

T.C.

İstanbul Üniversitesi

Sosyal Bilimler Enstitüsü

Özel Hukuk Anabilim Dalı

Yüksek Lisans Tezi

**AVRUPA BİRLİĞİ GENEL VERİ KORUMA
TÜZÜĞÜNÜN KİŞİLERİN GİZLİLİĞİNİN
KORUNMASI KONUSUNDA TİCARİ
İŞLETMELER ÜZERİNDEKİ ETKİSİ**

Firuz RAJABOVA

2501191633

Dr.Öğr.Üyesi Mine Tan DEHMEN

İstanbul-2022

ÖZ

**AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜNÜN KİŞİLERİN
GİZLİLİĞİNİN KORUNMASI KONUSUNDA TİCARİ İŞLETMELER
ÜZERİNDEKİ ETKİSİ**

FİRUZA RAJABOVA

Çoğu işletme büyük miktarlarda tüketici verisi toplar. Dünyadaki neredeyse her internet kullanıcıını kapsayan çok büyük miktarlarda veri noktası vardır. İşletmeler, veri sahiplerinin kişisel verilerini toplayarak ve işleyerek bundan ciddi kazançlar elde etmektedir. Veriler toplandığında, bir kullanıcının sanal kimliği oluşturulur ve kaydedilir. Veri toplama ve sanal kimliklerle ilgili sorunlar, bunların isabetsiz olmasıdır. Kullanıcı verilerinin toplanması, güvenlik sorunları, ayrımcılığı teşvik edebilecek veri segmentlerinin oluşturulması, hedefli reklamlar gibi bir dizi soruna yol açabilir. Verilerin ekonomik faaliyetlerde kullanımı ve rolündeki hızlı değişimin yanı sıra verilerin kötüye kullanımı, düzenleyici çerçevede bir değişimi gerektirmiştir. Avrupa Birliği'nin 95/46 sayılı önceki Veri Koruma Direktifi'nin teknoloji sektöründeki yeni gelişmelere ayak uyduramaması nedeniyle, AB düzeyinde veri koruma ve gizliliğe ilişkin kapsamlı bir mevzuatın kabul edilmesine ihtiyaç duyulmuştur. Direktif ayrıca, Avrupa Birliği üye ülkelerinin veri koruma yasaları arasında yeknesaklık ve tutarlılık sağlama yönündeki temel hedeflerini de gerçekleştirilemiyordu. 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR), AB sınırlarını aşan önemli bir etkiye sahip olan en kapsamlı mevzuattır. Tüzük teorik olarak veri sahiplerinin temel haklarını korumanın yanı sıra her iki tarafın hakları arasında denge oluşturmak amacıyla işletmeleri de desteklemektedir.

Bu yüksek lisans tezi dört ana bölümden oluşmaktadır. İlk bölümde, veri toplamanın neden önemli olduğu analiz edilmeye çalışılmıştır. İkinci bölümde Avrupa'da veri korumanın yasal arka planı incelenmiştir. Sonraki bölümde Tüzüğün kapsamı, veri sahiplerine sağladığı haklar, veri işleyen şirketlere getirdiği yükümlülükler ve getirdiği yenilikler incelenmiştir. Bu yüksek lisans tezinin son

bölümünde ise Tüzüğün veri sahipleri ile işletmeler arasındaki dengeyi sağlamada başarılı olup olmadığı araştırılmaktadır. Buna ek olarak, belirli işletme yapılarının bu Tüzüğe uyum sağlamada karşılaştıkları mevcut zorluklar ele alınmaktadır. İlâveten, bu tez, konunun kapsamlı bir analizini hazırlamak için akademisyen ve profesyonellere ait farklı görüşler sunmaktadır.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin Korunması, Gizlilik, Genel Veri Koruma Tüzüğü, İşletme Özgürlüğü

ABSTRACT
THE IMPACT OF GDPR ON COMMERCIAL ENTERPRISES REGARDING
THE PROTECTION OF PERSONAL PRIVACY

FIRUZA RAJABOVA

Most businesses collect large amounts of consumer data. There are huge amounts of data points that cover nearly every internet user in the world. By collecting and processing personal data of data subjects, businesses are making serious profit from it. When data is collected, a virtual identity of a user is created and saved. The problems with data collection and virtual identities are their inaccuracy. Collection of user data can lead to a series of problems, such as security issues, creation of data segments which can encourage discrimination, targeted ads. The rapid change in the use and role of data in economic activity, as well as misuse of data require a shift in the regulatory framework. Since 95/46 numbered previous Data Protection Directive was not up to date with new developments in the technology sector, there was a need to adopt a comprehensive legislation about data protection and privacy at the EU level. The Directive was also unable to accomplish its primary objectives of ensuring uniformity and consistency among European Union member states' data protection laws. European

Union General Data Protection Regulation numbered 2016/679 is the most comprehensive piece of legislation that has a significant impact that goes beyond the boundaries of the EU. GDPR theoretically protects the fundamental rights of data subjects as well as supports businesses to create a balance between the rights of both sides. This master's thesis concludes four main parts. In the first part, the reason why data collection is important is tried to be analysed. The second part looks at the legislative background of data protection in Europe. The next part examines the scope of GDPR, rights that are given to data subjects, obligations that are put on to data processing companies and novelties that have been brought by it. The last part of this master's thesis explores whether the GDPR is successful in maintaining the harmony between data subjects and businesses. Additionally, it addresses the existing difficulties that particular business structures face in complying with this Regulation.

In addition, this thesis presents diverse viewpoints from academics and professionals in order to prepare a thorough analysis of the topic.

Keywords: Personal Data, Data Protection, Privacy, General Data Protection Regulation, Freedom to Conduct a Business



ÖNSÖZ

Sıkı bir internet kullanıcısı olarak bu tezi yazmaya kafamda iki ana soruyla başladım. İlk soru, şirketlerin çevrimiçi olarak bilgilerimizi nasıl topladığını ve işlediğini bulmaktı. Neredeyse her gün farklı web sitelerinin farklı çerez ve gizlilik politikalarını, sitenin bu veri toplama uygulamalarının ne kadar ötesine geçtiğini fark etmeden kabul ediyorum. Bu nedenle, şirketlerin veri koruma uygulamaları hakkında bilgi edinmek için bu tezi büyük bir hevesle yazmaya başladım. Bu konuyu araştırdıkça, en kapsamlı mevzuat parçalarından biri olan Avrupa Veri Koruma Tüzüğüne göz atmaya daha fazla ilgi duydum. Avrupa Veri Koruma Tüzüğünü inceleyerek, teorik olarak veri sahiplerine gelişmiş haklar sağlamaya çalışan en iyi düzenlemelerden biri olduğunu görebildim. Aklımdaki ikinci soru ise bu düzenlemenin işletmeleri gerçekten nasıl etkilediğini bulmaktı. Avrupa Veri Koruma Tüzüğü'nün yürürlüğe girmesinin üzerinden artık dört sene geçiyor. Tez konusunun seçilmiş olmasının nedeni, bu dört senede Tüzüğün pratikte nasıl uygulandığını incelemek ve onun kabul olunduğu zaman hedeflenen amaçlarına ulaşip ulaşılmadığının değerlendirilmesidir. Tüzük veri koruma alanında ilk kapsamlı mevzuat olduğu için ve sınırları aşan etkiye sahip olduğu için, ondan hangi dersler alınabileceği de ilgi çekmektedir. Tüzük yeni bir düzenleme olduğu için uygulamada işletmeler üzerindeki etkisi ve kullanıcılar üzerindeki etkisinin derinlemesine araştırılması gerekmektedir.

Bu vesileyle, yazma süreci boyunca değerli yorum ve yönlendirmeleriyle bana katkıda bulunan değerli hocam ve tez danışmanım Dr.Öğr.Üyesi Mine Tan Dehmen'e teşekkür etmek isterim.

FİRUZA RAJABOVA

İSTANBUL, 2022

İÇİNDEKİLER

ÖZ	ii
ABSTRACT	iv
ÖNSÖZ	vi
KISALTMALAR.....	x
GİRİŞ	1

BİRİNCİ BÖLÜM

ÇEVİRİMİÇİ VERİ GİZLİLİĞİ

1. Veri Toplamanın Önemi	3
2. Veri Toplamaya İlişkin Temel Sorunlar	5

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİ'NDE VERİ KORUMANIN YASAL GEÇMİŞİ

1. Veri Korumanın Yasal Arka Planı	8
2. 95/45/EC Sayılı Direktif ve Eksiklikleri.....	11
3. Tüzüğün Hazırlık Süreci	12

ÜÇÜNCÜ BÖLÜM

GENEL VERİ KORUMA TÜZÜĞÜ

1. Tüzüğe Genel Bakış	14
1.1. Kişisel Veriler	14
1.2. Veri Sahibi.....	16

1.3. Takma Ad Verme ve Anonimleştirilmiş Veriler	16
1.4. İşleme	17
1.4.1. Kontrolör	17
1.4.2. İşleyiciler	18
1.4.3. Ortak Kontrolörler.....	20
1.5. Konu itibariyle Uygulama Alanı	20
1.6. Yer İtibariyle Uygulama Alanı.....	22
1.7. Veri İşleme İlkeleri.....	24
1.7.1. Yasaya Uygunluk, Adalet, Şeffaflık	24
1.7.2. Amaç Sınırlaması.....	26
1.7.3. Veri Minimizasyonu.....	27
1.7.4. Doğruluk.....	29
1.7.5. Depolama Sınırlaması	30
1.7.6. Bütünlük ve Gizlilik.....	30
1.7.7. Sorumluluk	31
2. Tüzükle Gelen Önemli Değişiklikler.....	32
2.1. Veri Sahiplerinin Yeni Hakları	32
2.1.1. Avrupa Adalet Divanının 101/01 ve 131/12 Sayılı Kararlarının Mukayesesi.....	39
2.2. Onay.....	42
2.3. Veri Güvenliği.....	48
2.5. Tasarlanan ve Varsayılan olarak Gizlilik.....	51
2.6. Veri İhlalleri.....	53
3. Genel Veri Koruma Tüzüğü'ne Uygunluğun Sağlanması	55
3.1. Etki Değerlendirmeleri	55
3.2. Veri Koruma Görevlisi	58

3.3. Davranış Kuralları	61
3.4. Sertifikasyon	63

DÖRDÜNCÜ BÖLÜM

GENEL VERİ KORUMA TÜZÜĞÜ'NÜN İŞLETMELER ve VERİ SAHİPLERİNİN HAK ve MENFAATLERİ BAKIMINDAN DEĞERLENDİRİLMESİ

1. İşletme Özgürlüğü	64
2. İşletmeler İçin Zorluklar	67
2.1. Uygulama Maliyetleri	67
2.2. Tüzüğün Rekabet Üzerindeki Etkileri.....	69
2.3. Tek Elden Denetim Mekanizması.....	70
2.4. Dahili Veri Aktarımı Sorunu	73
3. Veri Sahiplerinin Zayıf Konumu.....	74
SONUÇ	76
KAYNAKÇA	78
I. Basılı Kaynaklar	78
II. İnternet Kaynakları	82

KISALTMALAR

A.e.	: Aynı eser
AB	: Avrupa Birliği
AK	: Avrupa Birliği Komisyonu
a.g.e.	: Adı geçen eser
Ariz. Summit L. Rev.	: Arizona Summit Law Review
Bkz.	: Bakınız
BNB	:The Bureau of National Affairs
Bs.	: Bası
C.	:Cilt
Clev. St. L. Rev	: Cleveland State Law Review
CNIL	: Commission nationale de l'informatique et des libertés
DPA	: Data Protection Authority
DPO	: Data Protection Officer
EDPB	: European Data Protection Board
GDPR	: General Data Protection Regulation
GEO. L. TECH. REV	:Georgetown Law Tech Review
IAPP	: International Association of Privacy professionals
Iowa L. Rev.	: Iowa Law Review
ITGPI	: IT Governance Privacy Team
K.	: Karar
Minn. JL Sci. & Tech.	: Minnesota Journal of Law, Science & Technology
OECD	: Organisation for Economic Co-operation and Development
para	: Paragraf
Penn St. L. Rev	: Penn State Law Review
Rich. JL & Tech	: Richmond Journal of Law and Technology
S.	: Sayı
s.	: sayfa
T.	: Tarih
Seattle J Soc Just	:Seattle Journal for Social Justice
U. Pa. L. Rev	: University of Pennsylvania Law Review

WP 29

: Working Party 29



GİRİŞ

Avrupa Birlięi Genel Veri Koruma Tüzüğü, temel insan hakkı olarak verilerin korunmasını güçlendirmeyi amaçlamaktadır.

Avrupa Birlięi Genel Veri Koruma Tüzüğü (“Tüzük”)¹, Avrupa Birlięi gizlilik mevzuatının temel taşıdır. Dijital dünyamızda kişisel veriler, birçok ticari faaliyete katkı sağlayan kilit unsurlardan biridir. Bu nedenle, Tüzüğün şirketler üzerinde önemli etkileri olması kaçınılmazdır. Tüzük, Avrupa gizlilik mevzuatında halihazırda yerleşik olan birkaç görüşü detaylandırmaktadır ve veri sahiplerine ek haklar vermektedir. Bunun sonucunda, verileri kullanan şirketlerin de ek uyum sorumlulukları bulunmaktadır. Tüzük, Avrupa Birlięi’ndeki kişiler için geçerli olan veri gizlilięi standartlarını iyileştirme ve uyumlaştırmayı ve aynı zamanda AB dışındaki Avrupa Birlięi vatandaşlarının kişisel verilerinin aktarımını düzenleyerek veri korumaya ilişkin coęrafi alanı genişletmeyi amaçlamaktadır. Tüzüğün temel amacının bireylerin ve ticari işletmelerin yeni kanunlardan faydalanmalarını sağlamak olduęu bilinmektedir. Sonuç olarak, AB yasama organı her zaman ortak refaha büyük önem atfetmiştir.

Teorik olarak, tüzük mevzuat şartları ve uygulaması rekabet veya yatırım gibi ortak refahın dięer unsurlarına zarar vermeden bireysel gizlilięi güçlendirerek toplum yararını en yüksek seviyeye getirmektedir. Bu tezde tartışıldıęı üzere, tüzük dijital hizmet tüketicilerine faydalı olmuş ve veri sahiplerinin haklarını korumuş olmasına rağmen, dijital pazar yerlerindeki devasa çevrimiçi platformların gücünü artırarak rekabete zarar da vermiştir.

Bu çalışmanın konusu olarak “Kişisel gizlilięin korunması açısından Tüzüğün ticari işletmeler üzerinde etkisinin” seçilmesinin nedeni, Tüzüğün veri koruma açısından Avrupa Birlięi’ndeki en yeni mevzuat olmasıdır. Bu yüzden Tüzük

¹ European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)” (“2016/679 Avrupa Birlięi Genel Veri Koruma Tüzüğü”), (Çevrimiçi), <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679> , 2 Eylül 2021.

uygulandığında pratikte ortaya çıkabilecek olası zorlukların incelenmesi önem arz etmektedir.

Mevcut araştırma sırasında çeşitli yöntemler kullanılmıştır:

- Teorik yöntem: akademisyenlerin çalışmalarının, akademik makalelerin ve profesyonel görüşlerin incelenmesi.

- Betimsel analiz: belirli Tüzük maddelerinin değerlendirilmesi.

- Nicel teknik: bağlantılı çalışmalardan bulguların çıkarılması.

Tez altı bölümden oluşmaktadır: giriş, dört bölüm ve sonuç. Birinci bölümde çevrimiçi veri toplamaya genel bakış ve güvenlik sorunları ile verilerin kötüye kullanımı gibi veri işlemeye ilişkin yaygın gizlilik sorunları sunulmuştur. İkinci bölümde AB ve uluslararası düzeyde veri korumanın yasamaya ilişkin arka planının bir özeti sunulmuştur. İlaveten, Tüzüğün neden önceki Veri Koruma Direktifinin (“Direktif”)² yerini aldığı incelenmiştir. Üçüncü bölümde Tüzüğün Avrupa veri gizliliğine getirdiği yeni değişiklikler, temel hükümleri, kişisel veriler, yer itibarıyla uygulama alanı, konu itibarıyla uygulama alanı, işletmelere yönelik yeni yükümlülükler ve veri sahiplerine verilen yeni haklar gibi genişletilmiş konseptlere (kapsam genişletmesi) ilişkin genel bir bakış sunulmuştur. Dördüncü bölümde ise, işletme özgürlüğü ve bu hakkın veri koruma haklarıyla dengelenip dengelenmediği incelenmiştir. Ayrıca, Tüzüğün ticari işletmeler üzerindeki etkileri tartışılmaktadır. Bu bölümün sonunda, Tüzüğün veri sahipleri için faydaları incelenmiştir. Tezin sonuç kısmında ise bu çalışmanın başlıca bulguları ve değerlendirmeler özet olarak yer almıştır.

² “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, (‘95/46 Avrupa Birliği Veri Koruma Direktifi’), (Çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>, 2 Mart 2020.

BİRİNCİ BÖLÜM

ÇEVİRİMİÇİ VERİ GİZLİLİĞİ

1. Veri Toplamanın Önemi

Teknoloji geliştikçe ve dünyamız her gün daha dijital hale geldikçe, kişilerin çevrimiçi hizmetleri kullanmaları kaçınılmaz olmuştur³. İnsanlar internete göz attıklarında veya bir mobil uygulama kullandıklarında, kendi bilgilerini eş zamanlı olarak bazı şirketlerle paylaşırlar⁴. Çevrimiçi alanda mevcut olan şirketler, kullanıcıların kendi internet sitelerini kullanma davranışları hakkında bilgi edinmek üzere veri analiz araçlarını kullanırlar. Veri araçları gibi bazı şirketler, izleme araçları aracılığıyla kullanıcıların diğer internet sitelerinde neler yaptıkları hakkında bilgi toplama konusunda uzmanlaşmışlardır⁵.

Kullanıcı verileri birkaç şekilde toplanmaktadır: çerezler⁶, arama sorguları ve sosyal medyada yayınlanan bilgiler. Ayrıca veriler, müşterilerin fiziksel konumunu ve mobil cihaz kullanımını izleyerek dolaylı şekilde de elde edilir⁷. Veri araçları, genellikle bilgileri dışında olmak üzere inanılmaz sayıda kişinin devasa miktarda kişisel bilgilerini toplamıştır⁸. Örneğin, Acxiom isimli aracı şirket, “kendi veri tabanlarının dünya genelinde yaklaşık 700 milyon tüketici hakkında bilgi içermesiyle ve neredeyse her Amerikalı tüketici için 3000’den fazla veri bölümüne sahip

³ Neeka Hodaie, "Real You Meets Virtual You: It is Time for Consumers to Regain Power Online," **Seattle J Soc Just**, C. 18, S.2, 2020, s.647.

⁴ Rebecca Lipman, "Online Privacy and the Invisible Market for Our Data." **Penn St. L. Rev.** 120, 2015, s. 777.

⁵ Hodaie, **a.g.e.**, s.656.

⁶ İki farklı çerez türü vardır: flash çerezleri ve HTTP çerezleri. Flash çerezleri HTTP çerezlerine göre daha fazla veri depolar ve son kullanma tarihi yoktur. Öte yandan, HTTP çerezleri ise varsayılan olarak her bir göz atma oturumu bittiğinde sona ermek üzere ayarlanır, bkz. Omer Tene & Jules Polenetsky, "To Track Or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising." **Minn. JL Sci. & Tech.**, C.13, 2012, s.281.

⁷ Carolyn Gray, "Who Pays the Price: Regulation of Data Tracking and Online Behavioral Advertising," **Ariz. Summit L. Rev.**, C.8, 2014, s.385.

⁸ Brittany A. Martin, "The Unregulated Underground Market For Your Data: Providing Adequate Protections For Consumer Privacy in The Modern Era.", **Iowa L. Rev.**, C.105, 2019, s.871.

olmasıyla” övünmüştür⁹. Hedefe yönelik reklamlar veya toplanan verilerin satışı gibi bu verilerin paraya çevrilebileceği çeşitli olası yöntemler vardır ve tüm bu yöntemler, genellikle verileri sunmuş olan kullanıcılar tarafından bilinmemektedir¹⁰.

Modern teknolojiler o kadar ilerlemiştir ki, kullanıcıların gizliliği görünmez şekilde ihlal edilebilir hale gelmiştir. Tüketicilerin mobil uygulama kullanımı ve fiziksel konumu, çevrimiçi olmadıklarında bile mobil telefonları aracılığıyla takip edilebilir ki, bu da verilerin dolaylı olarak elde edilmesinin başka bir yoludur¹¹. Örneğin, Groupon, farklı seyahat, etkinlik ve ürün indirimleri sunarak tüketicilerin yerel işletmelerle bağlantı kurmasını sağlayan bir e-ticaret platformudur. Yerel işletmelerden indirim almak için, kullanıcıların kendi konumlarını Groupon’la paylaşması gerekmektedir. Ancak kullanıcılar Groupon tarafından konumlarının her 20 dakikada bir kontrol edilebildiğini ve reklamcılarla paylaşılabilirliğini bilselerdi, bunu kabul ederler miydi¹²?

Google, Instagram, Gmail ve Facebook gibi çevrimiçi platformlar, görünürde müşterilerine ücretsiz hizmet vermektedir. Ancak bu hizmetlerin ücretsiz olmasının tek nedeni, kişilerin kendi verileriyle bedel ödemeleridir. Yukarıda belirtilen hizmetler reklam satışı yaparak birçok gelir elde etmektedir. Eğer bu gibi platformlara verilerimizi toplamaları yasaklansa, bu zaman onlar hedefe yönelik reklam sunamazlar. Sonuç olarak, hizmetleri ücretsiz olarak vermeyi bırakırlar. Kullanıcılar, ücretsiz hizmet karşılığında nelerden vazgeçtiklerini çok anlamayarak bu pazarlığı kabul etmektedir¹³.

⁹ Edith Ramirez, “Data Brokers A Call for Transparency and Accountability”, Federal Trade Commission, 14 May 2014, s.8, (Çevrimiçi) <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>, 15 Aralık 2021.

¹⁰ Adam Schwartz et. al., “New Rules to Protect Data Privacy: Where to Focus, What to Avoid, Electronic Frontier Foundation”, 2 Temmuz 2018, (Çevrimiçi), <https://www.eff.org/deeplinks/2018/07/new-rules-protect-data-privacy-where-focus-what-avoid>, 15 Aralık 2021.

¹¹ Gray, a.g.e., s.388.

¹² Mary Beth Quirk“Study: Some Popular Android Apps Tracking User Location Once Every Three Minutes”, 24 March 2015, (Çevrimiçi), <https://consumerist.com/2015/03/24/study-some-popular-android-apps-tracking-user-location-once-every-three-minutes/index.html> , 15 Aralık 2021.

¹³ Lipman, a.g.e., s.784.

2. Veri Toplamaya İlişkin Temel Sorunlar

Veri aracıları tarafından toplanan veri türleri ad, soyad, ırk, etnik köken veya alışveriş etkinliği, sosyal medya hesapları, sağlık koşulları gibi geniş kapsamlı ve daha ziyade heterojen olabilir¹⁴. Veri toplamaya ilişkin olarak sahte bilgiler, kategorilere ayırma, kullanıcıların profilinin çıkarılması, güvenlik sorunları, bildirim eksikliği gibi bazı sorunlar mevcuttur. Veriler toplanırken, bir kullanıcının sanal kimliği oluşturulur ve saklanır. Genel olarak, veri koruma uygulamalarının bir ürünü olan sanal kimlikle ilişkilendirilmiş olan fiili kişi kendi sanal kimliğinden çoğunlukla habersizdir¹⁵. Veri toplama ve sanal kimliklerle ilgili sorunlardan biri, bunların doğruluğudur. Örneğin, Deloitte tarafından yapılan bir araştırma, araştırma katılımcılarının üçte ikisinden fazlasının kendileri hakkında elde edilen bilgilerin “*toplamda %0 ila %50 [doğru]*” olduğunu bildirdiklerini göstermiştir¹⁶.

Toplanan verilere göre, tüketiciler farklı “*veri segmentlerine*” yerleştiriliyorlar¹⁷. Bireylerin hizmetlere erişim türünü belirlerken veri segmentleri sıklıkla kullanılmaktadır¹⁸. Veri segmentleri hedefe yönelik reklamları ve ırk ya da sınıflara dayalı ayrımcılığı teşvik edebilir. Bu veri segmentlerine dayalı olarak, kişilerin iş veya banka kredileri de reddedilebilir¹⁹. Örneğin, bir kişi pişirme malzemeleri satın alırsa, “*Pişirmeyle İlgileniyor*” etiketli bir veri segmentine konulabilir. Bu tür bir kategori zararsız görünebilirken, “*Bankacılık Hizmetlerini Nadiren Kullanma Göstergesi*”, “*Kredibilite*” ve *diğerleri gibi*” tamamen

¹⁴ Ramirez, a.g.e., s.46.

¹⁵ Hodaie a.g.e., s.648.

¹⁶ Deloitte Insights, Predictably Inaccurate: The Prevalence and Perils of Bad Big Data, 31 Temmuz 2017, (Çevrimiçi) <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-21/analytics-bad-data-quality.html> , 31 Kasım 2021.

¹⁷ Ramirez, a.g.e., s.19.

¹⁸ Economist, How To Think About Data in 2019, 22 Aralık 2018, (Çevrimiçi) <https://www.economist.com/leaders/2018/12/22/how-to-think-about-data-in-2019>, 31 Kasım 2021.

¹⁹ Justin Brookman & G.S. Hans, "Why collection matters: surveillance as a de facto privacy harm." Big data and privacy: making ends meet, **The Center For Internet And Society-Stanford Law School**, 2013, s.3, (Çevrimiçi), <https://cdt.org/insights/report-why-collection-matters-surveillance-as-a-de-facto-privacy-harm/>, 31 Kasım 2021.

müşterilerin finansal durumuna odaklanan diğer veri segmentleri daha sorunludur. Bazı müşteriler bu veri segmentleri nedeniyle önyargıyla karşılaşabilir²⁰.

Veri toplamayla ilgili diğer sorun, bilgilendirilme eksikliğidir. Kullanıcılara çevrimiçi gizlilikleri hakkında bilgi verilmesinin yolu, gizlilik politikalarıdır. Bu yüzden kullanıcılar günlük olarak birçok gizlilik politikasına maruz kalmaktadır. Gizlilik politikalarının kullanılmasının ardındaki ana düşünce, kullanıcıların tüm bu geniş çaplı gizlilik politikalarını okuduktan sonra kişisel verilerini vermenin avantajları ve dezavantajları hakkında yerinde karar verebilmeleridir. Yine de bu düşünce, kullanıcıların anlaşılması zor olabilecek uzun gizlilik politikalarına maruz kaldıkları gerçeği göz önüne alındığında pek kullanışlı değildir²¹. Ayrıca, kullanıcılar günlük olarak birçok gizlilik politikasına maruz kaldığından, bu durum karar yorgunluğuna yol açmaktadır. Bazı akademisyenler, karar yorgunluğunun kullanıcıların uğraşlarını en aza indirmelerine ve gizlilik politikalarını okumadan ya da verilerine yönelik olası riskleri değerlendirmeden doğrudan kişisel bilgilerini göndermelerine neden olduğuna inanmaktadır²². Gizlilik politikaları, kullanıcılara, verilerinin nasıl toplandığını, kullanıldığını, nerede saklandığını ve paylaşıldığını iletmelidir. Bununla birlikte, veri işleme sistemi o kadar karmaşık olabilir ki, "sadece bir avuç derin uzman tam bir açıklamayı bir araya getirebilir"²³.

Veri toplama, kullanıcılar için daha önemli riskler oluşturan güvenlik sorunlarını da beraberinde getirir. Güvenlik sorunları, veri ihlallerinden ve verilerin dahili olarak kötüye kullanılmasından kaynaklanabilir. Veri ihlalleri, harici siber saldırılar ya da yetersiz güvenlik nedeniyle ortaya çıkabilir. Siber suçlular için cazip bir hedef, müşterilerinin kapsamlı bir veri tabanına sahip bir işletme olabilir. İşletmeler müşterileri hakkında daha fazla veri edindikçe, veri ihlali ihtimali artacaktır²⁴. Bu

²⁰ Martin, **a.g.e.**, s.872.

²¹ John A. Rothchild, "Against notice and choice: The manifest failure of the proceduralist paradigm to protect privacy online (or anywhere else).", **Clev. St. L. Rev.**, C.66, 2017, s.614.

²² Jie Tang, Umair Akram, and Wenjing Shi, "Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits." **Journal of Enterprise Information Management**, s.1103, 2020 (Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung, 'The role of privacy fatigue in online privacy behavior' istinaden), **Computers in Human Behavior**, C.81, s.42-51,2018.

²³ Helen Nissenbaum "A contextual approach to privacy online.", **Daedalus**, C.140, S. 4, 2011, s. 35.

²⁴ Brookman, **a.g.e.**, s.2.

nedenle Google ya da Twitter gibi daha büyük şirketler bile güvenlik sorunlarına karşı dokunulmaz değildir. Örneğin, 2018'de Google, Google+'da harici bilgisayar korsanlarının üç yıl boyunca yarım milyon kullanıcının verilerine erişimine sebep olan bir "bug" bulduktan sonra Google+'yı kapatma planını açıkladı. Birkaç ay sonra, Google+ API'sinde²⁵ 52,5 milyon kullanıcının²⁶ verilerini açığa çıkaran başka bir hata tespit edildi.

Kişisel verilerin ticari olarak toplanmasının gerektirdiği ciddi bir endişe de personel tarafından iç suistimaldir. Bu, daha önce tartışıldığı gibi, genellikle "veri röntgenciliği" olarak bilinir. Örneğin, bir Google mühendisi birçok gencin kullanıcı hesaplarına casusluk yapmış, kişi listelerini, sohbetlerini ve arama kayıtlarını incelemiştir. Ardından bu verileri aynı gençleri kontrol etmek için kullanmıştır²⁷. 2019'da eski Twitter çalışanları, hükümetekarşı çıkan 6.000'den fazla hesabın kişisel bilgilerini elde ettikleri için Suudi Arabistan'a casusluk yapmakla suçlanmıştır²⁸.

²⁵ API, uygulama programlama arayüzü anlamına gelmektedir. İki farklı uygulama türü olan yazılımı birbirine bağlayan bir veri aktarım protokolüdür. API'ler, kullanıcıların yürütebileceği etkinlikler, giriş verileri ve çıktı verileri dahil olmak üzere kullanıcıların yazılıma nasıl bağlandığını tanımlayan sözleşmeler olarak düşünülebilir. Bkz., Oleksandr Sh, 'What Is an API: Concept and Architecture Types Explained on Real Life Examples' , (Çevrimiçi), <https://www.cleveroad.com/blog/what-is-an-api>, 12 Ocak 2022.

²⁶ Bkz. Lily Hay Newman, A New Google+ Blunder Exposed Data From 52.5 Million Users, (Çevrimiçi), <https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/>, 12 Ocak 2022.

²⁷ Brookman, **a.g.e.**, s.3.

²⁸ The Guardian, (Çevrimiçi), [Former Twitter employees charged with spying on Saudi Arabia | Twitter | The Guardian](#), 31 Kasım 2021.

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİ'NDE VERİ KORUMANIN YASAL GEÇMİŞİ

1. Veri Korumanın Yasal Arka Planı

Tezin ana odağı tüzük olmasından dolayı ve işletmelerin buna uymada karşılaşabilecekleri zorluklar nedeniyle, veri koruma mevzuatının yasal arka planının bilmek önemlidir.

Bilgi ve iletişim teknolojilerinin kullanımındaki artış, kişisel verilerin toplanmasını, depolanmasını, işlenmesini ve dağıtılmasını büyük ölçüde kolaylaştırmıştır. Veri işleme teknolojilerindeki bu hızlı ilerleme, kamu ve özel sektörün kişisel veriler ve veri koruma yasaları hakkındaki görüşlerini de değiştirmiştir. Veri koruma yasaları başlangıçta veri sahibi ile devlet arasındaki ilişkiye odaklanırken, şu an özel sektörü; bir şirket ile bir kişi arasındaki ilişkiyi içerecek şekilde genişlemiştir. Bu değişim, veri koruma politikalarının oluşturulmasına sebep olmuş ve doğal olarak veri korumanın bir yasal düzenleme alanı olarak ortaya çıkmasını sağlamıştır.

OECD (Organisation for Economic Co-operation and Development), 23.09.1980 tarihinde OECD Kişisel Verilerin Gizliliğinin Korunması ve Sınır Ötesi Akışlarına İlişkin Kılavuz İlkeler'i²⁹ benimseyerek kişisel verilerin korunması konusunda uluslararası alanda adım atan ilk kurumdur. Bununla birlikte, bu kurallar doğası gereği esnek yasalardır. OECD ilkelerinin bugün yetersiz kalmasının sebebi, bu ilkelerin teknolojinin bugünkü kadar gelişmediği, kişilerin kendileri hakkında çok fazla bilgi ve görseli dünyanın dört bir yanındaki sosyal medya hesaplarında özgürce paylaşmadıkları bir dönemde kabul görmüş olmasıdır. Teknolojinin ilerlemesi ve internetin yaygın kullanımı, ilkeler ilk kurulduğunda öngörülemeyen ek tehditler üretmiştir³⁰.

²⁹ OECD, (Çevrimiçi) “ Guidelines on the Protection of Privacy and Transborder Flows of personal Data”

<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part2>, 13 Ocak 2021.

³⁰ Murat Volkan Dülger, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması." , **Yaşar Hukuk Dergisi**, C.1 S.2,2019, s.74.

Avrupa Birliđi düzeyinde, "Kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı ile ilgili olarak kişilerin korunmasına ilişkin 24 Ekim 1995 tarihli Avrupa Parlamentosu ve Konseyi'nin 95/46/EC sayılı Direktifi"³⁷ 24 Ekim 1995 tarihinde yayınlanmıştır. Bu Direktif, AB düzeyinde geniş ve kapsamlı bir veri koruma sistemi sunmaktadır. Avrupa Birliđi Genel Veri Koruma Tüzüğü tarafından yürürlükten kaldırılana kadar AB'deki birincil veri koruma mevzuatıydı³⁸. Direktif, kişisel verilere daha güçlü koruma sağlama ve Üye Devletlerin iç hukuklarını uyumlu hale getirme ve kişisel verilerin serbest dolaşımını sağlama ihtiyacı nedeniyle ortaya çıkmıştır. İç pazarda, malların, paranın, hizmetlerin ve insanların serbest dolaşımı, verilerin de serbest dolaşımını ihtiyacını ortaya çıkarıyordu. Üye Devletler eşit derecede yüksek bir veri koruma³⁹ seviyesine güvenmedikçe bu başarılamazdı. Bununla birlikte, Direktif ikincil mevzuattı, yani Üye Devletlerin bunu kendi iç hukuklarına aktarmaları gerekiyordu. Üye Devletler, aktarma gerçekleştiğinde bir takdir yetkisine sahip olduklarından, Direktif farklı ülkelerde farklı yorumlanmıştır ve iç hukuka tek tip olarak aktarılmamıştır. Sonuç olarak, Direktif AB'de⁴⁰ kişisel verilerin korunmasına ilişkin yeknesaklık sağlayamamıştır.

7 Aralık 2000 tarihinde imzalanan Avrupa Birliđi Temel Haklar Şartı (AB Şartı), 1 Aralık 2009 tarihinde Lizbon Antlaşması'nın kabulü ile bağlayıcı hale gelmiştir.⁴¹ Bu Şart'ın 7.⁴² ve 8.⁴³ maddeleri, AB hukuk düzeninde veri gizliliđi hakkı ve veri koruma hakkının temelini oluşturmaktadır. Veri koruma ve veri gizliliđi politikaları açısından Lizbon Antlaşması'nın⁴⁴ 16. maddesi önemlidir. Anlaşmanın 16.

³⁷Mevzuatın tam metni için bkz., (Çevrimiçi), [EUR-Lex - 31995L0046 - EN \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046) , 15 Ocak 2022.

³⁸ Dölger, , **a.g.e.**, s.79.

³⁹ Giakoumopoulos, **a.g.e.**, s.29.

⁴⁰ **A.e.**,s 30.

⁴¹ European Union, Charter of Fundamental Rights of The European Union, (Çevrimiçi), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>, 15 Ocak 2022.

⁴² Madde 7: "*Herkes özel hayatına, aile hayatına, evine ve yazışmalarına saygı duyma hakkına sahiptir.*"

⁴³ Madde 8: "*Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir.*"

⁴⁴ Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, S. 2007/C306/01, 13 Aralık 2007, (Çevrimiçi) <https://www.refworld.org/docid/476258d32.html> , 27 Temmuz 2022.

maddesi veri koruma hakkından bahsederken Avrupa Parlamentosu'nun veri koruma mevzuatının şekillendirilmesinde daha fazla yer alacağını da belirtmektedir⁴⁵.

2. 95/45/EC Sayılı Direktif ve Eksiklikleri

Direktifin veri işleme faaliyetleri üzerindeki etkisi yadsınamaz: ilkeleri kişisel verileri, kişisel verilerin kullanımına yönelik düzenleyici tepkileri ve veri koruma politikasındaki diğer gelişmeleri tanımlamıştır. Veri Koruma Direktifi veri işlemenin dosya sistemleri ve anabilgisayarları gibi yöntemlerle yapıldığı 1995 yılında kabul edilmiştir. Bu tür bir modelle gelen riskler, her rol⁴⁶ için kurallar ve yükümlülükler belirleyerek kolayca kontrol edilebilir. Bu nedenle, bu düzenleme, internetin ticarileştirilmesiyle birlikte yaşanan köklü değişiklikler karşısında çağdışı kalmaktadır. Çünkü yapay zeka, makine öğrenimi gibi bu dönüşüm sırasında hayatımıza hızla giren yeni teknolojiler bir yandan, önemli faydalar sağlamaktadır, diğer bir yandan ise, veri toplama, işleme, depolama ve yeniden kullanma ile ilgili modern riskler de getirmektedir. Bu nedenle yeni gelişmelere uyum sağlamak için yeni düzenlemelerin benimsenmesi kaçınılmaz hale gelmektedir.

Ek olarak, bu Direktifin temel amacı, yerel düzenlemeleri uyumlu hale getirerek veri sahiplerinin gizlilik hakkına sahip olduklarından emin olmak ve kişisel verilerin Avrupa pazarında serbest akışının önündeki engelleri kaldırmaktır. Bu nedenle, Direktif gelecekteki veri işleme ve gizlilik konularıyla başa çıkabilecek yasal bir çerçeve oluşturmayı hedeflemiyordu⁴⁷.

Direktif tam uyumlaştırma (ve yüksek derecede koruma) sağlamayı amaçlamakla birlikte, Üye Devletler tarafından farklı şekilde uygulanmıştır. Bu,

⁴⁵ Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 Aralık 2007, 2007/C 306/01, (Çevrimiçi), <https://www.refworld.org/docid/476258d32.html>, 27 Temmuz 2022.

⁴⁶ Neil Robinson et al, "Review of the European Data Protection Directive", **Rand**, 2009, s.7, (Çevrimiçi), https://www.rand.org/pubs/technical_reports/TR710.html, 10 Aralık 2021.

⁴⁷ A.e., s.7.

tanımları ve gereksinimleri farklı şekilde yorumlayan ulusal mevzuatlarla birlikte AB genelinde farklı veri koruma standartlarının oluşmasına yol açmıştır. Ek olarak, uygulamanın kapsamı ve cezaların ciddiyeti Üye Devletler arasında farklılık göstermiştir. Bu faktörler, AB veri koruma düzenlemelerindeki son revizyonlara katkıda bulunmuştur⁴⁸.

3. Tüzüğün Hazırlık Süreci

Tüzüğü değerlendirmeden önce, bu noktaya kadar olan olayları göz önünde bulundurmak çok önemlidir. Tüzüğün hazırlık süreci, Avrupa Birliği Komisyon'un 2010 planıyla başladı⁴⁹. Avrupa Komisyonu, iletişimin yayınlanması yoluyla, AB'nin değişen küreselleşen ortama uyum sağlamak ve gelişmekte olan teknolojiyle ilgili kalmak için yeni yasalara ihtiyacı olduğunu göstermiştir. Ek olarak, Avrupa Komisyonu, kişisel gizlilikle ilgili yeni endişeler ortaya çıktıkça Veri Koruma yasasını değiştirme talebini belirtti.

Daha sonra, Avrupa Birliği Komisyonu 95/46/EC sayılı Direktifte kapsamlı değişiklikler içeren bir öneri hazırladı ve 25 Ocak 2012'de bunu yayınladı. Aynı gün, Başkan Yardımcısı Viviane Reding bu teklifi Avrupa Komisyonu adına kamuoyuna açıkladı. Reding, yaptığı açıklamada, 17 yıl önce Avrupa'da internet kullanıcılarının oranının sadece %1 olduğunu, bugün ise saniyeler içinde kıtalar arasında büyük miktarda veri aktarımı yapıldığını ve önerilerin sektörün sağlıklı büyümesini sağlarken bireylerin dijital ortamda kişisel verilerinin korunmasını güçlendireceğini vurguladı⁵⁰.

⁴⁸ Giakoumopoulos **a.g.e.**, s.30.

⁴⁹ Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions A Comprehensive approach on personal data protection in the European Union, (Çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52010DC0609>, 11 Aralık 2021.

⁵⁰ Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, 25 Ocak 2012, (Çevrimiçi), http://europa.eu/rapid/press-release_IP-12-46_en.htm, 11 Aralık 2021.

Daha sonra, Madde 29 Çalışma Grubu⁵¹ (Article 29 Working Party) sonrasında da veri korumada reforma ihtiyaç olduğunu belirtmiştir⁵².

Tüzüğün kabul edilmesinden önce, Komisyon, Parlamento ve Konsey arasında bir toplantı yapıldı. 15 Aralık 2015 tarihinde, Avrupa Parlamentosu ve Komisyon arasında, AB genelinde veri koruma yasasının temel çerçevesini belirleyen modern ve uyumlaştırılmış yeni veri koruma kurallarının benimsenmesi konusunda bir anlaşmaya varılmıştır. Tüzüğün son taslağı 27 Nisan 2016'da kabul edilmiş ve 4 Mayıs 2016 tarihinde AB Resmi Gazetesi'nde yayınlanmıştır. Tüzük 99 madde ve 173 genel gerekçeden (recitals)⁵³ ibarettir. Yeni mevzuat bir tüzük olduğundan, AB'nin tüm üye devletlerine eşit ve otomatik olarak uygulanır, bu nedenle ulusal mevzuata aktarılmasını gerektirmez. Tüzükler, Avrupa Birliği'nin tüm üye devletleri için yasal olarak bağlayıcıdır⁵⁴.

Tüzük, bürokratik kağıt tabanlı gereklilikleri ortadan kaldırmaya ve AB veri korumasının odağını pratik uyumluluğa, yasal yeknesaklığa ve bireysel güçlendirmeye kaydırmaya çalıştığından, Kopernik devriminebenzer bir etki yaratacağı belirtildi. Bu çerçevede tüzüğün kişilerin haklarını vurgulayan yeni bir anlayış getirdiği vurgulanmaktadır⁵⁵.

⁵¹ 95/46/EC sayılı Direktifin 29. Maddesi, AB üye devletlerinin veri koruma makamlarının temsilcilerinden, Avrupa Veri Koruma Denetçisi'nden ve Avrupa Komisyonu'ndan oluşan çalışma grubunu ifade eder. Bu Çalışma Grubu bir karar verici olmamasına rağmen, çalışmalarında bağımsızdı. Veri korumada ortaya çıkan sorunların çözülmesi ve güncel konularda görüş hazırlanması gibi yönlendirici bir etkiye sahipti. Tüzüğün yürürlüğe girmesiyle Madde 29 Çalışma Grubu sona ermiş ve yerine Avrupa Veri Koruma Kurulu (EDPB) kurulmuştur. Tüzüğün 68. maddesi ile oluşturulan yeni Kurul, veri koruma makamlarının başkanları ve AB üye ülkelerinin temsilcileri ile Avrupa Veri Koruma Denetçisi temsilcilerinden oluşmaktadır, (Çevrimiçi), [Who we are | European Data Protection Board \(europa.eu\)](http://www.european-data-protection-board.europa.eu), 10 Aralık 2021.

⁵² EDPS, The History of the General Data Protection Regulation, (Çevrimiçi), https://edps.europa.eu/data-protection/dataprotection/legislation/history-general-data-protection-regulation_en, 10 Aralık 2021.

⁵³ Gerekçeler, maddeleri doğru bir şekilde anlamak ve uygulamak için ek bilgi ve destekleyici bağlam sağlar.

⁵⁴ Types of EU Law, (Çevrimiçi), https://ec-europa-eu.translate.goog/info/law/law-making-process/types-eu-law_en? x tr sl=en& x tr tl=tr& x tr hl=tr& x tr pto=op.sc, 10 Aralık 2021.

⁵⁵ Christopher Kuner, "The European Commission's proposed data protection regulation: A copernican revolution in European data protection law." **Bloomberg BNA Privacy and Security Law Report**, 6 February 2012, (Çevrimiçi), http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-DataProtection-Law.pdf, 10 Aralık 2021; Kopernik, daha önce inanılan aksine, dünyanın güneşin etrafında döndüğünü keşfetmiştir (detaylı bilgi için bkz.) What is the Copernican Revolution in Kant, (Çevrimiçi), <https://www.the-philosophy.com/copernican-revolution-kant>, 10 Aralık 2021.

ÜÇÜNCÜ BÖLÜM

GENEL VERİ KORUMA TÜZÜĞÜ

1.Tüzüğe Genel Bakış

1.1. Kişisel Veriler

Tüzük, sadece verilerin işlenmesi kişisel verileri içerdiğinde geçerlidir. Tüzüğün 4(1). maddesi uyarınca

"kişisel veriler" tanımlanmış veya tanımlanabilir bir gerçek kişiyle ("veri sahibi") ilgili herhangi bir bilgi anlamına gelmektedir; tanımlanabilir bir gerçek kişi, doğrudan veya dolaylı olarak, özellikle bir isim, kimlik numarası, konum verileri, çevrimiçi bir tanımlayıcı gibi bir tanımlayıcıya veya söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak tanımlanabilen kişidir."

Yani, bir kişinin kimliğini açıkça ortaya koyan veya ek bilgilerle ortaya çıkarılmasını mümkün kılan bilgilerdir.

Madde 4 (1), "herhangi bir bilginin" kişisel veri olabileceğini ve bunun son derece kapsayıcı bir husus olduğunu içerir. Çünkü hem kişinin yaşı, boyu gibi nesnel verileri hem de görüşler, yargılar veya tahminler gibi öznel verileri gerektirir. Bir kişinin kredibilitesinin değerlendirilmesi, öznel veriler için bir örnek olabilir. Bilgi, belirli bir kişiye yanlış bir şekilde atanmış olsa bile, ister olgusal olarak yanlış olsun, ister gerçekte başka bir kişiyle ilgili olsun, yine de o kişiyle ilgili olduğu için kişisel veri olarak kabul edilir. Veriler, bir kişiyi tanımlamak için kullanılamayacak ölçüde hatalıysa, kişisel veri olarak kabul edilmez⁵⁶.

Tüzük uyarınca, gerçek bir kişiyi doğrudan veya dolaylı olarak tanımlamak için kullanılabilecek herhangi bir verinin kişisel veri olarak sınıflandırılması muhtemeldir. Bir veri sahibi yalnızca işlenmekte olan bilgilere dayanarak tanımlanabiliyorsa, bu da bir veri sahibini diğer bireylerden ayırıyorsa, bu doğrudan tanımlama olarak kabul edilir. Bir veri sahibi, ek bilgileri diğer bilgilerle birleştirerek tanımlanabiliyorsa, bu

⁵⁶ What is Considered Personal Data Under the EU GDPR?, (Çevrimiçi), <https://gdpr.eu/eu-gdpr-personal-data/>, 10 Aralık 2021.

dolaylı tanımlamadır. İşletmeler zaten ek bilgilere sahip olabilir ya da bunları farklı bir kaynaktan edinmiş olabilir⁵⁷.

Madde 4 (1), kişisel verilerin tanımlanabilir bir bireyle “ilgili” olması gerektiğini belirtir. Bu, işlenen verilerin bir şekilde bireyi ilgilendirmesi gerektiği anlamına gelir⁵⁸.

Madde 4 (1), tanımlayıcıların bir listesini "*bir isim, bir kimlik numarası, konum verileri, bir çevrimiçi tanımlayıcı*" verir. Gerekçe 30. madde ayrıca çevrimiçi tanımlayıcılara açıklama getirmektedir. Bu gerekçeden dolayı, farklı çerez türleri, internet protokol adresleri ve radyo frekansı tanımlama etiketleri gibi diğer tanımlayıcılar çevrimiçi tanımlayıcılar olarak nitelendirilebilir. Gerekçe 30 madde, çevrimiçi tanımlayıcıların kapsamlı bir listesini sunmaz. Tanımlayıcılar, belirli bir cihazı tanımlamak için kullanılabilecek herhangi bir bilgi parçası olabilir⁵⁹.

Özetle, bilgi gerçek bir kişiyle ilişkilendirilemediği takdirde kişisel veri olarak kabul edilmez. Kişisel veri, veri sahipleri ile herhangi bir şekilde ilişkilendirilebilecek her şey olarak tanımlanmaktadır. Sonuç olarak, şirketlerin verilerin toplanma ve kullanılma şekli konusunda dikkatli olmaları gerekmektedir, çünkü veri sahibinin anonimliğini tehlikeye atacak şekilde yanlışlıkla yeterli bilgi toplamak kaçınılmaz olabilir⁶⁰.

⁵⁷Information Commissioner’s Office, Personal Data, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>, 10 Aralık 2021.

⁵⁸ Information Commissioner’s Office, Personal Data, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>, 10 Aralık 2021.

⁵⁹ What is Considered Personal Data Under the EU GDPR?, (Çevrimiçi), <https://gdpr.eu/eu-gdpr-personal-data/>, 10 Aralık 2021.

⁶⁰ ITGP Privacy Team “EU General Data Protection Regulation: An Implementation and Compliance Guide”, Bs.2, IT Governance Publishing, 2017, (bu kaynağa çevrimiçi ortamda ulaşılmıştır ve sayfa numaraları bulunmamaktadır) <https://learning.oreilly.com/library/view/eu-general-data/9781849289467/>, 28 Ocak 2022.

1.2. Veri Sahibi

Tüzük uyarınca, yalnızca gerçek kişiler veri sahibi olarak kabul edilebilir. Tüzük, "*gerçek kişi*" terimini kullanarak, tüzel kişilerin veri sahibi olmadığını, çünkü onlarla ilgili verilerin kişisel veri olarak nitelendirilmediğini belirtir. Ek olarak, bir veri sahibi olarak nitelendirilmek için, bir kişinin hayatta olması gerekir. Vefat eden kişilerin çoğu durumda tüzük kapsamında herhangi bir hakkı yoktur⁶¹.

Bir şirketin vergi işleri hakkındaki bilgilere erişimi içeren bir davada, Avrupa Birliği Adalet Divanı (ABAD), bir tüzel kişi hakkındaki bilgiler ile gerçek bir kişi hakkındaki bilgiler arasındaki temel bir farkı onayladı⁶². Divan, tüzük kapsamında yalnızca ikinci veri kategorisinin korunduğunun altını çizmiştir⁶³.

1.3. Takma Ad Verme ve Anonimleştirilmiş Veriler

Tüzük Gerekçe 26. maddeye göre, takma ad verilen kişisel veriler kişisel veri olarak kalır ve tüzük hükümlerine tabidir. Takma ad vermenin tanımı, Madde 4 (5)'te "*kişisel verilerin, artık ek bilgi kullanılmadan belirli bir veri sahibine atfedilemeyeceği şekilde işlenmesi*" olarak verilmiştir. Buna karşılık, anonimleştirilmiş veriler kişisel veri olarak kabul edilmez ve bu nedenle tüzük hükümlerine tabi değildir. Gerekçe 26.madde ayrıca, anonimleştirilmiş verileri "*tanımlanmış veya tanımlanabilir bir gerçek kişiyle veya veri sahibinin tanımlanamayacağı veya artık tanımlanamayacağı şekilde anonim hale getirilen kişisel verilerle ilgili olmayan bilgiler*" olarak açıklamaktadır.

Anonimleştirme ve takma ad verme arasındaki ayrım, verilerin yeniden tanımlanabilmesidir. Uygun şekilde gerçekleştirildiğinde, anonimleştirme, kişisel

⁶¹ ITGP Privacy Team, a.g.e.; <https://gdpr.eu/eu-gdpr-personal-data/>, 28 Ocak 2022.

⁶² ABAD, Land Nordrhein-Westfalen, T. 10 Aralık 2020, K.620/19, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?jsessionid=08A045CD30C784065E25601D79A42B31?text=&docid=235346&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=290311>, 11 Aralık 2021.

⁶³, Christopher Kuner, et al. "The EU General Data Protection Regulation: A Commentary/Update of Selected Articles." Update of Selected Articles , Oxford University Press, 2021, s.26.

verilerin işlenmesini ve depolanmasını Tüzüğün kapsamından muaf tutar⁶⁴. Madde 29 Çalışma Grubu, gerçek veri anonimleştirmenin üstesinden gelinmesinin zor olduğunu açıkça belirtmiş olsa da veri denetliycileri verileri anonimleştirmede sıklıkla başarısız olmaktadır⁶⁵.

1.4. İşleme

Veri işleme, kişisel veriler üzerinde otomatik veya otomatik olmayan bir şekilde gerçekleştirilen herhangi bir işlemi veya bir dizi faaliyeti ifade etmektedir. Veri işleme, kişisel veriler üzerinde aşağıdaki faaliyet kümelerini içerir: *"toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri alma, danışma, kullanma, iletim yoluyla açıklama, yayma veya başka bir şekilde kullanıma sunma, hizalama veya birleştirme, kısıtlama, silme veya imha"*. Kişisel veriler üzerinde ve bunlarla ilgili olarak gerçekleştirilen her faaliyet veri işlemedir⁶⁶.

1.4.1. Kontrolör

Tüzük madde 4(7)'deki tanıma gelince: *"kontrolör"*, veri işlemenin amaç ve vasıtalarının Birlik hukuku veya üye devlet hukuklarından birine tabi olduğu hallerde, kişisel verilerin işlenmesinin amaçlarını ve vasıtalarını tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu otoritesi, kurum veya diğer organ anlamına gelmektedir". Bu, veri kontrolörünün, kişisel verilerin işleme amaçlarına ve araçlarına karar verdikleri için birincil karar vericiler olduğu anlamına gelir. Bu

⁶⁴ Bazı akademisyenler anonimleştirilmiş verilerin de yeniden tanımlanabileceğini savunuyorlar, bkz., Boris Lubarsky, Re-Identification of "Anonymized" Data, **Geo. L. Tech. Rev.**, C.1, s.202 vd. 2017.

⁶⁵ Matt Wes "Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization, APP", 25 Nisan 2017, (Çevrimiçi), <https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/>, 12 Aralık 2021.

⁶⁶ Tüzük madde 4(2).

kategori altında: özel şirketler veya diğer tüzel kişiler gibi tüzel kişilerin yanı sıra, anonim olmayan bir kuruluştaki ortaklar gibi gerçek kişiler, diğer serbest meslek sahipleri de düşünülebilir⁶⁷. Kontrolör tipik olarak veri sahiplerinin bilgilerini sağladığı "*halka açık*" varlıktır⁶⁸. Bu tezin amacı doğrultusunda, özel kuruluşlara odaklanacağız.

Tüzüğün 24. maddesi, kontrolörlerin tüm veri koruma ilkelerine aktif olarak tam uymaları gerektiğini belirtir. Bu madde nedeniyle, veri işlemenin niteliğini, amacını, kapsamını ve veri sahiplerinin özgürlüklerine ve haklarına yönelik herhangi bir risk olasılığını göz önünde bulundurmamak bir veri kontrolörünün sorumluluğundadır. Bu nedenle, veri kontrolörleri "*işlemenin bu Tüzüğe uygun olarak gerçekleştirildiğini göstermek ve gösterebilmek için uygun teknik ve organizasyonel önlemleri uygulayacaklardır.*" Gerekçe 75.madde, ayrıca veri sahiplerinin hak ve özgürlüklerine yönelik risklerin bir açıklamasını vermektedir.

Madde 28(1) uyarınca, veri kontrolörleri, verileri onların adına işleyen herhangi bir işleyicinin tüzük hükümlerine uymasını sağlamaktan da sorumludur.

1.4.2. İşleyiciler

Veri işleyiciler, gerçek kişiler veya şirketler ya da kontrolör tarafından kendi adlarına işleme faaliyetlerini gerçekleştirmek üzere sözleşmeli diğer tüzel kişiler olabilir⁶⁹. Bir sözleşme veya başka bir yasal işlem, veri kontrolörü ve işleyici arasındaki ilişkileri düzenler⁷⁰. Kontrolör ve işleyiciler arasındaki sözleşmeler tüzüğün 28.maddesinde belirtilen çeşitli koşullara tabidir. Sözleşme, işlenecek kişisel veri türlerini, işlemenin hedef ve amacını ve işleme süresini belirtmelidir. Veri işleyiciler

⁶⁷ GDPR Data Controllers and Processors, (Çevrimiçi), <https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/> , 16 Aralık 2021.

⁶⁸ ITGP Privacy Team, **a.g.e.**

⁶⁹ Tüzük madde 4(8).

⁷⁰ Tüzük madde 28(3).

operasyonel kararları bağımsız olarak aldığından kontrolörün veri işlemenin her yönünü belirtmesi gerekmez⁷¹.

Veri işleyici ve kontrolör arasında ayırım yapmak çok önemlidir, çünkü veri işlemcileri veri kontrolör ile aynı uyumluluk yükümlülüklerine tabi değildir. Bununla birlikte, Tüzüğün 28. maddesine göre, veri işleyici, bu tüzüğün standartlarına uymak için yeterli organizasyonel ve teknolojik önlemleri uygulamalıdır. İşleyiciler, veri sahiplerinin haklarının korunmasını sağlamaktan sorumludur ve bu nedenle kendi güvenlik önlemlerini uygulamalıdır⁷².

İşleyicilerin yalnızca veri kontrolörlerinin yasal talimatları doğrultusunda işleme faaliyetleri gerçekleştirmesine izin verilir ve işleyici ve kontrolör ilişkisi esas olarak bir sözleşmeye tabidir. İşleyiciler, belirli bir sözleşmenin yerine getirilmesine yardımcı olması için "kontrolörün önceden özel veya genel yazılı onayı olmadan" başka bir işleyiciyi görevlendiremez⁷³. Bu, kontrolörün veri işleme zincirinin her seviyesinde gerçekleşen güvenlik önlemlerinin farkında olmasını sağlar⁷⁴.

Veri işleyiciler, Tüzük 82.madde uyarınca kontrolör ile birlikte veri ihalleri için sorumluluk taşımaktadırlar. Bununla birlikte, paragraf 2'de belirtildiği gibi, işleyicinin sorumluluğu, onun özel yükümlülüklerinin ihlali ile sınırlıdır. Her iki taraf da kendi suçsuzluğunu ortaya koyma seçeneğine sahiptir. Bunu yapmak için, veri sahibine zararlarla sonuçlanan olayda hatalı olmadıklarını ispatlamaları gerekir⁷⁵.

⁷¹ ITGP Privacy Team, **a.g.e.**

⁷² GDPR Data Controllers and Processors, (Çevrimiçi), <https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/> , 16 Aralık 2021.

⁷³ Tüzük madde 28(2), madde 29.

⁷⁴ ITGP Privacy Team, **a.g.e.**

⁷⁵ Processing, (Çevrimiçi), <https://gdpr-info.eu/issues/processing/>, 16 Aralık 2021.

1.4.3. Ortak Kontrolörler

Tüzüğün 26 (1) maddesine göre, “*iki veya daha fazla kontrolörün veri işlemenin amaçlarını ve yöntemlerini ortak belirlediği hallerde, bunlar ortak kontrolörlerdir*”. Veri kontrolörleri, ortak veri kontrolörleri olarak diğer taraflarla işbirliği içinde veri işleme faaliyetlerinin amaçları ve araçları hakkında ortak karar verebilir. Aynı veriler farklı amaçlar için işlendiği durumlarda, bu ortak kontrolörlük olarak kabul edilmez. Ortak kontrolörlerin ortak bir amacı vardır, onlar aynı veri tabanı kümesini kullanır ve veri işleme faaliyetini ortak bir amaç için hayata geçirmektedirler⁷⁶.

Ortak kontrolörlerin her ikisi de güvenlik ihlallerinden eşit derecede sorumludur. Kontrolörlerin ilgili sorumlulukları Birlik veya üye devlet hukuku tarafından belirlenmediği halde, ortak kontrolörler sorumluluklarını, bu Tüzük kapsamındaki yükümlülüklerle uygunluklarını, aralarında yaptıkları bir sözleşme vasıtasıyla şeffaf bir şekilde belirleyebilirler⁷⁷. Bununla birlikte, “*veri sahibi, kontrolörlerin her biri ile ilgili olarak ve aleyhine bu Tüzük kapsamındaki haklarını kullanabilir*”⁷⁸.

1.5. Konu itibariyle Uygulama Alanı

Tüzüğün şirketlere uygulanabilmesi için, yer itibariyle ve konu itibariyle uygulama alanına girmeleri gerekir. Tüzüğün konu itibariyle uygulama alanı 2.maddede belirlenmiştir. Tüzük, yalnızca kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesi durumunda ve yalnızca kişisel veriler bir dosyalama sistemine dahil

⁷⁶ GDPR Data Controllers and Processors, (Çevrimiçi), <https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/> , 16 Aralık 2021.

⁷⁷ Tüzük madde 26(1).

⁷⁸ Tüzük madde 26(3).

edildiğinde veya dahil edilmesi amaçlandığında otomatik olmayan işleme için maddi anlamda uygulanabilir.

Madde 2 (2) Tüzüğün uygulama alanına istisnalar getirmektedir: ilgili ulusal güvenlikle ilgili veri işlenmesi gibi AB hukukunun yetki alanı dışında kalan veri işleme faaliyetleri; AB üye ülkelerinin ortak dış ve güvenlik politikalarına ilişkin işlemler; yalnızca kişisel veya ev içi faaliyetler için doğal olarak işleme; kamu güvenliğine yönelik risklerin korunması ve önlenmesi de dahil olmak üzere cezai suçları önlemek, soruşturmak, tespit etmek veya kovuşturmak ya da cezai yaptırımlar uygulamak için yetkili makamlar tarafından kişisel verilerin işlenmesi.

Maddi kapsam zaten geniş olduğundan, büyüklüğüne bakılmaksızın, kişisel verileri herhangi bir şekilde kullanan herhangi bir şirket, Tüzüğe uymak zorundadır. Bazı maddeler 250'den az çalışanı olan küçük işletmeleri muaf tutsa da küçük işletmelerin hala Tüzük hükümlerine uyması gerekir. Madde 30'a göre, her işletme veri işleme faaliyetlerinin kayıtlarını tutmak zorundadır. Madde 30 (5), 250'den az çalışanı olan işletmeleri bu yükümlülüğünden açıkça muaf tutar. Bununla birlikte, bu muafiyet mutlak değildir. 250'den az çalışanı olan işletmeler, veri sahiplerinin hakları için risk oluşturması muhtemel işleme faaliyetleri gerçekleştirirse veya düzenli olarak işleme faaliyetleri yürütürse veya madde 9'da belirtilen özel veri kategorilerini veya cezai mahkumiyet veya suçlarla bağlantılı verileri işlerse, kayıt tutmaları gerekir. Bununla birlikte, bu tür işletmelerin yalnızca madde 30 (5)'te açıklanan işleme kategorileri için işleme faaliyetlerinin kayıtlarını tutmaları gerekmektedir⁷⁹.

Madde 9 veya 10'da açıklanan kişisel verileri işlemeyen işletmeler, veri sahiplerinin "büyük ölçekte" düzenli ve sistematik bir şekilde gözetimini yapmadıkları sürece bir veri koruma görevlisi (Data Protection Officer-DPO) işe almaktan muaftır. Büyük ölçekli işleme, Tüzükde tanımlanmamıştır. Madde 29 çalışma grubu, işlemenin

⁷⁹ Article 29 Working Party, Position Paper on the Derogations from the Obligation to Maintain Records of Processing Activities pursuant to Article 30(5) GDPR (2018), (Çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/position-paper-derogations-obligation-maintain-records_en, 16 Aralık 2021.

büyük ölçekte gerçekleştirilip gerçekleştirilmediğini değerlendirirken aşağıdaki öğelerin özellikle değerlendirilmesini önermektedir: ilgili veri sahiplerinin sayısı, kayıt sayısı (veri kümelerinin hacmi), işlemenin kalıcılığı. Küçük bir işletmenin büyük ölçekli işlemeye dahil olmadığını gösterebilmesi durumunda, bir veri koruma görevlisi belirlenmesi gerekmez⁸⁰.

1.6. Yer İtibariyle Uygulama Alanı

Tüzük madde 3(1) uyarınca: *“bu Tüzük, veri işleme faaliyetinin Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, bir kontrolör veya veri işleyicinin Birlik içerisinde bulunan işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır.”* Tüzüğün dikkat çekici özelliklerinden biri, sınır aşan bir uygulama alanına sahip olmasıdır. Tüzük coğrafi olarak AB merkezli olmasına rağmen, uygulama alanı Avrupa Birliği⁸¹ sınırlarından daha geniştir.

Tüzüğün, sınır aşan erişimi açısından, veri işleyenin değil de veri sahibinin konumu daha önemlidir. Bununla birlikte, hem veri sahibinin konumu, hem de veri işleyenin konumu Tüzüğün uygulanmasına yol açabilir⁸². Madde 3(2) uyarınca:

“bu Tüzük, işleme faaliyetlerinin aşağıdakilerle ilgili olduğu hallerde, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde yerleşik olmayan bir kontrolör veya işleyici tarafından işlenmesine uygulanır:

a) veri sahibinin ödeme yapmasının gerekip gerekmediğine bakılmaksızın, Birlik içindeki veri sahiplerine mal veya hizmet sunulması; veya

b) veri sahiplerinin davranışlarının Birlik içinde gerçekleştiği sürece izlenmesi”

İşletmelerin AB sakinleri için mal ve hizmet sunup sunmadığını değerlendirmek için, Gerekçe 23’e bakmamız gerekmektedir. Bu gerekçe nedeniyle, AB içerisinde yerleşik olmayan bir kontrolör veya işleyici tarafından AB içerisinde bulunan veri

⁸⁰ GDPR for Small Businesses Under 250 Employees, (Çevrimiçi), <https://www.clarip.com/blog/Tüzük-under-250-employees/>, 16 Aralık 2021.

⁸¹ Paul Voigt, Axel von dem Bussche “**The EU GDPR: A Practical Guide**”, Cham: Springer International Publishing, 2017, s.22.

⁸² Kimberly A. Houser, W. Gregory Voss "GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy.", **Rich. JL & Tech**, C.25, S.1, 2018, s.64.

sahiplerine mal veya hizmet sunma niyetinin belirlenmesi için, kontrolör veya veri işleyicinin AB içerisindeki bir veya daha fazla üye devlette bulunan veri sahiplerine hizmet sunmayı öngördüğünün açık olup olmadığı tespit edilmelidir. Kontrolörün, veri işleyicinin veya bir aracının AB içerisindeki web sitesine, e-posta adresine veya diğer iletişim bilgilerine erişilmesi ya da kontrolörün yerleşik olduğu üçüncü ülkede genel olarak kullanılan bir dilin kullanılması söz konusu niyetin tespit edilmesi için yeterli değildir. Kontrolörün web sitesinde bir veya daha fazla üye devlette genel olarak kullanılan bir dilin veya para biriminin kullanılması ve söz konusu dillerde mal ve hizmetlerin sipariş edilebilmesi ya da AB içerisinde bulunan müşterilerden veya kullanıcılardan bahsedilmesi gibi faktörler kontrolörün AB içerisindeki veri sahiplerine mal veya hizmet sunmayı öngördüğünü açıkça ortaya koyabilir. Örneğin, Türkiye'de faaliyet gösteren bir seyahat şirketinin web sitesini kullanan bir AB vatandaşının bu site aracılığıyla Türkiye'deki bir otel için rezervasyon yaptırdığını varsayalım. Bu durumda, Türkiye'deki şirket bu kişi için Tüzük başvurusu ile karşı karşıya kalabilir.

"İzleme"⁸³ bireyleri çevrimiçi olarak izlemeyi ve kişisel tercihlerini, davranışlarını analiz etmek ve tahmin etmek için profil oluşturma tekniklerini kullanmayı gerektirir. Madde 3(2)(b)'nin arkasındaki mantık nispeten basittir. İşletmeler ancak veri sahiplerini hedef aldıkları takdirde bu Tüzük onlar hakkında uygulanabilir. Bu nedenle, AB hukuku ile veri kontrolörü arasındaki tek bağlantı veri sahiplerinin AB'de ikamet ediyor olması ise, Tüzük uygulanamaz⁸⁴.

⁸³ Tüzük Gerekçe madde 24: "Bir işleme faaliyetinin veri sahiplerinin davranışlarını izlemek için düşünüldüğü düşünülmemeyeceğini belirlemek için, gerçek kişilerin, özellikle kendisiyle ilgili kararlar almak veya kişisel tercihlerini, davranışlarını ve tutumlarını analiz etmek veya tahmin etmek amacıyla, gerçek bir kişinin profilinin çıkarılmasından oluşan kişisel veri işleme tekniklerinin daha sonraki potansiyel kullanımı da dahil olmak üzere internet üzerinden izlenip izlenmediğinin tespit edilmesi gerekir."

⁸⁴ Paul de Hert Michal Czerwinski "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context." **International Data Privacy Law**, C.6, S. 3, 2016, s.238.

1.7. Veri İşleme İlkeleri

İşletmelerin kişisel verileri nasıl ele aldıklarını düzenlemek için Tüzük, madde 5 bir dizi veri işleme ilkesini listeler. Bu ilkeler, işletmelerin temel sorumluluklarının bir taslağı olarak düşünülmelidir. Diğer yükümlülükleri yorumlarken, bu ilkeler dizisi akılda tutulmalıdır⁸⁵.

Madde 5 yedi yol gösterici ilkeyi tanımlamaktadır: "yasaya uygunluk, adalet ve şeffaflık", "amaç kısıtlaması", "veri minimizasyonu", "doğruluk", "depolama sınırlaması", "bütünlük ve gizlilik" ve "hesap verebilirlik". Ayrıca, veri işleme yukarıda belirtilen ilkelere bağlı kalmalıdır.

1.7.1. Yasaya Uygunluk, Adalet, Şeffaflık

Birinci ilke, ayrı ayrı inceleyeceğimiz üç bileşenden oluşur. İlk bileşen, veri işlemenin yasal olması gerektiğidir. İşletmeler veri işleme faaliyetlerinin yasal olarak kabul edilmesini istiyorlarsa, işleme için belirli gerekçeler belirlemelidirler. Veri işlemenin yasal dayanakları Madde 6'da belirtilmiştir. Veri işleme faaliyetleri için hangi zeminin seçileceğinin belirlenmesi, yalnızca işletmelerin amaçlarına ve veri sahipleriyle olan ilişkilerine bağlı olmalıdır⁸⁶. Veri işlemenin yasal dayanakları şunlardır⁸⁷:

- 1) Onay - veri sahiplerinin verilerini işlemek için açık izinleri varsa. Bölüm 3'te onaya daha detaylı olarak bakacağız.
- 2) İşleme, veri sahibinin taraf olduğu bir sözleşmenin ifası için gerekli olduğunda veya bir sözleşmeye girmeden önce veri sahibinin talebi üzerine gerekli adımların atılması için işlemenin gerekli olması halinde;
- 3) Yasal zorunluluk- veri işleme, kontrolörün tabi olduğu yasal bir yükümlülüğe uyması için işleme zorunlu olduğunda;

⁸⁵ ITGP Privacy Team, **a.g.e.**

⁸⁶ Information Commissioner's Office, Lawfulness and transparency, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> , 18 Aralık 2021.

⁸⁷ Tüzük Madde 6.

- 4) Hayati çıkarlar- veri işleme, veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarını korumak için gerekli olduğunda;
- 5) Kamu görevi- veri denetleyicisinin kamu yararına bir görevi yerine getirmesi ya da kontrolöre verilen resmi yetkiyi kullanması için işlemenin gerekli olması halinde;
- 6) Meşru menfaat - veri işleme, veri sahiplerinin kişisel verilerini korumak için bu meşru menfaatlerden daha ağır basan zorlayıcı bir neden olmadıkça, veri kontrolörlerinin veya üçüncü tarafların meşru çıkarları için gerekli ise, özellikle de veri sahibinin küçük olduğu durumlarda. Bu esas, kamu makamlarının resmi sorumluluklarını yerine getirmek için verileri işlemesi durumunda geçerli değildir.

Ek olarak, yasallık, veri kontrolörlerinin geniş anlamda verilerle yasadışı bir şey yapmaması gerektiği anlamına gelir. Buna genel olarak medeni hukuk ve ceza hukuku yükümlülükleri dahildir⁸⁸.

Veri işleme faaliyetleri adil de olmalıdır. Veri işlemenin herhangi bir bölümünün haksız olması durumunda, veri kontrolörleri bu ilkeyi ihlal etmiş olacaktır. İşleme için yasal bir temel gösterme tek başına yeterli olmayıp, veri işlemenin de adil olması gerekir.

Genel olarak, adalet, veri sorumlularının yalnızca yasal olarak verilerini paylaşma yetkisi olan veri sahiplerinden veri toplanması gerektiği anlamına gelir; veri sorumluları veri toplarken kimseyi aldatmamalı veya yanlış yönlendirmemelidir⁸⁹. Ayrıca, adalet, kişisel verilerin yalnızca veri sahiplerinin makul olarak öngörebileceği şekillerde kullanılmasını ve verilerinin kullanılmasının veri sahipleri üzerinde haksız olumsuz etkiler yaratmamasını gerektirir. Ancak, veri sahibini etkileyen zarar gerekçelendirilebiliyorsa, adil olarak kabul edilebilir. Veri sahipleri kişisel verilerine ilişkin haklarını kullanmak istediklerinde de adil muamele görmelidirler. Bu, veri

⁸⁸ Information Commissioner's Office, Lawfulness and transparency, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> , 18 Aralık 2021.

⁸⁹ ITGP Privacy Team, **a.g.e.**

sorumlularının veri sahiplerinin haklarını kullanmalarını kolaylaştırma sorumluluğu ile bağlantılıdır⁹⁰.

Şeffaflık adalete sıkı sıkıya bağlıdır. Gerekçe madde 60'ta belirtildiği gibi, Tüzük'ten de görebiliyoruz ki, *"Adil ve şeffaf işleme ilkeleri, veri sahibinin işleme işleminin varlığı ve amaçları hakkında bilgilendirilmesini gerektirir."* Veri sahibi, verilerinin nasıl işlendiği hakkında bilgilendirilme hakkına sahiptir. Bu, Tüzüğün şeffaflık açısından kritik bir yükümlülüğüdür. Kontrolörler, veri sahiplerine: veri saklama süreleri, veri işleme hedefleri ve kişisel verileri kimlerle paylaştıkları bilgilerini sağlamalıdır. Şeffaflık, kontrolörlerin gerçek kimliklerini veri sahiplerinden gizlememelerini ve veri sahiplerinden elde edilen kişisel verileri nasıl kullanmayı planladıkları konusunda dürüst olmalarını gerektirir. Şeffaflık, kontrolörlerin veri sahipleriyle doğrudan etkileşimi olmadığında ve kişisel bilgilerini başka bir kaynaktan elde etmediğinde bile esastır. Veri sahipleri, verilerinin toplandığının ve işlendiğinin farkında olmayabileceğinden, veri haklarını kullanma imkanlarını sınırlayabileceğinden, belirli durumlarda daha da kritik olabilir. Buna genellikle *"görünmez işleme"* denir⁹¹.

1.7.2. Amaç Sınırlaması

Amaç sınırlaması ilkesi iki *"temel unsur"*dan oluşur. Amaç belirtimi unsuru, kişisel verilerin *"belirli, açık ve meşru amaçlar için toplanmasını"* gerektirir. Amaca uygun işleme unsuru, özel verilerin *"amaçla uyumsuz bir şekilde daha fazla işlenmemesini"* gerektirir⁹².

⁹⁰Information Commissioner's Office, Lawfulness and transparency, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> , 18 Aralık 2021.a

⁹¹ Information Commissioner's Office, Lawfulness and transparency, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> , 18 Aralık 2021.

⁹² Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation" WP 203, 2 Nisan 2013, s.11, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 19 Aralık 2021.

Amaç sınırlaması, işleme amaçlarının açıkça ortaya çıkarılması, açıklığa kavuşturulması ya da anlaşılır bir biçimde temsil edilmesi gerektiğini şart koşar⁹³. Ayrıca, veri işleme faaliyetlerinin, ilgili tüm veri koruma mevzuatı hükümlerine ve tüketici koruma⁹⁴ yasaları gibi diğer geçerli yasalara uyacak şekilde yürütülmesini gerektirir. Bununla birlikte, amaç spesifikasyonunun en önemli şartı, amacın, hangi tür işlemlerin tanımlanan amaç içinde yer alıp almadığının belirlenmesine, ayrıca yasaya bağlılığın değerlendirilmesine ve veri koruma önlemlerinin uygulanmasına izin verecek kadar ayrıntılı olması gerektiğidir⁹⁵. Kişisel verilerin türü ve elde edildikleri özel kaynak, sağlanan amacın yeterince ayrıntılı olup olmadığını belirler⁹⁶.

Amaca uygun işleme unsuru, veri kontrolörün resmi bir değerlendirme yerine önemli bir değerlendirme yapmasını gerektirir. Bu değerlendirmedeki önemli faktörler, verilerin niteliği, orijinal amaç ile sonraki işleme amacı arasındaki bağlantı, verilerin hangi kaynaktan elde edildiği ve veri sahiplerinin verilerinin bu kaynaktan daha sonra kullanılmasına ilişkin makul beklentileri, sonraki işlemin veri sahipleri üzerindeki etkileri ve adil işlemeyi garanti altına almak ve veri sahipleri üzerinde aşırı etkilerden kaçınmak için kontrolör tarafından uygulanan önlemlerdir.

1.7.3. Veri Minimizasyonu

Veri minimizasyonu, işlemeye konu olacak verilerin, *"işlenme amaçlarıyla bağlantılı olarak yeterli, ilgili ve gerekli olanlarla sınırlı olması"*⁹⁷ gerektiği anlamına gelir. Bu, kontrolörlerin amaçları için kesinlikle gerekli olandan daha fazla veri işleyemeyeceği anlamına gelir⁹⁸.

⁹³ A.e., s.17.

⁹⁴ A.e., s.19.

⁹⁵ A.e., s.15.

⁹⁶ A.e., s.16.

⁹⁷ Tüzük madde 5(1)(c).

⁹⁸ ITGP Privacy Team, a.g.e.

Kişisel verilerin işlenmesi, meşru bir amaca ulaşmak için gerekli olan verilerle sınırlandırılmalıdır. Veri işleme, söz konusu menfaatlere, haklara ve özgürlüklere orantısız bir şekilde gerçekleştirilmemelidir. İşleme faaliyetlerinin belirtilen genel amacını yerine getirmek için, işlenmek üzere seçilen veri kategorileri gerekli olup, bir denetleyici, verilerin edinilmesini belirli bir işleme amacı ile doğrudan ilgili olan verilerle dikkatlice sınırlandırmalıdır⁹⁹. Bu ilke, Facebook gibi sosyal medya şirketleri için daha büyük önem taşımaktadır. Çünkü doğum tarihinden başlayarak bir kişinin ilgi alanlarına, arkadaşlarına kadar her türlü kişisel veriyi toplamaktadır. Bu ilke sayesinde sosyal medya şirketleri artık topladıkları veriler hakkında kullanıcıyı şeffaf bir şekilde bilgilendirmek ve veri sahibinin haklarını kullanabilmesini sağlamak için işlenen verilere ilişkin veri tabanını sunmak zorundadır. Bu nedenle, Facebook kullanıcıları, bu verilerin Facebook tarafından işlenmesinin ve saklanması, Tüzüğün 5 (1) (c) ve 5 (1) (e) maddelerinde düzenlenen ilkeler çerçevesinde gerçekleşmesi gerektiğini unutmamalıdır. Madde 16 uyarınca, veri sahipleri, işleme amaçları için yetersiz olan, kendileriyle ilgili eksik verileri düzeltme hakkına sahiptir. Madde 17 uyarınca, işleme amaçları için *"artık gerekli olmayan"* herhangi bir verinin silinmesini talep edebileceklerdir.

Veri işleme, veri kontrolörlerinin amaçlarına ulaşmasında yardımcı olmuyorsa, sahip oldukları kişisel veriler büyük olasılıkla yetersizdir. Kişisel veriler, amaç için yetersiz olması halinde işlenmemelidir¹⁰⁰.

⁹⁹ Giakoumopoulos, **a.g.e.** , s.125.

¹⁰⁰ Information Commissioner's Office, Data minimisation, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> , 18 Aralık 2021.

1.7.4. Doğruluk

Doğruluk ilkesi, verilerin "*doğru olmasını ve gerektiğinde güncel tutulmasını*" gerektirir¹⁰¹. Kontrolör, tüm işleme faaliyetleri boyunca veri doğruluğunun korunmasını sağlamaktan sorumludur¹⁰². Veri sahiplerinin düzeltme ve silme hakkı, veri sahibine yanlış bilgilerin düzeltilmesini ve silinmesini talep etme imkanını veren bu ilkenin bir sonucudur¹⁰³. Yanlış bilgiler mümkün olan en kısa sürede silinmeli veya düzeltilmelidir. Doğruluğu sağlamak için, verileri sık sık incelemek ve güncellemek gerekebilir¹⁰⁴.

Madde 5(1)(d), verilerin güncellenmesinin "*gerektiğinde*" yapılması gerektiğini belirtir. Tıbbi veriler gibi saklanan verilerin güncellenmesine yasalarca izin verilmediği durumlar olabilir, çünkü verileri saklamanın birincil amacı tarihsel bir "anlık çekim" olarak hizmet etmektir. Bu yüzden bir hastanın yanlış teşhisinden kaynaklanan yanlışlıklar olsa bile, bu veriler silinemez. Bunun yerine, önceki veriler korunurken sonraki bulgular kayıtlara eklenebilir. Yanlış verilerin saklanması veri sahiplerine potansiyel olarak zarar verebileceğinden verilerin doğruluğunu güncellenmenin ve rutin olarak doğrulamanın vazgeçilmez olduğu durumlar da vardır¹⁰⁵.

Bu ilke, veri sahibini kimlik hırsızlığı da dahil olmak üzere çeşitli tehditlere karşı korur. Ayrıca, veri sahibi hakkında otomatik profil oluşturma seçimlerinin doğru veriler kullanılarak yapılmasını garanti eder¹⁰⁶.

¹⁰¹ Tüzük madde 5(1)(d).

¹⁰² Giakoumopoulos, **a.g.e.** , s. 127.

¹⁰³ ITGP Privacy Team, **a.g.e.**

¹⁰⁴ Giakoumopoulos, **a.g.e.** , s. 128.

¹⁰⁵ Giakoumopoulos, **a.g.e.** , s.130.

¹⁰⁶ ITGP Privacy Team , **a.g.e.**

1.7.5. Depolama Sınırlaması

Depolama sınırlaması ilkesine göre, veriler *"kişisel verilerin işlendiği amaçlar için gerekli olan süreyi aşmayacak şekilde, veri sahiplerinin tanımlanmasına izin veren bir biçimde tutulur"*. Bu, kişisel verilerin, veri işleme amaçları yerine getirildikten sonra silineceği veya anonim hale getirileceği anlamına gelir¹⁰⁷.

Gerekçe madde 39'da *"Kişisel verilerin gereğinden uzun süre saklanmamasını sağlamak için, kontrolör tarafından silme veya periyodik inceleme için zaman sınırları belirlenmelidir"* şeklinde bir ifade yer almaktadır. Bu ilkeye uyulduğunda, veri kontrolörleri kişisel bilgilerin alakasız, aşırı, yanlış veya güncel olmama olasılığını sınırlandırabilir. Ayrıca, bu tür verileri yanlış kullanma tehlikesini - tüm tarafların menfaatine olacak şekilde - azaltır¹⁰⁸.

1.7.6. Bütünlük ve Gizlilik

Bütünlük ve gizlilik ilkesi nedeniyle, kontrolörler, uygun teknolojik veya organizasyonel önlemlerin kullanılmasıyla, *"yetkisiz veya yasa dışı işlemeye ve kazara kayıp, imha veya hasara karşı koruma da dahil olmak üzere kişisel verilerin uygun güvenliğini"* garanti etmelidir¹⁰⁹. Finansal açıdan bakıldığında, bu muhtemelen en önemli ilkedir. Diğer veri koruma ilkelerinin ihlali veri sahiplerine zarar verebilse dahi sonuçlar genel anlamda sınırlıdır. Diğer yandan, bu ilkeye uyulmaması, genellikle veri ihlallerine neden olur; veri koruma yetkililerinin verilerin güvenli bir şekilde korunmadığını kanıtlaması oldukça kolaylaşır - veri ihlalinin kendisi ikna edici bir kanıttır¹¹⁰.

¹⁰⁷ Giakoumopoulos, **a.g.e.**, s 129.

¹⁰⁸ Information Commissioner's Office, Storage Limitation, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>, 18 Aralık 2021.

¹⁰⁹ Tüzük madde 5(1)(f).

¹¹⁰ ITGP Privacy Team, **a.g.e.**

1.7.7. Sorumluluk

Sorumluluk veya hesap verebilirlik ilkesi, veri kontrolörlerin ve işlemcilerin önceki altı veri işleme ilkesine uymalarını ve bunlara uygunluğu kanıtlamalarını gerektirir. Hesap verebilirlik, kontrolörlerin ve veri işleyicilerinin proaktif olarak ve sürekli olarak veri işleme faaliyeti sırasında veri koruma önlemlerini dikkate almalarını gerektirir¹¹¹. Veri işleyiciler, veri kontrolörlerinin yanı sıra, işleme faaliyetlerinde¹¹² veri işleme ilkelerine uyumdan eşit derecede sorumlu tutulabilirler. Bu ilkeye bağlılık, veri koruma ile ilgili konularla ilgilenecek bir veri koruma görevlisinin¹¹³ atanmasını, ayrıca veri ihlallerinin 72 saat içinde bildirilmesini¹¹⁴, veri koruma politikalarının benimsenmesini ve uygulanmasını, işleme faaliyetlerinin¹¹⁵ belgelendirilmesinin sürdürülmesini, veri koruma etki değerlendirmelerinin yapılmasını gerektirdiğinden zahmetlidir¹¹⁶.

Özellikle, hesap verebilirlik sorumluluk ilkesi, şirkete veri aktaran veya şirketten veri alan herhangi bir şirket tarafından Tüzüğe uygunluğu sağlamak için şirketin sınırlarının ötesine geçer¹¹⁷. Diğer bir deyişle, bir işletme, harici bir veri kaynağından veri aldığı anda, verilerin Tüzüğe uygun olarak alınmasını ve kullanılmasını sağlamaktan sorumludur. Yani, bir işletme verileri üçüncü bir tarafa aktardığında, alıcının Tüzüğe uyduğunu doğrulaması gerekir. Öncelikle, aktaran işletme, veri işlemenin yalnızca veri sahibinin rıza gösterdiği amaçlar doğrultusunda gerçekleştiğini doğrulamalıdır. Bu ilkeye uyum, işletmelere veri aktardıkları üçüncü tarafın veri işleme faaliyetlerini izleme, tarama ve denetleme maliyeti gibi doğrudan ve üçüncü tarafın Tüzüğe uyumlu olmayarak topladığı verileri kullanma kapasitesinin kaybı gibi dolaylı maliyetler getirir. Küçük işletmeler, Tüzüğe uymak ve üçüncü taraf

¹¹¹ Giakoumopoulos, **a.g.e.**, s.174.

¹¹² **A.e.**, s.174.

¹¹³ Tüzük madde 37.

¹¹⁴ Tüzük madde 33-34.

¹¹⁵ Tüzük madde 30.

¹¹⁶ Tüzük madde 35.

¹¹⁷ Michal Gal; Aviv Oshrit, "The Competitive Effects of the GDPR", **Journal of Competition Law & Economics**, C.16, S. 3, 2020, s.366.

uyumluluğunu izlemek için daha az kaynağa sahip oldukları için daha büyük bir yük altındadır¹¹⁸.

2. Tüzükle Gelen Önemli Değişiklikler

2.1. Veri Sahiplerinin Yeni Hakları

Tüzük, veri sahiplerine yeni haklar sağladı ve mevcut bazı hakları pekiştirdi. Tüzüğün 17 (1) maddesi, veri sahiplerine "*silme hakkı*" sağlar. Bu hak uyarınca, veri sahipleri onaylarını geri çektiklerinde veya veri işleme Tüzüğün diğer hükümlerini karşılayamadığında, verilerin silinmesi gerekir. Silme hakkı, derhal cevap vermesi gereken veri kontrolörlerine karşı çağrılabilir.

İşletmelerin, veri tabanlarından veri silmeyi reddetme imkanları sınırlı olacaktır. Bu, büyük ölçekli veri işleme veya uzun bir süre boyunca veya farklı biçimlerde elde edilen verilerle uğraşırken işletmeler için özellikle zor olabilir. Bu nedenle, işletmelerin gerektiğinde verilerin tamamen silinebilmesini sağlamak için silme işlemini gerçekleştirmek veya mevcut işleme faaliyetlerini değerlendirmek için bir mekanizma geliştirmeleri önerilir¹¹⁹.

Bu hak aşağıdaki durumlarda geçerlidir:

- 1) Kişisel verilerin orijinal işleme veya toplama amaçları için artık gerekli olmaması durumunda;
- 2) Veri sahiplerinin onay işlemlerini geri çekmeleri ve işleme için alternatif yasal dayanakların bulunmaması durumunda;

¹¹⁸ Damien Geradin, Dimitrios Katsifis, and Theano Karanikioti "GDPR Myopia: How A Well-Intended Regulation Ended Up Favouring Large Online Platforms-The Case of Ad Tech.", **European Competition Journal**, C.17, S. 1, 2021, s.60.

¹¹⁹ ITGP Privacy Team, **a.g.e.**

- 3) Veri sahiplerinin itiraz haklarını meşru menfaatler temelinde kullanmaları ve veri kontrolörlerinin itirazı geçersiz kılan meşru işleme gerekçelerini gösterememesi durumunda;
- 4) Veri denetleyicisinin AB hukuku veya Üye Devlet hukuku kapsamındaki yasal bir yükümlülüğe uymak için verileri silmesi gerekiyorsa;
- 5) Veri işlemenin hukuka aykırı olması durumunda.

Mayıs 2014'te, Avrupa Adalet Divanı, K.132/12 sayılı¹²⁰ kararında unutulma hakkının tanınması yönünde önemli bir adım attı. Dava, ABAD tarafından Google Inc. ile Google İspanya arasındaki bir anlaşmazlık hakkında verilen bir ön kararı ve Bay Costeja Gonzalez ile İspanyol Veri Koruma Ajansı arasındaki ihtilafı içermektedir. Bay Costeja Gonzalez, günlük bir gazete olan La Vanguardia ve Google Inc. ve onun İspanyol yan kuruluşu Google İspanya hakkında İspanyol Veri Koruma Ajansı'na şikayette bulundu. Bay Costeja Gonzalez'in davası, 16 yıl önce borçlu olduğu ve hala La Vanguardia'nın web sitesinde görüntülenen sosyal güvenlik borçlarının tahsiline ilişkin iki mülk açık artırma bildiriminden kaynaklandı. Başvuru sahibi, gazeteyi bu materyali değiştirmeye, silmeye veya korumaya ve Google'ı bu sitelere olan bağlantıları değiştirmeye, silmeye veya gizlemeye yönlendiren bir talepte bulundu. Veri Koruma Kurumu, gazeteye karşı yapılan şikayeti reddetti ve gazetenin meşru bir şekilde tanıtıldığı ve meşru bir amacı olduğu için bu verileri web sitesinde tutmakta haklı olduğu sonucuna vardı. Bununla birlikte, Google'a karşı açılan davayı destekledi. ABAD, K.132/12 sayılı kararında, bireylerin kendileri hakkındaki verilerin veri tabanlarından silinmesini talep etme hakkına sahip olduklarını ve daha sonra Google'ın, veri sahibinin haklarının hem arama motorunun ticari çıkarlarından hem de kamunun bu bilgileri keşfetme konusundaki ilgisinden daha ağır basması nedeniyle kişisel bilgilere olan bağlantıları arama motorundan silmesi beklendiğini kabul etti.

ABAD'ın Google İspanya kararı, AB hukukunda unutulma hakkının kapsamlı bir şekilde oluşturulmasının yolunu açtı¹²¹. Madde 17 (2)'deki "unutulma hakkı",

¹²⁰ ABAD, Google Spain, T:13 Mayıs 2014, K.132/12, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en>, 5 Ağustos 2022.

¹²¹ Federico Fabbrini and Edoardo Celeste, "The right to be forgotten in the digital age: the challenges of data protection beyond borders.", *German law journal*, C.21, S.S1, 2020, s.59.

Tüzük kapsamında tartışmalıdır. Veri kontrolörü kişisel verileri kamuya açıklarsa ve Madde 17 (1)'de belirtilen gerekçelerden biri geçerliyse, kontrolör diğer tüm kontrolörleri bilgilendirmek için makul adımları atmalıdır. İnternete aşına olan herkes, her web sayfasından, haberlerden, arama motoru sonuçlarından ve veri tabanından belirli bir kişiye yapılan tüm referansları ortadan kaldırmanın imkansız olduğunu görecektir¹²². Bu sebeple, Tüzük, silme talebinin *"mevcut teknoloji ve uygulama maliyeti dikkate alınarak, kontrolörleri bilgilendirmek için teknik önlemler de dahil olmak üzere makul adımlar atılması"*¹²³ suretiyle yerine getirilmesi gerektiğini belirten makul bir talep içermektedir.

Bir kavram olarak *"makul adımlar"* Tüzükte daha ayrıntılı olarak açıklanmadığından, bu makul adımlar bakımından objektif kriterler olmadığı anlamına gelir; bunun yerine, sübjektif kriterler söz konusudur, yani bir veri kontrolörü tarafından atılan adımların makul olup olmadığı duruma göre değerlendirilecektir. Küçük, orta ölçekli işletmelere yük getirebilecek *"makul adımlar"* için objektif tanımlayıcı kriterler olduğunu varsayalım. Ancak, orijinal denetleyicilerin verileri işleyen diğer denetleyicileri tanımlaması ve silmesi zor olabilir. Bu nedenle, işletmelerin kişisel verilerin alıcılarını izlemek için teknik ve organizasyonel önlemler almaları önerilir¹²⁴.

Bu kuralın ifade özgürlüğü ve bilgi edinme ile ilgili bazı sınırlamaları vardır. Silme hakkı, ifade ve bilgi edinme özgürlüğü ile çarpıştığında veya işlemenin yasal bir yükümlülüğü yerine getirmek için çok önemli olduğu durumlarda geçerli değildir. İşleme, hukuki iddiaları savunmada veya tarihsel ve bilimsel nedenlerle yapılacak arşivlemelerde için gerekli olabilir¹²⁵.

17. madde kapsamında alınacak silme önlemlerinin coğrafi kapsamı belirsizdir¹²⁶. Fransız Veri Koruma Kurumu CNIL, 15 Mayıs 2015'te Google'a ilgili kişisel verileri tüm alanlardan ve aramalardan tamamen silmesini emretti. Google,

¹²² ITGP Privacy Team, **a.g.e.**

¹²³ Tüzük madde 17(2).

¹²⁴ Voigt, **a.g.e.**, 163.

¹²⁵ Tüzük madde 17(3).

¹²⁶ Voigt, **a.g.e.**, s.164.

CNIL'in böyle bir karar vermek için dünya çapında yetkiye sahip olmadığını belirterek bu soruya cevap verdi¹²⁷.

24 Eylül 2019'da ABAD, unutulma hakkının AB içinde uygulanabileceği görüşünü savunarak Google lehine karar verdi. Tüzüğün bölge dışı uygulanmasına oldukça pragmatik bir yaklaşım getiren bu karar "büyük teknoloji" için bir zafer olarak görülebilir¹²⁸. Bu karar, Avrupa Adalet Divanı'nın gücü Üye Devletlere geri vermesi nedeniyle eleştirildi. Son birkaç on yılda AB veri koruma çerçevesinin uyumlaştırılmasında başarılanların çoğunu görmezden geldiği için "*Avrupa entegrasyonunun ruhuna karşı bir günah*" olarak adlandırıldı¹²⁹. Kararın 72. paragrafı uyarınca: "Buna göre, bir Üye Devletin denetim veya yargı makamı, bir yandan veri sahibinin mahremiyet hakkını ve kendisiyle ilgili kişisel verilerin korunması hakkını, diğer yandan da bilgi edinme hakkını ve bu hakları temel hakların korunmasına ilişkin ulusal standartlar ışığında birbirleriyle karşılaştırdıktan sonra, uygun olduğunda, o arama motorunun operatörüne, o arama motorunun tüm sürümleriyle ilgili bir referans kaldırma işlemi gerçekleştirmesini emretme hakkına sahiptir." Devletlerin bu yorumdan cesaret alıp almayacağını ve farklılaştırıcı ulusal standartlar yaratıp yaratmayacağını göreceğiz.

Fransız vatandaşı bir kişinin Google'dan özel verileri dizine eklemek istediği bir durumu ele alacak olursak, Google'ın yalnızca ".fr, gr" gibi AB alan adlarında dizinden çıkarılması gerekir. Teorik olarak, bu dizinden çıkarma işlemi sonrasında herhangi bir Üye Ülkedeki herhangi biri, ilgili Fransız kişi hakkında kişisel veriler içeren web sayfalarındaki bir bağlantıya erişemez. Bununla birlikte, endeksten arındırılmış materyalin, AB'deki herkes tarafından çeşitli tekniklerle erişilebilir olması son derece muhtemeldir. İnternetin dünya çapındaki erişimi nedeniyle, en basit yöntem

¹²⁷ "We believe that no one country should have the authority to control what content someone in a second country can access" Peter Fleischer, Google Global Privacy Counsel, 'Implementing a European, not global, right to be forgotten', 30 Temmuz 2015, (Çevrimiçi), [Google Europe Blog: Implementing a European, not global, right to be forgotten \(googleblog.com\)](https://www.googleblog.com/2015/07/implementing-a-european-not-global-right-to-be-forgotten.html), 23 Aralık 2021.

¹²⁸ Helen Bourne, Reece Corbett-Wilkins, John Moran "Reflecting on the Google LLC v CNIL (Case C507/17) ECJ Judgment: A UK and Australian Perspective", 28 Ocak 2020, (Çevrimiçi), <https://www.lexology.com/library/detail.aspx?g=86b16836-0673-427e-b10c-317a3320514e>, 23 Aralık 2021.

¹²⁹ Oskar J Gstrein,.: *The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17)*, 9 Eylül 2019, (Çevrimiçi) , <https://verfassungsblog.de/the-judgment-that-will-be-forgotten/>, 23 Aralık 2021.

AB üyesi olmayan bir internet kullanıcısının aramayı yapmasını sağlamaktır. AB'de dizinden çıkarılmış bilgilere erişmenin bir başka yöntemi, arama motoru sürümünden bağımsız olarak coğrafi engelleme gibi önlemleri atlatabilen sanal özel ağların kullanılmasıdır¹³⁰.

İddiaya göre, arama motoru sağlayıcıları AB internet kullanıcılarının dizinden çıkarılmış bağlantılar elde etmelerini engellemek için adımları başarıyla uygularsa, yine de, dizinden çıkarılmış bağlantıları gören AB üyesi olmayan internet kullanıcılarının kişi üzerinde doğrudan ve ciddi bir etkisi olması muhtemeldir¹³¹. Muhtemelen, bu açıklamalar Mahkeme'nin evrensel bir uygulamanın internetin küresel karakteri nedeniyle bu hakkı yeterince koruyabileceğini kabul ettiğini göstermektedir¹³².

Tüzük, veri sahiplerine yeni bir hak olarak, "*veri taşınabilirliği*" sağlar;- bunu yaparak Tüzük, bireylerin kişisel verileri üzerindeki kontrolünü güçlendirir ve onlara daha fazla ekonomik özgürlük sağlar¹³³. Bu hak, veri sahibinin talebi üzerine verilerin bir bilişim teknolojileri ortamından diğerine kopyalanmasını, taşınmasını ve aktarılmasını kolaylaştırır¹³⁴.

Bu hak, yalnızca ilk işlemenin veri sahibinin rızasıyla gerçekleştirilmesi veya veri sahibi ile kontrolör¹³⁵ arasındaki sözleşmenin yerine getirilmesi için işlemenin gerekli olması durumunda, ayrıca işlemenin otomatik yollarla gerçekleştirilmiş olması durumunda geçerlidir¹³⁶.

¹³⁰ Mary Samonte, "Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law.", *European Papers-A Journal on Law and Integration*, C.4, S. 3, s.839-851, 2019, (Çevrimiçi), <https://doi.org/10.15166/2499-8249/332>, 23 Aralık 2021.

¹³¹ K.507/17 Para 57: "Küreselleşmiş bir dünyada, internet kullanıcılarının - Birlik dışındakiler de dahil olmak üzere - çıkar merkezi Birlik'te bulunan bir kişiyle ilgili bilgilere atıfta bulunan bir bağlantıya atıfta bulunmaya erişiminin, Birliğin kendi içindeki bu kişi üzerinde derhal ve önemli etkileri olması muhtemeldir."

¹³² Mary Samonte, "Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law.", *European Papers-A Journal on Law and Integration*, C.4, S. 3, 2019, (Çevrimiçi), <https://doi.org/10.15166/2499-8249/332>, 23 Aralık 2021.

¹³³ Voigt, *a.g.e.*, s.168.

¹³⁴ Article 29 Working Party, Guidelines on the right to data portability, 2016, s.3, (Çevrimiçi) https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-dataportability_e, 26 Aralık 2021.

¹³⁵ Tüzük madde 20(1).

¹³⁶ Tüzük madde 20(2).

Bu veriler doğrudan veri sahibi tarafından sağlanabilir. Veriler tarama geçmişlerini gözlemleyerek veya bir hareket izleyicisi tarafından veri sahibinden alınıyorsa, sözleşme ilişkileri sırasında kontrolör tarafından elde edilebilir. Bu nedenle, veri sahibinin kontrolöre bir erişim seçeneği sunması yeterli zemini oluşturmaktadır. Ancak kontrolörün kişiselleştirme yoluyla profil oluşturduğu veriler bu hakkın kapsamına girmez¹³⁷.

Takma isim verileri de veri taşıma hakkının uygulama alanına girer, bu tür verilerle veri sahibine ulaşılması mümkündür¹³⁸.

Verilerin kontrolörler arasında taşınmasına yönelik taleplerin yönetilmesi Avrupa'nın birçok yerinde yaygındır. Bazı üye ülkelerdeki bankaların çok daha önceden bu kurala uyduğu örneği verilebilir¹³⁹. Tüzüğün kabulünden sonra ise , veri taşıma taleplerinin yönetmek tüm işletmeler için bir gereklilik haline geldi. Bu bazı işletmeler için bir yük, bazı işletmeler içinde bir iş fırsatı olarak görülebilir¹⁴⁰. Örneğin, küçük ölçekli işletmeler daha büyük ölçekli meslektaşlarının veri kayıtlarından yararlanabilir¹⁴¹.

Tüzükde veri formatlarıyla ilgili net bir standart yoktur. Veriler *"yaygın olarak kullanılan, makine tarafından okunabilir ve birlikte çalışabilir formatta"*¹⁴² aktarılmalıdır. Kişisel veriler, bir birey tarafından talep edildiğinde veri kontrolörleri tarafından yeniden kullanılabilir bir biçimde sağlanmalıdır¹⁴³. Bir kişi veri taşıma hakkını kullandığında ve doğrudan bir aktarım talep ettiğinde, veri kontrolörü verileri "engel" yaratmadan başka bir kontrolöre aktarmalıdır¹⁴⁴. Verileri transfer etmesi

¹³⁷Voigt, **a.g.e.**, s.171.

¹³⁸ **A.e.**, s.170.

¹³⁹ Houser, **a.g.e.**, s.75.

¹⁴⁰ ITGP Privacy Team, **a.g.e.**

¹⁴¹ Houser, **a.g.e.**, s.75.

¹⁴² Tüzük madde 20(1), gerekçe madde 68.

¹⁴³ Article 29 Working Party, Guidelines on the right to data portability, 2016, s.13, https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-dataportability_e, 26 Aralık 2021.

¹⁴⁴ Tüzük madde 20(1)

gereken veri kontrolörleri bazen finansal veya teknik engeller yaratabilirler¹⁴⁵. Bu tür engeller şunlar olabilir:

- a) verileri transfer etmesi gereken veri kontrolörünün diğer bir kontrolöre verilerin teslim edilmesi için ücret talep etmesi;
- b) verileri kabul eden kontrolörün, verileri transfer eden kontrolör tarafından sağlanan herhangi bir veri formatına veya uygulama programlama arayüzüne erişememesi;
- c) tüm veri kümesinin transferinin verileri transfer eden kontrolör tarafından aşırı geciktirilmesi veya zorlaştırılması;
- d) verileri transfer etmesi gereken kontrolör tarafından veri kümesinin kasıtlı olarak gizlenmesi veya veri transferi için belirli ve yersiz veya aşırı sektörel standardizasyon veya akreditasyon talebinde bulunması.

Veri sahibinin kendisiyle ilgili kişisel verileri iletme veya alma hakkı, kontrolörler için teknik olarak uyumlu işleme sistemlerini benimseme veya sürdürme yükümlülüğü yaratmamalıdır¹⁴⁶.

Tüzük ayrıca bu hakka bazı kısıtlamalar¹⁴⁷ getirmektedir. Aktarılan veriler diğer bireylere ilişkin bilgiler içeriyorsa, bu durumda veri aktarımı bu kişilerin hak ve özgürlüklerine zarar vermemelidir¹⁴⁸. Bu nedenle, işletmelerin diğer veri sahiplerinin hak ve özgürlüklerine zarar vermeden veri aktarımı gerçekleştirip gerçekleştiremeyeceklerini belirlemek için veri depolama seçeneklerini yeniden değerlendirmeleri tavsiye edilmektedir¹⁴⁹.

Ayrıca, veri taşınabilirliği hakkının temel amacı, hizmet sağlayıcılar arasında adil rekabeti teşvik etmek ve pazara "kilitlenmeyi"¹⁵⁰ önlemektir. Bu hakkın bulunmaması, kullanıcıları hizmet sağlayıcılarına bağımlı kılabilir; böylece

¹⁴⁵ Article 29 Working Party, Guidelines on the right to data portability, 2016, s.15, https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-dataportability_e, 26 Aralık 2021.

¹⁴⁶ Tüzük gerekçe madde 68.

¹⁴⁷ Tüzük madde 20(3): "Bu hak, kamu yararına yürütülen bir görevin yerine getirilmesi veya kontrolöre verilen resmi yetkinin kullanılması için gerekli olan işlemlere uygulanmaz."

¹⁴⁸ Tüzük madde 20(4).

¹⁴⁹ ITGP Privacy Team, **a.g.e.**

¹⁵⁰ Voigt, **a.g.e.**, s.176 (Jotzo Albrect, Datenschutzrecht, Individuelle Datenschutzrechte(2017) istinaden), Tüzük gerekçe madde 19.

kullanıcılar platformları, servis sağlayıcıları değiştirmek konusunda istekli olmayacaklardır.

2.1.1. Avrupa Adalet Divanının 101/01 ve 131/12 Sayılı Kararlarının Mukayesesi

ABAD, hem Lindqvist hem de Google İspanya davasında, kişisel verilerin çevrimiçi bir sayfaya yüklenmesinin "işleniyor" olarak kabul edilmesi gerektiğine karar vermiştir.

Adalet Divanı'nın K.101/01 sayılı Lindqvist kararında şu ifadeler yer almaktadır:

"95/46 sayılı Direktifin 2(b) maddesindeki tanıma göre, madde 3(1)'de kullanılan bu tür verilerin işlenmesi terimi, otomatik yollarla olsun veya olmasın, kişisel veriler üzerinde gerçekleştirilen her türlü işlemi veya işlem grubunu kapsar. Bu hüküm, verilerin iletilmesi, yayılması veya başka bir şekilde kullanıma sunulması yoluyla ifşa edilmesi de dahil olmak üzere bu tür işlemlere çeşitli örnekler vermektedir. Dolayısıyla, kişisel verilerin bir internet sayfasına yüklenmesi bu tür bir işlem olarak kabul edilmelidir"¹⁵¹.

Bir internet sayfasına bilgi göndermek, o sayfayı bir sunucuya yükleme işlemini ve bu sayfayı internete bağlı olanların kullanımına sunmak için gereken eylemleri içerir. Bu tür işlemler otomatik olarak kısmen gerçekleştirilir. Bir web sayfasında çeşitli kişilere atıfta bulunmak ve onları telefon numaralarını veya istihdam koşulları ve hobileri hakkında ayrıntılı bilgi vermek gibi isimleriyle veya başka yollarla tanımlamak, 95/46 sayılı Direktifin 3 (1). maddesinde yer alan "kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesini" kapsar¹⁵².

ABAD, Google İspanya kararında, arama motoru operatörleri ile web sayfaları arasında ayırım yapmış, web sitesi yayıncılarının bir internet sayfasına veri yükleyen kişiler olduğu belirtmiştir ¹⁵³.

¹⁵¹ ABAD, Lindquist, T.6 Kasım 2013, K.101/01, para 25, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=312375>, 26 Aralık 2021.

¹⁵² ABAD, Lindquist, T.6 Kasım 2013, K.101/01, para 26,27, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=312375>, 26 Aralık 2021.

¹⁵³ ABAD, Google Spain, T.13 Mayıs 2014, K.131/12, para 35, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en>, 26 Aralık 2021.

Otomatik, sürekli ve sistematik olarak internette bilgi arayarak, arama motoru verileri toplar. Daha sonra arama motoru, bu verileri dizin oluşturma programları içine "alır", "kaydeder" ve "düzenler", sunucularında "depolar" ve uygun olduğu şekilde, kullanıcılarına işlemeyi oluşturan arama sonuçları listeleri biçiminde "açıklar" ve "kullanıma sunar"¹⁵⁴.

Arama motoru operatörü "kontrolör" kategorisine girer. Çünkü arama motorları, bu faaliyet kapsamında gerçekleştirilen kişisel verilerin işlenmesinin amaçlarına ve yöntemlerine karar verir ve madde 2 (d) uyarınca bu tür bir işlemenin 'kontrolörü' olarak kabul edilmelidir. Arama motorlarını veri kontrolörü olarak görmemek, Veri Koruma Direktifinin 2 (d) maddesine ve amacına aykırı olacaktır. Arama motoru operatörlerinin, üçüncü taraf web sayfalarında yayınlanan bilgiler üzerinde kontrol sahibi olmadıkları için veri kontrolörü olarak kabul edilmemesi durumunda veri sahiplerinin yeterli ve eksiksiz korunması tehlikeye atılır. Ek olarak, arama motorlarının faaliyeti, kişisel verilerin genel olarak yayılmasına, bu verilerin farklı türde yayınlandığı web sayfasını keşfetmeyecek olan internet kullanıcıları da dahil olmak üzere, veri sahibinin adını arayan herhangi bir internet kullanıcısı için erişilebilir hale getirerek önemli ölçüde katkıda bulunur. Ek olarak, arama sonuçları, o kişi hakkında internette bulunan materyallerin sistematik bir özetini verir ve veri sahibinin kapsamlı bir profilini oluşturmalarına olanak tanır. Web sitesi yayıncıları, arama motoru operatörlerini hariç tutma protokolleri aracılığıyla, sitelerinde yayınlanan belirli bilgilerin otomatik dizine eklemenin dışında tutulması gerektiğini bildirebilir. Bununla birlikte, yayıncıların bunu yapmaması durumunda, arama motoru operatörünü kişisel verilerin işlenmesi sorumluluğundan muaf tutmaz¹⁵⁵.

Lindqvist davasında, kişilerin ifade özgürlüğü ve veri koruma hakkı belirlenmiştir. Mahkeme, 95/46 sayılı Direktifin gerekliliklerinin kaçınılmaz olarak ifade özgürlüğünün geniş ilkeleriyle çatışan bir sınırlama getirmediğini, ancak söz konusu haklar ve çıkarlar arasında adil bir denge kurmanın ulusal mahkemelere bağlı

¹⁵⁴ ABAD, Google Spain, T.13 Mayıs 2014, K.131/12, para 28, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en>, 26 Aralık 2021.

¹⁵⁵ ABAD, Google Spain, T.13 Mayıs 2014, K.131/12, para 33-41, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en>, 26 Aralık 2021.

olduğunu tespit etmiştir. Veri koruma ve ifade özgürlüğü birbirine karşı dengelenmelidir ve ilgili Direktif bu dengelemeyi gerçekleştirmek için çok sayıda araca sahiptir. Başvurulan Mahkeme, 95/46 sayılı Direktifi içeren düzenlemelerin ihlalinin uzunluğu ve veri korumasının etkilenen bireylerle olan ilgisi de dahil olmak üzere davanın tüm yönlerini ilgili Tüzükler doğrultusunda değerlendirmelidir¹⁵⁶.

Google İspanya örneğinde, arama motoru operatörlerinin çıkarları ve internet kullanıcılarının erişim hakkı, veri sahiplerinin çıkarlarına karşı dengelenmiştir. Veri sahiplerinin ilgi alanları aşağıdakileri içerir:

"... Bir arama motorunun operatörü tarafından gerçekleştirilen ana işlemlerde söz konusu olan kişisel verilerin işlenmesi, bu motor aracılığıyla yapılan aramanın bir kişinin adı temelinde gerçekleştirilmesi durumunda, mahremiyete ve kişisel verilerin korunmasına ilişkin temel hakları önemli ölçüde etkilemektedir. Çünkü bu işlem, herhangi bir internet kullanıcısının, sonuç listesi aracılığıyla, internette bulunabilecek o kişiyle ilgili bilgilere dayanan bir genel bakış elde etmesini sağlar - potansiyel olarak özel hayatının çok sayıda yönünü ilgilendiren ve arama motoru olmadan ulaşılamayacak ya da yalnızca büyük zorluklarla ulaşılabilecek bilgiler - böylelikle kişinin az ya da çok ayrıntılı bir profilini oluşturur. Ayrıca, veri sahibinin bu haklarına yapılan müdahalenin etkisi, modern toplumlarda internet ve arama motorlarının oynadığı önemli rol nedeniyle artmaktadır¹⁵⁷. "

Arama motoru operatörlerinin ekonomik çıkarları vardır. Bu tür bir müdahalenin potansiyel sonuçları göz önüne alındığında, arama motoru operatörleri tarafından yapılan işlemler ekonomik çıkarlarla haklı gösterilemez. Sonuç listelerindeki bağlantıların web'den kaldırılması, bu bilgilere erişmek isteyen internet kullanıcılarının çıkarlarını engelleyebilir. Bu nedenle Mahkeme, bu menfaat ile veri sahibinin Avrupa Birliği Temel Haklar Şartı'nın 7. ve 8. maddeleri kapsamındaki temel hakları arasında adil bir denge kurulması gerektiğini belirtmiştir. Gerçekte, veri sahibinin bu maddeler tarafından korunan hakları genellikle internet kullanıcılarının çıkarlarından daha ağır basmaktadır. Bununla birlikte, bu haklar arasındaki denge söz konusu bilginin türüne, duyarlılığına ve bu bilgilere erişimdeki kamu yararına bağlı

¹⁵⁶ ABAD, Lindquist, T.6 Kasım 2013, K.101/01, para 82-87, 90, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=312375>, 26 Aralık 2021.

¹⁵⁷ ABAD, Google Spain, T.13 Mayıs 2014, K.131/12, para 80, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en>, 26 Aralık 2021.

olarak değişebilir; bu, veri sahibinin kamusal yaşamdaki rolüne bağlı olarak da değişebilir¹⁵⁸.

2.2. Onay

Yasal bir gerekçe olmadıkça veri işlemeye izin verilmez. Tüzük, veri işleme için altı yasal gerekçe¹⁵⁹ sunar, onay bunlardan biridir. Onay, en basit ve iyi bilinen veri işleme temellerinden biridir, ancak veri kontrolörleri için yasal zorluklara neden olma olasılığı yüksektir¹⁶⁰. Yeni Tüzük, veri sahiplerinden geçerli onay almak için daha katı standartlar içermektedir¹⁶¹. Onayın geçerliliği için bir dizi kriterin karşılanması gerekir. Tüzüğün 4. maddesi şöyledir: "*Veri sahibinin 'onayı', veri sahibinin, bir beyanla veya açık bir olumlu eylemle, kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini ifade eden iradesinin serbestçe , spesifik, bilgilendirilmiş ve açık bir şekilde belirtilmesi anlamına gelir*".

İlk olarak, onay "*serbestçe verilmelidir*". Madde 7 (4)'e göre:

"onayın özgürce verilip verilmediği değerlendirilirken, diğer hususların yanı sıra, bir hizmetin sağlanması da dahil olmak üzere bir sözleşmenin ifasının, söz konusu sözleşmenin ifası için gerekli olmayan kişisel verilerin işlenmesine onay gösterilmesi şartına bağlı olup olmadığı da dikkate alınmalıdır."

Başka bir deyişle, veri sahipleri onay verirken veri kontrolörlerinin etkisinde kalmamalıdır. Bir kullanıcı tarafından verilen onay gönüllü olarak verilmezse, onay

¹⁵⁸ ABAD, Google Spain, T.13 Mayıs 2014, K.131/12, para 81, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en>, 26 Aralık 2021.

¹⁵⁹ Tüzük madde 6 (1)'de belirtildiği gibi, veri işlemenin diğer yasal gerekçeleri şunlardır: sözleşme, yasal yükümlülükler, veri sahibinin hayati çıkarları, kamu yararı ve meşru menfaat.

¹⁶⁰ ITGP Privacy Team, **a.g.e.**

¹⁶¹ Voigt, **a.g.e.**, s.93.

geçerli olarak kabul edilemez. Ayrıca, işletmeler, hizmetin sağlanması için özel işlem gerekli olmadıkça, hizmet sunumu için onay alınması gerektiğini şart koşmayacaktır. Örneğin, çeşitli hizmetleri tek bir pakette birleştirilmiş ve "*kabul ediyorum*" yazan bir onay kutusu sunmak kabul edilemez¹⁶².

Onayın "*spesifik*" olması gerektiği kriteri bulunmaktadır. Bu kriter, verilerin birden fazla amaç için işlendiği durumlarda geçerlidir. Konuya ait onaydan bahsedebilmek için, işleme amaçlarının her biri için veri sahibinden onay alınmalıdır. Verilen onay, veri işleme faaliyetlerini ve amaçlarını tam olarak kapsamalıdır. Farklı işleme amaçları ve faaliyetleri ayrı ayrı değerlendirilmelidir. Veri sahiplerine, bazı amaçlara onay verme ve diğerlerine onay vermeme imkanı sunulmalıdır. Diğer tüm amaçlar için yeni onay alınmalıdır ve geniş kapsamlı onaylar geçerli değildir¹⁶³. Kullanıcılar bir web sitesine tarayıcıları aracılığıyla coğrafi konum verilerine erişme izni verirse, bu, izinleri olmadan hiçbir ek bilginin toplanmaması gerektiğini gösterir¹⁶⁴. Planet 49 kararında ABAD, onayın "özellikle söz konusu verilerin işlenmesiyle ilgili olması gerektiği ve veri sahibinin başka amaçlara ilişkin isteklerinden hareketle onay verildiği sonucunun çıkarılamayacağı anlamında 'spesifik' olması gerektiğini" açıklığa kavuşturmuştur¹⁶⁵.

Üçüncüsü, veri sahibi işlemenin tüm yönleri hakkında tam olarak "*bilgilendirilmelidir*". ABAD, veri sahiplerinin "*açıkça anlaşılabilir*" ve "*yeterince ayrıntılı*" bir şekilde bilgilendirilmesi gerektiğini açıklar. Ayrıca, ABAD C-673/17 kararına göre açık ve kapsamlı bilgilendirme, veri sorumlularının veri sahiplerine veri işleme ilgili açık ve kapsamlı bilgi vererek veri sahiplerinin iyi bilgilendirilmiş olmasını ve verdikleri onayın sonuçlarını kolayca belirleyebilecek durumda olmalarını

¹⁶² Lukas Zolejnik "How to: GDPR, consent and data processing", 2 Ocak 2018, (Çevrimiçi), <https://blog.lukaszolejnik.com/how-to-gdpr-consent-data-processing/>, 28 Ocak 2022.

¹⁶³ Jakub Misek "Consent to personal data processing–The Panacea or The dead end?." , **Masaryk University Journal of Law and Technology**, C.8, S.1,2014, s.73.

¹⁶⁴ Zolejnik, a.g.e., (Çevrimiçi), <https://blog.lukaszolejnik.com/how-to-Tüzük-consent-data-processing/>, 28 Ocak 2022.

¹⁶⁵ ABAD, Planet 49, T.1 Ekim 2019, K.673/17, para 58, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=319731>, 28 Ocak 2022.

sağlayabilecekleri anlamına gelir¹⁶⁶. Kullanıcılar, işlenen verilerinin depolanmasından kimin sorumlu olduğu, kendileri hakkında hangi bilgilerin işlendiği ve bu verilerin kimlerle paylaşıldığı konusunda bilgilendirilmelidir. Ayrıca, kullanıcılar işlemenin amaçları ve onaylarını geri çekme gibi hakları ve bu hakların nasıl kullanılabileceği hakkında bilgilendirilmelidir.

Tüzük, onayın nasıl alınabileceğine dair resmi gereklilikler öngörmemektedir. Bu, onayın hem sözlü hem de yazılı olarak alınabileceği anlamına gelir. Bununla birlikte, kontrolörlerin *"ispat yükü"* olduğu için yazılı onay almaları önerilir¹⁶⁷. Madde 7, onayın yazılı bir biçimde verilmesi durumunda, onay talebinin *"açık ve sade bir dil kullanılarak, anlaşılır ve kolay erişilebilir bir biçimde"* verileceğini belirtir. Bu nedenle, gizlilik ve çerez politikalarının dili, yasal jargonla doldurulmak yerine kısa ve net olmalıdır. Onay isteklerinin kullanıcılar için anlaşılması kolay olmalıdır. Çünkü neyi kabul ettiklerini anlamazlarsa, rızalarının geçerliliği sorgulanabilir. İşletmeler hedef kitlelerini değerlendirmeli ve onay taleplerini buna göre uyarlamalıdır¹⁶⁸.

Google, şeffaflık eksikliği nedeniyle 26 Şubat 2020 tarihi itibarıyla Fransa'da önemli ölçüde para cezası aldı¹⁶⁹. Fransız Veri Koruma Kurumu CNIL'e göre, kullanıcılar Google'ın işleme kapsamını kavrayamadılar ve Google'ın gizlilik bildirimlerinde kullanılan terimler çok belirsiz ve yüzeyseldi. CNIL, belgelerde açıklanan veri işleme amaçlarının *"içerik ve reklam açısından kişiselleştirilmiş hizmetler sunmak, ürün ve hizmetlerin güvenliğini sağlamak, hizmetlerin sağlanması ve geliştirilmesi, vb."*, gerçekleştirilen işlemenin kapsamı ve bu işlemenin sonuçları göz önüne alındığında aşırı derecede yüzeysel olduğunu tespit etmiştir. Bu terimlerde kullanılan dil *"Topladığımız bilgiler, tüm kullanıcılarımıza sunulan hizmetleri geliştirmek için kullanılır. [...] Topladığımız bilgiler ve bunları nasıl kullandığımız,*

¹⁶⁶ ABAD, Planet 49, T.1 Ekim 2019, K.673/17, para 74, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=319731>, 28 Ocak 2022.

¹⁶⁷ Kontrolörün işleme için onay alması gerektiği durumlarda, veri sahibinin işlemeyi kabul ettiğini göstermelidir.

¹⁶⁸ Zolejnik, a.g.e., (Çevrimiçi), <https://blog.lukaszolejnik.com/how-to-Tüzük-consent-data-processing/>, 28 Ocak 2022.

¹⁶⁹ CNIL Restricted Committee, SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC., (Çevrimiçi), <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>, 27 Temmuz 2022.

hizmetlerimizi nasıl kullandığınıza ve gizlilik ayarlarınızı nasıl yönettiğinize bağlıdır" ifadesi çok belirsizdir¹⁷⁰.

Son olarak, geçerli onay "*açık*" olmalıdır. Tüzük, veri sahiplerinin geçerli onaylarını bir beyan veya olumlu hareketle ifade etmelerini gerektirir. Bu nedenle, geçerli bir onay, olumlu bir hareket veya beyan yoluyla alınmalıdır. Veri sahibinin belirli bir işlemeyi anladığı ve onayladığı açık olmalıdır¹⁷¹. Sonuç olarak, Tüzük kapsamında bir devre dışı bırakma modeline izin verilmez. Tüzük ayrıca, "*sessizlik, önceden işaretlenmiş kutular veya hareketsizlik*" in açık izin olarak yorumlanmaması gerektiğini açıkça belirtmektedir: Bunlar geçerli bir onay için yetersizdir¹⁷². ABAD, "*veri sahibinin onayı, veri sahibinin onayını 'açık bir şekilde' vermiş olması koşuluyla bu tür bir işlemeyi yasal hale getirebilir. Yalnızca veri sahibinin onayını vermek amacıyla aktif davranışı bu gerekliliği yerine getirebilir*"¹⁷³."

Veri kontrolörleri, ispat yükünü taşıdıkları için veri sahibinin olumlu onay verdiğini ispat edebilmelidir. Bu ispat, veri kontrolörleri için zor olabilir. Bu, çevrimiçi onay alındığında alakalı hale gelir, çünkü Tüzük bunun nasıl gerçekleştirilmesi gerektiğini belirtmez. Literatürde, kontrolörler için çift aşamalı bir prosedür önerilmektedir. Çift aşamalı bir prosedür şu şekilde çalışır. İlk başta veri sahibinin, e-posta adreslerine girmeleri ve çevrimiçi bir form doldurarak onaylarını beyan etmeleri istenecek. İkinci olarak veri sahibi, onay verme işlemi tamamlamak için tıklamaları gereken özelleştirilmiş bir köprü içeren bir doğrulama e-postası alacaktır. Doğrulama e-postası, üçüncü bir tarafın veri sahibinin e-posta adresini kötüye kullanmasını önlediğinden, kontrolör onayın alındığını ve veri sahibinin bu izni verdiğini gösterebilir¹⁷⁴.

¹⁷⁰ CNIL Restricted Committee, SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC., s.16, para. 112, (Çevrimiçi), <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>, 27 Temmuz 2022.

¹⁷¹ Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 28 Kasım 2017 s.17, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, 28 Ocak 2022.

¹⁷² Tüzük gerekçe madde 32.

¹⁷³ ABAD, Planet 49, T.1 Ekim 2019, K.673/17, para 54, (Çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=319731>, 28 Ocak 2022.

¹⁷⁴ Voigt, a.g.e., s.93.

Bir sözleşmenin yerine getirilmesi için bir koşul olarak onay kesinlikle yasaktır. Bu maddenin tam kapsamı hala bilinmemektedir. Bu, kişisel verilerin sunulması karşılığında verilen çevrimiçi hizmetleri önemli ölçüde etkileyecektir. Kanunkoyucular, kişileri son yıllarda işletmeler için kazançlı bir hale gelen kişisel verilerinin kötüye kullanılmasından korumak istiyor gibi görünmektedir¹⁷⁵. Bu nedenle, işletmeler "gereksiz" verilerin toplanmasını en aza indirmelilerdir. Çünkü madde 7 (4) 'ün ihlali halinde, madde 83 (5) 'te öngörülen para cezaları ile cezalandırılabilirler.

Özel kişisel veri kategorileri yasal olarak yalnızca bazı durumda¹⁷⁶ işlenebilir. Veri kontrolörü, aşağıdaki durumlarda veri sahibini bilgilendirmeli ve veri sahibinden açık onay almalıdır:

- 1) veri sahipleriyle ilgili hassas verileri işlerken;
- 2) otomatik bireysel karar verme halinde¹⁷⁷;
- 3) verileri üçüncü ülkelere aktarırken, yeterli ve uygun önlemler yoksa¹⁷⁸.

Reşit olmayanların onayı, bilgi toplumu hizmetleri alanında farklılık gösteren bir meseledir. 16 yaşın altındaki kişiler için ebeveynlerinden ekstra bir onay veya izin alınması gerekmektedir. Yaş kısıtlaması esneklik sağlanmasına tabidir. Üye Ülkeler, 13 yaşın altına düşmemesi koşuluyla daha düşük bir yaşı geçerli sayabilirler. Sağlanan hizmet açıkça reşit olmayanlara yönelik değilse, bu hüküm geçerli değildir. Oysa verilen hizmet hem yetişkinlere hem de küçüklere yönelikse, bu hüküm geçerli hale gelir¹⁷⁹.

Tüzüğün 7 (3) maddesi, kontrolörün, onayın veri sahibi tarafından verildiği kadar kolay bir şekilde ve kişisel verilerin işlenmesi süresince herhangi bir noktada geri çekilebileceğini garanti edeceğini öngörmektedir. Onayın geri çekilmesi, onay vermek kadar basit olmalıdır. Tüzük, onay vermenin ve geri çekmenin aynı kanallardan yapılmasını şart koşmaz. Bu, veri sahiplerinin onaylarını bir tıklama veya kaydırma yoluyla elektronik olarak vermeleri durumunda, onaylarını aynı kolaylıkla geri

¹⁷⁵ Voigt, **a.g.e.**, s.96.

¹⁷⁶ Tüzük madde 9.

¹⁷⁷ Tüzük madde 22.

¹⁷⁸ Tüzük madde 49.

¹⁷⁹ Tüzük madde 8.

çekebilmeleri gerektiği anlamına gelir. Hiç şüphe yok ki, veri kontrolörleri onay almak ve geri çekmek için aynı arayüzleri kullanmalıdır. Yalnızca onayı geri çekmek amacıyla başka bir arayüze geçmek, veri sahipleri için aşırı derecede uğraştırıcı olacaktır¹⁸⁰. Örneğin, veri kontrolörleri, e-posta, telefon görüşmesi veya iyi gizlenmiş bir alt sayfa gerektiren onayın geri çekilmesi için onay almak için iyi tasarlanmış bir çevrimiçi form kullanmamalıdır¹⁸¹.

Ek olarak, veri sahibi, onaylarını geri çektiklerinde kontrolör tarafından herhangi bir zarara uğratılmamalıdır. Bu kontrolörün, veri sahibinin onayını ücretsiz olarak geri çekmesi veya sağlanan hizmetin kalitesini düşürmesi gerektiği anlamına gelir. Onay geri çekildiğinde, geri çekilmeden önce gerçekleşen onaya dayanan tüm veri işleme işlemleri yasal kalır; Bununla birlikte, kontrolör söz konusu işlemekte olduğu faaliyetlerini durdurmalıdır. Verileri işlemek için başka bir yasal dayanak yoksa, kontrolör verileri imha etmelidir¹⁸².

Teoride, bildirim ve onay oldukça uygun bir seçenek gibi görünmektedir, ancak işleyişte bazı zorlukları vardır. Bir yandan, bildirim ve onay çerçevesi, veri sahiplerinin özel verileri hakkında özgür, bilinçli kararlar almalarını sağlar. Öte yandan, herhangi birinin bilgiyi ifşa etmenin maliyetlerini ve avantajlarını göz önünde bulundurması, verilerinin gelecekte nasıl kullanılabileceğini anlamadan işlenmesine izin vermesi işleyiş olarak zordur¹⁸³. Bir soru, veri kontrolörlerinin veri sahiplerini veri işleme faaliyetleri hakkında ne ölçüde bilgilendirebileceğidir. Çünkü bazı veri işleme sistemleri o kadar karmaşıktır ki, yalnızca küçük bir uzman grubu bunu anlayabilir¹⁸⁴.

Tüzük tüketici gizliliğini korumayı amaçlasa da, kişiler hala şirketlerin veri işleme faaliyetlerine izin vermeye zorlanmaktadır. Facebook gibi online şirketler, hizmetlerini kullanmak için veri sahiplerinin gizlilik kurallarına izin vermelerini

¹⁸⁰ Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 28 Kasım 2017 s.21, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, 28 Ocak 2022.

¹⁸¹ Zolejnik, **a.g.e.**, (Çevrimiçi), <https://blog.lukaszolejnik.com/how-to-Tüzük-consent-data-processing/>, 28 Ocak 2022.

¹⁸² Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 28 Kasım 2017 s.22, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, 28 Ocak 2022.

¹⁸³ Daniel Solove "Privacy self-management and the consent dilemma.", **Harvard Law Review**, C.126, S.7,2013, s.1881.

¹⁸⁴ Nissenbaum, **a.g.e.**, s.35.

gerektirir. Örneğin, Facebook kullanıcıları sosyalleşme karşılığında veri sunar. Bu şirketlerin hizmetlerini kullanan bireyler, veri ifşasını ücretsiz hizmetler karşılığında yaptıkları anlaşmanın bir parçası olarak görürler¹⁸⁵.

Kayıt olurken Facebook'a verilen onay Tüzükle uyumlu olarak kabul edilebilir mi? Her şeyden önce, kayıt sayfası büyük alanlarla iyi tasarlanmışken, gizlilik terimleri çerez politikaları dikkat çekmeyen kadar küçük olarak görüntülenir. Facebook'un onay çerçevesine yaklaşımı ya hep ya hiçtir. Bireylerin çeşitli amaçlar için toplu onay vermeleri gerekmektedir. Bu nedenle, bir kullanıcı Facebook'un bir veri işleme amacına rıza gösterip de diğer veri işleme amacını rededemiyor. Yukarıda açıklandığı gibi, Tüzük bireylerden her amaç için olumlu onay talep eder. Facebook'a kaydolma eylemi, olumlu onay almak için yeterli görülmecektir¹⁸⁶.

2.3. Veri Güvenliği

Tüzüğün "veri bütünlüğü ve gizliliği" ilkesine ilişkin 5(1)(f) maddesi, geniş veri güvenliği kavramı ile ilgilidir. Veri güvenliği, şirketlerin kişisel verilerin yanlışlıkla veya kötü niyetli olarak tehlikeye atılmasını önlemek için yeterli güvenliğe sahip olması gerektiği anlamına gelir. Veri güvenliği sadece siber güvenlik önlemlerini değil, aynı zamanda iç organizasyonel güvenlik önlemlerini de gerektirir¹⁸⁷.

Veri kontrolörleri ve işleyiciler, işlenen verilerin güvenliğinden sorumludur ve yeterli güvenlik önlemlerini almalıdır.

1995 Direktifi, neyin yeterli bir güvenlik önlemi oluşturduğunu değerlendirmeyi kontrolöre bırakırken, Tüzük daha kuralcı bir yaklaşım benimsemektedir. Tüzük, madde 32 olası veri koruma önlemlerinin bir listesini içerir¹⁸⁸.

¹⁸⁵ Ahmed Javed et. al. "GDPR compliant consent driven data protection in online social networks: A blockchain-based approach", **3rd International Conference on Information and Computer Technologies (ICICT)**, 2020, s.310.

¹⁸⁶ A.e., s.310-311.

¹⁸⁷ Information Commissioner's Office, Security, (Çevrimiçi), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>, 29 Aralık 2021.

¹⁸⁸ Houser, a.g.e., s.90.

Bu maddeye göre veri güvenliği önlemleri aşağıdakileri içerir ancak yalnızca bunlarla sınırlı değildir¹⁸⁹:

- Takma ad verme ve kişisel verilerin şifrelenmesi
- İşleme sistemlerinin ve hizmetlerinin gizliliğini, bütünlüğünü, kullanılabilirliğini ve esnekliğini sürekli olarak sürdürmek
- Veri kaybı durumunda, kullanılabilirliği ve kişisel verilere erişimi zamanında geri yüklemek
- Güvenlik önlemlerinin etkinliğinin test edilmesi, ölçülmesi ve değerlendirilmesi.

Tüzük, veri güvenliği önlemleriyle ilgili risk tabanlı bir yaklaşım benimser. Madde 32 (2)'nin belirttiği gibi, veri işleme faaliyetini hayata geçiren işletmeler tarafından *"uygun güvenlik seviyesinin değerlendirilmesinde, özellikle iletilen, saklanan veya başka bir şekilde işlenen kişisel verilerin kazara veya yasa dışı imhası, kaybı, değiştirilmesi, yetkisiz ifşası veya erişiminden kaynaklanan işleme yoluyla ortaya çıkan riskler özellikle dikkate alınacaktır."* Bu da şirketlerin güvenlik önlemlerini belirlemeden önce veri riskini analiz etmeleri gerektiği anlamına gelmektedir. Gerekçe madde 76'ya göre: *"Risk, veri işleme operasyonlarının basit bir risk mi yoksa yüksek risk mi içerdiğinin belirlendiği objektif bir değerlendirme temelinde değerlendirilmelidir"*. Uygun güvenlik önlemleri derecesini belirlemek için objektif bir risk değerlendirmesi kullanılmalıdır. Risk analizi üç farklı grup çerçevesinde gerçekleştirilebilir : veri sahiplerinin hesaplarına, meşru menfaatlerine yönelik riskler; veri kontrolörleri ve işlemcileri için riskler; üçüncü taraflarca veya veri kontrolörleri ve işlemciler tarafından dayatılan riskler¹⁹⁰.

Gerekçe madde 75, veri sahiplerinin hak ve özgürlüklerine yönelik risklerin bir listesini verir: ayrımcılık , kimlik hırsızlığı veya sahtekarlık, finansal kayıp, itibar kaybı veya diğer büyük ekonomik veya sosyal zararlar; veri sahiplerinin hak ve özgürlüklerinden mahrum bırakılma veya kişisel verileri üzerinde kontrol sahibi olmalarının engellenmesi; verilerin işlenmesi kişinin ırk veya etnik kökeni, siyasi

¹⁸⁹ Tüzük madde 32(1).

¹⁹⁰ Voigt, **a.g.e.**, s.40.

düşüncesi, din veya felsefi inancı, sendika üyeliğini ve genetik verilerini, sağlıkla ilgili veriler veya cinsel hayatına ilişkin verileri veya ceza mahkumiyetleri ve suçlarının ortaya çıkmasına neden olması; kişisel profiller oluşturmak veya kullanmak amacıyla, veri sahibinin kişisel hususlarının özellikle işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri veya ilgi alanları, güvenilirliği veya davranışı, konumu ile ilgili hususların analiz edilmesi veya tahmin edilmesi; özellikle çocuklar olmak üzere savunmasız gerçek kişilerin kişisel verilerinin işlendiği veya işlemenin büyük miktarda kişisel veri içerdiği ve çok sayıda veri sahibini etkilemesi.

Bununla birlikte, risk değerlendirmesi sadece veri sahiplerinin çıkarlarından daha fazlasını içermelidir. Devlet müdahalesi gibi üçüncü taraf riskleri de değerlendirilebilir. Veri kontrolörleri ve işlemcilerle yönelik riskler de ele alınmalıdır.

Kontrolörlerin ve işleyicilerin karşılaştığı riskler sıklıkla veri sahiplerinin karşılaştığı risklerle örtüşür. Örneğin; 1) para cezaları ve cezalar gibi veri koruma yükümlülüklerine uyulmamasından kaynaklanan yasal riskler; 2) veri gizliliği yönetim sistemlerinin iyileştirilmesiyle ilgili hasar talepleri ve maliyetler gibi finansal riskler; 3) iş hedeflerine ulaşılamaması gibi iş riskleri, işletmenin itibarı ile ilişkili riskler¹⁹¹.

Madde 32 (3), şirketlerin veri güvenliği gerekliliklerine uygunluğu, “*madde 40'ta kabul edilmiş olan davranış kurallarına veya madde 42'de kabul edilmiş olan bir sertifikasyon mekanizmasına*” bağlı olduklarını ortaya koymak suretiyle kanıtlayabileceklerini ifade etmektedir.

Madde 32(4) şöyle der: “*Kontrolör ve işleyici, kontrolörün veya kişisel verilere erişimi olan işleyicinin yetkisi altında hareket eden herhangi bir gerçek kişinin, Birlik veya Üye Ülke yasaları tarafından zorunlu kılınmadıkça, kontrolörlerin talimatları dışında bunları işlememesini sağlamak için adımlar atacaktır*”.

Yukarıda belirtildiği gibi, şirketlerin ayrıca tüm personelin veri güvenliği ve veri koruma yasaları kapsamındaki gizlilik sorumlulukları konusunda sık sık eğitilmesi, veri işleme alanlarında, özellikle kişisel verileri üçüncü taraflara veya veri sahiplerine

¹⁹¹ Voigt, a.g.e., s.41.

işleme veya ifşa etme seçimlerinde rollerin ve yetkinliklerin tanımlanması gibi işletme içi önlemler almaları gerekir¹⁹².

2.5. Tasarlanan ve Varsayılan olarak Gizlilik

Tüzüğün 25. maddesi, veri gizliliğini işletmelerin operasyonel faaliyetlerine entegre etmek ve veri korumasının artık ikincil bir husus olmadığını garanti etmek amacıyla, tasarlanan ve varsayılan olarak adlandırılan iki karmaşık ilke içermektedir¹⁹³. Tasarlanan ve varsayılan olarak gizliliğin bazı özellikleri Direktifte bulunabilse de, bu kavramlar AB düzeyinde veri koruması için nispeten yenidir. Tüzüğün 25. maddesinin Direktifte birebir karşılığı bulunmamaktadır¹⁹⁴.

Tasarım gereği gizlilik, işletmelerin tasarımın ilk aşamalarında ve kişisel verileri içeren yeni mallar, süreçler veya hizmetler geliştirme sürecinin tamamı boyunca gizlilik yasasına uygun olarak uygun teknik ve organizasyonel önlemleri uygulamayı düşünmelerini gerektirir¹⁹⁵. İşletmeler, hangi teknolojik ve organizasyonel önlemlerin uygun olduğunu belirlerken aşağıdaki faktörleri göz önünde bulundurmalıdır:

- teknik;
- uygulama maliyeti;
- işlemenin niteliği, kapsamı, bağlam ve amaçları;

¹⁹² Giakoumopoulos, **a.g.e.**, s.167.

¹⁹³ A&L Goodbody, The GDPR: A Guide for Businesses, 5 Ekim 2016, s.24, (Çevrimiçi), https://www.algoodbody.com/media/The_GDPR-AGuideforBusinesses1.pdf, 28 Ocak 2022.

¹⁹⁴ Lee A. Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements." **Oslo Law Review**, C.4, S. 2, 2017, s.108.

¹⁹⁵ Shay Dannon, GDPR Top Ten: #6 Privacy by Design and by default , 10 Şubat 2017, (Çevrimiçi), <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-top-ten-6-privacy-by-design-and-by-default.html>, 11 Şubat 2022.

-işlemenin kişilerin haklarına yönelik riskleri¹⁹⁶.

Takma ad, veri güvenliği göz önünde bulundurularak işlemenin tasarlanmasının bir örneğidir. Gerekçe madde 78, "takma ad" da dahil olmak üzere tasarlanan olarak gizliliği sağlamak için diğer uygun önlemlerin listesini verir. Aynı zamanda, madde 25 (1), veri koruma ilkelerini uygulamak için uygun önlemlerin amaçlanmasını gerektirir ve bu, örnek olarak "veri minimizasyonu" ilkesinden bahsedilerek doğrulanır. 25. maddede tanımlanan yükümlülükler, 35. maddede belirtilen etki değerlendirmesi¹⁹⁷ yapma yükümlülüğü ile yakından bağlantılıdır. Bununla birlikte, etki değerlendirmeleri, işlemenin "gerçek kişilerin hak ve özgürlükleri için yüksek bir riskle sonuçlanması muhtemel" olduğunda yapılmalıdır. 25. maddede belirtilen yükümlülükler için böyle bir gereklilik yoktur¹⁹⁸.

İşletmeler, "varsayılan olarak, yalnızca işlemenin her bir özel amacı için gerekli olan kişisel verilerin işlenmesini" sağlamak için uygun önlemleri uygulamalıdır¹⁹⁹. Bu, veri sahiplerine verilerinin ne kadarının başkalarıyla paylaşılabilirliğini seçme seçeneği sunulduğunda, varsayılanın her zaman en gizlilik dostu olacak şekilde ayarlanması gerektiği anlamına gelir²⁰⁰.

Varsayılan olarak gizlilik yükümlülüğü aşağıdakiler için geçerlidir:

- toplanan kişisel verilerin kapsamı;
- toplanan verilerin işlenmesinin kapsamı;
- saklama süresi ve erişilebilirlik²⁰¹.

Madde 42 uyarınca onaylanmış bir belgelendirme yöntemi, tasarım gereği gizlilik standartlarına ve varsayılan olarak gizlilik standartlarına uygunluğu göstermek için bir bileşen olarak kullanılabilir²⁰².

¹⁹⁶ Tüzük madde 25.

¹⁹⁷ Konuya ilişkin açıklama için bkz. Üçüncü Bölüm,3.1 Etki Değerlendirmeleri.

¹⁹⁸ Bygrave, a.g.e, s.115.

¹⁹⁹ Tüzük madde 25.

²⁰⁰ Shay Dannon, GDPR Top Ten: #6 Privacy by Design and by default , 10 Şubat 2017, (Çevrimiçi), <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-top-ten-6-privacy-by-design-and-by-default.html>, 11 Şubat 2022.

²⁰¹ Tüzük madde 25(2).

²⁰² Tüzük madde 25(3).

Tüzük, gizliliği tasarlanan ve varsayılan olarak zorunlu hale getirerek, bireylere verileri üzerinde daha fazla kontrol sunmayı amaçlamaktadır. Varsayılan olarak, veri sahiplerine en gizlilik dostu seçeneği sunmak, verileri üzerinde gerçek kontrol sahibi olmalarını sağlar. Gizliliği etkili bir şekilde uygulamanın tek yolu, veri sahibini tasarlama yoluyla gizliliği geliştirme sürecine dahil etmektir. Sonuç olarak, bu yaklaşımlar işletmelerin verimliliği artırmalarını sağlarken aynı zamanda veri sahiplerinin güvenini kazanmalarını sağlar²⁰³.

2.6. Veri İhlalleri

İlk kez, Tüzükde Avrupa çapında bir veri ihlali bildirim yükümlülüğü getirildi. Direktif, şu anda Tüzüğün gerektirdiği gibi veri koruma makamlarının bir ihlalden haberdar edilmesini zorunlu kılmamıştır²⁰⁴. Bu kapsamda, veri ihlali *"iletilen, saklanan veya başka bir şekilde işlenen kişisel verilerin kazara veya yasa dışı imhasına, kaybına, değiştirilmesine, yetkisiz olarak ifşa edilmesine veya bunlara erişilmesine yol açan bir güvenlik ihlali"* anlamına gelir²⁰⁵.

Tüzüğe göre, veri ihlalleri gerçekleştiğinde veri koruma makamlarına "çok gecikme olmadan, en geç 72 saat içinde"²⁰⁶ bilgi verilmelidir. İşletmeler, veri sahiplerinin hak ve özgürlüklerini riske atma olasılığı yüksek olan veri ihlallerini bildirmelidir. Veri ihlali bildirimini 72 saatten daha geç bir süre içinde veri koruma

²⁰³ Shay Dannon, GDPR Top Ten: #6 Privacy by Design and by default , 10 Şubat 2017, (Çevrimiçi), <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-top-ten-6-privacy-by-design-and-by-default.html>, 11 Şubat 2022.

²⁰⁴ Houser, **a.g.e.**, s.59.

²⁰⁵ Tüzük Madde 4(12).

²⁰⁶ Tüzük Madde 33(1).

yetkilisine sunulduğunda, gecikmenin nedeni de bildirilmelidir²⁰⁷. Zorunlu bildirim şunları içermelidir:

- İhlalin niteliği, veri kategorileri, etkilenen bireylerin tahmini sayısı ve kişisel veri kayıtları;
- Veri koruma görevlisinin veya diğer temsilcilerin adı ve iletişim bilgileri;
- Kişisel veri ihlalinin olası sonuçlarının açıklanması;
- Herhangi bir olumsuz sonucu sınırlamaya yönelik eylemler de dahil olmak üzere, kontrolörün kişisel veri ihlaline verdiği yanıtın detayları²⁰⁸.

Veri kontrolörü, hak ve özgürlükleri açısından yüksek risk oluşturabilecek veri ihlallerini "*çok gecikme olmaksızın*" veri sahiplerine bildirmelidir²⁰⁹. Bu bildirimde kişisel veri ihlalinin niteliği açık ve sade bir dille açıklanmalıdır. Bu bildirim, veri yetkilisine yapılan bildirimin içerdiği bilgilere benzer bilgiler içerecektir²¹⁰. Bazı durumlarda veri kontrolörünün veri sahibine bildirimde bulunma yükümlülüğü bulunmamaktadır. Örneğin, veri kontrolörü, şifreleme gibi uygun teknik ve organizasyonel koruma önlemlerini almış ve bu önlemleri kişisel veri ihlalden etkilenen kişisel verilere uygulamışsa, bildirimde bulunma yükümlülüğü altında değildir²¹¹. Veri kontrolörü, ihalden sonra meydana gelen yüksek risk olasılığını azaltmak için önlemler almışsa bildirim gerekmecektir²¹². Bildirim orantısız bir çaba gerektiriyorsa, veri sahibi ihlal hakkında eşit derecede etkili farklı yollarla, örneğin kamuya açık bir bildirim veya benzer önlemlerle bilgilendirilebilir²¹³.

Bir veri ihlalinin bildirilmemesi, dünya çapındaki cironun %4'üne veya 20.000.000 EUR'ya kadar yaptırımlarla sonuçlanır. Uber, Hollanda Veri Koruma Kurumu (DPA) tarafından tüketicilere ve sürücülere ait isimlere, e-posta adreslerine

²⁰⁷Tüzük Madde 33(1).

²⁰⁸ Tüzük Madde 33(3).

²⁰⁹ Tüzük madde 34(1).

²¹⁰ Tüzük madde 34(2).

²¹¹ Tüzük madde 34(3)(a).

²¹² Tüzük madde 34(3)(b).

²¹³ Tüzük madde 34(3)(c).

ve telefon numaralarına yetkisiz erişimle sonuçlanan bir veri ihlali 72 saat içinde bildirmediği için 28 Şubat 2020 itibarıyla 600.000 Euro para cezası aldı²¹⁴.

Kontrolörlerin, tüketici için tehlike oluşturan veri ihlalinin haberdar olduklarında bilgi vermeleri beklenir. Veri ihlali küçük olsa bile, şirket kayıtları dahil olarak korumalıdır²¹⁵. Veri işlemcileri biraz daha fazla hareket alanına sahiptir - kontrolörleri 'çok gecikme olmadan' bilgilendirmelidirler²¹⁶.

72 saatlik kural, iyileştirme tamamlanana kadar ihlali gizli tutmak isteyen işletmeler için zorlayıcı olacak ve belki de suçlunun bulunmasıyla sonuçlanacaktır. Veri ihlali halka açık hale getirmek, şüphesiz suçluyu bilgilendirecek ve sonuç olarak sessiz kalabilecektir²¹⁷. Ayrıca, 72 saatlik süre, şirketin veri sahiplerinin sonuçlarını doğru bir şekilde değerlendirmesi için yetersiz görünebilir. Sonuç olarak, işletmelerin bir veri ihlalinin bir bildirim zorunluluğu doğurma ihtimalinin yüksek olup olmadığını belirlemek için bir sisteme sahip olmaları gerekir.

3. Genel Veri Koruma Tüzüğü'ne Uygunluğun Sağlanması

3.1. Etki Değerlendirmeleri

Teknoloji sürekli geliştiğinden ve veri işleme daha karmaşık hale geldiğinden, işleme faaliyetleri veri sahiplerinin hak ve özgürlükleri için risk oluşturmaktadır. Bu nedenle, işletmeler bu riskleri, planlanan işleme faaliyetlerine başlamadan önce öngörülen etkisini belirleyerek ele almalıdır. Bu, işletmelerin riskleri önceden etkili

²¹⁴ Dutch DPA: fine for data breach Uber, Autoriteit Persoonsgegevens, 27 Kasım 2018, (Çevrimiçi), <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber>, 12 Şubat 2022.

²¹⁵ Tüzük madde 33(5).

²¹⁶ Tüzük madde 33(2), Ralph O'Brien "Privacy and security: The new European data protection regulation and it's data breach notification requirements.", **Business Information Review**, C. 33, S. 2, 2016, s.82.

²¹⁷ Houser, **a.g.e.**, s.61.

bir şekilde tanımlamasına, değerlendirmesine ve azaltmasına olanak tanıyarak, işleme nedeniyle veri sahipleri üzerinde olumsuz bir etki olasılığını önemli ölçüde azaltır²¹⁸.

İşletmelerin veri işlemlerinin veri sahipleri üzerindeki etkisini değerlendirmelerine yardımcı olmak için, Tüzüğün 35. maddesi, bir veri koruma etki değerlendirmesinin gerçekleştirilmesini zorunlu kılar. Etki değerlendirmesi, bir şirketin belirli bir teknolojiyi veya sistemi kullanması nedeniyle var olan riskleri tanımlamak ve analiz etmek için kullanılan bir araçtır. Riskleri azaltmak için ilgili öneriler, değerlendirme sonuçlarına göre seçilmeli ve yürütülmelidir²¹⁹.

Bununla birlikte, etki değerlendirmeleri, işlemenin *"gerçek kişilerin hak ve özgürlükleri için yüksek bir riskle sonuçlanması muhtemel"* olduğunda yapılmalıdır²²⁰. Tüzük, yüksek risk olasılığının nasıl değerlendirileceğini belirtmez; Bunun yerine, Gerekçe madde 73 ne tür risklerin olabileceğini belirtmektedir. Madde 35, etki değerlendirmesinin özellikle gerekli olduğu yüksek riskli işleme faaliyetlerinin bir listesini içerir:

- Profil oluşturma da dahil olmak üzere otomatik işlemeye dayanan ve gerçek kişi hakkında hukuki etkiler yaratan veya benzer şekilde gerçek kişiyi önemli ölçüde etkileyen kararların dayandığı gerçek kişilerle ilgili kişisel yönlerin sistematik ve kapsamlı bir değerlendirmesi;
- Özel kategorilerdeki verilerin veya cezai hükümler ve suçlarla ilgili kişisel verilerin büyük ölçekte işlenmesi;
- Kamuya açık bir alanın büyük ölçekte sistematik olarak izlenmesi²²¹.

Denetim makamları, etki değerlendirmesi gerektiren işleme faaliyetlerinin bir listesini geliştirecek ve yayınlayacaktır. Ek olarak, bu gereksinimden muaf tutulan işleme süreçlerinin bir listesini geliştirebilirler²²².

²¹⁸ Giakoumopoulos, **a.g.e.**, s.179.

²¹⁹ Felix Bieker et. al. "A process for data protection impact assessment under the European general data protection regulation." **In Annual Privacy Forum**, Springer, Cham, 2016, s.22.

²²⁰ Tüzük madde 35(1).

²²¹ Tüzük madde 35(3).

²²² Tüzük madde 35(4),35(5).

Etki deęerlendirmeleri ve genel olarak risk ynetimi arasında bir ayrım yapılmalıdır. Her ikisinin de ortak bir risk deęerlendirmesi vardır, iřletmeler olası bir yksek risk olup olmadığını belirlemelidir. Etki deęerlendirmeleri veri sahipleri iin riskleri ele alırken, genel risk ynetimi iřletmeleri ve faaliyetleri ele alır. Bu ayrım, ikincisi altındaki bazı risk durumları haklı gsterilebilse de, veri sahiplerine ynelik riskler ve verilerini kiřisel alana izinsiz girme konusunda hibir gereke bulunmadığı anlamına gelir²²³.

Madde 29 alıřma Grubu, etki deęerlendirmeleri ve iřlemenin yksek risk oluřturup oluřturmadığına nasıl karar verileceğı konusunda kılavuzlar yayınladı. Belirli bir durum iin bir veri koruma etki deęerlendirmesinin gerekli olup olmadığına karar vermede yardımcı olmak iin ařağıdaki dokuz faktr ortaya ıkmıřtır: profil oluřturma ve tahmin etme dahil olmak zere deęerlendirme veya puanlama; yasal veya benzer nemli bir etkiye sahip otomatik karar verme; sistematik izleme; hassas veriler; byk lekte iřlenen veriler; veri kmelerini eřleřtirme veya birleřtirme; savunmasız veri sahipleriyle ilgili veriler; teknolojik veya ngrlebilir verilerin yeniliki kullanımı veya uygulanması rgtsel czmler; ve iřlemenin *"veri sahiplerinin bir hakkı kullanması veya bir hizmeti veya szleřmeyi kullanmasını engellenmesi"*²²⁴. Bir iřleme faaliyeti bu faktrlerden yalnızca birini karřılıyorsa, etki deęerlendirmesi gerekli deęildir. Bununla birlikte, birok faktr varsa, bir etki deęerlendirmesi yapılmalıdır²²⁵. Madde 29 alıřma Grubu, *"veri kontrolrlerinin veri koruma mevzuatına uymalarına yardımcı olmak iin yararlı bir ara"* olduėu iin gerekli olup olmadığından emin olunmadığında bir etki deęerlendirmesi yapılmasını nermektedir. Yeni bir veri iřleme teknolojisi uygulandığında veri koruma etki deęerlendirmesi yapmak ok nemlidir.²²⁶

Etki deęerlendirmeleri belgelenmeli ve ek olarak veri koruma kurumlarının standartlarına uymalıdır. Madde 35(7), etki deęerlendirmesi ieriğı asgari standartları

²²³ Bieker, **a.g.e.**, s.24.

²²⁴ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Kasım 2017, s.10-11,(evrimii), https://ec.europa.eu/newsroom/document.cfm?doc_id=44137, 10.02.2022.

²²⁵ **A.e.**, s.11.

²²⁶ **A.e.**, s.9.

ortaya koymaktadır: öngörülen işleme faaliyetlerinin tanımı, işlemenin amaçları ve işleme faaliyetlerinin gerekliliğinin ve amaçlarla orantılılığının değerlendirilmesi; veri sahiplerinin hak ve özgürlüklerine yönelik risklerin değerlendirilmesi, risklerin ele alınması için öngörülen önlemler.

3.2. Veri Koruma Görevlisi

Veri Koruma Görevlileri (DPO-Data Protection Officer), veri koruma yasalarına uygunluğun sağlanması konusunda verileri işleyen kuruluşlara tavsiyelerde bulunur. Uyumluluğu kolaylaştırarak hesap verebilirliğin temel taşı olarak hizmet ederken, aynı zamanda yetkili makamlar, veri sahipleri ve onları seçen işletme arasında irtibat kurarlar²²⁷.

Madde 37(1) uyarınca, aşağıdaki koşullar altında, kontrolörlerin ve işleyicilerin veri koruma görevlisini belirlemeleri gerekmektedir:

- işleme faaliyetinin, yargısal işlevlerini yerine getiren mahkemeler hariç olmak üzere, bir kamu makamı veya organı tarafından gerçekleştirilmesi;
- kontrolör veya işleyicinin temel faaliyetlerinin niteliği, kapsamı ve/veya amaçları itibarıyla veri sahiplerinin büyük ölçekte düzenli ve sistematik bir şekilde izlenmesini gerektiren işleme faaliyetlerinden oluşması;
- kontrolörün veya veri işleyicinin temel faaliyetlerinin 9. madde uyarınca özel kategorilerdeki verilerin ve 10. maddede atıfta bulunulan cezai mahkumiyetlere ve suçlara ilişkin kişisel verilerin büyük ölçekte işlenmesinden oluşması durumunda.

Tüzük, "*büyük ölçekli*" veri işlemenin ne anlama geldiği konusunda ayrıntılı bilgi vermemektedir. "Veri Koruma Görevlileri Hakkında Kılavuzlar" da, Madde 29 Çalışma Grubu özellikle işleme faaliyetlerinin büyük ölçekte yürütülüp yürütülmediğini belirlerken aşağıdaki konularda değerlendirilmesini tavsiye eder: ilgili veri sahiplerinin sayısı, kayıt sayısı (veri kümelerinin hacmi), işlemenin kalıcılığı, işlemenin bölgesel kapsamı. Gerekçe madde 97 ayrıca, bir kontrolörün temel faaliyetlerinin ana faaliyetler ile sınırlı olduğunu ve kişisel verilerin yardımcı bir faaliyet olarak işlenmesini içermediğini açıklamaktadır. "*Temel faaliyetler*",

²²⁷ Giakoumopoulos, a.g.e., s.175.

kontrolörlerin ve işleyicilerin hedeflerine ulaşmak için ihtiyaç duydukları temel işlemler olarak düşünülebilir. Temel faaliyetler, veri işlemenin kontrolörün veya işleyicinin faaliyetinin temel bir parçası olan faaliyetleri hariç tutacak şekilde ele alınmamalıdır²²⁸. Bir işletme, kişisel verileri işlemekten hizmetlerini sağlayamıyorsa, veri işleme, işletmenin temel faaliyetlerinden biri olarak kabul edilmelidir ve bu nedenle bir veri koruma görevlisinin belirlenmesi zorunludur.

Madde 29 Çalışma Grubuna göre, aşağıdakilerden biri veya daha fazlası "*düzenli*" veri işleme olarak kabul edilebilir: belirli bir süre boyunca belirli aralıklarla devam eden veya gerçekleştirilen veri işleme faaliyetleri, yinelenen veya belirli zamanlarda tekrarlanan veri işleme faaliyetleri, sürekli veya periyodik olarak gerçekleşen veri işleme faaliyetleri. Madde 29 Çalışma Grubuna göre, aşağıdakilerden biri veya daha fazlası 'sistematik' veri işleme anlamına gelmektedir:

- Bir düzen uyarınca gerçekleştirilen veri işleme faaliyetleri;
- Önceden düzenlenmiş, organize edilmiş veya metodik veri işleme faaliyetleri;
- Veri toplama için genel bir planın parçası olarak gerçekleştirilen veri işleme faaliyetleri;
- Bir stratejinin parçası olarak yürütülen veri işleme faaliyetleri²²⁹.

Daha önceki bir Tüzük taslağı, bu yükümlülüğü 250'den fazla çalışanı olan işletmelerle sınırlandırdı. Bu nedenle, Tüzüğün kendisi, bu tür bir gerekliliğin birincil faaliyet olarak büyük ölçekli işleme gerçekleştiren tüm işletmeler için geçerli olması da dahil olmak üzere nitel değerlendirmeyi tercih etmektedir.

Tüzük, veri koruma görevlilerinin bağımsız olarak çalışmasını sağlamak için çeşitli temel önlemler sunar. Veri koruma görevlileri, personel üyelerinden seçilebilir veya çalışmaları hizmet sözleşmelerine dayanan profesyoneller olabilir. Kontrolörler veya işlemciler, atamadan sonra veri koruma görevlisinin iletişim bilgilerini yayınlamalıdır²³⁰. İşletmeler, veri koruma görevlilerinin veri koruma sorumluluklarını

²²⁸ Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01, last revised and adopted 5 Nisan 2017, s.7, (Çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/612048>, 12 Şubat 2022.

²²⁹ Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01, last revised and adopted 5 Nisan 2017, s.8-9, (Çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/612048>, 12 Şubat 2022.

²³⁰ Tüzük madde 37(7).

yerine getirirken herhangi bir talimat almadıklarını garanti etmelidir. Ayrıca, en yüksek yönetim seviyesindekiler de dahil olmak üzere, işletmeden, görevlerini yerine getirdikleri için hiçbir şekilde kovulmayacak veya cezalandırılmayacaktır²³¹.

Madde 38 (6), veri koruma görevlilerinin ek görev ve sorumluluklarını yerine getirmelerine izin verir. Bununla birlikte, şirketin bu tür görev ve sorumlulukların çıkar çatışması yaratmadığını garanti etmesini gerektirir. Çıkar çatışmaları, veri koruma görevlilerinin bağımsız hareket etme gerekliliği ile ayrılmaz bir şekilde ilişkilidir. Veri koruma görevlilerinin başka görevleri yerine getirmelerine izin verilse de, şirket içinde veri işleme faaliyetlerinin amaçlarına ve yöntemlerine karar vermelerini sağlayan roller üstlenemezler²³².

28 Nisan 2020'de Belçika Veri Koruma Kurumu (Belçika DPA), veri koruma görevlilerinin atanmasıyla ilgili Tüzüğe uymadığı için büyük bir telekom operatörüne 50.000 € para cezası verdi. Belçika Veri Koruma Kurumu, veri koruma görevlisinin Tüzük kapsamındaki sorumluluklarının uyumluluk, denetim, risk direktörü olarak konumuyla çeliştiğini belirledi. Para cezası, veri koruma görevlisinin işletme içinde ikinci bir pozisyona sahip olması nedeniyle değil, ikinci pozisyonun onu Tüzük madde 38 (6) 'yı ihlal ederek önemli bir çıkar çatışması yaratan kişisel verileri işlemenin amaçları ve yöntemleri ile ilgili kararlar almaya zorladığı için verildi²³³.

Ek olarak, madde 27, AB'deki veri sahiplerinin davranışlarını izleyen veya onlara hizmet veya mal sunan AB'de herhangi bir kuruluşu olmayan işletmelerin AB'de bir temsilci belirlemesini gerektirir. Bu temsilci, ulusal veri koruma kurumlarının irtibat kişisi olacaktır. Bunun arkasındaki mantık basittir: AB sakinlerinin, kişisel verilerini saklayan Avrupa dışındaki kontrolörler ve veri işleyicilerle, potansiyel olarak karmaşık, zorlu ve pahalı bir prosedür olan onlarla

²³¹ Tüzük madde 38(3).

²³² Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01, last revised and adopted 5 Nisan 2017, s.16, (Çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/612048>, 12 Şubat 2022.

²³³ Karar yalnız Hollandaca mevcuttur, bkz., (Çevrimiçi), <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-18-2020.pdf> ; Cordery Legal Compliance, Compliance with Data Protection Officer GDPR Requirements, 19 Mayıs 2020, (Çevrimiçi), <https://www.corderycompliance.com/belgian-dpa-dpo-fine/>, 16 Şubat 2022.

kendi merkezlerinde iletişime geçme zorunluluğu olmadan iletişime geçebilmelerini sağlar²³⁴.

3.3. Davranış Kuralları

Davranış kuralları, Tüzük hükümlerinin kendi sektörlerinde nasıl uygulanacağını açıklamak amacıyla çeşitli endüstriyel sektörlerde kullanılmak üzere tasarlanmıştır²³⁵. Bu kapsamda davranış kurallarının amacı, soyut ve teknik hukuk kurallarının pratik bir yorumunu yapmaktır. Bu nedenle davranış kuralları, belirli bir endüstri veya veri işleme faaliyetleriyle ilgili teknolojilerle ilgili çözümler sunmayı amaçlamaktadır²³⁶.

Tüzük, Üye Ülkeleri, denetim makamlarını, Komisyonu ve Avrupa Veri Koruma Kurulunu (EDPB- European Data Protection Board), hükümlerinin AB genelinde uygun şekilde uygulanmasına yardımcı olmak için davranış kuralları geliştirmeye teşvik eder. Davranış kuralları geliştirilirken mikro, küçük, orta ölçekli işletmelerin özel ihtiyaçları göz önünde bulundurulmalıdır²³⁷.

Tüzüğün herhangi bir kısmı davranış kurallarına konu olabilir. Davranış kurallarında ele alınabilecek hususlardan bazıları Tüzüğün 40. maddesinin ikinci fıkrasında örnek olarak yer almaktadır. Davranış kurallarının oluşturulması, değiştirilmesi veya genişletilmesi, kontrolörleri veya işlemcileri temsil eden dernekler ve diğer kuruluşlar tarafından yapılabilir. Gerekçe madde 99, davranış kuralları geliştirirken, derneklerin ve diğer kuruluşların mümkün olduğunda veri sahipleri de

²³⁴ Tim Bell, “Is Article 27 the GDPR’s Hidden Obligation?”, 3 Mayıs 2018, (Çevrimiçi), <https://iapp.org/news/a/is-article-27-the-gdprs-hidden-obligation/> , 16 Şubat 2022.

²³⁵ Giakoumopoulos, **a.g.e.**, s.181.

²³⁶ Voigt, **a.g.e.**, s.73.

²³⁷ Tüzük madde 40(1).

dahil olmak üzere ilgili kişilerle iletişim kurmaları ve bu tür istişareler sırasında alınan başvuruları ve ifade edilen görüşleri dikkate almaları gerektiğini belirtmektedir.

Davranış kuralları yalnızca bir Üye Ülkedeki işleme faaliyetleriyle ilgiliyse, kabul edilmeden önce, Tüzüğün hükümlerine uygunluklarını kontrol etmek için uygun denetim organına sunulmalıdır. Taslak halindeki davranış kuralları Tüzük hükümlerine uygunsa, ulusal denetim otoritesi bunu onaylar²³⁸. Onaylanan davranış kuralları ve bunların onaylanmasına yol açan gerekçeler, denetim makamları tarafından kamuya açıklanmalıdır. Taslak halindeki davranış kurallarının birden fazla Üye Ülkedeki işleme faaliyetleriyle ilgili olması durumunda, yetkili ulusal denetim otoritesi öncelikle taslak hakkında Avrupa Veri Koruma Kurulu'nun görüşünü almalıdır²³⁹. Avrupa Veri Koruma Kurulu, taslağın Tüzüğe uygun olduğunu onaylarsa, taslağı Komisyona sunar. Komisyon, "*uygulama yasalarıyla*", onaylanmış davranış kurallarının Birliğin tamamında geçerli olduğuna karar verebilir²⁴⁰.

Davranış kurallarına bağlılık, hem veri sahiplerine hem de veri kontrolörlerine önemli faydalar sağlar. Bu tür kurallar, mevzuat koşullarının her bir sektöre göre uyarlanmasını sağlarken aynı zamanda veri işleme faaliyetlerinin şeffaflığını artıran kapsamlı bir rehberlik sunar. Davranış kurallarına bağlılık, AB mevzuatına uygunluğu göstermek için de kullanılabilir; kontrolörler ve işlemciler, operasyonlarında yüksek öncelik veren ve veri korumasına kendini adanmış işletmeler olarak kamu imajlarını geliştirmek için kodlara bağlılıktan yararlanabilirler. Tüzüğün kuralları ile birlikte, onaylanmış davranış kuralları, verilerin AB dışına aktarılması için yeterli koruma olarak kullanılabilir²⁴¹. Onaylanmış davranış kurallarına uygunluk, sınır ötesi veri aktarımlarıyla ilgili olarak AB dışında bulunan kontrolörler ve işlemciler tarafından kullanılabilir. Davranış kurallarına ilişkin bu hüküm, uyumluluğu kolaylaştırarak pazarlarını genişletmek isteyen uluslararası işletmeler veya AB üyesi olmayan ortaklarla etkileşim kurmak isteyen işletmeler için fırsatlar yaratmaktadır.

²³⁸ Tüzük madde 40(5).

²³⁹ Tüzük madde 40(7).

²⁴⁰ Tüzük madde 40(9).

²⁴¹ Giakoumopoulos, *a.g.e.*, s.182.

3.4. Sertifikasyon

Şeffaflığı ve Tüzük ile uyumluluğu artırmak için, madde 42'de sertifikasyon prosedürleri ile veri koruma mühürleri ve işaretleri ile ilgili düzenleme getirilmiştir. Sertifika prosedürleri, işletmelerin Tüzük uyumluluğunu göstermelerinin başka bir yoludur. Ayrıca, sertifikasyon gönüllülük esasına göre yapılabilir. Akredite kuruluşlar veya denetim makamları, işletmelere sertifikalar sağlayabilir. Akredite belgelendirme kuruluşu olma şartları madde 43(2)'de belirtilmiştir. Sertifikasyon, denetleyici makamlar veya Avrupa Veri Koruma Kurulu tarafından onaylanan kriterlere göre gerçekleştirilebilir. Avrupa Veri Koruma Kurulu onaylı kriterlerin karşılandığı durumlarda, bu standart sertifika, Avrupa Veri Koruma Mührü ile sonuçlanabilir²⁴².

Sertifikalar, mühürler ve işaretler veri sahiplerinin işletmelerin veri işleme güvenliği derecesini hızlı bir şekilde değerlendirmesine olanak tanıdığından sertifikasyon sistemi kullanmayı tercih eden işletmeler, daha fazla görünürlük ve güvenilirlik kazanabilir. Bir kontrolörün veya işlemcinin böyle bir sertifika almış olmasının, onları Tüzüğün diğer tüm hükümlerine uyma yükümlülüklerinden ve sorumluluklarından muaf tutmadığını belirtmek önemlidir²⁴³.

²⁴² Tüzük madde 42(5).

²⁴³ Tüzük madde 42(4).

DÖRDÜNCÜ BÖLÜM

GENEL VERİ KORUMA TÜZÜĞÜ'NÜN İŞLETMELER ve VERİ SAHİPLERİNİN HAK ve MENFAATLERİ BAKIMINDAN DEĞERLENDİRİLMESİ

1. İşletme Özgürlüğü

AB Temel Haklar Şartı'nın 16. maddesinde belirtildiği gibi, *"Birlik hukukuna, ulusal yasa ve uygulamalara uygun olarak bir iş yapma özgürlüğü tanınmaktadır."* İşletme özgürlüğü, işletmenin kuruluşu ve yönetimi de dahil olmak üzere tüm iş döngülerini kapsar²⁴⁴. Yasal faaliyetlere yapılan herhangi bir müdahale, bir işi yürütme hakkına yapılan bir saldırı olarak kabul edilebilir²⁴⁵. Örneğin, Tüzüğe uyumdan kaynaklanan yüksek maliyetler, işletmenin bir pazarda yer alma yeteneğini etkilediği için müdahaleci olarak kabul edilebilir. Bununla birlikte, böyle bir müdahaleden söz edebilmek için maliyetlerin işletmeler üzerinde aşırı bir etkisinin söz konusu olması gerekir. İşletme özgürlüğü, şirketleri orantısız müdahalelerden korur²⁴⁶.

Avrupa Komisyonu, Tüzüğün amacının veri sahiplerinin temel gizlilik haklarını korumak ve aynı zamanda AB'nin tek iç pazarını güçlendirerek işletmelere yardımcı olmak olduğunu vurgulamıştı²⁴⁷. Yeni veri koruma çerçevesi ile milletvekilleri,

²⁴⁴ European Union Agency for Fundamental Rights (FRA), 'Freedom to conduct a business: exploring the dimensions of a fundamental right' 2015, s.33, (Çevrimiçi), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf , 27 Temmuz 2022.

²⁴⁵ Nils Wahl "The Freedom to Conduct a Business: A Right of Fundamental Importance for the Future of the European Union", AMTENBRINK, Fabian, et al. (Ed.), **The Internal Market and the Future of European Integration: Essays in Honour of Laurence W Gormley** içinde, Cambridge University Press, 2019, s.279.

²⁴⁶ Eyup Kun, "Inherent Role of the Freedom to Conduct a Business under GDPR: The Tailored Liability of Search Engines", 18 Ağustos 2020, s.5, (Çevrimiçi), <http://dx.doi.org/10.2139/ssrn.3933338> , 19 Şubat 2022.

²⁴⁷ European Commission, Press Release, European Data Protection Day 2013: Full speed ahead towards reliable and modern EU data protection laws, 28 Ocak 2013, (Çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/IP_13_57 , 27 Temmuz 2022.

AB'deki yüksek veri koruma standartlarını güçlendirerek iş fırsatları yaratmaya çalışıyorlardı²⁴⁸.

Gerekçe madde 4'e göre, veri sahiplerinin hakları mutlak değildir ve *"orantılılık ilkesine uygun olarak, toplumdaki işleviyle ilişkili olarak dikkate alınmalı ve diğer temel haklarla dengelenmelidir."*

Tüzüğün belirli hükümleri, kapsamlı veri koruması sağlarken şirketlerin bir iş yürütme özgürlüğünü koruduğunu göstermektedir.

Tüzük, veri sahiplerine veri taşınabilirliği hakkı sağlar. Literatürde, bu aktarımın veri kontrolörleri için irrasyonel maliyetlere neden olması durumunda, madde 20(4)'ün bir adli başvuruda başvurulabileceği iddia edilmiştir. Madde 20(4)'e dayanarak, taşınabilirlik hakkının başkalarının hak ve özgürlükleri üzerinde olumsuz bir etkisi olmaması gerektiğini belirten genel bir denge hükmüdür²⁴⁹. Ayrıca, Gerekçe madde 68 , *"veri sahibinin kendisiyle ilgili kişisel verileri iletme veya alma hakkı, kontrolörlerin teknik olarak uyumlu işleme sistemlerini benimsemeleri veya sürdürmeleri için bir yükümlülük oluşturmamalıdır"* demektedir. Teknik olarak uyumlu sistemlerin benimsenmesi ve sürdürülmesi mutlak bir kural olsaydı, bu işletmeler için gereksiz bir yük olurdu.

Madde 17 (2) uyarınca, veri kontrolörleri verilerini kamuya açıkladığında veri sahipleri unutulma hakkına sahiptir. Bununla birlikte, internet geniş olduğundan, veri kontrolörleri bu talepleri veri sahiplerinden aldığında, her web sayfasından ve arama motoru sonuçlarından belirli bir kişiye yapılan tüm referansları silmek mümkün olsa da oldukça zor olabilir. Madde 17 (2), bu talepler hakkında *"mevcut teknoloji ve uygulama maliyeti dikkate alınarak, kontrolörleri bilgilendirmek için teknik önlemler de dahil olmak üzere makul adımlar atacağını"* belirtir. Ayrıca, Tüzük "makul adımlar" üzerinde durmaktadır. Tüzükteki *"makul adımların"* kesin çizgilerle belirlenmesi, küçük, orta ölçekli işletmelere yük getirebilir. Sonuç olarak, *"uygulama*

²⁴⁸ European Commission, Questions and Answers – General Data Protection Regulation, (Çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387 , 19 Şubat 2022.

²⁴⁹ Gianclaudio Malgieri, "User-provided Personal Content in The EU: Digital Currency Between Data Protection And Intellectual Property." **International Review of Law, Computers & Technology**, C. 32, S.1, 2018, Note 7.

maliyeti" ve *"mevcut teknoloji"* kriterlerini ekleyerek, Tüzük veri sahibinin hakları ile işletme özgürlüğü arasında denge aramaktadır²⁵⁰.

Bunun bir başka örneği de Tüzüğün 25. maddesinde bulunabilir. Bu madde, veri kontrolörlerine doğrudan işleme eylemleriyle bağlantılı bir yükümlülük getirmektedir. Bu tür bir tasarımın uygulanması, kontrolörün kişisel verileri güvence altına almak için finansal ve organizasyonel kaynakları kullanma imkanını kısıtladığından, işletme özgürlüğüne bir müdahale olarak görülebilir. Bununla birlikte, madde 25 (1), gizliliğin tasarlama yoluyla uygulanması halinde 'uygulama maliyetinin' dikkate alınması gerektiğini öngörmektedir. Bu hüküm, tasarlanan gizliliği doğrudan zorunlu kılıp ilişkili maliyetleri dikkate almayacaksa, bu durum işletmelere aşırı ve orantısız harcamalar getirecektir. Bu tür mutlak sorumluluk, potansiyel piyasa katılımcılarını piyasaya katılmaktan veya piyasadan çıkmaktan caydıracak ve uyumlulukla ilişkili masraflar, orantısız müdahale oluşturan iş modellerini doğrudan etkileyecektir. Bu nedenle, Tüzük, bu hükümdeki *"uygulama maliyeti"* de dahil olmak üzere, iş yapma hakkını kişisel verilerin korunması ile uyumlu hale getirir²⁵¹.

Tüzüğün küçük ölçekli işletmeleri kayıt tutma faaliyetleri, veri koruma görevlisi ataması ve veri etki değerlendirmeleri gibi yükümlülüklerden hariç tuttuğunu da belirtmek önemlidir. 250'den az çalışanı olan işletmelerin, yüksek riskli işleme, düzenli olarak gerçekleşen işleme veya madde 9 (1) veya madde 10'daki hassas verileri içeren işlemeye dahil olmadıkça işleme faaliyetlerini kaydetmeleri gerekmez. Madde 9 veya 10'da açıklanan kişisel verileri işlemeyen işletmelerin, veri sahiplerinin "büyük ölçekli" sık ve sistematik gözetimini yapmadıkları sürece bir veri koruma görevlisi istihdam etmeleri gerekmez.

Tüzüğün veri koruma etki değerlendirmesine ilişkin 35. maddesi, bir etki değerlendirmesinin gerekli olup olmadığını değerlendirirken incelenecek alanlar olarak işlemenin *"kapsamı"* ve *"bağlamı"* ndan bahseder. Bu terminolojinin bir sonucu

²⁵⁰ Voigt, **a.g.e.**, s.163.

²⁵¹ Eyup Kun, **a.g.e.**, s.9.

olarak, işlemenin boyutu, veri sahiplerinin hak ve özgürlükleri için önemli bir risk olup olmadığına karar verirken göz önünde bulundurulması gereken bir husus olabilir.

2. İşletmeler İçin Zorluklar

2.1. Uygulama Maliyetleri

Tüzük hükümlerine uymak için şirketlerin yüksek fonlara sahip olmaları gerekir. Küçük ve orta ölçekli işletmelerin Tüzük gerekliliklerine uymak için milyonlarca dolar harcaması gerekir. 500 çalışanı olan işletmelerin Tüzüğe uymak için en az 3 milyon dolar harcaması gerekir²⁵². İlk aşamada uyumluluk maliyetleri şunları içerir: personelin eğitime ve uyumluluk stratejisinin uygulanmasına, onay yönetimi için yeni yazılımların tasarlanmasına ve yasal ücretlere harcanan fonlara ilişkin maliyetler²⁵³. Uyumluluk maliyetlerinin özellikle yeni başlayanlar üzerinde olumsuz etkileri vardır, çünkü istikrarlı gelirler elde etmeye başlamak için biraz zamana ihtiyaçları vardır²⁵⁴. Yeni başlayan küçük, orta ölçekli şirketler uyumluluk göstermekte zorlanıyor ve beş işletmeden neredeyse biri tam uyumun mümkün olmadığını düşünüyor²⁵⁵. Google gibi büyük şirketler, Tüzük ile uyumluluk konusunda çalışan birçok yasal veri uzmanının yanı sıra finansal kaynaklara da sahiptir. Tüzük uyumluluğu ile ilişkili insan kaynaklarının yanı sıra sermaye giderleri, sınırlı finansal

²⁵² Layton Roslyn, The 10 Problems of the GDPR The US can learn from the EU's mistakes and leapfrog its policy: Hearing on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation Before the S. Judiciary Comm., 116th Cong. 2019, s.4, (Çevrimiçi), <https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf>, 27 Temmuz 2022.

²⁵³ Data Grail, The Age of Privacy: The Cost of Continuous Compliance, Mayıs 2019, (Çevrimiçi), <http://www.portaldaprivacidade.com.br/wp-content/uploads/2019/05/GDPR-CCPA-cost-report.pdf>, 19 Şubat 2022; Nick Eckert, "What Are the Real Costs of GDPR Compliance?", 24 Ocak 2019, (Çevrimiçi), <https://www.privacy.com/blog/what-are-the-real-costs-of-gdpr-compliance>, 19 Şubat 2022.

²⁵⁴ Elizabeth Pollman, "Startup Governance", *Faculty Scholarship at Penn Law*, C. 168, 2019, (Çevrimiçi), <https://heinonline.org/HOL/P?h=hein.journals/pnlr168&i=159>, 19 Şubat 2022.

²⁵⁵ IAPP-EY, Annual Privacy Governance Report, 2018, s.67 (Çevrimiçi), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-iapp-ey-annual-privacy-gov-report-2018.pdf, 27 Temmuz 2022.

fonlar ve personel nedeniyle küçük ve orta ölçekli işletmeleri orantısız bir şekilde etkilenmektedir²⁵⁶.

Avrupa Komisyonu, Avrupa Birliği ve Konsey'e yaptığı bildirimde, Tüzüğün özellikle küçük ve orta ölçekli işletmeler için zorlayıcı olduğunu belirtmiştir. Risk temelli yaklaşıma göre, küçük ve orta ölçekli işletmeler için derogasyonlar vermek uygun olmayacaktır. Çünkü büyüklükleri veri işleme faaliyetleri konusundaki risklerin bir göstergesi değildir²⁵⁷.

Ek olarak, Tüzük, özellikle Avrupa bilgi teknolojisi işletmelerinde küçük ve orta ölçekli işletmelerin büyümesini engelledi. Bir ankete göre, daha az kişinin Tüzük gibi katı gizlilik gereksinimleriyle ilgilenmesi gereken işletmelere yatırım yapması muhtemeldir²⁵⁸.

²⁵⁶ Geradin, **a.g.e.**, s. 64.

²⁵⁷ European Commission, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24 Haziran 2020 , (Çevrimiçi), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264>, 27 Temmuz 2022.

²⁵⁸ Leonid Bershidsky, "Europe's Privacy Rules Are Having Unintended Consequences", 14 Kasım 2018, (Çevrimiçi), <https://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are>. , 19 Şubat 2022.

2.2. Tüzüğün Rekabet Üzerindeki Etkileri

Kapsamlı mevzuatın kabul edilmesinin temel hedeflerinden biri, Avrupa Birliği'nin iç pazarını iyileştirmek ve iş dünyası için oyun alanını dengelemektir²⁵⁹. Ancak tam tersi oldu. Küçük ve orta ölçekli işletmelerin Tüzüğün uğraştırıcı gereksinimlerine uyma konusundaki yetersizliği nedeniyle, küresel şirketler pazar hakimiyeti kazanmıştır. Tüzük kapsamındaki önemli cezaların yanı sıra sorumluluk endişeleri, reklam verenlerin reklam harcamalarını Google, Facebook ve Amazon gibi daha büyük aktörlere yönlendirmesine neden olmuştur²⁶⁰. Bu aktörler veri gizliliği tüzüğüne uyma konusunda uzmanlaşmışlardır. Araştırmaya göre, daha küçük AdTech şirketleri "önemli" pazar payını²⁶¹, kaybetti ve Google ve Facebook çevrimiçi reklamcılıktaki yerlerini güçlendirdi²⁶².

Ayrıca, Google ve Facebook gibi dev şirketlerin veri sahiplerinin rızasını toplaması daha kolaydır, çünkü birçok kişi hizmetlerine bağımlıdır. Örneğin, anket sonuçları, internet kullanıcılarının yüzde ellisinin Google ve WhatsApp'ın "*kesinlikle gerekli*" olduğunu düşündüğünü göstermektedir. Bu şirketler hizmetlerine erişilebilmesi için veri sahiplerinin bazı çerezlerin kabul edilmesi gerektiği anlamına gelen "*onayla ya da bırak*" yaklaşımını benimserler. Bazı kullanıcılar onayın alınma şeklinden memnun olmasalar da, Google'ın hizmetlerinin gerekli olarak algılanması ve güvenilir seçeneklerin azlığı, kişisel bilgilerin toplanmasıyla ilgili endişelerinden daha ağır basmaktadır²⁶³.

Otutum açılan platformlarda (Facebook gibi), hizmetlerine erişmek için belirli bir şirketin hüküm ve koşullarını kabul ettiklerinde veri sahiplerinden yalnızca bir kez izin alır. Bu tür oturum açma ortamlarına literatürde "*duvarlı bahçeler*" denir. "Duvarlı

²⁵⁹ European Commission, Press Release, European Data Protection Day 2013: Full speed ahead towards reliable and modern EU data protection laws, 28 Ocak 2013, (Çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/IP_13_57, 27 Temmuz 2022.

²⁶⁰ Geradin, *a.g.e.*, s.66.

²⁶¹ Bjorn Greif, Study: Google is the biggest beneficiary of the GDPR, 10 Ekim 2018, (Çevrimiçi), <https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr>, 24 Şubat 2022.

²⁶² Cale Guthrie Weissman, 'One Year in, GDPR Seems to have Helped Google & Facebook', (Çevrimiçi), <https://www.fastcompany.com/90351655/gdpr-helps-google-and-facebook-grow-uk-market-share-in-2019>, 24 Şubat 2022.

²⁶³ Anne Niedermann, 'Freely-Given and Informed Consent? The User's Perspective' Presentation of the Results of the Allensbach Survey, DLD Europe, 2019.

bahçelerin" yanı sıra, işletmelerin web sayfalarını ziyaret ettiklerinde veri sahiplerinin onaylarının alınması gerekir. Veri kontrolörlerinden gelen tekrarlayan onay taleplerine maruz kalan veri sahiplerinin, onay taleplerini reddetme olasılıkları yüksektir²⁶⁴.

Tüzük, daha küçük piyasa katılımcıları karşısında dev platformlara fayda sağlayabilir ve sonuç olarak, Tüzük piyasada güç odaklarının daha fazla yoğunlaşmasına yol açabilir²⁶⁵.

2.3. Tek Elden Denetim Mekanizması

Tüzük, "ana kuruluşun veya kontrolörün veya işleyicinin tek kuruluşunun denetim otoritesinin, baş denetim otoritesi olarak hareket etmeye yetkili olacağı" tek elden bir mekanizma benimsemektedir²⁶⁶.

İşletmelerin idari maliyetlerini hafifletmek ve sınır ötesi veri iletimini sağlamak için 'tek elden denetim esası' oluşturuldu. Bu, bir işletmenin birden fazla Üye Ülkenin bölgesinde faaliyet gösterdiği zaman ve fon harcamalarını azaltır. 'Tek elden denetim esası' hükmü, işletmelerin tek bir veri koruma yetkilisiyle iletişim kurmasını ve öncelikle etkileşimde bulunmasını sağlar²⁶⁷.

Bazı durumlarda, önde gelen veri koruma otoritesi olmayan bir ulusal veri koruma otoritesi, kontrolörleri veya işleyicileri denetleme ve soruşturma yetkisine sahip olabilir. Yani "konu yalnızca Üye Ülkedeki bir kuruluşla ilgili olduğunda veya yalnızca Üye Ülkedeki veri sahiplerini önemli ölçüde etkilediğinde"²⁶⁸. Bununla

²⁶⁴ Geradin, **a.g.e.**, s.67.

²⁶⁵ Gal, **a.g.e.**, s.387.

²⁶⁶ Tüzük madde 56(1).

²⁶⁷ ESET, "Is GDPR Good or Bad News for Business", 31 Mayıs 2017, (Çevrimiçi), https://www.eset.com/fileadmin/ESET/US/resources/whitepapers/Is_GDPR_good_or_bad_news_for_business.pdf, 24 Şubat 2022.

²⁶⁸ Tüzük madde 56(2).

birlikte, bu yalnızca lider veri koruma yetkilisi meseleyi ele almayı reddettiğinde gerçekleşebilir²⁶⁹.

Sonuç olarak, Tüzük, bazı veri koruma kurumlarına, yani dev dijital platformların merkezlerinin bulunduğu AB Üye ülkelerindeki veri koruma kurumlarına orantısız yaptırım yetkisi vermektedir. İrlanda, Google, Microsoft, Twitter ve Facebook gibi dev platformların ana kuruluşunun bulunduğu yerdir. Bu nedenle, İrlanda Veri Koruma Komisyonu'nun bu şirketleri inceleme ve cezalandırma kapasitesi ve istekliliği, uygunsuz veri işleme operasyonlarından kurtulup kurtulamayacaklarına veya sonuçlarla karşılaşp karşılaşmayacaklarına karar verir. İrlanda Veri Koruma Komisyonu, Tüzüğü ihlal edip etmediklerini aktif olarak izlemeyerek, soruşturma yürütmeyerek veya ceza vermeyerek bu dev teknoloji şirketlerine göz yumduğu için uzun zamandır eleştiriliyor²⁷⁰. Bir yandan, bunun nedeni, İrlanda Veri Koruma Komisyonu'nun dava yükünün büyük olmasıdır. Daralan bir bütçeyle ve sadece 140 avukatla, araştırmacı ve teknoloji uzmanından oluşan bir kadroyla, İrlanda Veri Koruma Komisyonunun aşırı yüklenmesi şaşırtıcı değildir²⁷¹. Öte yandan, İrlanda Veri Koruma Komisyonunun pasif konumu, İrlanda ile dev teknoloji şirketleri arasındaki büyük ekonomik bağımlılıktan kaynaklanıyor olabilir²⁷².

Ateşli veri koruma kurumlarının denetimine tabi olan kontrolörlerin ve işleyicilerin oldukça kapsamlı soruşturmalar ve önemli cezalarla karşı karşıya kalma olasılıkları daha yüksektir. Örneğin, Fransız Veri Koruma Kurumu, yürürlüğe girdiğinden beri Tüzüğü gayretle uygulamaktadır. Fransız Veri Koruma Kurumu, Temmuz 2018'de iki küçük yerel şirkete, Fidzup ve Teemo'ya resmi uyarılarda bulundu. Fransız Veri Koruma Kurumu, veri sahiplerine hedefli reklamlar hakkında ancak uygulamanın yüklenmesinden sonra bilgi verildiğinden, elde edilen rıza

²⁶⁹ Tüzük madde 56(3) (5).

²⁷⁰ Nicholas Vinocur, 'How One Country Blocks the World on Data Privacy' 24 Nisan 2019, (Çevrimiçi), <https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123>, 27 Temmuz 2022.

²⁷¹ Brave, 'Europe's Governments Are Failing the GDPR: Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities' Nisan 2020, s.7, (Çevrimiçi), <https://brave.com/static-assets/files/Brave-2020-DPA-Report.pdf>, 27 Temmuz 2022.

²⁷² Geradin, **a.g.e.**, s.70.

öncesinde bilgilendirilme yapılmadığı için bu şirketlerdeki veri işlemenin geçerli rızaya dayanmadığını iddia etti²⁷³.

Avrupa'daki veri koruma kurumlarını, bazıları -özellikle Fransız Veri Koruma Kurumu - diğer veri koruma kurumlarından daha katı bir duruş sergileyen bir dizi Tüzük yorumu benimsemiştir. Örneğin, Fransız Veri Koruma Kurumu'nun "*özgürce verilen onay*" yorumu, İrlanda Veri Koruma Komisyonu'nun aynı yorumundan daha geniştir. Fransız Veri koruma Kurumu'na göre: "*reddin kolaylıkla ifade edilebilmesi aslında serbest rızanın ifade edilebilmesinin karşılığıdır. Bu nedenle, kullanıcının seçim özgürlüğünü etkilememek için, rızanın ifade edilmesine yönelik mekanizma, reddin ifade edilmesine yönelik mekanizma ile aynı seviyede ve aynı teknik şekilde sunulmalıdır*"²⁷⁴. Bir websitesiye ulaşıldığı zaman çerezlerle ilgili açıklamanın yer aldığı bir pencere açılır. Fransız Veri Koruma Kurumu, açılan bu pencerede hem çerezlere onay gösterilmesi hem de reddedilmesi opsiyonunun aynı pencerede yer alması gerektiğini söylemektedir. Fransız Veri Koruma Kurumu'na göre kullanıcı nasıl kolaylıkla çerezleri kabul edebiliyorsa, onları reddedebilmesi de bu kadar kolay olmalıdır. Çünkü kullanıcılar çerezleri reddedebilmek veya yönetmek için başka bir pencereye yönlendirildiklerinde bu onlar için kafa karıştırıcı olabilir. İrlanda Veri Koruma Komisyonu ise şunu belirtmektedir, çerezlerle ilgili açılan pencere üzerinde "*kabul et*" seçeneği olan bir düğme kullanıldığında, kullanıcının çerezleri "*reddetmesine*" izin veren bir seçenek veya çerezleri yönetmelerine izin veren ve bunu yapmalarına izin vermek için onları başka bir pencereye yönelten bir seçenek eşit değer taşımaktadır²⁷⁵. Yani, bu zaman kullanıcıların çerezleri yönetmesi veya reddedebilmesi için başka bir sayfaya yönlendirilmesine izin veriliyor. İrlanda Veri Koruma Komisyonu için önemli olan, veri sahiplerinin çerezleri reddetmekten

²⁷³Kristof Van Quathem, French Supervisory Authority Issues 2 GDPR Warnings, 1 Ağustos 2018, (Çevrimiçi), <https://www.natlawreview.com/article/french-supervisory-authority-issues-2-gdpr-warnings>, 27 Şubat 2022.

²⁷⁴ CNIL, 'Draft Recommendation on the Practical Procedures for Collecting the Consent Provided for in Article 82 of the French Data Protection Act, Concerning Operations of Storing or Gaining Access to Information in the Terminal Equipment of a User (Recommendation "Cookies and other trackers")' (14 Ocak 2020) para 35, (Çevrimiçi), <https://www.cnil.fr/en/cnil-launches-public-consultation-its-draft-recommendation-cookies-and-other-trackers>, 27 Şubat 2022.

²⁷⁵ Irish Data Protection Commission, 'Guidance Note: Cookies and Other Tracking Technologies' Nisan 2020 .s.9, (Çevrimiçi), <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> , 27 Temmuz 2022.

alıkonulmamasıdır²⁷⁶. Özetlemek gerekirse, veri sahipleri açık bir reddetme düğmesi gördüğünde, çerezleri reddetmek için ikinci katmana yönlendirildikleri zamana kıyasla çerezleri reddetme olasılıkları daha yüksektir.

Tüzük, AB genelinde oyun alanını dengelemeyi amaçlasa da, şirketler ana kuruluşlarının konumuna bağlı olarak değişen onay gereksinimlerine tabi olmaya devam ediyor. Uygulamada, Fransız Veri Koruma Kurumu'nun denetlediği şirketlere katı yaptırımlar uygulanırken, teknoloji devlerine daha esnek yaptırımlar uygulanıyor²⁷⁷.

2.4. Dahili Veri Aktarımı Sorunu

Veri koruma kurumları, harici veri aktarımlarına kısıtlamalar getirdiler, ancak büyük dijital platformların çeşitli bölümlerinde dahili veri paylaşımını önlemek için çok az şey yaptılar. Tüzüğün amaç kısıtlama ilkesinin yetersiz uygulanması, yalnızca kullanıcı gizliliği için önemli bir tehlike oluşturmakla kalmaz, aynı zamanda farklı veri kullanımlarına ilişkin onayı birleştirebildikleri için dev platformlara rekabet avantajı sağlar. Örneğin, Facebook'un veri politikası, doğrudan meta ürünlerinden toplanan önemli kullanıcı verilerini toplamasına izin veriyor. Bu *"herkese açık dahili veriler"* iki nedenden dolayı endişe uyandırmaktadır. Öncelikle, bu uygulama farklı kullanıcı süper-profillerinin oluşturulmasına izin vererek Google ve Facebook gibi dev platformların internet kullanıcıları hakkında kapsamlı bir görüş edinmelerini sağlamaktadır. Bu, kullanıcı gizliliği için önemli bir risk oluşturur. Bu geniş hedefler, veri işleme hedeflerinin açık ve net bir şekilde belirtilmesini gerektiren amaç sınırlama ilkesinin amaç belirleme unsurunu sağlamamaktadır. İkincisi, verilerin bu çapraz kullanımı, Tüzüğe bağlı olan ancak benzer bir pazar konumundan ve tüketiciye yönelik çeşitli mallardan yoksun olan işletmeler karşısında büyük platformlara önemli bir rekabet avantajı sağlar²⁷⁸.

²⁷⁶ Irish Data Protection Commission, 'Guidance Note: Cookies and Other Tracking Technologies' Nisan 2020 ,s.9, (Çevrimiçi), <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> , 27 Temmuz 2022.

²⁷⁷ Geradin, **a.g.e.**, s.73.

²⁷⁸ Geradin, **a.g.e.**, s.74-76.

Alman Federal Kartel Ofisi "*herkese açık dahili veriler*" konusunu ele alarak Facebook'un kullanıcı bilgilerini kullanıcı izni olmadan web sitesinden, meta ürünlerinden ve üçüncü taraf şirketlerden entegre etmesini yasaklayan bir karar aldı ve Facebook'un hizmet şartlarını ve işletme stratejisini değiştirmesini talep etti. Ancak Facebook tarafından yapılan temyiz başvurusu üzerine Düsseldorf Yüksek Bölge Mahkemesi, Facebook'un veri toplama ve işleminin rekabete aykırı sonuçlar doğurmadığını belirtmiştir. Ancak Alman Federal Kartel Ofisi bu karara itiraz etti ve Alman Yüksek Adalet Mahkemesi rekabet otoritesinin lehine karar verdi²⁷⁹.

3. Veri Sahiplerinin Zayıf Konumu

Tüzük, gizliliğin kendi kendini işleteceği anlayışına dayanır; bu, veri sahiplerinin haklarını iddia etme veya feragat etme seçeneğine sahip oldukları anlamına gelir. Bununla birlikte, veri sahipleri, bir şirketin veri işleminin kabul edip etmeme ve bu hakları kullanma konusunda yeterince bilgi sahibi olmayıp, özgür kararlar verme kapasitesinden yoksundur. Bu konuyu incelemek için, bireyler arasında Tüzük bilgisini araştırmak için yapılan Eurobarometer^{487a}²⁸⁰ özel anketinin sonuçlarına ve ayrıca veri paylaşımı ve veri koruma ile ilgili daha genel tutum ve davranışlara bir göz atacağız.

Ankete katılanların beşte birinden sadece biraz fazlası, kişisel verilerinin çevrimiçi olarak işlenmesiyle ilgili şartlar ve koşullar hakkında her zaman bilgilendirildiklerini düşünüyor. İnternet kullanıcılarının çoğunluğu (yüzde 57), verilerinin toplandığı ve daha sonra kullanılabileceği hakkında bazen veya her zaman bilgilendirildiklerini düşünüyor. Beşte birinden biraz fazlası (%22) her zaman bilgilendirildiklerini düşünüyor. %35'i bazen bilgilendirildiklerini düşünüyor. Yüzde 21'lik bir kesim ise nadiren bilgilendirildiğini ya da hiç bilgilendirilmediğini, yüzde 13'ü ise hiç bilgilendirilmediğini düşünüyor. On İnternet kullanıcılarından altısı gizlilik

²⁷⁹ Natasha Lomas, Antitrust case against Facebook's 'super profiling' back on track after German federal court ruling, 23 Haziran 2020, (Çevrimiçi), <https://rb.gy/wfwdsc>, 27 Temmuz 2022.

²⁸⁰ Special Eurobarometer 487a, GDPR, (Çevrimiçi), <https://cnpd.public.lu/content/dam/cnprd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf>, 27 Temmuz 2022.

politikalarını okuyor; yalnızca küçük bir yüzde bunu tamamen yapıyor. Ankete katılanların çoğunluğu (% 60) gizlilik politikalarını okuyor, ancak sadece % 13'ü bunları tam olarak okuyor, % 47'si kısmen okuyor. Ankete katılanların üçte birinden fazlası (%37) bu politikaları okumamaktadır. Okumayanlar, uzunlukları nedeniyle gizlilik politikalarını okumamaktadır.

Veri sahipleri, işletmeler tarafından veri işlemeye izin vermek zorundadır. Veri sahipleri, verilerinin toplanmasını devre dışı bırakmayı seçerse, şirketin hizmetlerinin çoğu onlar için kullanılamaz hale gelir. Gmail, Facebook, Instagram ve Uber gibi büyük şirketler, kullanıcıların hizmetlerini kullanabilmeleri için gizlilik politikalarını kabul etmelerini zorunlu kılar. Bu durumda, devre dışı bırakma genellikle internet'ten vazgeçme anlamına gelir, çünkü çoğu şirket veri sahiplerinin onayını talep eder. Bu nedenle, Tüzük yanıltıcı bir gizlilik duygusu üretir. İşletmelerin, başlangıçta gerçek bir seçeneği olmayan bir veri sahibi nedeniyle hala büyük miktarlarda kişisel veri elde etmelerine izin verilmektedir.

Eurobarometer'in araştırmaları, katılımcıların onda üçünden fazlasının (%31) ankette ele alınan tüm hakları bildiğini, dörtte birinden fazlasının (%27) ise hiçbirini bilmediğini ortaya koymaktadır. Neredeyse dörtte üçü (%73) Tüzük ile güvence altına alınan en az bir hakkı bilmektedir. Ankete katılanların çoğunluğu, kişisel veri haklarını korumaktan sorumlu yerel bir denetim otoritesini duymuştur. Ankete katılanların onda birinden fazlası haklarını zaten kullanmıştır. Görüldüğü gibi, bu rakam o kadar yüksek değil. Bazı akademisyenlere göre, bireyler haklarını etkili bir şekilde kullanmak için genellikle zaman, kaynak ve deneyim açısından çok zayıftır.

Tüzüğün kabulündeki amaç, bireylerin önemli seçeneklerden yoksun olduğu ve çevrimiçi işletmelerin gizlilik politikalarını kabul etmek zorunda olduğu mevcut veri işleme uygulamalarıyla uyumlu değildir. Tüzüğün maliyetli gereklilikleri, küçük ve orta ölçekli işletmelere önemli bir yük getirmektedir, ancak aynı zamanda pazardaki küçük ve orta ölçekli işletmeleri haksız yere reddederek adalet konusunda ciddi sorular ortaya çıkarmaktadır.

SONUÇ

İlk bölümde ele alındığı gibi profillemeye, gelişmiş veri noktaları, güvenlik sorunları ve kişisel verilerin kötüye kullanımı gibi online veri toplamayla ilgili problemler, kapsamlı bir veri koruma çerçevesini gerektirmektedir. Teorik olarak veri korumaya ilişkin en kapsamlı düzenleme muhtemelen Tüzüktür ve diğer birçok veri koruma kanunu da bundan esinlenmiştir.

İkinci bölümde, niçin yeni bir mevzuat kabul edilmesi gerektiğine baktık. Daha önceki Direktif, teknoloji sektöründeki bütün gelişmelerle uyumlu değildi. Tüzük, teknolojik gelişmelerle gelen yasal sorunları çözemiyordu. Ayrıca Tüzük, veri koruma standartlarını harmonize etme ve AB veri korumasının vurgusunu kağıt üzerindeki bürokratik kurallardan daha pratik bir niteliğe, yasal tutarlılığa ve bireylerin yetkilendirilmesine yönelik değişiklikler getirme amaçlarıyla kabul edilmiştir.

Üçüncü bölümde Tüzük hükümlerine, bilhassa da Tüzük ile belirlenen yeni kavramlara daha yakından inceledik.

Son bölümde ise işletme özgürlüğünü ele aldık. Birtakım hükümleri ve Gereke 4'ü analiz ettiğimizde, Tüzüğün birey ve işletmelerin veri koruma hakları arasında bir denge kurmaya çalıştığını gördük. Sözü edilen gerekçeye istinaden bireylerin veri koruma hakları, diğer temel haklar ile uyumlu hale getirilmelidir. Tüzük, kapsamlı veri korumasını güvence altına alırken işletmelerin işlerini yürütme özgürlüğüne de saygı duyar. Örneğin Tüzük küçük işletmeleri kayıt tutmak, bir veri koruma memuru görevlendirmek ve veri etki değerlendirmeleri yürütmek gibi sorumluluklardan muaf tutar. 250 kişiden az işçi çalıştıran işletmeler, yüksek riskli işleme yapmadıkları sürece kayıt işleme işlemlerinden muafır.

Aynı bölümde, Tüzüğün pratikte beklenmeyen sonuçları olduğu sonucuna da vardık.

Tüzüğün AB'de çok daha gelişmiş veri koruması olmasına rağmen beklenmedik sonuçları olduğu görülmektedir. İlk olarak Tüzüğün artmış bir pazar yoğunluğu bulunmaktadır. Büyük şirketler, yeteri kadar uzman ve fona sahip olmaları sebebiyle

uyumluluk şartlarını kolayca karşılayabilir ve piyasa hakimiyeti kazanabilirler. Birçok şirket, Facebook ve Google gibi büyük platformların Tüzük uygulama konusunda başarılı olduğu varsayımından dolayı bu platformlara güvenmektedir. Tüzük, AB çapında etkili ve evrensel olarak uygulanmalıdır. Yukarıda açıklandığı üzere, tek elden denetim esaslı büyük platformların sadece belirli veri koruma kurumlarının soruşturma yürütmek ve yaptırım uygulamak konusunda isteksiz olmaları nedeniyle değil, aynı zamanda pratik sınırlamalar nedeniyle de sorumluluktan kaçınmalarını sağlamaktadır. Herkese açık dahili veri uygulamaları, Tüzük ile uyumlu olan fakat karşılaştırılabilir bir piyasa konumuna sahip olmayan şirketler karşısında büyük şirketlere kayda değer bir rekabet üstünlüğü sağlamaktadır. Buna ek olarak bu yöntem, büyük platformlara internet kullanıcılarının tam olarak görüntülenmesini sağlaması sebebiyle kullanıcıların veri gizliliğine önemli bir tehdit oluşturmaktadır. Ayrıca bu uygulama, Tüzüğün “amaçla kısıtlılık” ilkesini ihlal etmektedir.

Son bölümde de Tüzüğün veri sahipleri için olan yararlarını ele aldık. Birçok veri sahibinin gizlilik politikalarının tamamını okumadıkları göz önüne alındığında, verileri hakkındaki muhakemelerinin nasıl doğru olabileceğini sorgulamak makul olmaktadır. Dolayısıyla, veri sahiplerinin verdiği rızanın tamamıyla bilgilendirilmiş olarak veya özgürce verilmiş olduğunu söylemek mümkün olmaz. Ayrıca veri sahipleri halen kişisel verileri üzerinde kısıtlı kontrole sahiptir. Veri sahiplerinin uygun başka alternatifleri olmamasından ötürü, büyük platformların veri toplama uygulamalarını kabul etmek zorunda kalmaktadırlar.

KAYNAKÇA

I. Basılı Kaynaklar

- Ahmed, Javed; et al. : "GDPR compliant consent driven data protection in online social networks: A blockchain-based approach", **3rd International Conference on Information and Computer Technologies (ICICT)** ,s. 307-312, 2020.
- Albrecht, Jotzo : Allgemeine Bestimmungen, Rechtmäßigkeit der Datenverarbeitung; **Individuelle Datenschutzrechte**, Einschränkungen der Rechte, 2017.
- Bieker, Felix; et al. : "A process for data protection impact assessment under the European general data protection regulation." **In Annual Privacy Forum**, Springer, Cham, 2016, s. 21-37.
- Brookman, Justin; : "Why collection matters: surveillance as a de facto privacy harm." Big data and privacy: making ends meet, **The center for internet and society-Stanford Law School**, 2013, s.1-6.
- Gautam , Hans S.
- Bygrave, Lee A. : "Data protection by design and by default: deciphering the EU's legislative requirements." **Oslo Law Review**, C.4, S. 2, 2017, s.105-120.
- De Hert, Paul; : "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context." **International Data Privacy Law**, C.6, S. 3, 2016 , s. 230-243.
- Czerniawski, Michal
- Dülger, Murat Volkan : "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması." **Yaşar Hukuk Dergisi** C.1 S.2, 2019, s.71-174.

- Fabbrini, Federico; Celeste, Edoardo : "The right to be forgotten in the digital age: the challenges of data protection beyond borders.", **German law journal**, C.21, S.S1, 2020, s.55-65.
- Gal, Michal S.; Aviv, Oshrit "The competitive effects of the GDPR ", **Journal of Competition Law & Economics**, C.16, S. 3, 2020, s.349-391.
- Geradin, Damien; Karanikioti, Theano; Katsifis, Dimitrios : "GDPR Myopia: how a well-intended regulation ended up favouring large online platforms-the case of ad tech.", **European Competition Journal**, C.17, S. 1, 2021, s.47-92.
- Giakoumopoulos, Christos; Buttarelli, Giovanni; O'flaherty, Michael : "Handbook on European data protection law", **Publications Office of the European Union**, Luxembourg, 2018.
- Gray, Carolyn : "Who Pays the Price: Regulation of Data Tracking and Online Behavioral Advertising.", **Ariz. Summit L. Rev.**, C.8. , 2014, s.385-404.
- ITGP Privacy Team : "EU General Data Protection Regulation: An Implementation and Compliance Guide", Bs.2, IT Governance Publishing, 2017, (Çevrimiçi) <https://learning.oreilly.com/library/view/eu-general-data/9781849289467/> , 28 Ocak 2022.
- Hodaie, Neeka : "Real You Meets Virtual You: It is Time for Consumers to Regain Power Online," **Seattle J Soc Just**, C. 18, S.2, 2020, s.647-686.

Houser, Kimberly A.; Voss, Gregory W. : "GDPR: The end of Google and Facebook or a new paradigm in data privacy.", **Rich. JL & Tech**, C.25, S.1, 2018, s.1-109.

Kuner, Christopher, et.al. : **"The EU General Data Protection Regulation: A Commentary/Update of Selected Articles."** Update of Selected Articles , Oxford University Press, 2021.

Kun, Eyup : "Inherent Role of the Freedom to Conduct a Business under GDPR: The Tailored Liability of Search Engines", 18 Ağustos 2020, (Çevrimiçi), <http://dx.doi.org/10.2139/ssrn.3933338> , 19 Şubat 2022.

Lipman, Rebecca : "Online Privacy and the Invisible Market for Our Data." , **Penn St. L. Rev.** , 120, 2015, s.777-806.

Lubarsky, Boris : Re-Identification of "Anonymized" Data, **Geo. L. Tech. Rev.**, C.1, 2017, s.202-213.

Nissenbaum, Helen : "A contextual approach to privacy online." **Daedalus**, C.140, S.4, 2011, s. 32-48.

Martin, Brittany A : "The unregulated underground market for your data: Providing adequate protections for consumer privacy in the modern era.", **Iowa L. Rev**, C.105, 2019, s.865-900.

- Malgieri, Gianclaudio : "User-provided personal content'in the EU: digital currency between data protection and intellectual property." , **International Review of Law, Computers & Technology**, C. 32, S.1,2018, s.118-140.
- Misek, Jakub : "Consent to personal data processing–The Panacea or The dead end?." , **Masaryk University Journal of Law and Technology**, C.8, S.1, 2014, s.69-83.
- O'brien, Ralph : "Privacy and security: The new European data protection regulation and it's data breach notification requirements." , **Business Information Review**, C. 33, S. 2, 2016, s.81-84.
- Pollman, Elizabeth : "Startup Governance", **Faculty Scholarship at Penn Law**, C. 168, 2019, s.155- 221, <https://heinonline.org/HOL/P?h=hein.journals/pnlr168&i=159>. 19 Şubat 2022.
- Rothchild, John A. : "Against notice and choice: The manifest failure of the proceduralist paradigm to protect privacy online (or anywhere else)." ,**Clev. St. L. Rev.**, C.66,2017, s.559-648.
- Samonte, Mary : "Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law." ,**European Papers-A Journal on Law and Integration** , C.4, S. 3, 2019, s.839-851, (Çevrimiçi), <https://doi.org/10.15166/2499-8249/332> , 23 Aralık 2021.
- Solove, Daniel J. : "Privacy self-management and the consent dilemma." , **Harvard Law Review**, C.126, S.7, 2013, s.1880-1903.

- Tang, Jie; Akram, Umair; Shi, Wenjing : "Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits.", **Journal of Enterprise Information Management**,2020. s.1097-1120.
- Tene, Omer; Polenetsky, Jules : "To track or do not track: advancing transparency and individual control in online behavioral advertising.", **Minn. JL Sci. & Tech.**, C.13, 2012, s.281-358.
- Voigt, Paul; Von Dem Bussche, Axel : **"The EU GDPR : A Practical Guide"**, Cham: Springer International Publishing,2017.
- Wahl, Nils : "The Freedom to Conduct a Business: A Right of Fundamental Importance for the Future of the European Union", AMTENBRINK, Fabian, et al. (Ed.), **The Internal Market and the Future of European Integration: Essays in Honour of Laurence W Gormley** içinde, Cambridge University Press, 2019, s.273-287.

II. İnternet Kaynakları

- A&L Goodbody :The GDPR: A Guide for Businesses, 5 Ekim 2016, (Çevrimiçi), https://www.algoodbody.com/media/The_GDPR-AGuideforBusinesses1.pdf, 28 Ocak 2022.
- Article 29 Working Party :Guidelines on Consent under Regulation 2016/679, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, 28 Ocak 2022.
- Article 29 Working Party : Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Kasım 2017, (Çevrimiçi), https://ec.europa.eu/newsroom/document.cfm?doc_id=44137, 10 Şubat 2022.

- Article 29 Working Party : Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01, son gözden geçirme ve kabul tarihi 5 Nisan 2017, (Çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/612048,12> Şubat 2022.
- Article 29 Working Party : Guidelines on the right to data portability, (Çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-dataportability_e, 26 Aralık 2021.
- Article 29 Working Party : 'Opinion 03/2013 on purpose limitation' WP 203, 2 Nisan 2013, (Çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 19 Aralık 2021.
- Article 29 Working Party : Position Paper on the Derogations from the Obligation to Maintain Records of Processing Activities pursuant to Article 30(5) GDPR (2018), (Çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/position-paper-derogations-obligation-maintain-records_en, 16 Aralık 2021.
- Bell, Tim : "Is Article 27 the GDPR's Hidden Obligation?", 3 Mayıs 2018, (Çevrimiçi), <https://iapp.org/news/a/is-article-27-the-gdprs-hidden-obligation/>, <https://iapp.org/news/a/is-article-27-the-Tüzüks-hidden-obligation/>, 16 Aralık 2021.
- Bershidsky, Leonid : "Europe's Privacy Rules Are Having Unintended Consequences", 14 Kasım 2018, (Çevrimiçi), <https://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are.>, 19 Şubat 2022.
- Bourne, Helen; Corbett-Wilkins, Reece; Moran, John : "Reflecting on the Google LLC v CNIL (Case C507/17) ECJ Judgment: A UK and Australian Perspective", 28 Ocak 2020, (Çevrimiçi), <https://www.lexology.com/library/detail.aspx?g=86b16836-0673-427e-b10c-317a3320514e>, 23 Aralık 2021.
- Brave : "Europe's Governments Are Failing the GDPR: Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities" Nisan 2020, (Çevrimiçi), <https://brave.com/static-assets/files/Brave-2020-DPA-Report.pdf>, 27 Şubat 2022.

- Council of Europe : “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, 108 sayılı, 1981, (Çevrimiçi), <https://rm.coe.int/1680078b37> , 13 Ocak 2022.
- Council of Europe, : European Convention on Human Rights, (Çevrimiçi), https://www.echr.coe.int/Documents/Convention_ENG.pdf , 13 Ocak 2022.
- Cordery Legal Compliance : Belgian Regulator Imposes Euro 50,000 Fine for Non-Compliance with Data Protection Officer GDPR Requirements, 19 Mayıs 2020, (Çevrimiçi), <https://www.corderycompliance.com/belgian-dpa-dpo-fine/> . 16 Şubat 2022.
- CNIL : Draft Recommendation on the Practical Procedures for Collecting the Consent Provided for in Article 82 of the French Data Protection Act, Concerning Operations of Storing or Gaining Access to Information in the Terminal Equipment of a User (Recommendation “Cookies and other trackers”)’ 14 Ocak 2020, (Çevrimiçi), <https://www.cnil.fr/en/cnil-launches-public-consultation-its-draft-recommendation-cookies-and-other-trackers>, 27 Temmuz 2022.
- CNIL Restricted Committee : SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC., (Çevrimiçi), <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>, 27 Temmuz 2022.
- Dannon, Shay : GDPR Top Ten: #6 Privacy by Design and by default , 10 Şubat 2017, (Çevrimiçi), <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-top-ten-6-privacy-by-design-and-by-default.html>, 11 Şubat 2022.
- Data Grail : The Age of Privacy: The Cost of Continuous Compliance, may 2019, (Çevrimiçi), <http://www.portaldaprivacidade.com.br/wp-content/uploads/2019/05/GDPR-CCPA-cost-report.pdf>, 19 Şubat 2022.
- Deloitte Insights : Predictably Inaccurate: The Prevalence and Perils of Bad Big Data, 31 Temmuz 2017, (Çevrimiçi), <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-21/analytics-bad-data-quality.html> ,31 Kasım 2021.

- Dutch DPA : Fine for data breach Uber, Autoriteit Persoonsgegevens, Kasım 2018, (Çevrimiçi), <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber>., 12 Şubat 2022.
- Economist : How to think about data in 2019, 22 Aralık 2018, (Çevrimiçi), <https://www.economist.com/leaders/2018/12/22/how-to-think-about-data-in-2019>, 31 Kasım 2021.
- Eckert, Nick : What Are the Real Costs of GDPR Compliance?, 24 Ocak 2019, (Çevrimiçi), <https://www.priviq.com/blog/what-are-the-real-costs-of-gdpr-compliance>, 19 Şubat 2022.
- European Data Protection Supervisor : (Çevrimiçi), https://edps.europa.eu/data-protection/dataprotection/legislation/history-general-data-protection-regulation_en, 27 Temmuz 2022.
- European Union, : “Charter of Fundamental Rights of the European Union”, (Çevrimiçi), <https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT> , 27 Temmuz 2022.
- European Union, : “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, (Çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>, 2 Mart 2020.
- European Union : Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 Aralık 2007, 2007/C 306/01, (Çevrimiçi), <https://www.refworld.org/docid/476258d32.html> , 27 Temmuz 2022.
- European Union Agency for Fundamental Rights : ‘Freedom to conduct a business: exploring the dimensions of a fundamental right’ (2015), (Çevrimiçi), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf , 27 Temmuz 2022.

- European Commision : Press Release, European Data Protection Day 2013: Full speed ahead towards reliable and modern EU data protection laws, 28 Ocak 2013, (Çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/IP_13_57, 27 Temmuz 2022.
- European Commision : Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020 COM(2020), (Çevrimiçi), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264>, 27 Temmuz 2022.
- European Commision : Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, 25 Ocak 2012, (Çevrimiçi), http://europa.eu/rapid/press-release_IP-12-46_en.htm, 27 Temmuz 2022.
- European Commision : Questions and Answers – General Data Protection Regulation, (Çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/MEM_O_18_387 , 19 Şubat 2022.
- ESET : 'Is GDPR Good or Bad News for Business' , 31 Mayıs 2017, (Çevrimiçi), https://www.eset.com/fileadmin/ESET/US/resources/whitepapers/Is_GDPR_good_or_bad_news_for_business.pdf, 24 Şubat 2022.
- Fleischer, Peter : Google Global Privacy Counsel, 'Implementing a European, not global, right to be forgotten' ,30 Temmuz 2015, (Çevrimiçi) <https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html>, 23 Aralık 2021.

Greif, Bjorn	: Study, Google is the biggest beneficiary of the GDPR, 10 October 2018, (Çevrimiçi), https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr , 24 Şubat 2022.
Gstrein, Oskar J	: The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17), 9 Eylül 2019, (Çevrimiçi) , https://verfassungsblog.de/the-judgment-that-will-be-forgotten/ , 23 Aralık 2021.
IAPP-EY	: IAPP-EY Annual Privacy Governance Report 2018, (Çevrimiçi), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-iapp-ey-annual-privacy-gov-report-2018.pdf , 27 Temmuz 2022.
Information Commissioner's Office	: Lawfulness and transparency, (Çevrimiçi), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ , 18 Aralık 2021.
Information Commissioner's Office	Data minimisation, (Çevrimiçi), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ , 18 Aralık 2021.
Information Commissioner's Office	Storage Limitation, (Çevrimiçi), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ , 18 Aralık 2021.
Information Commissioner's Office	: Security, (Çevrimiçi), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ , 29 Aralık 2021.
Information Commissioner's Office	: Personal Data, (Çevrimiçi), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ , 10 Aralık 2021.
Irish Data Protection Commission	: 'Guidance Note: Cookies and Other Tracking Technologies' Nisan 2020, (Çevrimiçi),

<https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> ,27 Temmuz 2022.

Kuner, Christopher

: "The European Commission's proposed data protection regulation: A copernican revolution in European data protection law." Bloomberg BNA Privacy and Security Law Report, 6 Şubat 2012, s.1-15, (Çevrimiçi) http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-DataProtection-Law.pdf ,10 Aralık 2021.

Layton Roslyn

: The 10 Problems of the GDPRThe US can learn from the EU's mistakes and leapfrog its policy: Hearing on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation Before the S. Judiciary Comm., 116th Cong. 5 (2019), (Çevrimiçi), <https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf>, 27 Temmuz 2022.

Lomas, Natasha

: Antitrust case against Facebook's 'super profiling' back on track after German federal court ruling,23 Haziran 2020, (Çevrimiçi), <https://rb.gy/wfwdsc>, 27 Temmuz 2022.

Newman, Lily Hay

: A New Google+ Blunder Exposed Data From 52.5 Million Users, 10 December 2018, (Çevrimiçi), <https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/> , 12 Ocak 2022.

OECD

: " Guidelines on the Protection of Privacy and Transborder Flows of personal Data" , (Çevrimiçi), <https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm#part2> , 13 Ocak 2021.

Quirk, Mary B.

: "Study, Some Popular Android Apps Tracking User Location Once Every Three Minutes", 24 Mart 2015, (Çevrimiçi), <https://consumerist.com/2015/03/24/study-some-popular-android-apps-tracking-user-location-once-every-three-minutes/index.html> , 15 Aralık 2021.

Quathem, Kristof Van

: French Supervisory Authority Issues 2 GDPR Warnings, 1 Ağustos 2018, (Çevrimiçi), <https://www.natlawreview.com/article/french-supervisory-authority-issues-2-gdpr-warnings>, 27 Temmuz 2022.

- Ramirez, Edith : “Data Brokers A Call for Transparency and Accountability”, Federal Trade Commission, 14 Mayıs 2014, (Çevrimiçi), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>, 15 Aralık 2021.
- Robinson, Neil et. al. : “Review of the European Data Protection Directive”, Rand, 2009, (Çevrimiçi), https://www.rand.org/pubs/technical_reports/TR710.html, 10 Aralık 2021.
- Schwartz, Adam et. al. “New Rules to Protect Data Privacy: Where to Focus, What to Avoid, Electronic Frontier Foundation”, 2 Temmuz 2018, (Çevrimiçi), <https://www.eff.org/deeplinks/2018/07/new-rules-protect-data-privacy-where-focus-what-avoid>, 15 Aralık 2021.
- Sh, Oleksandr : “What Is an API: Concept and Architecture Types Explained on Real Life Examples”, (Çevrimiçi), <https://www.cleveroad.com/blog/what-is-an-api>, 12 Ocak 2022.
- The Guardian : [Former Twitter employees charged with spying for Saudi Arabia | Twitter | The Guardian](#) , 31 Kasım 2021.
- Vinocur, Nicholas : ‘How One Country Blocks the World on Data Privacy’ 24 Nisan 2019, (Çevrimiçi), <https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123>, 27 Temmuz 2022.
- Wes, Matt : “Looking to comply with GDPR? Here’s a primer on anonymization and pseudonymization, APP”, 25 April 2017, (Çevrimiçi), <https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/>, 12 Aralık 2021.
- Weissman, Cale Guthrie : ‘One Year in, GDPR Seems to have Helped Google & Facebook’, (Çevrimiçi), [GDPR helps Google and Facebook grow U.K. market share in 2019, 17 May 2019, https://www.fastcompany.com/90351655/gdpr-helps-google-and-facebook-grow-uk-market-share-in-2019](#), 24 Şubat 2022.
- Zolejnik, Lukas : ‘How to: GDPR, consent and data processing’, 2 Ocak 2018, (Çevrimiçi), <https://blog.lukaszolejnik.com/how-to-gdpr-consent-data-processing/> , 28 Ocak 2022.

