneciler Derneği Genel Merkezi Yayınları No.21, Ankara, 1996

Dağlı, İlke ve Derviş, Erel. Medeni Özgürlük Üzerine Düşünceler (revised by Prof.Esin Orucu), http://www.peterforsskal.com/thetext-tu.html, (02.06.2020)

Dam, Rob van der. The Trust Factor in the Digital Economy: Why Privacy and Security is Fundamental for Successful Ecosystems, 14th International Telecommunications Society (ITS) Asia-Pacific Regional Conference: "Mapping ICT into Transformation for the Next Information Society", Kyoto, 2017, **ECONSTOR,** https://www.econstor.eu/bitstream/10419/-168536/1/Rob-van-den-Dam.pdf, (02.06.2020)

Danezis, George ve Domingo-Ferrer, Josep, Hansen, Marit, Hoepman, Jaap-Henk, Le Métayer, Daniel, Tirtea, Rodica, Schiffner, Stefan. "Europa Union, Privacy and Data Protection by Design from Policy to Engineering", **ENISA**, December 2014, https://www.enisa.europa.eu/publ-ications/privacy-and-data-protection-by-design, (02.06.2020)

De Hert, Paul ve Czerniawski, Michal. "Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context", **International Data Privacy Law**, Cilt.6, Sayı 3, 2016, ss. 230-243

De Hert, Paul ve Papakonstantinou, Vagelis. "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", **Computer Law & Security Review**, Cilt.28, Sayı.2, 2012, ss. 130-142

Demirdal, M.Balkan. "Uluslararası İnsan Hakları Hukukunda Ölüm Cezasının Kaldırılması ve Türkiye'deki Süreç", **Politik Ekonomik Kuram**, Cilt.2, Sayı.1, 2018, ss. 57-72

Develioğlu, Hüseyin Murat. **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, 1.Baskı, Oniki Levha Yayınları, İstanbul, 2017

Diaz Diaz, Efrén. "The New European Union General Regulation on Data Protection and the Legal Consequences for Institutions", **Church, Communication and Culture**, Cilt.1, Sayı.1, 2016, ss. 206-239

"Der Grundrechtssatz von der Menschenwürde: Entwurf eines praktikablen Wertsystems der Grundrechte aus Art.1 Abs. I in verbindung mit Art.19 Abs. II des Grundgesetzes", Archiv des Öffentlichen Rechts, Cilt.81, (N.F.42), Sayı. 2, 1956, ss. 117,127, Aktaran Matthias Mahlmann, "Human Dignity and Authonomy in Modern Constitutional Orders", **The Oxford Handbook of Comparative Constitutional Law** (Ed. Michel Rosenfeld, Andras Sajo), Oxford University Press, 2012, https://www.jura.unihamburg.de/media/ueberdiefakultaet/personen/albersmarion/seoul-national-university/course-outline/mahlmann-2013-human-dignity-and-autonomy-in-modern-constitutional-orders.pdf, (02.06.2020)

Digital Europe. "A Transformational Agenda For The Digital Age: Digital Europe's Vision 2020", **WhitePaper,** 2009, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=157&language=enUS&PortalId=0&TabId=353, (02.06.2020)

Diker Vanberg, Aysem ve Ünver, Mehmet Bilal. "The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?", **European Journal of Law and Technology**, Cilt.8, Sayı.1, 2017, ss. 1-22

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning processing of personal data and the protection of privacy in the electronic communications sector (*Directive on Privacy and Electronic Communications*) **Official Journal L 201**, 31.7.2002, ss.37-47, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=15507563229-30&uri=CELEX:32002L0058, (02.06.2020)

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No.2006/2004 of the European Parliament and of the Council ("Unfair Commercial Practices"), **Official Journal, L 149**, 11.6.2005, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1540545283496&u-ri=CELEX:32005L0029, (02.06.2020)

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services, **Official Journal**, **L 337/37,** 18.12.2009, https://eurlex.europa.eu/legalcontent/en/ALL/?uri=CELEX:32009L0140, (02.06.2020)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, **Official Journal L 281**, 23/11/1995 P.0031 – 0050, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31-995L0046, (02.06.2020)

Dittrich, Paul-Jasper. "Balancing Ambition and Pragmatism for the Digital Dingle Market", **Berlin Jacques Delors Institut Policy Paper 204**, 7.9.2017, https://institutdelors.eu/wpcontent/uploads/2018/01/balancingambitionandpragmatismforthedigitalsinglemarket-dittrich-jdib-sept2017.pdf, (02.06.2020)

Doğan, Korcan ve Arslantekin, Sacit. "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum", **Ankara Üniversitesi Dil ve Tarih Coğrafya Fakültesi Dergisi**, Cilt.56, S.1, 2016, ss. 15-36

Doğan, Pınar Bahar. "Çatışan İki Değer: Haber Verme Hakkı ve Kişilik Hakkı", **Ankara Barosu Dergisi**, Sayı.4, ss. 477-493

Dollar, David. "Globalization, Poverty and Inequality since 1980", **World Bank Policy Research Working Paper 3333**, 2004, https://openknowledge.worldbank.org /bitstream/handle/10986/14128/wps3333.pdf?sequence=1, (02.06.2020)

Donnelly, Jack. Human Rights as Natural Rights, Human Rights Quarterly, **Johns Hopkins University Press,** Cilt. 4, Sayı.3, 1982, ss. 391-405

Dürig, Günter. "Die Menschenauffassung des Grundgesetzes", 1952, s.259 Aktaran Matthias Mahlmann, "Human Dignity and Authonomy in Modern Constitutional Orders", **The Oxford Handbook of Comparative Constitutional Law** (Ed. Michel Rosenfeld, Andras Sajo), Oxford University Press, 2012, https://www.jura.uni-hamburg.de/media/ueber-die-fakultaet/personen/albers-marion/seoul-national-university/course-outline/mahlmann-2013-human-dignity-and-autonomy-in-modern-constitutional-orders.pdf, (02.06.2020)

Eberle, Edward J. "The German Idea of Freedom", **Oregon Revıew of Int'l Law**, Cilt.10, 2008, ss.1-76, http://docenti.unimc.it/benedetta.barbisan/teaching/2014/12694/files/thirteenth-and-fourteenth-class-10-11november/human-dignity-in-the-german-basic-law-2, (02.06.2020)

Ekonomist Dergisi, 21 Aralık 2019 tarihli sayısı, Business Bölümü, "California's Data Sheriffs"

ENISA. "The European Cyber Security Challenge: Lessons Learned", **ENISA Report**, 2017, https://www.enisa.europa.eu/publications/the-european-cyber-security-challenge-lessons-learned-report , (02.06.2020)

ENISA. https://www.enisa.europa.eu/about-enisa, (02.06.2020)

Esayas, Samson Yoseph. "The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the 'All or Nothing' " **Approach, European Journal of Law and Technology**, Cilt.6, Sayı.2, 2015, ss. 1-23

Eurojust, http://eurojust.europa.eu/Pages/home.aspx , (02.06.2020)

European Commision. **Digital Agenda for Europe**, 2014, http://eige.europa.eu/resources/-digital_agenda_en.pdf, (02.06.2020)

European Commission and its Priorities. "Cross-border Portability of Online Content Services", 2019, https://ec.europa.eu/digital-single-market/en/cross-border-portability-online-content-services, (02.06.2020)

European Commission. "Communication on an Action Plan on VAT Towards a Single EU VAT Area Time to Decide", **148 final,** 7.4.2016, https://ec.europa.eu/taxation_customs/sites/taxation/files/com_2016_148_en.pdf, (02.06.2020)

European Commission. "A Comprehensive Approach to Stimulating Cross-border E-Commerce for Europe's Citizens and Businesses", **320 Final**, 25.5.2016, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-320-EN-F1-1.PDF, (02.06.2020)

European Commission. "A Digital Single Market for Europe: Commission Sets Out 16 Initiatives to Make it Happen", **Press Release**, 2015, http://europa.eu/rapid/press-release_IP-15-4919_en.htm, (02.06.2020)

European Commission. "A Digital Single Market Strategy for Europe", (**COM 192) Final,** 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A520-15DC0192, (02.06.2020)

European Commission. “Analysis of options beyond 20% GHG emission reductions: Member State Results”, **Commission Staff Working Paper,** 1.2.2012, https://ec.europa.eu/clima/sites/clima/files/strategies/2020/docs/swd_2012_5_en.pdf, (02.06.2020)

European Commission. “Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A New Skills Agenda for Europe, Working together to strengthen human capital, employability and competitiveness”, **COM (2016) 381 final,** 10.06.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52-016DC0381, (02.06.2020)

European Commission. “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on the Mid-term, Review on the Implementation of the Digital Single Market Strategy, A Connected Digital Single Market for All”, **(COM 228) final**, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%-3A2017%3A228%3AFIN, (02.06.2020)

European Commission. “Communication on an Action Plan on VAT Towards a Single EU VAT Area Time to Decide”, **148 final,** 7.4.2016, https://ec.europa.eu/taxation_customs/sites/taxatio-n/files/com_2016_148_en.pdf, (02.06.2020)

European Commission. “Communication Towards a Modern, More European Copyright Framework”, **626 final**, 9.12.2015, https://ec.europa.eu/digital-single-market/en/policies/copyright, (02.06.2020)

European Commission. “Completing a Trusted Digital Single Market for All, The European Commission’s contribution to the Informal EU Leaders’ Meeting on Data Protection and the Digital Single Market in Sofia on 16 May 2018”, **COM 320 Final**, 2018 https://ec.europa.eu/transparency/reg-doc/?fuseaction=list&coteId=1&year=2018&number=320&language=EN, (02.06.2020)

European Commission. “Completing the Internal Market”, **White Paper,** Milan, 28-29.06.1985, https://op.europa.eu/en/publicationdetail//publication/4ff490f3dbb64331a2eaa3ca59f974a8/language-en, (02.06.2020)

European Commission. “Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society”, **COM 300 final**, 14.9.2016, https://ec.europa.eu/digital-single-market/en/news/communication-connectivity-competitive-digital-single-market-towards-european-gigabit-society, (02.06.2020)

European Commission. “Digital Agenda for Europe, Rebooting Europe’s Economy”, **EU Publications**, 2014, https://op.europa.eu/en/publication-detail/-/publication/27a0545e-03bf-425f-8b09-7cef6f0870af, (02.06.2020)

European Commission. “Digital Single Market: EU Negotiators Reach a Political Agreement to Update the EU’s Telecoms Rules”, **Press Release**, 2018, http://europa.eu/rapid/press-release_IP-18-4070_en.htm, (02.06.2020)

European Commission. “Directorate General Internal Market and Services, Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries”, **Summary of Responses,** 4.7./12.9.2012, https://ec.europa.eu/digital-single-market/en/news/archive-e-commerce-directive-what-happened-and-its-adoption, (02.06.2020)

European Commission. “E-commerce Action Plan 2012-2015, State of Play 2013”, **SWD 2013, 153 final,** http://ec.europa.eu/information_society/newsroom/image/document/2017-4/130423_report-ecommerce-action-plan_en_42073.pdf, (02.06.2020)

European Commission. “End of Roaming Charges in the EU in 2017: Commission Agrees on New Approach to Make it Work for All Europeans”, **Press Release**, 21.09.2016, http://europa.eu/rapid/press-release_IP-16-3111_en.htm, (02.06.2020)

European Commission. “Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth”, **Com (2010) 2020 Final,** 3.3.2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=C-OM:2010:2020:FIN:EN:PDF, (02.06.2020)

European Commission. “European Commission President Jose Manuel Barrosso Proposes a Partnership for Progress and Ambition to the European Parliament”, **Press Release Data Base, IP/09/1272**, 2009, http://europa.eu/rapid/press-release_IP-09-1272_en.htm, (02.06.2020)

European Commission. “Integration of Digital Technology, Digital Economy and Society Index Report”, 2018, http://ec.europa.eu/information_society-/newsroom/image/document/201820/4_desi_report_integration_of_digital_technology_B61BEB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf, (02.06.2020)

European Commission. “Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)”, Brussels, **COM (2012), 11 Final,** 25.1.2012, https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF, (02.06.2020)

European Commission. “Reflection Paper on Harnessing Globalisation”, **COM (2017) 240**, 10.05.2017, https://eurlex.europa.eu/legal-content/EN/TXT/?qid=-1544609950797&uri=CELEX:52017DC0240, (02.06.2020)

European Commission. “Shaping Europe’s Digital Future, a European Strategy for Data”, **Policy**, https://ec.europa.eu/digital-single-market/en/p-olicies/building-europeandataeconomy , (02.06.2020)

European Commission. “Shaping Europe’s Digital Future, Open Science”, **Policy,** https://ec.europa.eu/digital-single-market/en/open-science, (02.06.2020)

European Commission. “State of the Union 2016: Commission Paves the Way for More and Better Internet Connectivity for all Citizens and Businesses”, **Press Release**, 14.09.2016, http://europa.eu/rapid/press-release_IP-16-3008_en.htm, (02.06.2020)

European Commission. “The EU and The Digital Single Market”, **EU Publications**, 2017, http://publications.europa.eu/webpub/com/factsheets/digital/en/, (02.06.2020)

European Commission. “The European Union Explained Digital Agenda for Europe”, 2014, https://eige.europa.eu/resources/digital_agenda_en.pdf, (02.06.2020)

European Commission. “Towards a Safer Use of Internet for Children in the European Union – A Parents’ Perspective”, Analytical Report, **Flash Eurobarometer Series** 248, The Gallup Organization, 2008, https://ec.europa.eu/commfrontoffice/publicopinion/flash/fl_248_en.pdf, (02.06.2020)

European Commission. **Adequacy Decisions**, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (02.06.2020)

European Commission. 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 final**, 4.11.2010, https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF, (02.06.2020)

European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “A Digital Agenda for Europe”, **COM 245**, 2010, https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF, (02.06.2020)

European Commission. Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, 10.1.2017, **COM (2017) 7 final**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN, (02.06.2020)

European Commission. Directorate-General for Research & Innovation, "H2020 Programme, Guidelines to the rules on Open Access to the Scientific Publications and Open Access to Research Data in Horizon 2020", **H2020 Programme,** Version 3,2, 21.03.2017, https://ec.europa.eu/research/p-articipants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf, (02.06.2020)

European Commission. Directorate-General for Research and Innovation, "Digitalisation Research and Innovation – Transforming European Industry and Services", August 2017, https://ec.europa.eu/pro-grammes/horizon2020/sites/horizon-2020/files/dt_booklet.pdf, (02.06.2020)

European Commission. **Press Release Database**, "Data Protection Reform – Frequently asked Questions", 4.11.2010, http://europa.eu/rapid/press-release_MEMO-10-542_en.htm (02.06.2020)

European Commission. **Press Release**, "Agreement on Commission's EU Data Protection Reform will Boost Digital Single Market", Brussels, 15.12.2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm, (02.06.2020)

European Commission. **Press Release**, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses", Brussels, 25.01.2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm, (02.06.2020)

European Commission. **Press Release**, "Digital Single Market: EU Negotiators agree to set up new European rules to improve fairness of online platforms' trading practices", Strasbourg, 14.02.2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168, (02.06.2020)

European Commission. Special Eurobarometer, **"Cyber Security Report",** 404, 2013, http://ec.europa.eu/commfrontoffice/publicopinion-/archives/ebs/ebs_40-4_en.pdf, (02.06.2020)

European Commission. "Communication from the Commission to the European Parliament and the Council, Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018", 24.01.2018, **COM (2018) 43 Final**, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?-uri=CELEX:52018DC0043&from=EN, (02.06.2020)

European Commission. "Communication on the Mid-Term Review on the Implementation of the Digital Single Market Strategy, A Connected Digital Single Market for All", **228 final**, 10.5.2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0228 (02.06.2020)

European Council. "Proposal for a Directive of the European Parliament and the Council on copyright in the Digital Single Market", **COM/2016/0553 final – 2016/0280 (COD),** 14.9.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0593 , (02.06.2020)

European Data Protection Board. "Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679", **Guidelines 2/2018,** 25.05.2018, https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2018/06/edpb_guidelines_2_2018_derogations_en.pdf, (02.06.2020)

European Data Protection Supervisor. "Dissemination and Use of Intrusive Surveillance Technologies", **Opinion 8/2015**, https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf, (02.06.2020)

European Data Protection Supervisor. "Towards a New Digital Ethics: Data, Dignity and Technology", **Opinion 4/2015,** https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf , (02.06.2020)

European Open Data Portal. http://data.europa.eu/euodp/en/home, (02.06.2020)

European Parliament. Parliamentary Questions, 15 September 2016, **Ref. E-005636/2016**, http://www.europarl.europa.eu/doceo/document/E-8-2016-005636-ASW_EN.html, (02.06.2020)

European Parliament. "Contribution to Growth: The European Digital Single Market, Delivering Economic Benefits for Citizens and Businesses", Policy Department for Economic, Scientific and Quality of Life Policies, by authors: J.Scott Marcus, Dr.Gerorgios Petropoulos, Dr.Timothy Yeung, **Study,** January 2019, Table 1, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/631044/IPOL_STU(2019)631044_EN.pdf, (02.06.2020)

European Parliament. "Free Flow of Non-Personal Data in the European Union", **Briefing EU Legislation in Process,** https://www.europarl.europa.eu/RegData-/etudes/BRIE/2017/614628/EPRS_BRI%282017%29614628_EN.pdf, (02.06.2020)

European Parliament. "Legislative Train Schedule Connected Digital Single Market, JD-Modernisation of European Copyright Rules: Directive on Copyright in the Digital Single Market", 2019, http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-directive-on-copyright-in-the-digital-single-market, (02.06.2020)

European Parliament. "Lisbon European Council 23 and 24 March 2000 Precidency Conclusions", **Summits**, 2000, http://www.europarl.europa.eu/summits/lis1_en.htm, (02.06.2020)

European Parliament. "The Ubiquitous Digital Single Market, Fact Sheet on the European Union", 2018, http://www.europarl.europa.eu/ftu/pdf/en/FTU_2.1.7.pdf , (02.06.2020)

European Parliament. "Proposal for a Directive of the European Parliament and of the Council Establishing the European Electronic Communications Code", **COM**

(2016), 590, 2016, https://eurlex.europa.eu/legalcontent/EN/ALL/?uri=comnat:COM_2016_0590_FIN, (02.06.2020)

European Policy Center. "The Economic Impact of a European Digital Single Market, Final Report", **Copenhagen Economics,** 2010, https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/5/305/1435823773/study_by_copenhagen.pdf , (02.06.2020)

European Union Agency for Fundamental Rights. **Handbook on European Data Protection Law**, 2018, Luxembourg, https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf , (02.06.2020)

European Union Agency for Fundamental Rights. **Handbook on European Data Protection Law**, Belgium, 2014, https://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition, (02.06.2020)

European Union. **Charter of Fundamental Rights of European Union**, 2000/C, 364/01, 18.12.2000, http://www.europarl.europa.eu/cha-rter/pdf/text_en.pdf, (02.06.2020)

European Union. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Official Journal of the European Union, L 119/1**, 4.5.2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj , (02.06.2020)

European Union. **Treaty of Lisbon, amending the Treaty on European Union and the Treaty Establishing the European Community,** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT, (02.06.2020).

European Union. **Treaty on European Union**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT, (02.06.2020)

European Union. **Consolidated Version of The Treaty on the Functioning of the European Union**, OJ 2010/C, 83/01, 30.03.2010, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2010:083:FULL&from=EN, (10.08.2020)

European Union. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Cloud Initiative – Building a Competitive Data and Knowledge Economy in Europe", **COM (2016) 178 final,** 19.4.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0178&from=en, (02.06.2020)

European Union. "Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union", **OJ L 194,** 19.7.2016, https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1539674899977&uri=CELEX:32016L1148, (02.06.2020)

European Union. "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")", **Official Journal**, **L 178**, 17.7.2000, https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1540545333940&uri=CELEX:32000L0031, (02.06.2020)

European Union. "Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of Audiovisual Media Services, (Audiovisual Media Services Directive)", **Official Journal, L 95/1,** 15.4.2010, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013, (02.06.2020)

European Union. "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA", **OJ L 218**, https://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CEL-EX:32013L0040&rid=11, (02.06.2020)

European Union. "Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation)", **Official Journal L 364**, 9.12.2004, https://eur-lex.europa.eu/legal-content/EN/ALL-/?uri=CELEX%3A32004R2006, (02.06.2020)

European Union. "Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union", **Official Journal of the EU L 303/59,** 28.11.2018, https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1544179728555&uri=CELEX:32018R1807, (02.06.2020)

European Union. "Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)", **Official Journal of the European Union, L 119,** 4.5.2016, https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1540463136351&uri=-CELEX:32016R0679, (02.06.2020)

European Union. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", **JOIN 2013, 1 Final**, https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN, (02.06.2020)

European Union. "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural person with regard to the Processing of Personal data by Competent Authorities for the Purposes of the Prevention, Investigation, detection or prosecution of criminal offences or the

execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA", **Official Journal of the European Union, L 11989**, 4.5.2016, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016L0680&qid=1540463803208&from=EN, (02.06.2020)

European Union. "Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No.2006/2004", **Official Journal of the European Union**, **L345/1**, 27.12.2017, https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32017R2394&from=EN, (02.06.2020)

Europol. https://www.europol.europa.eu/about-europol, (02.06.2020)

Eurostat Statistics. "Demographic Balance", 2018, https://ec.europa.eu/eurostat/statisticsexplained/index.php?title=File:Demographic_balance,_2018_(thousands).png, (02.06.2020)

Fatema, Kaniz, Hadziselimovic, Ensar, Pandit, Harshvardhan, Debruyne, Christophe, Lewis, Dave ve O'Sullivan, Declan, "Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model", Adapt Center, Trinity College, Dublin, http://www.tara.tcd.ie/bitstream/handle/-2262/82659/88248c5b669175f267069c3319d9ac2d3e84.pdf?sequence=1 (02.06.2020)

Fırat, Muhammet Sabır. Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu, **Hacettepe Hukuk Fakültesi Dergisi**, Cilt: 5, Sayı: 2, 2015, ss. 101-116

Foco, Eugenio. "The Codification of the Right to be Forgotten in the Digital Era: From Directive 95/46/EC to the General Data Protection Regulation", 17.11.2016,

http://www.medialaws.eu/the-codification-of-the-right-to-be-forgotten-in-the-digital-era-from-directive-9546ec-to-the-general-data-protection-regulation/, (02.06.2020)

Freese, Jan. "The Swedish Data Act, Swedish Institute", **Current Sweden**, Swedish Institute, No.178, 1977, https://www.ncjrs.gov/pdffiles1/Digitization/49670 NCJRS.pdf , (02.06.2020)

French Data Protection Authority, (CNIL - The Commission Nationale de L'Informatique et des Libertes). Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019, Pronouncing a Financial Sanction Against GOOGLE LLC, https://www.cnil.fr/sites/default/files/a-toms/files/san-2019-001.pdf, (02.06.2020)

Freude, Alvar C.H. ve Freude, Trixy. "Echos of History: Understanding German Data Protection", Bertelsmann Foundation, **Newpolitik**, https://www.bfna.org/wpcontent/uploads/2017/04/Echoes_of_history_Understanding_German_Data_Protection_Freude.pdf, (02.06.2020)

Fromholz, Julia M. "The European Union Data Privacy Directive", **Berkeley Technology Law Journal**, Cilt. 15, Sayı.1, 2000, ss. 460-484

Fuster, Gloria Gonzales. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, Law, Governance and Technology Series 16, Springer, Heidelberg, 2014

Geradin, Damien ve Petit, Nicolas. "The Development of Agencies at EU and National Levels: Conceptual Analysis and Proposals for Reform", **Jean Monnet Working Paper**, 01/04, 2004, https://papers.ssrn.com-/sol3/papers.cfm?abstract_id=489722, (02.06.2020)

Giurgiu, Andra ve Lommel. Gerard. "A New Approach to EU Data Protection, More Control Over Personal Data and Increased Responsibility", **Critical Quarterly for Legislation and Law**, Cilt. 97, Sayı. 1, 2014, ss. 10-27

Goddard, Michelle. "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact", **International Journal of Market Research**, Cilt.59, Sayı.6, ss. 703-705

Goebel, Roger. "Supranational? Federal? Intergovernmental? The Governmental Structure of the European Union After the Treaty of Lisbon", **Columbia Journal of European Law**, Cilt.20, Sayı.1, 2013, ss. 77-142, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?articl-e=1576&context=faculty_scholarship (02.06.2020)

Golla, Sebastian J. "Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR", **Journal of Intellectıal Property, Information Technology and E-Commerce Law**, Cilt.70, Sayı. 8 (1), 2017, ss. 70-78

Google. "The Advisory Council to Google on the Right to be Forgotten", 6.2.2015, https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf, (02.06.2020)

Grant, Hazel, Amy Lambert, Kate Pickering. "Data Protection Day-Data Processors and the GDPR", **LexisNexis,** 2016, https://www.lexology.com/library/de-tail.aspx?g=3477a69d-812f-45d2-93f4-49f60cf946ce, (02.06.2020)

Güner, Semih. Sır Saklama Yükümlülüğü, **Ankara Barosu Dergisi**, Sayı. 3, 2000, ss. 43-52

Haltern, Ulrich. "Integration Through Law", **European Integration Theory** (Ed. By Antje Wiener, Thomas Diez)", 2. Baskı, Oxford University Press, 2009

Hansen, Marit, Schwartz, Ari, Cooper, Alissa. "Privacy and Identity Management", **IEEE Computer Society**, 2008, https://cdt.org/files/privacy/2008s-hwartzcooper.pdf, (02.06.2020)

Heermann, Max. Political Contestation in the Digital Single Market: Exploring Party Politics in the EU's Digital Policy, (Yayınlanmamış Yüksek Lisans Tezi) **Utrecht Faculty of Law, Economics and Governance Theses**, 2016, https://dspace.library.uu.nl/handle/1874/344610 (02.06.2020)

Held, David, McGrew, Anthony, Goldblatt, David, Perraton, Jonathan. "Global Transformations: Politics, Economics and Culture", **Politics at the Edge**, (Ed. Chris Pierson, Simon Tormey), Political Studies Association Yearbook Series, Palgrave Macmillan, London, 2000

Hilbert, Martin. "Big Data for Development: From Information to Knowledge Society", **Pre-published version**, 2013, http://ssrn.com/abstract=2205145, (02.06.2020)

Hinteregger, Monica. "The Protection of Personality Rights in Private Law: Remedies", **The Legal Protection of Personality Rights: Chinese and European Perspectives**, (Ed.Ken Oliphant, Zhang Pinghua, Chen Lei, Brill Nijhoff), Brill/Nijhoff, Leiden, 2018.

Hofmann, Herwig C. "The Right to an 'Effective Judicial Remedy' and the Changing Conditions of Implementing EU Law", Université du Luxembourg, Faculty of Law, Economics and Finance, **Law Working Paper Series**, Paper No. 2013-02, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2292542, (02.06.2020)

Hon, W.Kuan, Millard, Christopher ve Walden, Ian. "The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated?- the Cloud of Unknowing", part 1, Queen Mary University of London, **Legal Studies Research Paper No.75/2011**, ss. 1-46

Hornung, Gerrit ve Schnabel, Christoph. "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination" Computer Law & Security Report, Cilt. 25, Sayı 1, 2009, ss.84-88

Hornung, Gerrit ve Schnabel, Christoph. "Data Protection in Germany II: Recent Decisions on Online-searching of Computers, Automatic Number Plate Recognition and Data Retention", **Computer Law & Security Review**, Cilt.25, Sayı.2, 2009, ss. 115-122

Human Rights Watch (HRW). "The EU General Data Protection Regulation", **HRW Questions and Answers**, 06.06.2018, https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation, (02.06.2020)

Information Commissioner's Office, UK **(ICO).** "Data Protection by Design and Default", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/, (02.06.2020)

Ireland Data Protection Commissioner. "Privacy as a Human Right, Section Two", https://www.dataprotection.ie/documents/teens/cspe%20resource%20booklet/Section_2_-_Privacy_as_a_Human_Right.pdf (02.06.2020)

İlkiz, Fikret ve Günaydın, Barış. "Kişilik Hakları, Medyada Etik ve Yargı Kararları", **Küresel İletişim Dergisi**, Sayı.2, 2006

İstanbul Bilgi Üniversitesi. İnsan Hakları Hukuku Uygulama ve Araştırma Merkezi, **Duyurular**, https://insanhaklarimerkezi.bilgi.edu.tr/tr/news/none-kisisel-verilere-dair-sozlesme-bakanlar-kurul/, (02.06.2020)

Jabko, Nicolas. **Playing the Market: A Political Strategy for Uniting Europe, 1985-2005**, 1.Edition, Cornell University Press, Ithaca, London, 2006

Jackson, Camille Marie. "Estonian Cyber Policy after the 2007 Attacks: Driven of Change and Factors for Success, New Voices in Public Policy", **George Mason University, School of Public Policy,** Cilt.7, Sayı.1, 2013, ss. 1-15

Jacoby, Wade ve Meunier, Sophie. “Europe and the Management of Globalization: Responding to Globalization Pressures”, **Working Paper**, https://www.researchgate.net/publication/242547663_Europe_and_the_Management_of_Globalization, (02.06.2020)

Joint Declaration by the High Representative for Foreign Affairs and Security Policy on behalf of the European Union and the Secretary General of the Council of Europe on the occasion of the European and World Day against the Death Penalty, **Joint Declaration**, 10 October 2019, https://rm.coe.int/2019-joint-declaration-final-003-/16809818b6, (02.06.2020)

Jozwiak, Magdalena. “Balancing the Rights to Data Protection and Freedom of Expression and Information in the EU: The Vulnerability of Rights in an Online Context”, **SSRN**, 2016, ss.1-23, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3138296, (02.06.2020)

Judgment by European Court of Human Rights. Case of Niemietz v. Germany, **ECHR Application no. 13710/88**, 16.12.1992, Strasbourg, https://hudoc.echr.coe.int/e-ng#{"itemid":["001-57887"]}, (02.06.2020)

Judgment by the European Court of Human Rights. Case of Malone v. The United Kingdom, **ECHR Application No. 8691/79**, Strasbourg, 1984, https://hudoc.echr.coe.int/EN-G#{"itemid":["001-57533, (02.06.2020)

Judgment by the European Court of Human Rights. Case of von Hannover v. Germany, **ECHR Application No. 59320/00**, 24.06.2004, https://www.juridice.ro/wp-content/uploads/2016/07/von-Hannover-v-Germany-ECHR-24-June-2004.pdf, (02.06.2020)

Judgment of the Court of Justice (Fourth Chamber). Rynes v. Urad Case, 11 December 2014, **ECJ C 212/13**, http://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=EN, (02.06.2020)

Judgement of the Court of Justice of the European Union (Grand Chamber). **ECJ C-801**, 1.10.2019, German Federation of Consumer Organisations v. Planet49 GmbH, http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8867771, (02.06.2020)

Judgment of the Court of Justice (Grand Chamber). **ECJ C-518/07**, 9 March 2010, European Commission supported by European Data Protection Supervisor v. Federal Republic of Germany, http://curia.europa.eu-/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5404007, (02.06.2020)

Judgment of the Court of Justice (Third Chamber). **ECJ C-553/07**, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 7 May 2009, http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1065929, (02.06.2020)

Judgment of the Court of Justice of the European Union (Fourth Chamber). EUR-Lex, Reports of Cases, **ECJ C-291/12**, Schwarz v. Bochum, 17.10.2013, https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:62012CJ0291&rid=3, (02.06.2020)

Judgment of the Court of Justice of the European Union (Fourth Chamber). 17.10.2013, **ECJ Case C291/12**, Michael Schwarz v. Stadt Bochum, http://curia.europa-.eu/juris/liste.jsf?num=C-291/12, (02.06.2020)

Judgment of the Court of Justice of the European Union (Grand Chamber). EUR-Lex, Reports of Cases, **ECJ Case C-131/12**, 13.05.2014, Google Spain SL, Google Inc. V. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=C-ELEX%3A62012CJ0131, (02.06.2020)

Judgment of the Court of Justice of the European Union (Grand Chamber). EUR-Lex, Reports of Cases, **ECJ C-28/08**, Commission v. Bavarian Lager Co., 29.6.2010, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CEL-EX%3A62008CJ0028, (02.06.2020)

Judgment of the Court of Justice of the European Union (Grand Chamber). EUR-Lex, Reports of Cases, **ECJ C-362/14**, Maximillian Schrems v. Data Protection Commissioner, 6.10.2015, Request for a preliminary ruling from the High Court (Ireland)— Transfer of personal data to the United States, https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62014CJ0362, (02.06.2020)

Judgment of the Court of Justice of the European Union (Third Chamber). EUR-Lex, Reports of Cases, **ECJ C-342-12**, Worten-Equipamentos Para o Lar SA v. Autoridade para as Condiçoes de Trabalho (ACT) (Authority for Working Conditions), 30.5.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=-1551084733669&uri=CELEX:62012CJ0342, (02.06.2020)

Judgment of the Court of Justice of the European Union (Third Chamber). EUR-Lex, Reports of Cases, **ECJ C-70/10**, Scarlet Extended SA v. Societe Belge Des Auteurs, Compositeurs et Editeurs SCRL (SABAM), 24.11.2011, https://eur-lex.europa.eu/legal-content/EN/TXT-/?qid=155108483381-6&uri=CELEX:62010CJ0070, (02.06.2020)

Judgment of the Court of Justice of the European Union (Third Chamber). EUR-Lex, Reports of Cases, **ECJ C-473/12**, Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and others,7.11.2013, https://eurlex.europa.eu/search.html?qid=155108 4899834&text=IPI%20v.%20Englebert&scope=EURLEX&type=quick&lang=en, (02.06.2020)

Judgment of the Court of Justice of the European Union, (Second Chamber). EUR-Lex, Reports of Cases, **ECJ C-434/16**, Peter Nowak v. Data Protection

Commissioner, 20.12.2017, https://eur-lex.europa.eu/legal-content/EN/T-XT/?uri=C-ELEX%3A62016CJ0434, (02.06.2020)

Judgment of the Court of Justice of the European Union. **ECJ Case C-101/01**, Criminal Proceedings Against Bodil Lindqvist, 6.11.2003, http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130de32c334f6a84d4d948303f434d25f29fc.e34KaxiLc3eQc40LaxqMbN4Pb30Oe0?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=385015, (02.06.2020)

Judgment of the Court of Justice of the European Union (Grand Chamber), EUR-Lex, Reports of Cases, ECJ C-311/18, Data Protection Commissioner v. Maximillian Schrems & Facebook Ireland Ltd., 16.07.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1597766650136&from=EN (16.08.2020)

Karaarslan, Enis, Ergin, Ali Murat, Turğut, Nalin ve Kılıç, Özgür. "Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti", **İNET-TR 2015,** https://www.researchgate.net/profile/Enis_Karaarslan/publication/287975276_Elektronik_Saglik_Kayitlarinin_Gizlilik_ve_Mahremiyeti/links/576cc6ff08ae9bd709961314/Elektronik-Saglik-Kayitlarinin-Gizlilik-ve-Mahremiyeti.pdf, (02.06.2020)

Karakaş, Işıl. "Ulusalüstü Anayasada Temel Haklar Problematiği: Teorik ve Pratik Sorunlar", **Anayasa Yargısı Dergisi**, Cilt.22, 2005, ss. 292-305

Karner, Ernst. "Human Rights and the Protection of Personality Rights in Europe: Comparative Reflections", **The Legal Protection off Personality Rights, Chinese and European Perspectives**, (Ed. Ken Oliphant, Zhang Pinghua, Chen Lei), Brill Nijhoff, Leiden, 2018

Kaya, Mine. "Telekomünikasyon Alanında Kişilik Haklarının Korunması", **Ankara Barosu Dergisi**, Sayı.4, 2010, ss. 279-334

Kerber, Wolfgang ve Schweitzer, Heike. "Interoperability in the Digital Economy", **Joint Discussion Paper Series in Economics by MAGKS, No. 12**, 2017, https://www.unimarburg.de/fb02/makro/forschung/magkspapers/paper_2017/12-2017_kerber.pdf, (02.06.2020)

Keser Berber, Leyla. **Çevirimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması**, I. Baskı, XII Levha Yayınları, 2014

Khine, Pwint Phyu ve Shun, Wang Zhao. "Big Data For Organizations: A Review", **Journal of Computer and Communications**, Cilt.5, 2017, ss. 40-48

Khor, Martin. **Rethinking Globalization: Critical Issues and Policy Choices**, Zed Books, UK, 2001

Khoury, Alessandro El. "The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EY-USA Data Transfers?", **European Journal of Risk Regulation**, Cilt.6, Sayı.4, 2015, ss. 659-664

Kılınç, Doğan. "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 61, Sayı: 3, 2012, ss. 1089-1170

Kilkelly, Ursula. "The Right to Respect for Private and Family Life, A Guide to the Implementation of Article 8 of the European Convention on Human Rights", **Council of Europe, Human Rights Handbooks,** No.1, Strasbourg, 2001

Kirby, Michael. "The History Achievement and Future of the 1980 OECD Guidelines on Privacy", **International Data Privacy Law**, Cilt.1, Sayı.1, 2011, ss. 6-14

Kostic, Bojana ve Penagos, Emmanuel Vargas. "The Freely Given Consent and the "Bundling" Provision under the GDPR", **Computerrecht,** Cilt.4, Sayı.153, 2017, ss. 217-222

Kulk, Stefan, Zuiderveen Borgesius, Frederick. “Privacy, Freedom of Expression and the Right to be Forgotten in Europe”, **Cambridge Handbook of Consumer Privacy** (Ed. Jules Polonetsky, Omer Tene, Evan Selinger), Cambridge University Press, 2017

Kuner, Christopher, Cate, Fred H., Millard, Christopher ve Svantesson, Dan Jerker B. “The Challenge of “big data” for data protection”, **International Data Privacy Law**, Editorial, 2012, Cilt. 2, Sayı.2, ss. 47-49

Kuner, Christopher. “Beyond Safe Harbour: European Data Protection Law and Electronic Commerce”, **The International Lawyer**, Cilt.35, Sayı.1, 2001, ss. 79-88

Kuner, Christopher. “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future”, TILT (Tilburg Institute for Law, Technology and Society) **Law and Technology Working Paper Series**, No. 016/2010, http://ssrn.com/abstract=1689483 (02.06.2020)

Küzeci, Elif. **Kişisel Verilerin Korunması**, 2. Baskı, Turhan Kitapevi, Ankara, 2018

Lapavitsas, Costas, Kaltenbrunner, Annina, Lindo, Ducan, Michell, J., Painceira, Juan Pablo, Pires, Eugenia, Powell, Jeff, Stenfors, Alexis ve Teles, Nuno. “Eurozone Crisis: Beggar Thyself and Thy Neighbour, Research on Money and Finance”, **Journal of Balkan and Near Eastern Studies**, Cilt.12, Sayı 4, 2010, ss. 321-373

Laudati, Laraine. “Summaries of EU Court Decisions Relating to Data Protection 2000-2015”, European Anti-Fraud Office **(OLAF)**, 2016, https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, (02.06.2020)

Lavrijssen, Saskia, Ottow, Annetje. “Independent Supervisory Authorities: A Fragile Concept”, **Legal Issues of European Integration**, Cilt.39, Sayı.4, 2012, ss. 419-446

Lindqvist, Jenna. "New Challenges to Personal Data Processing Agreements: is the GDPR Fit to Dealwith Contract, Accountability and Liability in a World of the Internet of Things", **International Journal of Law and Information Technology**, Cilt.26, Sayı 1, 2017, ss. 45-63

Livingstone, Sonia, Haddon, Leslie. "EU Kids Online: Final Report, The London School of Economics and Political Science", **EC Safer Internet Plus Programme,** Deliverable D6.5, 2009

Loukaides, Loukes G. "Essays on the Developing Law of Human Rights"**, International Studies in Human Rights**, Kluwer Academic Publishers, Boston, 1995

Macenaite, Milda ve Kosta, Eleni. "Consent for Processing Children's Persona Data in the EU: Flowing in the US Footsteps?", **Information and Communication Technology Law**, Cilt.26, Sayı.2, 2017, ss. 146-197

Madsen, Wayne. **Handbook of Personal Data Protection**, 1.Baskı, Palgrave Macmillan, UK, 1992

Mahlmann, Matthias. "Human Dignity and Authonomy in Modern Constitutional Orders", **The Oxford Handbook of Comparative Constitutional Law** (Ed. Michel Rosenfeld, Andras Sajo), Oxford University Press, 2012, https://www.jura.uni-hamburg.de/media/ueber-die-fakultaet/personen/albers-marion/seoul-national-university/course-outline/mahlmann-2013-human-dignity-and-autonomy-in-modern-constitutional-orders.pdf, (02.06.2020)

Malgieri, Gianclaudio ve Comande, Giovanni. "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", **International Data Privacy Law**, Cilt.7, Sayı 4, 2017, ss. 243-265

Mansfield-Devine, Steve. "Meeting the Needs of GDPR with Encryption", **Computer Fraud and Security**, Cilt.2017, Sayı 9, 2017, ss. 16-20

Mayer-Schönberger, Viktor ve Cukier, Kenneth. **Big Data A Revolution that Will Transform How We Live, Work and Think**, Houghton Mifflin Harcourt Publishing, USA, 2013

McCrudden, Christopher. "Human Dignity and Judicial Interpretation of Human Rights", **The European Journal of International Law**, Cilt.19, Sayı. 4, 2008, ss. 655-724

McGann, James G. "2015 Global Go To Think Tank Index Report", TTCSP Global Go To Think Tank Index Reports, **University of Pennsylvania**, Paper 10, https://repository.upenn.edu/cgi/viewcontent.cgi?article=1009&context=think_tanks, (02.06.2020)

McKinsey Global Institute. "Digital Globalization: The New Era of Global Flows", March 2016, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx, (02.06.2020)

McKinsey Global Institute. "Global Flows in a Digital Age: How Trade, Finance, People and Data connect the World Economy", April 2014, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/Globalization/Global%20flows%20in%20a%20digital%20age/MGI%20Global%20flows%20in%20a%20digial%20age%20Executive%20summary.ashx, (02.06.2020)

Medin, Burak. "Dijitalleşen Dünyada Fikri Haklar Sorunu", **Kırıkkale Üniversitesi Sosyal Bilimler Dergisi**, Cilt 7, Sayı 2, 2017, ss. 51-68

Meunier, Sophie. "Managing Globalization? The EU In International Trade Negotiations", **Journal of Common Market Studies (JCMS)**, Cilt 45, Sayı. 4, 2007, ss. 905-926

Micheline, R. Ishay. **The History of Human Rights: From Ancient Times to the Globalization Era**, 2.Baskı, University of California Press, 2008

Milkaite, Ingrida ve Lievens, Eva. "The GDPR Child's Age of Consent for Data Processing Across the EU – One Year Later", **Ghent University**, 1.7.2019, https://biblio.ugent.be/publication/8621651/file/8621654.pdf, (02.06.2020)

Miller, Katherine. **Communication Theories: Perspectives, Processes and Contexts**, 2.Baskı, McGraw Hill, Boston, 2005

Miri, Mina, Foomany, Farbod H., Mohammed, Nathanael. "Complying with GDPR: An Agile Case Study", **ISACA Journal**, Cilt.2, 2018, ss. 1-7

Mock, William B.T. "On The Centrality of Information Law: A Rational Choice Discussion of Information Law and Transparency", **John Marshall Journal of Computer & Information Law**, Cilt.17, 1999, ss. 1069-1100

Monti, Mario. "A New Strategy for the Single Market At the Service of Europe's Economy and Society, Report to the President of the European Commission Jose Manuel Barroso", **Report**, 2010, https://www.kfw.de/migration/Weiterleitung-zur-Startseite/Homepage/KfW-Group/Research/PDF-Files/Monti_Report.pdf , (02.06.2020)

Mooney, Stephan J., Westreich, Daniel J., El-Sayed, Abdulrahman M."Epidemiology in the Era of Big Data", **Epidemiology**, Cilt. 26, Sayı. 3, 2015, ss. 390-394

Neethling, Johann. "Personality Rights: A Comparative Overview", **The Comparative and International Law Journal of Southern Africa**, Cilt.38, Sayı.2, 2005, ss. 210-245

Niemann, Arne ve Schmitter, Philippe C. "Neofunctionalism", **European Integration Theory** (Ed. Antje Wiener, Thomas Diez), 2.baskı, Oxford University Press, 2009

OECD. Guidelines On the Protection of Privacy and Transborder Flows of Personal Data, Part 1/b, **OECD GL,** 1980, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1, (02.06.2020)

OECD. Recommendation of the Council concerning OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, **OECD/Legal/0188,** https://legalinstruments.oecd.org/public/doc/114/114.en.pdf (02.06.2020)

OECD. **The OECD Privacy Framework**, 2013, http://www.oecd.org/sti/-ieconomy/oecd_privacy_framework.pdf, (02.06.2020)

OECD. **Thirty Years After the OECD Privacy Guidelines**, 2011, http://www.oecd.org/sti/ieconomy/49710223.pdf, (02.06.2020)

Opinion of Advocate General. Mr. Szpunar delivered on 21 March 2019, **Case c-673/17**, Planet49 GmbH v. German Federation of Consumer Organisations, http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8867771, (02.06.2020)

Oxman, Stephen A. "Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?"; **Boston College International and Comparative Law Review**, Cilt.24, Sayı.1, 2000, (02.06.2020)

Özbudun, Ergun. "Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği", **Ankara Hukuk Fakültesi Ellinci Yıl Armağanı**, Cilt 1, 1977, ss. 265-295, https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/10322, (02.06.2020)

Özdemir, Hayrunnisa. **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Birinci Baskı, Seçkin Yayınevi, Ankara, 2009

Öztürk, İbrahim Hakkı. "Dünyanın en dinamik ve en rekabetçi bilgi ekonomisi olmak ya da olamamak: Avrupa Birliği Lizbon Stratejisi ve Eğitim Boyutu", **Ankara Avrupa Çalışmaları Dergisi,** Cilt.7, Sayı.2, 2008, ss. 13-32

Parliament and of the Council. "On cross border parcel delivery services", 2016/0149 (COD), **Pre-Cons 69/17**, http://data.consilium.europa.eu/doc/-document/PE-69-2017-INIT/en/pdf, (02.06.2020)

Patel, Oliver ve Lea, Nathan. "EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?" **UCL European Institute, Brexit Insights**, 2019, https://www.ucl.ac.uk/european-institute/sites/european-institute/files/eu-uk_data_flows_brexit_and_no-deal.pdf, (02.06.2020)

Patsa, Agapi ve Benmayor, Aliki. "Competition and Antitrust in the Digital Age", **Baker McKenzie**, 20.07.2017, https://www.bakermckenzie.com//media/files/insight/publications/2017/10/ar_antitrust_digitalage_oct17.pdf?la=en, (02.06.2020)

Politou, Eugenia, Alepis, Efthimios ve Patsakis, Constantinos. "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions", **Journal of Cyber Security**, Cilt.4, Sayı.1, 2018, ss. 1-20

Pollack, Mark A. "The New Institutionalisms and European Integration", **European Integration Theory** (Ed. Antje Wiener, Thomas Diez), 2.baskı, Oxford University Press, 2009

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communicatios), **COM (2017) 10 Final,** 2017/0003 (COD), 10.1.2017, https://eurlex.europa.eu/legalcontent/E-N/TXT/?qid=1550836328519&uri=CELEX:52017PC0010 , (02.06.2020)

Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Proccessing of Personal Data and on Free Movement of Such Data (General Data Protection Regulation), **11 Final, 2012/0011 (COD),** 25.01.2012, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52012PC0011 (02.06.2020)

Proposal for a Regulation of the European Parliament and of the Council on cross border parcel delivery services, 2016/0149 (COD), **Pre-Cons 69/17**, http://data.consilium.europa.eu/doc/document/PE-69-2017-INIT/en/pdf (02.06.2020)

Recio, Miguel. "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability, Practitioner's Corner", **European Data Protection Law Review**, Cilt.3, Sayı.1, 2017, ss. 114-118

Reding, Viviane. "Independent Data Protection Authorities: Indispensable Watchdogs of the Digital Age European Commission", **Press Release Database**, 7.12.2011, http://europa.eu/rapid/press-release_SPEECH-11-863_en.htm (02.06.2020)

Reding, Viviane. "Privacy matters-Why the EU needs new Personal Data Protection Rules", European Commission, **Press Release Database**, 30.11.2010, http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm, (02.06.2020)

Regulation 2017/1128 of the European Parliament and of the Council of 14 June 2017 on crossborder portability of online content services in the internal market, (Portability Regulation), **Official Journal**, **L 168/1**, 30.06.2017, https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2017.168.01.0001.01.ENG (02.06.2020)

Regulation 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394

and Directive 2009/22/EC (Text with EEA relevance), **Official Journal L 60I**, 2.3.2018, ss.1-15, https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.LI.2018.060.01.0001.01.ENG&toc=OJ:L:2018:060I:TOC, (02.06.2020)

Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (Text with EEA relevance), **Official Journal L 60I**, 2.3.2018, ss.1-15, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uri-serv:OJ.LI.2018.060.01.0001.01.ENG&toc=OJ:L:2018:060I:TOC (02.06.2020)

Report of an Independent High-Level Study Group Established on the Initiative of the President of the European Commission, "An Agenda for a Growing Europe, Making the EU Economic System Deliver", 2003, https://artnet.unescap.org/tid/artnet/mtg/g-mscb_growingeurope.pdf , (02.06.2020)

Risse, Thomas. "Social Constructivism and European Integration", **European Integration Theory** (Ed. Antje Wiener, Thomas Diez), 2.baskı, Oxford University Press, 2009

Roagna, Ivana. **Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması**, Avrupa Konseyi İnsan Hakları El Kitapları Serisi, Strazburg, 2012

Rubinstein, Ira S. Big Data: The End of Privacy or a New Beginning?, **NYU School of Law, Public Law Research Paper, No.12-56**, 2012, International Data Privacy Law, "Forthcoming: 2013", 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659, (02.06.2020)

Ruffert, Matthias. "The European Debt Crisis and European Union Law", **Common Market Law Review**, Cilt. 48, Sayı 6, 2011, ss. 1777-1806

Sanchez, Amaya Noain. "'Privacy by default' and active 'informed consent' by layers: Essential measures to protect ICT users' privacy", **Journal of Information, Communication and Ethics in Society**, Cilt. 14, Sayı. 2, 2016, ss. 124-138

Sanioğlu, Hilal. "Avrupa Birliği Hukukunda İnsan Hakları", **Türkiye Barolar Birliği Dergisi**, Sayı.74, 2008, ss.77-111

Sarıtaş, Hatice. **Hasta Hakları Açısından Hekim Sorumluluğu**, Bilge Yayınevi, Ankara, 2005

Sassatelli, Monica. "Imagined Europe: The Shaping of a European Cultural Identity Through EU Cultural Policy", **European Journal of Social Theory,** Cilt.5, Sayı. 4, 2002, ss. 435-451

Savcı, Bahri. "İnsan Hakları Üzerine Uluslararası Alanda, Norm İlkeler ve Türk İç Hukuku", **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Cilt.35, Sayı 1, 1980, ss. 7-18

Saygın, Didem. "Avrupa Birliği'nde Temel Haklar: ABAD İçtihatları Üzerinden Bir Değerlendirme", **International Conference on Awareness**, Poland, 2017, https://www.researchgate.net/publication/322952247_AVRUPA_BIRLIGI'NDE_TEMEL_HAKLAR_ABAD_ICTIHATLARI_UZERINDEN_BIR_DEGERLENDIRME, (02.06.2020)

Schimmelfenning, Frank, Engert, Stephan, Knobel, Heiko. "Costs, Commitment and Compliance: The Impact of EU Democratic Conditionality on Latvia, Slovakia and Turkey", **Journal of Common Market Studies**, Cilt. 41, Sayı.3, 2003, ss. 496-518

Schmidt, Rolf, Seidel, Stephanie, Grundrechte, 2001, Bremen, s. 257 ile Schulz, Wolfgang, Verfassungsrechtlicher Schutzauftrag in der Informationsgesellschaft, in: Die Verwaltung, 1999, s.140 Aktaran Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2008

Sedelmeier, Ulrich. "Europeanisation in New Member and Candidate States", **Living Reviews in European Governance**, Cilt. 6, Sayı. 1, 2011, ss. 5-32

Single European Act. **Official Journal L 169**, 29.6.1987, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:11986U/TXT, (02.06.2020)

Smitis, Spiros. "Reviewing Privacy in an Information Society", **University of Pennsylvania Law Review**, Cilt 135, 1987, ss. 707-746

Spataru-Negura, Laura-Cristiana ve Lazar, Cornelia. "Lifting the Veil of the GPPR to Data Subjects", Challenges of the Knowledge Society, Public Law, **Nicolae Titulescu University**, 2018, ss. 658, http://cks.univnt.ro/articles/12.html, (02.06.2020)

Spindler, Gerald ve Schmechel, Philipp. "Personal Data and Encryption in the European General Data Protection Regulation", **Journal of Intellectual Property, Information Technology and E-Commerce Law**, Cilt.7, Sayı.2, 2016, ss. 163-177

Statista. "Digital Media Report", 2018, https://www.statista.com/s-tudy/44526/digital-media-report/, (02.06.2020)

Statista. "Statistics and Market Data on Media and Advertising", https://www.statista.com/markets/417/media-advertising/, (02.06.2020)

Stutz, Frederick P. ve Warf, Barney. "Economic Geography: An Introduction", **The World Economy Geography, Business, Development**, (Ed. Stutz & Warf), 6.Baskı, Pearson New International Edition, UK, 2014

Swire, Peter P. ve Litan, Robert E. "None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive", **Harvard Journal of Law & Technology**, Cilt.12, Sayı. 3, 1999, ss. 683-702

Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2008

T.C. Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü, İnsan Hakları Dairesi Başkanlığı, Basın Birimi. Kişisel Verilerin Korunması-**Tematik Bilgi Notu**, 2015, http://inhak.adalet.gov.tr/inhak_-bilgi_bankasi/tematik_bilg-inotu/bilgi/Protection%20of%20personal%20data%20(kişisel%20verilerin%20korunması).pdf, (02.06.2020)

T.C. Avrupa Birliği Bakanlığı. **Avrupa Birliği Müzakere Sürecinde Yargı ve Temel Haklar Faslı**, Avukatlar için Yargı ve Temel Haklar Projesi, 013, Ankara

T.C. Kalkınma Bakanlığı. **2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı**, Yayın No.2939, 2015, ISBN NO. 978-605-904153-9, https://abdigm.meb.gov.tr/projeler/ois/004.pdf , (02.06.2020)

Tapscott, Don. **Dijital Ekonomi, Ağ Üzerindeki Akıl Çağında Umut ve Tehlike**, 1.Baskı, Koç Sistem Yayınları, İstanbul, 1998

Taşdemir, Hakan ve Bağbaşlıoğlu, Arif. "Avrupa Birliği Hukuk Düzenindeki İnsan Hakları Anlayışına Avrupa Birliği Temel Haklar Şartının Getirdikleri", **Gazi Üniversitesi İİBF Dergisi**, Cilt.9, Sayı.3, 2007, ss. 21-36

Tekin, Nurullah. "Kişisel Verilerin Korunması ile ilgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", **Uyuşmazlık Mahkemesi Dergisi**, Cilt. 4, 2014, ss. 222-262

Tekinalp, Gülören ve Tekinalp, Ünal. **Avrupa Birliği Hukuku**, 2.Baskı, Beta Yayınları, İstanbul, 2000

The London School of Economics and Political Science (LSE). "Media Policy Project Block, European Court Rules Against Google in Favour of Right to be Forgotten", http://blogs.lse.ac.uk/mediapolicyprojec-t/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten/, (02.06.2020)

The National Academies of Sciences. "Engineering, Medicine, At the Nexus of Cyber Security and Public Policy: Some Basic Concepts and Issues", 2014, https://www.nap.edu/download/18749, (02.06.2020)

Tikkinen-Piri, Christina, Rohunen, Anna ve Markkula, Jouni. "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", **Computer Law and Security Review: The International Journal of Technology Law and Practice**, Cilt.34, Sayı.1, 2018, ss. 134-153

Toth, Beatrix. "Estonia under Cyber Attack", **Hun-CERT**, https://www.cert.hu/sites/default/files/Estonia_attack2.pdf , (02.06.2020)

Türkiye Cumhuriyeti Avrupa Birliği Genel Sekreterliği. **Avrupa Birliği Terimler Sözlüğü**, Ankara, 2009, https://www.ab.gov.tr/files/Sozluk-/glossary_for_the_european_union.pdf (02.06.2020)

Uçkan, Özgür. "Internet, Mahremiyet ve Kişisel Verilerin Korunması", https://www.evrensel.net/haber/67935/internet-mahremiyet-ve-kisisel-verilerin-korunmasi, Evrensel Haber, 2013, (02.06.2020)

United Nations General Assembly. **Universal Declaration of Human Rights**, 1948, http://www.verklaringwarenatuur.org/Downloads_files/Universal%20Declaration%20of%20Human%20Rights.pdf, (02.06.2020)

United Nations. **Universal Declaration of Human Rights**, (Illustrations by Yacine Ait Kaci), 2015, http://www.un.org/en/udhrbook/pdf/udhr_bookle-t_en_web.pdf , (02.06.2020)

Virginia Haklar Bildirgesi, 1776, https://tr.wikisource.org/wiki/Virgin-ia_İnsan_Hakları_Bildirgesi, (02.06.2020)

Voigt, Paul ve Von dem Bussche, Axel. **The EU General Data Protection Regulation (GDPR), A Practical Guide**, Springer, 2017

Voorhoof, Dirk. “European Court of Human Rights, Case of Von Hannover v. Germany”, **IRIS Merlin 2004-8:2/2**, http://merlin.obs.coe.int/article/3137, (02.06.2020).

Voss, W. Gregory. “After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change”, **The Business Lawyer**, Cilt. 71, Sayı.1, Winter 2015-2016, ss. 281-292

Voss, W.Gregory. “European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting”, **Business Lawyer**, Cilt.72, Sayı.1, Winter 2016-2017, ss. 221-234

Voss, W.Gregory. “Preparing for the Proposed EU General Data Protection Regulation: With or Without Amendments”, **Business Law Today** Cilt.1, 2012, ss.1-5

Vosskuhle, Andreas. “European Integration Through Law, the Contribution of the Federal Constitutional Court”, **European Journal of Sociology**, Cilt.58, Sayı.1, 2017, ss. 145-168

Wachter, Sandra, Mittelstadt, Brent, Floridi, Luciano. “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, **International Data Privacy Law**, Cilt.7, Sayı.2, 2017, ss. 76-99

Wachter, Sandra. “Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR”, **Computer Law and Security Review**, Cilt.34, Sayı.3, 2018, ss. 436-449

Walker, Robert Kirk. “The Right to be Forgotten”, **Hasting Law Journal**, Cilt. 64, Sayı.1, 2012, ss. 257-286

Werry, Nikola, Kirschbaum, Benjamin ve Koch, Jens-Marwin. "Germany", **The Privacy, Data Protection and Cybersecurity Law Review** (Ed. Alan Charles Raul), 4.Baskı, The Law Reviews, UK, 2017

Wicks, Elisabeth. "The Meaning of Life: Dignity and the Right to Life in International Human Rights Treaties", **Human Rights Law Review**, Cilt.12, Sayı.2, 2012, ss. 199-219

Wiener, Antje ve Diez, Thomas. "Introducing the Mosaic of Integration Theory", **European Integration Theory**, (Ed. Antje Wiener, Thomas Diez**)** 2.baskı, Oxford University Press, 2009

World Economic Forum. "The Europe 2020 Competitiveness Report, Building a More Competitive Europe", 2014, http://www3.weforum.org/docs/WEF_Europe2020_CompetitivenessReport_2014.pdf, (02.06.2020)

Yang, Chaowei, Huang, Qunying, Li, Zhenlong, Liu, Kai ve Hu, Fei. "Big Data and Cloud Computing: Innovation Opportunities and Challenges", **International Journal of Digital Earth**, Cilt. 10, Sayı.1, 2017, ss. 13-53

Yerdelen, Erdal. "Klonlamanın (Kopyalama) Ceza Hukukundaki Yeri", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 63, Sayı: 3, 2014, ss. 643-685

Yılmaz, H.Banu. "Lizbon Sonrası AB 2020 Stratejisi," **TOBB, Ekonomik Forum**, 2010, https://www.tobb.org.tr/AvrupaBirligiDairesi/Dokumanlar/Raporlar/AB%202020%20Stratejisi.pdf, (02.06.2020)

Yılmaz, Sefer ve Kalkan, Duhan K. "Enerji Güvenliği Kavramı: 1973 Petrol Krizi Işığında Bir Tartışma", **Uluslararası Kriz ve Siyaset Araştırmaları Dergisi**, Cilt.1 Sayı.3, 2017, ss. 169-199

Yüksel, Mehmet. "Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar", **Ankara Üniversitesi SBF Dergisi**, Cilt. 64, Sayı.1, 2007, ss. 275-298

Zarsky, Tal Z. “Incompatible: The GDPR in the Age of Big Data”, **Seton Hall Law Review**, Cilt.47, Sayı 4(2) 2017, ss. 995-1020

Zevkliler, Aydın, Acabey, Mehmet Beşir ve Gökyayla, K.Emre. **Medeni Hukuk, Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku**, 6.Baskı, Seçkin Yayınevi, Ankara, 2000

Zliobaite, Indre ve Custers, Bart. “Using Sensitive Personal Data May be Necessary for Avoiding Discrimination in Data-Driven Decision Modals”, **Artificial Intelligence and Law**, Cilt. 24, Sayı 2, 2016, ss. 183-201