BESTE YILMAZ

KİŞİSEL VERİLERİN KORUNMASI VE REKABET HUKUKU BAĞLAMINDA VERİ TAŞINABİLİRLİĞİ HAKKI

Bilkent Üniversitesi 2022

KİŞİSEL VERİLERİN KORUNMASI VE REKABET HUKUKU BAĞLAMINDA VERİ TAŞINABİLİRLİĞİ HAKKI

Yüksek Lisans Tezi

BESTE YILMAZ

Hukuk Bölümü
İhsan Doğramacı Bilkent Üniversitesi
Ankara
Ağustos 2022

Aileme

KİŞİSEL VERİLERİN KORUNMASI VE REKABET HUKUKU BAĞLAMINDA VERİ TAŞINABİLİRLİĞİ HAKKI

İhsan Doğramacı Bilkent Üniversitesi
Ekonomi ve Sosyal Bilimler Enstitüsü

BESTE YILMAZ

Özel Hukuk Disiplininde Yüksek Lisans Derecesi
Kazanma Yükümlülüklerinin Bir Parçasıdır.

HUKUK BÖLÜMÜ
İHSAN DOĞRAMACI BİLKENT ÜNİVERSİTESİ
ANKARA

Ağustos 2022

KİŞİSEL VERİLERİN KORUNMASI VE REKABET HUKUKU BAĞLAMINDA VERİ TAŞINABİLİRLİĞİ HAKKI
Beste YILMAZ

Bu tezi okuduğumu, kapsam ve nitelik bakımından Hukuk Yüksek Lisans derecesi için yeterli bulduğumu beyan ederim.

Hüseyin Can AKSOY
Tez Danışmanı

Bu tezi okuduğumu, kapsam ve nitelik bakımından Hukuk Yüksek Lisans derecesi için yeterli bulduğumu beyan ederim.

Pınar ÇAĞLAYAN AKSOY
Tez Jüri Üyesi

Bu tezi okuduğumu, kapsam ve nitelik bakımından Hukuk Yüksek Lisans derecesi için yeterli bulduğumu beyan ederim.

Selin ÖZDEN MERHACI
Tez Jüri Üyesi

Ekonomi ve Sosyal Bilimler Enstitüsü Müdürü'nün onayı

Refet Soykan GÜRKAYNAK
Enstitü Müdürü

ABSTRACT

THE RIGHT TO DATA PORTABILITY IN THE CONTEXT OF PERSONAL DATA PROTECTION AND COMPETITION LAW

Yılmaz, Beste

LL.M., Private Law Program

Supervisor: Asst. Prof. Dr. Hüseyin Can Aksoy

Haziran 2022

Obtaining significant economic benefits by processing data has made it an economic necessity to obtain, process and flow data in every market, especially in digital markets. Unlimited and unreasonable processing of personal data within this data set has created the need for the protection of personal data. With the regulations that meet this need some rights have been granted to the data subjects and some obligations have been imposed on the data controllers. The right to data portability which has been introduced for the first time by the European Union General Data Protection Regulation, gives individuals more control over their personal data. While it will affect the level of competition in the markets due to the economic interests of data controllers, it is accepted that the right to data portability will also affects the interests of individuals in terms of the protection of personal data. In this study, the question of what should be understood from the right to data portability and how the right will affect competition has been answered by considering the multifaceted relationship between the protection of personal data, the right to data portability and competition law.

Key Words: Personal Data, Data Portability, Competition Law, Digital Markets.

ÖZET

KİŞİSEL VERİLERİN KORUNMASI VE REKABET HUKUKU BAĞLAMINDA VERİ TAŞINABİLİRLİĞİ HAKKI

Yılmaz, Beste

Yüksek Lisans, Özel Hukuk Programı

Tez Danışmanı: Dr. Hüseyin Can Aksoy

Haziran 2022

Verinin işlenmesi yoluyla önemli ekonomik menfaatler elde edilmesi, başta dijital pazarlar olmak üzere her türlü pazarda verinin elde edilmesini, işlenmesini ve akışının sağlanmasını ekonomik bir gereklilik haline getirmiştir. Bu veri kümesi içerisinde kişisel verilerin sınırsız ve ölçüsüz olarak işlenmesi kişisel verilerin korunması ihtiyacını doğurmuş, bu ihtiyaca cevap veren düzenlemelerle ilgili kişilere birtakım haklar tanınırken veri sorumlularına da bazı yükümlülükler getirilmiştir. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ilk kez tanıttığı veri taşınabilirliği hakkı, bireylere kişisel verileri üzerinde daha fazla kontrol imkânı tanımaktadır. Veri taşınabilirliği hakkının, bireylerin kişisel verilerin korunması yönünden menfaatlerine etki ederken, veri sorumlularının ekonomik menfaatleri dolayısıyla pazarlardaki rekabet düzeyine yönelik etkiler göstereceği kabul edilmektedir. Bu çalışmada, kişisel verilerin korunması, veri taşınabilirliği hakkı ve rekabet hukuku arasındaki çok yönlü ilişki dikkate alınarak veri taşınabilirliği hakkından ne anlaşılması gerektiği ve bu hakkın rekabeti nasıl etkileyeceği sorusu cevaplanmıştır.

Anahtar kelimeler: Kişisel Veri, Veri Taşınabilirliği, Rekabet Hukuku, Dijital Pazarlar.

TEŞEKKÜR

Tez yazım sürecimde yalpaladığım her anda desteğini cömertlikle sunan, önümü göremediğim zamanlarda yolumu aydınlatan pek çok kişi olduğunu mutlulukla ifade edebilirim. Öncelikle değerli tez danışmanım, Bilkent Üniversitesi Hukuk Fakültesi Medeni Hukuk Ana Bilim Dalı'nın kıymetli üyesi sayın Dr. Hüseyin Can AKSOY'a yalnızca tez sürecimde gösterdiği sonsuz sabır, verdiği emek ve destek için değil; bu tezin başlangıç aşamasından çok daha önce, henüz fakülte sıralarındayken kazandırdığı bakış açısıyla yolumu çizmemi sağladığı için teşekkürlerimi sunarım.

Tez savunma jürisinde yer alarak büyük bir titizlikle tezi inceleyen hocalarım sayın Dr. Selin ÖZDEN MERHACI'ya ve yine fakülte yıllarından bu yana kapısını her çaldığımda içtenlikle karşılayan sayın Dr. Pınar ÇAĞLAYAN AKSOY'a teşekkürlerimi sunarım.

Tez yazımı sürecinde, 2210-A Genel Yurt İçi Yüksek Lisans Bursu kapsamında sağladıkları imkân için TÜBİTAK Bilim İnsanı Destekleme Dairesi Başkanlığına teşekkür ederim.

Ve son olarak hayatı daha renkli, renkleri daha parlak hale getiren, hayatımın her bir parçasına; özellikle anneme, babama ve ailem haline gelen dostlarıma en içten teşekkürlerimi sunarım. İyi ki varsınız.

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM

KISALTMALAR CETVELİ

ABAD **:** Avrupa Birliği Adalet Divanı

ABD **:** Amerika Birleşik Devletleri

API **:**Uygulama Programlama Arayüzü (“*Application Programming Interface*”)

Birlik **:** Avrupa Birliği

CCTV **:** Close Circuit TeleVision

CSV **:** Comma Separated Values

Direktif **:** 95/46/AT sayılı Veri Koruma Direktifi

DMA **:** Dijital Pazarlar Yasası *(“Digital Markets Act”)*

DSA **:** Dijital Hizmetler Yasası *(“Digital Services Act”)*

GDPR **:** Genel Veri Koruma Tüzüğü

GPS **:** Global Positioning System

JSON **:** JavaScript Object Notation

KVKK **:** Kişisel Verilerin Koruması Kanunu

m. **:** madde

OECD **:** Ekonomik Kalkınma ve İş Birliği Örgütü *(“Organisation for Economic Co-operation and Development”)*

PDF **:** Portable Document Format

TFEU **:** Avrupa Birliği’nin İşleyişi Hakkında Anlaşma *(“Treaty on the Functioning of the European Union”)*

TMK **:** Türk Medeni Kanunu

XML **:** Extensible Markup Language

EKG **:** Elektrokardiyografi

RKHK **:** Rekabetin Korunması Hakkında Kanun

EIM **:** Export-Import Module

GİRİŞ

Sanayi devriminin bilgi teknolojileri yönünden önemli gelişmeler meydana getirmesiyle beraber veriye duyulan ihtiyaç artmıştır. Öyle ki veri, teknolojik gelişimin ticari metası, gün geçtikçe büyüyen dijital ekonominin yakıtı haline gelmiştir. Bu sebepledir ki endüstriyel ilerleme bakımından veri, yeni petrol olarak değerlendirilmektedir[1]. Verinin ve özellikle de kimliği belirli veya belirlenebilir bir gerçek kişiye ait olan veri anlamına gelen kişisel verinin yoğun ve kontrolsüz biçimde işlenmesi bir taraftan dijital ekonomiyi beslerken diğer taraftan kişilerin bazı hukuki menfaatlerinin korunması zorunluluğunu doğurmuştur. Bu menfaatlerin korunması açısından önemli ve kapsamlı bir düzenleme niteliği taşıyan ve 2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü (*"General Data Protection Regulation"*-GDPR), Avrupa Komisyonu'nun Dijital Tek Pazar Stratejisi oluşturma düşüncesine dayanmaktadır. Ekonomik etkisi de dikkate alındığında, kişisel verilerin, ilgili kişilere ait birtakım hak ve özgürlükler açısından korunurken rekabeti engellemeyecek, bilhassa rekabeti destekleyecek biçimde korunması suretiyle kişisel hak ve özgürlüklerin tüketici refahı anlayışı çerçevesinde ele alınması sağlanmış olacaktır.

Bir taraftan kişisel verilerin korunmasını amaçlarken diğer taraftan tüketici refahını artırması ve rekabet hukukunu desteklemesi beklenen düzenlemeler kişisel verilerin korunması ile rekabet hukuku arasındaki ayrımı belirsizleştirmiştir. GDPR'ın 20. maddesi ile düzenlenen veri taşınabilirliği hakkı, tam da kişisel verilerin korunması ile rekabet hukuku arasındaki kesişim kümesinde kalmaktadır. Hakkın GDPR'da öngörülme amacı bireylerin kişisel verileri üzerinde daha fazla kontrol imkânına sahip

[1] The Economist (2017), *Regulating the internet giants: The world's most valuable resource is no longer oil, but data,* (https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, E. T.: 16.12.2021).

olmasını sağlarken kişisel verilerini bir kere herhangi bir veri sorumlusu ile paylaşmış olmalarından ötürü hareket edememe tehlikesi altında kalmalarını önlemektir. Dolayısıyla GDPR'ın doğrudan rekabet hukukunu etkileme girişimi bulunmasa da rekabet hukuku alanında olumlu etki doğurması beklenen bir hakkı ilgili kişilere tanıdığı anlaşılmaktadır. Ne var ki hakkın rekabet hukukuna etkisini somut olarak ortaya koyan veriler henüz mevcut olmadığı gibi hakkın rekabet üzerindeki etkisi yönünden de tartışmalar bulunmaktadır.

Hakkın uygulamasının henüz Avrupa Birliği'nde (Birlik) de yeterince yaygınlaşmamış olması, tüm veri sorumluları için öngörülmüş olmasına karşın dijital pazarlarda uygulanma kabiliyetinin daha yüksek olması ve dijital pazarların geleneksel pazarlardan daha farklı karakteristik özellikler göstermesi veri taşınabilirliği hakkının hem kişisel verilerin korunması hukuku yönünden hem de rekabet hukuku yönünden incelenmeye değer noktalar barındırdığına işaret etmektedir. Bu çalışmada, kişisel verilerin korunması bakımından Avrupa Birliği'ndeki en kapsamlı ve güncel düzenlemeyi teşkil eden GDPR sistematiği içerisinde veri taşınabilirliği hakkının amacı, kapsamı, sınırları ve benzer müesseselerden farkının ortaya konması, Avrupa Birliği ve Türk rekabet hukuku çerçevesinde hakkın olası etkileri üzerine bir değerlendirme yapılarak kişisel verilerin korunması ve rekabet hukuku bağlamında hakkın ele alınması amaçlanmaktadır.

Bu doğrultuda çalışmanın ilk bölümünde veri taşınabilirliği hakkına ilişkin olarak Amerika Birleşik Devleri (ABD), Avrupa Birliği ve Türk hukukundaki gelişim çizgisi hakkında bilgi verilecektir. Ardından hakkın amacı, tanımı, unsurları, maddenin lafzında kullanılan terminolojik terimlerin ne anlama geldiği açıklanacak ve

bu sayede madde lafzının muğlaklığı giderilmeye çalışılacak; hakkın benzer kavramlardan farkları ortaya konacaktır.

Çalışmanın ikinci bölümünde, hakkın yer ve konu bakımından kapsamı ele alınacak, hakka ilişkin genel ve özel sınırlama sebepleri incelenecektir. Ardından hakkın kullanılması bakımından önem taşıyan hususlara değinilecek, Kişisel Verilerin Korunması Kanunu (KVKK) ve Genel Veri Koruma Tüzüğü çerçevesinde hakkın kullanımına ilişkin esaslar ifade edilecektir.

Nihayet son bölümde, kişisel verilerin korunması hukuku ile rekabet hukuku ilişkisi örnek kararlar üzerinden irdelenecek, veri taşınabilirliği hakkını destekleyen rekabet hukuku düzenlemeleri ile ilgili bilgi verilecektir. Ayrıca hakim durumun kötüye kullanılması, anlaşma, uyumlu eylem, teşebbüs birliklerinin karar ve eylemleri ve rekabeti bozucu, kısıtlayıcı, engelleyici etki doğurabilecek birleşme ve devralmalar veri taşınabilirliği hakkı çerçevesinde ele alınacak, özellikle dijital pazarlarda etki gösteren değiştirme maliyetleri, ağ etkileri, ölçek ve kapsam ekonomileri ile pazara giriş engelleri gibi karakteristik özellikler dikkate alınarak veri taşınabilirliği hakkının rekabet hukukuna etkisi incelenecek ve son olarak doktrindeki görüşler hakkında bilgi verilerek değerlendirmede bulunulacaktır.

BİRİNCİ BÖLÜM

VERİ TAŞINABİLİRLİĞİ HAKKI

§ 1. GENEL OLARAK VERİ TAŞINABİLİRLİĞİ KONUSUNDAKİ DÜZENLEMELER VE TÜRK HUKUKUNDAKİ DURUM

I. AMERİKA BİRLEŞİK DEVLETLERİ'NDE VERİ TAŞINABİLİRLİĞİNE İLİŞKİN DÜZENLEMELER

Avrupa'da 2018 senesinde yürürlüğe giren GDPR öncesinde var olan veri taşınabilirliğine yönelik rekabet hukuku temelli değerlendirmeler, Amerika Birleşik Devletleri'nde de rekabet hukuku düzenlemeleri olan *Sherman Act* ve *Clayton Act* uyarınca rekabet hukuku bağlamında sürdürülmüştür. ABD'de hala federal düzeyde veri taşınabilirliği hakkı tanıyan bir düzenleme bulunmasa da Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası (*The 1996 Health Insurance Portability and Accountability Act*)[2], bireylere kendileri hakkında tutulan sağlık verilerine erişim hakkı sağlayan ilk düzenleme olması dolayısıyla önem taşımaktadır. Ne var ki bu düzenleme ile tam anlamıyla bir veri taşınabilirliği hakkı tanındığı söylenemez. Nitekim bugün GDPR anlamında kişisel verilerin alınması, ilgili kişi tarafından bir başka veri sorumlusuna[3] iletilmesi veya doğrudan veri sorumluları arasında iletimin gerçekleşmesini ifade eden veri taşınabilirliğinden farklı olarak bu düzenlemede, GDPR m. 15'te öngörülen erişim hakkının bir benzeri olduğu kabul edilmektedir. 2010

[2] Düzenleme için bkz. (https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf, E.T.: 05.05.2022).

[3] GDPR m. 4/7 ve KVKK m. 3/1-ı uyarınca kişisel verilerin işleme amaçlarını ve vasıtalarını tek başına veya birlikte belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, kamu kurum ve kuruluşu teknik anlamda veri sorumlusu ("*controller*") sıfatını taşımaktadır. İşleme amaç ve vasıtalarının kim tarafından belirlendiği somut olayın özelliklerine göre belirlenmelidir. Somut olayda hangi kişisel verilerin toplanacağına, bunların ne şekilde ve nerede muhafaza edileceğine, hangi yollarla korunacağına, kimlere aktarılacağına vb. karar verme yetkisine sahip olan gerçek veya tüzel kişi veri sorumlusudur. **Çekin**, M. S.: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, İstanbul 2020, s. 54-56.

tarihli Dodd-Frank Wall Street Reformu ve Tüketicinin Korunması Yasası (*Dodd-Frank Wall Street Reform and Consumer Protection Act)*[4] finansal ve mali haklar bakımından tüketicilere bir kontrol sağlamış ve taşınabilirliği kabul etmiştir.

Esasen ABD'de veri taşınabilirliği hakkını geliştirmek üzere çalışmalar yapılmış, Bilim ve Teknoloji Politikası Ofisi (*Office of Science and Technology Policy*) paydaş görüşlerini[5] toplamıştır. Paydaş görüşleri, bugün GDPR ile düzenlenen veri taşınabilirliği hakkına ilişkin doktrinde ileri sürülen görüşlerle paralellik göstermesi bakımından önem taşır. Ancak ifade etmek gerekir ki ABD'de hakkın ele alınış biçimi Avrupa'daki gibi ilgili kişinin hakkı niteliğinde değil, veri sorumlusunun tercihi niteliğindedir[6].

Eyalet düzeyindeki düzenlemelere bakıldığında ise veri taşınabilirliği hakkının uygulamaya daha fazla dahil edilmeye çalışıldığına ilişkin göstergeler mevcuttur. Bu kapsamda, 2018 tarihli California Tüketici Gizliliği Yasası (*California Consumer Privacy Act*)[7] teşebbüslerin bir erişim talebi doğrultusunda tüketiciye elektronik olarak veri sağladıkları takdirde bu verilerin, teknik olarak uygulanabilir olduğu ölçüde, engelsiz olarak üçüncü taraflara iletilmesine ve kolayca kullanılabilmesine izin veren bir formatta olması gerektiğini öngörmektedir. Federal düzeyde bir düzenleme bulunmasa da Avrupa'da mevcut olan veri taşınabilirliği düzenlemelerine benzemekle

---

[4] Düzenleme için bkz. (https://www.govinfo.gov/content/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf, E.T.: 05.05.2022).

[5] Çağrı metni için bkz. (https://www.govinfo.gov/content/pkg/FR-2016-10-07/pdf/FR-2016-10-07.pdf 69873-69874, E.T.: 05.05.2022). Toplanan görüşlere ilişkin detaylı açıklama için bkz. **Vanberg**, A. D.: *The Right to Data Portability in the GDPR: What Lessons Can Be Learned From the EU Experience?*, Journal of Internet Law 2018, Vol. 21, No.7, s. 17.

[6] **Vanberg**, s. 17.

[7] Düzenleme için bkz. (https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121, E.T.: 05.05.2022).

beraber daha esnek bir dil benimseyen eyalet düzenlemesinin tüketicinin korunması ve kişisel verilerin korunması anlamında önemli bir adım olduğu söylenmelidir.

II. AVRUPA BİRLİĞİ'NDE (BİRLİK) VERİ TAŞINABİLİRLİĞİNE İLİŞKİN DÜZENLEMELER

Bugün veri taşınabilirliği kişisel verilerin korunması alanında gündeme gelen bir başlık olsa da Avrupa Birliği'nde GDPR'ın yürürlüğe girmesinden çok daha önce Avrupa Birliği'nin İşleyişi Hakkında Anlaşma (*Treaty on the Functioning of the European Union*-TFEU)[8] m. 102'de hakim durumun kötüye kullanılması durumu altında incelenen bir rekabet hukuku sorunu olarak ele alınmaktaydı. Kişisel verilerin korunması alanındaki çalışmaların başladığı ilk yıllarda kişisel verinin ne olduğu ve korunmasını gerektiren menfaat gibi daha temel sorunlar gündeme alınmış, taşınabilirlik bir rekabet hukuku meselesi olarak irdelenmeye devam edilmiştir. 1995 senesine gelindiğinde, Avrupa Birliği düzeyinde kişisel verilerin korunması alanında atılmış en önemli adımlardan biri olan[9] 95/46/AT sayılı Veri Koruma Direktifi'nin

[8] Consolidated version of the Treaty on the Functioning of the European Union, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT, E.T.: 05.05.2022).

[9] Avrupa Komisyonu tarafından hazırlanan "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 95/46/AT sayılı Direktif" 20 Şubat 1995 yılında kabul edilmiş, 24 Ekim 1995 tarihinde onaylanmış ve bundan üç yıl sonra 25 Ekim 1998'de yürürlüğe girmiştir. TFEU m. 16'da herkesin kendisiyle ilgili kişisel verilerin korunması hakkına sahip olduğu öngörülmüş olup Direktif'in temelini de bu hüküm oluşturmaktadır. Direktif'in amacı, özel hayatın gizliliği ile kişisel verilerin dolaşımı arasında dengenin kurulabilmesidir. 2018 yılında yürürlüğe giren 2016/679 sayılı GDPR ile 95/46/AT sayılı Direktif yürürlükten kalkmış olsa da gerek GDPR gerekse Türk hukuku açısından 6698 sayılı Kişisel Verilerin Korunması Kanunu dahil olmak üzere pek çok devletin iç hukuk düzenlemeleri nezdinde dikkate alınan kaynaklardan birini teşkil etmiştir. 95/46/AT sayılı Direktif ile birtakım önemli organlar kurulmuş, bu organlar kişisel verilerin korunması alanında çeşitli görevler üstlenmiştir. Ayrıca 95/46/AT sayılı Direktif düzenlemesinden sonra telekomünikasyon sektörüne özel olarak *lex specialis* niteliğinde 97/66/AT sayılı direktif çıkarılmıştır. Esasen 95/46/AT sayılı Direktif'in asıl önemi Avrupa Birliği hukuku kapsamında direktiflerin normlar hiyerarşisi içindeki yerinden kaynaklanmaktadır. Direktifler, TFEU'nun 28. maddesi uyarınca doğrudan bağlayıcı olmayan kaynaklardır. Tüm üye devletlere ayrıca yönlendirilmeleri gerekmeksizin şekil ve yöntem bakımından yetkisi bırakırken, son noktada direktifin getirdiği temel ilkeleri içeren ulusal mevzuat düzenlemesi yapmak ve direktifle uyumlu hale getirmek yönünden eşit ağırlıkta olmaları beklenmektedir. Bu yönü ile Direktif ile ilgili kişilere (veri sahiplerine) doğrudan tanınmış olan hakların ihlali halinde Avrupa Birliği'ne üye devletlerin vatandaşlarının, Direktif'te yer alan hükümlere dayanarak yargı yoluna başvurması mümkündür. Bu hususta detaylı açıklama için bkz. **Akıncı**, A. N.: *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından*

(Direktif)[10] veri taşınabilirliği hakkına yer vermediği görülmektedir. Bununla birlikte, ilerleyen yıllarda veri taşınabilirliği hakkı sınırlı bir kapsamda da olsa özel düzenlemelere konu edilmiştir. 2002 senesinde telekomünikasyon alanında yapılan önemli bir düzenleme ile cep telefonu kullanıcılarının belli bir operatörden bir başkasına geçmesini kolaylaştıran Evrensel Hizmet Direktifi (*Universal Service Directive*)[11] kabul edilmiştir. Kamu sektörü bilgilerinin yeniden kullanımına ilişkin 2013 tarihli Kamu Sektörü Bilgi Direktifi'nde (*Public Sector Information Directive*)[12] bilgi sistemleri arasında taşınabilirliği kolaylaştıracak hükümler öngörülmüştür. Bankacılık sektöründe ise Ödeme Hizmetleri Direktifi (*Payment Services Directive*)[13] ile 2015 senesinde, ödeme hizmetlerini kolaylaştırmak için müşteri hesap verilerinin bir bankacılık kurumuna taşınabilirliği düzenlenmiştir.

Nihayet Avrupa Birliği düzeyinde 2018 tarihli GDPR ile düzenlenen veri taşınabilirliği hakkı GDPR'ın sistematiği içinde ilgili kişinin haklarını düzenleyen Bölüm III'te[14], Veri Taşınabilirliği Hakkı ("*Right to Data Portability*") olarak

---

Değerlendirilmesi, Çalışma Raporu-6, 2017, s. 10.; **Başalp**, N.: Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s. 31. Direktif'in 29. maddesi uyarınca kurulan 29. Madde Çalışma Grubu'nun ("*Article 29 Data Protection Working Party*"), kişisel verilerin korunması konusunda rapor, görüş ve yorumlar ile teori ve uygulamaya yol gösteren önemli organlardan biri olduğu yönünde bkz. **Develioğlu**, H. M.: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017, s. 11; **Küzeci**, E.: Kişisel Verilerin Korunması, 4. Baskı, Ankara 2020, s. 177.

[10] Direktif'in tam metni için bkz. (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML, E. T.: 05.05.2022).

[11] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services, (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32002L0022, E.T.: 05.05.2022).

[12] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, (https://eur-lex.europa.eu/eli/dir/2013/37/oj, E.T.: 05.05.2022).

[13] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366, E.T.: 05.05.2022).

[14] Türk hukukunda 6698 sayılı KVKK ile ilgili kişiye tanınan tüm haklar GDPR'da da öngörülmüş olmakla beraber GDPR'da ilgili kişiye bunlar dışında başka haklar da tanınmaktadır. Bu kapsamda ilgili kişiye; kişisel verilerin işlenip işlenmediğini öğrenme hakkı (T.C. Anayasası m. 20, KVKK m. 11/1-a ve GDPR m. 15/1), işlenmiş kişisel verilere ilişkin bilgi talep etme hakkı (T.C. Anayasası m. 20, KVKK

ifadesini bulmuştur. TFEU hariç olmak üzere daha önceki düzenlemelerden farklı olarak tüzük olarak çıkarılan GDPR, üye devletler için doğrudan bağlayıcı ilk düzenleme olması bakımından önem taşır. Bu düzenleme ile veri taşınabilirliği, rekabet hukuku düzenlemelerinden sıyrılarak kişisel verilerin korunması alanında önemli bir yer edinmiştir. Her ne kadar aksini savunanlar bulunsa da hakkın rekabeti güçlendirmeye, tüketici refahını artırmaya, inovasyonu destekleme potansiyeli olduğu ifade edilmektedir[15]. Hakkın, bu bölümde detaylı olarak incelenmeye çalışılan unsurları henüz uygulamada net olarak anlaşılabilir olmadığından, muğlak ifadelerin hakkın uygulanmasını etkilediği görülmektedir. Öyle ki GDPR m. 20 ile getirilen veri taşınabilirliği hakkı uygulamada henüz ne veri sorumluları ne de ilgili kişiler tarafından yeterince özümsenmiştir. Maddenin pek çok teknik terim içeren ve bu terimlerin nasıl anlaşılması gerektiğini netleştirmeyen lafzı yanında 29. Madde Çalışma Grubu'nun yayımladığı rehber de bu bakımdan yetersiz görünmektedir[16]. GDPR m. 20'nin uygulamada nasıl karşılandığını somut biçimde ortaya koymak için farklı sektörlerden veri sorumlularına 230 veri taşınabilirliği talebinde bulunan[17], spor

m. 11/1-b ve GDPR m. 15/1), (T.C. Anayasası m. 20, KVKK m. 11/1-c ve GDPR m. 15/1-a) kişisel verilerin işlenme amaçlarını ve işlemenin amaca uygunluğunu öğrenme hakkı (T.C. Anayasası m. 20, KVKK m. 11/1-c ve GDPR m. 15/1-a), kişisel verilerin yurt içinde ve dışında aktarıldığı üçüncü kişileri öğrenme hakkı (T.C. Anayasası m. 20, KVKK m. 11/1-ç ve GDPR m. 15/1-c), kişisel verilerin işlenmesinde eksikliğin giderilmesi ve yanlışlığın düzeltilmesi hakkı (T.C. Anayasası m. 20, KVKK m. 11/1-d ve GDPR m. 16), kişisel verilerin silinmesini isteme hakkı (T.C. Anayasası m. 20, KVKK m. 11/1-e ve GDPR m. 15/1-e ile m. 17), eksiklikleri giderme, düzeltme, silme taleplerinin üçüncü kişilere bildirilmesini talep hakkı (KVKK m. 11/1-f ve GDPR m. 19), itiraz hakkı (KVKK m. 11/1-g ve GDPR m. 15/1-h ile m. 21), tazminat hakkı (KVKK m. 11/1-ğ ve GDPR m. 82) tanınmaktadır. Türk hukukundan farklı olarak GDPR m. 18 ile ilgili kişiye işlemenin sınırlandırılması hakkı ve m. 20 ile veri taşınabilirliği hakkı tanınmıştır.

[15] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, (https://ec.europa.eu/newsroom/article29/items/611233, E. T.: 03.05.2022), s. 3. Hakkın rekabet hukuku ile ilişkisi aşağıda ayrıca ele alınacaktır.

[16] **Wong**, J./**Henderson**, T.: *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, International Data Privacy Law 2019, Vol. 9, No. 3, s. 186.

[17] **Wong/Henderson**, s. 174.

esnasında sağlık verilerini tutan 7 veri sorumlusunun dönütlerini inceleyen[18], mevcut veri sorumlusunda bulunan kişisel verilerin doğrudan başka bir veri sorumlusuna iletilmesi hakkını düzenleyen m. 20/2'nin uygulamasını incelemek üzere 182 veri sorumlusuna başvuran[19], hakkın uygulanabilirliğini[20] sorgulayan, hakka ilişkin kullanıcı görüşlerini[21] araştıran çeşitli sosyal araştırmalar yapılmıştır. Tüm bu çalışmalar, uygulamada veri taşınabilirliği hakkının gerek veri sorumluları gerekse ilgili kişiler tarafından anlaşılmadığını, hakkın ne şekilde kullanılması gerektiğinin bilinmediğini, bu yolla anlamlı bilgilere erişmenin zorluklarını ortaya koymaktadır. Veri taşınabilirliği hakkının uygulamasının yaygınlaşması ile hakkın sağlaması beklenen rekabet ve tüketici refahı artışının gerçekleşip gerçekleşmeyeceğine ilişkin somut dönütlerin de artması muhtemeldir.

Verinin dijital ekonominin kaldıracı olarak görülmesi, Birlik sınırları dahilinde verinin kolaylıkla akışını sağlayacak mekanizmalar kurarak dijital bir ortak pazar kurma amacına hizmet eder. Bu anlamda yukarıda açıklanan düzenlemelerden sonra kişisel olmayan verilerin de Birlik içerisinde akışını kolaylaştıracak bir düzenleme yapma ihtiyacı duyulmuş, Kişisel Olmayan Verilerin Serbest Akışına İlişkin Tüzük (*Regulation on a Framework for the Free Flow of Non-Personal Data in the European*

[18] **Zwiebelmann**, Z./**Henderson**, T.: *Data Portability as a Tool for Audit*, Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers 2021, s. 277.
[19] **Syrmoudis**, E./**Mager**, S./**Kuebler-Wachendorff**, S./**Pizzinini**, P./**Grossklags**, J./**Kranz**, J.: *Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20*, Proceedings on Privacy Enhancing Technologies 2021, Vol.2021(3), s. 351.
[20] **Turner**, S./**Quintero**, J. G./**Turner**, S./**Lis**, J./**Tanczer**, L. M.: *The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment*, New Media & Society 2021, Vol. 23(10), s. 2862.
[21] **Karegar**, F./**Pulls**, T./**Fischer-Hübner**, S.: *Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This?*, Lehmann, A., Whitehouse, D., Fischer-Hübner, S., Fritsch, L., Raab, C. (eds) Privacy and Identity Management Facing up to Next Steps. Privacy and Identity 2016. IFIP Advances in Information and Communication Technology, Vol 498, Springer, Cham., s. 169.

Union)[22] kabul edilmiştir. Düzenlemenin temelinde kişisel olmayan veriler ile kişisel veriler beraber taşınabilir olacak şekilde yapılandırılmadıkça veri iletim süreçlerinin daha uzun ve maliyetli olacağı ve bunun da Avrupa Birliği'nde rekabetçi ve veri odaklı hedeflere tam olarak ulaşılmasını engelleyeceği düşüncesi[23] bulunmaktadır.

Son olarak, bir süredir görüşmelerine devam edilen Dijital Pazarlar Yasası (*Digital Markets Act*)[24] hakkında Avrupa Parlamentosu ve Avrupa Konseyi 24 Mart 2022 tarihinde geçici bir anlaşmaya varmış bulunmaktadır. İnternet ortamında daha adil rekabeti, inovasyonu ve kullanıcıların korunmasını sağlamayı amaçlayan taslak, aynı zamanda geçit bekçisi ("*gatekeeper*") konumundaki teşebbüslerin birlikte çalışabilir sistemler kurmasını öngörmektedir[25].

III. TÜRK HUKUKUNDA VERİ TAŞINABİLİRLİĞİNE İLİŞKİN DÜZENLEMELER

Türk hukukunda kişisel verilerin korunması alanında var olan düzenlemelerde veri taşınabilirliği hakkı bulunmamaktadır. Veri taşıma anlamında Türk hukukunda yer alan tek düzenleme Avrupa'daki Evrensel Hizmet Yönetmeliği'ne paralel olarak çıkarılan Numara Taşınabilirliği Yönetmeliği'dir[26]. Buna karşılık kamu sektöründe

[22] 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, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807, E. T.:05.05.2022).

[23] **Unver**, M.: *Turning the crossroad for a connected world: Reshaping the European prospect for the Internet of Things*, International Journal of Law and Information Technology 2018, Vol. 26(2), s. 106.

[24] Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) ("Dijital Pazarlar Yasası Taslağı"), COM (2020) 842 final, 15.12.2020, (https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf, E. T.: 06.05.2022).

[25] Avrupa Komisyonu Başkan Yardımcısı Margrethe Vestager'in taslak metne ilişkin açıklamaları ve metnin ekim ayında yürürlüğe girmesinin beklendiği yönündeki beyanı için bkz. (https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_2042, E. T.:05.05.2022).

[26] Düzenleme için bkz. (https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=13180&MevzuatTur=7&MevzuatTertip=5, E. T.: 05.05.2022).

birlikte çalışabilirlik esaslarının benimsenmesine ilişkin politikalar benimsenmiştir[27]. Ne var ki bunlar da bugün dijital ortamlardaki gereklilikleri karşılayacak düzeyde olmayıp kamuda kullanılan teknik standartlar ve formatlara ilişkin genel esaslar niteliğindedir.

Türk hukukunda kişisel verilerin korunması alanında yapılan çalışmalar Avrupa'daki çalışmalara nazaran geç kalmıştır[28]. Ancak bu durum aynı zamanda Avrupa'da işleyen sistemi gözlemleme ve deneyimlerden yararlanma olanağı da sunmuştur. Bu kapsamda 6698 sayılı KVKK'nın hazırlık çalışmalarında, henüz o dönemde yürürlükte olan 95/46/AT sayılı Direktif esas alınmıştır[29]. 95/46/AT sayılı Direktif'te veri taşınabilirliği hakkının öngörülmemiş olması KVKK'da bu hakka neden yer verilmediğini açıklamaktadır[30]. Oysa kanun koyucunun aynı dönemlerde tamamlanma aşamasında olan GDPR'dan haberdar olmaması beklenemez. Bu bölümde ele alınmaya çalışıldığı üzere GDPR m. 20 ile öngörülen veri taşınabilirliği hakkı muğlak ve problemli pek çok nokta barındırmaktadır. Bu sebeple Türkiye'de bir düzlem kazanması çok yakın bir tarihe dayanan kişisel verilerin korunması alanında temkinli davranmak isteyen, bu alanda farkındalık ve kişisel veri koruma kültürü tam olarak oluşmadan karmaşık bir düzenleme ile uygulamayı içinden çıkılamaz bir hale

[27] Kamu Bilgi Sistemlerinde Birlikte Çalışabilirlik Esasları Rehberi ilk olarak 2005 yılında yayımlanmış, bu belgenin ikinci sürümü 28.02.2009 tarih ve 27155 sayılı Resmî Gazete'de yayımlanan 2009/04 sayılı Başbakanlık Genelgesi uyarınca hazırlanmıştır.

[28] Türk hukukunda konuya ilişkin çalışmalar 1989 yılına uzansa da ulusal düzenlemelerin geçmişi pek de eskiye dayanmamaktadır. Kişisel verilerin korunması bağlamında Türk hukukunda ilk olarak 12 Ekim 2004 tarih ve 5237 sayılı Türk Ceza Kanunu'nun 9. bölümünde düzenlemeye yer verilmiştir. Konunun anayasal bir zemine kavuşması ise 2010 yılında "Özel hayatın gizliliği" başlıklı 20. maddeye eklenen fıkra ile gerçekleşmiştir. Özel düzenleme yapma ihtiyacının doğması sebebiyle 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

[29] **Çekin**, s. 3; **Dülger**, M. V.: Kişisel Verilerin Korunması Hukuku, 1. Baskı, İstanbul 2019, s. 73.

[30] Buna karşılık KVKK ve GDPR'ın kabul edildiği tarihler arasında son derece küçük bir zaman farkı bulunmaktadır. Bu sebeple doktrinde KVKK'nın yapımı aşamasında GDPR'ın temel alınmaması eleştirilmiştir**.** Bkz. **Çekin**, s. 3.

getirmekten kaçınan yasa koyucunun bir yasama politikası olarak da değerlendirilebilir.

§ 2. VERİ TAŞINABİLİRLİĞİ HAKKININ AMACI, TANIMI VE UNSURLARI

I. HAKKIN AMACI

İnternet kullanımının yaygınlaşması, bulut bilişim, yapay zekâ gibi alanlardaki teknolojik gelişmeler ile kullanıcılar, bir çevrimiçi platformda oluşturdukları profillerin, arkadaş listelerinin, özel konuşmalarının ve bunun gibi pek çok kişisel verinin meydana getirdiği birer dijital kimliğe sahip olmuşlardır. Ticari faaliyetlerin yürütülmesinde çevrimiçi alışveriş uygulamalarının, teşebbüslere rekabet avantajı sağlaması ve bu platformlarda toplanan ve biriken verilerin çevrimiçi itibar[31] adı verilen bir değeri ortaya çıkarması ile dijital kimliğin bu türden verileri de içerdiği kabul edilmeye başlanmıştır. Kullanıcının bir uygulamadan, çevrimiçi platformdan veya hizmet yahut ürün aldığı veri sorumlusundan bir diğerine geçmesi halinde bir birikimin ürünü olan dijital kimliğin yok olması tehlikesi, kişileri mevcut veri sorumlularının sistemlerinden ayrılamamalarına sebep olmaktadır[32]. Dahası bu durum, günümüzde dijital kimliğin kişiliğin önemli bir parçasını oluşturduğu dikkate

[31] Çevrimiçi itibar bir teşebbüsün, organizasyonun, kişinin sosyal medya gibi çevrimiçi ortamlardaki itibarını ifade eder. Çevrimiçi satın alma uygulamalarında sıklıkla kullanılan alıcı ve satıcı puanlama geri bildirimleri çevrimiçi itibarın unsurlarından biri olarak değerlendirilebilir.

[32] **European Commission, Commission Staff Working Paper**, *Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Impact Assessment report),* SEC(2012) 72 final, (https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf, E. T.: 06.05.2022), s. 28.

alındığında herkesin maddi ve manevi varlığını koruma ve geliştirme şeklindeki temel hakkının beslenmesinin önünde büyük bir engel oluşturmaktadır.

Söz konusu olumsuz etkileri ortadan kaldırmaya yönelik girişimin doğal bir sonucu olarak veri sorumlusu hizmet sağlayıcılar arasındaki rekabetin etkilenmesi azımsanmayacak bir etki doğurmaktadır. Bir tarafta ilgili kişilerin kişisel verilerinin korunması menfaati, diğer tarafta ise veri sorumlusu hizmet sağlayıcıların ilgili pazardaki rekabet güçlerini korumaya ve inovasyonun desteklenmesine yönelik menfaatleri bulunmaktadır. Çatışan iki menfaat arasında ilgili kişinin kişisel verilerinin korunması, veri sorumlularının ilgili pazardaki rekabet güçlerini korumalarına üstün tutulmuştur. Nitekim bu husus yalnızca GDPR'da değil, Avrupa Birliği bünyesinde rekabet hukuku alanında yapılan çalışmalarda da kendini göstermektedir. Rekabet hukukunun gayesi de teşebbüsler arasında adil rekabeti sağlamak, inovasyonu desteklemek, dışlayıcı davranışları engellemektir. Bu yönü ile GDPR m. 20 düzenlemesinin amacı rekabet hukukunun güttüğü amaçla paraleldir ancak bu amacı kişisel verilerin korunması perspektifinden benimsemiştir[33]. Ayrıca tekelci güce ulaşmak isteyen teknoloji platformlarının kullanıcılar üzerinde dört duvar arasındaki bahçe ("*walled garden*") etkisine sahip olduğu da dikkate alınmalıdır. Dört duvar arasındaki bahçe, kullanıcılar bunun içinde sıkışmış hissedene dek rahat bir yerdir ancak veri taşınabilirliği hakkını teşvik etmek, kullanıcıların, rahatsızlık hissettikleri noktada hizmet sağlayıcıların duvarlı bahçelerindeki kapıları bulmalarına olanak tanır[34].

[33] GDPR'ın rekabet mantığından ayrıştırılması ve farklı yorumlanması gerektiği yönündeki görüş için bkz. **Lynskey**, O.: *Aligning data protection rights with competition law remedies? The GDPR Right to data portability*, European Law Review 2017, s. 810.

[34] **Nixdorf**, W.: *Planting in a Walled Garden: Data Portability Policies to Inform Consumers How Much (If Any) of the Harvest Is Their Share,* Transnational Law and Contemporary Problems 2019, Vol. 29, No. 1, s. 138, 165.

Tüm bu ihtiyaçlara cevap vermek üzere benimsenen veri taşınabilirliği hakkının nihai amacı, bilgi gizliliği ve veri sorumluları arasındaki adil rekabeti koruyarak kişiliğin korunması ve geliştirilmesine katkıda bulunmak, kişisel veriyi işleyecek veri sorumlusunu seçme olanağı tanıyarak enformasyonel self determinasyon hakkına işlerlik kazandırmak[35], kişisel veri transferleri üzerinde kontrol ve kişisel verinin yeniden kullanılmasını sağlamak ve eşitliği kolaylaştırmaktır[36]. GDPR'ın lafzi yorumundan anlaşıldığı üzere hakkın her koşulda uygulanması zorunlu tutulmamaktadır. Bununla beraber henüz pek çok devlette veri taşınabilirliği hakkı iç hukuk düzenlemelerinde yer almamaktadır. Ayrıca hakkın bir yandan ilgili kişilerin kişisel verileri üzerindeki kontrolü artırırken diğer yandan rekabeti güçlendirici bir araç olarak görülmesi, ekonomik birtakım menfaatlerin de hakka dahil olduğunu ortaya koymaktadır. Bu hususlardan hareketle hakkın temel insan hakkı mertebesinde olmadığı söylenebilir[37].

II. HAKKIN TANIMI VE UNSURLARI

GDPR m. 20 ile ilgili kişiye tanınmış bir hak olan veri taşınabilirliği hakkı, ilgili kişinin veri sorumlusuna sağladığı ve veri sorumlusu tarafından otomatik yollarla tutulan kişisel verilerini (i)yapılandırılmış, yaygın şekilde kullanılan ve makine tarafından okunabilir bir formatta almasına ve veri sorumlusunun herhangi bir engellemesine maruz kalmaksızın bunları bir başka veri sorumlusuna iletmesine veya (ii)bu verilerin başka bir veri sorumlusuna iletilmesini istemesine imkân tanımaktadır. Bu yönü ile veri taşınabilirliği hakkını, ilgili kişinin GDPR m. 15'te düzenlenen erişim

[35] **Zanfir**, G.: *The right to Data portability in the context of the EU data protection reform*, International Data Privacy Law 2012, Vol. 2, No. 3, s. 151.
[36] **Ursic**, H.: *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, SCRIPTed: Journal of Law, Technology and Society 2018, Vol. 15, No. 1, s. 45.
[37] **Swire**, P./**Lagos**, Y.: *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, Maryland Law Review 2013, Vol. 72, No. 2, s. 367.

hakkının bir uzantısı olarak kabul edenler mevcuttur[38]. Oysa veri taşınabilirliği en basit ifadesi ile kişisel veriyi cihazlar ve hizmetler arasında yeniden kullanma yeteneğidir[39].

A. İşlenen Kişisel Verileri Alma ve İletme Hakkı (Dolaylı Taşınabilirlik-"*Indirect Portability"*)

Veri taşınabilirliği hakkını düzenleyen hüküm içerik bakımından iki farklı hak tanımaktadır. İlk olarak GDPR m. 20/1 ilgili kişiye, kendisi ile ilgili olarak bir veri sorumlusuna sağladığı ve veri sorumlusunca GDPR m. 6/1-a veya 9/2-a uyarınca ilgili kişinin rızasına ya da GDPR m. 6/1-b uyarınca sözleşmeye dayalı olarak ve otomatik yollarla işlenen kişisel verilerini yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma ve kişisel verilerin sağlandığı veri sorumlusunun herhangi bir engellemesi olmaksızın bu verileri başka bir veri sorumlusuna iletme hakkı[40] tanımaktadır. Esasen veri taşınabilirliği hakkının erişim hakkını düzenleyen GDPR m. 15'in uzantısı olarak görülmesinin sebebi de bu tanımda yatmaktadır. Nitekim hakkın kullanılmasının iki aşaması mevcuttur. İlk aşama, ilgili kişinin hükümdeki şartlara bağlı kalarak, veri sorumlusu tarafından işlenen kişisel verilerini hükümde belirtilen formatta alması, ikinci aşama ise bu kişisel verilerini bir başka veri sorumlusuna bizzat kendisinin iletmesidir. Veri taşınabilirliği hakkının ileri sürüldüğü veri sorumlusunu ilk veri sorumlusu, daha sonra kişisel verilerin ilgili kişi tarafından iletildiği veri sorumlusunu ikinci veri sorumlusu olarak nitelemek mümkündür. Ancak bu iki veri sorumlusu arasında doğrudan bir iletişim söz konusu değildir. Hakkın kullanılması ilgili kişinin iki aşama arasında adeta köprü vazifesi

[38] **Vanberg**, s. 11. İki hakkın ilişkisi ve daha detaylı değerlendirme için bkz. Birinci Bölüm §2, III, B.
[39] **Custers**, B./**Ursic**, H.: *Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection*, International Data Privacy Law 2016, Vol. 6, No:1, s. 8-9.
[40] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 4.

üstlenmesine bağlı olduğundan veri taşınabilirliğinin bu türü dolaylı taşınabilirlik ("*indirect portability*") olarak adlandırılmaktadır.

GDPR m. 20'de ilgili kişinin kendisi tarafından veri sorumlusuna sağlanan kişisel verilerini yapılandırılmış, yaygın ve makine tarafından okunabilir bir formatta alma hakkından söz edilmişse de ne madde içeriğinde ne de GDPR'ın gerekçesinde "yapılandırılmış, yaygın ve makine tarafından okunabilir bir format" ifadesinin ne anlama geldiği açıklanmıştır[41]. Hukuki etki ve sorumluluk doğuracak bir düzenlemede teknik terimlerin kullanılması kimin zaman kaçınılmaz olsa da bunlar kullanılırken büyük bir hassasiyet gösterilmesi gerekir. Ne ifade ettiği anlaşılamayan, muğlak, çift anlamlı düzenlemeler hukuki belirlilik ilkesine zarar verir. Veri taşınabilirliği gibi teknolojik gelişmelerle, bilgisayar diliyle iç içe bir konunun düzenlenmesi bazı teknik terimlerin kullanımını gerektiriyorsa da bunların ne anlama geldiğinin uygulamayı sağlayacak düzeyde ortaya konması bir zorunluluktur. Bu hususta, 29. Madde Çalışma Grubu'nun yayımlamış olduğu rehberde birtakım açıklamalar bulunsa da madde metninde ifade edilen tüm terimlerin açıklanmadığı, açıklanan terimlerin ise yeterince detaylandırılmadığı göz önüne alındığında GDPR m. 20 ekseninde bu zorunluluğun karşılanamadığı açıkça ifade edilmelidir.

1. Yapılandırılmış Veri ("*Structured Data*")

Tüm verilerin kendi içerisinde bir yapısı olmakla birlikte veri taşınabilirliği hakkının unsurlarından birini oluşturan "yapılandırılmış veri" kavramı veriye ait ögeler arasındaki yapısal ilişkinin bir bilgisayar diskinde depolanma biçiminde açık

[41] Hükmün ifadesindeki belirsizlikler doktrinde de eleştirilmiştir. Bkz. **De Hert**, P./**Papakonstantinou**, V./**Malgieri**, G./**Beslay**, L./**Sanchez**, I.: *The right to data portability in the GDPR: Towards user-centric interoperability of digital services,* Computer Law & Security Review 2018, s. 199; **Graef,** I./**Verschaleken,** J./**Valcke**, P.: *Putting the right to data portability into a competition law perspective,* Law: The Journal of the Higher School of Economics Annual Review 2013, s. 63.

olmasını ifade eder[42]. Bunlar bir şemaya bağlı olarak sınırlandırılmıştır. Yapılandırılmış biçimin en yaygın kullanılan örneği verilerin satır ve sütunlar halinde bulunduğu formatlardır. Son derece yaygın olarak kullanılan *Excel* uygulamasında satır ve sütunlarda düzenlenen veriler bir elektronik tablo oluşturmakta, bu da bilgisayar tarafından okunabilirliği kolaylaştırmaktadır. *Extensible Markup Language* (XML) ve *Comma Separated Values* (CSV) birçok yapı türünün sunulmasına izin veren ve en yaygın şekilde kullanılan biçimlerdendir. Bir şema tarafından sınırlandırılmayan, bir başka ifade ile yapılandırılmamış verinin en yaygın örneği *Wold Wide Web*'tir[43]. Teknik olarak veri yalnızca yapılandırılmış ve yapılandırılmamış olarak değil bir üçüncü kategori olan yarı yapılandırılmış veri başlığı altında da konumlanabilir. Esasen tam yapılandırılmış formatlarda olduğu gibi bir modele bağlı çalışan ancak aynı zamanda yapılandırılmamış veri özellikleri de içeren yarı yapılandırılmış format veri içeriği ile şemayı[44] birleştirir. Günümüzde en yaygın şekilde kullanılan yarı yapılandırılmış format, insan tarafından okunabilen bir düz metin depolama biçimi olan *JavaScript Object Notation* (JSON)'dır.[45]. Bu açıklamalar ışığında GDPR m. 20 metninde geçen yapılandırılmış veri ifadesi teknik anlamda önceden belirlenmiş bir şemaya bağlı olarak çalışmayan, analiz etmeye hazır durumda olmayan veri dışında kalan verileri kapsar. Örneğin *Portable Document Format* (PDF) yapılandırılmış bir format değildir[46]. Madde metninde yalnızca

[42] **Open Data Handbook Glossary,** (https://opendatahandbook.org/glossary/en/terms/structured-data/, E. T.: 20.12.2021).
[43] **Buneman**, P.: *Semistructured Data*, ODS '97 Proceedings of the sixteenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems. ACM 1997, s. 117.
[44] Yarı yapılandırılmış verilerde, bir şema ile ilişkilendirilen bilgilerin, kendi kendini tanımlayan veriler içinde yer alabildiği ancak bazı yarı yapılandırılmış veri biçimlerinde ayrı bir şemanın olmadığı hakkında bkz. **Buneman**, s. 117.
[45] **Durner**, D./**Leis**, V./**Neumann**, T.: *JSON Tiles: Fast Analytics on Semi-Structured Data*, International Conference on Management of Data (SIGMOD'21), s. 445.
[46] **Swire/Lagos**, s. 345.

yapılandırılmış verilerden bahsedilmekte ise de yarı yapılandırılmış verilerin de madde kapsamına girdiğinin kabulü gerekir[47].

2. Yaygın Format ("*Commonly Used*")

Hakkın etkili biçimde kullanılabilmesini teminen ilgili kişiye alma hakkı kapsamında sunulan kişisel verilerin herkesçe kullanılabilen, özel bir teknik bilgi yahut cihaz gerektirmeyen bir formatta olması yerinde olacaktır. Doktrinde, "yaygın olarak kullanılan" ifadesinin genel bulut ("*public cloud*") adı verilen bir işletme, akademik veya bir devlet kuruluşu ya da bunların bir kombinasyonu tarafından sahip olunan, yönetilen, işletilen, genel halk tarafından açık kullanım için sağlanan bilgi işlem hizmetlerine atıf olarak kullanılmış olabileceği yönünde bir görüş bulunmaktadır[48]. Bununla birlikte farklı sektörel alanlarda, yaygın olarak kullanılan sistem ve formatlar farklılık gösterebilir[49]. Sektörel olarak yaygın biçimde kullanılan bir format yoksa veri sorumluları, ilgili kişinin söz konusu kişisel verileri yeniden kullanmasına elverişli açık formatlarla[50] ve metaverilerle kişisel veriyi sunmalıdır[51]. GDPR'da standart bir formatın öngörülmemesi ve çevrimiçi hizmetlerin tasarım özelliklerindeki farklılıklar da dikkate alındığında yaygın kullanılan formatın standart biçimde belirlenmemesi yerinde bir tercih olmuştur. Aksi halde standart formatı

---

[47] **Wong/Henderson,** s. 187.
[48] **Zanfir**, s. 157.
[49] **Bozdag**, E.: *Data Portability Under GDPR: Technical Challenges,* 2018, (http://dx.doi.org/10.2139/ssrn.3111866, E. T.: 25.12.2021), s. 5; **Graef**, I./**Husovec**, M./**van den Boom**, J.: *Spill-overs in data governance: the relationship between the GDPR's right to data portability and EU sector-specific data access regimes*, 2019, TILEC Discussion Paper No. DP 2019-005, s. 22.
[50] Avrupa Komisyonu, veri taşınabilirliğini talep hakkına ilişkin verdiği bir örnekte, Belçika'daki bir özel kliniğin hastasının, elektronik dosyalarda tutulan sağlık verilerinin Almanya'ya gönderilmesini talep etmesi halinde Belçikalı kliniğin ilgili kişiye ait kişisel verileri yaygın olarak kullanılan XML, JSON, CSV gibi bir açık format ile vermesi gerektiğini; veri formatı belirlenirken veri sorumlusunun, ilgili kişinin bu formattaki kişisel verileri yeniden kullanmasının mümkün olup olmadığını gözetmesi gerektiğini, bu anlamda ilgili kişiye ait kayıtların PDF formatında sağlanmasının yeniden kullanım için yeterli olmayabileceğini belirtmiştir. Bkz. (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_en, E. T.: 05.05.2022).
[51] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 18.

sağlayabilmek için tasarımların ve uygulamaların değiştirilmesi zorunluluğu[52] doğacaktır. Öte yandan hızla gelişen teknoloji, teknik anlamda katı kurallar benimsenmesini de anlamsız ve işlevsiz kılar. Bu sebepledir ki gerekli standart format üzerinde anlaşma veri sorumlularına bırakılmış, böylece sektörün gerektirdiği özellikler ve kullanılan uygulamalar dahilinde kişisel verilerin yeniden kullanılmasına elverişli format benimsenmesi ve birlikte çalışabilir ("*interoperable*") sistemler kurulması beklenmektedir. Ancak bu tercihin veri sorumlularına bırakılmış olması ortak bir karar alma sürecini güçleştireceğinden eleştirilmektedir. Sektörel düzenleyicilerin ivedi biçimde hakkın uygulanabilirliğini kolaylaştırmak adına bu eksiklikleri giderecek belirlemeleri yapması en makul çözüm olarak görünmektedir[53].

3. Makine Tarafından Okunabilirlik ("*Machine Readability*")

GDPR'ın 2012 yılında sunulan ilk taslak metninin veri taşınabilirliği hakkını düzenleyen 18. maddesinde "yapılandırılmış ve yaygın olarak kullanılan format" ölçütüne yer verilirken makine tarafından okunabilirlik ölçütü metnin daha sonra kabul edilen ve kesinleşen haline eklenmiştir.

Kamu sektörü bilgilerinin yeniden kullanımına ilişkin 2003/98/AK sayılı Direktifi değiştiren 26 Haziran 2013 tarihli Avrupa Parlamentosu ve Konseyinin 2013/37/AT sayılı Direktif'in 21 numaralı Gerekçe'sinde makine tarafından okunabilirlik tanımlanmıştır. Buna göre, "*Bir belge, yazılım uygulamalarının kolayca tanımlayabileceği, tanıyabileceği ve ondan belirli verileri çıkarabileceği şekilde yapılandırılmış bir dosya biçimindeyse, makine tarafından okunabilir bir biçimde*

[52] **Graef/Verschaleken/Valcke**, s. 57.

[53] **Turner/Quintero/Turner/Lis/Tanczer**, s. 2876; **Wong/Henderson**, s. 187-188. ***Wong*** ve ***Henderson*** ayrıca şu an için "yaygın format"ın, yeni teknolojiler benimseme zahmeti doğurmaksızın makine tarafından okunabilir olmasının teknik olarak mümkün olduğu format olarak anlaşılabileceğini belirtmektedirler.

olduğu kabul edilmelidir. Makine tarafından okunabilir formatta yapılandırılmış dosyalarda kodlanmış veriler, makine tarafından okunabilen verilerdir. Makine tarafından okunabilen formatlar açık veya tescilli olabilir; resmi standartlar olabilir veya olmayabilir. Otomatik işlemeyi sınırlayan bir dosya biçiminde kodlanmış belgeler, veriler onlardan çıkarılamadığı veya kolayca çıkarılamadığı için makine tarafından okunabilir bir formatta düşünülmemelidir. Üye Devletler, uygun olduğunda, açık, makine tarafından okunabilen biçimlerin kullanımını teşvik etmelidir"[54].

Makine tarafından okunabilirlik bir taraftan birlikte çalışabilirliği desteklerken diğer taraftan hakkın özellikle dijital pazarlarda daha yoğun biçimde uygulanabileceği şeklinde yorumlanabilir.

4. Engelsiz Olarak İletim ("*Without Hindrance*")

GDPR m. 20/1'de ilgili kişinin alma hakkı düzenlenirken kişisel verilerin sağlandığı veri sorumlusunun herhangi bir engellemesi olmaksızın bu verileri bir başka veri sorumlusuna iletme hakkı hüküm altına alınmıştır. Lakin madde metninde veya gerekçede engelsiz aktarıma ilişkin bir açıklama yapılmamıştır. Uygulama bakımından veri sorumlusunun uygun teknik altyapısının bulunmasına karşın talebi reddetmesi, hakkın uygulanabilirliğini sekteye uğratacak ölçüde kullanışsız veri formatları ile talebin kabul edilmesi, teknik gerekliliklerin bilinçli olarak sağlanmaması gibi sebepler ilgili kişinin veri taşınabilirliği hakkını kullanmasını örtülü bir yolla engelleyebilir. Tüm bu zorlukların aşıldığı varsayımında dahi veri güvenliğine ilişkin önlemler sebebiyle kişisel verilerin kolaylıkla bir başka veri

[54] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0037&from=FR, E. T.: 05.05.2022).

sorumlusuna iletilmesi mümkün olmayabilir[55]. Ancak bu son hali kişisel verilerin güvenliğinin sağlanması için genel bir zorunluluk olarak ele almak gerekir. Öyle ki bu halde makul güvenlik endişeleri, hakkın özünden beklenen faydayı kasıtlı olarak engelleyen davranışlardan ayrılmaktadır. Makul dengenin bulunmasında somut olayda dürüstlük kuralına uygun davranılıp davranılmadığının incelenmesi bir ölçüt olabilecektir. Her durumda, veri taşınabilirliğinin veri sorumlusunun herhangi bir engeli ile karşılaşmadan gerçekleşeceği öngörüldüğünden, ilgili kişinin veri taşınabilirliği hakkı kapsamındaki menfaatlerinin, hakkın icrasının veri sorumlusunun karşılaşabileceği yüklere üstün tutulduğu ileri sürülmektedir[56].

5. Metaveri ("Metadata")

Metaveri, bir veri setine ilişkin başlık, açıklama, tarih, yazar ve yayıncı, toplama yöntemi gibi kullanılabilirliğe yardımcı olacak verilerdir[57]. Daha sade bir ifade ile verinin verisinin çıkarılmasıdır. 29. Madde Çalışma Grubu, veri sorumlularının mümkün olan en iyi ayrıntı düzeyinde olabildiğince çok metaveri sağlanması gerektiğini, bu şekilde değiş tokuş edilen bilgilerin kesin anlamını koruyacağını ifade etmiştir[58]. Pratikte bunun anlamı, veri setinde bulunan veriler için en uygun formatın bulunabilmesini sağlayan üst bilgiye sahip olmak demektir. Örneğin, finansal veriler bakımından CSV, çevrimiçi topluluk verileri için JSON daha iyi bir format[59] olabilir. Dosya formatları tek başına makine tarafından okunabilir

---

[55] **Bozdag**, s. 5. İlgili kişinin veri sorumlusundaki tüm verilerini engel olmaksızın bir diğer veri sorumlusuna taşımanın, taşınabilirliğin yararlarından daha ağır basacak güvenlik riskleri oluşturabileceği yönünde bkz. **Swire/Lagos**, s. 366.

[56] **Van der Auwermeulen**, B.*: How to attribute the right to data portability in Europe: A comparative analysis of legislations,* Computer Law § Security Review 2017, Vol. 33, s. 68.

[57] **Open Data Handbook Glossary,** (https://opendatahandbook.org/glossary/en/terms/metadata/, E. T.: 20.12.2021).

[58] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 18.

[59] Yazarlar, araştırmaları neticesinde veri sorumlularından aldıkları yanıtları bu doğrultuda paylaşmışlardır, bkz. **Wong/Henderson**, s. 186.

nitelik taşısa da yeterli metaveri olmaksızın daha fazla içerik işlenemeyecektir[60]. Ayrıca ilgili kişinin bu haktan beklediği amacın sağlanmasını teminen kişisel verilerin bir veri sorumlusundan diğerine taşınması için gereken metaverilerin de madde kapsamına girdiğinin kabulü gerekir[61].

B. İşlenen Kişisel Verilerin Bir Veri Sorumlusundan Başka Bir Veri Sorumlusuna İletilmesini Talep Hakkı (Doğrudan Taşınabilirlik-*"Direct Portability"*)

Maddenin ikinci fıkrasında ikinci tür veri taşınabilirliği düzenlenmiştir. GDPR m. 20/2 ilgili kişinin veri taşınabilirliği hakkını kullanırken, teknik açıdan uygulanabilir olması halinde kişisel verilerinin bir veri sorumlusundan başka bir veri sorumlusuna ilettirme hakkı[62] bulunduğunu düzenlemektedir. Bu hakkın uygulanabilmesi için bir yazılımın başka bir yazılımın özelliklerini kullanabilmesi veya verileri doğrudan ağ üzerinden okuması için geliştirilen uygulama programlama arayüzü ("*application programming interface*"-API) kullanılabilir[63]. Veri taşınabilirliği talebinin ileri sürüldüğü veri sorumlusu gönderici veri sorumlusu, talep doğrultusunda kişisel verilerin iletildiği veri sorumlusu ise alıcı verici sorumlusu olarak nitelendirilebilir. Bu halde, m. 20/1 hükmünden farklı olarak ilgili kişi, gönderici veri sorumlusunda bulunan verilerini kendisi almamakta, dolayısıyla m. 20/1'deki köprü vazifesi de bulunmamaktadır. Kişisel verileri taşıma işlemi veri

[60] **Wong/Henderson**, s. 188.
[61] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 18; **Vanberg**, s. 12. Karş. Metaverilerin ve veri işleme algoritmalarının taşıma talebi kapsamına girmediği yönündeki karşıt görüş için bkz. **Picht**, P. G.: *Towards an Access Regime for Mobility Data*, IIC : International Review of Intellectual Property and Competition Law 2020, s. 951.
[62] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 5.
[63] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 5, 15; **Lynskey**, O.: *Article 20. Right to data portability*, The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020. Oxford Scholarship Online, 2021, s. 505.

sorumluları arasında gerçekleşmekte olduğundan veri taşınabilirliğinin bu türü doğrudan taşınabilirlik ("*direct portability*") olarak adlandırılmaktadır.

1. Teknik Açıdan Uygulanabilir Olma Kavramı ("*Technically Feasible*")

Teknik açıdan uygulanabilirlik kavramı doğrudan veri taşınabilirliği hakkının kullanılmasına ilişkin bir şart olarak öngörülmüştür. GDPR m. 20/2 hükmü uyarınca ilgili kişinin, kişisel verilerinin doğrudan bir veri sorumlusundan diğer veri sorumlusuna iletilmesini talep etmesi bunun teknik olarak uygulanabilir olmasına bağlanmıştır. Hükmün lafzi yorumundan, doğrudan veri taşınabilirliği hakkının kullanılmasına imkân verecek teknik altyapının kurulmasının veri sorumluları açısından bir zorunluluk olmadığı sonucuna varılabilir. Kişisel verilerin engelsiz olarak iletilmesi ifadesinden de teknik açıdan uygulanabilirliği bir zorunluluk olarak anlamak gerektiği sonucu çıkartılamaz. Bu bakımdan maddenin veri sorumlularına olumlu bir yükümlülük yüklemediği, gönderici veri sorumlusunun kişisel verileri iletimini teknik olarak engellememesini öngördüğü yorumu daha yerinde olacaktır[64]. Öte yandan hakka muhatap olabilecek veri sorumluları yönünden ölçek ayrımı yapılmamıştır. GDPR teknik açıdan elverişli sistemler kurmayı zorunlu tutmamışsa da aksi görüşün kabul edilmesi halinde küçük ölçekli bir veri sorumlusuna, doğrudan taşıma hakkını kullanmaya elverişli bir altyapı oluşturma yükümlülüğü getirilmesi gereksiz ve oransız birtakım maliyet artışlarına sebep olabilir[65]. Ne var ki birlikte çalışabilir sistemlerin kullanılmasının önerilmesinin, veri sorumlularına teknik uygulanabilirliği sağlama yükümlülüğü getirmemesi, veri sorumlularının hakkı

[64] Her ne kadar böyle bir yorum mümkünse de maddenin lafzından, ilgili kişinin kişisel verilerini kolayca dışa aktarma hedefini gerçekleştiren yazılımı sağlamak için kişisel verilerin sağlandığı veri sorumlusuna olumlu bir yükümlülük yüklendiği yönündeki görüş için bkz. **Swire/Lagos**, s. 345.
[65] **Swire/Lagos**, s. 351-352.

sağlamaktan kaçınması için bir araç olarak kullanılabilecek bir boşluk oluşturması dolayısıyla eleştirilmektedir[66].

Veri sorumlularından birisinin teknik altyapısı için uygulanabilir olan işlemin bir diğeri için uygulanabilir olmaması, teknik açıdan uygulanabilirliğin ne kapsamda ele alınması gerektiğine ilişkin soru işaretleri oluşturmaktadır. Her şeyden önce teknik açıdan uygulanabilirliğin doğrudan taşıma talebinin gerçekleştirilebilmesi için bir koşul olduğu dikkate alınmalı ve doğrudan taşıma hakkının tarafları nezdinde bir sonuca varılmalıdır. Doğrudan taşınabilirlik, talepte bulunmak dışında ilgili kişinin sürece aktif bir katkısının bulunmadığı bir kişisel veri iletim yöntemidir. Kişisel veri akışı gönderici veri sorumlusu ile alıcı veri sorumlusu arasında gerçekleşmektedir. Dolayısıyla gönderici veri sorumlusunun, işlemiş olduğu kişisel verileri karşı tarafa iletebileceği, alıcı veri sorumlusunun dışardan gelen bu kişisel verileri kabul edebileceği bir sisteminin bulunması; sistemler arasında iletişim ve veri güvenliği sağlanarak kişisel veri akışının gerçekleştiği bir yapının varlığı halinde doğrudan veri taşınabilirliği hakkı tam anlamıyla kullanılabilir.

2. Birlikte Çalışabilirlik ("*Interoperability*")

Veri taşınabilirliğini düzenleyen GDPR m. 20'de birlikte çalışabilirlik ifadesine açıkça yer verilmemekle beraber hakka ilişkin Gerekçe 68'de veri sorumlularının veri taşınabilirliğini sağlayacak birlikte çalışabilir formatlar geliştirmeye teşvik edilmesi gerektiği belirtilmiştir. Buna karşılık Gerekçe'de de birlikte çalışabilirliğin tanımına yer verilmemiştir. Avrupa kamu idareleri için birlikte çalışabilirlik çözümlerine ilişkin 16 Eylül 2009 tarih ve 922/2009/AK sayılı Avrupa

[66] **Graef/Verschaleken/Valcke**, s. 62. Yazarlar bu hususta, uygulama kapsamının, kilitlenme derecesinin yüksek olduğu sosyal ağlar gibi elektronik işleme sistemleriyle sınırlandırılabileceği önerisinde bulunmaktadır.

Parlamentosu ve Konseyi Kararı'nın "Tanımlar" başlıklı 2. maddesinde birlikte çalışabilirlik, "*farklı ve çeşitli kuruluşların karşılıklı yarar sağlayan ve üzerinde anlaşmaya varılan ortak hedefler doğrultusunda, kuruluşlar arasında bilgi ve bilgi birikimi paylaşımını içeren, destekledikleri iş süreçleri aracılığıyla ve kendi bilgi ve iletişim teknolojileri arasında veri alışverişi yoluyla etkileşim kurma yeteneği*"[67] olarak tanımlanmıştır. Avrupa Komisyonu "Sınırlar ve Güvenlik için Daha Güçlü ve Daha Akıllı Bilgi Sistemleri" düzenlemesinde ise birlikte çalışabilirlik, bilgi sistemlerinin veri alışverişi yapma ve bilgi paylaşımı sağlama yeteneği olarak tanımlanmıştır[68].

Gerekçe 68'de de belirtildiği ve 29. Madde Çalışma Grubu tarafından da değinildiği üzere ilgili kişinin kendisiyle ilgili kişisel verileri alma veya iletme hakkı, veri sorumlularının teknik olarak uyumlu işleme sistemlerini benimsemesi veya sürdürmesi yönünde bir yükümlülük oluşturmamaktadır[69]. Ancak sistemlerin birlikte çalışabilirliğinin sağlanması için kişisel verileri gönderici veri sorumlusundan dışa aktaracak ve alıcı veri sorumlusunun içe almasını sağlayacak[70] bir dışa aktarma-dahil etme modülünün ("*export-import modül*"-EIM) oluşturulması teknik bir gereklilik meydana getirmektedir[71]. Buna karşılık birlikte çalışabilirliğin bir zorunluluk olarak öngörülmemesi doktrin ve uygulama tarafından eleştirilmiş, birlikte çalışabilir ve teknik olarak uyumlu sistemlerin veri sorumlusunun inisiyatifi ile benimsenmesinin

[67] Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA), (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009D0922, E. T.: 05.05.2022).
[68] Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A205%3AFIN, E. T.: 05.05.2022).
[69] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 17.
[70] **Swire/Lagos**, s. 344.
[71] **Eskens**, S.: *A Right to reset your user profile and more: GDPR-rights for personalized news consumers*, International Data Privacy Law 2019, Vol. 9, No. 3, s. 171; **Unver**, s. 115.

hakkın uygulanmasında zorluklar çıkarabileceğine değinilmiştir[72]. Nitekim GDPR m. 20 öncesinde numara taşınabilirliğine ilişkin düzenlemeler kapsamında telekom sektöründe yaşanan deneyimlerin böyle bir zorunluluğu gerektirebileceğine vurgu yapılmaktadır[73].

Birlikte çalışabilirliğin iki türü bulunmaktadır. Yatay birlikte çalışabilirlik, kullanıcıların yararlandığı ürün ve hizmetler bakımından dijital hizmet sağlayıcıların rakipleri ile iletişim kurabilme yeteneğini ifade ederken dikey birlikte çalışabilirlik verileri, içeriği veya işlevleri birleştirebilme anlamına gelir[74]. Bu yönü ile yatay birlikte çalışabilirlik veri sorumlusunun sağladığı hizmetten yararlanan kişilerle bu hizmete dahil olmadan iletişim kurabilmektir. Dikey birlikte çalışabilirlik ise örneğin bir sosyal medya platformunun bir e-ticaret platformu ile kullanıcıların verilerini veya içeriği paylaşması suretiyle sorunsuz satın alımlar gerçekleştirmesini ve kullanıcının sosyal medya platformundaki bağlantılarının da aynı satın alma işlemini yapmasına izin vermektir[75]. Özellikle sosyal medya platformları için anlam taşıyan bu düşünce, belirli bir platformu kullanmakta olan kişinin, bir diğer platformdaki yakınları ile birlikte çalışabilir sistemler aracılığıyla mesajlaşabilmesi ve bu gibi işlemleri yaparken engelle karşılaşmamasını ifade eder. Ancak bu yolla gerçek rekabetin sağlanabileceği ve ilgili kişilerin kişisel verileri üzerinde tam kontrole sahip olabilecekleri düşünülmektedir[76]. Nitekim 2007 tarihinde *Microsoft*'un birlikte çalışabilirlik bilgilerini sağlamayı ve pazardaki diğer teşebbüslerce kullanımına izin vermeyi

[72] **Graef/Verschaleken/Valcke,** s. 63.
[73] **Eskens**, s. 171.
[74] **OECD**, *Data portability, interoperability and digital platform competition, OECD Competition Committee Discussion Paper*, 09.06.2021, (http://oe.cd/dpic, E. T.:06.05.2022), s. 12.
[75] **OECD**, *Data portability, interoperability and digital platform competition, OECD Competition Committee Discussion Paper*, s. 12.
[76] **Edwards**, L.: *Data Protection: Enter the General Data Protection Regulation* (May 21, 2018). Forthcoming in L Edwards ed Law, Policy and the Internet (Hart Publishing, 2018), s. 44; **Eskens**, s. 171.

reddetmesi Avrupa Komisyonu tarafından hakim durumunu kötüye kullanması olarak değerlendirilmiş, *Microsoft*'un cezaya karşı yaptığı temyiz başvurusu sonucunda Komisyon tarafından verilen ceza onanmıştır[77]. Görüleceği üzere birlikte çalışabilirlik bilgilerinin pazarda faaliyet gösteren rakiplere sunulmaması rekabet hukuku bakımından ihlal olarak değerlendirilebilmektedir. Birlikte çalışabilir altyapıların oluşturulması özellikle veri temelli pazarlarda hakim durumdaki teşebbüslerin ihlal niteliğindeki davranışlarını en aza indirmek bakımından bir gereklilik olarak ortaya çıkmaktadır. Avrupa Birliği'nin dijital pazarları düzenleme amacıyla hazırladığı yasa taslağı ile geçit bekçisi konumundaki platformların diğer yazılımlarla birlikte çalışabilmesini sağlamayı öngören düzenleme, söz konusu ihtiyacı karşılayabilecek bir mekanizma öngörmektedir[78].

Birlikte çalışabilirlik ve veri taşınabilirliği arasındaki ilişki bir parça-bütün ilişkisi olmanın çok daha ötesindedir. Doğrudan taşınabilirliğin sağlanması için birlikte çalışabilirlik gerekli şartlardan biri olsa da birlikte çalışabilirlik bir platformdaki kullanıcıların bir başka platformdaki kullanıcı ile aynı uygulamayı kullanmasına gerek kalmaksızın iletişime geçebilmesini sağlarken, taşınabilirlik bir platformdaki kişisel verilerin bir başka platforma taşınması ve bu bilgilerle yeni bir hesap açılabilmesi anlamına gelir[79].

Birlikte çalışabilirlik GDPR kapsamında bir zorunluluk olarak öngörülmemişse de büyük teknoloji şirketleri konunun kaçınılmaz bir ihtiyaca dönüştüğünün farkına varmış ve veri taşınabilirliğini sağlayacak teknolojik altyapının oluşturulması çabasına girmişlerdir. 2007 senesinde küçük bir grup mühendisin

[77] Case T-201/04, *Microsoft Corp. v Commission of the European Communities*, 17.10.2007, ECLI:T:2007:289.
[78] Bkz. Üçüncü Bölüm, §2, II.
[79] **Engels**, B.: *Data portability among online platforms*, Internet Policy Review 2016, Vol. 5(2), s. 4.

girişimi ile kullanıcıların çevrimiçi ortamdaki verilerini kolaylıkla başka platformlara iletebilmesini sağlamak üzere Veri Özgürlüğü Cephesi ("*Data Liberation Front*") başlamış, kısa bir süre sonra *Google* ve *Facebook* da bu girişime dahil olmuş; 2011'de *Google* elliden fazla ürününde kullanıcılara Verini İndir ("*Download Your Data*") seçeneği sunmaya başlamış[80] ve nihayet 2018 senesinde başlatılan Veri Transferi Projesi ("*Data Transfer Project*") ile açık kaynaklı ve hizmetten hizmete veri taşınabilirliği sağlayan bir platform[81] oluşturulmuştur. Bugün *Apple, Facebook, Google, Microsoft, Smugmug* ve *Twitter*'ın paydaşı olduğu bu girişim, birlikte çalışabilir sistemleri benimsemeye ve bu doğrultuda oluşacak kullanıcı taleplerini desteklemeye başlamıştır.

Avrupa Birliği'nde kişisel verilerin doğrudan akışını sağlayabilecek birlikte çalışabilir sistemlerin kurulması için Avrupa Birlikte Çalışabilirlik Çerçevesi ("*European Interoperability Framework*")[82] oluşturulmuştur. Bu hareket ile Avrupa'da dijital kamu hizmetlerinin nasıl kurulacağına ilişkin çalışmalar yapılmaktadır.

III. Veri Taşınabilirliği Hakkının Benzer Kavramlardan Ayırt Edilmesi

A. Kişisel Verilerin Üçüncü Kişilere Aktarılması ve Veri Taşınabilirliği

[80] Google tarafından başlatılan Proje'nin duyurusu için bkz. (https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html, E. T.: 06.05.2022).
[81] Projeye ait internet sayfası için bkz. (https://datatransferproject.dev/, E. T.: 06.05.2022).
[82] Ancak bu Avrupa Birliği'nde yapılan çalışmalardan yalnızca biridir. Birlikte çalışabilirliği sağlamak amacıyla atılan diğer adımlar için bkz. (https://joinup.ec.europa.eu/collection/interoperable-europe/initiatives, E. T.: 05.05.2022).

Kişisel verilerin üçüncü kişilere aktarılması ile alıcı veri sorumlusuna iletilmesi bahsinde ilk olarak alıcı ve üçüncü kişi kavramlarının birbirinden ayırt edilmesi gerekir. Alıcı ("*recipient*"), üçüncü bir kişi olup olmadığına bakılmaksızın kişisel verilerin paylaşıldığı kişi, organ veya makamdır[83]. Üçüncü kişi ("*third party*") ise ilgili kişi, veri sorumlusu, veri işleyenin doğrudan yetkisi altında olan, kişisel verileri işleme yetkisi bulunan kişiler dışındaki bir gerçek veya tüzel kişi, kamu kurum ve kuruluşudur[84]. Tanımlardan hareketle alıcı grubunun üçüncü kişilerden daha geniş olduğu sonucuna varılmaktadır. Alıcı ve üçüncü kişi arasındaki temel fark işlenmiş olan kişisel verinin açıklanmasının hukukiliği boyutunda kendini gösterir[85]. Örneğin veri sorumlusunun çalışanları, kişisel verinin işlendiği operasyonun bir parçası olarak görev yapmakta iseler başka bir hukuki gerekliliğin yerine getirilmesine gerek kalmaksızın kişisel verinin alıcısı haline gelebilirler[86]. Zira veri sorumlusunun yetkilendirmesi ile ilgili işi gerçekleştirmek için işleme faaliyetinde bulunmaktadırlar. Buna karşılık üçüncü kişi veri sorumlusundan veya veri işleyenden bağımsız olarak ve onun yetkilendirmesinden bağımsız bir hukuki gerekçeye dayalı olarak verinin ulaştırıldığı kişidir. Aynı örnek üzerinden devam etmek gerekirse, veri sorumlusunun ilgili işleme faaliyetinin bir parçası olarak görev yapmayan herhangi bir çalışanı verilerin paylaşılması yönünden üçüncü kişi konumunda olacaktır.

KVKK m. 8 uyarınca kişisel verilerin üçüncü kişilere aktarımı veri sorumlusunun iş stratejisi, depolama, işleme, saklama gibi ihtiyaçları doğrultusunda ilgili kişinin açık rızası veya diğer hukuki işleme sebeplerine dayalı olarak yurt içinde

[83] Veri Sorumluları Sicili Hakkında Yönetmelik m. 4/1-a; GDPR m. 4/9.
[84] GDPR m. 4/10.
[85] **Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights**: *Handbook on European data protection law: 2018 edition*, Publications Office 2018, s. 111.
[86] **Develioğlu**, s. 44.

ve m. 9 uyarınca gerekli şartların varlığı halinde yurt dışında; GDPR nezdinde yurt içinde aktarımın yanı sıra Birlik'e üye devletler arasında ve Birlik üyesi olmayan devletlerde bulunan başka bir veri işleyene[87] veya veri sorumlusuna kişisel verilerin iletilmesi anlamına gelir. Avrupa Birliği'nin dijital tek pazar oluşturma hedefi ekseninde şekillenen GDPR'da kişisel verilerin Birlik'e üye devletler içerisinde herhangi bir kısıtlama veya yasaklamaya maruz kalmadan dolaşabileceği "Konu ve Hedefler" başlıklı m. 1/3'te ifade edilmiştir. Söz konusu amaç, 108 sayılı Sözleşme'nin 14. maddesinde de belirtilmiş, yalnızca Sözleşme'nin ihlal edilmesine yol açacağı konusunda gerçek ve ciddi bir risk olduğu takdirde Sözleşme taraflarının birbiri içinde kişisel veri akışını engelleyebileceği hüküm altına alınmıştır. Gerek GDPR gerekse Sözleşme, taraf olmayan bir devlete veya uluslararası organizasyona kişisel verilerin aktarımı konusunda uygun koruma seviyesi sağlanmış ise aktarıma izin vermektedir. Kişisel verilerin aktarılmasının, GDPR m. 4/2 kapsamında bir veri işleme faaliyeti olduğu, işlemeye dayanak sebeplerin kısıtlanmamış olması dolayısıyla GDPR m. 6 ve m. 9'da öngörülen dayanaklarla yapılan işleme faaliyetinin hukuka uygun olduğu unutulmamalıdır. Özellikle doğrudan taşınabilirlik yönünden GDPR m. 20/2'nin lafzında geçen ilettirme ("*transmit*") ifadesi ile aktarımın ("*transfer*") ayırt edilmesi gerekir. Aktarımın da bir veri işleme faaliyeti olduğu ve veri taşınabilirliği

[87] GDPR m. 4/8 ve KVKK m. 3/1-ğ uyarınca kişisel verileri veri sorumlusu adına işleyen gerçek veya tüzel kişi, kamu kurum ve kuruluşu teknik anlamda veri işleyen ("*processor*") sıfatını taşımaktadır. GDPR n. 28/1'de ifade edildiği üzere veri işleyen konumundaki kişinin işleme faaliyeti veri sorumlusu ile arasındaki bir sözleşme ilişkisine dayanmaktadır. Veri işleyeni veri sorumlusundan ayıran en önemli nokta verilerin işlenme amaçlarını ve vasıtalarını belirleme yetkisinin bulunmamasıdır. Veri işleyen, işleme faaliyetini veri sorumlusundan aldığı yetki ve talimat çerçevesinde gerçekleştirmektedir. Bu bakımdan veri işleyenin, işlenen kişisel veriler üzerinde karar alma yetkisine sahip olması durumunda veri sorumlusu haline geleceği şüphesizdir. Veri sorumlusu ile veri işleyen arasındaki ayrım hukuki sorumluluklarının belirlenmesi yönünden önem taşır. Her ne kadar veri işleyen de kişisel verilerin korunması için gerekli hukuki, fiziki ve teknik tedbirleri almakla yükümlü ise de veri sorumlusunun verinin akıbetinin güvenceye alınması bakımından daha büyük bir sorumluluğu bulunmaktadır. Veri işleyen, veri sorumlusunun kendi çalışanı olabileceği gibi bir üçüncü kişi de olabilir. Öte yandan veri sorumlusunun kendi çalışanı olan bir kişinin veri işleyen olabilmesi için de bu kişinin, veri sorumlusunun organizasyonunun dışında olması gerekir.

kapsamında ilgili kişinin iletme ve ilettirme haklarının olduğu, bu kapsamda ilettirme kavramının aktarıma ilişkin genel kurallarla karıştırılabileceği dikkate alınarak GDPR metninde iki farklı terim kullanıldığı dikkat çekmektedir. Fakat ilgili kişinin, veri taşınabilirliği hakkı kapsamında veri sorumlusu tarafından işlenen kişisel verilerinin Birlik dışında bir devlete gönderilmesini talep edebilirliği hususuna dair belirsizlik söz konusudur[88]. Böylesi bir durumda GDPR Bölüm V'te düzenlenen hükümlerin uygulama alanı bulup bulamayacağı tartışılabilir.

Bir açıdan, veri sorumlularının bu türden bir taleple karşılaşmaları halinde, veri taşınabilirliği hakkının aktarıma ilişkin maddelere ve aktarıma ilişkin maddelerin de veri taşınabilirliği hakkına atıf yapmadığından bahisle GDPR'ın sistematiği içinde bunların beraber uygulanmayacağını ileri sürerek GDPR Bölüm V'teki prosedürden kaçınmaları söz konusu olabilir.

Diğer bir açıdan ise veri taşınabilirliği hakkı ilgili kişiye, maddedeki diğer gereklilikler sağlanmak koşuluyla, kendisine ait kişisel verileri alma ve bir başka veri sorumlusuna iletme veya işleyen veri sorumlusu tarafından doğrudan iletilmesini talep etme hakkı verir. GDPR m. 4/1 uyarınca ilgili kişi sıfatına sahip olan herkes, GDPR m. 3'te öngörülen bölgesel kapsam dahilinde veri taşınabilirliği hakkına sahiptir. Veri taşınabilirliği hakkının GDPR ile ilgili kişiye tanınan bir hak olduğu ve hakkın yer bakımından uygulanmasının GDPR m. 3'te ifadesini bulan mülkilik ilkesi esaslarına bağlı olduğu göz önüne alındığında alıcı veri sorumlusunun Birlik dışındaki bir devlette bulunması halinde üçüncü devletler veya uluslararası kuruluşlara kişisel veri aktarımı düzenleyen GDPR Bölüm V hükümlerinin uygulanması gerekir. GDPR Bölüm V'te yer alan hükümler aktarıma ilişkin genel kuralları düzenlemektedir.

[88] **Quinn**, P.: *Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?*, Global Jurist 2018, Vol. 18, No. 2, 18, 20180021, s. 8.

Nitekim kişisel verilerin aktarımı bir işleme faaliyeti olsa da ilgili kişinin hakkı aktarım değil, veri taşınabilirliğini talep hakkıdır.

B. Kişisel Verilere Erişim Hakkı ve Veri Taşınabilirliği

Veri taşınabilirliği hakkının ilgili kişiye tanıdığı alma hakkı, doktrinde GDPR m. 15'te düzenlenen kişisel verilere erişim hakkına benzetilmiştir[89]. Oysa veri taşınabilirliği hakkının ileri boyutta bir erişim hakkı sağladığı görüşünün doğru olmadığını, veri taşınabilirliği hakkının tamamen yeni ve farklı bir hak[90] olduğunu savunanlar da bulunmaktadır.

İlk bakışta GDPR m. 20/1'de sunulan alma hakkı, kişisel verilere erişim hakkına benzetilebilir. Kişisel verilere erişim hakkı, ilgili kişinin işlenen kişisel verileri ile ilgili işleme amacını, ilgili kişisel veri kategorilerini, bu veriler aktarılıyorsa alıcı gruplarını, işleme süresi ve ölçütlerini, düzeltme, sildirme ve itiraz etme hakkını, şikayet etme hakkını, otomatik karar alma mekanizmaları varsa bunlar tarafından yürütülen mantığı, yurt dışına aktarımlarda güvenlik hususunu öğrenme ve bu kişisel verilerinin bir nüshasını talep etme hakkını içerir. Ne var ki veri taşınabilirliği hakkı yalnızca ilgili kişinin kendisine ait kişisel verileri alma hakkını tanımakla kalmayıp alma hakkını mümkün kılan işleme gerekçesi, işleme yöntemi, kişisel verilerin sunulacağı format ve kişisel verilerin toplanma yolu bakımından sınırlamalar öngörmekte; kişisel verilerin ilgili kişi tarafından bir başka veri sorumlusuna iletilmesinde ilk veri sorumlusunun engellemesi ile karşılaşmasını bertaraf etmeyi hedeflemektedir. Görüleceği üzere veri taşınabilirliğinin gereklilikleri daha fazla ve

[89] GDPR Taslak çalışmalarında m. 18 ile öngörülen veri taşınabilirliği hakkı, 12 Mart 2014 tarihinde Avrupa Parlamentosu tarafından kabul edilen metinde ayrı bir hak olarak öngörülmemiş, m. 15'teki erişim hakkının bir parçası olarak ele alınmıştır. Veri taşınabilirliği hakkının GDPR m. 15'e eklenen hali içi bkz. (https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_EN.html, E. T.: 03.05.2022).

[90] **Swire/Lagos**, s. 371.

karmaşıktır. GDPR m. 20/2 ile tanınan doğrudan taşınabilirlik ise erişim hakkından açıkça farklılık göstermektedir[91].

Gerek erişim hakkı gerekse veri taşınabilirliği hakkı veri sorumlusuna söz konusu talepleri yanıtlamak için bir teknik altyapı oluşturma yükümlülüğü getirmez. Erişim hakkı ilgili kişiye işlenen kişisel verilerine ilişkin geniş çaplı bir bilgi edinme hakkı tanır. Veri taşınabilirliği hakkının ve bunun bir alt kolu olarak alma hakkının amacı ise ilgili kişiye bilgi sağlamak değil, dilediği veri sorumlusuyla özgürce ilişki kurabilmesini sağlamak, enformasyonel self determinasyon hakkı ile kişiliğin korunması ve geliştirilmesi hakkını güçlendirmek, veri sorumluları arasındaki rekabeti desteklemektir. Teorik olarak söz konusu iki hak arasında önemli amaçsal farklılıklar bulunmaktadır. Ancak uygulamada ilgili kişinin kişisel verilerini erişim hakkı kapsamında mı yoksa veri taşınabilirliği hakkı kapsamında mı talep ettiği veya bu talebin pratik sonuçlarının neler olduğu tartışılabilir. Hangi hakkın kullanılması gerektiği hususunda aşama aşama inceleme yapılarak bir sonuca varmak gerekir.

Öncelikle ilgili kişinin maksadı, işlenmiş olan kişisel verilerini veri sorumlusundan temin etmek ise ilk bakışta erişim hakkı ile veri taşınabilirliği kapsamında alma hakkı yarışan iki hak olarak görünmektedir. Bu anlamda erişim hakkı, alma hakkından daha geniş bir talep yelpazesi sunmaktadır çünkü alma hakkı yalnızca ilgili kişinin kendisi tarafından veri sorumlusuna sağlanan ve otomatik yollarla işlenen kişisel veriler için söz konusu olabilirken erişim hakkına konu kişisel

[91] İlgili kişi, banka ve üçüncü taraf sağlayıcı arasındaki ilişkide ödeme yapmak isteyen ilgili kişinin ödeme işlemlerini başlatmak için bankayı aracı tutması örneğindeki gibi gerçek zamanlı erişim gerektiren işlemlerde erişim hakkının; sosyal medya platformlarındaki adres kayıt defterinin başka bir platforma taşınması örneğindeki gibi üçüncü tarafların kendi hizmetlerini geliştirebilmek için ilk veri sorumlusunda bulunan kişisel verilerin bir kopyasına ihtiyaç duyduğu durumlarda veri taşınabilirliği hakkının kullanılmasının daha uygun olduğu yönünde bkz. **Graef/Husovec/van den Boom**, s. 18. Ayrıca yazarlar, veri taşınabilirliği hakkını, bir başka veri sorumlusuna kişisel veri iletilmesi bakımından daha büyük güvenlik tehlikeleri ile karşı karşıya görmektedir.

veriler ilgili kişi dışında biri tarafından sağlanmış olabilir[92] ve talep edilen verilerin otomatik yollarla tutulması gerekliliği bulunmamaktadır. Ancak bu ifadeden erişim hakkının içeriğinin daha geniş olması dolayısıyla "çoğun içinde azı da vardır" sonucu çıkarılmamalıdır. Veri taşınabilirliği hakkı, hakkın tanınma amacını gerçekleştirebilmek üzere erişim hakkının sağlamadığı birtakım zorunlulukları da beraberinde getirmiştir. Öyleyse ilk olarak, ilgili kişi kağıt ortamında tutulan kişisel verilerini temin etmek istiyorsa alma hakkını kullanamayacak, bu verilerin bir nüshasını GDPR m. 15/3 ve 15/4 uyarınca erişim hakkı dahilinde alabilecektir. Buna karşılık ilgili kişinin talep ettiği kişisel verileri veri sorumlusunca otomatik yollarla tutulmakta ise bu sefer işlenen kişisel verilerin ilgili kişi tarafından sağlanıp sağlanmadığı araştırılacaktır. İşlenen kişisel veriler ilgili kişiden başkası tarafından sağlanmışsa alma hakkı kullanılamayacak, hakka ilişkin diğer şartların mevcudiyeti halinde, erişim hakkı kullanılabilecektir. İşlenen kişisel veriler ilgili kişi tarafından sağlanmış ise hem erişim hakkı hem de veri taşınabilirliği hakkı kullanılabilecek durumdadır. Bir diğer ölçüt olarak işleme faaliyeti rıza veya sözleşme dışında bir hukuki gerekçeye dayanmakta ise alma hakkı kullanılamayacak; yalnızca bunlardan birine dayanıyorsa erişim hakkı da alma hakkı da söz konusu olabilecektir.

Bir sonraki aşamada amaç bakımından bir değerlendirme yapmak gerekir. Erişim hakkına ilişkin m. 15/3'te ilgili kişinin erişim talebini elektronik yollarla ileri sürmesi ve aksini talep etmemesi halinde bilgilerin yaygın kullanılan bir elektronik yolla sağlanacağı belirtilmektedir. Veri taşınabilirliği hakkında ise talebin hangi yolla ileri sürüldüğüne bakılmaksızın kişisel verilerin yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta sağlanması öngörülmektedir.

[92] Bu sebepledir ki GDPR m. 15/1-g'de kişisel verilerin ilgili kişiden elde edilmemesi halinde bu verilerin kaynağına ilişkin bilgi talep etme hakkı tanınmıştır.

Özellikle dijital platformlar, bulut bilişim sistemleri gibi veri sorumluları arasındaki geçiş ihtiyacı dikkate alınarak oluşturulan veri taşınabilirliği hakkı kapsamında veri sorumlusunun kişisel verileri ilgili kişiye sunacağı format daha katı biçimde öngörülmüştür. Hükümler arasındaki benzer ifade dolayısıyla ilgili kişilerin yanılgıya düşmesi olağandır. Bu sebeple ilgili kişi tarafından kullanılması talep edilen hakka yanıt vermeden önce her iki hakkın da kullanılabilir olduğu veri sorumlusunca anlaşılabiliyorsa, ilgili kişinin hakları yönünden aydınlatılması[93] gerekir. Her halükarda bu kapsamda yapılacak aydınlatmanın içerik yönünden amaca hizmet edecek açıklıkta ve bilgi düzeyinde olması gerekir[94]. Veri taşınabilirliğine ilişkin 2019 senesinde yapılan bir araştırma neticesinde araştırmaya dahil edilen 216 veri sorumlusundan 160 tanesinin gizlilik politikası hazırlamış olduğu, bunlardan yalnızca 63'ünün açıkça veri taşınabilirliği hakkına atıfta bulunduğu, bu 63 veri sorumlusunun 56'sının ilgili kişiye veri taşınabilirliği hakkı bulunduğunu ifade etmekle yetinip daha fazla açıklamada bulunmadığı görülmüştür[95]. Böylesi bir durumda ilgili kişiye gerekli bilgilendirmenin sağlandığı kabul edilemez.

İlgili kişinin erişim hakkı adı altında talep ettiği, kendisi tarafından sağlanan, sözleşmeye veya rızaya dayalı olarak otomatik yollarla işlenen ve veri sorumlusunun inisiyatifi ile yapılandırılmış, yaygın olarak kullanılan, makine tarafından okunabilir

[93] KVKK m. 10'da veri sorumluları için getirilen aydınlatma yükümlülüğü, GDPR m. 12'de ilgili kişinin bilgilendirilme hakkı olarak düzenlenmiştir. Türk hukukunda konu, ilgili kişinin talebi aranmaksızın veri sorumlusu tarafından yerine getirilmesi gereken bir yükümlülük olarak ele alınmıştır. Bu düzenlemeler ile maksat, ilgili kişilerin kişisel verilerinin hangi amaçla, kimler tarafından işlendiğini, işlemenin hukuki sebebini, kimlere aktarılabileceğini, sahip oldukları hakları bilmelerini sağlamaktır. Bu yolla ilgili kişiler, rıza verdikleri bir işleme faaliyetinin tam olarak neyi ihtiva ettiğini bilecek, rıza vermedikleri takdirde kişisel verilerinin hangi gerekçe ile işlendiğini anlayabilecek ve kişisel verileri üzerinde gerçek anlamda söz sahibi olabilecektir.

[94] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 13.

[95] **Turner/Quintero/Turner/Lis/Tanczer**, s. 2866-2867. Aynı çalışmada, veri sorumlularının GDPR m. 20/2'nin icrasıyla kendilerine sağlanacak kişisel verileri ne şekilde alacaklarına ilişkin açıklamada da yetersiz kaldığı görülmüştür.

formatta kendisine sunulan kişisel verilerini bir başka veri sorumlusuna iletmesi halinde, ilgili kişinin erişim hakkını kullanmak ve kişisel verilerini bir veri sorumlusuna vermek şeklinde nitelendirdiği aksiyonların bütünü GDPR m. 20/1 anlamında veri taşınabilirliği hakkını teşkil etmektedir.

Son olarak belirtmek gerekir ki kişisel verilerin kağıt ortamında tutulması gibi veri taşınabilirliği hakkının kullanılmasına engel teşkil eden bir durum mevcut ise erişim hakkını kullanan ilgili kişinin, kişisel verilerini bir diğer veri sorumlusuna iletme hakkı bakidir. Veri taşınabilirliğinde veri sorumlusunun herhangi bir engellemesi ile karşılaşmadan iletme hakkının kullanılabileceği ifade edilmiş olmakla beraber, erişim hakkının kullanılması ile elde edilen kişisel verinin başka bir veri sorumlusuna iletilmek istenmesi durumunda da veri sorumlusunun elektronik yolla sunduğu kişisel verileri kolaylıkla açılamayacak bir formatta vermesi gibi engel oluşturacak nitelikte davranışlardan kaçınması gerekir.

C. Kişisel Verilerin Silinmesini İsteme Hakkı (Unutulma Hakkı) ve Veri Taşınabilirliği

GDPR m. 20/3'te, dolaylı taşınabilirliğe ilişkin m. 20/1'de öngörülen hakkın kullanılmasının 17. maddede öngörülen unutulma hakkına halel getirmeyeceği belirtilmiştir. Unutulma hakkı kapsamında ilgili kişinin kendisiyle ilgili kişisel verilerin silinmesini talep etme ve veri sorumlusunun da bu talebi gecikmeksizin yerine getirme yükümlülüğü bulunur. Unutulma hakkının ileri sürülebileceği durumlara bakıldığında genellikle hukuki dayanaktan yoksun olarak yapılan işleme

faaliyetlerinin yer aldığı, buna paralel olarak hakka ilişkin istisnaların da GDPR m. 6 ile düzenlenen hukuki dayanaklar çerçevesinde belirlendiği görülmektedir[96].

Veri taşınabilirliği hakkının kullanılmasının unutulma hakkı ile ilişkisini incelerken hem hakkın kullanılma şartları boyutundan hem de başkalarının hak ve özgürlükleri boyutundan iki farklı değerlendirmede bulunmak gerekir. Öncelikle, veri taşınabilirliğinin şartları GDPR m. 20/1'de sayılmış; teknik açıdan uygulanabilir olması halinde bu hakkın bir veri sorumlusundan diğerine kişisel verilerin iletilmesini isteme şeklinde de kullanılabileceği m. 20/2'de belirtilmiştir. Görüleceği üzere hakkın kullanımı bakımından ilgili kişinin, ilk veri sorumlusunda bulunan kişisel verilerinin taşıma işleminden sonra otomatik olarak silinmesini gerektiren bir düzenleme bulunmamaktadır[97]. Buna karşın, ilgili kişinin veri sorumlusundaki kişisel verilerinin silinmesini talep etmesinin önünde de bir engel bulunmamaktadır. İlgili kişinin bir hizmeti başka bir veri sorumlusu hizmet sağlayıcıdan almak istemesi ve ilk veri sorumlusu ile ilişkisini sonlandırmasında olduğu gibi kişisel verilerin işlenmesinin gerekli olmadığı durumlar oluşabilir. Ancak taşıma talebi bundan başka bir amaca dayanabilir ve ilgili kişi ile ilk veri sorumlusu arasındaki ilişki devam edebilir ki bu durumda kişisel verilerin yalnızca taşıma talebi dolayısıyla silinmesi doğru olmayacaktır[98]. İlgili kişinin silme hakkını kullanması halinde veri taşınabilirliği silme işlemini geciktirmek veya reddetmek amacıyla kullanılamayacağı gibi kişisel verilerin taşınmış olması gönderici veri sorumlusunun bu verileri muhafaza edebileceği süreyi de etkilemez[99]. Açıklanan sebeplerle GDPR m. 20/3 ilgili kişinin hakları bakımından

[96] **Li,** W.: *A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation*, International Data Privacy Law 2018, Vol. 8, No. 4, s. 312.
[97] **Eskens**, s. 170; **Graef/Husovec/van den Boom**, s. 8.
[98] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 7.
[99] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 7.

yorumlandığında, her ne kadar veri taşınabilirliği hakkının kullanılması veri sorumlusundaki kişisel verilerin doğrudan silinmesini gerektirmese de ilgili kişinin talebi üzerine m. 17'de öngörülen unutulma hakkının icrası gerekir. Buna karşılık aksi durumda, önce kişisel verilerinin silinmesini talep eden ilgili kişinin artık veri taşınabilirliğini talep hakkı kalmayacaktır[100] çünkü silme işleminin gerçekleşmesinden sonra veri sorumlusu nezdinde tutulan bir kişisel veri de kalmayacaktır. Veri taşınabilirliği talebinin kişisel verilerin silinmesi talebi ile aynı anda ya da henüz silme işlemi gerçekleşmeden önce ve fakat silme talebi iletildikten sonra ileri sürülmesi halinde, henüz her iki talebin de karşılanabiliyor olması dolayısıyla ilgili kişinin talepleri güven teorisi[101] çerçevesinde kişisel verilerin önce taşınması ve ardından silinmesi talebi olarak değerlendirilmelidir.

İkinci açıdan ise veri taşınabilirliği talebi ile unutulma hakkı arasındaki ilişki esas olarak başkalarının hak ve özgürlükleri söz konusu olduğunda kendini gösterir. GDPR m. 20/3, veri taşınabilirliği hakkının m. 17'ye halel getirmeyeceğini belirtmiş ancak burada "üçüncü kişilerin 17. maddeye dayalı talepleri" vurgusu yapmamışken m. 20/4, veri taşınabilirliği hakkının başkalarının hak ve özgürlüklerini olumsuz etkilemeyeceğini düzenlemiştir[102]. Başkalarının hak ve özgürlükleri söz konusu

[100] Yine de hesap kapatma veya sözleşmenin feshi gibi durumlarda silme işleminden önce ilgili kişinin veri taşınabilirliği hakkıyla ilgili bilgilendirilmesinin uygun olduğu yönündeki değerlendirme için bkz. **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability,* s. 13.

[101] Güven teorisine göre bir kimsenin, karşı tarafa yönelmiş bir irade beyanında bulunduğu düşüncesini haklı olarak oluşturması halinde böyle bir davranış gerçekte söz konusu irade beyanının unsurlarını ve yöneldiği hukuki sonucu oluşturma arzusunu taşımasa dahi hukuki sonuç doğuracaktır. Doktrinde ve mahkeme içtihatlarında kabul edilen güven teorisine ilişkin açıklamalar için bkz. **Oğuzman**, M. K./**Öz**, M. T.: Borçlar Hukuku, Genel Hükümler, Cilt 1, Gözden Geçirilmiş 14. Bası, İstanbul 2016, s. 70. İrade beyanlarının yorumlanmasında kullanılan bu teori çerçevesinde bir kişinin iradesinin hangi sonuca yöneldiği makul ve orta zekalı bir kişinin olayın şartlarına göre bu irade beyanından ne anladığı araştırılarak belirlenir. Bkz. **Eren**, F.: Borçlar Hukuku Genel Hükümler, 22. Baskı, Ankara 2017, s. 155. Bu çerçevede, ilgili kişinin silme ve taşıma taleplerini bir arada ileri sürmesi halinde, her iki hakkın da kullanılmasına elverişli durumlarda güven teorisi çerçevesinde irade beyanının yorumlanması uygun olacaktır.

[102] **Li**, s. 312.

olduğunda ilgili kişinin kendisi ile ilgili kişisel verilerin silinmesini veri sorumlusundan isteyebileceğini öngören GDPR m. 17 kapsamında unutulma hakkının da bu kümeye dahil olduğu düşünüldüğünde veri taşınabilirliği hakkının, unutulma hakkına halel getirmeyeceğini düzenleyen m. 20/3 ve başkalarının hak ve özgürlüklerini olumsuz etkilemeyeceğini düzenleyen m. 20/4'te benzer görünen iki düzenleme bulunmaktadır. Doktrinde bu hususta, m. 20/3'ün tek bir ilgili kişi tarafından unutulma hakkı ve veri taşınabilirliği hakkının müşterek kullanımına ilişkin olduğu, m. 20/4'ün ise iki hakkın farklı ilgili kişiler tarafından çatışacak şekilde kullanılması ile ilgili olduğu ifade edilmiştir[103].

Bir başka yorumla m. 20/3'ün hem ilgili kişinin hem de üçüncü kişilerin unutulma hakkına veri taşınabilirliğine kıyasla üstünlük tanınması ve m. 20/4'teki olumsuz etkilenme ölçütü daha esnek yorumlanırken unutulma hakkının söz konusu olduğu her durumda katı biçimde unutulma hakkının ön plana alınması sonucunun çıkarılması da muhtemeldir. Buna karşılık bazı durumlarda üçüncü kişilerin unutulma hakkı ile veri taşınabilirliği hakkı arasındaki çatışma, ilgili veri setinden üçüncü kişilerin kişisel verilerinin ayıklanması gibi teknik yöntemlerle de çözülebilir. Öyleyse her iki hakkı da uygulama olanağı bulunduğunda m. 17'yi doğrudan üstün tutmak doğru bir yaklaşım olmayabilir.

Unutulma hakkı ile veri taşınabilirliği hakkını bir terazinin iki kefesine koyarak iki hakkın kullanımı arasındaki çatışmanın çözülebilmesi için erişim hakkı[104] ile ilgili kısıtlamaların dikkate alınması gerektiğini söyleyenler bulunmaktadır. Nitekim GDPR m. 15/4'in erişim hakkı kapsamında bir nüsha elde etme hakkının başkalarının hak ve

[103] **Li**, s. 312.
[104] **Cormack**, A.: *Is the Subject Access Right Now Too Great a Threat to Privacy*, European Data Protection Law Review 2 2016, s. 25-26.

özgürlüklerini olumsuz etkilememesi gerektiğini düzenlemesi dolayısıyla erişim hakkı, üçüncü kişilerin mahremiyetlerinin korunması hakkını ihlal etmemelidir[105]. Bu görüş uyarınca, unutulma hakkı ile veri taşınabilirliği hakkı arasında amaçsal bir karşılaştırma yapıldığında unutulma hakkı, doğrudan kişinin mahremiyetini korumakta[106], veri taşınabilirliği hakkı ise rekabeti güçlendirme amacı dolayısıyla ekonomik bir amaç taşımaktadır[107]. Mahremiyetin ekonomik amaçtan üstün tutulması gerekliliği, unutulma hakkını da veri taşınabilirliği hakkına kıyasla güçlendirmektedir. Bu görüşün eleştirilebilecek en önemli tarafı, veri taşınabilirliği hakkını rekabeti güçlendirme amacına indirgemesidir. Sistematik olarak düşünüldüğünde, kişisel verilerin korunması alanındaki bir düzenlemede salt rekabeti koruyucu ve güçlendirici bir amaçla ilgili kişiye hak tanınması makul görünmemektedir. Nitekim hakkın esas amacı ilgili kişinin kişisel verileri üzerindeki kontrolünü artırmaktır[108]. Bu sebeple amacı yalnızca rekabetin korunmasına indirgeyen bir değerlendirme de her durumda makul görünmemektedir. Menfaatlerin dengelenmesi için iki hakkı da beraber uygulayabilecek veya bunların birbirini olumsuz etkilemesini engelleyebilecek yöntemlerin bulunması halinde bu teknik çözümlere başvurulması, taşınacak kişisel verideki üçüncü kişiyi olumsuz etkileyici içeriğin çıkarılamaması, maskelenememesi veya teknik başka bir çözümün bulunmaması halinde unutulma hakkına üstünlük tanınması söz konusu olabilecektir. Bu sonuca yalnızca hakların amaçlarını baz alan

[105] Erişim hakkının ve veri taşınabilirliği hakkının mahremiyetin korunması hakkını ihlal ettiği yönünde bkz. **Cormack**, s. 25-26; **Li**, s. 316. Buna karşılık ***Li***, veri taşınabilirliği hakkının enformasyonel self determinasyon hakkını desteklemesi ve kişisel veriler üzerinde daha fazla kontrol imkânı tanıması ile yorumlanması güç bir karakter taşıdığını da kabul etmektedir. Bkz. **Li**, s. 316-317.

[106] Oysa GDPR m. 17 hükmünde hakkın öngörülüş biçimi incelendiğinde silinmesi talep edilen kişisel veri mahremiyeti ihlal ediyor olsun ya da olmasın hakkın kapsamında kalmaktadır. Bu sebeple unutulma hakkının saf biçimde mahremiyeti koruma amacına yöneldiği de söylenemez. Bkz. **Li**, s. 316.

[107] **Cormack**, s. 26.

[108] ***Li***, hakka hangi açıdan bakıldığında göre resmin değişeceğine işaret etmiş ve rekabete dayalı bir anlayışın hakkı güçsüzleştirebileceğini ancak insan haklarına dayalı anlayışın hakka daha fazla ağırlık kazandıracağını belirtmiştir. Bkz. **Li**, s. 317.

bir yaklaşımla ulaşmak pek uygun görünmemektedir. İlgili kişinin kendisi ile ilgili kişisel verileri sınırlı düzeyde ve daha zahmetli de olsa bir başka veri sorumlusuna verme hakkı her zaman bulunmaktadır. Oysa üçüncü kişinin unutulma hakkının pratik bir alternatifi bulunmamaktadır. Böyle bir durumda veri taşınabilirliği hakkında ısrarcı olunması her ne kadar hakkın amacını aşmamakta ise de başkaları için zarar doğurma ihtimali yüksek olduğundan hakkın kötüye kullanılması[109] teşkil edebilecektir. Öyleyse bu iki hakkın birbirine karşı konumunu genellemek yerine somut olayın özellikleri dikkate alınarak bir sonuca varmak daha yerinde bir çözüm sunacaktır.

[109] Avrupa Birliği hukukunda hakkın kötüye kullanılması hali ve etkileri için bkz. **Lenarts**, A.: *The General Principle of the Prohibition of Abuse of Rights: A Critical Position on Its Role in a Codified European Contract Law*, European Review of Private Law 2010, Vol. 18(6), s. 1121-1154.

İKİNCİ BÖLÜM

VERİ TAŞINABİLİRLİĞİ HAKKININ KAPSAMI VE KULLANILMASI

§ 3. VERİ TAŞINABİLİRLİĞİ HAKKININ KAPSAMI

I. VERİ TAŞINABİLİRLİĞİ HAKKININ YER BAKIMINDAN KAPSAMI

Veri taşınabilirliği hakkı GDPR'ın ilgili kişilere tanıdığı bir hak olduğundan hakkın yer bakımından uygulanabilirliği GDPR'ın uygulanabildiği coğrafyadan ayrı düşünülemez. Bu sebeple GDPR'ın uygulama alanı bulduğu noktalarda veri taşınabilirliği hakkı da ileri sürülebilecektir. GDPR m. 3'e göre işleme faaliyeti Birlik içinde gerçekleşsin ya da gerçekleşmesin Birlik içindeki bir veri sorumlusu ya da işleyenin faaliyetleri kapsamında kişisel verilerin işlenmesinde, ilgili kişinin Birlik içinde olmasına karşın işleme faaliyetini mal ve hizmet sunumuna veya davranışların Birlik içinde gerçekleştiği ölçüde davranışların izlenmesine dayandıran ve Birlik dışındaki veri sorumlusu ya da veri işleyenin kişisel veri işleme faaliyetinde veya Birlik içinde olmamasına rağmen Birlik'e üye bir devletin hukukunun uygulandığı yerde uygulanmaktadır.

II. VERİ TAŞINABİLİRLİĞİ HAKKININ KONU BAKIMINDAN KAPSAMI

A. İşleme Faaliyeti Yönünden

Bir kişisel verinin veri taşınabilirliği hakkının konusu olabilmesi için verinin işlenmesinin hukuki dayanağı ilgili kişinin açık rızasının bulunması ya da verinin bir sözleşmenin ifası amacıyla işlenmiş olmasıdır. Bunlar dışında herhangi bir gerekçe ile işlenmiş olan kişisel veri bakımından veri taşınabilirliği hakkının kullanılması söz konusu olmayacaktır. Ayrıca veri taşınabilirliği, veri sorumlusuna, kişisel verilerin

saklanacağı sürenin ötesinde bir muhafaza yükümlülüğü getirmediği gibi ilgili kişinin taleplerini karşılamak için kişisel veri işleme yükümlülüğü de yüklemez[110]. Dolayısıyla ilgili kişi tarafından alenileştirilen veya veri sorumlusunun meşru menfaati kapsamında işlenen kişisel veriler yönünden ilgili kişinin veri taşınabilirliği hakkına dayalı taleplerde bulunması mümkün değildir. Bu anlamda veri sorumlusunun, işlemiş olduğu kişisel veriyi hangi hukuki dayanakla işlediğinin doğru tespit edilmesi önem taşımaktadır.

Kişisel verinin hangi hukuki dayanakla işlendiğinin belirgin olması en başta verinin hukuka uygun olarak işlenip işlenmediğinin tespitini kolaylaştırır. Bir adım ileri gidildiğinde, hukuka uygun olarak işlenmiş kişisel verinin taşınması talep edildiğinde, veri sorumlusunun ilk olarak irdelemesi gereken hususun işlemenin hangi gerekçeye dayandığını belirlemek olduğu görülecektir. Bu belirleme kişisel verilerin işlendiği esnada işlemenin hukuki dayanağı esas alınarak açıkça anlaşılır gruplandırma yaptırmak şeklinde karşılanabileceği gibi veri sorumlusu her somut taşınabilirlik talebinde ilgili kişiye ait işlemiş olduğu kişisel verileri tek tek inceleyerek de talebe yanıt verebilir. Zaman ve kaynak kullanımı bakımından son derece maliyetli görünen bu gereklilik, veri sorumlusunun taşıma talebine uygun bir altyapı hazırlayabilmesi için bir zorunluluğa dönüşmektedir. Öyle ki veri sorumlusu, işlediği kişisel verilerden GDPR m. 20 lafzında yer alan rızaya veya sözleşmeye dayalı işlenmiş olanları ayıklayarak yalnızca bunların taşınması taleplerine, diğer şartların da karşılanması halinde, olumlu yanıt vermelidir. Böyle bir ayıklama yapılmaksızın veri sorumlusunun işlediği ve ilgili kişiye ait tüm kişisel verilerin doğrudan veya dolaylı taşınabilirlik yolu ile taşınması beraberinde pek çok sorunu getirebilecektir. İlk olarak, veri taşınabilirliği

[110] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 5.

hakkına ilişkin 29. Madde Çalışma Grubu tarafından da dile getirilen endişelerden biri kişisel verilerini alma hakkını kullanan ilgili kişinin veri güvenliği konusunda bilgilendirilmesi[111] gerekliliğidir. Çünkü kişisel verileri koruma hukuku bağlamında veri sorumlusuna veri güvenliğinin sağlanması için birtakım yükümlülükler getirilmişse de ilgili kişiler için bu türden bir güvenlik gerekliliği bulunmadığından şahsi olarak alınmış güvenlik önlemlerinin düşük seviyede olması halinde kişisel verinin karşılaşabileceği riskler mevcuttur[112]. İkinci olaraksa doğrudan taşınabilirlik yolu ile kişisel verilerin bir veri sorumlusundan diğer veri sorumlusuna aktarılması esnasında gönderici veri sorumlusunda bulunan tüm kişisel verilerin herhangi bir ayıklama işlemine tabi tutulmadan iletilmesi alıcı veri sorumlusunun gereğinden fazla veri işlemesine neden olabilecek ve bu yönü ile de amaçla bağlantılı, sınırlı ve ölçülü işleme (veri minimizasyonu) ilkesine ters düşecektir[113].

1. İşleme Faaliyetinin Rızaya Dayanması

İlgili kişinin rızası GDPR m. 4/11'de "*ilgili kişinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren, özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge*" olarak tanımlanmıştır. Bu anlamda, Türk hukukunda ifade edildiği şekliyle açık rıza ("*consent*"), belirli bir konuya ilişkin olarak yapılan bilgilendirme sonucunda, özgür iradeye dayalı olarak, birden fazla anlama gelmeyecek şekilde ve net olarak verilmiş olan rızayı ifade eder[114].Rıza, GDPR m. 6 ve m. 9 kapsamında kişisel verilerin işlenmesi için öngörülen

[111] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 19; **Bozdag**, s. 4.
[112] Kullanıcılarla veri taşınabilirliği hakkı üzerinde yapılan küçük çaplı bir araştırmada, kullanıcıların bir kısmının veri sorumlusundaki kişisel verilerini kendi cihazlarına indirmek yönünden güvenlik endişeleri yaşadıkları ve bu nedenle tercih edilebilir bulmadıkları dönütü alınmıştır. Araştırma dönütleri için bkz. **Karegar/Pulls/Fischer-Hübner**, s. 178.
[113] **Bozdag**, s. 4.
[114] 6698 sayılı KVKK m. 3/1-a; GDPR m. 4/11 ve m. 7. GDPR'da açık rıza ("*explicit consent*") ve rıza ("*consent*") kavramlarının her ikisine de yer verilmekle beraber yalnızca özel nitelikli kişisel verilerin

en önemli hukuka uygunluk sebeplerinden birini oluşturur. GDPR Gerekçe 42 uyarınca kişisel veri işleme faaliyetinin ilgili kişinin rızasına dayandığının ispatı veri sorumlusundadır.

İç hukukta rıza beyanının geçerliliğini etkileyen ehliyet gibi unsurların tam olup olmadığı ayrıca incelenmelidir. Keza rıza beyanını geçersiz bir durumun varlığı halinde kişisel verinin işlenmesi için verilmiş bir rızadan da söz edilemeyecektir. Ehliyet yönünden dikkate alınması gereken bir husus olarak GDPR m. 8'de bilgi toplumu hizmetlerine yönelik işleme faaliyetlerinde çocukların kişisel verilerinin rıza kapsamında işlenebilmesi, çocuğun en az 16 yaşında olmasına bağlanmıştır. Aynı maddede üye devletlere 13'ten aşağı olmamak üzere çocuklarda rızanın geçerliliği için 16'dan daha küçük bir yaş öngörebilme yetkisi de tanınmıştır. Çocukların kişisel verilerinin işlenmesinde, çocuğun söz konusu olgunluk ölçütünü karşılamaması durumunda rızanın geçerliliği çocuğun velayetini taşıyan kişinin rıza vermesine veya yetkilendirmesine bağlıdır[115].

Açık rızanın belirli bir konuya ilişkin olmasından anlaşılması gereken alınan rızanın tam olarak hangi konuda istendiğinin açıkça ortaya konmasıdır. Toptancı bir yaklaşımla "tüm verilerimin işlenmesini kabul ediyorum" şeklinde verilmiş bir rıza beyanı açık rızaya vücut vermeyeceği gibi rıza alınan işleme faaliyetlerinden başka yurt dışına aktarım gibi ikincil işleme faaliyetlerinin ortaya çıktığı durumda veya işleme amaçlarında değişiklik olması halinde ayrıca açık rıza alınması gerekir. Böyle bir belirliliğin sağlanabilmesi içinse ilgili kişi tarafından verilen rızanın ne için istendiği ve sonuçları bakımından veri sorumlusu tarafından bilgilendirmede

işlenmesinde açık rıza aranmaktadır. Buna karşılık KVKK'da kural olarak her tür verinin işlenmesinde açık rıza aranmaktadır.

[115] **Develioğlu**, s. 54.

bulunulması gerekmektedir. Elbette bu bilgilendirmenin rızanın verilmesinden önce veya en geç o anda yapılmış olması, açık, anlaşılır biçimde gerçekleştirilmesi gerekmektedir. Son olarak, ilgili kişi tarafından verilecek rızanın özgür iradeye dayalı olması gerekir ki bu da davranışının bilincinde olan makul bir bireyin irade sakatlığı halleri veya ehliyetsizlik gibi geçersizlik sebepleri bulunmaksızın rıza vermiş olması ve gerçek anlamda seçim hakkının[116] bulunması anlamına gelir.

Tarafların eşit müzakere gücünde olmadığı durumlarda veya hizmetin açık rıza şartına bağlandığı durumlarda da iradenin özgür olup olmadığının somut olayın koşulları içinde değerlendirilmesi gerekmektedir. Öyle ki rızanın özgür iradeye dayalı olması taraflar arasında güç dengesizliğinin bulunmamasını, rıza vermeyi reddetme hakkının açıkça tanınmış olmasını; spesifik olması işleme amacına uygun ve bununla sınırlı olmasını; bilinçli olması veri sorumlusu tarafından gerekli bilgilendirmenin yapılmış olmasını ve açık gösterge ise rızanın başka bir anlama gelmeyecek şekilde verilmiş olmasını ifade eder[117]. Kişisel verileri koruma hukuku bağlamında enformasyonel self determinasyon hakkının kullanılabilmesi ancak bu şartların sağlanmış olmasına bağlıdır.

Kişisel veri bu şartlar çerçevesinde rızaya dayanarak işlenmekte ise işleme faaliyeti yönünden veri taşınabilirliği hakkının kapsamına girmektedir.

2. İşleme Faaliyetinin Sözleşmeye Dayanması

İşlenen kişisel verinin işleme faaliyeti yönünden veri taşınabilirliği hakkının kapsamına girmesi için rıza dışındaki diğer seçenek işlemenin GDPR m. 6/1-b'de öngörülen "*ilgili kişinin taraf olduğu bir sözleşmenin ifası veya bir sözleşme yapılmadan önce ilgili kişinin talebiyle adımlar atılması için*" yapılmasıdır. Sözleşme

[116] **Çekin**, s. 91.
[117] **Develioğlu**, s. 52-57.

görüşmeleri sırasında bu dayanakla elde edilen kişisel verilerin, işlemenin genel ilkelerine bağlı olarak tutulması, görüşmeler sözleşmenin kurulması ile sonlanmamışsa gecikmeksizin işlenen verilerin imha edilmesi gerekir[118].

GDPR m. 6 veya m. 9'da öngörülmüş olsa dahi rıza ve sözleşme dışındaki sebeplere dayalı işleme faaliyeti, söz konusu kişisel veriler için veri taşınabilirliği hakkının kullanılmasına engeldir. Gerekçe 68'de ve 29. Madde Çalışma Grubu tarafından hazırlanan Rehber'de neden yalnızca bu iki işleme sebebinin madde kapsamına alındığına dair bir açıklama yapılmamıştır. Buna karşın bu tercihin sebebi, açık rıza veya sözleşmeye dayalı işleme faaliyeti dışındaki kişisel veri işleme sebeplerinin korumayı güttüğü menfaatlerin hukuki bir yükümlülüğün yerine getirilmesi, kişilerin üstün yararının korunması, kamu yararı için gerçekleştirilen bir görevin icrası veya meşru menfaatler gibi sebepler olması dolayısıyla ilgili kişilerin kişisel verileri üzerindeki kontrollerinin artırılması bakımından ekonomik amaçlı işleme faaliyetlerinden ayrılması olabilir. Öyle ki GDPR, ilgili kişilerin kişisel verileri üzerinde daha fazla söz sahibi olmasını amaçlarken veri taşınabilirliği hakkını, veri sorumluları bünyesinde kilitli kalmalarını önleyecek bir mekanizma olarak öngörmektedir. Söz konusu diğer işleme sebeplerinde kilitlenme hali bakımından dikkate alınmaya değer ekonomik menfaatler açık rıza ve sözleşmeye dayalı işlemelere kıyasla çok daha zayıftır ya da hiç bulunmamaktadır. Dolayısıyla diğer işleme sebeplerinde ekonomik menfaatleri dengelemeyi amaçlayan rekabet hukuku yönünden ciddi bir tehlike görünmemektedir. Tüm bu hallerde işlenen kişisel verilerin rıza ile işlenmesi de mümkündür ancak rızanın olmadığı durumlarda bu gerekçelerle kişisel verinin işlenebilmesi, ekonomik kaygısı son derece düşük olan sağlık, yasal

[118] **Develioğlu**, s. 61.

yükümlülükler, kamu yararı gibi kavramlara bağlanmıştır. Özellikle bir sözleşmenin tarafı olmak veya rıza göstermenin ilgili kişinin iradesine bağlı olduğu dikkate alındığında veri taşınabilirliği hakkının yalnızca bu işleme sebepleri ile sınırlandırılması anlaşılabilir. Diğer taraftan, veri taşınabilirliği hakkının açık rızaya ve sözleşmeye dayalı işleme sebepleri ile işlenen kişisel verilerle sınırlı tutulması, ilgili kişi tarafından veri sorumlusuna sağlanmaksızın, veri sorumlusunun kendi teknolojisi ve yapabilme bilgisi (*"know-how"*) sayesinde elde ettiği bilgi ve çıkarımların korunması olarak değerlendirilebilir.

B. İşlenen Kişisel Veriler Yönünden

1. İlgili Kişiye İlişkin Kişisel Verilerin Bulunması

Veri taşınabilirliği hakkının ilgili kişiye, kişisel verilerinin korunması hakkı bağlamında tanınmış bir hak olduğu düşünüldüğünde GDPR m. 20 ile getirilen düzenlemenin yalnızca kişisel verileri kapsadığını kabul etmek gerekir[119]. Öyle ki veri kümesi kişisel veri kümesinden çok daha geniştir. Kişisel veri ise bu veri kümesi içinde kişiyi belirli veya belirlenebilir kılan verileri ifade eder[120]. Bu bakımdan anonim hale

[119] Avrupa Komisyonu'nun 25 Ocak 2012 tarihinde görüşmeye açtığı GDPR taslağının (GDPR Taslağı) veri taşınabilirliği hakkını düzenleyen 18. maddesinde ilgili kişi tarafından veri sorumlusuna sağlanan kendisiyle ilgili kişisel verilerin ve diğer bilgilerin ("…*personal data and any other information provided by the data subject*…") bir veri sorumlusundan diğerine taşınması öngörülmüş olup kişisel veri dışındaki bilgilerin aktarımına yönelik ifade haklı olarak eleştirilmiş ve 2016'da kabul edilen GDPR metninde diğer bilgiler ifadesine yer verilmemiştir. Hakikaten de kişisel verilerin korunması alanında getirilen bir düzenlemede kişisel verileri aşacak ölçüde, tüm veriler yönünden bir yükümlülük getirmek isabetli görünmemektedir.

[120] Bu anlamda verinin içerik, amaç veya sonuç yönünden "kimliği belirli veya belirlenebilir bir kişiye ilişkin" *("related to")* olup olmadığının ortaya konması gerekmektedir. Kişinin belirli olması mevcut verilerin makul vasıtalar kullanılarak gerçek kişiyle ilişkilendirilmesi suretiyle o kişinin doğrudan doğruya tanımlanabilir hale gelmesini, bir diğer ifade ile ayırt edilmiş olmasını ifade etmektedir. Belirlenebilir olmak ise mevcut verilerin, bir kişiyi doğrudan doğruya ve ayırt edilmiş şekilde belirlemeye elverişli olmasa da yardımcı vasıtalar ile bu sonucu doğurabilecek durumda olması anlamına gelir. Verinin kişiye ilişkin olup olmadığı telefon numarası, kimlik numarası gibi bazı veri kategorileri için kolaylıkla ve açıkça görülebilirken, IP adresi gibi bazı veriler bakımından bu tespiti yapmak her zaman kolay olmamaktadır. Bir kişiye ilişkin olmayıp kişi ile yakın bir ilişki içinde bulunan nesnelere ait verilerin de kişiye ait veriler gibi kabul edilmesi, bu yakın ilişkinin, nesneye ait verilerin her durumda kişiye ait hale getirmesinden kaynaklanmaktadır. Araç plakalarının veya IP adreslerinin kişisel veri kabul edilmesinin sebebi budur. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün gerekçesinde ise veriyi elinde bulunduranın tek başına bu verilerle verinin ilişkili olduğu kişiyi tespit

getirilmiş verinin "kişisel" niteliği bulunmadığından anonim veriler nezdinde veri taşınabilirliği hakkının kullanılması da mümkün olamayacaktır[121]. Buna karşılık verinin ancak ek bilgi yardımıyla belirli veya belirlenebilir bir kişi ile ilişkilendirilmesini sağlayan takma adlaştırma yöntemi verinin "kişisel" olma niteliğini ortadan kaldırmadığından bu kapsamda işlenmiş olan veri için hakkın kullanılması söz konusu olabilecektir.[122]

Hakka konu olabilecek kişisel veriler yalnızca veri taşınabilirliği talebini ileri süren kişinin kendisi ile ilgili kişisel verilerdir. Bir başkasına ait kişisel veriler üzerinde hakkın icra edilmesi söz konusu değildir. İlgili kişinin kendisi ile ilgili kişisel verilerin bulunduğu bir veri setinde, örneğin sosyal medyadaki fotoğraflarında, üçüncü kişilerin de kişisel verilerinin bulunması halinde hakkın ileri sürülüp sürülemeyeceği ise tartışmalıdır[123].

2. Verilerin İlgili Kişi Tarafından Sağlanması

GDPR m. 20 kapsamında veri, ilgili kişinin verileri bizzat verme gibi aktif bir davranışı ile kendisi tarafından sağlanabileceği gibi ilgili kişinin bir hizmet veya servisin kullanması yolu ile veri sorumlusuna sağladığı arama geçmişi, trafik kayıtları

---

edebiliyor olmasının zorunlu olmadığı ifade edilmektedir. Bu bakımdan GDPR'ın, mevcut verinin üçüncü bir kişi elindeki herhangi bir veri ile birleştirilmesi sonucunda verinin bir kişi ile ilişkilendirilmesinin mümkün olup olmadığı değerlendirilmelidir. Detaylı açıklamalar için bkz. **Aksoy**, H. C.: Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010, s. 24, 28-29; **Article 29 Data Protection Working Party,** *Opinion 4/2007 on the Consept of Personal Data*, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, E. T.: 03.05.2022), s. 12; 83-89; **Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights**, s. 88; **Çekin**, s. 45.

[121] İlgili kişinin, kişisel verilerin anonim hale getirilmesinden önce veri taşınabilirliği talebinde bulunması halinde herhangi bir sorun oluşmayacaktır ancak anonim hale getirme işleminden sonra bu talep ileri sürüldüğünde, belirli bir veri sorumlusunun sağladığı hizmet veya ürün içerisinde kilitli kalma ("*lock-in*") hali gündeme gelecektir. Bu bakımdan veri taşınabilirliği elverişsiz olacağı, bireyin mahremiyetinin korunduğu ölçüde veri taşınabilirliği hakkının amaçsız kalacağı ve bu durumun, hakkın niçin kişisel verilerin korunması hukuku kapsamında düzenlenmiş olduğunu açıkladığı hakkında bkz. **Zanfir**, s. 159.

[122] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 9.

[123] Bkz. Birinci Bölüm, §2, III, C ve İkinci Bölüm, §1, III, C, 1.

gibi veri sorumlusu tarafından gözlenen veriler ile de sağlanmış olabilir. Verinin ilgili kişi tarafından aktif veya pasif yolla sağlanmasının yanında hakkın kapsamında kalan verinin ne tür bir veri olduğunun da belirlenmesi gerekir. Bu çerçevede veriler ham, gözlenen veriler ("*observed data*"), türetilmiş veriler ("*derived data*") ve çıkarsanan veriler ("*inferred data*") olarak gruplandırılabilir. Bir verinin bu türlerden hangisine tabi olduğunun tespiti her zaman kolay olmamaktadır. GDPR'da da konuyla ilgili ayrıma yer verilmediği dikkat çekmektedir. Öte yandan 29. Madde Çalışma Grubu Veri Taşınabilirliği Hakkı Rehberi'nde hakkın kapsamına yalnızca gözlenen verilerin girdiğini belirtmekte, türetilmiş veya çıkarsanan verilerin taşınabilir olmadığına vurgu yapmaktadır. Bu anlamda bir hizmet sağlayıcı veri sorumlusu tarafından çevrimiçi itibar değerlendirmesi[124] gibi istatistiki ve analitik amaçlarla[125] oluşturulan verilerin taşıma talebine konu olup olamayacağı konusunda madde hükmünde açıklık bulunmamaktadır[126]. Bu hususta, alıcı/satıcı puanlaması gibi uygulamalarla oluşan veri gözlenen/ham veri kabul edilebilecek ve bu şekilde taşınabilecekken veri sorumlusunun bu veriyi tekrar değerlendirerek eriştiği puan ortalaması verisi artık ham bir veri sayılmayacak ve taşıma talebine konu olamayacaktır[127]. Kişisel verilerin ilgili

[124] Alıcı veya satıcı puanlamalarına ilişkin geri bildirim veri sorumlusu tarafından sağlansa da ilgili kişinin veri sorumlusunda bulunan kişisel verilerini bir başka veri sorumlusuna taşıma talebi doğrultusunda, çevrimiçi itibarına ilişkin bu verilerin talebe konu olabileceği yönünde bkz. **Graef/Verschaleken/Valcke**, s. 56; **Ursic**, s. 65-66; **Vanberg**, s. 11-12. Çevrimiçi itibara ilişkin detaylı bir inceleme bu çalışmanın kapsamını aşmakta olduğundan platform ekonomileri, blokzincir ve Kişisel Bilgi Yönetim Sistemi (*Personal Information Management Systems*-PIMS) üzerinden daha geniş bir inceleme için bkz. **Hesse**, M./**Teubner**, T.: *Reputation portability – quo vadis?*, 2019, Electronic Markets, Springer;IIM University of St. Gallen, Vol. 30(2), s. 331-349. Ayrıca çevrimiçi itibarın önemli unsurlarından olan kullanıcı görüşlerinin telif haklarına konu olup olamayacağının da değerlendirilmesi gerekir. Her türlü kullanıcı görüşünün telif hakkı içerdiği söylenemez. Kullanıcı yorumları üzerindeki mülkiyetin platform işleticisine mi yoksa yorum sahibine mi ait olduğu hususunu irdeleyerek GDPR'ın mevcut veri taşınabilirliği düzenlemesinin kullanıcı yorumlarının taşınabilirliğine izin vermediği yönündeki açıklamalar için bkz. **Kathuria**, V./**Lai**, J. C.: *User Review Portability: Why and How?*, Computer Law & Security Review 2018, Vol. 34, s. 1298-1299.

[125] İstatistiki ve analitik amaçlarla toplanan kişisel verilerin veri taşınabilirliği hakkının kapsamına girmediği yönünde bkz. **Graef/Verschaleken/Valcke**, s. 56.

[126] **Graef/Verschaleken/Valcke**, s. 56.

[127] **Vanberg**, s. 12.

kişi tarafından sağlanması gerekliliğinin, ilgili kişinin tüm kişisel verileri üzerinde söz sahibi olmasını engellediğinden bahisle enformasyonel self determinasyon hakkını güçlendirmek bakımından yetersiz olduğu, madde kapsamında kişisel verileri alma hakkının enformasyonel self determinasyonu yalnızca bir ölçüde garanti ettiği[128] ve kullanıcıya özgü içerik kişiselleştirmesinin çıkarsanan veriler temelinde gerçekleştirilmesi dolayısıyla veri taşınabilirliği hakkının sistem odaklı kişiselleştirme için faydalı olmayıp yalnızca kullanıcı odaklı kişiselleştirmede etki kazanabileceği[129] yönünde eleştiriler bulunmaktadır.

a. Türetilmiş Veriler ("*Derived Data*")

Türetilmiş veriler, diğer verilerin basit akıl yürütme veya matematiksel olarak işlenmesi ile oluşan, tahmin oluşturma amacıyla kullanılabilen ancak çıkarsanan verilerdeki gibi olasılığa dayalı akıl yürütmeye dayalı olmayan, mekanik işleme verileridir[130]. Örneğin, bir işletmenin satış yaparak gelir elde etmesi için ortaya çıkan maliyetler ile elde ettiği gelir arasındaki farkın hesaplanması yoluyla bulunan müşteri karlılığı verisi[131], matematiksel hesaplamaya dayalı olarak tespit edilen bir veridir. Bulunan değer işletmenin sonraki dönemlerde elde edeceği müşteri karlılığını tahmin etmek için kullanılabilir.

b. Çıkarsanan Veriler ("*Inferred Data*")

[128] **Fialova**, E.: *Data Portability and Informational Self-Determination*, Masaryk University Journal of Law and Technology 2014, Vol. 8, No. 1, s. 50.
[129] **Eskens**, s. 171.
[130] **OECD**, *Summary of the Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21.03.2014, (https://one.oecd.org/document/DSTI/ICCP/REG(2014)3/en/pdf, E. T.: 06.05.2022), s. 5.
[131] **OECD**, *Summary of the Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, s. 5.

Çıkarsanan veriler, bireyleri sınıflandırmak için olasılığa dayalı, davranış tahminleri oluşturmaya yönelik olarak yürütülen analitik süreçlerin ürünüdür[132]. İlgili kişinin aktif veya pasif bir davranışla sağlamış olduğu veriden çeşitli yollarla yeni bir veri üretilebilmektedir. Örneğin, ilgili kişinin konum bilgilerinin veri sorumlusuna ait bir algoritma ile incelenmesi sonrasında kişinin ev veya iş adresinin belirlenmesine yönelik bir veri elde edilebilir. Oysa ilgili kişi veri sorumlusuna bu bilgiyi aktif olarak sağlamamış ve hatta veri sorumlusunun verdiği hizmeti kullanmak suretiyle de bu verinin üretilmesine neden olmamıştır. Konum bilgileri, belirli konumların ziyaret edilme sıklığı, bu konumlarda bulunulan saatler veya geçirilen süre gibi bilgiler bir araya getirilerek kişinin ev veya iş adresini gösteren[133] yeni bir veri üretilmiştir. Dolayısıyla bu süreçte veri sorumlusu ham veriyi almış, onu işlemiş ve yeni bir veri üretmiştir.[134] Benzer şekilde, kredi puanlaması, sağlık verilerine dayalı olarak çıkarsanan yaşam beklentisi puanı gibi istatistiki veriler[135] ve gelecekte karşılaşılması beklenen hastalıklara ilişkin gelişmiş analitik veriler[136] çıkarsanan veri grubundadır.

c. Gözlenen Veriler ("*Observed Data*")

---

[132] **Krämer**, J.: *Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations,* Journal of Competition Law & Economics 2020, Vol. 17(2), s. 266; **OECD**, *Summary of the Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, s. 5.

[133] Verinin doğru olup olmadığının kişisel veri olma niteliği yönünden önemi olmadığı hakkında bkz. **Aksoy**, s. 14. Günümüz teknolojisi akıllı telefonlar ve dijital cihazlar arasında kurulan bağlantılar ile bu tür veriler elde etmeyi olağan hale getirmiştir. Akıllı telefonların şahsi araçların kullanımı esnasında bu araçlarla bağlantısının kurulması halinde, akıllı telefona adres bilgisi kaydedilmemiş olsa dahi ziyaret sıklığı ve geçirilen süre gibi hususlar algoritmalar vasıtasıyla incelenmekte ve konum servislerinin açık olması durumunda araç ile telefon arasındaki bağlantı ev olarak tanımladığı adrese giden yolun ne kadar süreceğini tespit edip bildirim gönderebilmektedir. Aynı durum aracın konumunun tespit edilmesinde de söz konusu olur ve telefon aracın park halinde olduğu bilgisine bu yolla erişir. Akıllı telefonda ev olarak tanımlanan adresin kişinin ikamet adresi olması zorunluluğu bulunmamaktadır. Söz konusu adres konum bilgilerinin veri sorumlusunun algoritması ile düzenli ziyaretten ötürü tespit edilen herhangi bir yer olsa da verinin kişisel veri olma niteliği mevcuttur.

[134] 29. Madde Çalışma Grubu da bu hususta, veri taşınabilirliği hakkı kapsamında kalan verinin, ilgili kişinin davranışının gözlemlenmesinden kaynaklanmakla beraber bu davranışın bir sonraki analizini içermeyen veri olduğu görüşündedir.

[135] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 10.

[136] **OECD**, *Summary of the Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, s. 5.

Gözlenen veriler, veri işleme sürecinin ham materyalini ifade eder. Gözlenen veriler, diğer verilerin başkaları tarafından gözlenmesi ve dijital formatta kaydedilmesi ile elde edilen, oluşum aşamasında veya daha sonra iletilebilen, çevrimiçi çerez verileri, yüz tanıma ile birleştirilmiş CCTV kameraları tarafından yakalanan veriler gibi verileri ifade eder[137]. Örneğin, bir kişinin konum bilgileri bir GPS hizmetinin kullanılması yoluyla ilgili kişi tarafından pasif olarak sağlanmış olan veriler olabilir. Bu anlamda hakka konu teşkil edecek verinin ilgili kişi tarafından sağlanması şartının veri türünü de kapsayacak biçimde yorumlanması gerekir. Hizmet sağlayıcısı olan bir veri sorumlusunun, ilgili kişi tarafından kullanılan bir hizmet vasıtasıyla elde etmiş olduğu veri, bu veriden yeni bir veri oluşturma işlemine girişilmedikçe ilgili kişinin davranışları doğrultusunda yalnızca gözlenen veri olma özelliğini korumaktadır. Veri sorumlusunun söz konusu veriyi üretmeye yönelik hizmeti veya cihazı kullanıma sunmaktan ve sistemi işletmekten başka aktif bir müdahalesi bulunmamaktadır. Nitekim bir kişinin aktif bir davranışı ile sunulmuş olan veya veri sorumlusu tarafından ilgili kişinin davranışının izlenmesi ile elde edilen bu tür veriler ilgili kişi tarafından sağlanma ölçütünü karşıladığı gibi gözlenen veri türüne dahil olarak veri taşınabilirliği hakkına da konu olabilmektedir. Buna karşılık türetilmiş ve çıkarsanan verilerde veri sorumlusu son verinin üretim sürecine müdahil olduğundan bu verilerin ilgili kişi tarafından sağlanan veri olarak değerlendirilmesi de yerinde olmayacaktır. Bu doğrultuda 29. Madde Çalışma Grubu'nun yalnızca gözlenen verilerin taşınabilir olduğu yönündeki değerlendirmesi, GDPR m. 20'nin lafzında geçen, verinin ilgili kişi tarafından sağlanması şartı kapsamında uygun bir değerlendirmedir. Lakin konuya rekabet hukuku perspektifinden getirilen bir bakış, veri taşınabilirliği hakkının

[137] **Krämer**, s. 266; **OECD**, *Summary of the Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, s. 5.

kapsamına ilgili kişi tarafından beyan edilmek yoluyla sağlanan veya gözlenen verilerin girdiğini kabul etmekle beraber Avrupa Birliği Temel Haklar Şartı'nın "Teşebbüs serbestisi" başlıklı 16. maddesi ile topluluk hukuku ile ulusal hukuk ve uygun olarak teşebbüs serbesti tanınmasının bir temel insan hakkı olarak öngörülmüş olduğu, veri taşınabilirliği hakkının bir temel insan hakkı teşkil etmediği, rakip iki teşebbüsten birinin gözlenen verileri elde etmek yolu ile adil olmayan bir avantaj elde edebileceği, bu nedenle gözlenen verilerin taşınmasında pasif veri alımından daha üst düzey yöntemlerle elde edilen verilerin hakkın kapsamına girmemesi gerektiği, aksi bir uygulamanın iki rakip teşebbüs arasındaki adil rekabete orantısız ve dayanılmaz bir müdahale teşkil edeceği düşüncesini savunmaktadır[138].

Bu hususta sorun teşkil eden mesele, bir verinin türetilmiş veya çıkarsanan bir veri olup olmadığının tespit edilmesindeki güçlüktür. GDPR'da konuya ilişkin bir açıklama bulunmadığı gibi 29. Madde Çalışma Grubu da bu verilerin ayırt edilmesi için uygun ölçütler öngörmemiştir. Örneğin, bir günün çeşitli saatlerinde farklı yerlerde çekilen ve nerede çekildiğini anlaşılabilir kılacak emarelerin bulunduğu fotoğraflar vasıtasıyla kişinin gün içinde en azından fotoğrafın çekildiği an itibariyle bulunduğu konumun bilgisine ulaşılabilir. Bu şekilde elde edilmiş olan verinin bir gözlenen veri mi yoksa çıkarsanan veri mi olduğu sorusuna iki farklı şekilde cevap verilebilir: Cadde veya sokak adının yazdığı bir tabeladan veya Anıtkabir gibi herkesçe bilinen bir yer olmasından ötürü konum bilgisi fotoğraftan anlaşılabiliyorsa, başka bir araca gerek duyulmaksızın söz konusu veriye kolaylıkla ulaşılabilir ve bu durumda ham bir veriden söz edilebilir. Fotoğraftaki mekan görüntülerinden konum kolaylıkla tespit edilemiyorsa ve mekan görüntüsünü internet üzerinde arayarak en uygun

[138] **Belo**, J./**Macedo Alves**, P.: *The Right to Data Portability: An In-Depth Look*, Journal of Data Protection and Privacy 2018, Vol. 2, No. 1, s. 60.

sonuçları belirleyen bir algoritmaya ihtiyaç duyulursa çıkarsanan bir veri bulunuyor olabilir. Böyle bir durumda verinin türünü belirleyebilmek için verinin kullanıcıya ne şekilde sunulduğuna bakılması bir çözüm getirebilir.[139]

İlgili kişinin veriyi doğrudan aktif bir davranışla sağladığı durumlarda hakkın kapsamına yalnızca bu verinin girdiğini kabul etmek gerekir. Keza bu halde veri sorumlusunun bu veri üzerinden algoritma yardımıyla elde ettiği yeni veriler çıkarsanmış veri olacağından veri taşınabilirliği hakkı kapsamı dışında kalacaktır. İlgili kişinin bir hizmet veya cihazı kullanması dolayısıyla elde edilen veriler bakımındansa ikili bir ayrıma gitmek ve verinin türünü somut olay nezdinde bu değerlendirmeyi yaparak tespit etmek gerekir. İlgili kişinin hizmet veya cihazı kullanmaktaki amacına ancak birtakım başka verilerin analiz edilmesi, dönüştürülmesi, ayıklanması gibi yollarla veya buna uygun algoritmalar ile ulaşılabiliyorsa veri sorumlusunun basit olmayan bir yolla işlemiş olduğu bu veri de ham/gözlenmiş veri niteliği taşıyacaktır. Ne var ki veriler üzerinde hizmet veya cihazın kullanılması ile beklenen amacı aşan nitelikte bir işlem gerçekleşiyorsa bu şekilde elde edilen veriler çıkarsanan veri olacaktır. Örneğin, giyilebilir teknoloji ürünlerinin gelişmesiyle birlikte elektrokardiyografi (EKG) ölçümü yapma ve raporlama özelliğine sahip akıllı saatler üretilmeye başlanmıştır. Akıllı saatin bu özelliğini kullanmak isteyen bir kişi kalp atış hızının ölçülmesi ve bunun sistematik olarak raporlanmasını amaçlamaktadır. Bu bağlamda uygulamanın sunacağı veri bir ham veri olacaktır. Oysa aynı akıllı saatin, ilgili kişinin gün içinde attığı adım sayısı, uyku düzeni, kulaklık cihaza bağlı iken cihazda kullandığı ses düzeyi, EKG verisi gibi ilgili

[139] **Bozdag**, s. 3. Yazar kalp atış hızı örneği üzerinden ele aldığı bu konuda kalp atış hızının birtakım başka ölçüler üzerinden veya algoritma yardımıyla belirlenmiş olsa dahi kullanıcıya bir uygulama vasıtasıyla sunuluyorsa ham veri olarak değerlendirilebileceği kanaatindedir.

kişinin bir arada değerlendirilmesini amaçlamadığı verileri bir araya getirerek otomatik olarak bir sağlık profili çıkarması halinde veri, çıkarsanan veri niteliğindedir.

Kişisel verinin ham/gözlenen bir veri olduğu tespit edildikten sonra gündeme gelebilecek bir diğer sorun ise başka birtakım verilerin bir araya getirilmesi ile elde edilen ham verilerin taşınması halinde söz konusu ham veriyi oluşturan diğer verilerin de taşınıp taşınmayacağıdır.[140] Örneğin, bir akıllı saatin ilgili uygulamasınca tutulan EKG verisinin taşınması talep edildiğinde, bu veriyi oluşturan kalp atış hızı gibi alt verilerin de taşıma talebine dahil olup olmayacağı madde metninden anlaşılamamaktadır. Taşınma talebine muhatap olan kişisel verilerin, zaman bakımından bunlardan daha önce veya daha sonra elde edilen aynı ya da benzer amaçtaki verilerle bir bütün olarak analiz edilebilmesi veya bu verilerin kullanılıp daha üst düzeyde bir veriyi oluşturan hizmet yahut cihazın kullanılabilmesi ihtiyacı doğabilecektir. Bu sebeple ham veriyi oluşturan diğer verilerin de taşınması uygun olacaktır.

C. Kişisel Verilerin Otomatik Yollarla Tutulması

Gerek Avrupa Birliği düzenlemelerinde gerekse 6698 sayılı Kanun'da kişisel verilerin işlenmesi ("*processing*") bahsi, teknolojik gelişmelerin hızı karşısında sınırlı düzenleme yapma imkânının bulunmadığından örnekseme yolu ile sayılmıştır. Bu kapsamda *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde*

[140] **Bozdag**, s. 3.

gerçekleştirilen her türlü işlem"[141][142] veri işleme sayılmaktadır. Görüleceği üzere işleme faaliyeti kişisel veri üzerinde gerçekleştirilen her türlü operasyonu kapsayacak kadar geniş anlaşılmaktadır.

Verinin kısmen veya tamamen otomatik yollarla işlenmesi[143] ifadesinin, kişisel verinin bir bilgisayar, telefon, tablet gibi mobil araçlar, dron, yönlendirici gibi araçlar vasıtasıyla işlenmesi olarak anlaşılması gerekmektedir. Tam otomatik kişisel veri işleme faaliyetinde verinin tamamen sistem tarafından işlenmesi söz konusu iken kısmi otomatik veri işleme faaliyetinde veriler sisteme bir insan müdahalesi ile eklenmektedir[144]. Öte yandan herhangi bir veri kayıt sisteminin ("*filing system*") parçası olmak kaydıyla ve otomatik olmayan yollarla örneğin yalnızca kağıt üzerinde kişisel verilerin işlenebileceği de kabul edilmiştir. Bu bağlamda veri kayıt sisteminden anlaşılması gereken kişisel verilerin belirli ölçütlere göre sistematik bir biçimde kategorize edilmesi ve bu ölçütlere göre ulaşılabilir hale getirilmesidir[145]. Görüleceği üzere kişisel verinin elde edilmesinden itibaren ömrünün devam ettiği her safhada

[141] ABAD'a yansıyan *František Ryneš* davasında ev için koruma amaçlı kullanılan CCTV mekanizması aracılığıyla evin camlarını kıran iki kişinin görüntülerinin kaydedildiği olayda kişisel verilerin kaydedilmesini ve saklanmasını içeren video kayıtlarının otomatik veri işleme kapsamına girdiğine karar verilmiştir, bkz. Case C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů,* 11.12.2014, ECLI:EU:C:2014:2428, par 25.

[142] 6698 sayılı KVKK m. 3/1-e. Benzer tanımlar için bkz. GDPR m. 4/2, 108 no.'lu Sözleşme m. 2/b.

[143] Bir internet sayfasında çeşitli kişilerin isim, telefon numarası veya hobiler gibi bilgileriyle anılmasının 95/46/AT m. 3 uyarınca tamamen veya kısmen otomatik yollarla veri işlenmesi teşkil edeceği yönünde bkz. Case C-101/01, *Criminal proceedings against Bodil Lindqvist,* 6.11.2003, ECLI:EU:C:2003:596, para. 27. Herhangi bir kişisel verinin önceki bir süreçte kamuya açık hale getirilmesi durumunda da veri üzerinde gerçekleştirilen her türlü işlemin veri işleme kapsamında değerlendirileceği yönünde bkz. Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13.05.2014, ECLI:EU:C:2014:317.

[144] **Aşıkoğlu**, Ş. İ.: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul 2018, s. 70; **Başalp**, s. 32-33; **Çekin**, s. 26; **Develioğlu**, s. 39-41.

[145] 6698 sayılı KVKK m. 3/1-h; GDPR m. 4/6. OECD'nin otomatik veri işlemeye ("*automated data processing*") ilişkin "*İnsan yardımı veya müdahale ihtiyacını en aza indirecek şekilde birbirine bağlı ve etkileşimli bir elektronik veya elektrikli makine sistemi tarafından gerçekleştirilen veri işleme operasyonları*" tanımı için bkz. (https://stats.oecd.org/glossary/detail.asp?ID=4370, E. T.: 05.05.2022).

gerçekleştirilen muhafaza, depolama, aktarım vb. dahil tüm operasyonlar kişisel verinin işlenmesi anlamına gelecektir.

Veri taşınabilirliği hakkına ilişkin Gerekçe 68'de, hakkın uygulanabilirliği kişisel verilerin otomatik yollarla[146] işlenmiş olmasına bağlanmıştır. Bankacılık, eczacılık, havayolları gibi sektörler başta olmak üzere kişisel verinin işlendiği küçük bir teşebbüs dahi hakkın uygulanması bakımından aynı konumdadır[147]. Sosyal medya başta olmak üzere arama motorları, fotoğraf depolama, e-posta veya çevrimiçi alışveriş hizmetlerinde[148], bulut bilişim, internet hizmetleri, akıllı telefon sistemleri ve diğer otomatik yolla veri işlemelerde[149] veri taşınabilirliği hakkı uygulama alanı bulur. Kağıt ortamında tutulan kişisel veriler için hakkın kullanılamayacak olması[150], hakka özellikle internet kullanımı dolayısıyla ortaya çıkan sorunlarla ihtiyaç duyulmasından kaynaklanmaktadır. Dijital kimliğin, kişiliğin bir parçası haline gelmesi dijital ortamda tutulan kişisel veriler yönünden self determinasyon hakkının, kişiliğin korunması ve geliştirilmesi hakkının yeni yöntemlerle korunmasını zorunlu hale getirdiğinden Avrupa Komisyonu'nun madde metnine yalnızca otomatik yollarla işlenen kişisel verileri dahil etmesi pek de haksız görünmemektedir[151]. Öte yandan kağıt ortamında tutulan veri bakımından erişim hakkı, ilgili kişiye söz konusu verilerin nüshasını alma hakkı tanıdığından yeterli bir işlevi halihazırda taşımaktadır.

III. HAKKA İLİŞKİN SINIRLAMALAR

A. Genel Sınırlama Sebepleri

[146] 2012 yılında sunulan GDPR taslak çalışmasının 18. maddesinde yer verilen veri taşınabilirliği hakkına ilişkin metnin ilk halinde, mevcut metindeki otomatik yollarla ("*by automated means*") ifadesi elektronik yollarla ("*by electronic means*") olarak belirtilmişti.
[147] **Graef/Verschaleken/Valcke**, s. 62; **Vanberg**, s. 11.
[148] **Vanberg**, s. 11.
[149] **Vanberg**, s. 11; **Zanfir**, s. 149.
[150] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 9.
[151] **Zanfir**, s. 157.

GDPR m. 23'te, veri sorumlusu veya veri işleyenin tabi olduğu Birlik veya devlete; temel hakların özüne dokunulmaksızın milli güvenliğin, savunmanın, kamu güvenliğinin, suçun önlenmesinin, soruşturulmasının, kamu yararına yönelik hedeflerin, yargı bağımsızlığının ve adli süreçlerinin korunmasının, düzenlenmiş mesleklere ilişkin etik kuralların ihlalinin önlenmesinin, bazı hallerde resmi yetkinin kullanımı ile bağlantılı izleme, denetleme, düzenlemenin, ilgili kişinin veya başkalarının hak ve özgürlüklerinin korunmasının, medeni hukuktan kaynaklanan taleplere ilişkin kararların icrasının güvence altına alınması için gerekli ve orantılı olduğu ölçüde 12 ila 22. maddeler ile 34. maddenin ve 5. madde hükümleri 12 ila 22. maddelerde hükme bağlanan hak ve yükümlülüklere uygun olduğu sürece 5. maddenin kapsamını kısıtlama yetkisi tanınmıştır.

Öngörülen hüküm ilgili kişinin tüm haklarına ilişkin genel bir sınırlama sebebi teşkil etmektedir. Gerekçe 73'te de belirtildiği üzere bu kısıtlamaların her halde Avrupa Birliği Temel Haklar Şartı ile Avrupa İnsan Hakları Sözleşmesi'ne uygun olması gerekir. Ayrıca GDPR m. 11 uyarınca veri sorumlusunun, ilgili kişinin kimliğini teşhis edebilecek durumda olmadığından ilgili kişiyi haberdar etmesi üzerine teşhise elverişli bilgilerin sağlanmaması halinde GDPR Bölüm III'te öngörülen haklar kullanılamayacaktır.

B. Kamu Yararına Gerçekleştirilen Bir Görevin Yerine Getirilmesi veya Veri Sorumlusuna Verilen Resmi Bir Yetkinin Kullanılması

GDPR m. 6/1-e uyarınca, kişisel verilerin işlenmesi kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için gerekliyse rıza bulunmasa dahi bu amaçla bağlantılı ve sınırlı olarak kişisel veriler işlenebilecektir. Bir başka deyişle, m. 6/1-e bu hali bir

hukuka uygunluk sebebi olarak öngörmüştür. Kamu yararına gerçekleştirilen görev bir kamu otoritesine ait olabileceği gibi kamu hizmetinin görülmesi suretiyle bu görevin ifası özel bir teşebbüse de bırakılmış olabilir.

Kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için gereken işleme faaliyetlerinde veri taşınabilirliği hakkının uygulanmayacağını öngören m. 20/3 hükmü, hakkın kapsamına bir sınırlama getirmektedir. Maddenin birinci fıkrasında veri taşınabilirliği kapsamına giren işleme faaliyetinin rıza veya sözleşmeden kaynaklandığı belirtilmiştir. Bunun dışındaki herhangi bir sebebe dayalı olarak işlenmiş kişisel veriler için veri taşınabilirliği hakkı ileri sürülemeyecektir. GDPR, maddenin üçüncü fıkrasında hakkın kullanımına bir istisna hali getirirken daha önceki ifadesini tekrarlamamakta, bu fıkrada kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması durumunu rızanın olmadığı takdirde işlemeyi hukuka uygun kılacak bir sebep olarak değil işleme amacı olarak[152] belirtmektedir. Hakikaten, söz konusu amaçla kişisel verilerin işlenmesi, işlenen veriler ilgili kişi tarafından ve onun rızasıyla sağlanmış olsa, veri sorumlusu tarafından otomatik yollarla işlense dahi veri taşınabilirliği hakkının ekonomik gerekçelerle ilgili kişilerin kişisel verileri üzerinde daha fazla enformasyonel self determinasyon hakkına sahip olmalarını sağlayarak rekabeti ve inovasyonu artırma amacına hizmet edebilecek türden değildir[153]. Öyle ki bu hallerde işleme faaliyeti ilgili kişinin kişisel verilerini veri sorumlusuna sağlama niyetinde olup olmadığına bakılmaksızın kamu yararı veya resmi bir yetkinin uygulanması gibi daha üstün bir menfaate dayanmaktadır. Kamu hukukunun doğurduğu bir gereklilik

[152] **De Hert/Papakonstantinou/Malgieri/Beslay/Sanchez**, s. 198.
[153] **De Hert/Papakonstantinou/Malgieri/Beslay/Sanchez**, s. 198.

çerçevesinde işlenen veriler sebebiyle ilgili kişinin bir veri sorumlusu bünyesinde sıkışıp kalma ihtimali son derece düşüktür. Dahası, alıcı veri sorumlusunun bu yönde bir görevi veya yasal yükümlülüğü bulunmamakta ise söz konusu verilerin de taşınması gereğinden fazla verinin işlenmesi sonucunu doğurabilir. Dolayısıyla, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması amacıyla gerçekleştirilen bir işleme faaliyeti veri taşınabilirliği hakkının gerekliliklerini sağlasa dahi bu kişisel verilerin taşınması talep edilemeyecektir. Buna karşılık olası taşınabilirlik taleplerini karşılayabilecek, ilgili kişilerin bu kapsamda işlenen kişisel verilerini kolayca indirmelerini sağlayacak bir hizmetin sağlanması yararlı bir uygulama olarak belirtilmektedir[154].

C. Başkalarının Hak ve Özgürlüklerinin Korunması

1. Üçüncü Kişilerin Hak ve Özgürlüklerinin Korunması

GDPR m. 20/4'te ilgili kişiye tanınan veri taşınabilirliğini talep hakkının başkalarının hak ve özgürlükleri ile çatışması hali özel olarak düzenlenmiştir. Kişisel verilerin korunması hakkını bir temel insan hakkı olarak ele alan görüş uyarınca[155],

[154] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 9.

[155] Verinin ekonomik menfaatle olan sıkı ilişkisi dolayısıyla ABD'de yaygın olan görüş uyarınca ekonomik bir değer olarak kişisel verilerin korunması gerektiği görüşünü ileri sürenler mevcuttur. Konu hakkındaki detaylı açıklamalar için bkz. **Aksoy**, s. 64 vd.; **Çekin**, s. 20; **Dülger**, s. 45; **Küzeci**, s. 67 vd. Bugün Avrupa'da yaygın olan anlayış kişisel verilerin korunması hakkının "mahremiyet" alanı içinde ele alınarak insan hakkı olarak değerlendirilmesi gerektiği yönündedir. Mahremiyet alanı özel yaşam ile sıkı bir ilişki içindedir. Özel yaşam, kişilerin başkaları ile paylaşmak istemedikleri, yaşam tarzı, tavır, değer, zevk, tercih, ilişkiler gibi pek çok unsurdan oluşan ve "yalnız kalma hakkı"na benzer şekilde "kişinin kendi olmakta özgür olduğu" alandır. Özel hayatın ya da çok da geniş bir ifade ile gizliliğin korunması hakkı içinde kişinin bilgisel gizliliğin ölçüsünü belirleyebilme ve kendi bilgilerinin geleceğini tayin edebilme hakkı bulunmaktadır. Enformasyonel self determinasyon olarak adlandırılan bu hak, biyometrik ve genetik verilerin yahut diğer kişisel verilerin depolanması ve kullanılması, GPS denetim kayıtları veya kişinin siyasi aktivitelerine ilişkin kayıtlar gibi pek çok bilginin akıbetini ilgilendirmektedir. Tüm bu açıklamalara karşın Türk hukukunda kişisel verilerin korunması hakkının Anayasal dayanağını teşkil eden Anayasa m. 20/3'te hakkın, özel hayatın gizliliği başlığı altında düzenlenmiş olması sistematik bir yoruma tabi tutulduğunda, hakkı özel hayatın gizliliği hakkının bir alt başlığı olarak ele almak da mümkündür. Nitekim konu kişinin ve kişiliğin korunması bağlamında Kişisel Verileri Koruma Kurumu tarafından da bu biçimde ele alınmaktadır. Bunlara paralel olarak Avrupa İnsan Hakları Mahkemesi de kişisel verilerin korunması hakkını, İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi'nin *"özel ve aile hayatına saygı hakkı"* başlıklı 8. maddesine dayandırmaktadır. Bu hususta açıklamalar ve örnekler için bkz. **González**

diğer kişilerin kişisel verilerini de içeren veri setlerinin taşınmasında başta kişisel verilerin korunması hakkının olumsuz etkilenmesi gündeme gelebilir. Bunun yanı sıra taşınması talep edilen kişisel verinin içeriğine göre özel hayatın gizliliği veya haberleşme hürriyeti gibi temel insan haklarının ihlal edilmesi de söz konusu olabilecektir. Oysa veri taşınabilirliği hakkı diğer kişilere haksız bir zarar vermemeli veya meşru olmayan bir sınırlama getirmemelidir[156].

29. Madde Çalışma Grubu veri taşınabilirliği hakkına ilişkin rehberinde üçüncü kişilerin kişisel verilerinin, taşınması talep edilen veri setinde yer alması durumunda işlemenin hukuka uygunluğunu sağlamak için başka bir gerekçe bulunması gerektiğine dikkat çekmektedir[157]. Hakikaten ilgili kişinin kullanmakta olduğu bir hizmet (webmail servisi, fotoğraf-video depolaması, sosyal medya platformları vb.) dolayısıyla işlenmiş olan kişisel verilerinin başka bir hizmet sağlayıcıya aktarılmasını talep etmesi halinde taşınacak veri setinin içinde üçüncü bir kişiye ait görüntü veya iletişim bilgileri gibi kişisel verilerin bulunması muhtemeldir. Bu takdirde gerek gönderici veri sorumlusu tarafından yapılan iletim işleminin gerekse alıcı veri sorumlusu tarafından yapılan kaydetme, muhafaza etme, depolama gibi işlemlerin kişisel veri işleme anlamına geldiği dikkate alındığında söz konusu işleme faaliyetlerinin hukuka uygun olarak gerçekleştirilebilmesi için her iki veri sorumlusunun da uygun bir hukuki dayanak ekseninde hareket etmesi gerekir. Aksi halde bir sosyal medya platformunda yer alan konuşmaların başka bir sosyal medya platformuna taşınması talebi, konuşmanın diğer tarafını teşkil eden ve taşınabilirlik

Fuster, G.: The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing, Law, Governance and Technology Series, Volume 16, Heidelberg 2014, s. 94-103.

[156] **De Hert/Papakonstantinou/Malgieri/Beslay/Sanchez**, s. 198.

[157] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 10-11.

talebi bakımından alıcı ve gönderici veri sorumluları ile ilgili kişi açısından üçüncü kişi konumunda bulunan kişilerin kişisel verilerinin korunması hakkını ve bu doğrultuda unutulma hakkını[158] ya da daha ileri bir boyutta haberleşmenin gizliliği hakkını ihlal edebilecektir. Ne var ki üçüncü bir kişiye ait kişisel verinin bulunduğu her olayda taşınabilirlik hakkının kısıtlandığını kabul etmek hakkın işlerliğini önemli ölçüde sekteye uğratacaktır. Öte yandan doktrinde, hakka getirilecek böylesi katı bir sınırlamanın inovasyon ve tüketici refahı üzerinde olumsuz bir etkisinin olacağı, tüketicilerin sonuçtan yine olumsuz etkileneceği ifade edilmiştir[159]. Bu sebeple üçüncü kişilerin hak ve özgürlükleri ile ilgili kişinin menfaati arasında makul bir dengenin kurulması gerekir.

GDPR m. 20'de öngörülen diğer şartların da sağlanması koşuluyla ilgili kişinin veri sorumlusunda bulunan kişisel verilerini alma hakkını kullanması, alma hakkını kullandıktan sonra bu verileri bir başka veri sorumlusuna iletmesi veya kişisel verilerinin bir veri sorumlusundan diğerine doğrudan iletilmesini talep etmesi hallerinin her biri için üçüncü kişilere ait kişisel verilerin akıbeti ve bu kişilerin hak ve özgürlüklerinin zarar görüp görmediği ayrı ayrı incelenmelidir.

Öncelikle, kişisel verilerin dolaylı olarak iletilmesinin ilk aşamasını oluşturan alma hakkı bakımından incelendiğinde ilgili kişinin kendisine ait kişisel verileri alma hakkını kullanması, bu veriler içinde üçüncü kişilere ait kişisel veriler bulunsa dahi tek başına üçüncü kişilerin hak ve özgürlüklerinin olumsuz etkilenmesi anlamına gelmeyecektir. Nitekim alma hakkını kullanan ilgili kişinin bu kişisel verileri tamamen

[158] **Li**, sonraki/alıcı veri sorumlusunun üçüncü kişilerin kişisel verilerinin işlenmesi için başka bir hukuki dayanak bulsa dahi veri taşınabilirliği hakkı ile unutulma hakkının çatışma halinin ortadan kalkmayacağını, bu sebeple de unutulma hakkının her durumda olumsuz etkileneceğini belirtmektedir. Bkz. **Li**, s. 313.
[159] **Vanberg**, s. 14.

kendisiyle ilgili bir faaliyet kapsamında işlemesi söz konusu olabilecektir ki bu da gerek Türk hukukunda gerekse GDPR'da konu bakımından sınırlama sebepleri içinde öngörülen istisnalardan biridir. Bir başka ifade ile bu halde KVKK veya GDPR uygulama alanı bulamayacaktır. İlgili kişinin bu yolla eriştiği kişisel veri seti içinden, üçüncü kişiye ait kişisel verileri kullanmak suretiyle bu kişilerin hak ve özgürlüklerini ihlal etmesi mümkünse de alma hakkının kullanılması ile üçüncü kişilerin hak ve özgürlüklerinin ihlal edilmesi arasında doğrudan bir illiyet bağı bulunmamaktadır. Bu ihtimalde üçüncü kişilerin hak ve özgürlükleri ancak alma hakkını kullanmış olan ilgili kişinin, elinde bulundurduğu üçüncü kişilere ait kişisel verilere yönelik hukuka aykırı nitelikte bir davranışta bulunması halinde ihlal edilebilecektir. Dolayısıyla ihlalin sebebi alma hakkı değil, ilgili kişinin hukuka aykırı davranışı olacaktır. Bu bağlamda, alınan kişisel verinin güvenliği dahil olmak üzere işleme faaliyetiyle ilgili sorumluluk, veri sorumlusunca karar verilmediği sürece, ilgili kişide olacaktır[160].

Diğer bir halde, alma hakkını kullanan ilgili kişinin, ilk veri sorumlusundan edindiği kişisel verileri bir başka veri sorumlusuna iletmeden önce bunların içinde üçüncü kişilere ait kişisel verilerin bulunup bulunmadığını araştırması uygun olacaktır. Hal böyle iken ilgili kişinin, iletme hakkı bağlamında sonraki veri sorumlusuna bu kişisel verileri aktarmadan önce üçüncü kişilere ait kişisel verileri veya bunların sonraki veri sorumlusu tarafından işlenmesinin gerekliliği meselesini tam ve doğru olarak belirlemesini beklemek pek isabetli görünmemektedir. Öte yandan, doğrudan taşınabilirliğin söz konusu olduğu halde de gönderici veri sorumlusu ilgili kişinin taşıma talebini gerçekleştirmeye yönelik adımlarında üçüncü kişilerin kişisel verilerini alıcı veri sorumlusuna göndermekte çekimser bir tutum sergileyebilir veya doğrudan

[160] **Vanberg**, s. 12.

taşınan veriyi otomatik araçlarla kabul eden alıcı veri sorumlusu gereğinden fazla veri işleme tehlikesiyle karşılaşabilir. Her iki durumda da iletme veya ilettirme hakkının kullanılması üçüncü kişilerin hak ve özgürlüklerini olumsuz etkileyebilecek durumdadır. Öyle ki üçüncü kişinin kişisel verileri kendisinin rızası alınmadan hatta belki bilgisi dışında ikinci/alıcı veri sorumlusuna iletilecek ve bu veri sorumlusu tarafından işlenecektir. İşleme faaliyetinin hukuka uygunluğunu düzenleyen GDPR m. 6 ve m. 9 hükümlerine göre ise ilgili kişinin GDPR dolayısıyla sahip olduğu herhangi bir hakkını kullanması işlemenin hukuka uygunluğunu sağlayacak sebeplerden biri değildir. Öyleyse ikinci/alıcı veri sorumlusu üçüncü kişilerin kişisel verilerini ihlal etmemek adına bu kişilerin kişisel verilerini işlememelidir denebilir mi? Soruya olumlu cevap verildiği takdirde GDPR'ın veri taşınabilirliği ile ilgili kişiye sağlamayı hedeflediği hakkın pratik faydasını önemli ölçüde ortada kalkmaktadır. Zira özellikle sosyal medya platformları gibi alanlarda veri taşınabilirliği hakkından beklenen yalnızca ilgili kişinin isim, soy ismi, iletişim bilgileri gibi kişisel verilerinin zahmetsizce başka bir platforma iletilmesi değil, bir platformun kullanımı dolayısıyla burada biriken dijital geçmişin taşınmasıdır. Böylesi bir durumda iletilmesi istenen veri seti içinde üçüncü kişilere ait konuşma kayıtlarının, iletişim ve adres bilgilerinin, görüntülerin ve daha pek çok kişisel verinin bulunması muhtemeldir. İkinci/alıcı veri sorumlusunun bu verileri hiçbir surette işleyememesi haktan beklenen faydayı sağlamayacağından veri sorumlularının da hakkın kullanımını kolaylaştıracak teknik altyapıyı oluşturmaktan imtina etmesine yol açacaktır. Soruya olumsuz cevap verildiği takdirde ise üçüncü kişilerin rızası alınmadan ya da diğer hukuka uygun işleme sebeplerinden herhangi biri karşılanmadan kişisel verilerinin işlenmesi söz konusu olacaktır ki bu ilk bakışta kişisel verilerin korunması hakkını ihlal etmekte, akabinde

iletilen verinin içeriğine göre üçüncü kişinin özel hayatının gizliliği veya haberleşme hürriyeti gibi birtakım hak ve özgürlüklerini de tehdit etmektedir. Dahası, bu kişisel verilerin başka bir veri sorumlusuna iletilmesi ile ilk veri sorumlusunun mahremiyeti sağlamak için getirdiği kısıtlamalar aşılabilir[161]. Oysa üçüncü kişi, korumayı yetersiz bulması nedeniyle belirli bir veri sorumlusuna kişisel verilerini özellikle sağlamamış olabilir. Böyle bir tercih bulunsun ya da bulunmasın taşımanın gerçekleştirilmesi, üçüncü kişinin enformasyonel self determinasyon hakkının etkisiz bırakılması ve kişilik haklarının ihlali anlamına gelebilir.

29. Madde Çalışma Grubu, üçüncü kişilerinin hak ve özgürlüklerinin korunması gerekliliğine işaret ederken iletilen veri ilk/gönderici veri sorumlusu ile aynı amaçta veri işleniyorsa, örneğin bir banka hesabı geçmişinin iletilmesinde hesaba para gönderen veya alan üçüncü kişilerin kişisel verilerinin ikinci/alıcı veri sorumlusu tarafından işlenmesinin üçüncü kişilerin hak ve özgürlüklerini olumsuz etkilemediği değerlendirmesinde bulunmuştur. Ancak burada önemli bir hususa dikkat çekilmiş ve üçüncü kişilerin bu işleme faaliyetinden zarar görmelerini engellemek için kişisel verilerin yalnızca ilgili kişinin kullanımına ve kontrolüne açık olduğu ölçüde işlenmesine izin verildiği değerlendirmesi yapılmıştır[162]. Dolayısıyla ikinci/alıcı veri sorumlusunun taşıma sebebiyle işlediği verileri reklamcılık, pazarlama gibi kendi amaçları için kullanmasının hukuka aykırı olacağı ifade edilmiştir[163].

---

[161] **Engels**, s. 5.

[162] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 12. 29. Madde Çalışma Grubu'nun veri taşınabilirliği rehberinde yer alan bu ifadeye yönelik, GDPR'ın hiçbir yerinde işlemenin kişisel veya ev içi kullanımla sınırlı olması koşulunun aranmadığı ve bu koşulu uygulamanın, taşınabilirliğin doğurması beklenen yeniliğe gereksiz bir müdahale teşkil ettiği eleştirisi için bkz. **Lynskey**, s. 814.

[163] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 12; **Vanberg**, s. 12-13.

Veri taşınabilirliği hakkının pratik anlamda uygulanabilirliğini etkileyen bu hususta sınırlayıcı bir tutum, ilgili kişinin menfaatini ve GDPR m. 20 ile hedeflenen amacı zedeleyebilecek iken aksi yönde bir tutum da üçüncü kişilerin hak ve özgürlüklerini hukuka aykırı bir işleme faaliyeti ile ihlal etme tehlikesi yaratmaktadır. Her şeyden önce ikinci/alıcı veri sorumlusunun ister yalnız ilgili kişinin kullanımına sunsun ister kendi amaçları için yararlansın taşınan verileri kaydetmesi, yapılandırması, saklaması, elde etmesi ve bunun gibi her türlü işlem GDPR m. 4/2 ışığında işleme faaliyeti kapsamında kalacaktır. Hukuki bir işleme faaliyeti ya ilgili kişinin rızasına ya da kişisel verinin özel nitelikli veri[164] olup olmamasına bağlı olarak GDPR m. 6 veya m. 9'daki diğer sebeplere bağlı olarak gerçekleşebilir. Aksi halde işleme faaliyeti hukuka aykırı olacaktır. Keza ikinci/alıcı veri sorumlusu taşınan kişisel verileri kendi amaçları için işlemese dahi taşıma ile elde ettiği veriler vasıtasıyla üçüncü kişilerin özel hayatına ilişkin bilgiler edinebilir ve bunları hukuka aykırı olarak kullanabilir, haberleşmenin gizliliğini ihlal edebilir. İşleme faaliyetinin hukukiliğine ilişkin ilk durumda, üçüncü kişinin kişisel verilerinin korunması hakkı, ilgili kişinin veri taşınabilirliği hakkını kullanmasından dolayı olumsuz etkilenebilir. Buna karşılık ikinci/alıcı veri sorumlusunun elde edilen veri içeriği üzerinden üçüncü kişinin diğer temel hak ve özgürlüklerini ihlal ettiği ikinci durumda veri taşınabilirliği hakkı ile ihlal arasındaki illiyet bağı, tıpkı ilgili kişinin alma hakkında olduğu gibi, veri sorumlusunun hukuka aykırı davranışı dolayısıyla kesilmiştir.

[164] Gerek KVKK'da gerekse GDPR'da kişisel veri, belirli veya belirlenebilir bir gerçek kişiye ait her türlü bilgi olarak tanımlanmış, bu veri kümesi içinde özel korumayı gerektiren birtakım veriler ayrıcalıklı hükümlere tabi tutulmuştur. Özel korumayı gerektiren kişisel veri grubu "özel nitelikli kişisel veri" veya "hassas veri" olarak adlandırılmaktadır. Özel nitelikli kişisel veriler sınırlı olarak sayılmıştır. Konuya ilişkin detaylı açıklama için bkz. **Aksoy**, s. 33-34; **Küzeci**, s. 279.

GDPR m. 20 ile güdülen amaç ve m. 20/4 hükmünün lafzı dikkate alındığında, taşınması talep edilen veri setinde üçüncü kişilerin kişisel verilerinin bulunması halinin, taşıma talebinin ileri sürülmesine bir istisna olarak belirlenmediği sonucu çıkmaktadır. Nitekim hükmün lafzında, daha geniş bir ifade kullanılarak üçüncü kişilerin hak ve özgürlüklerinden bahsedilmektedir. Ayrıca üçüncü kişilerin kişisel verilerinin yine GDPR'ın bizzat kendisi ile koruma altında olduğuna şüphe bulunmamaktadır.

Bu kapsamda uygulamada ortaya çıkabilecek sorunlar için *ex post* koruma mekanizmaları temel hak ve özgürlükler alanında ulusal ve uluslararası düzenlemelerle sağlanmıştır. Ancak bu hakların ihlalinden sonrası için getirilen çözümler hakkın en baştan korunmasından beklenen faydayı sağlamak kadar yeterli değildir ve bu sebeple *ex ante* koruma yollarının öngörülmesi gerekmektedir. Üçüncü kişilerin kişisel verilerinin, taşınması talep edilen veri setine dahil olması halinde veri sorumlusunun meşru menfaati kapsamında kişisel verilerin işlenebileceği düşünülebilir. Ancak bu halde üçüncü kişilerin temel hak ve özgürlüklerinin zarar görmediği, veri sorumlusunun meşru, güncel ve etkin bir menfaatinin bulunduğunun somut olarak ortaya konabilmesi gerekmektedir. 29. Madde Çalışma Grubu, ilgili kişinin gerekli ve gereksiz verileri seçme ve eleme yöntemi uygulayabileceği araçların gönderici ve alıcı veri sorumluları tarafından benimsenebileceğini belirtmekte, üçüncü kişilerin işleme faaliyetine rıza vermeye istekli oldukları durumlarda işlemenin rızaya dayanarak gerçekleştirilmesini önermektedir[165]. Somut olay üzerinden yapılacak değerlendirmede, veri sorumlusunun meşru menfaati veya açık rıza dışındaki hukuka uygun işleme sebeplerinden birinin var olduğu tespit edildiği takdirde işleme bu

[165] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 12.

gerekçeye dayandırılacaktır. Dolayısıyla 29. Madde Çalışma Grubu'nun söz konusu önerisi ancak başka bir işleme sebebinin bulunmadığı hallerde devreye girecek bir çözüm olabilir. Hakikaten, üçüncü kişilerin kişisel verileri ile hak ve özgürlüklerinin korunması için alınacak makul tedbirler ve uygun şekilde oluşturulacak hukuki dayanaklar işleme faaliyetinin hem ilgili kişi yönünden hem de üçüncü kişi yönünden korunması beklenen menfaatlerini dengelemeye hizmet eder. Benzer şekilde taşıma talebine konu olan veri seri içinde üçüncü kişinin hak ve özgürlüklerini olumsuz etkileyebilecek bir durumun bulunması halinde ilk/gönderici veri sorumlusunun bu hususta ilgili kişiyi aydınlatması da bir önlem olarak uygulanabilir.

2. Ticari Sırların Korunması

Avrupa Birliği'nin 2016/943 sayılı "Know-how ve Ticari Sırların Hukuka Aykırı Olarak Elde Edilmesine, Kullanılmasına ve Açıklanmasına Karşı Korunması Direktifi"nin[166] "Tanımlar" maddesinde ticari sır[167], genellikle söz konusu bilgi ile ilgilenen kişilerin kolaylıkla bilmediği ve ulaşamadığı, ticari değeri olan, bilgiyi kontrolü altında bulunduran kişinin bilginin gizliliğini sağlayabilmek için makul önlemleri aldığı bilgi olarak tanımlanmıştır. Ticari hayatta faaliyet gösteren veri sorumluları bir taraftan müşterilerinin bilgilerini kaydetmek suretiyle kişisel veri işlemekte ise de diğer taraftan bu bilgilerle bir müşteri listesi oluşturarak iş planlarını ve politikalarını bunun üzerinden oluşturmaktadır. Ticari sır niteliğindeki bu bilgilerle bir nevi ilgili kişilerin kişisel verileri dolayısıyla maddi olmayan tekelci bir güce sahip

[166] Directive (EU) 2016/943 of The European Parliament and of The Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN, E. T.: 05.05.2022).

[167] Türk hukukunda, Amerikan hukukunda, Avrupa Birliği hukukunda ve milletlerarası düzenlemelerde ticari sırrın ne şekilde ele alındığı ve dijital ortamda ticari sırrın korunmasına ilişkin daha detaylı açıklamalar için bkz. **Bozkurt Yüksel,** A. E.: *Ticari Sırların Dijital Ortamda Korunması*, TAAD 2018, Y. 9, S. 33, s. 143-192.

olmaktadırlar[168]. Bir tarafta veri sorumlusunun ticari menfaatlerinin korunması diğer tarafta ilgili kişinin kişisel verilerinin korunması meselesi bulunduğundan çatışan bu iki menfaatin dengelenmesi ihtiyacı doğmaktadır. Know-how ve Ticari Sırların Hukuka Aykırı Olarak Elde Edilmesine, Kullanılmasına ve Açıklanmasına Karşı Korunması Direktifi'ne ilişkin 28. Gerekçe'de ticari sırların, yasa dışı edinilmelerine, ifşa edilmelerine ve kullanılmalarına karşı korumak için alınan önlemlerin, çevrenin korunması ve çevresel sorumluluk, tüketicinin korunması, sağlık ve güvenlik gereklilikleri, fikri mülkiyet ve gizlilik hakkı dahil olmak üzere diğer alanlarda ilgili diğer yasaların uygulanmasını etkilemeyeceği ifade edilmektedir. Bu ifadeden, ticari sırların korunması ile kişisel verilerin korunması bakımından bir çatışma ortaya çıktığında ilgili kişinin menfaatinin üstün tutulacağı sonucuna varılabilir[169]. Buna karşılık GDPR m. 20'de veri taşınabilirliği hakkına ilişkin düzenleme içinde ticari sırların söz konusu olması halinde uygulanacak yöntem belirlenmemiş; 95/46/AT sayılı Direktif m. 41'in lafzında ve erişim hakkını düzenleyen GDPR m. 15'in 63 numaralı Gerekçe'sinde erişim hakkının ticari sırları olumsuz etkilememesi gerektiği belirtilmiştir. GDPR m. 20 hükmünden açıkça anlaşılamayan bu ikilem hakkında aydınlatıcı bir açıklama sunamayan 29. Madde Çalışma Grubu rehberleri de yetersiz kalmıştır. Dolayısıyla ticari sır ve kişisel verilerin bir arada bulunması halinde ilgili kişinin kişisel verilerinin korunması menfaatinin üstün tutulacağı şeklindeki toptancı yaklaşımdan ziyade somut olayın şartları içinde her iki tarafın da menfaatleri değerlendirilerek bir sonuca varmak en uygun çözüm olacaktır.

[168] **Malgieri**, G.: *Trade Secrets v Personal Data: a possible solution for balancing rights,* International Data Privacy Law 2016, C. 6, S. 2, s. 102.
[169] **Malgieri,** s. 103.

İlgili kişinin kişisel verilerini taşıma talebi karşısında veri sorumlusunun, talebe konu veri setinde ticari sırlarına ilişkin bilgiler bulunduğunu tespit etmesi halinde talebi doğrudan reddetmesi hakkın uygulanabilirliğini neredeyse imkânsız hale getirebilir. Oysa söz konusu veri taşınabilirliği olduğunda hakkın özelliğinden kaynaklı olarak, erişim hakkında olandan daha makul bir sınırlama kendiliğinden mevcuttur. Öncelikle ilgili kişi yalnızca kendisi tarafından veri sorumlusuna sağlanan kişisel verilerinin taşınmasını talep edebilecektir. Her ne kadar gözlenen verilerin de bu kapsama dahil edilmesini adil rekabete orantısız ve dayanılmaz bir müdahale olarak değerlendirenler mevcutsa da[170] gözlenen veriler ile türetilmiş ve çıkarsanan verilerin üretim süreçleri bir arada değerlendirildiğinde, gözlenen veriler üzerinde tersine mühendislik uygulamaları gerçekleştirilerek rakip teşebbüsün ticari sırrı niteliğinde bir bilgiye erişmek ya da önemli bir rekabet avantajı elde etmek pek mümkün görünmemektedir. Dolayısıyla kişisel verilerin iletileceği ikinci/alıcı veri sorumlusunun, ilk/gönderici veri sorumlusunun işlediği veriler ve varsa kullandığı algoritmalar üzerinden ekonomik menfaat sağlama yolu ile rekabet avantajı kazanması söz konusu olmamaktadır. Bir diğer taraftan taşıma talebinde bulunulan kişisel veriler veri sorumlusunca rıza veya sözleşmeye dayanılarak işlenmiş olan verilerdir. Bu iki unsur bir arada değerlendirildiğinde görülecektir ki taşınması talep edilen bu türden verilerin ticari sır niteliğinde bilgi içermesi ihtimali önemli ölçüde azalmaktadır. Ancak erişim hakkının tarafları yalnızca veri sorumlusu ile ilgili kişi olmakta iken veri taşınabilirliği hakkında üç taraflı bir ilişki bulunmakta, bu sebeple kişisel verilerin ifşası ticari sırrın rakip bir teşebbüs ile paylaşılması ihtimali doğurmaktadır[171].

[170] **Belo/Macedo Alves,** s. 60.
[171] **Malgieri,** s. 115.

Menfaat çatışmasına bir çözüm olarak doktrinde değinilen[172] ve 29. Madde Çalışma Grubu[173] tarafından da işaret edilen bağlamından arındırma ("*decontextualisation*") tekniği önerilmektedir. Bağlamından arındırma, kişisel verilerin, ticari sır niteliği bulunan veri seti içindeki ticari sırlardan ayrıştırılarak sunulmasıdır. Bu yolla ilgili kişinin taşıma talebi makul bir ölçüde karşılanabilmektedir. Aynı zamanda veri sorumlusunun piyasadaki rekabet gücü ve ticari plan ve politikaları olumsuz etkilenmemiş olmaktadır. Ancak söz konusu çözümün yeni bir maliyet kalemi oluşturacağından her ölçekteki veri sorumlusundan beklenmesi uygun olmayabilir.

3. Fikri Mülkiyet Haklarının Korunması

Fikri mülkiyet, klasik mülkiyet anlayışının kapsadığı cismani varlıklar dışındaki sanat eserleri, ticari marka veya işaretler gibi fikri yaratımları ifade eder[174]. Fikri mülkiyet haklarının korunması, fikri ürünü meydana getirenler ile kullanıcılar, teşebbüsler ve rakipleri, gelişmiş ve gelişmemiş ülkeler arasındaki menfaat çatışmalarını dengelemek için gereklidir[175]. Fikri ürünler üzerinde sahiplik haklarının tanınması ve korunması, her şeyden önce üretici konumunda bulunan kişinin korunması, desteklenmesi ve bu yolla inovasyonun tercih edilir sonuçlar doğurması için gereklidir. Taşıma talebine konu veri seti içerisinde müzik, video gibi içeriklerin bulunması halinde fikri mülkiyet haklarının korunması gereksinimi duyulabilir.

Veri taşınabilirliği hakkının, ilgili kişinin kişisel verileri üzerinde daha fazla söz sahibi olması yoluyla rekabeti ve inovasyonu desteklemeyi amaçladığı

---

[172] **Malgieri**, s. 105, 114.
[173] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 12.
[174] **Tekinalp, Ü.:** Fikrî Mülkiyet Hukuku, Güncelleştirilmiş ve Genişletilmiş Beşinci Bası, İstanbul 2012, s. 1-3.
[175] **World Intellectual Property Organization,** *What is Intellectual Property?*, 2020, (https://www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf, E.T.: 06.05.2022).

düşünüldüğünde, bu talebe konu olabilecek bir fikri ürünün sağladığı değerlerin korunmaması çelişkili olacaktır. Fikri mülkiyet hakları söz konusu olduğunda bir tarafta üçüncü kişilerin diğer tarafta veri sorumlusunun fikri mülkiyeti söz konusu olabilir. Üçüncü kişilerin haklarının olumsuz etkilenmemesi gerekliliğini ifade eden GDPR m. 20/4, aynı zamanda erişim hakkını düzenleyen GDPR m. 15'e ilişkin Gerekçe 63'te belirtilen ticari sırlar veya fikri mülkiyet hakları dahil olmak üzere başkalarının hak veya özgürlükleri ve özellikle yazılımları koruyan telif haklarının korunmasını da içerir[176]. Üçüncü bir kişinin fikri eserinin taşıma talebine konu edilmesi fikri hakların korunmasına ilişkin düzenlemelere aykırılık teşkil etmekte ise hakkın uygulanması söz konusu olmayacaktır. Benzer şekilde bir veri sorumlusunun geliştirmiş olduğu program, eser, algoritma veya yöntem yolu ile çıkarsamış olduğu verilerin bir başka veri sorumlusuna aktarılması pazardaki rakipler arasındaki rekabeti etkileyeceği gibi veri sorumlularının inovatif çalışmalarda bulunma motivasyonunu azaltacaktır. Ne var ki bir görüş, bu verilere erişim hakkı bulunduğu için taşıma hakkının kullanılamamasının tek başına beklenen amacı sağlayamayacağını, yalnızca taşıma sürecini yavaşlatacağını ileri sürmektedir[177]. Hakikaten de ilgili kişi, söz konusu çıkarsanan verilerini erişim hakkına dayanarak talep edebilir, dilerse bunları daha sonra bir başka veri sorumlusuna sağlayabilir. Her durumda veri taşınabilirliği hakkı, haksız uygulamalar ile fikri mülkiyet haklarının ihlaline izin veren bir yasal temel oluşturmamaktadır[178]. Bu durumda da fikri mülkiyet haklarını koruyucu düzenlemeler uygulama alanı bulabilecektir.

[176] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 12.
[177] **Martinelli**, S.: *Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights"*, Reins, L. (eds) Regulating New Technologies in Uncertain Times. Information Technology and Law Series 2019, Vol. 32, T.M.C. Asser Press, The Hague, s. 149.
[178] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 12.

Bu hususta önem arz eden ve veri taşınabilirliği hakkının kullanılabilirliğine ilişkin tartışma yaratabilecek konu dijital ortamlarda oluşan fikri mülkiyet hakları ve bunlarla ilgili lisans sözleşmeleridir. Dijital ortamlarda oluşturulan ve sunulan nitelikli fikri tapu (NFT) gibi dijital eserler yaygınlaştıkça bunlar üzerindeki hak sahipliği irdelenmeye başlamıştır. Bunun yanında sosyal medya platformlarının daha geniş kitlelere ulaşma imkânı tanıması, maliyetsiz olması gibi avantajlar dolayısıyla çeşitli eserlerin bu platformlar üzerinden kullanıcılara sunulduğu görülmektedir. Bunlarla ilgili çarpıcı bir örnek *Instagram*'ın kullanıcılara hesap oluşturma aşamasında sunduğu hüküm ve şartlarda yer almaktadır: Kullanıcı, *Instagram*'a içeriklerini kullanmak için "münhasır olmayan, telifsiz, devredilebilir, alt lisanslanabilir ve uluslararası bir lisans"[179] verir. Bu hüküm ile *Instagram*, paylaşılan içeriğin sahibi olmasa da hak sahibinin hemen hemen tüm haklarına sahip olmaktadır[180]. Söz konusu husus fikri mülkiyet hakları ve veri taşınabilirliği hakkı çerçevesinde değerlendirildiğinde, kayıt esnasında *Instagram*'a tanınan bu hakkın geçerliliğine ilişkin tartışmalar bulunmakla beraber, ilgili kişinin veri taşınabilirliği hakkını kullanmayı talep etmesi halinde lisans sağlamış olduğu bu kişisel veriler için ilgili kişinin hak sahipliği devam etmekte olduğundan bu yetkinin *Instagram*'a talebi reddetme hakkı tanımayacağı sonucuna varılabilir. Aksi halde birlikte çalışabilir sistemler bulunsa dahi veri taşınabilirliği hakkının icrası fikri mülkiyet ve lisans hakları engeline takılabilirdi.

[179] *Instagram*'ın güncellenmiş Kullanım Hükümleri için bkz. (https://help.instagram.com/581066165581870/?helpref=uf_share, E. T.: 06.05.2022).

[180] **Bosher**, H./**Yeşiloğlu**, S.: *An analysis of the fundamental tensions between copyright and social media: the legal implications of sharing images on Instagram*, International Review of Law, Computers & Technology 2019, Vol. 33, No.2, s. 173-174.

Ticari sırlar bahsinde ifade edildiği üzere fikri mülkiyet haklarının söz konusu olduğu taşıma taleplerinde de bağlamından arındırma tekniğinin uygulanması işlevsel bir çözüm olabilecektir[181].

§ 4. VERİ TAŞINABİLİRLİĞİ HAKKININ KULLANILMASI

I. İLGİLİ KİŞİNİN TALEP YÖNTEMİ VE KİMLİĞİNİN DOĞRULANMASI

KVKK m. 13 uyarınca ilgili kişi Kanun'un uygulanmasından doğan taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir. Bu doğrultuda çıkarılan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5. maddesinin birinci fıkrasında Kanun'un ilgili kişilerin haklarını düzenleyen 11. maddesine dayalı taleplerini *"...yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla…"* veri sorumlusuna ileteceği öngörülmüştür. GDPR'da ilgili kişinin haklarını kullanmak için izlemesi gereken özel bir yöntem öngörülmemiştir. Bu sebeple başvurunun sözlü veya yazılı olarak yapılması mümkündür. Bununla beraber uygun olduğu takdirde başvurunun elektronik olarak yapılmasının önünde de bir engel yoktur. GDPR m. 12/2'ye göre veri sorumlusu, ilgili kişinin haklarını kullanmasında kolaylık sağlamalıdır. Bu sebeple veri sorumlusunun taşınabilirlik talebini almak ve karşılamak için oluşturduğu bir

[181] **Malgieri**, s. 114.

sistem varsa bu da tercih edilebilecektir. Bununla beraber başvuranın gerçekten kişisel verisi işlenen kişi olup olmadığının tespiti gerekmektedir. Nitekim Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5. Maddesinin ikinci fıkrası, başvuruda bulunan kişinin ilgili kişi olduğunu tevsik edici ad, soyad, başvuru yazılı ise imza, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası ve diğer bilgilerin bulunmasını zorunlu tutmuştur.

GDPR m. 11/2'de veri sorumlusunun ilgili kişiyi teşhis edecek bir konumda bulunmadığını gösterebilmesi durumunda, veri sorumlusu tarafından gerçekleştirilebilecekse ilgili kişinin haberdar edilmesi; ilgili kişinin kimliğini tespite elverişli ek bilgilerin sağlanmaması halinde ilgili kişiye tanınan hakların kullanılamayacağı hüküm altına alınmıştır. İlgili kişinin hakları nezdinde genel bir sınırlama sebebi teşkil eden bu düzenleme, veri taşınabilirliği hakkının uygulanması bakımından da bir sınır oluşturmaktadır: Veri sorumlusu ilgili kişinin kimliğini tespit edememekte ise ve ilgili kişi tarafından kimliği teşhise elverişli ek bilgi sağlanmamışsa veri taşınabilirliği hakkı da kullanılamayacaktır.

Aşağıda[182] gönderici ve alıcı veri sorumlularının GDPR'da öngörülen genel yükümlülüklere tabi olduğu, kişisel verilerin taşınması sırasında ve sonrasında karşılaşılabilecek risklere karşı uygun güvenlik önlemlerini almakla yükümlü oldukları açıklanmaktadır. Kişisel verilerin güvenliğinin sağlanması veri sorumlularının en önemli yükümlülüklerinden biri olmakla beraber konu veri taşınabilirliği hakkı olduğunda kişisel verilerin gerçek hak sahibi tarafından ileri sürülen talebe uygun, idari ve teknik açıdan en makul ve güvenli yöntemle bir başka

[182] Bkz. İkinci Bölüm, §2, III.

veri sorumlusuna iletilmesi büyük önem taşımaktadır. Keza talebin gerçek hak sahibince ileri sürülmemiş olması isim benzerliği gibi basit bir ihtimalden kaynaklanabileceği gibi bir veri hırsızlığı girişimine de işaret ediyor olabilir. Söz konusu tehlike ise kişisel verilerin yanlış bir izlenimle hukuki bir dayanağa bağlı görünen talep neticesinde pek çok farklı veri sorumlusuna kontrolsüzce ulaşmasına sebep olabilecek niteliktedir. Açıklanan nedenlerle Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in ilgili kişinin haklarını kullanmak üzere veri sorumlusuna başvuru usulüne ilişkin düzenlemesinde olduğu gibi GDPR m. 11 uyarınca da veri taşınabilirliği hakkının kullanılabilmesi için ilgili kişinin kimliğinin teşhis edilmesi gerekmektedir. Özellikle talebe konu kişisel verinin büyüklüğü, özel nitelikli veri niteliğinde olup olmadığı, şüpheli işlem durumlarında talebin karşılanmasından önce ilgili kişinin kimliğinin iki kez kontrol edilmesi[183], güvenlik düzeyi artırılmış doğrulama prosedürü benimsenmesi gibi yöntemler benimsenmelidir[184]. Öyle ki doktrinde ifade edildiği üzere bir anlık kimlik sahtekarlığı ömür boyu kişisel veri ihlaline dönüşebilir[185].

Hakkın kullanımı ve güvenliği açısından gündeme gelen bu konunun önem arz eden tarafı, veri sorumlusunun güvenliği sağlamaya yönelik faaliyeti doğrultusunda ilgili kişiden ek bilgi istemesinin zorunlu olup olmaması meselesidir. Bir taraftan ilgili kişinin kişisel verilerini korumak için kimliği teşhise elverişli bilgi gerekirken diğer taraftan bu amaçta gereksiz verinin işlenmesi de veri minimizasyonu ilkesine ters düşecektir[186]. Örneğin bir fotoğraf depolama uygulaması kullanmakta olan ilgili

[183] **Swire/Lagos**, s. 375.
[184] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 13; **Lynskey**, Data Portability, s. 506.
[185] **Swire/Lagos**, s. 380.
[186] **Bozdag**, s. 5.

kişinin bu kişisel verilerini bir başka uygulamaya taşıma talebini karşılamak üzere ilk/gönderici veri sorumlusunun, ilgili kişinin vatandaşlık numarası, sosyal güvenlik numarası veya kan grubu gibi bir bilgi ile kimlik teşhisinde bulunması her ne kadar veri güvenliği bakımından gerekli ise de uygulamanın amaçları doğrultusunda kalmayan bir kişisel verinin işlenmesini gerektirecektir. Bahsi geçen örnekte depolanan fotoğraflardan ilgili kişi tarafından önceden belirlenmiş küçük kesitlerin pek çok seçenek içinden seçtirildiği bir yöntem fazladan veri işlemeyi gerektirmediğinden ihtiyaca cevap verebilecektir. Ancak bu halde dahi veri sorumlusunun böyle bir ek maliyeti üstlenmesinin kabul edilebilirliği tartışma konusudur[187]. Böyle bir durumda veri sorumlusunun maruz kaldığı ek maliyetleri ilgili kişiye yansıtması ile ortaya çıkacak olumsuz sonuç, veri taşınabilirliği hakkının kullanılması ile sağlanan faydayı aşıyorsa veri sorumlusunun ek maliyetleri üstlenmesinin zorunlu olmadığı sonucuna varılabilir. Özellikle küçük ölçekli teşebbüsler bakımından önem arz eden bu konuda denge testi yapılarak ağır basan menfaatin belirlenmesi yerinde olacaktır.

II. VERİ SORUMLUSUNUN TALEBE CEVAP VERMESİ VEYA TALEBİ REDDETMESİ

Veri sorumlusunun, GDPR Bölüm III'te öngörülen hakların kullanılması için ilgili kişiden gelen talepleri, GDPR m. 12/3 uyarınca gereksiz bir gecikme olmaksızın talebin alındığı tarihten itibaren bir ay içinde cevaplandırması gerekmektedir. KVKK m. 13'te de benzer şekilde veri sorumlusunun başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırması öngörülmüştür. Buna karşılık GDPR'da sürenin uzatılmasını

[187] **Bozdag**, s. 5.

gerektiren sebeplerin varlığı halinde yine bir ay içinde bu sebeplerin süre uzatımına ilişkin bilgi ile birlikte ilgili kişiye bildirileceği ve uzatma süresinin iki ayı aşamayacağı düzenlemesi yer almaktadır. Ayrıca GDPR m. 12/4'e göre, veri sorumlusunun ilgili kişinin talebi ile ilgili cevap vermemesi halinde de gecikmeye mahal vermeden ve talebin alındığı tarihten itibaren en geç bir ay içinde ilgili kişiye, sessiz kalma sebepleri, bir denetim makamına şikâyette bulunma hakkı ve kanun yoluna başvurma olanağı hakkında bilgi verilmelidir. GDPR m. 12/1 uyarınca veri sorumlusu tarafından sağlanan bildirimin açık ve kolay anlaşılır olması gerekir ki bu özellikle karışık veri setleri söz konusu olduğunda ilgili kişinin anlamasını kolaylaştıracak şema ve yöntemlerin kullanılmasını gerektirebilir[188]. Her halükârda GDPR m. 12/5'te veri sorumlusu tarafından sağlanan cevabın ücretsiz olacağı, taleplerin asılsız ve önceki talepleri içerik olarak ya da makul süre geçmeden tekrarlar nitelikte olması[189] örneklerinde olduğu gibi ölçüsüz olduğu hallerde bu husus veri sorumlusu tarafından gösterilmek şartıyla cevabın makul bir ücret karşılığı sağlanmasının veya taleple ilgili işlemin reddedilmesinin söz konusu olabileceği öngörülmüştür. İlgili kişinin taleplerinin ölçüsüz olduğunun ortaya konmasında genel sistem maliyetleri talebi reddetmek bakımından haklı bir gerekçe oluşturmamaktadır[190]. Veri taşınabilirliği hakkının kullanılması talebinde bulunulan veri sorumlusunun talebe cevap verirken, kişisel verileri ileteceği diğer veri sorumlusunun söz konusu verileri koruyacak güvenlik önlemlerini almadığından

[188] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 18.
[189] Taleplerin asılsız ve ölçüsüz olması ile ilgili olarak bkz. (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/#:~:text=A%20request%20may%20be%20excessive,overlaps%20with%20other%20requests . E. T.: 07.06.2022).
[190] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 15.

bahisle ilgili kişinin talebini reddedip reddedemeyeceği tartışılabilir[191]. Bu hususta veri sorumlusunun talebi doğrudan bu gerekçe ile reddedemeyeceği ancak alıcı veri sorumlusunda tespit ettiği bir güvenlik zaafiyeti olması halinde ilgili kişiyi bilgilendirerek bu doğrultuda taşıma işlemine devam etmesi gerektiği düşünülebilir. Ancak her halde alıcı veri sorumlusunun alması gereken güvenlik önlemlerinin gönderici veri sorumlusunca denetlenmesi zorunlu olmadığı gibi alıcı veri sorumlusunun gerekli güvenlik önlemlerini almamış olması gönderici veri sorumlusu bakımından bir sorumluluk doğurmaz.

III. GÖNDERİCİ VE ALICI VERİ SORUMLULARININ HAK VE YÜKÜMLÜLÜKLERİ

Gönderici veri sorumlusunun ilgili kişiye yönelik kişisel veri işleme faaliyeti devam ettiği sürece ve alıcı veri sorumlusunun ilgili kişiye yönelik kişisel veri işleme faaliyetinin başladığı andan itibaren işleme faaliyetini GDPR'da öngörülen genel ilkelere ve kurallara uygun olarak gerçekleştirmesi gerekmektedir. Dolayısıyla kişisel veri işleme faaliyetinde bulunan veri sorumlusu her durumda kişisel verilerin korunması mevzuatından doğan ve hak ve yükümlülükleri dairesinde hareket etmeli; aydınlatma yükümlülüğünü, uygun güvenlik düzeyini sağlama yükümlülüğünü, bildirim yükümlülüğünü ve mevzuattan doğan diğer yükümlülüklerini yerine getirmelidir. Kişisel verilerin işlenmesinde KVKK ve GDPR'da ortak olarak öngörülen hukuka uygunluk, adalet ve şeffaflık, amacın sınırlandırılması, veri minimizasyonu, doğruluk, saklama süresinin sınırlandırılması, bütünlük ve gizlilik, hesap verebilirlik ilkelerine riayet etmelidir.

[191] **Vanberg**, s. 16.

Veri taşınabilirliği hakkı söz konusu olduğunda bu ilkelerden özellikle veri minimizasyonunun sağlanması önem taşır. GDPR'ın "Kişisel verilerin işlenmesine ilişkin ilkeler" başlıklı 5/1-c maddesinde kişisel verilerin işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanlarla sınırlı olduğu ve KVKK'nın "Genel İlkeler" başlıklı 4/2-ç maddesinde kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçüsü olması gerektiği ifade edilmiştir. Verilerin en az seviyeye indirilmesi anlamına gelen veri minimizasyonu ilkesi doğrultusunda ikinci/alıcı veri sorumlusunun taşınma talebine konu amaç bakımından işlemesi gereken verilerin neler olduğunu tespit etmesi, bu amacı aşan veya gereksiz herhangi bir veriyi toptancı bir yaklaşımla işlememesi[192] gerekmektedir. Bu açıdan gönderici veri sorumlusunun da iletilecek kişisel verilerin aşırı olmamasını sağlaması gerekmektedir[193]. Diğer taraftan ilgili kişinin ilk/gönderici veri sorumlusunda bulunan kişisel verilerinin silinmesini talep etmesi yahut veri sorumlusu ile ilgili kişi arasındaki ilişkinin kısmen devam ediyor olması hallerinde ilk/gönderici veri sorumlusu da veri minimizasyonu ilkesine riayet etmeli, işlemenin hukuki dayanağı bulunmuyorsa işleme faaliyetine son vermelidir.

KVKK m. 12/1'de ve GDPR m. 24'te veri sorumlularına, kişisel verilerin güvenliğini sağlama yükümlülüğü getirilmiştir[194]. Bu anlamda veri sorumlusu kişisel verilerin güvenliğini sağlamak için her türlü teknik ve idari tedbiri almalı, örneğin

[192] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 7.
[193] **Article 29 Data Protection Working Party**, *Guidelines on Right to Data Portability*, s. 7.
[194] Kişisel verilerin güvenliğinin sağlanması için gerekli önlemleri almak ve denetim mekanizmalarını oluşturmak aynı zamanda bir güvenlik açığı olduğunda bunu zamanında tespit edebilmek ve derhal söz konusu duruma son verebilmeyi de içerir. Bu sebepledir ki veri sorumlularına, işledikleri kişisel verilere hukuka aykırı bir erişimin gerçekleşmesi durumunda bunu ilgilisine ve denetim makamına en kısa süre içinde bildirme yükümlülüğü getirilmiştir. KVKK'da bu hususta bir süre öngörülmemiş olup GDPR m. 33'te denetim makamına yapılacak bildirimin ihlalden haberdar olma anından itibaren en geç 72 saat içinde gerçekleşmesi gerektiği hüküm altına alınmış ve Türk kişisel veri koruma otoritesi tarafından verilen 24.01.2019 tarih ve 2019/10 sayılı kararlarda da bu süre benimsenmiştir. GDPR kişisel veri güvenliğinin sağlanması için KVKK'da bulunmayan bir dizi yükümlülük öngörmüştür. Bu kapsamda GDPR m. 35, veri işleme faaliyetinde ortaya çıkabilecek risklerin tespiti ve değerlendirilmesi için veri koruma etki analizi ("*data protection impact assessment*") yapılmasını, m. 37 uyarınca belirli şartlarda veri koruma görevlisinin ("*data protection officer-DPO*") bulundurulmasını zorunlu hale getirmiştir.

çalışanlarını kişisel verilerin korunması konusunda bilgilendirmeli, yetki matrisi oluşturmalı, kişisel verilere yetkisiz erişimi engelleyecek yazılım altyapılarını sağlamalı veya diğer gereklilikleri karşılamalıdır. Kişisel verilerin korunması ve olası riskleri en aza indirmek için uygun güvenlik düzeyinin alınması da her iki veri sorumlusu açısından yükümlülük teşkil etmektedir. İletim sürecinin başından sonuna kadar her aşamada veri hırsızlığı veya bilgisayar korsanlığı gibi riskler mevcuttur. Üstelik taşınan veri sağlık verisi gibi özel nitelikli veri olduğunda veri kaybı, verinin yanlış kullanımı ve risk, kişisel verinin niteliğinden dolayı daha yüksektir. Bu nedenle taşınan verinin özel nitelikli veri olduğu durumlarda daha yüksek güvenlik önlemlerinin alınması şarttır[195]. Öte yandan veri taşınabilirliği hakkının temel gereksinimlerinden bir tanesi birlikte çalışabilirlik olmakla beraber hususunda doktrinde, ironik olarak, birlikte çalışabilir sistemlerin kişisel verilerin güvenliğini tehdit eden ana unsur olarak görülmese de sistemler arasında tek tip süreçlerin uygulanması dolayısıyla güvenlik ihlallerinin sayısını artırabilecek nitelikte olduğuna vurgu yapılmıştır[196]. Her iki veri sorumlusu nezdinde de gerçekleşebilecek güvenlik açıklarının önemli kişisel veri ihlallerine sebep olacağı ve bu nedenle iki tarafın da veri güvenliğini sağlamak yönünden eş derecede yükümlülük altında olduğu kuşkusuzdur. Ne var ki burada her iki veri sorumlusundan da veri güvenliğinin sağlanması konusunda beklenen dikkat ve özen veri sorumlusu ile veri işleyen arasındaki ilişki ile karıştırılmamalıdır. Veri sorumlusu ile veri işleyen arasındaki müteselsil sorumluluk meselesinde, bir tarafta kişisel verilerin işlenmesine ilişkin kontrolü elinde bulunduran ve talimat verme yetkisine sahip olan veri sorumlusu, diğer tarafta ise veri

[195] **Barth**, M.: *A Case Study on Data Portability Measuring the Maturity of Data Portability Exports in IoT Platforms*, Datenschutz und Datensicherheit 2021, Vol. 3, s. 197.
[196] **Vanberg**, s. 15.

sorumlusunun talimatları çerçevesinde hareket eden veri işleyen bulunmaktadır. Buna karşılık gönderici ve alıcı veri sorumluları arasında emir-talimat ilişkisi bulunmamakta, her ikisi de bağımsız birer veri sorumlusu olma özelliklerini korumaktadır. Bu sebeple veri güvenliğine ilişkin bir ihlal halinde ihlalin kimden kaynaklandığı tespit edilecek ve yalnızca veri güvenliğini sağlamaya yönelik tedbirleri almadığı kanaatinde bulunulan veri sorumlusu açısından sorumluluk söz konusu olacaktır.

Birlikte çalışabilirliğin ve veri taşınabilirliğinin veri güvenliğini riske atmasını önlemek için veri taşınabilirliğine ilişkin düzenlemelerde doğrudan güvenlik standartlarının öngörülmesi yerinde bir uygulama olabilir[197]. Bu anlamda hakka ilişkin düzenlemelerde sektörel düzenleyicilere yetki vermek suretiyle sektörel bazı standartların öngörülmesi yolu ile de güvenlik önlemlerinin belirlenmesi mümkündür.

Gönderici veri sorumlusunun veri taşınabilirliği hakkı açısından en önemli yükümlülüklerinden birisi talepte bulunan kişinin gerçekten ilgili kişi olup olmadığını kontrol etmektir. İlgili kişinin kimliğini herhangi bir şüpheye yer vermeden tevsik etmesi ile süreç başlayacaktır. Sürecin devamında veri taşınabilirliği talebinde bulunan ilgili kişiden işlemin devam etmesi için onay alınması, iletme işlemi tamamlandıktan sonra alıcı veri sorumlusunun derhal alınan güvenlik önlemleri açısından ilgili kişiye bilgilendirmede bulunması ve uyguladığı şifreleme gibi bir yöntem varsa bunların en kısa zamanda uygulanabilmesi için ilgili kişinin teşvik edilmesi veri güvenliğinin sağlanması kapsamında düşünülebilir.

[197] Veri taşınabilirliğinde ortaya çıkan gizlilik ve güvenlik risklerine ilişkin ***Swire*** tarafından önerilen Taşınabilirlik Etki Değerlendirmesi ("*Portability Impact Assessments*") ve diğer gizlilik çözümlerine yönelik detaylı bilgi için bkz. **Hondagneu-Messner**, S.: *Data Portability: A Guide and a Roadmap,* Rutgers Computer and Technology Law Journal 2021, Vol. 47, No. 2, s. 265-273.

ÜÇÜNCÜ BÖLÜM

VERİ TAŞINABİLİRLİĞİ HAKKININ REKABET HUKUKU BOYUTUYLA DEĞERLENDİRİLMESİ

§ 5. KİŞİSEL VERİLERİN KORUNMASI HUKUKU VE REKABET HUKUKU İLİŞKİSİ

I. EKONOMİK BİR DEĞER OLARAK KİŞİSEL VERİ

Humby'nin "Veri yeni petroldür"[198] *("data is the new oil")*[199] deyişi, günümüz bilişim ve teknoloji alanındaki çalışmalarda hoş bir veciz olmaktan öte mühendislik, pazarlama, ekonomi, hukuk ve diğer pek çok alanda veri biliminin hangi inisiyatifle geliştiğini özetlemektedir. Veriyi para yerine yeni petrol olarak tanımlayan metaforda petrol, doğal kaynaklar ile ekonominin kaynak alanları arasında bir örtüşme içinde bulunur. Bu metafor verinin petrol gibi işlenmeden de bir değere sahip olduğu algısını doğurabilirse de *Humby*'nin öz olarak ifade etmeye çalıştığı bu değildir. Nitekim veri "petrol gibi" değil, "yeni petrol"dür[200]. Verinin işlenmesi ile bir değere kavuştuğunun kabul edilmesi halinde verinin bizatihi kendisinin değil[201] veri sahipliğinin ekonomik

---

[198] Verinin ekonomik değerini bir altyapı *("data as infrastructure")* veya varlık *("data as an asset")* olarak açıklamaya çalışan görüşler de bulunmaktadır. OECD (2015) veriyi altyapı olarak *("data as infrastructure")* değerlendirirken bunun su şebekesi veya telefon ağları gibi temel ekonomik faaliyetlerin yerleşke edindiği platform olduğu görüşünden hareket etmekte, verinin petrol gibi olmadığını, kullanılmakla tükenmediğini, bazı veriler yönünden sınırlılık/kıtlık söz konusu olamayacağından bunların rakipsiz olduğunu *("data as non-rivalrous"*), bazı verilerin ise toplanma yönünden kıtlık yarattığı ve bu sebeple de sermaye malı *("data as a capital good")* olarak değerlendirilebileceğini belirtmektedir. Bu açıdan değer, veri sahipliğine değil, verinin kullanıldığı bağlama verilmektedir. Veriyi varlık olarak *("data as an asset")* değerlendirenler açısından varlık her ne kadar kendiliğinden ekonomik değeri bulunan önemli bir terime yönelse de merkeze veri yönetimini alan ve ekonomik öneme ikinci planda değinen bir metafor olarak ortaya çıkar. Konu hakkındaki detaylı çalışma için bkz. **Nolin**, J. M.: *Data as oil, infrastructure or asset? Three metaphors of data as economic value*, JICES 2019, Vol. 18(1), s. 32-39; **OECD**, *Data-Driven Innovation: Big Data for Growth and Well-Being*, (https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en#page1, E. T.: 07.01.2022).

[199] The Economist (2017), *Regulating the internet giants: The world's most valuable resource is no longer oil, but data*, (https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, E. T.: 16.12.2021).

[200] **Nolin**, s. 33-34.

[201] **Colangelo**, G./**Maggiolino**, M.: *From fragile to smart consumers: Shifting paradigm for the digital era*, Computer Law & Security Review 2019, Vol. 35, s. 173; **Krämer**, s. 265.

bir değeri olduğu da ortaya çıkacaktır. Veriyi kendiliğinden ekonomik bir değeri ihtiva eden bir parça olarak değerlendirenler de bulunmakla beraber konuya ilişkin tüm görüşlerin ortak noktası günümüz dünyasında verinin ekonomik menfaatle sıkı ilişki içinde bulunduğunun kabul edilmesidir.

Veri temelli ekonomi, bilişim teknolojilerindeki ilerleme, gözetim teknolojilerindeki gelişmeler verilerin ve özellikle de kişisel verilerin hızlı ve kolay biçimde toplanmasını, saklanmasını, aktarılmasını ve bunlara benzer çeşitli işleme faaliyetlerine konu olmasını sağlarken aynı zamanda bu kişisel verileri elinde bulunduranlar tarafından, sınırsız sayıda amaç doğrultusunda kullanılabilmektedir. Bu itibarla veri yalnızca dijital pazarlarda değil, tüm pazarlarda veri, müşteri tercihlerinin belirlenmesi, işletme stratejilerinin oluşturulması, inovasyon süreçlerinin desteklenmesi bakımından bir hammaddeye dönüşmüştür. Bununla beraber nesnelerin interneti, yapay zekâ ve algoritmalar gibi uygulamalar kişisel olan ve olmayan verilerden beslenmekte, bu sebeple de dijital pazarlarda veri diğer pazarlarda olduğundan daha etkin bir kullanım alanına ve gerekliliğe ulaşmaktadır. Öyle ki ilk girdi olarak sürece dahil olan veri salt bu şekli ile varlığını sürdürmemekte, bu verilerinin üst verilerinin alınması, gözlenen, çıkarsanan veya türetilmiş verilere dönüştürülmesi, dönüştürülen veri üzerinde de aynı işlemlerin tekrarlanabilmesi verinin yalın hali ile sağladığı kullanım imkânlarını genişletmektedir. Veriye duyulan ihtiyacın yoğun olduğu dijital pazarlarda özellikle kullanıcı merkezli uygulamaların artması veri kümesi içindeki kişisel verilerin ekonomik bir değere dönüşmesini sağlamıştır.

Çevrimiçi alışveriş uygulamaları, mesajlaşma servisleri, fotoğraf ve video paylaşım araçları gibi dijital platformlarda kullanıcılar bir hizmet alırken genellikle

bunun karşılığında parasal bir ödeme yapmazlar. Buna rağmen söz konusu dijital platformlarda sunulan hizmetlerin karşılıksız olduğunu söylemek güçtür[202]. Platform işleticilerinin sağladıkları hizmetleri hiçbir maddi çıkarları bulunmaksızın sunmalarının ekonomik olarak kabul edilebilir olmadığı da göz önüne alındığında bu hizmetler kapsamında kullanıcıların platform işleticileri ile baş başa olmadıkları da ortaya çıkmaktadır. Dijital platformlarda elde edilen gelirin önemli bir kaynağını platform işleticilerinin kullanıcılarla buluşturmak için alan sağladıkları reklam verenler oluşturmaktadır. Profilleme ve kişiselleştirilmiş reklam uygulamaları[203] gibi yöntemlerle reklam verenler, kendileri ile ilgilenmeyen kullanıcılardan ziyade ürün veya hizmet alma potansiyeli daha yüksek olan kullanıcılarla doğrudan iletişime geçebilmekte ve böylece kaynaklarını daha verimli kullanmış olmaktadır[204]. Benzer şekilde platformların yeni bir ürün veya hizmet geliştirmek ya da var olanı yükseltmek için kullandıkları hammadde de yine kullanıcı verisi olmaktadır. Bu sebeple kullanıcıların dijital platformlarda aldıkları hizmet karşılıksız kalmamakta, kullanıcılar para ödemedikleri durumlarda dahi farkında olarak veya olmayarak kişisel verileri ile karşılık sağlamaktadır[205]. Elbette dijital olmayan pazarlarda da veri sorumlularının edindikleri kişisel veriler pazarda önemli bir iktisadi güç

---

[202] **Colangelo/Maggiolino**, Digital Era, s. 174; **Martinelli**, s. 134; **Javeed**, U.: *Data and Competition Law: Introducing Data As Non-Monetary Consideration and Competition Concerns in Data-Driven Online Platforms*, 2021, s. 6.

[203] Avustralya Rekabet ve Tüketici Komisyonu ("*Australian Competition and Consumer Commission*"- ACCC) 2019 yılında çıkardığı *Digital Reports Inquiry* raporunda, gelirlerini bir reklam verenden aldıkları ücret ile sağlayan çoğu platformun kullanıcıların kişisel verilerinin iş modelinin merkezinde bulunduğunu ifade etmektedir. Komisyon'un 2022'de çıkardığı *Digital Platform Services Inquiry* isimli geçici raporda ise reklam verenlerin bu yolla çok daha geniş bir veri havuzuna erişeceği ve bu yolla hedef kitleyi en doğru şekilde belirleyecek ve yakalayacak aram terimleri vasıtasıyla öne çıkabileceği belirtilmektedir. Bkz. **ACCC**, *Digital Platforms Inquiry*, 2019, (https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, E. T.: 06.05.2022); **ACCC**, *Digital Platform Services Inquiry*, 2022, (https://www.accc.gov.au/system/files/DPB%20-%20DPSI%20-%20March%202022%20-%20Full%20interim%20report%20-%2031%20March%202022.pdf, E. T.: 06.05.2022).

[204] Bkz. Üçüncü Bölüm, §1, B, 5.

[205] **Javeed**, s. 6.

oluşturmaktadır. Ancak dijital platformlarda diğer hizmetlere kıyasla çok daha fazla miktarda ve hızlı kişisel verinin işlenmesi, dijital platformların iktisadi karakterleri, yoğunlaşma durumları ve buna bağlı olarak kullanıcıların bu platformlara bağımlılıkları bir taraftan kişisel verilerinin korunması hukuku içinde endişeler meydana getirirken diğer taraftan kişisel verilerin veri sorumlusu dijital platformlara sağladığı rekabet avantajı, bu avantajın kullanıcı aleyhine kullanılmasını önlemek ve pazardaki rekabeti korumak adına rekabet hukuku incelemelerini de zorunlu kılmaktadır. Bu pazarlarda kişisel verinin ürün veya hizmetle iç içe geçmiş olması kişisel verilerin ve rekabetin korunması alanlarında net çizgilerin çizilmesini de engellemektedir.

II. KİŞİSEL VERİLERİN KORUNMASI İLE REKABET HUKUKU ETKİLEŞİMİNİN GELİŞİM SÜRECİ

Kişisel verilerin korunması ve rekabetin korunması konusunda etkileşimli bir ilişki bulunduğu Avrupa'da rekabet otoritelerinin başlangıçta kabul etmediği[206], kişisel verilerin rekabeti etkileme yeteneğini zaman içerisinde anladığı ve politikalarını da bu doğrultuda geliştirmeye başladığı bir mesele olmuştur[207]. Kişisel verilerin korunmasına ilişkin geniş çaplı düzenlemeyi getiren GDPR'da ilgili kişilerin kişisel verileri üzerinde daha fazla kontrol imkânı sağlayarak bilgi asimetrisini azaltma[208] ve rekabeti destekleme amacı bulunmaktadır. Bu husus tartışmalara sebep

---

[206] **Colangelo**, G./**Maggiolino**, M.: *Data Protection in Attention Markets: Protecting Privacy through Competition?*, Journal of European Competition Law & Practice 2017, Vol 8, No.6, s. 364-365. *Yazarlar* bu durumu, rekabet hukukunun bu zamana dek hiçbir zaman dijital platformların kişisel veri ve dijital kimlik ile uğraşan uygulamaları için bir kılıç olarak kullanılmadığını belirterek ifade etmektedir.

[207] **Zanfir-Fortuna**, G./**Ianc**, S.: *Data Protection and Competition Law: The Dawn of 'Uberprotection'*, Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds.), Edward Elgar Publ'g 2019, s. 249-250.

[208] **Vezzoso**, S.: *Competition Policy in Transition: Exploring Data Portability's Roles*, Journal of European Competition Law & Practice 2021, Vol. 12, No.5, s. 362.

olduğu gibi piyasalarda rekabeti düzenlemek ve denetlemek amacıyla çıkarılan DMA ve DSA gibi diğer düzenlemelerde de kişisel verilerle bağlantılı tedbir, yükümlülük ve yaptırımlar bulunmaktadır. Görüleceği üzere sınırları net olarak birbirinden ayrılamayan bu iki alanda düzenleyici otoritelerin ve kanun koyucuların alışılagelmiş düşünce tarzı ve yorum yöntemleri ile problemleri çözmesi veya bir diğerini yok sayan düzenlemeler yapması mümkün değildir. Nitekim veri koruma ve rekabet düzenlemeleri temelde farklı amaçlara hizmet etmekte ise de gizliliğe ilişkin konular sırf bu sebeple rekabet hukuku çerçevesinde yapılan değerlendirmelerden hariç tutulamaz[209].

A. *Asnef-Equifax/Ausbanc* Kararı[210]

2006 senesinde Avrupa Birliği Adalet Divanı'nın önüne gelen olayda finansal kredi kuruluşları birliği olan *Asnef*'in kredi verenler ve müşteriler arasında kredi ilişkisinden doğan risklerini azaltmak ve müşterilerin daha etkin biçimde kredi kullanabilmesini sağlamak için oluşturduğu çevrimiçi kayıt sistemi ile kredi verenlere bilgi paylaşımı yapması inceleme konusu olmuştur. Paylaşılan bilgiler arasında müşterilerin daha önceki borçlarına ilişkin ödeme bilgileri ve temerrüt durumları gibi bilgiler bulunmaktadır. Söz konusu bilgilerin kişisel veri niteliği taşıdığı yönünde kuşku bulunmamakla beraber kararda kişisel verilerin hassasiyetine[211] yönelik

[209] **Autorité de la Concurrence and Bundeskartellamt**, *Competition Law and Data Report*, 10.05.2016, (https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2, E. T.: 06.05.2022), s. 23.

[210] Case C-238/05, *Asnef-Equifax et al v. Asociaci ón de Usuarios de Servicios Bancarios*, 23.11.2006, EU:C:2006:734.

[211] Hassasiyet ("*sensitivity*") ifadesi ile kişisel verinin özel nitelikli olması değil korunmasını gerektiren sebepler kast edilmektedir.

sorunların rekabet hukuku ile ilgili olmadığı ve bunların, kişisel verilerin korunmasına yönelik kurallar dahilinde çözümlenmesi gerektiği belirtilmiştir[212].

B. *Google/DoubleClick* Kararı[213]

2008 senesinde *Google*'ın çevrimiçi reklamcılık hizmeti sunan *DoubleClick* ile birleşme girişiminin bildirilmesi üzerine başlatılan soruşturmada Avrupa Komisyonu *Google* ve *DoubleClick*'in aynı pazarda birbirlerine rakip olmadıkları, taraflar arasındaki anlaşma gereği reklam verenler dışında, taraflar da dahil olmak üzere üçüncü kişilerin kullanıcı verilerine erişemeyeceği ve taraflar arasında anlaşmaya konu olacak verilere pazardaki diğer teşebbüslerin de ulaşması imkânı bulunduğu gerekçeleri ile birleşme işlemine onay vermiştir. Federal Ticaret Komisyonu da birleşme işlemini benzer gerekçelerle onaylamış, yalnızca gizliliğe ilişkin gerekliliklerin geniş ve hızlı gelişen endüstrilerde rekabeti sekteye uğratabileceği vurgusu yapmıştır[214]. *Asnef-Equifax* kararının aksine bu kararda kişisel verilere erişebilme ve bunları kullanarak rekabeti etkileme potansiyeli Avrupa Komisyonu tarafından incelemeye dahil edilmiştir. Federal Ticaret Komisyonu'nun gizliliği rekabet hukuku ve politikaları alanındaki soruşturmaların dışında ancak buna paralel bir alan olarak görmesi ise *Asnef-Equifax* kararında Avrupa Komisyonu'nun gösterdiği yaklaşımla aynıdır.

C. *Facebook/WhatsApp* Kararı[215]

---

[212] Aynı ifadeye karar ilişkin Hukuk Sözcüsü'nün Görüşü'nün 56 numaralı paragrafında da yer verilmektedir.
[213] Case COMP/M.4731, *Google/DoubleClick*, 11.03.2008.
[214] FTC: Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No: 071-0170, (https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf, E. T.: 06.05.2022).
[215] Case COMP/M. 7217, *Facebook/WhatsApp*, 03.10.2014.

2014 senesinde *Facebook*'un kendisine kıyasla çok daha az kullanıcısı ve cirosu bulunan mesajlaşma uygulaması *Whatsapp*'ı satın alma girişimi birden çok pazarda rekabeti olumsuz etkileyecek bir birleşme endişesi uyandırmışsa da Avrupa Komisyonu söz konusu ilgili pazarlarda iki şirketin birbirine yakın rakip olmadıkları, *Whatsapp* kullanıcılarının büyük bir kısmının Facebook uygulamasını da kullanmakta oldukları, diğer uygulamalarda da gizliliğe dair politikaların benimsenmesinin *Facebook*'un *Whatsapp*'ı çevrimiçi reklam yayınlayabileceği bir mecra olarak görmekten uzaklaştıracağı, kullanıcı verileri bakımından *Facebook*'un tekel gücüne sahip olmadığı ve diğer uygulamalarca da kullanıcı verisinin toplanmakta olduğu gibi gerekçelerle birleşmeye onay vermiştir.

Karara ilişkin çarpıcı bir nokta, kararda veri taşınabilirliği ve birlikte çalışabilirlik hususlarının da irdelenmiş olmasıdır. Komisyon, çeşitli uygulamalar arasında kullanıcıların tercihlerini değiştirirken bir uygulamada var olan verilerinin ve geçmişinin kullanıcılar bakımından önemli bir geçiş maliyeti yarattığını ifade etmekle birlikte *Facebook/Whatsapp* davasında bu anlamda bir sorun bulunmadığı sonucuna varmıştır. Bu değerlendirmede uygulamalar aracılığıyla gerçekleştirilen iletişimin karakteristik olarak önemli ölçüde kısa ve spontane sohbetlerden oluştuğu, kullanıcının halihazırda kullanmakta olduğu uygulamada bulunan geçmişini silmediği müddetçe bu verilere erişimi mümkün olduğundan bir geçiş maliyeti oluşturmadığı ve ayrıca *Whatsapp*'ta yer alan kişi listesinin, kullanıcının rızası doğrultusunda rakip bir uygulamaya taşınabileceği hususlarına değinilmiştir[216]. Birlikte çalışabilirlik yönünden ise Komisyon, davanın görüldüğü sırada davaya konu tarafların ana rakiplerinin hiçbiri tarafından birlikte çalışabilirlik imkânının sunulmadığını ve bunun

[216] Case COMP/M. 7217, *Facebook/WhatsApp*, 03.10.2014, par 113, 134.

Whatsapp, Facebook Messenger veya diğer iletişim araçlarının pazara giriş ve genişlemelerini sürdüren bir unsur olmadığını değerlendirilmiştir[217]. Dikkat çeken konu, veri taşınabilirliği hakkının 2016'da kabul edilen ve 2018'de yürürlüğe giren GDPR ile bir ilgili kişi hakkı olarak tanınmasından önce henüz hazırlık safhasında iken Komisyon'un rekabet alanında inceleme kapsamına veri taşınabilirliğini dahil etmiş olmasıdır.

D. *Sanofi/Google/DMI JV* Kararı[218]

2016 yılında, dünya genelinde sağlık ürünleri hakkında araştırma, geliştirme, üretim ve pazarlama işleri ile iştigal eden ilaç firması *Sanofi*'nin, çok uluslu ve internet temelli arama ve ürün geliştiricisi *Google*'ın yaşam bilimleri ile ilgili çalışmalar yürüten yan kuruluşu *Verily* ile bir ortak girişim oluşturma talebi Avrupa Komisyonu tarafından değerlendirmeye alınmıştır. Ortak girişim kurulması hedeflenen alanda ilgili pazar insülin, insülin verme sistemleri, glikoz izleme sistemleri, entegre bir dijital tıp platformu ile yürütülen diyabet tedavisine yönelik hizmetler ve veri analizi hizmetleri olarak tanımlanmıştır. İnceleme genel olarak *Google*'ın sağlık verilerinin analizinde kullanılan veri araçları veya hizmetlerini rakip teşebbüslere sunmayı reddetmesinin dışlayıcı bir etki yaratarak pazarda rekabeti olumsuz etkileyip etkilemeyeceği hususunun araştırılmasına dayanmaktadır. Nihayetinde Komisyon, pazarı olumsuz etkileyecek davranışlara ilişkin tereddütlerin yerinde olmadığı kanaatine varmıştır.

Komisyon bu kararda her ne kadar gizliliğe ilişkin endişelerin Avrupa Birliği rekabet hukuku kurallarının değil veri koruma hukuku kurallarının kapsamına dahil olduğunu belirtmişse de kararda veri taşınabilirliğine ilişkin bir değerlendirmede

[217] Case COMP/M. 7217, *Facebook/WhatsApp*, 03.10.2014, par 122.
[218] Case M. 7813, *Sanofi/Google/DMI JV*, 23.02.2016.

bulunması dikkat çekmektedir. Ortak girişimin tarafları, hasta verilerine ilişkin veri taşınabilirliği imkânlarının ve verilerin birlikte çalışabilir formatlarda dışa aktarımının sağlanabilmesi için çalışacaklarını belirtmiş, Komisyon da buna paralel olarak kullanıcıların GDPR çerçevesinde veri taşınabilirliği taleplerini ileri sürme haklarının olduğu, ortak girişimin kullanıcıları tek bir platformda kilitleyerek pazara girişleri engelleme riskinin olmadığı değerlendirmesinde bulunmuştur.

E. *Microsoft/LinkedIn* Kararı[219]

2016 senesinde *Microsoft*'un profesyonel bir iş ağı ve sosyal paylaşım platformu olan *LinkedIn* ile birleşme işlemini incelemeye alan Avrupa Komisyonu, incelemeye konu olan tarafların ilgili pazarlarda ana rakiplerine nispeten düşük pazar paylarına sahip olmalarının rekabeti olumsuz etkilemeyeceği değerlendirmesinde bulunmuş, tarafların uygulamalar üzerinde entegrasyonu sağlarken rakip teşebbüsler açısından dışlayıcı etkilere sebep olabileceği, birleşme işlemi sonucunda büyüyen veri tabanının pazara giriş engeli oluşturabileceği hususlarını birleşme sonucunda oluşan genişlemiş veri tabanının diğer rakipler için bir zorunlu girdi teşkil etmediği sonucuna vararak tarafların belirli taahhütlerde bulunması koşuluyla birleşmelerine izin vermiştir. Birleşen verilerin pazarda münhasır olarak taraflarca tutulup tutulmadığı konusunun değerlendirilmesi rekabet alanındaki incelemeye teşebbüslerce tutulan verilerin önemli bir etkisi olabileceğinin Komisyon tarafından kabul edildiğini göstermektedir. Üstelik Komisyon, GDPR'a doğrudan atıfta bulunmakta, GDPR ile sağlanan hakların, ilgili kişilere kişisel verileri üzerinde daha fazla söz sahibi olma hakkı tanıyacak olması dolayısıyla *Microsoft*'un kullanıcı verilerini işleme yeteneğini sınırlandırabileceğine işaret etmektedir.

[219] Case COMP/M. 8124, *Microsoft/LinkedIn*, 06.12.2016.

F. *Google Shopping* Kararı[220]

2010 yılında birkaç arama motoru, *Google*'ın kendi arama motorunu ve Evrensel Arama Hizmeti'ni ("*Universal Search Service*") rakip arama motorlarına zarar verecek şekilde kullandığı gerekçesiyle Avrupa Komisyonu'na şikâyette bulunmuştur. Avrupa Komisyonu soruşturmasına *Google*'ın rekabeti engelleyici biçimde münhasırlık anlaşmaları yapıp yapmadığı, çevrimiçi reklamcılık verilerinin taşınmasını kısıtlayıp kısıtlamadığı, tüketicileri olumsuz etkileyecek şekilde rakip teşebbüslerin yatırım teşviklerini azaltacak yöntemler kullanıp kullanmadığı meselelerini de dahil ederek geniş çaplı bir inceleme gerçekleştirmiştir. İnceleme neticesinde *Google*'ın Avrupa Ekonomik Alanı'nda hâkim durumda olduğu tespiti yapılarak daha fazla kullanıcının bulunduğu platformların reklam verenler için daha çekici hale geldiği belirtilmiştir. Bununla beraber *Google*'ın, hâkim durumunu kötüye kullanarak reklam verenleri kendi platformuna kilitleme ve rakip arama motorlarına karşı dışlayıcı davranış sergileme anlamına gelecek kısıtlamalardan kaçınması gerektiğine işaret edilmektedir.

§ 6. VERİ TAŞINABİLİRLİĞİ HAKKININ REKABET HUKUKU ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

I. GENEL OLARAK

Aynı verinin aynı anda farklı kişilerce kullanılabilmesi verilerin rakipsiz ("*nonrival*") olması anlamına gelir. Verinin bizatihi kendisi rakipsiz olsa da veriden değer üretilmesi teşebbüsler arasında rekabeti meydana getirir[221]. Bu nedenledir ki bir

[220] Case AT.39740, *Google Search (Shopping)*, 27.06.2017.
[221] **Krämer**, s. 267.

teşebbüsün elde ettiği verilerin bir diğerine verilmesi veriden değer üretilebilmesi için pazarda mükemmel bir ikameyi oluşturduğundan teşebbüsler sahip oldukları verileri paylaşma eğiliminde değildir[222]. Buna karşılık veri taşınabilirliği hakkı ile ilgili kişilerin kişisel verilerini daha kolay paylaşma tercihinde bulunmasının, veri sorumlusu teşebbüslerin ekonomik çıkarlarını desteklediğini belirtenler de mevcuttur[223]. Söz konusu görüş, verilerin daha kolay ve şeffaf biçimde taşınabilmesinin kullanıcıların hareket alanlarını genişleteceğini, kendilerini daha özgür hissedeceklerini, buna bağlı olarak da kişisel verilerini veri sorumluları ile paylaşma konusunda önceye kıyasla daha rahat olacaklarını ifade etmektedir[224].

Veri temelli ekonomide sektörler, geleneksel sektör kalıplarından pek çok açıdan farklılık göstermektedir. Dijital pazarlarda ürün ve hizmetlerin sunumu geleneksel pazarlardan farklılık arz etmekte, verilerin önemli bir girdi oluşturması sayesinde kullanıcılara ilişkin veriler analiz edilerek kullanıcı tercihlerine ve ihtiyaçlarına yönelik öngörüler oluşturulmakta ve teşebbüs stratejileri buna göre geliştirilmektedir[225]. Ürün ve hizmetler karşılıksız değilse de çoğu zaman ücretsiz sunulduğundan fiyat rekabeti de dijital pazarlarda pek anlam ifade etmez[226]. Dijital pazarlar geleneksel sektörlerdekine kıyasla daha büyük bir yoğunlaşma ve tekelleşme eğilimi göstermektedir[227]. Başlangıç sermayeleri genellikle düşük olan, çoğu zaman

---

[222] **Krämer**, s. 269.
[223] **Van der Auwermeulen**, s. 60.
[224] **Van der Auwermeulen**, s. 60.
[225] **Jenny**, F.: *Competition law and digital ecosystems: Learning to walk before we run*, Industrial and Corporate Change 2021, Vol. 30(5), s. 1145.
[226] **Jenny**, s. 1146.
[227] **HM Treasury**, *Unlocking Digital Competition, Report of the Digital Competition Expert Panel*, 2019, (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf, E. T.: 06.05.2022), s. 31-32; **Stigler Center for the Study of the Economy and the State**, *Stigler Committee on Digital Platforms Final Report*, 2019, (https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf, E. T.: 06.05.2022), s. 7.

ürün veya hizmetleri kullanıcılardan para almaksızın sunan, ulusal veya küresel yaygınlığı bulunan, marjinal maliyetleri düşük, ağ etkileri, ölçek ve kapsam ekonomisi özellikleri yüksek olan bu pazarlarda yoğunlaşmanın güçlü olması kazananın tüm pazara egemen olması ("*winner takes all*") ve pazara giriş ve çıkış engelleri yaratması ile sonuçlanmaktadır[228]. Zaman içerisinde Avrupa Birliği'nde ve Türkiye'de rekabet otoritelerinin verdiği kararlardan da görüleceği üzere veri, fiyat dışı bir rekabet unsuru olarak rekabet incelemelerine dahil edilmiştir.

Teşebbüslerin elde ettikleri veri miktarı ve çeşitliliği rekabeti etkileyebilecek önemli bir faktör olarak ortaya çıkmaktadır. Daha fazla verinin işlenmesi pazarda şeffaflığı artırabilecek bir unsur olmakla beraber bu şeffaflığın veri sorumlusu teşebbüsler tarafından nasıl kullanıldığına bağlı olarak pazar üzerindeki etki değişmektedir. Bir taraftan genişleyen veri setleri ile tüketicilerin fiyat mukayesesi yapmasına imkân tanıyan şeffaflık diğer taraftan algoritmalar kullanılmak suretiyle veya internet ortamında kolaylıkla ulaşılabilen fiyatlama bilgileri sayesinde örtülü fiyat sabitleme anlaşmalarını da güçlendirebilir[229]. Algoritmaların pazardaki fiyatları izleme, sapmaları belirleme, rakip teşebbüslerce alınacak aksiyonları tahmin etme işlevi makine öğrenmesinin bir sonucu olarak algoritmalar arasında zımni fiyat anlaşmalarına vücut verebilecektir[230].

Geleneksel sektörlerde rekabeti bozucu etkiler doğurabilecek eylemler dijital pazarlarda da kendisini göstermekte, girdi olarak teknolojik bir hammaddenin, verinin, kullanılması ilgili pazarın tespiti, hakim durumun kötüye kullanılmasında dikkate alınacak hususlar, birleşme ve devralmalarda birleşerek büyüyen veri

[228] **Stigler Center for the Study of the Economy and the State**, *Stigler Committee on Digital Platforms Final Report,* s. 7-8.
[229] **Autorité de la Concurrence and Bundeskartellamt**, *Competition Law and Data Report,* s. 14.
[230] **Autorité de la Concurrence and Bundeskartellamt**, *Competition Law and Data Report,* s. 15.

sayesinde pazarda elde edilen güç, verinin münhasır olarak kullanılması ve diğer teşebbüslere sağlanmaması yönündeki dışlayıcı davranışlar gibi hususlarda pazarın özelliklerini dikkate alan yeni yorumların benimsenmesini gerektirmektedir. Veri taşınabilirliği hakkının ilgili kişilerin kişisel verileri üzerinde enformasyonel self determinasyon haklarını kuvvetlendirerek rekabeti artırma teşvikinin tüketicinin korunması ve rekabetin güçlendirilmesi bağlamında birtakım etkiler göstereceği şüphesizdir. Doktrinde GDPR'ın veri taşınabilirliğine ilişkin madde 20 ile ulaşmak istediği sonuçların pratikte rekabeti artıracağı ve tüketicilere daha fazla koruma sağlayacağını düşünenler bulunmakla beraber hakkın amacından uzak bir etki doğuracağını, rekabeti ve inovasyonu olumsuz etkileyeceğini savunanlar da vardır. GDPR m. 20'nin rekabet ve inovasyon üzerindeki etkisini rekabet hukukunun inceleme alanları içinde değerlendirmek gerekir.

II. REKABET HUKUKU DÜZENLEMELERİ KARŞISINDA VERİ TAŞINABİLİRLİĞİ HAKKININ GEREKLİLİĞİ VE HAKKIN UYGULANABİLİRLİĞİNİ DESTEKLEYİCİ DÜZENLEMELER

Avrupa Komisyonu'nun eski başkan yardımcısı *Joaquín Almunia*, 2012 yılında yapmış olduğu bir konuşmada veri taşınabilirliği hakkının pazarlarda sağlıklı bir rekabet ortamı yaratacağına, kullanıcı verilerinin saklanmasının platformlar arasında geçişe engel teşkil etmeyeceğine, kullanıcıların bir zaman için güvendikleri şirketlere kilitlenip kalmamaları gerektiğine ve dolayısıyla veri taşınabilirliği hakkının rekabet politikasının tam merkezine gittiğine vurgu yapmış, bunun ise bir regülasyon mu yoksa rekabet politikası mı olduğu hususunu zamanın göstereceğini belirtmiştir[231].

[231] Speech former Competition Commissioner Almunia, *Competition and personal data protection*, Privacy Platform event: Competition and Privacy in Markets of Data Brussels, 26.11.2012, (http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm, E. T.: 06.05.2022).

Kişisel verilerin korunması alanında yapılan bir düzenlemede rekabet hukuku ve politikalarının güttüğü amaçları güden bir hakkın benimsenmesi çokça tartışılmakla beraber esasında rekabet düzenlemeleri ile GDPR konuyu farklı boyut ve kapsamlarda ele almaktadırlar. Hâkim durumun kötüye kullanılması, anlaşmalar, uyumlu eylemler, teşebbüs birliği karar ve eylemleri ile birleşme ve devralmalar ekseninde yapılacak bir inceleme ile veri taşınabilirliği hakkının rekabet hukuku ve politikaları ile ilişkisi ortaya konacağı gibi konuya ilişkin düzenlemelerin birbirinden ayrılan ve kesişen yönleri de tespit edilebilecektir.

Öncelikle Avrupa Birliği'nin rekabet mevzuatının temelini teşkil eden TFEU, diğer düzenlemeler ve rekabet politikaları, pazardaki rekabet yapısını bozacak etkileri yasaklarken pazarda hâkim konumda bulunan, anlaşma veya uyumlu eylem içinde olan, birleşme devralma yolu ile pazar yapısını etkileme potansiyeli bulunan teşebbüsleri kadrajına almaktadır. Bu yönü ile rekabet hukuku ve politikaları her pazarda yalnızca belirli bir ya da birkaç teşebbüse veri taşınabilirliği yükümlülüğünü uygulatabilme kabiliyetine sahiptir[232]. Oysa GDPR m. 20 veri sorumluları bakımından herhangi bir ayrım yapmaksızın, maddede öngörülen şartlar gerçekleştiği takdirde her veri sorumlusunu veri taşınabilirliği hakkının etki alanına dahil etmektedir.

Bir başka açıdan ise rekabet hukuku ve politikalarının pazarda dikkate alacağı tek girdi kişisel veriler olmadığından, kişisel olmayan verilerin de rekabet alanında etki doğuracak biçimde ele alınacağı[233], örneğin hâkim durumdaki bir teşebbüsün

---

[232] **Graef**, I.: *Data Portability at the Crossroads of Data Protection and Competition Policy*, Big Data e Concorrenza, 9 novembre 2016, LUISS Guido Carli, (https://www.agcm.it/dotcmsDOC/eventi/convegni/20161109_07.pdf, E. T.: 09.03.2022), s. 3; **Lucchini**, S./**Moscianese**, J./**de Angelis**, I./**Di Benedetto**, F.: *Online Digital Services And Competition Law: Why Competition Authorities Should be More Concerned About Portability Rather than About Privacy*, Journal of European Competition Law & Practice 2018, Vol. 9, No.9, s. 565; **Lynskey**, s. 801-802.

[233] **Graef**, Crossroads, s. 3; **Graef/Verschaleken/Valcke,** s. 61; **Lucchini/Moscianese/de Angelis/Di Benedetto**, s. 565.

kişisel olmayan ancak zorunlu unsur teşkil eden bir veriyi rakip teşebbüslerle paylaşmamasının hâkim durumun kötüye kullanılması olarak değerlendirilebileceği unutulmamalıdır. GDPR doğrudan kişisel verilerin korunması alanında birtakım düzenlemeler getirmekle, kapsamına yalnızca kimliği belirli veya belirlenebilir bir gerçek kişiyi alan verileri dikkate almaktadır. Dahası, GDPR m. 20'de hakka konu olabilecek kişisel veride başka bazı şartlar daha aranmak suretiyle sınırlı bir kişisel veri kümesinin hakka konu olabileceği belirlenmiştir. Kişisel verinin ilgili kişinin kendisi tarafından sağlanması, yalnızca otomatik yollarla tutulan kişisel verilerin hakkın kapsamında olması, kişisel verilerin belirli formatlarda alınması, teknik açıdan uygulanabilirliğin bulunması gibi şartlar, GDPR'ın uygulama alanını önemli ölçüde daraltmaktadır. Buna karşılık rekabet hukuku ve politikaları çerçevesinde söz konusu olabilecek veride bu şartlar aranmadığından veri niteliği bakımından uygulama alanı daha geniş olmaktadır.

Görüleceği üzere ne rekabet hukuku ve politikaları ne de GDPR kişisel verilerin korunması ve pazarda rekabetin korunması ve geliştirilmesi ihtiyacını tek başına karşılayabilecek durumdadır. Rekabet düzenlemeleri veri niteliği yönünden daha geniş bir uygulama alanına sahip olsa da yalnızca hâkim durumun kötüye kullanılması veya birleşmeler gibi sınırlı alanlarda söz sahibi olabilecektir. GDPR ise veri niteliği yönünden sınırlandırılmış bir uygulama alanı içinde kalmakla beraber rekabeti bozucu bir etkinin olup olmadığını somut olarak tespite ihtiyaç duymadan işlerlik kazanmaktadır[234].

Özellikle teknolojik gelişmeler ile çoğu sektörün dijital pazarlara yönelmesi ve dijital mecralardaki en büyük girdi olarak kişisel verilerin kullanılması ile sınırları katı

[234] **Graef/Verschaleken/Valcke,** s. 61.

olarak belirlenmiş alanlara rastlamak güçleşmektedir. Veri taşınabilirliği hakkı rekabet hukuku ile kişisel verilerin korunması arasındaki kesişim bölgesinde bulunmaktadır. Bu bakımdan veri taşınabilirliği, bu iki dalın münferit gaye ve düzenlemeleri ile gerçek bir sonuca ulaşamamakta, aynı zamanda herhangi biri diğerinin alanını gasp etmemekte, bilakis birbirini tamamlamaktadır[235]. Hakkın bu bütüncül bakış açısı ile ele alınması her iki alanda da daha sağlıklı sonuçlara ulaşılmasını sağlayacaktır. Nitekim bir kısım yazarlarca rekabet hukuku ve politikalarının veri taşınabilirliği hakkının uygulanmasında önemli bir işlev gösterebileceği, GDPR m. 20'nin veri sorumlularına teknik açıdan uygulanabilir sistemler benimseme yönünde bir zorunluluk getirmemiş olmasına karşın rekabet mevzuatının bu hususta eksiği giderebileceği ifade edilmektedir[236]. Bunlara ek olarak Avrupa Birliği Dijital İçerik Direktifi'nde ("*Digital Content Directive*") sağlayıcılar, tüketicilerin dijital içerik ve hizmet sözleşmelerinde verileri üzerinde daha fazla kontrol sahibi olmasını sağlamak adına belirli istisnalar dışında tüketicinin talebi ile kişisel veriler dışındaki diğer dijital içeriği sağlama yükümlülüğüne tabi tutulmaktadır. Bu şekilde tüketici, kişisel verilerini GDPR m. 20 çerçevesinde alabilir ve bir başka veri sorumlusuna iletebilirken söz konusu düzenleme ile kişisel veriler dışındaki dijital içeriği herhangi bir engellemeye maruz kalmaksızın makul bir sürede, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta ücretsiz olarak alabilecektir[237]. Görüleceği

[235] **Colangelo/Maggiolini**, Digital Era, s. 177; **Graef**, Crossroads, s. 4.
[236] **Graef/Verschaleken/Valcke**, s. 60-61; **Vanberg**, A. D./**Unver**, M. B.: *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple and Dynamic Duo?*, European Journal of Law and Technology 2017, Vol. 8, No.1, s. 13.
[237] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770 , E. T.: 06.05.2022), m. 16/4. Veri taşınabilirliği hakkı yönünden kişisel verilerin korunması, rekabet hukuku ve tüketici hukuku sınırlarının belirsizleştiği ve birbirini tamamlayan düzenlemelerle ele alınmaya başlandığı hususundaki detaylı açıklamalar için bkz. **Graef**, I.: *Blurring boundaries of consumer welfare How to create synergies between competition, consumer and data protection law in digital markets*, Personal data in

üzere veri taşınabilirliği hakkının çok boyutlu yönü kişisel verilerin korunması, rekabet hukuku ve tüketici hukuku çerçevesinde birbirini tamamlayan uyumlu düzenlemelerle desteklenmektedir.

Avrupa Komisyonu'nun 2020 yılında taslak çalışmalarını tanıttığı, Mart 2022'de Avrupa Konseyi ve Parlamentosu arasında geçici anlaşmanın gerçekleştiği ve 5 Temmuz 2022 tarihinde Avrupa Parlamentosu tarafından kesin olarak onaylanıp kabul edilen Dijital Pazarlar Kanunu ("*Digital Markets Act*"-DMA) ve Dijital Hizmetler Kanunu ("*Digital Services Act"*-DSA), dijital pazarlarda rekabeti desteklemek için bu pazarlarda faaliyet gösteren ve geçit bekçisi olarak adlandırılan teşebbüslere bir dizi yükümlülük getirmektedir. Çevrimiçi aracılık hizmetleri, çevrimiçi arama motorları, sosyal ağlar, video paylaşım platformları, elektronik iletişim hizmetleri, işletim sistemleri, bulut servis sağlayıcılar ve bu hizmetlerden bir veya birkaçıyla ilgili olan reklam hizmeti sağlayıcılar çekirdek servis sağlayıcılar olarak kabul edilmektedir[238]. Dijital pazarlarda ilgili pazar tanımının yapılmasında karşılaşılan zorluklar da dikkate alınarak oluşturulan bu tasarıda Avrupa Birliği'nin ilgili pazar tanımı yapmaya gerek kalmadan söz konusu platformlarda hakimiyet ve rekabet analizi gerçekleştirmeyi hedeflediği ileri sürülmektedir[239]. Bu düzenlemelere göre iç pazarda önemli bir etkiye sahip olan, önemli bir veya daha fazla ağ geçidi işleten ve faaliyetlerini yerleşik ya da sağlam bir konumdan yararlanarak sürdüren ya

competition, consumer protection and intellectual property law: Towards a holistic approach. editor / Bakhoum, M./Conde Gallego, B./Mackenrodt, M-O&Surblytė-Namavičienė, G. Springer Verlag 2018. (MPI Studies on Intellectual Property and Competition Law), s. 121-151.

[238] Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) ("Dijital Pazarlar Yasası Taslağı"), COM (2020) 842 final, 15.12.2020, (https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf, E. T.: 06.05.2022), s. 2, par. 6.

[239] **Jenny**, s. 1160.

da bundan yararlanması muhtemel görülen çekirdek servis sağlayıcıları geçit bekçisi olarak adlandırılmaktadır[240].

Dijital Pazarlar Yasası ile geçit bekçisi konumundaki teşebbüslere getirilen yükümlülükler içinde veri taşınabilirliği hakkını ve birlikte çalışabilir sistemleri destekleyen hükümler bulunmaktadır. Yasa tasarısının 6. maddesinin birinci fıkrasının (e) bendinde son kullanıcıların geçit bekçisi tarafından sağlanan hizmetten başka hizmetlere geçişlerini ve bunlara abone olma yeteneklerini teknik olarak kısıtlamaktan kaçınma yükümlülüğü getirilerek doğrudan taşınabilirlik için aradan teknik açıdan uygulanabilirlik şartının bilinçli olarak engellenmesi ihtimalinin ortadan kaldırılması amaçlanmıştır. Aynı şekilde 6. maddenin birinci fıkrasının (f) bendinde geçit bekçileri tarafından sağlanan yan hizmetlerin kullanımında kurumsal kullanıcılar ve yan hizmet sağlayıcıların aynı hizmet, yazılım, işletim sistemi veya donanıma erişebilmesine ve birlikte çalışabilirliğine izin vermek geçit bekçileri için bir yükümlülük olarak öngörülmüştür. Nihayet tasarının 6. maddesinin birinci fıkrasının (h) bendinde kurumsal kullanıcılar ve son kullanıcıların etkinlikleri sonucunda üretilen verilerin etkin biçimde taşınabilirliğinin sağlanması ve özellikle GDPR ile uyumlu olarak veri taşınabilirliği hakkının kolaylaştırılması, sürekli ve gerçek zamanlı erişimin sağlanması yükümlülüğü getirilmiştir. Görüleceği üzere veri taşınabilirliği hakkı ile sıkı bir ilişki içinde bulunan hükümler, esasen veri taşınabilirliği hakkının kapsamından çok daha geniş bir kapsam sunmaktadır. Zira söz konusu yasa tasarısı bu hükümleri yalnızca kişisel verileri değil kişisel olmayan verileri de kapsayacak şekilde öngörmektedir. Buna karşılık sektörel kapsama alanı oldukça dar olan düzenleme

[240]Dijital Pazarlar Yasası Taslağı, m. 3/1.

yalnızca çekirdek hizmet sağlayıcıları kapsamakta, bunun dışındaki veri sorumluları açısından bir düzenleme getirmemektedir.

	Amaç	Hangi Tür Veriyi Kapsar?	Taşınabilirlik Yönünden Kimleri Etkiler?
TFEU	Adil rekabetin sağlanması ve korunması (rekabete ilişkin hükümler yönünden)	Kişisel+Kişisel olmayan veriler	Rekabeti etkileyebilecek hâkim durumun kötüye kullanılması, anlaşma, uyumlu eylem, karar, birleşme ve devralmalarda bulunan teşebbüsler
DMA/DSA	Adil rekabetin sağlanması ve korunması	Kişisel+Kişisel olmayan veriler	Geçit bekçisi olarak tanımlanan teşebbüsler (m.2/1)
Dijital İçerik Direktifi	Tüketicinin korunması	Kişisel olmayan veriler	Tacir olarak tanımlanan gerçek veya tüzel kişiler (m. 2/5)
GDPR	Kişisel verilerin korunması	Kişisel veriler	Tüm veri sorumluları (m. 4/7)

Tablo: Avrupa Birliği'nde çeşitli düzenlemelerde veri taşınabilirliği

III. HÂKİM DURUMUN KÖTÜYE KULLANILMASI YÖNÜNDEN REKABET DEĞERLENDİRMESİ

A. Hâkim Durum Kavramı ve Unsurları

TFEU'da hâkim durum tanımı yapılmamakla beraber Avrupa Birliği Adalet Divanı hâkim durumu "*bir teşebbüsün sahip olduğu ve bu teşebbüse rakiplerinden, müşterilerinden ve tüketicilerinden önemli ölçüde bağımsız hareket etme gücü vererek ilgili pazarda etkili rekabetin sürdürülmesini engelleme olanağı tanıyan ekonomik güç*"[241] olarak tanımlamıştır. 4054 sayılı Rekabetin Korunması Hakkında Kanun'un (RKHK) 3. maddesinde TFEU'da yer alan tanıma paralel olarak "*belli bir piyasadaki bir veya birden fazla teşebbüsün, rakipleri ve müşterilerinden bağımsız hareket ederek fiyat, arz, üretim ve dağıtım miktarı gibi ekonomik parametreleri belirleyebilme gücü*"

[241] Case 27/76, *United Brands v. Commission*, 14.02.1978, EU:C:1978:22, par. 65; Case 85/76, *Hoffmann-La Roche & Co. AG v Commission of the European Communities*, 13.02.1979.

tanımına yer verilmiştir. Özetle hâkim durum, bir teşebbüsün pazarda tek taraflı olarak rekabeti etkileyebilecek güce sahip olmasıdır.

Hâkim durumun tespitinde ilk olarak ilgili pazar doğru biçimde tanımlanmalıdır. Tanımdan yola çıkarak hâkim durumu belirlerken teşebbüsün ekonomik gücü, bağımsızlığı ve devamlılığı unsurlarının incelenmesi gerekmektedir. Ekonomik güç, pazarda faaliyet gösteren aktörlerin pazar paylarının ölçülmesi,[242] pazara giriş ve büyüme engellerinin araştırılması ve alıcıların gücü ile anlaşılmaktadır. Hakimin durumun tespitinde karlılık, performans göstergeleri, ürünlerin çeşitliliği gibi daha pek çok ölçüte bakılsa da özellikle ilk olarak incelenen husus pazar payları olmaktadır. Buna karşılık gerek TFEU'da gerekse RKHK'da hâkim durumun belirlenmesi bakımından sabit bir pazar payından bahsedilmemektedir. Bu her somut olayın özelliklerine göre değerlendirilmelidir. Buna karşılık gerek Rekabet Kurulu gerekse Avrupa Komisyonu, somut olayda söz konusu olan pazarın özellikleri doğrultusunda %40'ın altında pazar payına sahip olan teşebbüslerin de hâkim durumda olabileceğini kabul ettiği gibi[243] yerleşik uygulama kapsamında %40'ın altında pazar payına sahip olan teşebbüslerin hâkim durumda olma ihtimalinin düşük olduğu değerlendirmesinde bulunmaktadır[244]. Öte yandan Avrupa Birliği bünyesinde de somut olayın özellikleri dikkate alınmakta ancak özellikle pazar payının %50'nin

[242] **Aslan**, İ. Y.: Rekabet Hukuku Teori ve Uygulama, Güncellenmiş ve Genişletilmiş 6.Baskı, Bursa 2021, s. 696.

[243] Sosyal ağlar gibi dinamik pazarlarda yüksek pazar paylarının her zaman yüksek pazar gücünün göstergesi olmadığı yönünde bkz. **Graef/Verschaleken/Valcke,** s. 60; **Jones**, A./**Brenda**, S.: EU Competition Law: Text, Cases, and Materials. 4th ed. 2011, s. 332.

[244] Kurul, *Pepsi Cola* kararında, %70'in üzerinde kalan pazar payının, tek başına yeterli olmamakla beraber hâkim duruma ilişkin önemli bir belirti olduğunu, %40 ve altı pazar payının ise genel olarak teşebbüsün hâkim durumda bulunamayacağı yönünde bir belirteç olduğunu belirtmektedir. Bkz. Rekabet Kurumu, 10-52/956-335, 05.08.2010, par. 170. Aynı tespit Avrupa Komisyonu'nun TFEU m. 102 hakkında yayımlamış olduğu rehberde de yer almaktadır. İlgili ifade için bkz. Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, 2009/C 45/02, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN, E. T.: 06.05.2022), par. 14.

altına düştüğü durumlarda hakimiyetin tespitinde diğer etkenler önem arz etmektedir[245]. Üye devletlerin iç hukuklarında bu hususta farklı düzenlemeler getirmeleri mümkün olduğundan Almanya'da bir teşebbüsün pazar payının %35'e ulaşmış olması hâkim durumda sayılması için yeterli görülmektedir[246]. Ancak söz konusu dijital pazarlar olduğunda her durumda pazar paylarının hâkim duruma işaret eden güçlü bir indikatör olduğunu söylemek güçtür. Zira yerleşik bir teşebbüsün ürün ve hizmetlerindeki yenilikleri tanıtmadaki başarısızlığı bazen yeni girene avantaj sağlayabilmektedir[247]. Bağımsızlık unsuru ise bir tarafta teşebbüsün hukuki ve ekonomik olarak tek başına karar alabilme yeteneğini, diğer tarafta rakiplerinin ve müşterilerinin reaksiyonlarından ari olarak keyfi biçimde karar alabilme gücünü içerir[248]. Ayrıca Türk hukukunda hâkim durumun devamlılığına ilişkin bir süre öngörülmemişse de Avrupa Birliği'nde somut olayın özellikleri dikkate alınmak şartıyla hâkim durumun beş yıldan uzun sürmesi aranmaktadır[249]. Türk hukukunda bu hususta herhangi bir süre söz konusu olmadığından ve hâkim durumda olmanın değil, hâkim durumun kötüye kullanılmasının yasaklanmış olmasından ötürü hâkim durumun kötüye kullanmaya yetecek kadar sürmesinin devamlılık unsuru açısından yeterli olacağı[250] görüşü ileri sürülmüştür.

B. Hâkim Durumun Kötüye Kullanılması

TFEU m. 102'de, "*Bir veya birden fazla teşebbüsün, iç pazardaki veya iç pazarın önemli bir bölümündeki hâkim durumunu kötüye kullanması, üye devletler*

[245] **Güven**, P.: Türk Rekabet Hukuku ve Avrupa Birliği Rekabet Hukukunda Birleşme ve Devralmaların Denetlenmesi, Genişletilmiş 2. Baskı, Ankara 2003, s. 170.; **Jones/Brenda,** s. 328.
[246] **Güven**, s. 170
[247] **Vanberg/Unver**, s. 7.
[248] **Aslan**, s. 696.
[249] **Aslan**, s. 697; **Güven**, s. 170.
[250] **Aslan**, s. 697.

arasındaki ticareti etkilediği ölçüde, iç pazarla bağdaşmaz ve yasaktır." ifadesine yer verilmektedir. Hükümden anlaşıldığı üzere teşebbüslerin pazarda hâkim duruma gelmeleri değil, hâkim durumdaki teşebbüslerin bu güçlerini rekabeti olumsuz etkileyecek yönde kullanmaları yasaklanmıştır. Türk hukukunda da TFEU ile paralel olarak RKHK m.6'da da "*bir veya birden fazla teşebbüsün ülkenin bütününde ya da bir bölümünde bir mal veya hizmet piyasasındaki hâkim durumunu tek başına yahut başkaları ile yapacağı anlaşmalar ya da birlikte davranışlar ile kötüye kullanması hukuka aykırı ve yasaktır*" hükmü yer almaktadır. Hâkim durumun kötüye kullanılması hâkim durumdaki teşebbüslerin, adil rekabet ortamı içerisinde elde edemeyecekleri avantajlara ulaşmak için sahip oldukları pazar gücü vasıtasıyla, doğrudan veya dolaylı olarak tüketici refahını azaltacak davranışlarda bulunmaları[251] olarak açıklanabilir.

Her iki düzenlemede de hangi hallerin hâkim durumun kötüye kullanılması teşkil edeceğine ilişkin örnekler verilmiş ancak bunlar sınırlayıcı olarak sayılmamıştır. Pazara giriş engelleri koymak, rakiplerin piyasadaki faaliyetlerini zorlaştırmak, makul bir gerekçesi bulunmaksızın ayrımcı tutum ve davranışlar sergilemek, mal veya hizmetleri birbirine bağlamak veya ek yükümlülükler getirmek, bir pazarda elde edilen avantajı bir başka pazarda rekabeti bozucu bir güç olarak kullanmak, tüketicinin zararına olacak biçimde arzı, teknik gelişmeleri veya pazarlamayı sınırlandırmak, rakip teşebbüsler için zorunlu unsur teşkil eden girdileri vermemek, haksız ticari koşullar koymak gibi pazardaki diğer teşebbüslerin rekabet gücünü ve buna bağlı olarak tüketici refahını olumsuz etkileyen uygulamalar hakim durumun kötüye

[251] **Rekabet Kurumu**, Hâkim Durumdaki Teşebbüslerin Dışlayıcı Davranışlarına İlişkin Kılavuz, 2014, (https://www.rekabet.gov.tr/Dosya/kilavuzlar/hakim-durumdaki-tesebbuslerin-dislayici-davranislarina-iliskin-kilavuz1.pdf, E.T.: 06.05.2022), par. 22.

kullanılması anlamına gelmektedir. Bu anlamda haksız fiyatlama ile arz ve talebin kısıtlanması gibi birtakım davranışlar "sömürücü kötüye kullanma" teşkil ederken rakip teşebbüsleri engelleyecek girişimlerde bulunmak veya ürün bağlamak gibi davranışlar ise "dışlayıcı kötüye kullanma" niteliği taşımaktadır[252].

C. Veri Taşınabilirliği Hakkı Çerçevesinde Hâkim Durumun Kötüye Kullanılması

Veri taşınabilirliği ve birlikte çalışabilirlik konusunda doktrinde ifade edilen endişelerden biri, birlikte çalışabilir sistemler vasıtasıyla doğrudan taşınabilirliği mümkün kılacak teknik uygulanabilirliğin veri sorumluları için bir yükümlülük olarak öngörülmemiş olmasıdır. TFEU m. 102'de "*üretimin, piyasaların veya teknik gelişmelerin tüketicilerin zararına olacak şekilde sınırlandırılması*" hâkim durumun kötüye kullanıldığını gösteren bir davranış olarak belirtilmiştir. Buna göre, hâkim durumdaki veri sorumlusu teşebbüs, veri taşınabilirliği hakkının kullanılmasını engellemek maksadıyla teknik açıdan uygulanabilirliği sağlamamaktaysa veya veri taşınabilirliği hakkının kullanılmasını engellemek isterse tüketicileri kilitlenme ("*lock-in*") durumu ile karşı karşıya bırakabilecek ve bu da rekabeti bozucu bir etki davranış olarak değerlendirilebilecektir[253]. Benzer şekilde hâkim durumdaki teşebbüsün bu davranışı pazara giriş engelleri yaratabilecek ve pazardaki gelişmeyi tüketicilerin zararına olacak şekilde sınırladığından TFEU m. 102'nin kapsamına girecektir[254].

Pazarda hâkim durumda olan teşebbüsün rekabeti bozucu şekilde rakip teşebbüslerin pazardaki fırsatlarını azaltma eğilimini ifade eden dışlayıcı

[252] **Vanberg/Unver**, s. 7.
[253] **Geradin**, D./**Kuschewsky**, M.: *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue*, 2013, s, 11; **Graef**, Crossroads, s. 2.
[254] **Geradin**/ **Kuschewsky**, s. 11; **Graef**, Crossroads, s. 2.

davranışlar[255] hâkim durumun kötüye kullanılması hallerinden birini teşkil eder. Dijital pazarlarda veri en önemli girdiyi oluşturmaktadır. Kullanıcı temelli uygulamalarda ve özellikle sosyal medya platformlarında kişisel verilerin işlenmesi, yeni ürün ve hizmetler geliştirilmesini kolaylaştırmakta; işlenen verinin çeşitliliği ve miktarı, ağ etkileri, kapsam ve ölçek ekonomileri daha geniş bir veri tabanına sahip olan teşebbüslerin pazarda tutunmasına ve pazar gücünü artırmasına katkıda bulunmaktadır. Hal böyle iken yoğunlaşma ve tekel haline gelme potansiyeli yüksek olan teşebbüslerin işlemiş oldukları verilere erişimi engellemeleri pazara yeni teşebbüslerin girmesini engelleyebilir ve rakip teşebbüsler açısından rekabeti bozucu etki doğurabilir. Bu sebepledir ki *Google Shopping* kararında rekabet hukuku yönünden yapılan incelemede, *Google*'ın reklam verenleri *AdWords* platformundan başka bir platforma verilerin aktarılması yönünden kısıtlamasının bir tehlike olduğu düşüncesiyle verilerin paylaşılmasını engelleyen faaliyetlerini sonlandırması gerektiğine dikkat çekilmektedir.

Ne var ki hâkim durumdaki bir teşebbüsün işlemiş olduğu kişisel verilere erişimi engellemesi her durumda rekabet hukuku ihlali niteliği taşımamaktadır. Zorunlu unsur doktrini uyarınca pazardaki teşebbüslerin faaliyetlerine devam edebilmeleri ve tüketicilere ulaşabilmeleri için teknik, hukuki veya ekonomik sınırlamalar dolayısıyla bağımlı oldukları, kopyalanması imkânsız veya önemli ölçüde zor olan tesis veya altyapıya erişim hakkı bulunmalı ve hâkim teşebbüs rakip

[255] European Commission, *Glossary of Terms Used in EU Competition Policy, Antitrust and Control of Concentrations,* 2002, (https://www.concurrences.com/IMG/pdf/european_commission_glossary_of_terms_used_in_eu_competition_policy_-_antitrust_and_control_of_concentrations.pdf?40143/2eeffac1aa42eaa000f06738fda10e48e160afe2, E. T.: 06.05.2022), s. 18.

teşebbüslere bu imkânı sağlamalıdır[256]. Elbette hâkim durumdaki teşebbüsün rakiplerine zorunlu unsuru ücretsiz olarak sağlaması düşünülemez. Dolayısıyla zorunlu unsurun makul ücret karşılığında sağlanması bir erişim engeli olarak değerlendirilemez. Erişim engellerinin dışında ayrımcı faaliyetler, münhasır yetki anlaşmaları, ürün bağlama ve bir pazarda elde edilen avantajın diğer pazarda kullanılması şeklindeki çapraz kullanımlar da dışlayıcı davranış teşkil edebilir. Ayrımcılık yapmama gerekliliğini sağlamanın en basit şekli kendinin tercih edilmesi ("*self preferencing*") biçimindeki faaliyetlerde bulunmamaktır[257]. Bu doğrultuda bir teşebbüsün elinde bulundurduğu verileri rakiplerine sağlamayı reddetmesi, verilerin zorunlu unsur teşkil etmesi halinde hâkim durumun kötüye kullanılması anlamına gelebilecektir[258]. Ancak veriler söz konusu olduğunda gerekli girdiye "teknik, yasal veya ekonomik engellerle ulaşılamama"[259] durumunun gerçekleştiğinden söz edilmesi pek kolay değildir. Yeniden elde edilemeyen geçmiş dönem verileri veya güçlü ağ etkileri ile şekillenen iş modellerinin bulunması gibi hallerde söz konusu verilerin zorunlu unsur olduğu iddia edilebilir[260].

Fransız rekabet otoritesinin *GDF Suez* kararına konu olayda, gaz dağıtımı pazarında bir kamu teşebbüsü olarak faaliyet gösterdiği dönemde elde ettiği kullanıcı verilerini kendi lehine kullanarak, büyük veri tabanının sağladığı hâkim durumun

---

[256] **Guggenberger**, N.: *The Essential Facilities Doctrine in the Digital Economy: Dispelling Persistent Myths*, Yale Journal of Law&Technology 2021, Vol. 23, s. 303. Ayrıca Avrupa Birliği Adalet Divanı *IMS Health* ve *Microsoft* davalarında da bu hususa işaret edilmiştir. Bkz. Case C-7/97, Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs-und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, 26.11.1998; Case C-418/01, *IMS Health GmbH & Co OHG v NDC Health GmbH & C. KG*, 29.04.2004.
[257] **Guggenberger,** s. 325.
[258] **Jenny**, s. 1150.
[259] **Drexl**, J.: *Designing Competitive Markets for Industrial Data – Between Propertisation and Access,* Max Planck Institute for Innovation and Competition Research Paper No. 16-13, 2016, s. 48, https://ssrn.com/abstract=2862975.
[260] **Elfering**, S.: Unlocking the Right to Data Portability An Analysis of the Interface with the Sui Generis Database Right, Baden-Baden 2019, s. 56.

kötüye kullanılıp kullanılmadığı değerlendirmesi yapılmış ve nihayetinde söz konusu müşteri verilerinin pazarda zorunlu unsur teşkil ettiği gerekçesiyle rakip teşebbüslerle paylaşılması gerektiği sonucuna varılmıştır[261]. Benzer şekilde *Microsoft* davasında *Sun Microsystems*'ın iddiaları *Microsoft*'un kişisel bilgisayarlarda işletim sistemleri pazarında hâkim konumda olduğu, bu sistemlerle birlikte çalışabilirliği sağlayacak bilgileri pazardaki diğer teşebbüslerle paylaşmadığı veya ayrımcı anlaşmalar yaparak diğer teşebbüslerin rekabet gücünü etkilemesi sebebiyle hakimiyeti kötüye kullandığı noktasında toplanmakta idi[262]. *Microsoft*'un birlikte çalışabilirlik bilgisini paylaşmasının zorunlu bir unsur teşkil edip etmediği incelenmiş ve rakip teşebbüslerin bu bilginin ikamesine ulaşma imkânı olmadığının tespitiyle *Microsoft*'un hâkim durumunu kötüye kullandığına karar verilmiştir.

Microsoft davası dijital pazarlarda zorunlu unsur doktrinine dayanırken gözetilmesi gereken bir başka menfaati de gündeme getirmiştir. *Sun Microsystems*'ın iddialarına karşı *Microsoft*, haklı sebeplerle erişimi reddettiğini, birlikte çalışabilirlik bilgisini paylaşmasının rakipleri tarafından kolay taklit edilebilir hale gelmesini ve kendilerinin de inovasyon teşvikini azaltacağını ifade etmiştir. *Microsoft*'un savunması, GDPR m. 20 ile tanınan veri taşınabilirliği hakkı ve birlikte çalışabilirlik amacına yönelik doktrindeki temel eleştirinin somut bir örneğini teşkil etmektedir. Yalnızca veri taşınabilirliği hakkının uygulanması perspektifinden bakıldığında birlikte çalışabilir sistemlerin kurulması ve teknik elverişliliğin sağlanmasının GDPR'da veri sorumlularına bir yükümlülük olarak getirilmemesi eleştirilmektedir[263].

---

[261] Karara ilişkin basın açıklaması için bkz. (https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/9-september-2014-gas-market, E. T.: 06.05.2022).
[262] Case COMP/C-3/37.792, Microsoft, C(2004)900 final, 24.03.2004; Case T-201/04, *Microsoft Corp. V Commission of the European Communities*, 17.09.2007.
[263] **Eskens**, s. 171; **Graef/Verschaleken/Valcke,** s. 63.

Oysa rekabet hukuku perspektifinden konuyu ele alan bir görüş, GDPR m. 20 kapsamında birlikte çalışabilirliğin zorunluluk taşımamasına karşın DMA ve DSA ile yapılan düzenlemelerin, bütün veri sorumlularına birlikte çalışabilirliği sağlama yükümlülüğü getirmemekle beraber, geçit bekçisi olarak adlandırılan bir grup veri sorumlusuna birlikte çalışabilirliği bir yükümlülük olarak öngörmesinin bu teşebbüslerin fikri mülkiyet haklarının korunmasında ve inovasyon teşviklerinde olumsuz bir etki doğuracağını belirtmektedir[264].

Hâlbuki kişisel verilerin dijital pazarlarda rekabeti etkileme gücü göz önüne alındığında dışlayıcı davranış anlamına gelebilecek bir eylemin hâkim durumdaki teşebbüsün diğer bazı menfaatlerinden öncelikli görülmesi gerekmektedir. Hâkim teşebbüsün dışlayıcı davranışı, bir yanda pazardaki diğer teşebbüslerin rekabet gücünü kısıtlamakta diğer yanda ise hâkim teşebbüsün kendi menfaatlerini koruma amacına dayanmaktadır. Bu bağlamda bir teşebbüsün kendi veri tabanını geliştirebilmek için uçsuz bucaksız veri havuzu içinde hâkim teşebbüsün işlediği verilere ulaşmasının gerçekten zorunlu unsur teşkil ettiğini ispatlaması zor olacaktır[265]. Bu husus kullanıcı merkezli uygulamalar nezdinde ele alındığında uyuşmazlığa konu veri grubunun kişisel veri niteliği taşıdığı ve kişisel olmayan verilere kıyasla daha fazla zorunluluk doğurduğu düşünülebilir. Esasen bu halde dahi hâkim teşebbüs tarafından anonimleştirilmiş verilere erişim izni verilecektir. Zorunlu unsur doktrininin ve dışlayıcı davranışların dijital pazarlarda yeniden yorumlanmasında önem taşıyan husus zorunlu addedilen verinin hiçbir şekilde ikamesini bulma imkânının olmadığını veya çok zor şartlarda bulunabileceğini sağlıklı biçimde tespit etmektir. Geleneksel pazarlarda zorunlu unsurun tespiti buradaki kadar karmaşık değildir. Üstelik dijital

[264] **Jenny**, s. 1162.
[265] **Vanberg/Unver**, s. 11.

pazarlarda fikri mülkiyet haklarının korunması ihtiyacı da geleneksel pazarlara kıyasla çok daha ön plandadır[266]. Bu nedenle menfaatleri dengeleyebilmek için bir verinin ya da veri tabanının ne zaman zorunluluk addettiğinin makul biçimde ortaya konması gerekir.

Rekabet hukuku, dijital pazarlarda zorunlu unsur doktrini uyarınca en azından zorunlu unsur niteliğindeki kişisel veri ve veri setleri açısından yatay ve dikey birlikte çalışabilirlik esaslarının benimsenmesini gerektirmektedir[267]. Buna karşılık zorunlu unsur niteliği taşımayan kişisel veri veya veri setleri için birlikte çalışabilirlik yükümlülüğünün getirilmesi gerçekten de piyasa aktörlerinin gelişim hedeflerini olumsuz etkileyebilecektir. DMA yalnızca geçit bekçisi konumundaki veri sorumlularına birlikte çalışabilirlik yükümlülüğü getirmektedir. Bunun dışındaki dijital pazar aktörleri açısından ise birlikte çalışabilirliği sağlama yükümlülüğü olmadığını belirtmek gerekir. Keza TFEU m. 102 de yalnızca hâkim durumdaki teşebbüsün veri taşınabilirliği ve birlikte çalışabilirlik adımları atmasını zorunlu kılmaktadır. Veri taşınabilirliği hakkının yalnızca dijital pazarlarda faaliyet gösteren veri sorumlularına değil, GDPR m. 20'deki koşulların gerçekleştiği durumlarda tüm veri sorumlularına karşı ileri sürülebilir olması pek çok pazarda birlikte çalışabilirlik esaslarının benimsenmesinin önünde doğal bir engel oluşturmaya müsaittir.

GDPR m. 20/1 ile öngörülen dolaylı taşınabilirlik teknik gereklilikleri bakımından m. 20/2'de öngörülen doğrudan taşınabilirliğe kıyasla önemli bir sorun teşkil etmese de doğrudan taşınabilirlik, hakkın teknik açıdan uygulanabilir olmasına bağlı olduğundan pek çok pazarda veri sorumlularının birlikte çalışabilir sistemler

[266] **Posner**, R.: *Antitrust in the New Economy*, Antitrust Law Journal 2001, Vol. 68, No. 3, s. 926.
[267] Zorunlu unsurun dijital pazarlarda bu şekilde yorumlanması gerektiği, bu sayede birlikte çalışabilirliğin ağ etkilerini azaltarak pazara giriş engellerini de kaldırabileceği ve hatta kaldırması gerektiği yönünde bkz. **Guggenberger,** s. 326.

kurmaktan kaçınması muhtemeldir. Öyle ki m. 20/1'de öngörülen dolaylı taşınabilirliğin uygulanması kullanıcılar için çoğu zaman karmaşık ve zaman alıcı bir süreç oluşturmaktadır[268]. Bu sebeple kişisel verilerin tek seferlik dışa aktarımına izin verilmesi pazara giriş engellerinin kaldırılmasında büyük bir etki göstermez. Dijital pazarlar dışındaki herhangi bir pazarda hâkim durumdaki teşebbüsün, birlikte çalışabilirliği sağlama yükümlülüğü bulunmadığından, teknik açıdan uygulanabilirliği sağlamaktan bilinçli olarak kaçınması somut olayın şartları içinde dışlayıcı davranış olarak nitelendirilebilecektir[269].

IV. ANLAŞMALAR, UYUMLU EYLEMLER İLE TEŞEBBÜS BİRLİKLERİNİN KARARLARI VE EYLEMLERİ YÖNÜNDEN REKABET DEĞERLENDİRMESİ

A. Anlaşma, Uyumlu Eylem, Teşebbüs Birliklerinin Karar ve Eylemleri Kavramları ile Unsurları

TFEU m. 101'de Avrupa Birliği'ne üye devletler arasındaki ticareti etkileyebilecek nitelikte olan, amacı veya etkisi iç pazardaki rekabeti bozucu, kısıtlayıcı veya engelleyici teşebbüsler arası anlaşmalar, kararlar ve uyumlu eylemler yasaklanmıştır. Keza RKHK m. 4'te de "*Belirli bir mal veya hizmet piyasasında doğrudan veya dolaylı olarak rekabeti engelleme, bozma ya da kısıtlama amacını taşıyan veya bu etkiyi doğuran yahut doğurabilecek nitelikte olan teşebbüsler arası anlaşmalar, uyumlu eylemler ve teşebbüs birliklerinin bu tür karar ve eylemleri hukuka aykırı ve yasaktır.*" hükmü ile uyumlu eylemlerin yasaklanan faaliyetler arasında olduğu ifade edilmiş, yalnızca rekabeti bozma amacı taşıyan eylemler değil

[268] **Vanberg/Unver**, s. 10.
[269] **Lucchini/Moscianese/de Angelis/Di Benedetto**, s. 567; **Swire/Lagos**, s. 360.

bu etkiyi doğuran ya da doğurabilme potansiyeli bulunan tüm anlaşma, karar ve uyumlu eylemler kapsama dahil edilmiştir.

Söz konusu maddeler kapsamındaki anlaşma, karar ve uyumlu eylemler yalnızca sözleşmelerle sınırlandırılmamıştır. Bu anlamda "anlaşma"nın borçlar hukukundaki sözleşmelerden daha geniş yorumlanması gerekir. Borçlar hukukunun sözleşmelerin kurulması ve geçerlilik şartlarını düzenleyen hükümlerine aykırı olmasından ötürü geçersiz olan bir anlaşma dahi TFEU m. 101 ve RKHK m. 4'te ifadesini bulan anlaşma kavramı içinde değerlendirilmektedir[270]. Zira rekabet hukuku ve politikaları çerçevesinde anlaşma, borçlar hukuku bağlamında bir sözleşme niteliği taşımasa dahi en azından tarafların irade beyanlarını içeren[271], rakiplerden bağımsız olarak belirlenmiş bir pazar politikası arz etmeyen[272] uyuşmayı ifade eder. Uyumlu eylemler ise anlaşmadan farklı olarak açık bir irade beyanı düzeyine varmayan, teşebbüslerin rekabeti bozma amacıyla hareket etmedikleri durumda dahi teşebbüsler arasında bilinçli olarak paralel ve rekabeti bozucu nitelikteki davranışlar ile iş birliği faaliyetleri ifade eder[273]. Buna uygun olarak uyumlu eylemin unsurları; birden fazla teşebbüsün bulunması, bu teşebbüslerin faaliyetleri arasında bilinçli olarak paralellik ve bağlantı olması, paralel davranışları ekonomik ve rasyonel gerekçelerle açıklamaya

[270] **Akıncı**, A.: Mukayeseli Hukuk Açısından Amerikan ve Avrupa Topluluğu Hukukunda Rekabetin Yatay Kısıtlanması, Lisansüstü Tez Serisi No: 5, Ankara 2001, s. 145; **Jones/Brenda**, s. 142; RKHK m. 4 Gerekçesi. Karş. **Topçuoğlu**, M.: Rekabeti Kısıtlayan Teşebbüsler Arası İşbirliği Davranışları ve Hukuki Sonuçları, Rekabet Kurumu Lisansüstü Tez Serisi, Ankara, 2001, s. 133-138.

[271] **Aslan**, s. 227-228.

[272] **Aslan**, s. 232. Ayrıca rakiplerden bağımsız olarak belirlenmiş bir pazar politikasının varlığı araştırılırken tüzel kişiliklerin farklılığından ziyade ekonomik bütünlüğün esas alınması gerektiği ve bu anlamda ana şirket ile yavru şirket arasındaki anlaşmanın, aynı teşebbüsü meydana getirmelerinden ötürü rekabet hukukunun yasakladığı anlaşma kapsamı içine girmeyeceği yönünde bkz. **Aslan**, s. 228-229.

[273] **Akıncı**, s. 145; **Aslan**, s. 241; **Jones/Brenda**, s. 160; **Whish**, R./**Bailey**, D.: Competition Law, Seventh Edition, New York 2012, s. 102.

elverişli haklı bir nedenin bulunmaması ve rekabetin sınırlanması olarak sıralanabilir[274].

Bununla birlikte anlaşma ve uyumlu eylem unsurlarının bir arada olması halinde bunları ayrı ayrı incelemeye gerek kalmadan ortak bir sınıflandırma yapılmasının mümkün olduğu doktrinde ve rekabet otoriteleri ile yargının vermiş olduğu kararlarda kabul edilmektedir. Öyle ki rekabeti bozucu eylemler genel olarak gizli anlaşmalar doğrultusunda yürütülmekte, teşebbüsler arasındaki bağlantının irade beyanı açıklaması niteliği taşıyıp taşımadığının incelenmesinde pratik bir fayda bulunmamaktadır[275]. Avrupa Birliği Adalet Divanı *Asnef-Equifax* kararında kredi verenlere müşterilerin finansal bilgilerine ulaşabilecekleri bir alt yapı oluşturmak suretiyle iş birliği yapılmasında yapılan işlemin nitelik olarak anlaşma, uyumlu eylem veya karar olarak sınıflandırılmasına gerek olmadığı sonucuna varılmıştır[276]. Benzer şekilde Rekabet Kurulu da *Seramik Kararı*'nda uyumlu eylemi anlaşmadan tamamen ayrı bir kavram olarak değil "anlaşmanın varlığının ispatlanmasında bir araç"[277] olarak ele almaktadır. Bu hususta RKHK m. 4/3 ve m. 4/4 ispat yükünü tersine çevirmek suretiyle fiyat değişimi, arz ve talep dengesi, teşebbüslerin faaliyet bölgesi açısından rekabeti bozucu, kısıtlayıcı veya engelleyici davranışların sonuçlarına benzer sonuçların bulunması halinde uyumlu eylemin varlığını karineten kabul etmiştir. Bir başka ifade ile bu hallerde teşebbüslerin ekonomik ve mantıklı gerekçelerle söz konusu sonuçları açıklamaları ile sorumlulukları ortadan kalkacak, aksi halde teşebbüsler arasında uyumlu eylem bulunduğu kabul edilecektir.

---

[274] **Aslan**, s. 240; **Topçuoğlu**, s. 193-197.
[275] **Topçuoğlu**, s. 209-210.
[276] **Whish/Bailey**, s. 103.
[277] Rekabet Kurumu Başkanlığı, Kurul Kararları, Dosya Sayısı: 2002-1-44 (Soruşturma) Karar Sayısı: 04-16/123-26 Karar Tarihi: 24.02.2004.

Yalnızca münferit teşebbüsler arasındaki anlaşma ve uyumlu eylemlerin yasaklanması ilgili pazarda rekabetin korunması açısından tek başına yeterli değildir. Belli bir pazardaki teşebbüslerin müşterek menfaatlerini koruyacak teşebbüs birliklerinin aldığı kararların da pratik olarak teşebbüsler arasındaki anlaşma ve uyumlu eylemlerden farkı bulunmamaktadır[278]. Zira teşebbüs birliği kararları, teşebbüsleri belirli bir yönde hareket etme veya etmeme davranışına itmeye elverişlidir. Teşebbüs birliklerinin bağlayıcı kararları olabileceği gibi tavsiye niteliğinde kararları da olabilir. Ayrıca madde kapsamına teşebbüs birliği eylemlerinin de dahil edilmesi ile bağlayıcı olmayan teşebbüs birliği kararlarının bu yolla uygulanması ve kanuna karşı hile yapılması da engellenmiş olmaktadır.

B. Veri Taşınabilirliği Hakkı Çerçevesinde Anlaşmalar, Uyumlu Eylemler ile Teşebbüs Birliklerinin Kararları ve Eylemleri

Birlikte çalışabilirlik esasları söz konusu olduğunda pazardaki teşebbüsler arasında meydana gelebilecek danışıklı davranışlar birlikte çalışabilir sistemlerin kullanılmasından kaynaklanabilir[279]. Pazarda şeffaflığı sağlamaya çalışan adımlar çoklu pazar temasına yol açabilecek durumdadır[280]. Dahası algoritmaların birbirleriyle iletişime geçerek fiyat anlaşması yapması veya fiyat dışı rekabet unsurlarında eşgüdümlü faaliyetlerde bulunması mümkündür. Algoritmik gizli anlaşma ("*algorithmic collusion*") olarak adlandırılan bu durum, geleneksel pazarlarda var olan gizli anlaşma biçimlerini gerçekleştirmek için kullanılabilirken, daha önce

[278] **Aslan**, s. 264; **Jones/Brenda**, s. 168-169.
[279] **OECD**, *Competition Committee Discussion Paper*, 09.06.2021, (http://oe.cd/dpic, E. T.:06.05.2022), s. 35.
[280] **Fletcher**, A.: *Digital competition policy: Are ecosystems different?*, 2020, (https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf, E. T.: 06.05.2022), s. 11.

gözlemlenmemiş bir gizli anlaşmaya da vücut verebilecektir[281]. Pazarda faaliyet gösteren teşebbüslerin fiyat veya satışlarla ilgili olarak rekabet hukuku ile bağdaşmayacak durumdaki anlaşma, eylem ve kararlarında algoritmalar bunları uygulayıcı ve kolaylaştırıcı bir araç olarak kullanılabilir.

Veri taşınabilirliği yönü ile ilgili rekabet düzenlemelerinin incelemesinde görülecektir ki olağan olarak beklenen birincil rekabet ihlali pazardaki teşebbüslerin veri taşınabilirliği hakkının kullanılmasını önlemek için teknik açıdan elverişli sistemler kurmama yönünde anti rekabetçi eylemlerde bulunmalarıdır. Zira GDPR m. 20/2, teknik açıdan uygulanabilir olmaması halinde doğrudan veri taşınabilirliğini veri sorumlularına bir yükümlülük olarak öngörmemiştir. Konu ile ilgili sorun, teşebbüslerin gerekli teknik altyapıyı oluşturmaktan kaçınmalarındaki gerekçeyi belirleyebilmektir. Şöyle ki verilerin yoğun olarak kullanılmadığı ve birlikte çalışabilir sistemlerin benimsenmesinin ekonomik açıdan haklı görülebilecek ölçüde maliyetli olduğu pazarlarda veri sorumlusu teşebbüslerin GDPR m. 20'yi uygulamaya yönelik teknik girişimlerde bulunmamaları makuldür. Bu halde, teşebbüslerin rekabet hukuku ihlali niteliğinde anlaşma ve eylemler doğrultusunda hareket ettiğini kabul etmek hakkaniyete uygun olmayabilir. Öte yandan buradaki gibi makul bir gerekçenin tespit edilemediği ve pazardaki teşebbüslerin birlikte çalışabilir sistemler kurmayı reddettiği durumda ise rekabet ihlali niteliğinde davranışlar bulunabileceği dikkate alınarak şüpheyle yaklaşmak gerekebilir.

V. BİRLEŞME VE DEVRALMALAR YÖNÜNDEN REKABET DEĞERLENDİRMESİ

[281] **OECD**, *Algorithms and Collusion: Competition Policy in the Digital Age*, 2017, (https://www.oecd.org/daf/competition/Algorithms-and-collusion-competition-policy-in-the-digital-age.pdf, E. T.: 06.05.2022), s. 18-19.

A. Rekabet Hukuku ve Politikaları Bağlamında Birleşme ve Devralmalar

Gerek Türk gerekse Avrupa Birliği rekabet hukukunda teşebbüsler arasında birleşme ve devralma işlemleri yasaklanmış değildir. Rekabet hukuku anlamında birleşme ve devralma yalnızca yasal olarak gerçekleştirilen birleşme devralmaları değil, fiili düzeyde kalan birleşme ve devralmaları da kapsamına almaktadır[282]. Teşebbüsler arasındaki birleşme ve devralmanın hâkim durum yaratma, pazardaki rekabeti olumsuz etkileme gibi sonuçlar doğurma ihtimali mevcut ise bu işleme öncelikle denetim makamınca onay verilmesi gerekmektedir.

Birleşme ve devralma niyetinde olan teşebbüslerin aynı ürün veya hizmet pazarında faaliyet göstermesi ve birbirlerine rakip olması halinde yatay birleşme ve devralmadan; aynı pazarda olmakla beraber birbirine rakip olmaması, bir diğer ifadeyle ekonomik olarak birbirini izleyen süreçlerde bulunması halinde dikey birleşme devralmadan söz edilir[283]. Bunlara ek olarak aynı ürün ve hizmet pazarında yer almayan teşebbüslerin birleşmeleri ise aykırı veya karma birleşme devralma olarak adlandırılmaktadır[284].

Rekabet hukuku ve politikaları bağlamında[285] birleşme ve devralmadan bahsedebilmek için iki veya daha fazla teşebbüsün bulunması, bu bağımsız teşebbüslerin birleşmesi veya herhangi bir kişi ya da teşebbüs tarafından diğer bir teşebbüsün malvarlığı ya da ortaklık paylarının tümünün ya da bir kısmının ya da yönetimde hak sahibi olma yetkisi veren araçlarının devralınması yoluyla kontrolün

[282] **Güven**, s. 115.
[283] **Güven**, s. 116-117; **Aslan**, s. 820-824.
[284] **Güven**, s. 120; **Aslan**, s. 824.
[285] RKHK m. 7; TFEU m. 101-102. TFEU m. 101-102'de birleşme ve devralmalara ilişkin doğrudan bir hüküm bulunmamakla beraber bu hükümlerin birleşme ve devralmalara da uygulanacağı Avrupa Toplulukları Mahkemesi'nin çeşitli kararlarında belirtilmiştir. Ayrıca yan düzenlemelerde de birleşme ve devralmalara ilişkin hükümler bulunmaktadır. Ayrıntılı açıklamalar için bkz. **Güven**, s. 67-90.

ele geçirilmesi, birleşme veya devralmanın hakim durum oluşturması veya bu olasılığı kuvvetlendirmesi, bunlara bağlı olarak rekabetin olumsuz etkilenmesi gerekmektedir.

B. Veri Taşınabilirliği Hakkı Çerçevesinde Birleşme ve Devralmalar

Verinin özellikle dijital pazarlarda fiyat dışı bir rekabet unsuru oluşturduğunun anlaşılmasıyla rekabet otoriteleri birleşme ve devralmaların kontrolünde birleşme işleminin taraflarının sahip oldukları veri setleri ile oluşacak yoğunlaşmaları da inceleme konusu yapmaya başlamıştır. Öyle ki veri setlerinin birleşmesi pazarda yoğunlaşmayı artırıcı bir faktör olarak rol oynayabilmektedir[286]. *Google/DoubleClick* kararında bu hususu dikkate almayan Avrupa Komisyonu *Facebook/Whatsapp* ve *Microsoft/LinkedIn* kararlarında yaklaşımını değiştirerek birleşen veri setlerinin pazardaki rekabeti etkileme gücünü inceleme konusu yapmıştır. Dahası bu incelemelerde, birleşen veri setlerinin rakip teşebbüsler açısından zorunlu unsur niteliği taşıyıp taşımadığı değerlendirilmiş, bir bakıma birleşme sonucunda oluşabilecek dışlayıcı davranış potansiyeli araştırılmıştır.

ABD'de iki büyük biletleme firması *Ticketmaster* ve *Live Nation*'ın birleşme talebi üzerinde 2010 yılında ABD Adalet Bakanlığı Rekabetçi Etki Değerlendirmesi ("*Competitive Impact Assessment*") Raporu'nda, *Tickermaster*'ın elde ettiği verileri rakip teşebbüslere vermesi ve müşterilerinin, *Ticketmaster*'daki verilerini talep etmeleri halinde bu verilerin kendilerine verilmesi yoluyla teşebbüsler arasındaki geçiş maliyetlerinin azaltılması gerektiği vurgusu yapmış[287], aynı yıl verilen kararda

[286]**European Commission, Directorate-General for Competition, Montjoye, Y./Schweitzer, H./Crémer, J.,** Competition policy for the digital era, Publications Office, 2019, (https://data.europa.eu/doi/10.2763/407537, E. T.: 06.05.2022), s. 110.

[287] US Department of Justice, Competitive Impact Assessment, *U.S. and Plaintiff States v. Ticketmaster Entertainment, Inc. and Live Nation Entertainment, Inc.*, 1:10-cv-00139, 25.01.2010, III.

Ticketmaster'a yazılı talep halinde müşteri verilerinin 45 gün içinde sağlanması yükümlülüğü getirilmiştir[288].

Dikey birlikte çalışabilirlik esaslarının benimsendiği teşebbüslerin birleşmesinde birleşen teşebbüslerin en az bir ürünle ilgili kalıcı bir pazar gücüne sahip olup olmayacağı veri taşınabilirliği ve birlikte çalışabilirlik çerçevesinde dikkate alınması gereken rekabet hukuku problemini oluşturur[289]. Yatay birleşmelerde de buna benzer şekilde yoğunlaşma meydana gelebilecek ve rekabeti olumsuz etkileyebilecektir.

VI. VERİ TEMELLİ PAZARLARDA VERİ TAŞINABİLİRLİĞİ HAKKININ REKABET HUKUKUNA ETKİSİ

Veri temelli ekosistemlerde pazarın yapısına bağlı olarak kullanıcıları belirli bir teşebbüste kalmaya zorlayan, teşebbüsün sunduğu ürün ve hizmetleri kullanan kullanıcı sayısının artması ile ürün ve hizmet altyapısının gelişmesini sağlayan, bunlardan elde edilen verileri yeniden değerlendirip ekonomik değere dönüştüren, altyapının gelişmesi ile verimliliği artıran ve pazara yeni girmek isteyen teşebbüsleri engelleyen durumlarla karşılaşmak olağandır. Ancak bunların tam bir rekabet ortamına kavuşmayı imkânsız hale getirdiği unutulmamalıdır. Veri taşınabilirliği hakkı ve birlikte çalışabilirlik gereksinimleri rekabeti desteklemeyi bir yan amaç edinirken, hakkın uygulanışı yönünden bu amacın gerçekleşip gerçekleşemeyeceği tartışmalara sebep olmuştur.

Dijital pazarlarda kullanıcı verilerinin işlenmesi ile büyüyen ve gelişen hizmet ve ürünler, pazarda rakiplere üstünlük sağlamanın en önemli kaynağını oluşturur. Bu

[288] US Department of Justice, *U.S. and Plaintiff States v. Ticketmaster Entertainment, Inc. and Live Nation Entertainment, Inc.,* 1:10-cv-00139, 30.07.2010, IX, C.
[289] **OECD**, *Competition Committee Discussion Paper*, s. 32.

sebeple pazardaki aktörler, kullanıcılar tarafından doğrudan sağlanan, çıkarsama ya da türetme yolu ile elde edilen verileri rakip teşebbüslerle paylaşma yönünde bir eğilime sahip değillerdir. Bu bakımdan teşebbüslerin veri taşınabilirliğini sınırlandırması kullanıcılar için bir teşebbüsten diğerine geçişte önemli bir geçiş maliyeti ("*switching cost*") yaratmaktadır. Geçiş maliyetleri, kullanıcıların bir teşebbüsten rakip bir teşebbüse geçerken katlanmak durumunda olduğu maliyeti ifade eder[290]. Kullanıcıların teşebbüsler arasında geçiş yaparken karşılaşabileceği zaman maliyeti, çaba gibi faktörler caydırıcı bir sonuç doğurmaktadır ki bu da kullanıcıların mevcut platformlarında adeta hapsolması anlamına gelen kilitlenme durumuna sebebiyet verir[291]. Elbette kilitlenme hali, kullanıcıların bir platforma geçiş ile mevcut platformda kalma arasında yapacakları karşılaştırma sonucuna bağlı olacaktır. Mevcut platformun değiştirilmesi suretiyle kullanıcının elde edeceği avantaj, geçiş maliyetlerini tolere edebiliyorsa kullanıcının teşebbüsler arasında geçişi önemli ölçüde etkilenmeyecektir. Veri taşınabilirliği hakkının kullanıcılara bir platformdan diğerine kişisel verileri ile beraber kolayca geçiş hakkı tanıması, veri ve işleme sistemlerini birlikte çalışabilir hale getiren açık standartların uygulanması yoluyla[292] kullanıcıların kilitlenme durumunu azaltabilecektir[293].

Öte yandan bir ağ içindeki mal veya hizmetin değeri bu mal veya hizmeti kullanan kişi sayısına bağlı olarak artış gösterir. Ağ etkileri ("*network externalities*") olarak adlandırılan bu durumun doğrudan etkisi, kullanıcı sayısının yüksek olduğu

[290] **Jones/Brenda**, s. 348.
[291] **Graef/Verschaleken/Valcke,** s. 59.
[292] **Mula, D.:** *The Right to Data Portability and Cloud Computing Consumer Laws,* Personal data in competition, consumer protection and intellectual property law: Towards a holistic approach. editor / Bakhoum, M./Conde Gallego, B./Mackenrodt, M-O&Surblytė-Namavičienė, G. Springer Verlag 2018 (MPI Studies on Intellectual Property and Competition Law), s. 404.
[293] **Graef**, Crossroads, s. 2

platformlara katılmanın katılan kullanıcı için değerinin yüksek olmasını; dolaylı etkisi ise kullanıcıların yoğun olduğu platformlara üretici, satıcı, tedarikçilerin daha fazla rağbet etmesidir[294]. Elbette bir ürün veya hizmeti daha çekici hale getiren bu faktör zamanla yoğunlaşmanın artmasına ve büyük veri avantajına bağlı olarak hâkim durumun daha hızlı gelişmesine yol açmaktadır[295]. Dahası ağ etkilerinin bulunması halinde kullanıcıların yalnızca geçiş maliyetlerini düşürmek pratik olarak büyük bir fayda sağlamayacaktır. Öyle ki kullanıcıların, diğer kullanıcılar dolayısıyla belirli bir yerde kalma arzusu devam edecektir[296].

Bunlara ek olarak pazardan elde edilen avantajın bir başka pazarda kullanılabilmesi teşebbüslerin karlılığını artırmaktadır. Dijital pazarlarda veri avantajından yararlanan teşebbüslerin, bir hizmetin sunulması ile elde ettikleri verileri bir başka ürün veya hizmet içi kullanarak daha verimli hale getirme imkânı bulunmaktadır[297]. Örneğin bir kitap satış sitesinde kişinin beğendiği veya satın aldığı kitaplardan yola çıkarak ilgi alanları veya mesleği tespit edilebilir ve bu alanlardaki sertifika hizmetlerinde önemli bir reklam avantajı elde edilebilir. Kapsam ekonomileri ("*economies of scope*") olarak adlandırılan bu durum, ağ etkilerinden beslenmektedir.

Kapsam ekonomilerine benzer şekilde ölçek ekonomileri ("*economies of scale*") de teşebbüslerin büyüklüğündeki artış ile verimliliğin artışı arasındaki korelasyonu ifade eder[298]. Zira verilerin toplanması ve bu verilerden değer üretilmesi

[294] **Graef**, I.: *Mandating portability and interoperability in online social networks: regulatory and competition law issues in the European Union*, Telecommunications Policy 2015, Vol. 39(6), s. 510; **Krämer**, s. 274; **Martinelli**, s. 136.
[295] **Martinelli**, s. 136-137.
[296] **Krämer**, s. 274.
[297] **European Commission, Directorate-General for Competition, Montjoye, Y./Schweitzer, H./Crémer, J.,** s. 33.
[298] Detaylı açıklamalar için bkz. **Whish/Bailey**, s. 10.

teşebbüsler için sabit bir maliyete sebep olur[299]. Ağ etkilerinde kullanıcılar arasında ortaya çıkan cazibe durumundan faydalanılarak ölçek ekonomilerinde girdi olarak elde edilen veri miktarı ve çeşitliliği arttıkça teşebbüsün ürün ve hizmetleri geliştirmekte kullanabileceği girdi de artmış olmaktadır. Kalitesi yükselen ürün ve hizmetler ise kullanıcıları teşebbüse çeken bir faktör oluşturur.

Veri taşınabilirliği hakkı çerçevesinde pazarda gündeme gelebilecek karakteristik problemlerden söz ederken pazardaki aktörlerin pazara dahil olmalarını ve ayrılmalarını etkileyen hususların da irdelenmesi gerekir. Veri taşınabilirliği hakkının olmadığı durumda kullanıcıların bir veri sorumlusundan diğerine geçmeyi düşünmesi önemli geçiş maliyetlerinin de hesaba katılması ihtiyacını doğurmaktadır. Tıpkı GDPR m. 20 ile öngörülen veri taşınabilirliği hakkından çok daha önce uygulaması başlayan numara taşınabilirliğinde olduğu gibi kullanıcıların yaşadığı bu kaygı yeni aktörlerin pazara katılma motivasyonlarını azaltmakta ve pazara giriş engeli ("*barriers to entry*") oluşturmaktadır[300]. Zira veri temelli dijital pazarlarda pazara giriş engelleri işlenen verinin miktarından doğrudan etkilenir. Büyük ölçekli teşebbüsler daha fazla kullanıcıya hitap ettiğinden veri elde etme ve analiz etmede küçük ölçekli işletmelere göre daha avantajlı bir konumdadır. Küçük ölçekli teşebbüslerin bu verilere ulaşamayacak durumda olması pazara girişte önemli bir maliyet doğurmakta olup bu verileri yeniden oluşturmak zorunda kalması sosyal açıdan bir israf[301] olarak değerlendirilmektedir. Üstelik kullanıcıların mevcut teşebbüsten başka bir teşebbüse geçmelerini engelleyen geçiş maliyetlerinin oluşturduğu bağımlılık yeni girenlerin tercih edilebilirliğini azaltmaktadır. Bir kısım yazarlar bu hususdan yola çıkarak veri

[299] **OECD**, *Data portability, interoperability and digital platform competition, OECD Competition Committee Discussion Paper*, s. 12.
[300] **Lucchini/Moscianese/de Angelis/Di Benedetto**, s. 565.
[301] **Kathuria/Lai**, s. 1294.

taşınabilirliği hakkının rekabeti artırıcı bir etki gösterdiğini belirtmekte ancak bunun ileride rekabet hukuku sorunları doğurma ihtimaline karşı şüphe ile yaklaşmaktadırlar[302]. Tüm bunlara ek olarak Veri Transferi Projesi gibi veri taşınabilirliğini destekleyen girişimlerin teknoloji devi olarak nitelendirilebilecek teşebbüslerce yürütülmesi esasen, veri taşınabilirliği hakkını icra etmeye elverişli sistemlerin ve teknik altyapının oluşturulmasının önemli bir maliyet unsuru oluşturması ve küçük ölçekli teşebbüslere nazaran büyük ölçekli teşebbüslerin bu maliyet kalemlerini daha kolay karşılayabileceği düşüncesi olabilir.

VII. DEĞERLENDİRME

Veri taşınabilirliği hakkının rekabeti olumlu etkileyeceği düşüncesini savunanlar, geçiş maliyetlerinin düşeceğini, pazara girişin kolaylaşacağını, inovasyonların desteklenmesi için gerekli veri tabanlarının büyüyeceğini ve gelişeceğini[303] ve bu sayede teşebbüsler arasında rekabetin yoğunlaşacağını düşünmektedir[304]. Veri tabanlarının gelişmesi, kullanıcılara doğrudan hitap eden ürünlerin geliştirilmesi ile ürün maliyetlerini düşürebilir[305] ki bu da tüketici refahını artıracaktır. Hakkın uygulanmasının ilgili kişinin talebine bağlı olması dolayısıyla tüketici merkezli bir çözüm getirdiğini, bu anlamda veri sorumlularına doğrudan bir veri paylaşma yükümlülüğü getirmekten daha az etkili olsa da bir dereceye kadar rekabeti destekleyecek bir düzenleme olduğunu belirtenler de bulunmaktadır[306]. Konu

---

[302] **Lucchini/Moscianese/de Angelis/Di Benedetto**, s. 565.
[303] **Vezzoso**, s. 361-362.
[304] **Giovannetti**, E./**Siciliani**, P.: *The Impact of Data Portability on Platform Competition*, CPI Antitrust Chronicle November 2020, (https://www.competitionpolicyinternational.com/the-impact-of-data-portability-on-platform-competition/, E. T.: 06.05.2022).
[305] **Personal Data Protection Commission In collaboration with Competition and Consumer Commission of Singapore,** *Discussion Paper on Data Portability*, 2019, (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf, E. T.: 06.05.2022), s. 10.
[306] **Graef, I.:** *The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation*, CPI Antitrust Chronicle November 2020,

ile ilgili araştırmalar neticesinde hazırlanmış çeşitli raporlarda da kullanıcıların tek bir platforma kilitlenmesine ve pazara giriş engellerine sebep olabilecek durumlarda veri taşınabilirliği hakkının etkili bir çözüm getirdiği ifade edilmektedir[307]. GDPR m. 20 ile tanınan veri taşınabilirliği hakkını, dijital platformlar veya finansal kuruluşlar gibi sınır ötesi yayılım gösteren sektörler açısından değerlendiren bir görüş, Avrupa merkezli veri sorumlularının kişisel verilere erişim noktasında, bu verilere erişmek için özel algoritmalar geliştirmek mecburiyetinde kalan ABD merkezli şirketlere göre önemli bir avantaj elde ettiğini ileri sürmektedir[308]. Bankacılık sektörünü baz alan bir değerlendirmede veri taşınabilirliği ve açık bankacılık girişimlerinin yerleşik şirketleri ürün ve hizmetlerinde rekabet etmeye zorlayacağı belirtilmektedir[309]. Ayrıca kullanıcıların tüketici olarak daha fazla korunmasına da imkân vereceği, tüketici

(https://www.competitionpolicyinternational.com/the-opportunities-and-limits-of-data-portability-for-stimulating-competition-and-innovation/, E. T.: 06.05.2022). **Ramos**, E. F./**Blind**, K.: *Data portability effects on data-driven innovation of online platforms: Analyzing Spotify*, Telecommunications Policy 2020, Vol. 44(9), 102026, s. 13; **Vanberg**, s. 17; **Vezzoso**, s. 363.

[307] **Personal Data Protection Commission In collaboration with Competition and Consumer Commission of Singapore,** *Discussion Paper on Data Portability*, 2019, s. 9; **Stigler Center for the Study of the Economy and the State,** *Stigler Committee on Digital Platforms Final Report*, s. 16; **United Kingdom, Competition and Markets Authority**, *Online Platforms and Digital Advertising Market Study Final Report*, 2020, (https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, E. T.:06.05.2022), , s. 24.; **United States Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary**, *Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations*, 2020, (https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519, E. T.: 06.05.2022), s. 384. Ayrıca Avustralya Rekabet ve Tüketici Komisyonu veri taşınabilirliği ve birlikte çalışabilirliğin olumlu etkileri olabileceğini kabul etmekle beraber ağ etkileri ve pazara giriş engellerinin azalacağı beklentisi yönünden temkinli yaklaşmakta, bir bakıma hakkın etkilerinin gözlemlenmesi için zamana ihtiyaç olduğunu belirtmektedir. Bkz. **ACCC,** *Digital Platforms Inquiry Report*, s. 11.

[308] **Stites**, T.: *Data Protection on the Doorstep: How the GDPR Impacts American Financial Institutions*, Review Of Banking & Financial Law 2018, Vol. 38, s. 141. Yazar Fintech şirketleri nezdinde yaptığı değerlendirmede GDPR m. 20'nin Avrupa'da yarattığı olumlu hava dolayısıyla *Facebook* veya *Google* tipi bir Fintech'in Avrupa'da kurulma olasılığının da daha yüksek olduğunu ifade etmektedir. Bu durumdan hareketle ABD'de Tüketici Mali Koruma Bürosu'nun ("*Consumer Financial Protection Bureau*") GDPR'dakine benzer veri taşınabilirliği ilkelerini benimsemesinin olası olduğuna dikkat çekmektedir. Bkz. **Stites**, s. 142.

[309] **Borgogno**, O./**Colangelo**, G.: *Open Banking and the Ambiguous Competitive Effects of Data Portability*, Competition Policy International Antitrust Chronicle April 2021, (https://www.competitionpolicyinternational.com/open-banking-and-the-ambiguous-competitive-effects-of-data-portability/, E. T.: 06.05.2022).

hukukunun zayıf taraf olan tüketiciyi korumayı amaçladığı göz önüne alındığında bu amacın veri taşınabilirliği hakkı ile destekleneceği de ifade edilmektedir[310].

Veri taşınabilirliği hakkının rekabeti koruma ve geliştirme işlevi olduğunu savunanlar kadar beklenen bu etkiyi karşılamak bakımından yetersiz olduğunu ileri sürenler de mevcuttur. Hatta GDPR'ın veri taşınabilirliği hakkı ile sınırlı bir etki doğurabildiği ve uygulamada hala pek çok güçlüğün olduğu, veri taşınabilirliği hakkının henüz pazara giriş engellerini azaltmak ve rekabeti desteklemek yönünden yetersiz kaldığı Dijital Pazarlar Yasası Etki Değerlendirmesi Raporu'nda da kabul edilmiştir[311]. Aslında veri taşınabilirliği hakkı değiştirme maliyetleri ve pazara giriş engellerinin yanında ağ etkilerini de azaltmaya elverişli olabilir. Ancak bu yeterli sayıda kullanıcının veri taşınabilirliği hakkını kullanması ile mümkündür. Zira veri taşınabilirliği, ilgili kişinin talebi üzerine başlatılan bir süreçtir. Hakkın sağladığı bir diğer avantaj, zorunlu unsur doktrini uyarınca hâkim teşebbüslerin rakip teşebbüslere veri sağlama yükümlülüğünde, kullanıcıların kişisel verileri anonimleştirilerek iletilirken ilgili kişinin talebi ile gerçekleştirilen veri taşınabilirliği işleminde kişisel verilerin olduğu gibi iletilebilmesidir[312]. Bir görüş, GDPR m. 20 ile öngörülen veri taşınabilirliği hakkının üçüncü kişilerin hak ve özgürlüklerinin olumsuz etkilenmemesi gibi kısıtlamalara tabi tutulması karşısında standart veri taşınabilirliği hakkı ile iletilemeyen kişisel verilerin "kimlik taşınabilirliği" çerçevesinde iletilebileceğini öne sürmektedir[313]. Bu görüş çerçevesinde kimlik taşınabilirliği, ilgili

[310] **Elfering**, s. 57.
[311] European Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulatio of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), SWD(2020) 363 final, 15.12.2020, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0363, E. T.: 06.05.2022), s. 36.
[312] **Krämer**, s. 276.
[313] **Gans**, J.: *Enhancing Competition with Data and Identity Portability,* Hamilton Project Policy Brief 2018-10, s. 12-13.

kişinin taşınmasını talep ettiği kişisel verileri içerisinde üçüncü kişilere ait kişisel verilerin de bulunması durumunda üçüncü kişinin, belirlediği ilgili kişinin taşınabilirlik talepleri yönünden kendi kişisel verilerinin alıcı veri sorumlusunca işlenmesine rıza göstermiş sayılması olarak açıklanabilir. Buna göre, A kişisine mesaj alma ve gönderme izni verilirse ve A kişisi kullanmakta olduğu servis sağlayıcısını değiştirirse, A kişisi için verilmiş olan izin geçerliliğini sürdürecek ve yeni servis sağlayıcıdan da mesaj alışverişine devam edilebilecektir.

Oyun teorisinden yola çıkarak veri taşınabilirliği hakkı özelinde rekabet etki değerlendirmesinde bulunan bir görüş, hakkın geçiş maliyetlerini azaltması dolayısıyla tüketicilerin herhangi bir çekince duymaksızın çok daha fazla miktarda ve çeşitte verilerini yerleşik teşebbüslerle paylaşacağını, bunun yerleşik teşebbüsler için devasa bir veri analizi etkisi ve rekabetçi konum avantajı doğuracağını, sonuç olarak pazara giriş engelleri oluşacağını ve hakkın uzun vadede inovasyonu ve verimliliği azaltacağını belirtmektedir[314]. Geçiş maliyetlerinin azaltılmasına karşın ağ etkileri dolayısıyla veri taşınabilirliği hakkının yeterince işlevsel olmayacağını savunan bir görüş, söz konusu yetersizliğin, toplu taşınabilirlik düzenlemeleri ile giderilebileceğini öne sürmektedir[315]. Buna göre, kullanıcı gruplarının toplu olarak yeni bir teşebbüse geçmesi, kullanıcıların geride bırakacakları bir şey olmadığından geçiş maliyetlerini düşürürken söz konusu grubun özelliklerini dikkate alarak onların ihtiyaçlarına yönelik ürün oluşturulabilir. Bu durum ise ölçek ekonomileri ile ağ etkilerinin azaltılmasına yardımcı olur[316]. İstenmeyen etkilerin önlenmesinin bir başka yolu

[314] **Lam**, W. M. W./**Liu**, X.: *Does data portability facilitate entry?*, International Journal of Industrial Organization 2020, Vol. 69, 102564, s. 9-10.
[315] **Nicholas**, G.: *Taking It With You: Platform Barriers to Entry and the Limits of Data Portability*, Michigan Technology Law Review 2021, Vol. 27, s. 263-298.
[316] **Nicholas**, s. 293-294.

olarak asimetrik düzenleme ve yaptırım önerilmiştir[317]. Bunun anlamı, daha güçlü ve büyük ölçekli teşebbüslere uygulama bakımından daha katı davranılmasıdır. Ancak bu öneri de pazarda tarafsızlığın bozulmasına anlamına gelebileceğinden eleştirilmiştir[318].

Rekabet hukuku perspektifinden veri taşınabilirliği hakkını değerlendirenlerin bir kısmı ise hakkın rekabeti desteklemekten ziyade pazarda rekabeti daha çok kısıtlayıcı bir etki göstereceğini savunmaktadır. Bir görüş, oyun teorisi modelinden hareketle pazarda yerleşik veri sorumluları ile pazara yeni girecek veri sorumluları açısından hakkın etkilerini değerlendirmekte, pazarda yerleşik veri sorumlusunun yeni girenlere nazaran daha düşük ücret talep edeceğini, yerleşik veri sorumlularının karları düşerken yeni girenlerin daha yüksek karlılığa sahip olacaklarını, yerleşik veri sorumluları tarafından daha düşük ücretlerle karşılaşan tüketicilerin daha avantajlı durumda olacaklarını, yeni girenlerin yüksek ücretleri karşısında ise daha kötü durumda olacaklarını belirtmektedir[319]. Bu görüşün sunduğu en önemli argüman pazarda yerleşik teşebbüsün eski müşterileri veri taşınabilirliği hakkı ile daha iyi bir konuma kavuşacakken yeni müşterilerin, pazara yeni girenlerin rekabetçi konumunun güçlenmesi ile daha kötü bir duruma düşmesinin muhtemel olduğunu ortaya koymasıdır. Zira bu halde değiştirme maliyetleri azalmış olsa da bunun tüm tüketicilerin yararına olmadığı sonucuna varılmaktadır.

---

[317] **Graef,** Stimulating Competition, s. 5; **Ishii**, K.: *Discussions on the Right to Data Portability from Legal Perspectives*, Kreps, D./Ess, C./Leenen, L./Kimppa, K. (eds) This Changes Everything – ICT and Climate Change: What Can We Do?. HCC13 2018. IFIP Advances in Information and Communication Technology, vol 537. Springer, Cham., s. 352.

[318] **Wohlfarth**, M.: *Data Portability on the Internet an Economic Analysis*, Bus Inf Syst Eng 2019, Vol. 61(5), s. 564.

[319] **Krämer**, J./**Stüdlein**, N.: *Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the General Data Protection Regulation*, Economics Letters 2019, Vol. 181, s. 102.

Geçiş maliyetlerinin veri taşınabilirliği hakkı ile azalabileceğini kabul eden bir görüş, küçük ölçekli teşebbüslerin başlangıçta daha düşük ücretlerle hizmet veya ürün sunan teşebbüsleri tercih ederken, geçiş maliyetlerinin azalmış olması dolayısıyla bu teşebbüsleri kolaylıkla terk ederek büyük teşebbüsleri tercih edebileceği ve bunun da büyük ölçekli teşebbüsler lehine bir durum yaratacağını ifade etmektedir[320].

Ayrıca veri taşınabilirliği hakkını tam anlamıyla uygulamaya elverişli birlikte çalışabilir sistemlerin kurulması ve EIM modüllerinin kabul edilmesinin küçük ve orta ölçekteki işletmeler için maliyetli olması gerçeği karşısında hakkın uygulanışının pazara giriş engeli teşkil edecek ve inovasyonu azaltacak ölçüde orantısız maliyetlere sebep olmaması gerektiğini ifade edenler de bulunmaktadır[321]. Konuya bir başka bakış açısı, birlikte çalışabilirlik standartlarının büyük teşebbüslerce benimsenmesinin küçük ve orta çaplı teşebbüsler açısından uyum maliyetini daha da yükseltecek şekilde tasarlanması tehlikesi doğurabileceğine dikkat çekmektedir[322].

Veri taşınabilirliği hakkının rekabeti olumsuz etkileyeceğini savunan bir başka görüş, veri taşınabilirliği hakkının her çevrimiçi hizmet için uygulanmasının ve teşebbüslerin topladıkları verileri bir başka teşebbüse iletme yükümlülüğü altında kalmasının veri toplama ile bunları ekonomik bir değere dönüştürme teşvikini azaltacağını ve bunun da tüketici refahı üzerinde beklenenin aksine bir etki göstereceğini savunmaktadır[323]. Aynı hususta yola çıkan bazı yazarlar konuya Dijital Pazarlar Yasası taslağında öngörülen birlikte çalışabilirlik gereksinimi çerçevesinden

---

[320] **Nicholas**, s. 274.
[321] Birleşik Krallık Parlamentosu, İş, Yenilik ve Yetenekler Bakanlığı'ndan sorumlu devlet müsteşarı Baroness Neville Rolfe'nin 14 Aralık 2015 tarihli konuşmasında geçen ifade için bkz. (https://www.parliamentlive.tv/Event/Index/03e4655b-f6e9-44e6-b797-a6139c4b9156, E. T.: 10.05.2022); **Swire/Lagos**, s. 351.
[322] **Gal**, M. S./**Aviv**, O.: *The Competitive Effects of the GDPR*, Journal of Competition Law & Economics 2020, Vol. 16(3), s. 373-374.
[323] **Swire/Lagos**, s. 349; **Wohlfarth**, s. 564.

bakarak, birlikte çalışabilirlik esasının rakip teşebbüslerin sundukları hizmetlerin geliştirilmesine katkıda bulunabileceğini ifade etmekle beraber bu yükümlülüklerin platformlarda veri toplama teşvikini ve inovasyonu azaltma eğilimi yaratabileceği vurgulamaktadır[324].

Diğer bir görüş birlikte çalışabilirlik esaslarının teşebbüslerin sundukları hizmetlerde ve yazılımlarda standartların benimsenmesi dolayısıyla tek tipleşmenin artacağına, bu standartlara uyma yükümlülüğünün inovasyonları olumsuz etkileyeceğine, kullanıcılar açısından ise risklere sebep olabileceğine işaret etmektedir[325]. Keza pazara girişlerin de beklendiği gibi kolaylaşmayacağı, aksine giriş engellerinin artacağını düşünenler bulunmaktadır. Buna göre, pazara yeni katılan teşebbüsler açısından söz konusu olabilecek olumsuzlukların en başında veri taşınabilirliği ve birlikte çalışabilirlik gereksinimlerini sağlamanın bu teşebbüsler açısından ek maliyet anlamına gelmesidir[326].

Veri taşınabilirliği ve birlikte çalışabilirliğin hakikaten rekabeti desteklemeye elverişli olup olmadığı hakkın uygulandığı sektörün özellikleri ile de ilişkilidir[327]. Teknik açıdan uygulanabilirliğin halihazırda mevcut olduğu veya düşük maliyetlerle sağlanabileceği durumlarda kullanıcılara yansıyacak önemli bir maliyet olmayacağı gibi pazara yeni giren teşebbüslerin de pazarda faaliyet gösterebilmesi için oluşturdukları sistemlerden çok büyük sapma gerçekleştirmeden GDPR m. 20'deki

---

[324] **Jenny**, s. 1162.

[325] **Graef**, I./**Husovec**, M./**Putova**, N.: *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, German Law Journal 2018, Vol. 19, No. 6, s. 1387; **Kerber**, W./**Schweitzer**, H.: *Interoperability in the digital economy*, Journal of Intellectual Property, Information Technology and E-Commerce Law 2017, Vol.8, s. 42.; **OECD**, *Data Portability, Interoperability and Digital Platform Competition*, s. 22. Karş. **Engels**, s. 8.

[326] **Körber**, T.: *Is Knowledge (Market) Power? - On the Relationship Between Data Protection, 'Data Power' and Competition Law*, 2018, s. 18.

[327] **OECD**, *Data portability, interoperability and digital platform competition, OECD Competition Committee Discussion Paper*, s. 17.

gerekliliklerle uyumlanması mümkün olabilecektir[328]. Buna karşılık söz konusu teşebbüsün bulunduğu sektörün genel özellikleri de dikkate alındığında teknik açıdan uygulanabilir sistemler oluşturulmasının sektörel açıdan bir önem taşımadığı, bu sistemleri kurmanın sektörde kullanılan teknoloji üzerinden düşünüldüğünde ek maliyetler getirdiği durumlarda rekabeti koruma ve destekleme işlevini sağlamaktan uzaklaşılacağı düşünülebilir. Keza verinin yoğun olarak işlenmediği, temel girdiyi meydana getirmediği sektörlerde işlenen kişisel verilerin daha basit düzeyde kalması böyle bir maliyete katlanmayı gereksiz de kılabilir. Örneğin bir pazarda yalnızca müşterilerin isim, adres ve iletişim bilgileri ile çalışanlara ait kişisel verilerin işlenmesinin yeterli olduğu varsayımında, bu nitelikteki verilerin taşınması için gerekli altyapının oluşturulmasını beklemek büyük bir değer taşımayacaktır. Zira bu nitelikteki verinin müşterileri mevcut teşebbüste kilitlenme haline sokacak ve pazara giriş engeli yaratacak ağırlıkta olduğunu söylemek pek mümkün görünmemektedir. Oysa giyilebilir teknoloji ürünleri ile kaydedilen sağlık verilerinin ve bunlardan üretilen ikincil verilerin işlendiği ve analiz edildiği bir pazarda işlenen verilerin değiştirme maliyetleri ve pazara giriş engelleri yönünden aynı etkiye sahip olduğu düşünülemeyecektir.

Doktrinde ifade edilen tüm bu görüş ve endişeler ışığında veri taşınabilirliği hakkının rekabet hukuku bağlamında dikkate değer bir konumda olduğu görülmektedir. Her ne kadar GDPR m. 20 düzenlemesi veri sorumluları arasında bir ayrım yapmaksızın ilgili kişiye veri taşınabilirliği hakkı tanımışsa da hakkın büyük

[328] Bu husus bir taraftan yeni girenler için ek maliyet olarak algılanırken diğer taraftan pazarda eskiden beri var olan teşebbüslerin sistemlerini veri taşınabilirliği ve birlikte çalışabilirliğe uyumlu hale getirmesinin, yeni girenlerin bu standartta sistemler kurmasından daha fazla uyumluluk maliyetine sebep olacağı değerlendirmesi için bkz. **Personal Data Protection Commission In collaboration with Competition and Consumer Commission of Singapore,** *Discussion Paper on Data Portability*, s. 19.

oranda dijital pazarlarda uygulanabileceği açıktır. Dijital pazarlardaki yoğunlaşma, geçiş maliyetleri sebebiyle kullanıcı kilitlenmesi, ağ etkileri, ölçek ve kapsam ekonomileri göz önüne alındığında kullanıcılar yönünden, bunlara bağlı olarak ortaya çıkan pazara giriş engelleri ile olası rakip teşebbüsler yönünden hakkın umut verici olduğu anlaşılmaktadır. Henüz hakkın uygulamasına ilişkin somut örneklerin bulunmaması ve nispeten yeni sayılabilecek olması hakkın lehine ve aleyhine yapılan tüm yorumları şimdilik birer tahmin kılmaktadır. Buna karşılık hem hakkın rekabeti destekleyeceği düşüncesini savunanların hem de rekabeti olumsuz etkileyeceği düşüncesinde olanların kabul edilebilir gerekçeleri bulunmaktadır. Bunların başında veri sorumluları arasında hiçbir ayrım yapılmamış olması dolayısıyla küçük ve ortak ölçekteki veri sorumlusu teşebbüslerin olumsuz etkilenme ihtimallerinin kuvvetli görünmesidir.

Yukarıda rekabet hukuku ve politikaları ile yasaklanan davranışlar çerçevesinde incelendiği üzere veri taşınabilirliği hakkının uygulanmasında, kendine özgü şartları gerçekleştiği takdirde rekabet hukuku zorlayıcı bir konumda bulunmaktadır. Ne var ki TFEU m. 102 yalnızca hakim durumdaki teşebbüsün veri taşınabilirliği ve birlikte çalışabilirlik adımları atmasını zorunlu kılmaktadır. Benzer şekilde DMA da yalnızca dijital pazarlarda geçit bekçisi konumundaki veri sorumlusu teşebbüslere yönelik bir düzenleme getirmektedir. GDPR m. 20'nin her pazarda çok daha geniş bir veri sorumlusu kitlesine hitap etmesi, dijital pazarlar dışındaki pazarlardaki veya hakim durumda olmayan veri sorumlusu teşebbüslerin de maddedeki şartlar sağlandığı takdirde veri taşınabilirliği taleplerine maruz kalacağı göz önüne alındığında TFEU m. 102 ve DMA gibi rekabeti koruyucu düzenlemelerin varlığına karşın kişisel verilerin korunmasını amaçlayan bir düzenlemede neden

rekabeti destekleme hedefi taşıyan bir hakka yer verildiği de anlaşılmaktadır. Kişisel verilerin korunması alanındaki düzenleme kişisel veriler üzerinde daha fazla söz sahibi olma imkânı getirirken, rekabetin desteklenmesi amacının gerçekleşip gerçekleşmemesi yahut bilinçli olarak rekabetin engellenmesi meselesinin değerlendirmesini rekabet hukuku ve politikalarına bırakmaktadır. Bu durumda, veri taşınabilirliği hakkının kullanılmasını engellemek maksadıyla teknik altyapıyı oluşturmayan hâkim durumdaki veri sorumlusu teşebbüsün rekabet otoritesi tarafından denetleneceğini bilmesi, bu teşebbüs açısından zımni bir yükümlülüğün bulunduğu şeklinde yorumlanabilir. Bu ise dolaylı biçimde rekabetin desteklenmesi amacını gerçekleştirebilir. Veri taşınabilirliği hakkının pratik faydasının pek fazla olmadığı sektörlerde ise hâkim durumdaki teşebbüs için dahi birlikte çalışabilir sistemlerin bulunmaması zorunlu unsurun karşılanmasının reddedilmesi anlamına gelmeyeceği için bir yükümlülükten bahsetmek güçtür. Bu sebepledir ki anti rekabetçi davranışlar yönünden veri taşınabilirliği hakkı ve birlikte çalışabilirlik zorunlu unsur doktrini ekseninde değerlendirildiğinde rekabeti olumsuz etkileyecek bir potansiyel göstermemektedir. GDPR, ilgili kişilerin sahip oldukları hakları genişletirken bu hakkın kullanımını sağlayacak yolu her veri sorumlusu için zorunlu tutmamaktadır. Bu sayede veri taşınabilirliğini sağlamaya yönelik teknik altyapının oluşturulması için katlanılan maliyetlerin tüketici refahını olumsuz etkilediği durumlarda veri sorumlularına adeta bir açık kapı bırakılmakta, olumsuz bir etkinin doğmadığı hallerde hakkın uygulanması teşvik edilmekte, hakkın uygulanmasının engellenmesi suretiyle ilgili pazarlarda rekabeti bozucu sonuçların doğması halini ise rekabet hukuku ve politikaları çerçevesinde incelemelere bırakmaktadır.

Her halükarda bir kısım yazarın savunduğu gibi, her iki hukuk alanının kesiştiği bir bölgede bulunan veri taşınabilirliği hakkının tanınmasında sektörel özellikler, pazarda genel olarak kullanılan teknolojik altyapılar, veri sorumlularının büyüklükleri, pazarda hakimiyetin tespiti gibi birtakım ölçütler ile hakkın sınırlarının çizilmesinin, bu bağlamda bazı veri sorumlularına belirli şartlarda yükümlülük getirilirken bazılarının istisna tutulmasının, GDPR m. 3 kapsamındaki veri sorumlularını topyekûn hedef tutan bir düzenlemeden daha isabetli olup olmayacağı; mevcut hali ile veri taşınabilirliği ve birlikte çalışabilirlik hedeflerinin, birtakım veri sorumlularına ek maliyetler oluşturmak suretiyle tüketicilere yansıyan ve böylece tüketici refahını azaltan bir etki doğurmaya elverişli olup olmadığı hakkın uygulanması ile zaman içinde anlaşılacaktır.

Son olarak belirtmek gerekir ki kişisel veri koruma hukuku alanının her geçen gün daha büyük önem kazanması Türk hukukunda henüz düzenlenmemiş olan veri taşınabilirliği hakkının, Türk hukuk düzenine dahil edilmesinin pek de uzak olmadığını göstermektedir. Nitekim dijital pazarlarda yarışabilmek için veri akışının sağladığı avantajdan yararlanmak bir zorunluluk haline gelmektedir. Dahası verilerin yeniden kullanılabilmesi ve akışının sağlanması özellikle dijital pazarlarda sürdürülebilirliğin önemli bir parçasını oluşturur. Rekabet hukuku düzenlemeleri yönünden yukarıda da değinildiği üzere Avrupa Birliği'ndeki düzenlemelere paralel esasların benimsenmiş olduğu hukukumuzda, veri taşınabilirliği hakkına yönelik rekabet hukuku endişelerinin aynen geçerli olacağını söylemek mümkündür. Bu sebeple konu ile ilgili ciddi bir yasama çalışmasının bulunması halinde Avrupa Birliği'nin deneyimlerinden yararlanmak kadar Türk rekabet otoritesi Rekabet

Kurumu ile iş birliği içerisinde olmak ve hakkı rekabet hukuku başta olmak üzere her alanda desteklemek gerekmektedir.

SONUÇ

Kişisel verilerin korunmasına duyulan ihtiyacın artması ulusal ve uluslararası düzenlemelerin yapılması gerekliliğini doğurmuştur. Bu kapsamda Avrupa Birliği tarafından kabul edilen 95/46/AT sayılı Direktif esas alınarak Türk hukukunda da 6698 sayılı KVKK yürürlüğe girmiştir. KVKK'nın kabul edilmesinden kısa bir süre sonra Avrupa Birliği'nde GDPR kabul edilmiş, bu düzenleme 95/46/AT sayılı Direktif'i yürürlükten kaldırmıştır. Direktif'e göre çok daha kapsamlı hükümler içeren GDPR'ın tanıttığı en önemli haklardan bir tanesi veri taşınabilirliği hakkıdır.

GDPR'ın veri taşınabilirliği hakkını sunmasından önce birtakım sektörel ve özel düzenlemeler ile sınırlı kapsamda veri taşınabilirliği uygulamaları olduğu ve rekabet hukuku incelemelerinde konunun rekabeti etkileyen boyutuyla ele alındığı görülmektedir. KVKK'nın yapımı esnasında 95/46/AT sayılı Direktif'in esas alınması dolayısıyla Türk hukukunda veri taşınabilirliği hakkına ilişkin bir düzenleme getirilmemiştir. Buna karşılık ikincil düzenlemelerde etki alanı son derece dar olmakla beraber veri taşınabilirliği ve birlikte çalışabilirlik minvalinde politika ve düzenlemelere rastlanmaktadır.

Veri taşınabilirliği hakkı GDPR'ın 20. maddesinde bir ilgili kişi hakkı olarak tanınmıştır. Madde uyarınca ilgili kişinin kendisi ile ilgili olarak bir veri sorumlusuna sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma ve kişisel verilerin sağlandığı veri sorumlusunun herhangi bir engellemesi olmaksızın bu verileri başka bir veri sorumlusuna iletme, teknik açıdan uygulanabilir olması halinde, kişisel verileri doğrudan bir veri sorumlusundan diğerine ilettirme hakkı bulunmaktadır. Buna karşılık hakkın kapsamı ve uygulanması bakımından madde metninden ne anlaşılması

gerektiği, hakkın amacı ve sınırları pek çok belirsizliğe ve eleştiriye sebep olmaktadır. Nitekim yapılan sosyal araştırmalar hakkın uygulanmasının gerek veri sorumluları gerekse ilgili kişilerce tam olarak anlaşılmadığını ortaya koymaktadır.

Maddenin lafzından anlaşıldığı üzere ilgili kişinin veri taşınabilirliği hakkını kullanması iki şekilde mümkün olmaktadır: veri sorumlusunda bulunan kişisel verilerin alınması ve bir başka sorumlusuna iletilmesi veya kişisel verilerin mevcut veri sorumlusu tarafından bir başka veri sorumlusuna doğrudan iletilmesi. Hakkın ilk kullanılış biçimi dolaylı taşınabilirlik, ikincisi ise doğrudan taşınabilirlik olarak adlandırılmaktadır. Hakkın işlerlik kazanabilmesi için ilgili kişinin kendisi ile ilişkili kişisel verileri veri sorumlusuna açık rıza ile sağlaması veya sözleşme dolayısıyla işleme faaliyetinin gerçekleşmiş olması gerekmektedir. Ayrıca bu hukuki sebeple işlenen kişisel veriler otomatik yollarla işlenmiş olmalıdır. Söz konusu şartlar sağlandığı takdirde ilgili kişi dolaylı taşınabilirlik çerçevesinde kişisel verilerini, bir modele bağlı olarak çalışan yapılandırılmış veya yarı yapılandırılmış, hakkın kullanımını pratikte anlamsız hale getirmeyecek ölçüde yaygın olarak kullanılan ve yazılım uygulamalarının kolayca tanımlayabileceği makine tarafından okunabilir bir formatta alma ve mevcut veri sorumlusunun engellemesine maruz kalmaksızın bir başka veri sorumlusuna iletme hakkına sahiptir. Uygulamanın kolaylaşması ve daha verimli olması için söz konusu kişisel verilere ilişkin metaverilerin de olabildiğince çok ve tutarlı şekilde oluşturulması gerekmektedir. Doğrudan taşınabilirlik hakkının kullanılabilmesi içinse teknik açıdan uygulanabilirlik şartı getirilmiş ancak bu şartı sağlama zorunluluğu öngörülmemiştir. Teknik açıdan uygulanabilirlik veri sorumlularının birbirleri arasında veri paylaşımı gerçekleştirebilecekleri uygun bir altyapının oluşturulması anlamına gelmektedir. Her ne kadar madde metninde ifade

edilmese de bu şartı sağlamak için bilgi sistemleri arasında iletişim kurulabilmesi anlamına gelen birlikte çalışabilirlik esaslarının da benimsenmesi gerekmektedir.

Veri taşınabilirliği hakkı GDPR'da yer alan birtakım düzenlemelerle benzerlik göstermekte ancak içerik yönünden bunlardan ayrılmaktadır. İlk olarak kişisel verilerin üçüncü kişilere aktarılması bakımından incelendiğinde kişisel verilerin aktarımına ilişkin koşullar bir ölçüde veri taşınabilirliği hakkına da uygulanmaktadır ancak veri taşınabilirliği hakkı basit biçimde aktarım faaliyetine indirgenemeyecek bir içeriğe sahiptir. Bu sebeple GDPR veri taşınabilirliği hakkını düzenlerken bir başka veri sorumlusuna aktarma değil, iletme hakkından bahsetmektedir. İkinci olarak hak, erişim hakkına benzetilmekte ise de kapsam ve şartlar yönünden erişim hakkından önemli farklılıklar göstermekte, erişim hakkı basit bir elde etme hakkını ifade ederken veri taşınabilirliği hakkı verilerin yeniden kullanılabilmesine imkân veren ve bunu kolaylaştıran bir düzenleme içermektedir. Üçüncü olarak ise veri taşınabilirliği hakkının kullanılması mevcut veri sorumlusunda bulunan kişisel verilerin veri taşınabilirliği talebi üzerine doğrudan silinmesini gerektirmez. Bu husus ilgili kişinin kişisel verilerinin silinmesi yönündeki talebine bırakılmıştır.

Hakkın yer bakımından kapsamı GDPR m. 3'te öngörülen esaslara bağlıdır. Konu bakımından kapsamı ise rıza veya sözleşmeye dayalı işleme faaliyetini, ilgili kişinin kendisi tarafından veri sorumlusuna verilerin veya veri sorumlusunun sunduğu ürün ve hizmetlerin kullanılması yoluyla kullanım amacına uygun olarak veri sorumlusunca elde edilen ve otomatik yollarla tutulan kişisel verileri kapsamaktadır.

GDPR'da ilgili kişilerin haklarını kullanmaları bakımından öngörülmüş genel sınırlama sebepleri yanında, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması, üçüncü

kişilerin hak ve özgürlüklerinin olumsuz etkilenmesi, ticari sırlar ve fikri mülkiyet haklarının korunmasını gerektiren hallerin bulunması durumunda hakkın uygulanabilirliği sınırlanmaktadır.

GDPR'ın veri taşınabilirliği hakkını, bireylerin kişisel verileri üzerinde daha fazla söz sahibi olmaları için getirmiş olması amacı yanında hakkın rekabeti desteklemesi de Avrupa Birliği'nin amaçları arasındadır. Nitekim kişisel verilerin dijital pazarların en önemli girdisi haline gelmesi kişisel verilerin korunması ile rekabet hukuku arasındaki ayrımı belirsiz kılmaktadır. Bu doğrultuda Avrupa Birliği'nde veri taşınabilirliği ve birlikte çalışabilirlik meseleleri kimi rekabet incelemelerine konu olmuşsa da her iki alanın birbirini etkileyici önemli güçleri olduğu nispeten yeni anlaşılmıştır. Bugün veri taşınabilirliği rekabet hukuku ve politikaları ile kişisel verilerin korunması alanındaki en önemli kesişim noktalarından biri haline gelmiştir. Bu sebepledir ki hakkın uygulanmasından beklenen faydanın sağlanması için GDPR m. 20 ile öngörülen hakkın uygulanması çeşitli rekabet düzenlemeleri ile desteklenmiş, kişisel veri olmayan verilerin taşınabilirliği anlamında da önemli adımlar atılmıştır.

Rekabet hukuku ve politikalarının pazardaki rekabeti bozucu, kısıtlayıcı veya engelleyici olan hakim durumun kötüye kullanılması, anlaşma, uyumlu eylem, teşebbüs birliği karar ve eylemleri ile kontrolsüz birleşme devralmaları yasaklamış olmasının veri taşınabilirliği hakkı ile birlikte incelenmesi gerekmektedir. Veri taşınabilirliği hakkının kullanılmasını engellemek, bilinçli olarak teknik açıdan elverişli ve birlikte çalışabilir sistemleri kurmamak gibi eylemler somut olayın şartları içinde birer rekabet hukuku ihlali niteliği taşıyabilecektir. Tam da bu sebeple veri taşınabilirliği hakkının rekabeti destekleyecek bir mekanizma getirdiğine

inanılmaktadır. Zira hakkın geçiş maliyetlerini düşüreceği, ağ etkilerini, ölçek ve kapsam ekonomilerinin olumsuz etkilerini azaltacağı ve pazara giriş engellerini kaldıracağı düşünülmektedir. Buna karşılık veri taşınabilirliği hakkının rekabeti olumsuz etkileyeceği yönünde pek çok endişe bulunmaktadır. Genel olarak veri taşınabilirliği hakkının tüm veri sorumluları için öngörülmüş olması, gerekli sistemleri benimsemenin ek maliyetler anlamına gelmesi, ek maliyetlerin fiyatlara yansıması yoluyla tüketici refahının azalacağı ve aynı zamanda pazara giriş engelleri yaratacağı, küçük ölçekli teşebbüsler bakımından uygulamasının zorluğu ve inovasyonların gelişmesini engelleyeceği yönünde toplanan eleştirilerin haklılık payı bulunduğu açıktır. Hakkın rekabet hukukuna etkisinin görülmesi için zamana ihtiyaç olduğu açıktır. Bu bir anlamda kısa vadede karşılaşılacak sorunlar üzerine hakkın iyileştirilmesine de yardımcı olacaktır.

Türk hukukunda henüz düzenlenmemiş olsa dahi veri taşınabilirliği hakkının benimsenmesi dijital pazarlardaki rekabet koşulları göz önüne alındığında hukukumuzdaki kişisel veri koruma düzenlemeleri açısından da kaçınılmaz görünmektedir. Bu anlamda ciddi bir yasama çalışmasının yapılması sırasında Avrupa Birliği'nin deneyimlerinden faydalanmak ve rekabet otoritesi ile iş birliği içinde çalışmak, hakkı birtakım başka alanlarda yapılacak düzenlemeler ile desteklemek uygulama açısından en sağlıklı sonuçları verecektir.

BİBLİYOGRAFYA

I. KİTAP VE MAKALELER

Akıncı, A. N.: *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi,* Çalışma Raporu-6, 2017, s. 1-37.

Akıncı, A.: Mukayeseli Hukuk Açısından Amerikan ve Avrupa Topluluğu Hukukunda Rekabetin Yatay Kısıtlanması, Lisansüstü Tez Serisi No: 5, Ankara 2001.

Aksoy, **H. C.:** Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010.

Aslan, **İ. Y.:** Rekabet Hukuku Teori ve Uygulama, Güncellenmiş ve Genişletilmiş 6.Baskı, Bursa 2021.

Aşıkoğlu, **Ş. İ.:** Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul 2018.

Barth, **M.:** *A Case Study on Data Portability Measuring the Maturity of Data Portability Exports in IoT Platforms*, Datenschutz und Datensicherheit 2021, Vol. 3, s. 190-197.

Başalp, N.: Kişisel Verilerin Korunması ve Saklanması, Ankara 2004.

Belo, J./Macedo Alves, P.: *The Right to Data Portability: An In-Depth Look,* Journal of Data Protection and Privacy 2018, Vol. 2, No. 1, s. 53-61.

Borgogno, O./Colangelo, G.: *Open Banking and the Ambiguous Competitive Effects of Data Portability*, Competition Policy International Antitrust Chronicle April 2021, (https://www.competitionpolicyinternational.com/open-banking-and-the-

ambiguous-competitive-effects-of-data-portability/, E. T.: 06.05.2022), s. 1-6.

Bosher, H./Yeşiloğlu, S.: *An analysis of the fundamental tensions between copyright and social media: the legal implications of sharing images on Instagram*, International Review of Law, Computers & Technology 2019, Vol. 33, No.2, s. 164-186.

Bozdag, E.: *Data Portability Under GDPR: Technical Challenges*, 2018, (http://dx.doi.org/10.2139/ssrn.3111866, E. T.: 25.12.2021), s. 1-7.

Bozkurt Yüksel, A. E.: *Ticari Sırların Dijital Ortamda Korunması*, TAAD 2018, Y. 9, S. 33, s. 143-192.

Buneman, P.: *Semistructured Data*, ODS '97 Proceedings of the sixteenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems. ACM 1997, s. 117-121.

Colangelo, G./Maggiolino, M.: *Data Protection in Attention Markets: Protecting Privacy through Competition?*, Journal of European Competition Law & Practice 2017, Vol 8, No.6, s. 363-369.

Colangelo, G./Maggiolino, M.: *From fragile to smart consumers: Shifting paradigm for the digital era*, Computer Law & Security Review 2019, Vol. 35, s. 173-181 (Digital Era).

Cormack, A.: *Is the Subject Access Right Now Too Great a Threat to Privacy*, European Data Protection Law Review 2 2016, s. 15-27.

Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental

Rights: *Handbook on European data protection law: 2018 edition,* Publications Office 2018.

Custers, B./Ursic, H.: *Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection,* International Data Privacy Law 2016, Vol. 6, No:1, s. 4-15.

Çekin, M. S.: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, İstanbul 2020.

De Hert, P./Papakonstantinou, V./Malgieri, G./Beslay, L./Sanchez, I.: *The right to data portability in the GDPR: Towards user-centric interoperability of digital services,* Computer Law & Security Review 2018, s. 193-203.

Develioğlu, H. M.: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017.

Drexl, J.: *Designing Competitive Markets for Industrial Data – Between Propertisation and Access,* Max Planck Institute for Innovation and Competition Research Paper No. 16-13 2016, s. 1-69.

Durner, D./Leis, V./Neumann, T.: *JSON Tiles: Fast Analytics on Semi-Structured Data,* International Conference on Management of Data (SIGMOD'21), s. 445-458.

Dülger, M. V.: Kişisel Verilerin Korunması Hukuku, 1. Baskı, İstanbul 2019.

Edwards, L.: *Data Protection: Enter the General Data Protection Regulation* (May 21, 2018). Forthcoming in L Edwards ed Law, Policy and the Internet (Hart Publishing, 2018), s. 1-55.

Elfering, S.: Unlocking the Right to Data Portability An Analysis of the Interface with the Sui Generis Database Right, Baden-Baden 2019.

Engels, B.: *Data portability among online platforms*, Internet Policy Review 2016, Vol. 5(2), s. 1-17.

Eren, **F.:** Borçlar Hukuku Genel Hükümler, 22. Baskı, Ankara 2017.

Eskens, S.: *A Right to reset your user profile and more: GDPR-rights for personalized news consumers*, International Data Privacy Law 2019, Vol. 9, No. 3, s. 153-172.

European Commission, Directorate-General for Competition, Montjoye, Y./Schweitzer, H./Crémer, J., Competition policy for the digital era, Publications Office, 2019, (https://data.europa.eu/doi/10.2763/407537, E. T.: 06.05.2022).

Fialova, E.: *Data Portability and Informational Self-Determination*, Masaryk University Journal of Law and Technology 2014, Vol. 8, No. 1, s. 45-56.

Gal, M. S./Aviv, O.: *The Competitive Effects of the GDPR*, Journal of Competition Law & Economics 2020, Vol. 16(3), s. 349-391.

Gans, J.: *Enhancing Competition with Data and Identity Portability*, Hamilton Project Policy Brief 2018-10, (https://www.hamiltonproject.org/assets/files/Gans_20180611.pdf, E. T.: 06.05.2022).

Geradin, D./Kuschewsky, M.: *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue*, 2013, s. 1-16.

Giovannetti, E./**Siciliani**, P.: *The Impact of Data Portability on Platform Competition*, CPI Antitrust Chronicle November 2020, (https://www.competitionpolicyinternational.com/the-impact-of-data-portability-on-platform-competition/, E. T.: 06.05.2022).

González Fuster, G.: The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing, Law, Governance and Technology Series, Volume 16, Heidelberg 2014.

Graef, I.: *Blurring boundaries of consumer welfare, How to create synergies between competition, consumer and data protection law in digital markets*, Personal data in competition, consumer protection and intellectual property law: Towards a holistic approach. editor / Bakhoum, M./Conde Gallego, B./Mackenrodt, M-O&Surblytė-Namavičienė, G. Springer Verlag 2018 (MPI Studies on Intellectual Property and Competition Law), s. 121-151.

Graef, I.: *Data Portability at the Crossroads of Data Protection and Competition Policy*, Big Data e Concorrenza, 9 novembre 2016, LUISS Guido Carli, (https://www.agcm.it/dotcmsDOC/eventi/convegni/20161109_07.pdf, E. T.: 09.03.2022), s. 1-4 (Crossroads).

Graef, I.: *Mandating portability and interoperability in online social networks: regulatory and competition law issues in the European Union*, Telecommunications Policy 2015, Vol. 39(6), s. 502-514 (Mandating portability).

Graef, I.: *The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation*, CPI Antitrust Chronicle November 2020, https://www.competitionpolicyinternational.com/the-opportunities-and-limits-of-data-portability-for-stimulating-competition-and-innovation/, E. T.: 06.05.2022) (Stimulating Competition).

Graef, I./Husovec, M./Putova, N.: *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, German Law Journal 2018, Vol. 19, No. 6, s. 1359-1398.

Graef, I./Husovec, M./van den Boom, J.: *Spill-overs in data governance: the relationship between the GDPR's right to data portability and EU sector-specific data access regimes*, 2019, TILEC Discussion Paper No. DP 2019-005, s. 1-24.

Graef, I./Verschaleken, J./Valcke, P.: *Putting the right to data portability into a competition law perspective*, Law: The Journal of the Higher School of Economics Annual Review 2013, s. 53-63.

Guggenberger, N.: *The Essential Facilities Doctrine in the Digital Economy: Dispelling Persistent Myths*, Yale Journal of Law&Technology 2021, Vol. 23, s. 301-359.

Güven, P.: Türk Rekabet Hukuku ve Avrupa Birliği Rekabet Hukukunda Birleşme ve Devralmaların Denetlenmesi, Genişletilmiş 2. Baskı, Ankara 2003.

Hesse, M./Teubner, T.: *Reputation portability – quo vadis?*, 2019, Electronic Markets, Springer;IIM University of St. Gallen, Vol. 30(2), s. 331-349.

Hondagneu-Messner, S.: *Data Portability: A Guide and a Roadmap*, Rutgers Computer and Technology Law Journal 2021, Vol. 47, No. 2, s. 240-273.

Ishii, K.: *Discussions on the Right to Data Portability from Legal Perspectives,* Kreps, D./Ess, C./Leenen, L./Kimppa, K. (eds) This Changes Everything – ICT and Climate Change: What Can We Do?. HCC13 2018. IFIP Advances in Information and Communication Technology, vol 537. Springer, Cham., s. 338-355.

Javeed, U.: *Data and Competition Law: Introducing Data As Non-Monetary Consideration and Competition Concerns in Data-Driven Online Platforms*, 2021, s. 1-15.

Jenny, F.: *Competition law and digital ecosystems: Learning to walk before we run*, Industrial and Corporate Change 2021, Vol. 30(5), s. 1143-1167.

Jones, A./Brenda, S.: EU Competition Law: Text, Cases, and Materials. 4th ed. 2011.

Karegar, F./Pulls, T./Fischer-Hübner, S.: *Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This?*, Lehmann, A., Whitehouse, D., Fischer-Hübner, S., Fritsch, L., Raab, C. (eds) Privacy and Identity Management Facing up to Next Steps. Privacy and Identity 2016. IFIP Advances in Information and Communication Technology(), Vol 498, Springer, Cham., s. 164-181.

Kathuria, V./Lai, J. C.: *User Review Portability: Why and How?*, Computer Law & Security Review 2018, Vol. 34, s. 1291-1299.

Kerber, W./Schweitzer, H.: *Interoperability in the digital economy*, Journal of Intellectual Property, Information Technology and E-Commerce Law 2017, Vol.8, s. 164-181.

Körber, T.: *Is Knowledge (Market) Power? - On the Relationship Between Data Protection, 'Data Power' and Competition Law*, 2018, s. 1-31.

Krämer, J.: *Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations*, Journal of Competition Law & Economics 2020, Vol. 17(2), s. 263-308.

Krämer, J./Stüdlein, N.: *Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the General Data Protection Regulation*, Economics Letters 2019, Vol. 181, s. 99-103.

Küzeci, E.: Kişisel Verilerin Korunması, 4. Baskı, Ankara 2020.

Lam, W. M. W./Liu, X.: *Does data portability facilitate entry?*, International Journal of Industrial Organization 2020, Vol. 69, 102564, s. 1-49.

Lenarts, A.: *The General Principle of the Prohibition of Abuse of Rights: A Critical Position on Its Role in a Codified European Contract Law*, European Review of Private Law 2010, Vol. 18(6), s. 1121-1154.

Li, W.: *A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation*, International Data Privacy Law 2018, Vol. 8, No. 4, s. 309-317.

Lucchini, S./Moscianese, J./de Angelis, I./Di Benedetto, F.: *Online Digital Services And Competition Law: Why Competition Authorities Should be More Concerned About Portability Rather than About Privacy*, Journal of European Competition Law & Practice 2018, Vol. 9, No.9, s. 563-568.

Lynskey, O.: *Aligning data protection rights with competition law remedies? The GDPR Right to data portability*, European Law Review 2017, s. 793-814.

Lynskey, O.: *Article 20. Right to data portability*, The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020. Oxford Scholarship Online, 2021, s. 497-507 (Data Portability).

Malgieri, G.: *Trade Secrets v Personal Data: a possible solution for balancing rights*, International Data Privacy Law 2016, C. 6, S. 2, s. 102-116.

Martinelli, S.: *Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights"*, Reins, L. (eds) Regulating New Technologies in Uncertain Times. Information Technology and Law Series 2019, Vol. 32, T.M.C. Asser Press, The Hague, s. 133-152.

Nicholas, G.: *Taking It With You: Platform Barriers to Entry and the Limits of Data Portability*, Michigan Technology Law Review 2021, Vol. 27, s. 263-298.

Nixdorf, W.: *Planting in a Walled Garden: Data Portability Policies to Inform Consumers How Much (If Any) of the Harvest Is Their Share*, Transnational Law and Contemporary Problems 2019, Vol. 29, No. 1, s. 135-165.

Nolin, J. M.: *Data as oil, infrastructure or asset? Three metaphors of data as economic value*, JICES 2019, Vol. 18(1), s. 28-43.

Oğuzman, M. K./Öz, M. T.: Borçlar Hukuku, Genel Hükümler, Cilt 1, Gözden Geçirilmiş 14. Bası, İstanbul 2016.

Picht, P. G.: *Towards an Access Regime for Mobility Data*, IIC: International Review of Intellectual Property and Competition Law 2020, s. 940-976.

Posner, R.: *Antitrust in the New Economy*, Antitrust Law Journal 2001, Vol. 68, No. 3, s. 925-943.

Quinn, P.: *Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?,* Global Jurist 2018, Vol. 18, No. 2, 18, 20180021, s. 1-11.

Ramos, E. F./Blind, K.: *Data portability effects on data-driven innovation of online platforms: Analyzing Spotify*, Telecommunications Policy 2020, Vol. 44(9), 102026, s. 1-16.

Stites, T.: *Data Protection on the Doorstep: How the GDPR Impacts American Financial Institutions*, Review Of Banking & Financial Law 2018, Vol. 38, s. 132-146.

Swire, P./Lagos, Y.: *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, Maryland Law Review 2013, Vol. 72, No. 2, s. 335-380.

Syrmoudis, E./Mager, S./Kuebler-Wachendorff, S./Pizzinini, P./Grossklags, J./Kranz, J.: *Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20*, Proceedings on Privacy Enhancing Technologies 2021, Vol.2021(3), s. 351-372.

Tekinalp, Ü.: Fikrî Mülkiyet Hukuku, Güncelleştirilmiş ve Genişletilmiş Beşinci Bası, İstanbul 2012.

Topçuoğlu, M.: Rekabeti Kısıtlayan Teşebbüsler Arası İşbirliği Davranışları ve Hukuki Sonuçları, Rekabet Kurumu Lisansüstü Tez Serisi, Ankara, 2001.

Turner, S./Quintero, J. G./Turner, S./Lis, J./Tanczer, L. M.: *The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment*, New Media & Society 2021, Vol. 23(10), s. 2861-2881.

Unver, M.: *Turning the crossroad for a connected world: Reshaping the European prospect for the Internet of Things*, International Journal of Law and Information Technology 2018, Vol. 26(2), s. 93-118.

Ursic, H.: *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, SCRIPTed: Journal of Law, Technology and Society 2018, Vol. 15, No. 1, s. 42-69.

Van der Auwermeulen, B.*: How to attribute the right to data portability in Europe: A comparative analysis of legislations*, Computer Law § Security Review 2017, Vol. 33, s. 57-72.

Vanberg, A. D.: *The Right to Data Portability in the GDPR: What Lessons Can Be Learned From the EU Experience?*, Journal of Internet Law 2018, Vol. 21, No.7, s. 10-19.

Vanberg, A. D./Unver, M. B.: *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple and Dynamic Duo?*, European Journal of Law and Technology 2017, Vol. 8, No.1, s. 1-22.

Vezzoso, S.: *Competition Policy in Transition: Exploring Data Portability's Roles*, Journal of European Competition Law & Practice 2021, Vol. 12, No.5, s. 357-369.

Whish, R./Bailey, D.: Competition Law, Seventh Edition, New York 2012.

Wohlfarth, M.: *Data Portability on the Internet an Economic Analysis*, Bus Inf Syst Eng 2019, Vol. 61(5), s. 551-574.

Wong, J./Henderson, T.: *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, International Data Privacy Law 2019, Vol. 9, No. 3, s. 173-191.

Zanfir-Fortuna, G./Ianc, S.: *Data Protection and Competition Law: The Dawn of 'Uberprotection'*, Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds.), Edward Elgar Publ'g 2019, s. 249-272.

Zanfir, G.: *The right to Data portability in the context of the EU data protection reform*, International Data Privacy Law 2012, Vol. 2, No. 3, s. 149-162.

Zwiebelmann, Z./Henderson, T.: *Data Portability as a Tool for Audit*, Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers 2021, s. 276-280.

II. REHBERLER VE RAPORLAR

ACCC, *Digital Platform Services Inquiry*, 2022, (https://www.accc.gov.au/system/files/DPB%20-%20DPSI%20-%20March%202022%20-%20Full%20interim%20report%20-%2031%20March%202022.pdf, E. T.: 06.05.2022).

ACCC, *Digital Platforms Inquiry*, 2019, (https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, E. T.: 06.05.2022).

Article 29 Data Protection Working Party, *Guidelines on Right to Data Portability*, (https://ec.europa.eu/newsroom/article29/items/611233, E. T.: 03.05.2022).

Article 29 Data Protection Working Party, *Opinion 4/2007 on the Consept of Personal Data*, (https://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, E. T.: 03.05.2022).

Autorité de la Concurrence and Bundeskartellamt, *Competition Law and Data Report*, 10.05.2016, (https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2, E. T.: 06.05.2022).

Personal Data Protection Commission In collaboration with Competition and Consumer Commission of Singapore, *Discussion Paper on Data Portability*, 2019, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf, E. T.: 06.05.2022).

European Commission, Commission Staff Working Paper, *Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Impact Assessment report),* SEC(2012) 72 final, (https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf, E. T.: 06.05.2022).

European Commission, *Glossary of Terms Used in EU Competition Policy, Antitrust and Control of Concentrations*, 2002, (https://www.concurrences.com/IMG/pdf/european_commission_glossary

_of_terms_used_in_eu_competition_policy_-_antitrust_and_control_of_concentrations.pdf?40143/2eeffac1aa42eaa000f06738fda10e48e160afe2, E. T.: 06.05.2022).

Fletcher, A.: *Digital competition policy: Are ecosystems different?*, 2020, (https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf, E. T.: 06.05.2022).

Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, 2009/C 45/02, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN, E. T.: 06.05.2022).

HM Treasury, *Unlocking Digital Competition, Report of the Digital Competition Expert Panel*, 2019, (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf, E. T.: 06.05.2022).

OECD, *Algorithms and Collusion: Competition Policy in the Digital Age*, 2017, (https://www.oecd.org/daf/competition/Algorithms-and-collusion-competition-policy-in-the-digital-age.pdf, E. T.: 06.05.2022).

OECD, *Competition Committee Discussion Paper*, 09.06.2021, (http://oe.cd/dpic, E. T.: 06.05.2022).

OECD, *Data portability, interoperability and digital platform competition, OECD Competition Committee Discussion Paper*, 09.06.2021, (http://oe.cd/dpic, E. T.: 06.05.2022).

OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, (https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en#page1, E. T.: 07.01.2022).

OECD, *Summary of the Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21.03.2014, (https://one.oecd.org/document/DSTI/ICCP/REG(2014)3/en/pdf, E. T.: 06.05.2022).

Office of Science and Technology Policy, *Çağrı Metni*, (https://www.govinfo.gov/content/pkg/FR-2016-10-07/pdf/FR-2016-10-07.pdf 69873-69874, E.T.: 05.05.2022).

Rekabet Kurumu, Hâkim Durumdaki Teşebbüslerin Dışlayıcı Davranışlarına İlişkin Kılavuz, 2014, (https://www.rekabet.gov.tr/Dosya/kilavuzlar/hakim-durumdaki-tesebbuslerin-dislayici-davranislarina-iliskin-kilavuz1.pdf, E.T.: 06.05.2022).

Stigler Center for the Study of the Economy and the State, *Stigler Committee on Digital Platforms Final Report*, 2019, (https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf, E. T.: 06.05.2022).

United Kingdom, Competition and Markets Authority, *Online Platforms and Digital Advertising Market Study Final Report*, 2020, (https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, E. T.:06.05.2022).

United States Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations*, 2020, (https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519, E. T.: 06.05.2022).

World Intellectual Property Organization, *What is Intellectual Property?*, 2020, (https://www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf, E.T.: 06.05.2022).

III. İNTERNET KAYNAKLARI

Baroness Neville Rolfe'nin 14 Aralık 2015 tarihli konuşması: (https://www.parliamentlive.tv/Event/Index/03e4655b-f6e9-44e6-b797-a6139c4b9156, E. T.: 10.05.2022).

Data Transfer Project: (https://datatransferproject.dev/, E. T.: 06.05.2022).

FTC: Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No: 071-0170, (https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf, E. T.: 06.05.2022).

Google, Data Transfer Project Duyurusu: (https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html, E. T.: 06.05.2022).

Information Commissioners' Office, Manifestly unfounded and excessive requests: (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-

requests/#:~:text=A%20request%20may%20be%20excessive,overlaps%20with%20other%20requests. E. T.: 07.06.2022).

Instagram, Güncellenmiş Kullanım Hükümleri, (https://help.instagram.com/581066165581870/?helpref=uf_share, E. T.: 06.05.2022).

OECD, Glossary: (https://stats.oecd.org/glossary/detail.asp?ID=4370, E. T.: 05.05.2022).

Open Data Handbook Glossary, (https://opendatahandbook.org/glossary/en/terms/structured-data/, E. T.: 20.12.2021); (https://opendatahandbook.org/glossary/en/terms/metadata/, E. T.: 20.12.2021).

Speech former Competition Commissioner Almunia, *Competition and personal data protection*, Privacy Platform event: Competition and Privacy in Markets of Data Brussels, 26.11.2012, (http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm, E. T.: 06.05.2022).

The Economist (2017), *Regulating the internet giants: The world's most valuable resource is no longer oil, but data,* (https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, E. T.: 16.12.2021).

https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_2042

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_en

https://joinup.ec.europa.eu/collection/interoperable-europe/initiatives

https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/9-september-2014-gas-market

https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_EN.html

IV. MEVZUAT

2010 Dodd-Frank Wall Street Reform and Consumer Protection Act: https://www.govinfo.gov/content/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf, E. T.: 05.05.2022.

95/46/AT sayılı Direktif: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML, E. T.: 05.05.2022.

California Consumer Privacy Act: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121, E. T.: 05.05.2022.

Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A205%3AFIN, E. T.: 05.05.2022.

Consolidated version of the Treaty on the Functioning of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT, E. T.: 05.05.2022.

Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public

administrations (ISA): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009D0922, E. T.: 05.05.2022.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366, E. T.: 05.05.2022.

Directive (EU) 2016/943 of The European Parliament and of The Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN, E. T.: 05.05.2022.

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770, E. T.: 06.05.2022.

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32002L0022, E. T.: 05.05.2022.

Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector

information: https://eur-lex.europa.eu/eli/dir/2013/37/oj, E. T.: 05.05.2022.

Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0037&from=FR, E. T.: 05.05.2022.

Numara Taşınabilirliği Yönetmeliği: (https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=13180&MevzuatTur=7&MevzuatTertip=5, E. T.: 05.05.2022.

Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) ("Dijital Pazarlar Yasası Taslağı"), COM (2020) 842 final, 15.12.2020: https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf, E. T.: 06.05.2022.

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: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807, E. T.: 05.05.2022.

The 1996 Health Insurance Portability and Accountability Act: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf, E. T.: 05.05.2022.