T.C. CUMHURBAŞKANLIĞI
STRATEJİ VE BÜTÇE BAŞKANLIĞI

Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti

Uzmanlık Tezi

Ayşe Nur AKINCI

SEKTÖRLER VE KAMU YATIRIMLARI GENEL MÜDÜRLÜĞÜ
ŞUBAT 2019

T.C. CUMHURBAŞKANLIĞI STRATEJİ VE BÜTÇE BAŞKANLIĞI
Yayın No: 0001

Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti

Uzmanlık Tezi

Ayşe Nur AKINCI

SEKTÖRLER VE KAMU YATIRIMLARI GENEL MÜDÜRLÜĞÜ
ŞUBAT 2019

ISBN 978-605-7519-05-4

Bu çalışma Strateji ve Bütçe Başkanlığının görüşlerini yansıtmaz. Sorumluluğu yazara aittir. Yayın ve referans olarak kullanılması Strateji ve Bütçe Başkanlığının iznini gerektirmez.

Bu tez Yılmaz TUNA başkanlığında, Ahmet ÇELENKOĞLU, Nebi ÇELİK, İbrahim Emre İLYAS ve Doç. Dr. Mehmet CANSIZ'dan oluşan Strateji ve Bütçe Başkanlığı Tez Sınav Kurulu tarafından 25 Ocak 2019 tarihinde değerlendirilmiştir.

Bu yayın 500 adet basılmıştır.

TEŞEKKÜR

Bu çalışmanın hazırlanmasında, danışmanım olarak bana rehberlik eden, kıymetli yorum ve önerileriyle her zaman yol gösteren ve bu alandaki bilgi ve tecrübesini benden esirgemeyen Strateji ve Bütçe Uzmanı Sayın Hakan YERLİKAYA'ya,

Bu çalışma konusunun seçiminde ve her aşamasında verdiği değerli katkılar için Avrupa Yatırım Bankası Uzmanı Sayın Özhan YILMAZ'a,

Bilgi Toplumu Dairesi'nde göreve başladığım günden itibaren verdiği kıymetli katkı ve desteklerinden dolayı Sektörler ve Kamu Yatırımları Genel Müdürü Sayın Emin Sadık AYDIN'a,

Tezin Taslak halini okumaya ayırdıkları zaman ve olumlu eleştirileri ile çalışmanın olgunlaşmasına yaptıkları değerli katkılarından dolayı Bilgi ve İletişim Teknolojileri Dairesi Başkanı Sayın Furkan CİVELEK'e, Strateji ve Bütçe Uzmanı Sayın N. Murat İNCE'ye, Sayın Agâh Reha TURAN'a, Sayın Burak KARAGÖL'e, Sayın M. Yaşar ŞAF'a, Sayın M. Raşit ÖZDAŞ'a, Sayın Dilek YÜKSEL CİVELEK'e ve Sayın Abdullah YÜREKTÜRK'e

Tez aşamasındaki motive edici yaklaşımları, katkı ve destekleri için değerli mesai arkadaşlarım Sayın Emrullah KAYA'ya, Sayın Damla YAZAR'a, Sayın Nurullah DEVECİ'ye ve Sayın Burak KARAMAN'a,

Her zaman olduğu gibi, bu süreçte de benden sevgi, moral ve desteklerini hiç esirgemeyen sevgili annem Hatice AKINCI'ya ve babam Ahmet AKINCI'ya en içten teşekkürlerimi sunmayı borç bilirim.

Ayşe Nur AKINCI

Ankara, 2019

ÖZET

Strateji ve Bütçe Uzmanlığı Tezi

BÜYÜK VERİ UYGULAMALARINDA KİŞİSEL VERİ MAHREMİYETİ

Ayşe Nur AKINCI

Dünya genelinde üretilen dijital verideki üstel artış, büyük miktar, hız ve çeşitlilikteki verinin saklanması, yönetilmesi, işlenmesi ve anlamlı sonuçlar çıkarılmasını sağlayan büyük veri uygulamalarının gelişimini tetiklemiştir. Büyük veri teknolojileri sayesinde ortaya çıkan devasa verilerin etkin bir şekilde kullanımı ise iş süreçlerinde iyileşmeler, verim artışı ve sunulan hizmet kalitesinin artırılmasıyla kullanıcı memnuniyeti, rekabet avantajı ve yüksek kârlılığı beraberinde getirmiştir.

Önemli ekonomik ve sosyal faydaları bünyesinde barındıran büyük veri sayesinde, bugün bireyler hakkında hiç bir çağda olmadığı kadar bilgiye sahip olunabilmektedir. Bu durum ise veri mahremiyeti kurallarının uygulanması bakımından birtakım zorlukları beraberinde getirmektedir. Büyük verinin mahremiyet alanında ortaya çıkardığı soru işaretleri giderilmeden gelişmesi ve ilgili sektörlerde güven temin etmesi mümkün gözükmemektedir. 2012 yılından beri birçok ülkenin politikalarında ve mevzuatında kapsamlı bir gözden geçirme sürecine girmeleri bunun bir yansıması olarak ortaya çıkmıştır. Zira büyük veri, modern mahremiyet düzenlemelerinin dayandığı adil veri işleme ilkelerini derinden etkilemektedir.

Çalışma kapsamında, büyük verinin mahremiyet alanında ortaya çıkardığı sorunların tespit edilmesi ve çözüm önerileri geliştirilmesi amaçlanmıştır. Bu çerçevede büyük verinin veri mahremiyetine ilişkin ortaya çıkardığı zorlukların giderilerek başarılı bir şekilde kullanılabilmesini sağlamak amacıyla ortaya konulan yeni uluslararası düzenlemeler incelenmiştir. Çalışmada, literatür taraması ve araştırma, uluslararası örneklerin incelenmesi ve Türkiye'de mevcut düzenlemelerin değerlendirilmesi yöntemi benimsenmiştir.

Büyük veri alanında Türkiye'de üst politika hedefleri bulunmasına rağmen bu alandaki araştırma ve uygulama örneklerinin sınırlı kaldığı, dolayısıyla büyük verinin, ortaya çıkardığı riskler boyutuyla yeterince değerlendirilemediği ve veri mahremiyeti politika ve düzenlemelerinin ele alınmasında büyük verinin getirdiği yenilikçi değişimin dikkate alınmadığı görülmüştür. Bu çerçevede, Türkiye'de ihtiyaç duyulan hukuki altyapıya ilişkin öneriler geliştirilmiş ve ayrıca, mevcut düzenlemelere ilişkin değerlendirmeler yapılarak, Türkiye'de yapılan çalışmalara katkıda bulunulması amaçlanmıştır.

Anahtar Kelimeler: büyük veri, mahremiyet, kişisel verilerin korunması, algoritma, gizlilik, bilgi ve iletişim teknolojileri, veri hukuku, yenilikçi teknolojiler

ABSTRACT

Strategy and Budget Expertise Thesis

PERSONAL DATA PRIVACY IN BIG DATA APPLICATIONS

Ayşe Nur AKINCI

Exponential increase of digital data produced all around the world has triggered development of big data applications, which paves the way for storage, management, processing and analysis of data in large volume, velocity, and variety. Thanks to big data technologies effective use of large amounts of data has produced user satisfaction, competitive advantage and high profitability through improvements in business processes, increasing efficiency, and improved quality of service provision.

Today, thanks to big data, which brings about significant economic and social benefits, it is possible to have as much knowledge as ever about individuals. This situation raises a number of challenges with regard to implementation of data privacy rules. It seems unlikely that development of big data and confidence in the relevant sectors will be possible without resolving the problems in the field of privacy. In this context, it has emerged as a reflection of this fact that many countries have began a comprehensive review process in policies and legislations since 2012. Indeed, big data deeply affects fair data processing principles on which modern privacy regulations are built.

Within the scope of this study, it was aimed to identify problems emerged in the field of privacy due to big data and to develop proposals. In this context, new international data privacy regulations were examined in order to eliminate the challenges with regard to data privacy posed by big data and ensure a successful implementation thereof. With regard to the methodology, literature survey and analysis, examination of international cases and assessment of Turkey's current regulation framework have been adopted.

Despite presence of the higher policy objectives in Turkey, it has been observed that research and implementations in this field are limited; therefore, big data could not be adequately considered in terms of the risks that it reveals. It has also been seen that the innovative changes offered by big data have not been taken into consideration while addressing data privacy policies and regulations. In this context, proposals are developed for legal infrastructure needed in Turkey, and it is intended to contribute to the studies in Turkey through assessment of current regulations.

Keywords: big data, privacy, personal data protection, algorithm, information and communication technologies, data law, innovative technologies

İÇİNDEKİLER

Sayfa No

TEŞEKKÜR i
ÖZET ii
ABSTRACT iii
İÇİNDEKİLER iv
TABLOLAR viii
ŞEKİLLER ix
GRAFİKLER x
KUTULAR xi
KISALTMALAR xii
TANIMLAR xv
GİRİŞ 1
1. BÜYÜK VERİ 4
1.1. Kavramsal Çerçeve 4
1.1.1. Büyük verinin tanımı 5
1.1.2. Büyük verinin bileşenleri 6
1.2. Büyük Verinin İşlenmesi ve Teknolojik Çözümler 11
1.2.1. Bulut bilişim 12
1.2.2. Büyük veri işleme platformları 13
1.2.3. NoSQL veritabanları 14
1.3. Büyük Verinin Uygulama Alanları, Zorlukları ve Riskleri 15
1.3.1. Büyük verinin uygulama alanları 15
1.3.2. Büyük verinin beraberinde getirdiği zorluklar 19
1.3.3. Büyük verinin riskleri 21
1.4. Büyük Verinin Ekonomik Boyutu 24
1.4.1. Büyük verinin ticari amaçlarla kullanımı 25
1.4.2. Büyük verinin rekabet üzerindeki etkileri 26
1.4.3. Büyük veride tüketicinin korunması 30
1.4.4. Büyük veride işgücü/insan kaynağı 31

Sayfa No

2. BÜYÜK VERİ UYGULAMALARININ VERİ MAHREMİYETİ KURALLARI BAĞLAMINDA DEĞERLENDİRİLMESİ 33

2.1. Dijital Çağda Güvenlik ve Mahremiyet İhtiyacı 33

2.1.1. Büyük veri ile ortaya çıkan güvenlik ve mahremiyete ilişkin kaygılar 34

2.1.2. Güvenlik ve mahremiyetin tesisi için yapılması gerekenler 44

2.1.3. Geleceğe ilişkin hukuki senaryolar 45

2.2. Büyük Veri Uygulamalarının Veri Koruma Hukukuna Etkileri 47

2.2.1. Büyük veri çağında mahremiyet 47

2.2.2. Sınır ötesi mahremiyet 48

3. DÜNYADA VE TÜRKİYE'DE KAMU HİZMETLERİNİN SUNUMUNDA BÜYÜK VERİYE İLİŞKİN TEMEL POLİTİKA VE UYGULAMALAR 49

3.1. Avrupa Birliği 49

3.2. Birleşmiş Milletler 51

3.3. Amerika Birleşik Devletleri 53

3.4. Türkiye'de Büyük Veriye İlişkin Mevcut Durum 53

4. ULUSLARARASI ALANDA VE KARŞILAŞTIRMALI HUKUKTA VERİ MAHREMİYETİ 57

4.1. Veri Koruma Hukuku Bağlamında Mahremiyet Hakkı 57

4.2. Dünyada Kişisel Verilerin Korunması Alanında Mevcut Hukuki Düzenlemeler 59

4.2.1. Birleşmiş Milletler 61

4.2.2. Avrupa Konseyi 61

4.2.3. İktisadi İşbirliği ve Kalkınma Teşkilatı 64

4.2.4. Avrupa Birliği 72

4.2.4.1. 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif 72

4.2.4.2. Avrupa Birliği Genel Veri Koruma Tüzüğü 73

4.2.4.2.1. AB Veri Koruma Reformuna İlişkin Genel Bilgiler 76

4.2.4.2.2. AB Genel Veri Koruma Tüzüğü'nün Getirdiği Temel Değişiklikler 78

4.2.4.2.3. AB Genel Veri Koruma Tüzüğü'nün Kapsamı 78

4.2.4.2.4. AB Genel Veri Koruma Tüzüğü'ndeki Temel İlkeler 86

Sayfa No

4.2.4.3. Avrupa Birliği'nde veri korumaya ilişkin diğer düzenlemeler 88

4.2.5. Amerika Birleşik Devletleri....88

4.2.6. Çin Halk Cumhuriyeti 90

4.3. Büyük Veri Uygulamalarının Etkisiyle Veri Mahremiyeti Alanında Ortaya Çıkan Yeni Hukuki Yaklaşımlar....92

4.3.1. Avrupa Birliği 92

4.3.1.1. Veri Koruma Hukukunda büyük veriden doğan temel tartışma alanları 93

4.3.1.2. Veri Koruma Tüzüğü ile öngörülen çözüm önerileri 98

4.3.2. Amerika Birleşik Devletleri....109

4.3.3. İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD)....115

4.3.3.1. Veriye dayalı yenilikçiliğin mahremiyetle ilişkili muhtemel etkileri....118

4.3.3.2. Daha etkin bir mahremiyet koruması için yeni politika yaklaşımı önerileri....119

5. TÜRKİYE'DE VERİ MAHREMİYETİ 131

5.1. Türk Hukuku Bakımından Kişisel Verilerin Korunmasına İlişkin Düzenlemeler 131

5.1.1. Türkiye'de kişisel verilerin korunması ile ilgili ulusal politikalar....131

5.1.2. Türkiye'de kişisel verilerin koruması ile ilgili mevzuat 132

5.1.2.1. Anayasa'da kişisel verilerin korunması....132

5.1.2.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu 133

5.1.2.2.1. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Kapsamı134

5.1.2.2.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki Temel Kavramlar....135

5.1.2.2.3. 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki Temel İlkeler 138

5.1.2.2.4. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun AB Reformunun Getirdiği Yenilikler Bağlamında Değerlendirilmesi....140

5.1.2.3. Kişisel verilerin korunmasına ilişkin diğer düzenlemeler ...143

5.2. Türkiye'de Büyük Veri Uygulamalarının Veri Mahremiyeti Düzenlemelerine Etkileri 144

Sayfa No

5.2.1. Kişisel veri tanımı ve verinin işlenmesi bakımından değerlendirme . 144
5.2.2. İlgilinin açık rızası, amaçla sınırlılık ve sınırlı veri işleme ilkeleri bakımından değerlendirme 146
5.2.3. Verinin sınır ötesi aktarımı bakımından değerlendirme 147
5.2.4. Kanun'un geneline ilişkin hususlar 148
6. TÜRKİYE İÇİN DEĞERLENDİRME VE ÖNERİLER 150
SONUÇ 159
EKLER 162
KAYNAKLAR 174
DİZİN 183

TABLOLAR

Sayfa No

Tablo 1.1. Sabit Disk Veri Saklama Birimleri ve Fiziki Karşılıkları 8

Tablo 1.2. Büyük Veri ile Geleneksel Verinin Karşılaştırılması.....11

Tablo 2.1. İşletmelerin ve Bireylerin, Büyük Veriye Yönelik Algıları ile İlgili Anketlerin Temel Bulguları 40

Tablo 5.1. Kişisel Verileri Koruma İlkeleri Bakımından 6698 sayılı Kanun ile AB Genel Veri Koruma Tüzüğü'nün Karşılaştırılması 138

ŞEKİLLER

Sayfa No

Şekil 1.1. Büyük Verinin Üç Temel Bileşeni 7
Şekil 1.2. Büyük Verinin İşletmelere Sağladığı Avantajlar 27
Şekil 3.1. OECD Ülkelerinde Uygulanan Mahremiyet Politikaları 117
Şekil 3.2. Veriye Dayalı Yenilikçilik-Veri Değer Döngüsü 119

GRAFİKLER

Sayfa No

Grafik 1.1. Dünyada Dijital Verinin Yıllar İtibarıyla Artışı (2010-2025) 4

KUTULAR

Sayfa No

Kutu 1.1. Facebook'un Haber Akışı Deneyi 23
Kutu 2.1. Çin'de Uygulanan "Sosyal Kredi Sistemi".....43
Kutu 2.2. Varsayılan Bir Özellik Olarak Mahremiyet Koruması.....46

KISALTMALAR

AB	: Avrupa Birliği
ABAD	: Avrupa Birliği Adalet Divanı
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
API	: Uygulama Programlama Arayüzü (Application Programming Interface)
AYM	: Anayasa Mahkemesi
BCG	: Boston Danışmanlık Şirketi (Boston Consulting Group)
BİT	: Bilgi ve İletişim Teknolojileri
Bkz.	: Bakınız
BM	: Birleşmiş Milletler
BT	: Bilgi Teknolojileri
BTS	: Bilgi Toplumu Stratejisi
CBS	: Coğrafi Bilgi Sistemleri
DDS	: Dağıtık Dosya Sistemi
DoD	: Amerika Birleşik Devletleri Savunma Bakanlığı (Department of Defense)
DPIA	: Veri Koruma Etki Değerlendirmesi (Data Protection Impact Assessments)
DPO	: Veri Koruma Görevlisi (Data Protection Officer)
EC	: Avrupa Topluluğu (European Community)
e-DTr	: e-Dönüşüm Türkiye
e-Devlet	: Elektronik Devlet
e-Ticaret	: Elektronik Ticaret
FIPP	: Adil Veri İşleme Prensipleri (The Fair Information Practice Principles)
FTC	: Amerika Birleşik Devletleri Federal Ticaret Komisyonu (Federal Trade Comission)

GDPR	: Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation)
GPS	: Küresel Yer Belirleme Sistemi (Global Positioning System)
GWG	: Birleşmiş Milletler Küresel Çalışma Grubu (Global Working Group)
HDFS	: Hadoop Dağıtık Dosya Sistemi (Hadoop Distributed File System)
HIPAA	: Amerika Birleşik Devletleri Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Kanunu (Health Insurance Portability and Accountability Act)
IAPP	: Uluslararası Mahremiyet Uzmanları Birliği (International Association of Privacy Professionals)
IDC	: Uluslararası Veri Şirketi (International Data Corporation)
IoT	: Nesnelerin İnterneti (Internet of Things)
ITU	: Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
JHA	: AB Adalet ve İçişleri Konseyi (Justice and Home Affairs Council)
KDEP	: Kısa Dönem Eylem Planı
MAT	: Mahremiyet Artırıcı Teknoloji
MGI	: McKinsey Küresel Enstitüsü (McKinsey Global Institute)
MIT	: ABD Massachusetts Teknoloji Enstitüsü (Massachusetts Institute of Technology)
md.	: Madde
MOBESE	: Mobil Elektronik Sistem Entegrasyonu
M2M	: Makinalar Arası İletişim (Machine to Machine)
NASA	: ABD Ulusal Havacılık ve Uzay Dairesi (National Aeronautics and Space Administration)
NIH	: Amerika Birleşik Devletleri Ulusal Sağlık Enstitüsü (National Intitute of Health)
NSA	: Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı (National Security Agency)
OECD	: İktisadi İşbirliği ve Kalkınma Teşkilatı (Organization for Economic Co-operation and Development)

OTT	: Şebekeler Üstü (Over The Top)
STK	: Sivil Toplum Kuruluşu
SQL	: Yapılandırılmış Sorgu Dili (Structured Query Language)
TBMM	: Türkiye Büyük Millet Meclisi
T.C.	: Türkiye Cumhuriyeti
TCK	: Türk Ceza Kanunu
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
ve ark.	: ve arkadaşları
VKED	: Veri Koruma Etki Değerlendirmesi
WEF	: Dünya Ekonomik Forumu (World Economic Forum)
YPK	: Yüksek Planlama Kurulu

TANIMLAR

Anonimleştirme (anonymization): Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekmektedir.

Uygulama programlama arayüzü (Application Programming Interface-API): Bir yazılımın başka bir yazılımda tanımlanmış işlevlerini kullanabilmesi için oluşturulmuş tanımlar bütününü ifade etmektedir.

Bulanıklaştırma (pseudonymization): Bir kişinin kimliğinin artık veri üzerinden izi sürülemez hale getirilmesi amacıyla, kullanılan algoritma yardımıyla kişiyi belirleyici verilerin şifrelenmiş verilerle değiştirildiği teknik bir yöntem olarak tanımlanmaktadır.

Bulut Bilişim: İşlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde arttırılıp azaltılabildiği, kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür.

Dağıtık Mimari: Farklı nitelikte bilgisayarlardan oluşturulmuş bir bilgisayar ağı üzerinde uygulamaların dağıtılmış bir biçimde çalıştırılabilmesini sağlayan mimari yapıdır.

Kimliksizleştirme (de-identification): Kişisel verilerin bulanıklaştırma, şifreleme, anahtar kodlama ve veri paylaşımı gibi teknolojiler vasıtasıyla açık tanımlayıcılarından sıyrılması ve genelleştirilmesiyle kişiyi belirlenebilir kılan özelliklerinden arındırılması anlamına gelmektedir.

Kişisel verilerin ikincil kullanımı: Belirli bir amaç ile toplanan kişisel verilerin, başlangıçta toplandığından başka bir amaç için yeniden işlenmesini ifade etmektedir.

Nesnelerin İnterneti (IoT): Fiziksel ortamdaki nesnelerin iletişim ağlarına bütünleşik olarak fiziksel ortamları ve benlikleri ile ilgili verileri işlemeleri/üretmeleri olarak tanımlanmaktadır. Nesnelerin internetinde, farklı tipteki cihazlar (örnek sensörler, mobil telefonlar), hem diğer cihazlarla hem de internetle iletişim haline geçerek fiziksel dünyadaki değişimi gözeten veriler üretmektedir.

OTT (Şebekeler Üstü-Over The Top): İşletmecilerin şebekeleri üzerinden kullanıcılara sunulan, ancak şebeke sahibi işletmecilerin tasarım, sunum ve dağıtımında rol almadıkları ve dolayısıyla doğrudan gelir elde etmedikleri hizmetler, OTT hizmetleri olarak tanımlanmaktadır.

Programlama Dili: Bilgisayar programlarının yazıldığı yapısal dilleri ifade eder.

Sunucu: Ağ altyapısı ile bağlı olduğu diğer bilgisayarlara hizmet sunan bilgisayarı ifade etmektedir.

Varsayılan (data protection by default) ve Tasarımdan İtibaren Veri Koruması (data protection by design): Veri toplama ve analizi konusunda, güçlü mahremiyet önlemlerinin daha tasarım aşamasından itibaren dikkate alınması ilkesini ifade etmektedir. Söz konusu yaklaşım yedi temel ilkeden oluşmaktadır: reaktif değil proaktif-iyileştirici değil önleyici olma ilkesi, varsayılan ayar olarak mahremiyet ilkesi, tasarıma gömülü mahremiyet ilkesi, tam işlevsellik ilkesi, uçtan uca güvenlik ilkesi-tam yaşam döngüsü koruması, görünürlük ve şeffaflık ilkesi ve son olarak kullanıcı odaklı tutum-kullanıcı mahremiyetine saygı ilkesi.

Teknoloji tarafsız: Bir ilke ya da kuralın kullanılan teknolojiden bağımsız olarak uygulanma kabiliyetini haiz olmasını ifade etmektedir.

Veri Seti: Tablo formatında gösterilebilen düzenli veri kümesidir.

Verileştirme (datafication): Üretilen bütün bilginin ölçülebilir/nicel ve analiz edilebilir bir veri formatına dönüştürmesini ifade etmektedir.

Yapılandırılmış Veri: Belirli bir hiyerarşide tanımlı, biçimsel birimler halinde örgütlenmiş, dolayısıyla erişimi ve çözümlemesi geleneksel yöntemlerle en kolay ve hızlı biçimde gerçekleştirilebilen veriyi ifade etmektedir.

Yapılandırılmamış Veri: Belirli bir biçimsel kurala bağlı olmayan, işlenip çözümlenebilmesi için gelişmiş metin işleme, doğal dil işleme ve yapay zekâ gibi yeni yöntemlerin kullanılması gereken veri türünü ifade etmektedir.

Yarı-yapılandırılmış veri: Yapılandırılmış veri kadar tanımlı veri birimlerinden oluşmamakla birlikte belirli kurallar çerçevesinde, örneğin; etiketler ve veri sözlükleri aracılığıyla belirli bir seviyede erişim, derleme ve çözümleme sağlanabilen veriyi ifade etmektedir.

Yeniden kimliklendirme (re-identification): Veri bağlantı teknikleri yardımıyla bir verinin ilişkili olduğu bireylerin kimliğinin keşfi veya belirlenmesi olarak tanımlanmaktadır.

Geçmişte, insanlığın yapabilecekleri oldukça sınırlıydı... Bilgi düzeyindeki her artış insanlığın başarabileceklerini de artırmıştır. Bugünün ve muhtemelen geleceğin bilim dünyasında, atalarımızın en vahşi rüyalarının bile ötesinde, kötülerin daha büyük kötülükler; iyilerinse daha büyük iyilikler yapmaları mümkün olacaktır…

Bertrand Russell

GİRİŞ

Tarih boyunca ortaya çıkan her köklü yenilik, beraberinde tartışmaları da getirmiştir. Matbaanın icadından sonraki dönemde, gelecek nesillerin daha az bilme ihtiyacı hissedeceği ve ezber yeteneklerinin köreleceği endişesi hararetle tartışılırken; İkinci Dünya Savaşı sonrası toplumlar, nükleer silah teknolojisinin etkileri ve etiği üzerine uzun süre kafa yormuştur. Bertrand Russell'ın da ifade ettiği gibi bilgideki büyümeye karşılık olarak bilgelikte ilerleme olmaksızın tüm bu arayışlar nafile birer çaba olarak kalacaktır. Zira bilgiye irade ve duyguların, bir diğer deyişle bilgeliğin, eşlik etmediği her ilerleme insanlık için bir biçimde tehlike arz edebilme potansiyeline sahiptir. Elbette ki bu kaygı söz konusu teknolojileri göz ardı ederek ya da dışlayarak hayatın sürdürülmesini gerektirmemektedir. Zira bilgi ve iletişim teknolojilerindeki (BİT) gelişmeler gündelik hayatın rutinine oldukça sağlam bir şekilde yerleşmiş bulunmaktadır. Hızlı ve kullanışlı birer araç olarak benimsenen bu yenilikler, gün geçtikçe değerlenmektedir. Ancak söz konusu teknolojilerin 'nasıl' kullanıldıklarının ne denli önem arz ettiği ve ciddi sonuçlar doğurduğu unutulmamalıdır.

Teknolojik gelişmeler doğrultusunda giderek dijitalleşen ve hemen her şeyden verinin akmakta olduğu mevcut düzlemde, dünya her zamankinden daha hızlı, çeşitli ve büyük miktarlarda dijital veriyi barındırmaktadır. Büyük veri teknolojileri sayesinde söz konusu verilerin aynı hızla analizi de mümkün olmakta; algoritmaların daha doğru çıkarımlar yapması, isabetli kararlar vermesi, gizli içgörüleri keşfetmesi ve iş süreçlerinin otomatikleştirilmesi sağlanmaktadır. Böylece maliyetler düşürülmekte, sunulan ürün ve hizmetlerin kalitesi yükseltilmekte ve ekonomik büyüme hızı artmaktadır.

Büyük verinin beraberinde getirdiği sosyal ve ekonomik fayda bütün dünyada gerek özel sektör gerekse kamu verisinin büyük veri uygulamaları çerçevesinde değerlendirilmesi yaklaşımını ortaya çıkarmaktadır. Bu alana ilişkin ilk uygulama örnekleri büyük BİT firmalarının geliştiği Amerika Birleşik Devletleri (ABD) ve kişisel veriler bakımından önemli bir pazar teşkil eden Avrupa Birliği (AB) ülkelerinde ortaya çıkmıştır. Büyük veri alanındaki çalışmaların genel olarak özel sektör tarafından rekabet avantajı ve ticari amaçlarla ele alındığı, kamuda ise büyük veri

uygulamalarının geliştirilmesine yönelik üst politika hedefleri ile bu alanda araştırma ve uygulama çalışmalarının sürdürüldüğü görülmektedir.

Bununla birlikte, büyük veri, ortaya çıkardığı faydanın yanında işlenen verilerin büyük bir kısmının kişisel veriler olması dolayısıyla veri mahremiyeti kurallarının uygulanması bakımından birtakım zorlukları beraberinde getirmiştir. Bu durum başta İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD), AB ve ABD gibi politika yapıcı kurum, kuruluş ve ülkeleri yeni bir düzenleyici tepki ortaya koymaya teşvik etmiş, bu çerçevede kapsamlı güncelleme çalışmaları hızlıca ortaya konulmuştur. Zira büyük veri çağı henüz başlamasına rağmen bu teknolojinin veri mahremiyeti bakımından ortaya çıkardığı sorunlara ilişkin çözüm önerilerinin bir an önce geliştirilmesi önem arz etmektedir.

Bu çalışma kapsamında, büyük veriyle giderek daha da karmaşık bir hal alan veri mahremiyeti konusunda, dünyada bu sorununun ele alınışındaki temel yaklaşımlar irdelenmektedir. Literatür taraması ve ülke incelemeleriyle Türkiye'de büyük verinin mahremiyet alanında ortaya çıkardığı sorunların tespit edilmesi ve çözüm önerileri geliştirilmesi amaçlanmaktadır. Bu kapsamda, büyük verinin, veri mahremiyeti alanında ortaya çıkardığı riskler boyutuyla değerlendirilmesiyle bu alana ilişkin temel politika ve düzenlemelerde belirlenen yeni ihtiyaçlar irdelenmekte ve bu alanda atılması gereken adımlar ele alınmaktadır. Sonuç olarak, Türkiye'de ihtiyaç duyulan hukuki altyapının geliştirilmesi ve ayrıca, mevcut düzenlemelere ilişkin değerlendirmeler yapılarak Türkiye'de yapılan çalışmalara katkıda bulunulması öngörülmektedir.

Beş bölümden oluşan tezin birinci bölümünde büyük veri kavramı ile bileşenleri açıklanmaktadır. Bu alanda benimsenen teknolojik çözümler ele alınmakta, ardından büyük verinin uygulama alanları, zorlukları ve risklerine değinilmektedir. Bu bölümde, ayrıca, büyük verinin ekonomik boyutu, ticarileşmesi, rekabet üzerindeki etkileri, tüketicinin korunması ve bu alandaki insan kaynağı ihtiyacı konularına ilişkin yaklaşımlar ele alınmaktadır.

İkinci bölümde, büyük veri uygulamalarının veri mahremiyeti kurallarına etkilerinin değerlendirilmesi amacıyla, dijital çağda güvenlik ve mahremiyet alanında

ortaya çıkan yeni ihtiyaçlar ele alınarak, büyük veri bakımından güvenlik ve mahremiyete ilişkin kaygılar incelenmektedir. Bu alanda güvenlik ve mahremiyetin tesisi için atılması gerekli adımlar ve geleceğe ilişkin hukukî öngörüler değerlendirilmektedir. Büyük veri çağında mahremiyetin sınır ötesi mahiyeti de bu bölümde ele alınmaktadır.

Üçüncü bölümde, Avrupa Konseyi, OECD ve AB gibi uluslararası kuruluşlarda ve karşılaştırmalı hukukta veri mahremiyetine ilişkin kavramsal çerçeve ele alınmakta, bu alandaki hukuki düzenlemeler incelenmektedir. Ayrıca, büyük veri uygulamalarının etkisiyle veri mahremiyeti alanında dünyada ortaya çıkan yeni hukuki yaklaşımlar bu bölümde yer almaktadır.

Dördüncü bölümde, Türkiye'de üst politika belgelerinde ve hukuki düzenlemelerde yer alan veri mahremiyetine ilişkin temel hususlar ele alınmaktadır. Ardından, Türkiye'de büyük veri uygulamalarının veri koruma hukukuna etkileri bakımından bir değerlendirme yapılmakta, bu bağlamda mevcut düzenlemelerin söz konusu sorun alanını çözümlemekte yeterli olup olmadığı irdelenmektedir.

Son bölümde ise, büyük verinin veri mahremiyetine ilişkin ortaya çıkardığı zorlukların giderilerek başarılı bir şekilde uygulanabilmesini sağlamak amacıyla çalışma kapsamında incelenen uluslararası düzenlemeler ile Türkiye'deki mevcut durum ve gelişmeler çerçevesinde önerilere yer verilmektedir.

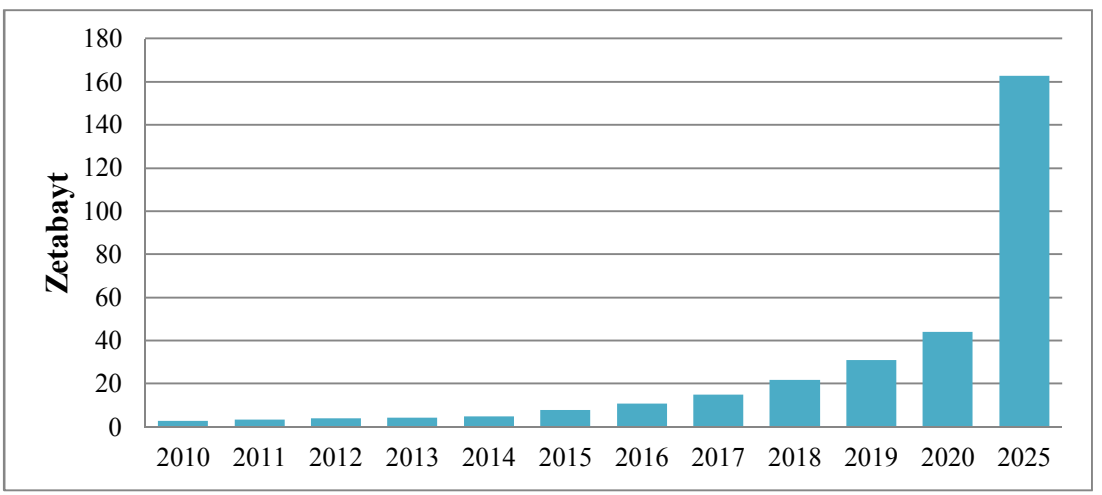
Ayrıca, doğrudan bu çalışmanın kapsamında yer almamakla birlikte yapılan incelemelerde, Türkiye'de özellikle kamu sektörü bakımından büyük veri alanındaki uygulama ve araştırma örneklerinin sınırlı olduğu görülmüştür. Bununla birlikte ülke pazarında faaliyet gösteren küresel BİT firmalarının ise bu alandaki etkinliklerini sürdürdüğü bilinmektedir. Konunun gerek ortaya çıkarılacak fayda gerekse bu alandaki riskler boyutuyla daha detaylı değerlendirilebilmesi, kamunun bu alanda yapacağı çalışmalarla hızlanacaktır.

1. BÜYÜK VERİ

1.1. Kavramsal Çerçeve

Bilgisayarların, internetin ve teknolojik altyapının hızlı gelişmesi sayesinde giderek dijitalleşen, hemen her şeyin birbiriyle bağlı olduğu bir çağ yaşanmaktadır. Dünya genelinde üretilen dijital veri her iki yılda bir ikiye katlanmaktadır. Şu anda, 10 yıl önce depolanabilen tüm dijital verinin 32 katı, 20 yıl öncekinin 1024 katı veri depolanabilmektedir. Yalnızca 2013 yılında üretilen dijital veri yaklaşık 4,4 zetabayttır. Bu değer $44*10^{19}$ bit'e ya da 1,4 milyar akıllı telefonun depolama kapasitesine eşittir. Söz konusu verinin 2020 yılında 45 zetabayt, 2025 yılında ise 163 zetabayt olacağı tahmin edilmektedir (Grafik 1.1).[1] İnternete bağlı olsun olmasın herhangi bir dijital ortam üzerinde gerçekleştirilen her işlem ardında bir veri kaydı bırakmaktadır.

Grafik 1.1. Dünyada Dijital Verinin Yıllar İtibarıyla Artışı (2010-2025)



Kaynak: International Data Corporation (IDC), 2017.

Büyük verinin ortaya çıkışında; akıllı telefonlardan, kredi kartlarından, sensörlerden, fare tıklarından, televizyonlardan, araçlardan, güvenlik kameralarından/mobeselerden başka bir deyişle hemen hemen her yerden hızla akan ve üstel olarak artan veriler temel tetikleyici olmuştur. Mevcut teknolojik düzlemde, bu veri kalabalığının büyük bir kısmı hala kullanılamaz bir nitelik arz ediyor olsa da, bu durum, nicelik ve nitelik itibarıyla katlanarak büyüyen verinin çok yakın bir

[1] IDC, 2017: 7

gelecekte önemli gelişmelere neden olacağı gerçeğini değiştirmemektedir. Zira bugün insanlığın elinde bulundurduğu verinin yalnızca yüzde birini analiz edebildiği düşünüldüğünde analiz edilemeyen veri yığınlarının önemli fırsatları bünyesinde barındırdığı öngörülebilmektedir.[2]

1.1.1. Büyük verinin tanımı

Son yıllarda özel sektör, akademi ve kamunun büyük ilgi gösterdiği konulardan biri haline gelen büyük veri, terim olarak ilk kez 1997'de NASA'da çalışan Michael Cox ve David Ellsworth isimli iki bilim adamı tarafından kullanılmıştır. Cox ve Ellsworth, büyük verilerin görselleştirilmesi konusunda yaşadıkları problemi; *"veri setleri, ana belleğe, yerel diske ve hatta uzaktaki diske dağılmış bir biçimde o kadar geniştir ki bilgisayar sisteminin bu durumu çözebilmesi büyük bir zorluk teşkil etmektedir."* şeklinde ifade etmiştir. İkili, karşılarına çıkan bu durumu ise "büyük veri sorunu" olarak adlandırmıştır. Veri setleri ana belleğe (çekirdeğe) ve hatta yerel diske sığmadığında en yaygın çözümün, daha fazla depolama kaynağı edinmek olduğu ifade edilmiştir.[3]

Günümüzde "sensörlerden ve çeşitli araçlardan gelen hacmi büyük, çeşidi bol, düzensiz, sorunlu ve hızla gelen veriyi; toplama, saklama, temizleme, görselleştirme, analiz etme ve anlamlandırma bilimi" olarak ifade edilen büyük veri, köklü bir devrim olarak görülmektedir.[4] Devasa boyutlara ulaşan verilerin anlamlı ve işlenebilir biçime dönüştürülmüş halini ifade eden bu olgu, 21. yüzyılın ilk on yılında meydana gelen gelişmelere bağlı bir seyir izlemiştir. Bu kavram, uzun zamandan beri gelişme gösteren teknolojilerin günümüzde ekonomik ve sosyal fayda için kullanılabilirlik eşiğinin aşılmasıyla ortaya çıkmıştır. McKinsey Global Institute (MGI) tarafından 2011 yılında yayımlanan Büyük Veri Raporu'da ifade edildiği haliyle büyük veri, yeni teknoloji ve algoritmalar kullanılarak, geleneksel verilere göre farklı şekilde toplanması ve analiz edilmesi gereken çok büyük veri kümelerini ifade eden bir endüstriyel terim olarak kabul edilmekte; "boyutları geleneksel veri tabanı yazılım araçlarının tutma,

[2] Gürsakal, 2014: 9
[3] Friedman, 2012: 2
[4] Mayer-Schönberger veCukier, 2013: 1

depolama, yönetme ve analiz etme yeteneğini aşan veri setleri" şeklinde tanımlanmaktadır.[5]

Yüksek hacimdeki verinin işlenerek daha doğru çıkarımların yapılması, gerek kamu gerekse özel sektörde daha sağlıklı kararların verilmesi, gizli içgörülerin keşfi ve iş süreçlerinin otomatikleştirilmesini sağlamaktadır. Bu sayede maliyetlerin düşürülmesi, sunulan ürün ve hizmetlerin kalitesinin yükseltilmesi ve ekonomik büyüme hızının artırılması mümkün hale gelmektedir. Zira dünya, her zamankinden daha hızlı ve büyük miktarlarda dijital veriyi barındırmaktadır. Bu çerçevede büyük veri, "toplumun faydalı fikirler veya değerli mal ve hizmetleri üretmek için bilgiyi yeni yollarla harekete geçirme kabiliyeti" ve "yeni anlayışlar ortaya çıkarmak veya değer biçimleri oluşturmak için daha küçük ölçeklerde yapılamayacak şeylerin büyük ölçekte yapılması" olarak tanımlanmaktadır.[6]

Görüldüğü üzere, gerek uygulamada gerekse akademik çevrelerde büyük verinin pek çok tanımı yapılmaya çalışılmaktadır. Ancak, bu tanımın üzerinde halen uzlaşıya varılamamış olmasının arkasında; söz konusu olgunun başta veri bilimi, yapay zekâ ve nesnelerin interneti (Internet of Things-IoT) gibi birçok dijital dönüşüm dalgasıyla yakın ilişki içinde olması yatmaktadır. Dolayısıyla, bu olguya ilişkin kavramsal açıklamaların önümüzdeki yıllarda da değişim geçirmeye ve yeniden düşünülmeye devam edeceği değerlendirilmektedir. Bu sebeple doktrinde büyük verinin tanımsal öneminden ziyade içeriğine ve getirdiği yeni anlayışa odaklanılması gerektiği savunulmaktadır. Zira büyük veri sözcüğünün etkisinin uzun sürmemekle birlikte son dönemde hayatımıza giren geniş ve yeni veri türlerinin etkisinin uzun süreceğine dikkat çekilmektedir.[7]

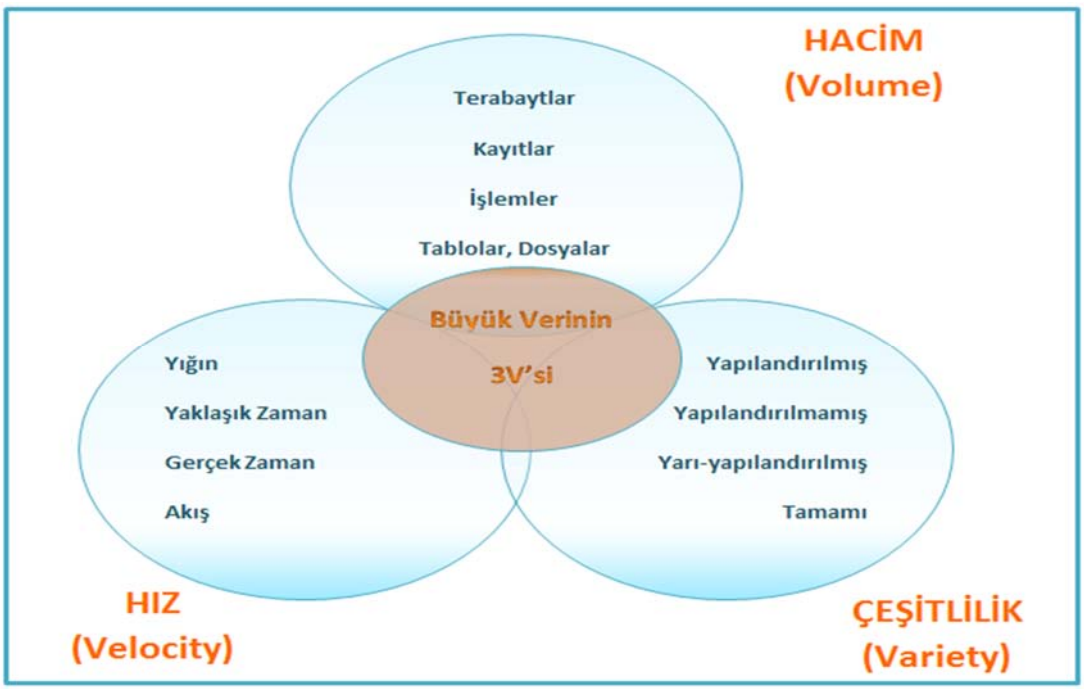
1.1.2. Büyük verinin bileşenleri

Büyük veri kavramının anlaşılabilmesi bakımından bu verilerin işlenmesi, anlamlandırılması ve kullanılabilmesindeki temel bileşenlerin ayrı ayrı açıklanması gerekmektedir. Gartner tarafından 2012 yılında kısaca 3V olarak ifade edilen bu

[5] MGI, 2011: 1
[6] Cukier ve Mayer-Schönberger, 2013: 2
[7] Davenport ve ark., 2012: 43–46

bileşenler; verinin hacmi (volume), hızı (velocity) ve çeşitliliği (variety) olarak kabul edilmektedir (Şekil 1.1).

Şekil 1.1. Büyük Verinin Üç Temel Bileşeni



Kaynak: Dridi ve ark., 2015.

i. *Verinin hacmi/büyüklüğü:* Çevrimiçi gerçekleştirilen faaliyetler, küresel yer belirleme sistemi (Global Positioning System-GPS) donanımlı akıllı telefonların ürettiği konum verileri, sosyal medya etkileşimleri veya akıllı uygulamaların hayatın her alanında kullanımı ile her saniye veri üretilmektedir. Bilinçli bir faaliyet sonucu üretilen bu veri yığınına bir de makinalarca otomatik olarak üretilen verinin eklenmesiyle bu miktar hızla artmaktadır. Örneğin; akıllı ev aletlerinin birbirleriyle ve internet servis sağlayıcısıyla gerçekleştirdiği veri iletimi oldukça büyük miktarda verinin üretilmesi ve paylaşılması anlamına gelmektedir. Bugün dünyada kullanılan pek çok tarım arazisi ve endüstriyel üretim tesisi veri toplama ve iletme amacıyla akıllı sensörlerle donatılmış durumdadır. Pilot uygulamalarına başlanan sürücüsüz otomobiller yakın bir gelecekte sokaklara çıkacak ve nereye giderlerse gitsinler çevrelerini gerçek zamanlı, dört boyutlu haritalarla algılayarak ve karar alarak hedeflerine

ulaşacaklardır. Sürekli büyüyen bu sensör bilgileri, fotoğraflar, metin, ses ve video tabanlı veriler büyük verinin temelini oluşturmaktadır.

Artan veri hacminin ölçülmesi amacıyla IDC tarafından 2017 yılında yayımlanan "Veri Çağı 2025 Raporu"na göre 2005 yılında küresel ölçekte 130 exabayt veri oluşturulmuş ve depolanmıştır. 2010 yılına gelindiğinde bu miktar 1.227 exabayta, 2015 yılında ise 7.910 exabayta yükselmiştir. Veri saklama birimlerinin fiziki dünyada karşılık geldiği durum Tablo 1.1'de gösterilmektedir. Büyük veri için verilebilecek en güncel örneklerden bir diğeri ise Avrupa Nükleer Araştırma Merkezi'nin yaptığı Büyük Hadron Çarpıştırıcısı deneyidir. Söz konusu çalışmada saniyede 40 terabyte veri üretilmektedir.[8]

Tablo 1.1. Sabit Disk Veri Saklama Birimleri ve Fiziki Karşılıkları

Birim	Birim karşılığı	Birimin fiziki karşılığı
8 Bit	1 Bayt	
1024 Bayt	1 Kilobayt	
1024 Kilobayt	1 Megabayt	
1024 Megabayt	1 Gigabayt	1 adet flash bellek
1024 Gigabayt	1 Terabayt	1 adet harici bellek (hard disk)
1024 Terabayt	1 Petabayt	2 veri merkezi kabinine yerleştirilen 16 adet backplaze saklama podu
1024 Petabayt	1 Exabayt	Bir şehir bloğunu oluşturan 4 katlı binaya sığabilecek büyüklükteki 2000 veri merkezi kabini
1024 Exabayt	1 Zetabayt	Exabaytla ifade edilen binaların 1000 katı, Manhattan'ın yüzde 20 alan büyüklüğü
1024 Zetabayt	1 Yotabayt	Delaware ve Rhode Island eyaletlerini kaplayacak büyüklükte bir milyon veri merkezi
1024 Yotabayt	1 Brontobayt	
1024 Brontobayt	1 Geopbayt	

Kaynak: Cognizant, "Making Sense of Big Data in the Petabyte Age", 2011, (çevrimiçi) https://www.cognizant.com/InsightsWhitepapers/Making-Sense-of-Big-Data-in-the-Petabyte-Age.pdf, 21.06.2016.

[8] Cukier, 2010: 198

Başlangıçta kilobaytlarla ifade edilen veri disketlerde, megabaytla ifade edilenler hard disklerde, terabaytlar disk dizilerinde saklanabilirken petabaytlar ancak bulutta saklanabilmektedir. Zengin kaynaklardan gelen veri miktarı arttıkça kullanılan teknoloji değişmekte, dosya isimlendirmesinden dosya kabinine ve oradan kütüphanelere gelinmektedir.[9]

Bir olgu ya da durum hakkında ne kadar çok veriye sahip olunursa, o kadar güvenilir bir şekilde yeni bilgiler edinilebileceği ve geleceğe ilişkin öngörüler konusunda o kadar isabetli kararlar alınabileceği ifade edilmektedir. Daha fazla veri noktası karşılaştırılarak daha önce kurulamayan ve/veya gizli olan ilişkiler ortaya çıkarılabilmekte, söz konusu çıkarımlar ise verilen kararları değiştirebilmektedir. Bu gerekçelerle veri hacminin önem arz ettiği ifade edilmektedir.[10]

Bununla birlikte, çoğunlukla en fazla ilgiye mazhar olan bileşen veri hacmi olsa da büyük verinin en doğru biçimde tanımlanması bakımından üç temel bileşenin (hacim, çeşitlilik, hız) bir arada bulunması gerektiği değerlendirilmektedir. Ayrıca, büyük verinin bileşenlerinin hacim, hız, çeşitlilik, *değer* ve *doğruluk* (volume, velocity, variety, value and veracity-5V) olmak üzere beş adet olduğunu savunan görüşler de mevcuttur.[11]

ii. Verinin hızı: Bu kavram, verinin ne sıklıkla iletildiği, depolandığı ve hangi hızla alınabildiğiyle ilişkilidir. Bu bağlamda örneğin; finans, ulaştırma, enerji, perakende ve çevrimiçi reklamcılık gibi anlık gelişmelerin önem arz ettiği sektörler bakımından verinin hızlı bir biçimde ve doğru işlenmesi hayati bir önemdedir. Bununla birlikte, verinin akış hızı oldukça önemli bir oranda artarken geleneksel hesaplama ve iletişim araçlarıyla bu denli büyük bir hızda akan veriye cevap verebilme yeteneği sınırlı kalmıştır.[12]

Geleneksel yöntemlerde, veri toplanır ve analiz edilmek üzere saklanır, daha sonrasında ise "zamanı geldiğinde" analiz edilirdi. Ancak mevcut teknolojik

[9] Anderson, 2008: 1
[10] Cukier, 2010: 19
[11] Demchenko, 2013: 8
[12] Vashist, 2015: 15

gelişmeler verinin toplanması ve analiz edilmesi arasındaki süreyi öyle kısaltmaktadır ki, "gerçek zamanlı analiz" (örneğin; trafik yoğunluğuna göre yeşil ışık sürelerinin belirlendiği tam adaptif trafik kontrol sistemleri) önemli bir nitelik halini almaktadır. Çünkü artık veriden değer yaratabilmenin en önemli göstergelerinden biri, veriyi toplandığı anda, eşzamanlı olarak analiz edebilme becerisidir. Verinin hızla aktığı ve yalnızca işlemsel sistemlerden değil, aynı zamanda sosyal medya güncellemeleri, sensör verileri, müzik, video, internet sayfası hareketleri gibi pek çok kaynaktan gerçekleşen bir akışın içerisinde bunu sağlamak oldukça zor olmaktadır.

Büyük veride akış halindeki verinin gerçek zamanlı analiz edilmesi anlamında öne çıkan örneklerden biri ABD'de uygulanmakta olan "Bunu hissettiniz mi?" isimli jeolojik araştırmadır. Söz konusu araştırmada Twitter üzerinden verilen tepkilerden oluşan internet yoğunluk haritaları ile bilimsel yollarla toplanan gerçek deprem verileri eşanlı olarak analiz edilmektedir.[13] Böylece sismik araçların mevcut olmadığı alanlara ilişkin değerlendirme yapılabilmiş, normalde kaydedilmesi mümkün olmayan küçük ölçekte depremler kaydedilmiş, acil müdahaleler için sarsıntı ve hasar derecesi hızlıca değerlendirilmiş ve deprembilimcilerin doğru öngörülerde bulunmasını sağlayan detaylı bilgiler elde edilmiştir.

iii. *Veri çeşitliliği:* Büyük veri kümeleri mobil cihazlar, bütünleşik devreler, sosyal medya kaynakları ve sensörler gibi pek çok farklı kaynaktan alınmaktadır. Bu kaynaklardan alınan veriler sosyal ağ mesajları, güncelleme ve görüntüleri; giyilebilir teknolojiler üzerindeki sensörlerden alınan kat edilen mesafe, süre, harcanan kalori bilgileri; cep telefonları ve diğer giyilebilir cihazların GPS sinyalleri; çevrimiçi alışverişler ve tüketim tercihleri ve nihayet pasif durumda bile veri üretmekte olan akıllı binalar, toplu taşıma araçları veya video kameralarından toplanan veriler gibi pek çok farklı formatta bulunmaktadır. Söz konusu veriler yapılandırılmış, yapılandırılmamış yahut yarı-yapılandırılmış olmak üzere pek çok farklı tür ve biçimde akmaktadır. Bu veri çeşitlerinin farklı dillerde ve farklı karakter kodlarında olabileceği de düşünüldüğünde, söz konusu

[13] Atkinson ve Wald, 2007: 362–368

verilerin bütünleşik hale getirilmesi ve birbirlerinin formatına dönüştürülmesi ihtiyacı bulunmaktadır.[14]

Bilhassa internet teknolojisinin yaygınlaşmasıyla birlikte yapılandırılmamış veri miktarı hızla artmaktadır. Dijital evrende yapılandırılmamış verinin oranının yüzde 90'ın üzerinde olduğu ifade edilmektedir.[15] Geleneksel analitik platformlar farklı çeşitlilikteki verilerle aynı anda baş edememekte ve geleneksel veritabanları farklı formattaki veriyi depolayamamaktaydı (Tablo 1.2.). Dolayısıyla, büyük veri teknolojilerinden önce, yapılandırılmamış veri yok sayılmakta veya çok düşük bir verimle kullanılabilmekteydi. Bugün ise, NoSQL yapısı kullanılarak tasarlanan veri tabanlarındaki yapısal olmayan veriler, veri madenciliği yöntemleri ve Hadoop ve MapReduce[16] gibi yeni tekniklerle yönetilebilir, işlenebilir ve analiz edilebilir hale gelmektedir.

Tablo 1.2. Büyük Veri ile Geleneksel Verinin Karşılaştırılması

	Geleneksel Veri	**Büyük Veri**
Veri tipi	Yapılandırılmış	Yapılandırılmış, yarı-yapılandırılmış, yapılandırılmamış
Veri hacmi	Terabaytlar	Petabaytlar ve exabaytlar
Veri yapısı	Merkezileştirilmiş	Dağıtık
Verilerin ilişkisi	Belirsiz	Karmaşık

1.2. Büyük Verinin İşlenmesi ve Teknolojik Çözümler

Büyük veri terimi sadece verinin kendisini değil aynı zamanda bu alandaki teknolojileri, sorunları ve yöntemleri de içermektedir. Bu kapsamda, verilerin sahip olduğu büyüklük, hız ve karmaşıklık gibi özellikleri nedeniyle depolanması ve analiz edilebilmesi bakımından geleneksel yöntemlerin ötesinde bir teknolojiye ihtiyaç duyulmaktadır.

Genellikle birbirlerinden farklı veri kaynaklarından toplanan geniş veri kümelerinin depolanması, işlenmesi ve analizi ile ilgili büyük veri çözüm ve

[14] Ünal, 2015: 10
[15] Ganz ve Reinsel, 2011: 2
[16] NoSQL, Hadoop ve MapReduce terimleri çalışmanın.1.2 no'lu bölümünde açıklanmaktadır.

uygulamalarının karakteristik, başka bir deyişle kendine özgü olması gerekmektedir. Özel olarak büyük veri, çoklu ilişkisiz veri kümelerinin birleştirilmesi, büyük miktarda yapısal olmayan verinin işlenmesi ve gizli bilginin kısıtlı zaman içinde toplanması gibi farklı gereksinimleri bünyesinde barındırmaktadır.[17]

Büyük veriyle ilgili sorunların çözümüne iki büyük teknolojik gelişmenin katkı sağladığı ifade edilmektedir.

Bu teknolojik gelişmelerden birincisi, bulut tabanlı çözümlerin ortaya çıkmasıyla veri depolama maliyetlerinin önemli ölçüde düşmesi ve ticari veri tabanlarının kullanımının yaygınlaşmasıdır. Açık kaynaklı veya belirli firmalara ait sanal dosya sistemleri şeklinde yönetilen yapılardan bilişim ihtiyaçlarının karşılanması ile hizmet tabanlı işletmeciliğe geçiş hızlanmıştır.[18]

İkincisi ise, büyük hacimli verilerin analizi amacıyla basit donanımların dağıtık dosya sistemleri ile birleşiminden oluşan yeni teknolojik çözümlerin oluşturulmasıdır. Bu çözümlerin başında; Google tarafından sorunları farklı birimlere bölerek hızlı işlemek için geliştirilen MapReduce, Facebook tarafından kullanılan Hadoop kümesi, Twitter'ın gerçek zamanlı veri işleme olanağı sağlayan Storm'u ve SAP firması tarafından geliştirilen ve verileri disk ortamında saklamak yerine ana bellekte daha hızlı işlemeye olanak sağlayan Hana gelmektedir. Söz konusu teknolojiler arasında Hadoop ve NoSQL (Not only SQL) günümüzde en yaygın olarak kullanılanlardır.

Gün geçtikçe etkinliği artan bulut bilişim ve dağıtık veri işleme teknolojileri aşağıda ayrıntılı olarak açıklanmakta olup, söz konusu teknolojilere ek olarak nesnelerin interneti, yapay zekâ, veri madenciliği, makina öğrenmesi, yapay sinir ağları gibi kavramlar büyük verinin saklanması ve analizine zemin hazırlayarak büyük veri setlerinin ortaya çıkmasını mümkün kılmıştır.

1.2.1. Bulut bilişim

Büyük verinin işlenmesiyle yakından ilişkili gelişmelerin başında, devasa büyüklükteki verilerin depolanabilmesi için gerekli olan depolama aygıtları gelmektedir. Veri miktarındaki artışın üstel olması dolayısıyla bu artıştaki veriyi

[17] Erl ve ark., 2016: 19
[18] Altunışık, 2015: 45

depolamak için teknolojik gelişmelerin de süreklilik arz etmesi gerektiği ifade edilmektedir. Zira özellikle fotoğraf, ses ve videolar veri hacmini genişletmekte ve depolama alanına olan ihtiyacı artırmaktadır.

2000'li yılların başındaki veri depolama ve işleme teknolojileri, gerek etkinlik gerekse maliyet açısından işletmelerin veri işleme ve analizini zahmetli ve pahalı hale getirmekteydi. Google, Amazon, Facebook ve Twitter gibi büyük BİT firmaları, karşılaştıkları bu sorunlara yönelik geçici çözümler bulmak zorunda kalmıştır. Bu aşamada ortaya çıkan bulut tabanlı çözümler, veri depolama maliyetlerini önemli ölçüde düşürmüş ve ticari veri tabanlarının kullanımına imkân sağlamıştır. Bu özelliğiyle bulut bilişim büyük veri teknolojilerini yakından ilgilendiren önemli bir teknolojik gelişimdir. Zira bulut bilişimin, depolama ve bilişim gücü konusunda sınırları büyük ölçüde esnetmesi büyük veriyi desteklemektedir. Son yıllarda verilerin, boyut, çeşitlilik ve karmaşıklık anlamında sürekli büyümesi ve büyümeye devam edecek olması, bulut bilişimle birlikte büyük veri konusunu bir sorun olmaktan çıkarıp bir çözüm odağı haline getirmektedir.

1.2.2. Büyük veri işleme platformları

Büyük veri uygulamaları, büyük verinin kendine has özellikleri nedeniyle, veri işleme ve saklama için yeni yöntem, araç ve tekniklere ihtiyaç duymaktadır. Zira yüksek hızlı verinin değerini yitirmeden işlenerek üretim süreçlerinde kullanılması verimlilik açısından kritik öneme sahiptir. Günümüzde, veri üzerinde daha hızlı ve daha verimli işlemler yapabilmesi için özellikle dağıtık mimarileri kullanabilen yeni araçlar üretilmesi ihtiyacı ortaya çıkmıştır. Bu doğrultuda, büyük verinin hacim, hız ve çeşitlilik karakteristiklerine göre işlenme ihtiyaçlarına yönelik farklı platformlar geliştirilmeye devam edilmektedir.[19] Bu platformlar ağırlıklı olarak BİT firmaları tarafından geliştirilmekte ve analiz araçlarının büyük bir kısmı açık kaynak kodlu olarak endüstrinin kullanımına sunulmaktadır.

Büyük veride üç temel uygulama mimarisinden bahsedilmektedir: yığın işleme, eş zamanlı akan veri işleme ve melez işleme mimarisi. Bunlardan yığın ve eş zamanlı veri işleme mimarileri en yaygın kullanılanlardır.[20]

---

[19] Kayabay ve ark., 2016: 3
[20] A.g.e.: 4

Yığın veri işlemek için günümüzde en çok tercih edilen teknoloji EşleİndirgE (MapReduce) yöntemini kullanan Hadoop'tur. Hadoop, verileri dağıtık ortamda saklamak için Hadoop Dağıtık Dosya Sistemini (Hadoop Distributed File System-HDFS) kullanmaktadır. HDFS, dağıtık ortamda bulunan disklerin tek bir sanal disk gibi çalışmasını sağlayan temel dosya sistemidir. Hadoop üzerinde büyük veri işlemek, anlamlandırmak, sorgulamak ve kaynak yönetimi için birçok araç ve teknoloji bulunmaktadır.[21]

Hadoop ve üzerinde çalışan teknolojiler ile büyük hacimli verileri birden çok bilgisayara dağıtmak ve EşleİndirgE ile işlemek mümkündür. Hadoop yığın veri işlemek üzere tasarlandığı için mimari öncelikleri ölçeklenebilirlik ve güvenilirliktir. Bu yüzden eş zamanlı akan veri işleme uygulamalarında örneğin; IoT, Sanayi 4.0 ve benzeri alanlarda yüksek hızda akan verileri eş zamanlı işlemek için tasarlanmış teknolojilere ihtiyaç duyulmaktadır. Akan verinin işlenmesibakımından günümüzde yaygın olarak kullanılan en önemli teknolojiler ise Storm, S4, Samza, Flink Streaming ve Spark Streaming olarak kabul edilmektedir.[22]

1.2.3. NoSQL veritabanları

NoSQL (Not Only SQL) veritabanları günümüzde kullanılan ilişkisel veritabanlarına alternatif olarak, gelişen ihtiyaçlar dolayısıyla ortaya çıkmıştır. Sistem temel olarak, verilerin farklı sunucularda yedeklemesini yapan dağıtık mimariyi kullanmaktadır. Klasik ilişkisel veri tabanı yönetim sistemlerinden farklı olarak yatay ölçeklemeye göre veri saklanmaktadır. Bu sistemde klasik veri tabanları alt küme olarak görülmektedir. Tasarımın basitliği, yatay büyüme ve erişilebilirlik konusunda daha iyi kontrol sağlaması sayesinde NoSQL veritabanları ilişkisel veritabanları içinde çözmenin zor olduğu problemleri çözebilmektedir.[23] Ayrıca sistem, kolayca yeni sunucular eklenerek büyütülebilmekte ve herhangi bir sunucunun arızalanması gibi olumsuzluklardan etkilenmemektedir.

[21] A.g.e.: 5
[22] A.g.e.: 5
[23] Özbilgin, 2015: 4

1.3. Büyük Verinin Uygulama Alanları, Zorlukları ve Riskleri

1.3.1. Büyük verinin uygulama alanları

Büyük miktar ve çeşitlilikteki verinin saklanması, yönetilmesi, işlenmesi ve bundan anlamlı sonuçlar çıkarılması, büyük veri teknolojileri sayesinde yönetilebilir, kolay ve hızlı bir hal almakta; dolayısıyla, ortaya çıkan verilerin hepsinin etkin bir şekilde kullanımı iş süreçlerinde iyileşmeler, kolaylıklar, avantajlar, verim artışı, kazanımlar ve sunulan hizmet kalitesinin artırılması ile müşteri memnuniyeti, rekabet avantajı ve yüksek kârlılık sağlamaktadır. Nitekim, Massachusetts Teknoloji Enstitüsü (MIT) tarafından gerçekleştirilen bir araştırmaya göre veriye dayalı karar alan işletmelerin kârlarını yüzde 5-6 civarlarında artırdıkları ifade edilmektedir.[24]

Büyük veri yığınlarından, işletme kararlarında kullanılacak bilginin üretilmesi ve anlamlandırılmasına ilişkin süreçlerin tamamı büyük veri analizi olarak adlandırılmaktadır. Günümüzde kamu ve özel tüm kurum ve kuruluşlar bu yeni fenomenle başa çıkmanın ve sunduğu fırsatlardan yararlanmanın yol, yöntem ve araçlarını bulmak durumundadır. Zira farklı kaynaklardan gelen ve farklı veri tiplerini içeren büyük boyutlu veriler başta sağlık ve finans sektörü olmak üzere birçok sektör ile bilimsel araştırmalar, büyük ölçekli e-ticaret uygulamaları ve internet arama motorları gibi pek çok alanda karşımıza çıkmakta; karar verme, risk yönetimi ve endüstriyel strateji geliştirme gibi önemli amaçlar için kullanılmaktadır. Nitekim, MGI tarafından yapılan araştırmada büyük verinin gerek kamu gerekse özel sektör bakımından sağlık, eğitim ve imalat gibi alanlarda dönüşümsel bir katkı sağladığı ortaya konulmaktadır.[25] Aşağıda büyük verinin katkı sağladığı alanlar/sektörler ele alınmıştır.

- *Sağlık Sektörü:* Veri odaklı tıbbî çalışmalar, çok sayıda tıbbi kayıt ve görüntünün eşanlı olarak değerlendirilmesine imkân vermesi sayesinde hastaya özel ilaç geliştirilmesini ve hastalığın erken evre teşhisine yardımcı olabilecek modeller öngörülmesini sağlamaktadır.

[24] Brynjolfsson ve ark., 2011: 5
[25] MGI, 2011

Sağlık hizmetleri bakımından maliyetlerin küresel anlamda giderek artış eğilimini sürdürdüğü hususu da dikkate alındığında, sağlık hizmetlerinde elektronik ortamda elde edilen, depolanan ve analiz edilen bilgilerden faydalanılmasının daha kaliteli hasta bakımı ve daha düşük maliyetler sağlayacağı hususu 2010 yılında ABD Başkanına sunulan bir raporda da yer almıştır.[26]

İngiltere'de, Ulusal Sağlık ve Klinik Mükemmeliyet Enstitüsü yeni ilaçların ve mevcut pahalı tedavilerin klinik etkililiğinin ve maliyet verimliliğinin araştırılması amacıyla büyük veri kümelerini incelemeye başlamıştır. Bu araştırma kuruma en iyi tedavileri saptama, maliyetle ilgili kuralları ortaya koyma ve ilaç ve tıbbi cihaz üreticisi firmalarla daha etkili bir müzakere yürütebilme olanağını vermektedir. Benzer şekilde, İtalya Tıp Dairesi de ulusal maliyet verimliliği programı çerçevesinde yeni pahalı ilaçlara ait klinik verileri toplayıp analiz etmekte ve analiz sonuçları doğrultusunda bu ilaçların fiyatlarını ve satış koşullarını yeniden değerlendirebilmektedir.[27]

- *Afet ve Acil Durum Yönetimi:* Sensör verilerinin bilhassa doğal afetlerin önceden tespitinde kullanılabilecek veriler olduğu değerlendirilmekte ve afetlerin öngörülmesi konusunda söz konusu veri yığınlarından faydalanılmasına yönelik çalışmalar sürdürülmektedir. Afet öncesi planlama, erken uyarı sistemleri, afet sonrası hasar tespiti ve yardım organizasyonu gibi temel konularda sensör verilerinin yanı sıra mobil teknoloji tabanlı büyük veri uygulamaları ile coğrafi bilgi sistemleri (CBS) altyapıları yaygın olarak kullanılmaktadır. Japonya'da uydu haberleşmesi ve sensör bazlı olarak afet erken uyarı sistemi kurulmuş; bunlara dayalı olarak deprem, dev dalga (tsunami) gibi afetlerden kısa süre önce devreye giren yangın önleme, bilgilendirme, tahliye gibi mekanizmalar oluşturulmuştur. Ayrıca afetler sonrasında sensörler ve görüntüleme cihazlarından elde edilen veriler kullanılarak yapılan insan davranış kalıplarına ilişkin çalışmalar doğrultusunda yardım kuruluşlarının hayatta kalanlara yardım etmesine yönelik çıkarımlarda bulunulabilmektedir.

---

[26] Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward, 2010, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-health-it-release.pdf, 10.12.2016

[27] Kalkınma Bakanlığı, 2013: 695

Dünya genelinde, afet anında kontrolü sağlayacak etkin bir yönetim mekanizmasının oluşturulması amacıyla büyük veri çalışmaları yürütülmekte, çalışmaların odağını ise afet sırasında ve sonrasında etkin bilgi paylaşımı oluşturmaktadır.[28]

- *Enerji Sektörü:* Enerjiye ayrılan pay kamu harcamaları bakımından en önemli kalemlerden birini teşkil etmektedir. Büyük veri analiziyle yapılacak çalışmalar sayesinde elektrik şebekelerinin daha etkin çalışması, dengeli kullanımın sağlanması ve böylece enerji israfının ve harcamaların azaltılması mümkündür.

  Enerji verimliliğinin sürdürülebilir bir toplumun en önemli önceliklerinden biri haline gelmesiyle uyumlu olarak sensörler, ağlar ve mobil cihazlardan akmakta olan büyük miktardaki veri, verimlilik ve tasarruf amacıyla, analiz edilmekte ve anlamlandırılmaya çalışılmaktadır. Bu çerçevede "Sayısal Avrupa" kapsamında hazırlanan "Enerjide Büyük Veri Analizi: Akıllı Ölçüm ve Akıllı Şebeke Teknolojilerinin Avantajlarının Kapısını Aralamak" başlıklı dokümanda[29], gerek enerji endüstrisi gerekse politika yapıcılara yönelik enerji alanındaki büyük veri yetkinliklerinin önemi anlatılmaktadır. Akıllı şebekelerin, ölçme ve analiz yatırımları ile bu alandaki düzenlemelerin sektörün dijital dönüşüm fırsatlarından yararlanmasını sağlayacak biçimde düzenlenmesi gerektiği vurgulanmaktadır.
- *Güvenlik Sektörü:* Emniyet güçleri, kaynakların daha etkin bir şekilde kullanımı ve caydırıcılığın temini amacıyla gerek kendi istihbarî veri kaynaklarından derlenen bilgilerin, gerekse kamu verisinin analizi yoluyla elde ettikleri sonuçlar doğrultusunda giderek daha veri odaklı stratejiler benimsemektedir.

  2013 yılında Los Angeles Polis Departmanı ve Kalifornia Üniversitesi işbirliğiyle gerçekleştirilen büyük veri pilot çalışması kapsamında, suç henüz meydana gelmeden ortaya çıkacak ihtimallerin öngörülmesini sağlayan bir çalışma neticesinde bölgedeki suç işleme oranlarında düşüş sağlanmıştır. Yapılan önleme çalışması neticesinde şiddet olaylarında yüzde 21, hırsızlık olaylarında yüzde 26 ve gasp olaylarında ise yüzde 12 oranında bir düşüş meydana gelmiştir. Söz konusu

[28] Bu alanda önemli örneklerden birini, University of California San Diego tarafından geliştirilen *Wildfire Detection* projesi oluşturmaktadır. Proje hakkında ayrıntılı bilgi için bkz. https://gizmodo.com/how-big-data-is-helping-snuff-out-californias-wildfire-1617073672, 20.10.2017.
[29] DIGITALEUROPE, 2015: 4-5

pilot çalışma için geçmiş 80 yıla ait 13 milyon tutuklama vakası incelenerek bir algoritma oluşturulmuş ve suç işlenen yerlerin haritası çıkarılarak o bölgeler hakkında tahminlerde bulunulmuştur.[30]

- *Finans Sektörü:* Büyük verinin en etkin kullanıldığı sektörlerden biri de finans sektörüdür. Günümüzde piyasa verilerinin yanında kredi kartı harcamalarından en basit hesap hareketlerine kadar tüketicilerce gerçekleştirilen tüm bankacılık işlemleri veri olarak kaydedilmekte ve analiz edilebilmektedir. Pek çok finans kuruluşu da piyasadaki risk durumunu tahmin edebilmek için elindeki bu verinin analizi amacıyla büyük veri teknolojilerinden faydalanmaktadır.

  Ayrıca, finans kuruluşlarının kendi sahip oldukları müşteri verilerinin de ötesinde sosyal medya paylaşımları ve arama motoru sorgu kayıtları gibi kaynaklardan elde edilen verilerle tahminleme yapılarak söz konusu verileri piyasadaki diğer değişkenlerle ilişkilendirmeye çalışan akademik çalışmalar ortaya konulmaktadır. Örneğin; Twitter paylaşımları ve hisse senedi hareketleri arasındaki ilişkiyi inceleyen bir çalışmada anlamlı çıkarımlar yapabilen bir model geliştirilmiştir.[31]

- *Çevrimiçi İşlemler / e-Ticaret:* Büyük veri analizinin etkilerinin en hızlı biçimde görüldüğü uygulama alanlarının başında kişiye özel hale getirilmiş e-ticaret hizmetleri gelmektedir. Çevrimiçi alışveriş tercihlerine ilişkin yönlendirmelerden, seyahat veya tatil planlanmasına; uçuş için en uygun zamanın seçiminden izlenecek içeriğe ilişkin birçok tüketici davranışı aslında söz konusu tüketicinin bilinçli ve/veya bilinçsizce ardında bıraktığı büyük veri yığınlarının analizinin bir sonucu olarak ortaya çıkmaktadır.

  Örneğin; Mart 2017 tarihinde açıklanan verilere göre dünyanın en büyük e-ticaret platformlarından biri olan Alibaba isimli e-ticaret sitesi, 100 petabayttan fazla işlenmiş veriyi kendi veri merkezinde depolamıştır. Yalnızca Bekârlar Günü-11/11[32] sırasında 278 milyon adet siparişe karşılık gelen alışveriş etkinliğinden 9,3 milyar Çin Yuanı tutarında satış yapmıştır. Kasım 2016 tarihinde ise şirket söz konusu tutarı 12 milyar Çin Yuanına (18 milyar ABD doları) çıkarmıştır. Senede bir gerçekleştirilen bu önemli alışveriş etkinliği için Alibaba saniyede 5 milyon

[30] Grill, 2013: 1
[31] Chen ve Lazer, 2013: 4-5
[32] Özgün ismi "Singles' Day" veya "Bachelors' Day" olarak bilinen ve her yıl 11 Kasım tarihinde Çin'de gerçekleştirilen bu etkinlik dünyanın en büyük e-ticaret festivali olarak kabul edilmektedir.

işlem gerçekleştirebilen Galaxy isimli bir gerçek zamanlı veri işleme platformu geliştirmiştir. Galaxy'nin günlük işleyebileceği veri miktarı 2 petabayt olarak ifade edilmektedir. Bu etkinlikle Alibaba, büyük veri kümelerini gerçek zamanlı olarak depolayıp işleyerek ve elde ettiği analiz sonuçlarını hızlı ve verimli bir biçimde yorumlayarak bir önceki döneme göre satışlarını önemli oranda artırmıştır.[33]

- *Kamu Hizmetlerinin Sunumu:* Büyük veri uygulamalarının kamu tarafından etkin bir biçimde kullanılması sonucunda aşağıdaki faydaların elde edileceği öngörülmektedir:
  i. Karar alma mekanizmalarının etkinliğinin artırılması: Büyük veri kamu yöneticilerinin veriye dayalı olarak karar verebilmelerine olanak tanımaktadır.
  ii. Hizmet kalitesinin artırılması: Büyük veri analizi sayesinde daha iyi kararların alınması sonucunda kamu hizmetlerinin kalitesi ve etkinliği artmaktadır.
  iii. Vatandaş memnuniyetinin artırılması: Vatandaş odaklı hizmet sunumu ve otomatize edilmiş hizmetler sayesinde hizmet kalitesi artmakta, bunun yanında büyük veri kamuda şeffaflığa ve açıklığa olanak sağlamaktadır. Vatandaşlar kamunun etkinliği hakkında sayısal verilere dayalı detaylı bilgiye sahip olabilmektedir.[34]
  iv. Maliyetlerin azaltılması: Verilerin analizlerde etkin bir şekilde kullanılması sonucunda yatırımlardaki mükerrerliğin azaltılması, vergi kaçaklarının ve sağlık harcamalarının azaltılması mümkündür.

1.3.2. Büyük verinin beraberinde getirdiği zorluklar

Büyük veri düşünme, algılama biçimi, araştırma ve iş yapış yöntemlerinde köklü bir değişim yaratmakta ve bazı zorlukları beraberinde getirmektedir. Söz konusu zorluklardan ilki veriye ilişkin temel politikanın belirlenmesidir. Zira veriye ilişkin politikalar, başta mahremiyet, güvenlik, fikri mülkiyet hakları ve verinin transferi olmak üzere birçok alanı düzenlemektedir. Başta sağlık ve finans sektörü verileri olmak üzere gerek bireysel güvenlik ve mahremiyeti doğrudan ilgilendiren kişisel veriler, gerekse devletlerin güvenliğini ilgilendiren verilere ilişkin korumacı politikalar artarken büyük veriden sağlanacak fayda ve değerin sınırlandırılması

[33] Jin ve ark., 2015: 59–64
[34] Kalkınma Bakanlığı, 2013: 715

tehlikesi ortaya çıkmaktadır. Bu çerçevede, söz konusu dengeyi sağlayacak veri politikalarının oluşturulması önem arz etmektedir.

Büyük veri analizinin temel zorluklarından bir diğeri, verinin bizatihi kendisine erişim olarak ifade edilmektedir. Geniş ölçekli verilere kolay erişim, söz konusu büyük veri setlerinden elde edilecek fayda ve değere erişimi de kolaylaştırmaktadır. Özellikle üçüncü tarafların verilerine (internetten, sosyal medya kanallarından, üçüncü kişi veri sahiplerinden vb.) erişilmesi ve söz konusu verilerin eldeki veri setleriyle birleştirerek kullanılması büyük veri analitiği bakımından önemli bir potansiyeli ortaya çıkarmaktadır. Bununla birlikte, özellikle uygulamada büyük veri setlerine sahip kurumların veri paylaşımı konusunda isteksiz davrandığı yahut veri karşılığında oldukça yüksek ücretler talep ettiği bilinmektedir. Örneğin sosyal medya şirketlerinin kullanıcılara veri tabanlarında depoladığı verileri alabilmeleri için sunduğu açık uygulama programlama arayüzlerinin (Application Programming Interface-API) tüm verilere erişim imkânı vermediği ifade edilmektedir.[35] Yine sağlık sektöründe faaliyet gösteren işletmeler ciddi yatırımlar yapmak istese de, kişilerin sağlık bilgileri sağlık bakanlıklarınca paylaşılmamaktadır.

Büyük veriden fayda sağlanması ve sahip olduğu değerin açığa çıkarılması hususunda ortaya çıkan bir diğer zorluk ise kuruluşların büyük veriden tam olarak nasıl faydalanılacağına dair bir kurumsal kültüre sahip olmamasıdır. Zira kuruluşların gerek kendi sahip oldukları gerekse internet, sosyal ağlar gibi farklı kaynaklardan elde ettikleri büyük veri setlerinden yararlanabilme, bu verileri kullanabilme yetenekleri ve veriye bakış açıları önem arz etmektedir. Büyük veriden fayda ve değer sağlamak isteyen kurum/kuruluşların bu konunun farkında olan yöneticilere, veri analistlerine, büyük verinin gerektirdiği teknolojik altyapıya ve yönetici ve çalışanlarının veriden elde edilen bilgi ve tecrübeyi birleştirebilme becerisine sahip olmaları gerekmektedir.[36]

Son olarak, veri güvenliği, veriye dayalı ayrımcılık ve mahremiyet konuları büyük veri analizinin en temel zorlukları olarak özellikle hukuk doktrininde tartışılmaya devam etmektedir. Bireylerin açık rızaları alınmaksızın kişisel ilgi

[35] Gürsakal, 2014: 16-17
[36] McAfee veBrynjolfsson, 2012: 1

alanları, konumları, hobileri, fiziksel özellikleri gibi pek çok kişisel verisinin özellikle verinin ikincil kullanımı vasıtasıyla açığa çıkabilmesi, mahremiyet ihlallerini doğurduğundan tartışma yaratmaktadır. Büyük veri analizi işletmelerin daha iyi pazarlamacılar ve hizmet sağlayıcıları haline gelmesine yardımcı olmaktadır. Ancak, aynı işletmeler bireyler hakkında pek çok farklı kaynaktan edindikleri oldukça tutarlı veriyle ayrımcılığa varan (örneğin; tüketicilerine kredi kullandırma, sigorta primleri konusunda rizikoya ilişkin değerlendirme yapma vb.) bir hareket serbestisine sahip olabilmektedir. ABD Federal Ticaret Komisyonu (Federal Trade Comission-FTC) tarafından hazırlanan "Büyük Veri: dışlama veya katılma konusunda bir araç mıdır?" raporu söz konusu hususu ele almaktadır.[37] Ayrıca, bireylerden açıkça rızaları alınmış olsa dahi, meşru yollarla elde edilen verilerin kaydedilmesi, dönüştürülmesi veya kullanımı esnasında ortaya çıkabilecek sızıntılar, hizmet sağlayıcıların sebebiyet verdiği güvenlik açıkları ve operatör hatası gibi sebepler veri güvenliği alanında önemli sorunları beraberinde getirmektedir.[38] Büyük veri analiziyle birlikte kişisel mahremiyetin öyle veya böyle sonunun geleceğine inanan araştırmacılar, bireylerin rızası ve veri güvenliği alanından teknik her türlü önlem alınsa bile söz konusu gücün veriyi kullanan kişilerce zamanla kötüye kullanılabileceğini ifade etmektedirler.[39] Büyük verinin mahremiyet alanında ortaya çıkardığı sorunlar ve çözüm önerileri bu tezin temel araştırma konusu olduğundan, ilerleyen bölümlerde daha detaylı ele alınacaktır.

1.3.3. Büyük verinin riskleri

Büyük veri, yenilikçi faydaları da dikkate alındığında pek çok kurumsal organizasyonun yeni fırsatları değerlendirmesi hususunda yollar açmaktadır. Bununla birlikte, söz konusu kavramın ardında yatan kurumsal dinamiklerin göz ardı edilmemesi gerektiği önemle vurgulanmaktadır. Zira büyük verinin, üstün yararı bulunan alanlarda da (bilimsel araştırmalar, kamu yararı sağlayan uygulamalar gibi) kullanılması öngörülüyor olsa bile temelde ticari kuruluşların ve teknoloji

[37] Marr, 2017: 1
[38] Chen ve ark., 2014: 207
[39] Mayer-Schönberger ve ark., 2013: 180

endüstrisinin ekonomik değer yaratma süreçlerini yansıttığı (Kutu1.1) ifade edilmektedir.[40]

Bu çerçevede üç temel risk alanının mevcut olduğu değerlendirilmektedir: Bunlardan ilki, büyük verinin sağlamakta olduğu ekonomik faydanın orantısız bir şekilde küresel anlamda gelişmiş ülkelere kayması riskidir. Zira büyük veri analizine dayalı iş geliştiren başta büyük BİT sektörü firmaları olmak üzere yenilikçi işletmelerin çoğunluğu veri pazarı olarak gözünü başta Asya olmak üzere doğuya çevirmiş bulunmaktadır. Hâlihazırda verinin, birkaç küresel merkezde gittikçe daha çok toplanan ve paraya çevrilen bir kaynak haline gelmekte olduğu görülmektedir.[41]

İkinci olarak, büyük veriden beklenen fayda veri mahremiyeti ve anonimliğin sağlanması konusundaki zorluk karşısında etkinliğini kaybedebilme riskini bünyesinde barındırmaktadır. Söz konusu riski oluşturan faktörlerin dünyanın her yerinde ve tüm veri sahiplerince aynı şekilde anlaşılması veya takdir edilmesi mümkün gözükmemektedir. Nitekim dünyada mahremiyet politikaları ve düzenlemeleri konusunda yeknesak bir yaklaşım olmadığı gibi mahremiyet algısı da toplumlar bakımından farklılık arz etmektedir.

Son olarak, büyük veriden değer yaratan ve ekonomik faydasının farkına varan aktörler, söz konusu alanda uzmanlık ve liderlik hususunda, daha en başından oldukça avantajlı konumda bulunmaktadır. Zira teknolojik sistemlere ve altyapıya hâkim olan bu aktörler bu alanda kalıcı düzenlemeleri, yaklaşımları, standartları ve uygulamaları belirlemektedir. Büyük veri analizi konusunda yalnızca veri sahiplerinin ve işlenen verinin değil aynı zamanda veriye ilişkin tüm bu işlemlerin (veri altyapılarının oluşturulması, veri analizinin yapılması, yazılan uygulamalar vb.) kimler tarafından yapıldığına da dikkat edilmesinin önem arz ettiği değerlendirilmektedir. Büyük veriden tam anlamıyla fayda sağlanması, veriye ilişkin tüm süreçlerde güçlü bir hâkimiyeti haiz olmayı gerektirmektedir.[42]

---

[40] Watson, 2016: 2
[41] Dalton, 2016: 1
[42] Stevens ve ark., 2016: 6

Kutu 1.1. Facebook'un Haber Akışı Deneyi[43]

Facebook tarafından 689.000 kullanıcısı üzerinde gerçekleştirilen gizli bir çalışmayla (News Feed deneyi), bireylerin arkadaş gönderileriyle aldıkları bilgilerin ruh hallerinde ve dolayısıyla davranışlarında ortaya çıkardığı etki denenmiş, bu deney kamuoyunda sert tepkilere neden olmuştur.

Facebook'un bireylerin ilişki durumu, gittiği ilkokul veya müzik zevki gibi kişisel bilgilerini biliyor olması günümüz toplumunda pek de yadırganmamaktadır. Ancak dünyanın en büyük sosyal paylaşım sitesi kabul edilen Facebook'un kullanıcılarını yalnızca birkaç tuşa dokunarak nasıl daha mutlu veya daha üzgün hissettirebildiğine ilişkin çalışmanın ortaya çıkmasıyla toplumda tepkiler oluşmuştur. Şirket tarafından ayrıntıları yayımlanan haber akışı deneyinde, 689.000 kullanıcının ana sayfalarında yayımladıkları bilgilerin nasıl manipüle edildiği ve sonucunda da "duygusal bulaşma" vasıtasıyla bireylerin nasıl daha pozitif veya negatif hissedebileceği ortaya konulmuştur.[44]

Deneyde Facebook, kullanıcılarının haber akışlarını[45] filtrelemektedir. Buna göre; bir grup kullanıcıya arkadaşlarının olumlu duygusal içerikleri daha az gösterilmiş, sonuçta o kullanıcının kendi haber akışında da olumlu duygusal içerik azalmıştır. Diğer grup kullanıcıya ise, arkadaşlarının olumsuz duygusal içerikleri daha az gösterilmiş ve sonuçta o kullanıcının kendi haber akışındaki olumsuz duygusal içeriklerinde de azalma meydana gelmiştir. Çalışmada, çevrimiçi sosyal ağlarda arkadaşlar tarafından ifade edilen duyguların, bireyin ruh halini doğrudan etkilediği ortaya konulmuştur. Bu sonucun sosyal ağlarda büyük çapta duygusal bulaşmaya ilişkin ilk deneysel kanıt olduğu ifade edilmektedir. Hukukçular, sivil toplum ve politika yapıcılar duygusal manipülasyon yoluyla yapılan bu kitle deneyin "ürkütücü" ve "rahatsız edici" olduğunu ifade etmektedir.

Bireylerin özel hayatlarına ilişkin bilgiler sosyal medya şirketleri tarafından manipüle edilmektedir. Facebook veya farklı sosyal medya şirketlerinin, bireylerin politika tercihlerini veya başka alanlardaki düşüncelerini manipüle edebilme kabiliyetiyle onları kontrol altına alması karşısında bireylerin korunması ve en azından bu kabiliyetten haberdar olmaları gerekmektedir.

Facebook, ABD Ulusal Bilimler Akademisi Bildiriler Kitabı'nda yayımlanan bu araştırmayla, hizmetlerini iyileştirmeyi ve kişilerin Facebook'ta gördükleri içeriği olabildiğince alakalı ve ilgi çekici hale getirmeyi amaçladığını ifade etmiştir. Bu amaçla, insanların arkadaşlarından gelen haberler veya takip ettikleri sayfalardan gelen bilgilerden oluşan farklı içerik türlerine nasıl tepki verdiklerini araştırdıklarını ifade etmiştir. Ancak söz konusu uygulama, seçimler öncesi bireyleri belirli bir siyasi amaca yönlendirme veya reklam gelirlerini artırmak amacıyla bireyleri olumlu düşüncelerle besleyerek bir sitede kalma süresini aşırı uzatmak gibi sonuçlara götüreceği bakımından eleştirilmektedir.

Söz konusu şirketlerin bireylerin fikir ve tercihlerini manipüle etme becerilerin en çarpıcı sonuçlarından biri ise 2016 ABD başkanlık seçimlerinde yaşanmıştır. Söz konusu manipülasyon olayının çok öncesinde, Barack Obama'nın 2008 yılı ABD başkanlık seçim kampanyasının çevrimiçi ayağını yürüten Blue State Digital'in kurucu ortağı Clay Johnson,

[43] Debatin ve ark.. 2009: 83-108
[44] Tufekci, 2014: 27
[45] Haber akışı terimi, kişilerin sosyal ağlarında yayımladığı yorumlar, videolar, resimler ve internet bağlantı akışlarını ifade etmektedir.

Facebook'un duygusal bulaşma deneyinin ürkütücü boyutlara ulaştığının altını çizmiştir. Nitekim, 2016 ABD başkanlık seçimlerine gelindiğinde, ABD Başkanı Donald Trump'ın sosyal medya sorumlusu tarafından söz konusu seçimlerde gizli Facebook paylaşımlarının kullanıldığı açıklanmış, çalışmada kullanılan algoritmanın ise vatandaşları iknayı değil, hiç oy vermemelerini sağlamayı hedeflediği ifade edilmiştir. Örneğin seçimlerde kritik önemi bulunan Philadelphia eyaletinde yaşayan Afro-Amerikan erkekler doğrudan hedef kitle olarak belirlenmiştir. Görünürlüğünü kampanya ekibinin kontrol ettiği, böylelikle yalnızca görmesini istedikleri insanların görebileceği, herkese açık olmayan, hedefli paylaşımlar tasarlanmış, böylece söz konusu insanların doğrudan kararlarını etkileyebildikleri ifade edilmiştir. Kampanyada kullanılan gizli paylaşımlarda ne olduğu bilgisi ise halen Facebook tarafından kamuoyuna açıklanmamıştır.

2017 yılı sonunda ise, Facebook üzerinden uygulama üreten bir dizi firmanın üyelerin kişisel verilerini hukuka aykırı olarak işledikleri, Facebook tarafından da kabul edilmiştir. Başta İngiltere merkezli Cambridge Analytica adlı veri analiz firması olmak üzere Facebook üzerinde çalışan pek çok uygulama üreticisi firma 50 milyon hesaptan kişisel veri toplamıştır. Cambridge Analytica'nın bu verileri 2016 yılında yapılan ABD seçimleri ile İngiltere Brexit referandumunu etkilemek için kullandığı iddiaları sebebiyle İngiltere Bilgi Komisyonu (Information Commissoners' Office-ICO), söz konusu iddiaların detaylı bir şekilde incelenmesi için soruşturma başlatmıştır. Kişisel veriler kullanılarak siyasi seçimlerin manipüle edildiği iddiaları sebebiyle Cambridge Analytica ve Facebook'un hukuki soruşturması 2018 yılı itibarıyla sürmektedir.

1.4. Büyük Verinin Ekonomik Boyutu

Büyük veri pazarı yeni araç ve yazılımlarla genişlemesini sürdürmektedir. IDC'nin "Dünya Çapında Büyük Veri ve Analitik Harcamaları Yarıyıl Rehberi"nde, büyük veri ve iş analitiği pazarının 2016 sonu itibarıyla 130 milyar ABD dolarına ulaştığı, 2020 yılında ise 203 milyar ABD doları olacağı öngörülmektedir. Bilhassa bankacılık ve bilgi teknolojileri (BT) sektöründeki teknoloji yatırımları bu öngörüyü desteklemektedir. Büyük verinin BT endüstrisine de güçlü bir ivme kazandıracağına kesin gözüyle bakılmaktadır. Büyük veri, bulut bilişim ve mobil teknolojiler BT endüstrisinin üçüncü nesil platformları olarak isimlendirilmekte ve IDC tarafından 2020 yılına kadar üçüncü nesil BT platformlarının pazar büyüklüğünün 5,3 trilyon ABD dolarına ulaşacağı tahmin edilmektedir. IDC tarafından 2013'ten 2020'ye kadar, BT sektöründeki büyümenin yüzde 90'ının bu teknolojiler eliyle yönlendirileceği ifade edilmektedir.[46]

[46] IDC, 2016: 2

2011 yılında sanal ağlar, işlemciler ve sensörler üzerinde yürütülen ekonomik faaliyetleri ifade etmek için W. B. Arthur tarafından ortaya atılan *"ikinci ekonomi"* kavramı temelde büyük veriyi çağrıştırmaktadır. 2030 yılında ikinci ekonominin büyüklüğünün ilk ekonomiye (başka bir deyişle geleneksel ekonomiye) yaklaşacağı tahmin edilmektedir. Bu hızlı büyümenin temelinde ise ikinci ekonominin temel desteğinin tükenmez ve sürekli zenginleşen bir kaynak olan büyük veri olacağı ifade edilmektedir. Bu çerçevede büyük veri perspektifinden değerlendirildiğinde, gelecekte ikinci ekonominin temel destekleyicisinin işgücü verimliliği değil, bilgi verimliliği olacağı öngörülmektedir.[47]

1.4.1. Büyük verinin ticari amaçlarla kullanımı

Ticari işletmelerde, verinin etkili yönetimi ile işletmenin mali performansı arasında çok güçlü bir bağlantı bulunmaktadır. Ancak günümüz iş dünyasında işletmeler pek çok kaynaktan beslenen farklı yapı ve formatta hızla akan, baş edilmesi güç bir veri yığınının bombardımanı altında bulunmaktadır. Artan rekabet ve yoğunlaşan pazar dinamizmi ise işletmeleri yeni arayışlara ve bugüne kadar eşi benzeri görülmemiş büyüklükte ve karmaşıklıkta veri yığınları içinde bir çıkar yol bulmaya zorlamaktadır. Bu kapsamda, bilişim teknolojileri alanındaki gelişmeler günümüz iş dünyasındaki dönüşüm için bir katalizör görevi üstlenmekte, veri önemli bir kaynak olarak karşımıza çıkmaktadır.

İşletmelerin veriyi etkin bir şekilde faydalı bilgiye dönüştürmesinde kullanılan büyük veri analizinin, genel bir kural olarak birçok işi ve sektörü yeniden şekillendireceğine kesin gözüyle bakılmaktadır. Veriyi verimli bir şekilde kullanarak esaslı bir dönüşüm geçirmesi muhtemel sektörlerin yalnızca BİT firmaları değil; bir şeylerin taşımacılığını yapan sektörler, tüketicilere satış yapan sektörler, makina ve teçhizat kullanan sektörler, içerik satan veya kullanan sektörler, hizmet sektörü, fiziksel tesisleri olan sektörler ve parayla ilişkisi olan tüm sektörler olduğu ifade edilmektedir. Kısacası kapsam dışında yer alan hiçbir sektör bulunmamaktadır.[48]

---

[47] Jin ve ark., 2015: 59
[48] Davenport, 2014: 40

Büyük verinin ortaya çıkışından kısa bir süre geçmiş olmasına rağmen farklı sektörlerden büyük kuruluşlar veri ekonomisine katılmakta ve büyük veriyi sadece daha iyi ve hızlı kararlar ile maliyet tasarrufu için değil, aynı zamanda müşterileri için veriye dayalı yeni ürün ve hizmetler yaratmak için de kullanmaktadırlar. 1980'lerden beri veriden değer kazanmak için yapılan çalışmaları etkileyen en geniş kapsamlı değişimin büyük veri ile geldiği ifade edilmektedir. Büyük verinin sağladığı esas değer ise, verinin ham halinden (ne kadar büyük olursa olsun) değil, analizi ve analiz sonucunda üretilen ürün ve hizmetlerden kaynaklanmaktadır.[49]

İşletmelerin büyük verinin etkisini daha hızlı görebilmeleri için atmaları gereken adımlar temelde iki önemli yaklaşımın benimsenmesini gerektirmektedir. Bunlardan ilki yeni teknolojilerin ve analiz yöntemlerinin getirdiği avantaj ve kolaylıklardan yararlanmak, diğeri ise işletme içerisinde veriye dayalı bir yönetim anlayışının benimsenmesi için işletme bünyesinde iş ve süreçlerin yeniden tasarlanması çalışmalarının hayata geçirilmesi olarak ifade edilmektedir.[50]

1.4.2. Büyük verinin rekabet üzerindeki etkileri

Büyük veri analizi gibi yenilikçi teknolojilerin ve e-ticaretin ortaya çıkışıyla birlikte iş yapma biçimleri köklü bir biçimde değişmiş; rekabet avantajının kaynağı olarak esneklik ön plana çıkmıştır. Bu çerçevede başarılı bir işletmenin, müşteri tercihlerini etkileyebilen, sektöre giren oyuncuların endüstri normlarında yaptığı değişikliklere, rakiplerinin öngörülemeyen hareketlerine ve zorluklara hızlı bir şekilde tepki verebilen, operasyonel esnekliği yüksek ve kendini yenileme kabiliyetine sahip olması gerektiği değerlendirilmektedir. Schumpeter tarafından ortaya atılan "yaratıcı yıkım" yaklaşımına göre de yenilikçi işletmeler yeni şeyler yapmanın yollarını bularak endüstriyi geliştirirken, buna adapte olamayan eski işletmeler pazarın dışına itilmektedir.[51]

Büyük verinin büyük miktarda verinin toplanmasına, depolanmasına ve işlenip eşanlı analiz edilmesine imkân sağlaması, rekabet alanında oynanan stratejik oyunu, analoji yapmak gerekirse, satranç tahtasındaki yavaş ve dikkatli konumundan, hızın

[49] A.g.e.: 216
[50] Altunışık, 2015: 45
[51] AT Kearney, 2013: 2

önemli bir faktör olduğu bir aksiyon oyununa doğru yönlendirmektedir. Büyük veriden değer ve yenilikçi faydalar yaratan işletmeler hem operasyon yönetimi hem de rekabet avantajı anlamında büyük fırsatlara sahip olacaktır.

Bir süre önce büyük veri analizi denilince akla ilk olarak BİT firmaları gelmekteydi. Ancak büyük verilerin depolanması ve işlenmesi konusunda teknik zorlukların sona ermesiyle ve büyük veri analizinin BİT firmalarınca bir hizmet olarak sunulmaya başlanarak altyapıya erişimin giderek kolaylaşmasıyla esnek olmayan sermaye yatırımlarının yükü de ortadan kalkmıştır.[52] Böylece büyük veri analizi yalnız BİT firmaları için değil hemen hemen bütün sektör firmaları için rekabet avantajı elde etme, daha iyi kararlar verme, yeni ürün ve hizmetler geliştirme, kalite ve verimliliği artırma, müşteri ve pazar dinamiklerini daha iyi anlama konusunda yol gösterici olmaktadır (Şekil. 1.2). Sağlıktan finansa, üretimden perakendeye kadar pek çok sektörde büyük verinin nimetlerinden faydalanmak için çalışmalar yapan işletmeler ortaya çıkmakta, toplanan büyük verinin analizi ile birlikte işletmeler için yeni iş fırsatları ve kullanım alanları ortaya çıkmaktadır.[53]

Şekil 1.2. Büyük Verinin İşletmelere Sağladığı Avantajlar

Geleceğin işletmelerinde rekabet üstünlüğünün işletme içinde ve dışında bulunan karmaşık bilginin üretilmesi, tüketilmesi ve yönetilmesi sayesinde mümkün olacağı değerlendirilmektedir. Söz konusu rekabet üstünlüğünün elde edilmesinde büyük verinin kullanılmasının şu avantajları sağlayacağı öngörülmektedir:

i. *Büyük veriyle hedef odaklı pazarlama:* Büyük veri, işletmelerin pazarlama yöneticilerine tüketiciye doğru bilgiyi doğru zamanda vererek tercihlerini

[52] Schultz, 2013: 39
[53] Çiğdem ve Seyrek, 2015: 1

etkilemek konusunda mükemmel bir araç sağlamaktadır. Bu alanda büyük veriyle sosyal medya analizi hizmetine ilişkin bir sektör çoktan oluşmuş bulunmaktadır. Mashable.com_adlı internet sitesi Facebook ve Twitter gibi farklı sosyal medya kanallarında, hatta gazete makaleleri ve bloglardaki metinleri tarayarak insanların ne istediğini öğrenmeye yardımcı olan 20 farklı API hizmeti sunmaktadır. Uygulama sayesinde tüketicinin promosyonlara ve diğer kampanya faaliyetlerine nasıl eriştiği hakkında gerçek zamanlı geri bildirimler de sağlanmaktadır.[54]

ii. *Tasarım odaklı yenilikler:* Büyük veri kaynaklarının ortaya çıkan diğer teknolojilerle kombinasyonu tasarım odaklı yeniliklere ilham vermektedir. Bu yenilikler, tüketiciler tarafından beklenmeyen ancak sonuçta hızla benimsenen yenilikler olarak sektörlerinde yıkıcı oyun değiştiricilere dönüşmektedir. Örneğin akıllı telefon üreticileri kullanıcıların yalnız sesli aramalarını değil, telefonla yapılanları ve düşünme biçimini değiştirmektedir. Bir kullanıcının evinin bir odası için renk ve tasarım şemaları oluşturmasından, mobil oyunlarda ne kadar süre geçirdiğine, ne sıklıkta haber okuduğundan hangi türde filmleri izlediğine kadar tüm verileri toplayan ve kullanıcıların yapmak isteyeceği her şey için akıllı telefonunu kullanacağı yeni uygulamalar geliştirmektedir. Dolayısıyla bir akıllı telefon artık yalnızca bir telefon değil, kullanıcısının hayatını değiştiren çok amaçlı bir araca dönüşmekte ve çoğu insan söz konusu cihazları bunun için tercih etmektedir. Dolayısıyla satın alınan ürünler endüstrinin ortaya koyduğu kimliksiz birer nesne olmanın ötesinde onu tasarlayanların değer ve kalıplarını yansıtmaktadır. İşletmelerce hayata geçirilen büyük veriye dayalı yenilikler yalnızca ortaya çıkarılan ürünü değil, müşterileri ile ortak değerleri paylaşma ve topluluğun bir parçası olma stratejisini ifade etmektedir.[55]

iii. *Kitle kaynaklı ve kitle fonlamalı yenilikler:* Büyük veri çağında işletmelerin ve kuruluşların çoğunun yeni iş fikir ve çözümlerini kendiliğinden ortaya atmadıkları, kitle-kaynaklı ve kitle-fonlu çözümler sayesinde söz konusu gelişmeleri ortaya koydukları görülmektedir. Büyük veri analizi yalnızca kitlelerin taleplerini algılayarak pazara daha iyi bakış açısı kazandırmakla

[54] Provost ve Fawcett, 2013: 51-59
[55] Verganti, 2009: 40

kalmamakta, aynı zamanda pazara hızlı bir şekilde yanıt verebilme kabiliyeti de kazandırmaktadır.

Yenilikçi aracılar tarafından oluşturulan, belirli bir probleme çözüm arayan şirketler ile olası çözümlerin biraraya getirilmesini öngören tarafsız platformlar sayesinde yenilikçi çözümlerin bulunması kolaylaşmaktadır. Örneğin; AstraZeta şirketi yenilikçiliğe ilişkin zorluklarına çözüm aramak için bir inovasyon altyapısı kurmuştur. Tümör hücrelerinin tedavisi amacıyla "Oligonükleotidlerin Hedefe Ulaştırılması" adında 100 bin ABD doları tutarında bir inovasyon fonu oluşturmuştur. Elde edilen büyük veri, projenin hedefine ulaşması amacıyla sürekli analiz edilmektedir.

Sosyal medya ve büyük verinin birbirini beslemesi sayesinde yeni fikirler, prototipler, ürünler ve senaryolar kitleler içerisinde işbirliği içinde tartışılmakta, geliştirilmekte ve sürekli olarak güncellenerek piyasa reaksiyonlarını tahmin etmek için gerçek zamanlı olarak kontrol edilmektedir.

Büyük veriyi faydaya dönüştürebilen işletmelerin başında Google, IBM, Oracle, Microsoft, Cloudera, SAS Institute, Teradata gibi bilişim firmaları gelmektedir. Wal-Mart, Alibaba ve Amazon ise büyük verinin perakende sektöründe kullanımı konusunda öncü kabul edilmektedir.[56] Wal-Mart büyük veri analizi sayesinde fiyatları ayarlayarak maliyetlerini düşürmekte ve azami fayda elde etmek amacıyla paydaşlarının kararlarını etkilemektedir. Amazon, Netflix, Target gibi firmalar büyük veri analizi yoluyla müşterilerinin kişisel tüketim tercihlerinden yola çıkarak yeni ürünler önermektedir. Amazon'un satışlarının yaklaşık üçte birinin, Netflix'in aldığı siparişlerin yaklaşık dörtte üçünün bu tavsiyeler sonucunda gerçekleştiği ifade edilmektedir.[57]

Başlangıçta sadece indekslediği internet sitelerinden ve arama sorgularından veri elde eden Google, günümüzde akıllı telefonlardan GPS cihazlarına kadar pek çok farklı kaynaktan günde yaklaşık 24 petabayt veri toplamakta ve işlemektedir. Şirket, yakın bir tarihte seyahat sektörüne girmiştir. Burada dikkat çeken husus ise şirketin, çevrimiçi reklam harcamaları yoluyla seyahat acentelerinin bizzat kendileri tarafından

[56] Mayer-Schönberger ve Cukier, 2013: 131
[57] Morabito, 2015: 120

finanse edilmekte olmasıdır. 2017 yılı sonu itibarıyla ABD'de seyahat rezervasyonlarının yüzde 88'i çevrimiçi olarak yapılmaktadır.[58] Seyahat acentelerince gerçekleştirilen çevrimiçi reklam harcamalarının yüzde 70 ila 90'ı ise Google üzerinden gerçekleştirilmektedir. Dolayısıyla bu sektörde rekabetin nasıl işlediği, müşterilere hangi kanallardan daha etkin erişilebildiği, bu alanda doğru niteliklere sahip analistlerin kimler olduğu ve söz konusu insan kaynağının yönetilme becerisi Google tarafından çok iyi bilinmekte, muazzam veri depolama kapasitesi ve sadık veri kaynakları sayesinde de sektörde önemli bir avantaj elde etmektedir. Söz konusu donanımları sayesinde Google'ın günümüz perakende pazarlarının tamamında başarıya erişebileceğini kestirmek ise hiç de zor olmamaktadır.[59]

Son olarak, IoT destekli akıllı şehirlere ilişkin gelişmelerin de önemli etkileri beraberinde getireceği değerlendirilmektedir. Çöp bidonlarından bisiklet tekerleğine su borularından trafik ışıklarına kadar akla gelen bütün nesnelere entegre edilen sensörler sayesinde elde edilen büyük verinin yapay zekâ teknolojisiyle birlikte kullanıldığı akıllı şehirler alanında IBM, Microsoft ve Cisco gibi büyük firmalar rekabet etmektedir. Zira hayatı kökünden değiştiren veriye dayalı teknolojik hizmetleri biraraya getirme becerisine sahip işletmeler rekabet avantajında öne geçmektedir.[60]

1.4.3. Büyük veride tüketicinin korunması

Büyük veri analiziyle "kitle özelleştirme" kavramı ön plana çıkmaktadır. Büyük veri işletmelere, her bir tüketiciyi satın alma geçmişi, fiziksel konumu, mali durumu gibi kişisel verilerinin yanı sıra iş geçmişi, grup üyelikleri ve sosyal ilişkileri/ilişki durumu gibi demografik verilerini dikkate alarak tercih ve satın alma alışkanlıklarına göre bireysel olarak hedefleme imkânı vermektedir. Söz konusu veriler içeriğin, tekliflerin, ürün ve hizmetlerin daha isabetli bir şekilde belirlenerek tüketicinin nihai olarak satın alma ihtimalini güçlendirmektedir.[61] Kitle özelleştirmesi olarak ifade edilen bu kavramın yanında büyük veriyle birlikte gelişen teknolojilerin (IoT, makinalar arası iletişim (machine to machine-M2M) vb.) iki önemli gelişmeyi

---

[58]Statista, Distribution of adults in the United States by their preference of hotel booking online or offline in 2017, (erişim tarihi: 21.09.2017) https://www.statista.com/statistics/666643/preference-of-online-or-offline-hotel-booking-us/
[59] Brumley, 2014: 2
[60] Morabito, 2015: 11
[61] Offsey, 2014: 1

daha tüketiciler bakımından tetikleyeceği değerlendirilmektedir. Bunlardan ilki, kendi kendini tüketiciye göre özelleştirebilen ürünler olarak ifade edilirken; ikincisi ise, tüketici tarafından satın alınan ürünün kendi verisini üretmeye devam eden gömülü bir yazılıma ve/veya M2M sağlayan bir donanıma sahip olması durumudur. Bu ikinci durumda, satın alınan ürün bir nesne olmanın ötesine geçerek kullanıcısına hizmet de sunabilecektir. Örneğin; sürücüsüz araçların kişisel bir asistan gibi hareket ederek programına göre tüketiciyi yönlendirebilmesi gibi.

Tüketicilerin verileri dikkate alınarak gerçekleştirilen büyük veri analiziyle tercihleri ve satın alma alışkanlıkları etkilenen bireyler bakımından, geleneksel tüketicinin korunması hukuku artık sınır ötesi bir mahiyete bürünmektedir. Analizi yapan işletme ile tüketicinin farklı hukuk sistemlerine tâbi olması ortaya çıkan uyuşmazlıkların çözümünde zorlukları beraberinde getirecektir. Ayrıca, büyük veri analizinde kullanılan gömülü yazılımlar tarafından nesnelerce üretilen verilerin üretici firmaya mı yoksa tüketiciye mi ait olduğu hususu yeni bir tartışma konusu olarak gündeme gelmektedir.

1.4.4. Büyük veride işgücü/insan kaynağı

Büyük veri çözümlerinin uygulanabilmesi kurum/kuruluşlarda ve devletlerde radikal dönüşümleri ve insan kaynaklarında köklü değişiklikleri gerektirmesinin yanında bu alanda ısrarcı bir üst yönetimi de gerektirmektedir MGI tarafından hazırlanan araştırma raporunda büyük verinin dönüştürücü etkisinin sağlık sektöründen perakende sektörüne, üretimden seçim kampanyalarına kadar pek çok sektör üzerinde ne kadar önemli olduğu ortaya konulurken, ABD'nin daha şimdiden 190 binden fazla derin analiz yapacak uzmana ve bu bilgileri yorumlayabilecek 1,5 milyondan fazla yöneticiye ihtiyacı olduğu öngörülmektedir.[62]

Son yıllarda büyük veri üzerine dünyadaki farklı birçok üniversitede birçok araştırma merkezi ve enstitü kurulduğu görülmektedir. Söz konusu üniversite ve araştırma enstitüleri, başta veri bilimcileri ve veri mühendisleri olmak üzere büyük veri analitiği üzerine çalışabilen yetenekleri yetiştirmek için lisans/lisansüstü müfredatlarını oluşturmuştur. Diğer yandan büyük veri çalışmaları yalnızca veri

[62] MGI, 2011: 39

bilimcileri veya BİT uzmanlarının yeterli olamayacağı; veri bilimi, matematik, sosyal bilimler, ağ bilimleri, sistem bilimi, psikoloji ve ekonomi de dâhil olmak üzere pek çok disipline hâkim olmayı gerektirir bir mahiyet arz etmektedir.

2. BÜYÜK VERİ UYGULAMALARININ VERİ MAHREMİYETİ KURALLARI BAĞLAMINDA DEĞERLENDİRİLMESİ

2.1. Dijital Çağda Güvenlik ve Mahremiyet İhtiyacı

Verinin bir değer kaynağı olarak analiz edilmesi, saklanması, üçüncü taraflara satışı, yeniden kullanımı ve/veya yeni amaçlarla kullanılmak üzere değiştirilmesi gibi etkinliklerin gün geçtikçe artması bireysel kaygıları da beraberinde getirmektedir. Zira büyük veri yığınlarıyla ve söz konusu yığınlardan anlamlı sonuçlar çıkarılması yeteneğinin gelişimiyle doğru orantılı olarak hemen hemen toplumun tamamı üzerinde gerçekçi analizler yapılabilmektedir. Bu durumun temel politikalar başta olmak üzere bütün düzenlemeleri derinden etkileyeceği öngörülmektedir.

İklim ve hava verilerinin kullanılmasıyla üretilen yenilikçi hizmetlerde olduğu gibi kişisel veriler hiç kullanılmadan büyük veri analizlerinin gerçekleştirildiği pek çok örnek bulunabilmektedir. Bununla birlikte, büyük veriyi oluşturan verilerin çoğunlukla bireyler hakkındaki veriler olduğu bilinmektedir. Kişisel verilerin işlenmesini içeren birçok büyük veri analizi örneği dikkate alındığında, veri işleyenlerin kişisel verilerin korunmasına ilişkin yükümlülüklere uygun hareket etmeleri gerekmektedir.

Kişisel veriler günümüz piyasasında en sıcak ticari mal olarak değerlendirilmektedir. Veri depolama ve işleme teknolojileri sayesinde bugün bireyler hakkında hiç bir çağda olmadığı kadar bilgiye sahip olunabilmektedir. Ticari işletmelerin, STK'ların ve kamu kurum ve kuruluşlarının bireylerin davranışlarını öngörmek ve kontrol etmek adına ellerinde bulunan veriyi nasıl kullandıkları hususu ise 21. yüzyılın en temel sorularından biri haline gelmiştir.

Bir yandan büyük veri analizinin faydaları (tüketici tercihleri, gelişmiş sağlık hizmetleri, terörden korunma gibi) artırılırken diğer yandan büyük verinin olumsuzluklarının azaltılması (mahremiyet eksiği, ayrımcılık gibi) gerekmektedir. Zira bireyler, işletmeler, araştırmacılar ve kamu bakımından çok önemli ekonomik ve sosyal faydaları bünyesinde barındıran büyük verinin, veri koruması ve mahremiyet alanlarında ortaya çıkardığı soru işaretleri giderilmeden gelişmesi ve ilgili sektörlerde güven temin etmesi mümkün gözükmemektedir.

Mahremiyet konusundaki endişelerin büyük verinin hangi temel özelliğiyle nasıl ilişkili olduğunun belirlenmesi ise bu alanda çözülmesi gereken temel hususlardan biridir. Hangi faaliyet ve işlemlerin (toplama, depolama, analiz, işleme, yeniden kullanım ve paylaşım gibi) mahremiyete ilişkin temel kaygıları getirdiğinin araştırılması gerekmektedir. Güçlü bir yönetişim ile süreç ve standartların doğru belirlendiği bir ekosistemin tesisi gerekmektedir.

2.1.1. Büyük veri ile ortaya çıkan güvenlik ve mahremiyete ilişkin kaygılar

Verinin yenilikçi kullanımlarının keşfi amacıyla depolanan büyük miktarlarda veriden (kişisel veri olmasa dahi), bireylere ilişkin cinsel yöneliminden sağlık durumuna kadar pek çok hassas kişisel veri konusunda ayrıntılı bilgi elde edilmesi mümkün hale gelmiştir.[63] Bireylere ilişkin en önemli veri kaynaklarından biri olarak internet ele alınırsa, bireylerin hayatlarına dair verecekleri en önemli kararlara ilişkin olarak dahi arama motorlarını çekinmeden kullanma eğiliminde oldukları görülmektedir. Örneğin; bireylerin sağlık durumuna dair endişelerini, gitmeyi planladığı mekânları veya iş değiştirme kararlarını kolaylıkla arama motorlarına sundukları düşünülürse söz konusu arama motorlarının bireyin hayatına dair birçok önemli bilgiye (yalnızca hareketleri değil düşünceleri de dâhil) sahip olduğu görülmektedir. Veri depolama teknolojileri sayesinde bu bilgiler saniyesi saniyesine tutulmakta, analiz edilmekte ve uzunca bir süre saklanabilmektedir. Bu anlamda, örneğin; Google'ın bireyler hakkında kendilerinin dahi hatırlayabildiğinden daha fazla bilgiye sahip olduğu[64] düzlemde, henüz eyleme bile dönüşmemiş düşüncelerin de depolanması karşısında gelecekte bu verilerden hangi çıkarımların ortaya konulacağı ve bu çıkarımların hangi amaçlarla kullanılacağı öngörülememektedir.

Verinin bir kez elde edilmesinden sonra söz konusu verinin kim tarafından, nasıl ve/veya hangi amaçlarla kullanıldığı konusunda bireylerin hiçbir kontrole sahip olmadığının inkâr edilemezliği karşısında kişisel verilerin kullanımı hususundaki mahremiyet kaygılarının dikkatle ele alınması ihtiyacı bulunmaktadır.

---

[63] Daniels, 2013: 1
[64] Mayer-Schönberger, 2011: 7

Ayrıca, bireylerin yukarıda ifade edildiği üzere bizzat kendileri tarafından doğrudan çevrimiçi sağlanan veriler dışında; işletmeler, kuruluşlar ve bireylerin tuttukları büyük veri setleri, neredeyse her ihtiyacı karşılayacak arama yapılabilen ve istenen verinin kolayca bulunabildiği pazar platformları işlevi görmektedir. Bu pazar platformları kişisel veri hazinesi mahiyetinde dijital platformlardır.

Veri pazarları, tek bir sektör üzerinde yoğunlaşanlarda olduğu üzere çok spesifik hizmetler sunabileceği gibi, birden fazla veri sahibi grubun izlendiği, tarihsel performans ve göstergeler gibi izlenen davranış kümelerinin değişken olduğu oldukça geniş bir kapsamda da hizmet verebilmektedir. Örneğin; *Thomson Reuters* firması, bir birey veya bir şirketle salt 'iş yapma riski' hakkında veri sunarken; *Gnip*, bütün sosyal medya kaynaklarına odaklanmakta veya *Microsoft Azure* yalnızca kendi müşteri ve ortaklarından elde ettiği veri setleri üzerinden ve onlara yönelik hizmetler sunarken; *Nielsen* firması çalışmakta olduğu bütün endüstri sektörlerine yönelik veri setleri üzerinden çeşitli hizmetler sunmaktadır. Ayrıca, birçok veri setinin bir araya toplanması ve izleme yönteminin kullanılması yoluyla odaklı kullanıcı profilleri (e-posta adresleri, ikamet adresi, isim, gelir, sosyal ağlar ve daha pek çok şey) oluşturarak reklam verenler odaklı çalışan Rapleaf, Acxiom, Choice-Point gibi firmalar da bulunmaktadır. Burada sayılan örnek firmalar pazarın yalnızca küçük bir kısmını temsil etmekte olup; bugün reklam yerleştirme, bireylerin nerede olduğunu belirleme, hayırsever bir bağış talep etme veya bir suçun nerede işlenebileceğini tahmin etme gibi amaçlarla veri setleri üzerinden hareket edilerek faydalı bilgi elde etmeye yardımcı olacak birçok analitik ve veriye dayalı hizmet sunulmaktadır.[65]

Satın alınabilen veya ücretsiz olarak temin edilebilen veri setlerinin sayısı, onları oluşturan verilerin kendisi kadar hızlı büyümektedir. Bu durum ise veri pazarlarının, kişisel verilere ulaşmayı kolaylaştıran herhangi bir veri setini hızlıca bulabilmesini ve satın almasını sağlamaktadır. Söz konusu veri pazarlarına kolayca erişilmesi ise bu verilerin sızdırılması gibi olumsuz sonuçları da beraberinde getirmektedir. AT&T firması tarafından yapılan bir araştırmaya katılan 120 internet sitesinin yüzde 56'sı doğrudan kişisel verileri sızdırdığını ifade etmiş; sitenin kullanıcılara sağladığı kullanıcı kimliğinin sızdırılmasının da kişisel veri sızdırması

[65] Craig ve Ludloff, 2011: 55

kabul edildiği durumda ise bu oranın yüzde 75'e çıktığını ifade etmiştir. Her bir kategori için incelenen 10 sitenin 9'unda, sağlık sitelerine gönderilen hassas veriler veya uçuş rezervasyon sitelerindeki güzergâh bilgileri de dâhil, veri sızdırıldığı ortaya çıkmıştır.[66]

Veri pazarları bağlamında, ne kadar fazla veri setine erişilir ve bağlanılabilirse, o kadar kişisel veri edinilebilmekte veya daha sonra bu veriler belirli bir kişiyle bağlantı kurmak amacıyla kolayca kullanılabilmektedir. Bu setlerin satın alınmasından sonra ne olacağı ve daha sonra işletmelerce veya araştırma amaçlı kuruluşlarca nasıl kullanılacağı bilinmemektedir. Anonimleştirmenin bir çözüm olarak öngörülmesi ihtimali ise, söz konusu teknik çözümün, Netflix'in araştırma yarışmasında da ortaya çıktığı üzere[67], büyük veriyle kolayca kırılabilmesi karşısında şüpheyle karşılanmaktadır. Zira günümüz teknolojileriyle, verilerin görünüşte tamamen anonim şekilde tutulduğu durumlarda bile (örneğin; belirli bir zaman dilimi içerisinde mağazaya giren müşteri sayısına ilişkin veritabanı ile güvenlik kontrollerini sağlamak için kullanılan kamera kayıt kontrol sistemi veritabanı olmak üzere), iki büyük veritabanı aynı anda kullanılarak kişisel bilgilerin ortaya konulması mümkün olabilmektedir.[68] Nitekim AB Veri Koruma Komiseri de kişilere ilişkin verilerin tam anlamıyla ve geri döndürülemeyecek şekilde anonimleştirilebilmesinin neredeyse imkânsız olduğunu ifade etmektedir.[69] Bu çerçevede veri madenciliği gibi büyük veri yöntemlerinden faydalanılmasıyla farklı kaynaklardan birden fazla veri seti kullanılarak kişinin kimliğini belirlenebilir kılan verileri biraraya getirmenin "mozaik etkisi" yaratacağı öngörülmektedir.

OECD 2017 Dijital Ekonomik Görünüm Raporu'nda da, büyük veri kapsamında toplanan verilerin ve büyük veri analizinin kullanılmasıyla mahremiyete ilişkin risklerin arttığı ifade edilmektedir. Raporda kişisel verilerin mahremiyetine ilişkin temel tehlike, başlangıçta kişisel verilerin kötü niyetli faaliyetler sonucu elde edilmesi veya kazara kaybı olarak ifade edilirken; bugün bunlara ek olarak, doğrudan

---

[66] Krishnamurthy ve ark., 2011: 1
[67] Narayanan ve Shamikov, 2007: 15
[68] Ohm, 2009: 53
[69] Avrupa Birliği Veri Koruma Komiserliği Resmi İnternet Sitesi, "Opinion on Privacy and Competitiveness in the Age of Big Data", 2014, (erişim tarihi 05.05.2016), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

kişisel veriye ihtiyaç duymayan kalıp ve korelasyonlar kullanılarak bu verilerden analiz yoluyla türetilebilecek tamamlayıcı verilerle, kişisel verilere erişilebilmesi olarak tanımlanmaktadır.[70]

Büyük veri analizlerinin kötüye kullanılmasından kaynaklanan kişisel verilere ve mahremiyete ilişkin ihlaller OECD tarafından aynı raporda şu iki başlık altında ele alınmaktadır:[71]

- *Ölçek ve profil bakımından kişisel veri ihlalleri artmıştır:* Kuruluşların büyük miktarda kişisel veriyi topladığı ve işledikleri bir ortamda, veri ihlalleri olarak adlandırılan kişisel verilerin mahremiyetini etkileyen ihlaller artmıştır. İngiltere Hükümeti tarafından 2014 yılında yapılan bir araştırmaya göre, büyük kuruluşların yüzde 81'i güvenlik ihlaline uğramıştır. 2015 yılında, 5,6 milyon parmak izini de içeren ABD Personel Yönetimi Bürosunun karşı karşıya kaldığı ihlalde, Büro tarafından depolanan 21 milyondan fazla kayıt çalınırken Japonya Emeklilik Hizmetleri'nden 1 milyon 250 bin vatandaşın verisi çalınmıştır. Raporda söz konusu ihlallerin maliyetlerinin hesaplanmasının zor olduğu ifade edilmektedir. Bununla birlikte, veri işleyen kuruluşlar için en büyük maliyet unsuru, iş kaybı veya ihlalinin tüketici güveni üzerindeki olumsuz etkisi olarak ifade edilmektedir. İkinci en yüksek maliyet unsuru ise, ihlal neticesinde ortaya çıkan zararın sorumlu kuruluş tarafından giderilmesi olarak ifade edilmektedir. Örneğin; 2006 yılında ChoicePoint, FTC'ye 26 milyon ABD dolarından fazla ödeme yapmak durumunda kalırken, AT&T şirketi, 2016 yılında yaklaşık 280 bin müşterisine ilişkin veri ihlalleriyle ilgili FTC soruşturmasında uzlaşma için 25 milyon ABD doları ödemeyi kabul etmiştir.
- *Büyük veri analizi ile bireysel mahremiyete yönelik yeni riskler ortaya çıkmıştır:* Veri analizinde kaydedilen ilerlemelerle, eski satın alma alışkanlıkları veya elektrik tüketimi gibi önemsiz görünebilecek bilgilerden dahi hassas kişisel verilere ulaşılmasının mümkün olduğu ifade edilmektedir. Nitekim ABD merkezli perakende şirketi Target'in geçmiş satın alma verilerine ilişkin kronolojik göstergelere ve müşterilerinin görsel analizine dayanan büyük veri çalışması

[70] OECD, 2017: 250
[71] OECD, 2017: 264-265

sonucunda bir genç kızın hamile olduğunu ailesinden önce tespit etmesinin, bu alanda çarpıcı bir örnek olduğu ifade edilmektedir. Büyük veri analizi kapsamında elde edilen öngörülerin kötüye kullanımının, mahremiyet hakkının temel değer ve ilkeleri olan bireysel özerklik, eşitlik ve ifade hürriyetini olumsuz etkileyebileceği ve toplumda öngörülmesi güç etkiler yaratabileceği tartışmalarını beraberinde getirmektedir.

Büyük miktarlarda tüketici verilerinin toplanması ve analiz edilmesiyle işletmelerin, tüketici talebindeki ve bireysel tercihlerdeki değişiklikler gibi toplam eğilimleri öngörebilecekleri ve böylece risklerini en aza indirerek pazarlama yatırım gelirlerini en üst düzeye çıkarabilecekleri ifade edilmektedir. Ayrıca, bireysel davranışları gözlemleyerek, ürün ve hizmetleri nasıl geliştireceklerini öğrenerek onları yeniden tasarlayabilecekleri ifade edilmektedir. Söz konusu kullanımların tüketici konumundaki bireylere fayda sağlayabileceği de kabul edilmektedir. Ancak, hedefli mesajların ve pazarlama tekliflerinin profil haline getirilmesi ve bu kişilere gönderilmesinin olumsuz sonuçlar da doğurabileceğinin göz ardı edilmemesi gerekmektedir. Zira bireylerin çevrimiçi etkinliklerinin izlenmesine itiraz etme; fiyat ayrımcılığının bir sonucu olarak daha yüksek fiyatları ödemeyi kabul etmeme ya da ihtiyaç duymayacakları ürün ya da hizmetlere yöneltilmeme istekleri önem arz etmektedir.

Büyük veri, modern mahremiyet düzenlemelerinin dayandığı adil veri işleme uygulamaları bakımından bir tehdit oluşturmaktadır. Büyük veri analizleri sayesinde işletmeler daha başarılı reklam/promosyon uygulamaları geliştirebilmekte, tüketici tercihlerini etkileyebilmektedir. Nitekim bazı analistler, bireylerin ciddi bir hastalığa yakalanma ihtimalini belirleyebileceklerini ve bu bilgileri kullanarak sigorta poliçesi pazarlamanın oldukça kolay olduğunu ifade etmektedir. Bugün, bazı hayat sigortalarının uygulanması konusunda sigorta şirketleri, bireylerin tüketim alışkanlıklarına ilişkin veriler üzerinden beklenen yaşam süresini hesaplamakta ve söz konusu veriler ışığında prim oranı ile hizmetin kapsamı gibi unsurlara karar vermektedir.[72]

---

[72] Drum, "Privacy is dead. Long live transparency!", 2013, (erişim tarihi: 11.07.2017) http://www.motherjones.com/politics/2013/10/future-of-privacy-nsa-snowden, 11.07.2017

Büyük verinin, savunmasız ve teknolojik açıdan yetersiz bireylerin mahremiyetini olumsuz etkilemesi karşısında bireylerin çevrimiçi eylemlerinin hassasiyet derecesini değerlendirebilir hale gelmesi önem arz etmektedir.

İşletmelerin ve bireylerin büyük veri hakkındaki algılarını ölçmek amacıyla bazı ülkelerde gerçekleştirilen ve sonuçları Tablo 2.1'de yer alan ankete göre işletmelerin büyük bir kısmı güvenlik ve mahremiyet konularında hazırlıksız olduklarını ifade etmişlerdir. Bireyler de işletmeler ile aralarındaki güven eksikliği ve kişisel bilgilerinin muhtemel kötüye kullanımı konusunda endişelerini dile getirmiştir.

Tablo 2.1.İşletmelerin ve Bireylerin, Büyük Veriye Yönelik Algıları ile İlgili Anketlerin Temel Bulguları

Anketi yürüten kuruluş	Dönem	Hedef kitle	Temel bulgular
İşletmelere yapılan anketler			
Software specialist, Informatica	2012	600 BT ve hizmet sektörü profesyoneli	Katılanların yüzde 38'inde güvenlik ve mahremiyet endişelerinin artmakta olduğu tespit edilmiştir.
BARC Institute	2012'nin ikinci yarısı	274 BT ve iş çözümleri profesyoneli (Almanya, Avusturya, İsviçre, Fransa, Birleşik Krallık)	Katılımcıların yüzde 25'i veri gizliliği sorunlarıyla karşılaşmayı beklediğini ifade etmiştir.
Information Systems Audit and Control Association (ISACA)	2013	2013 Avustralya ve Yeni Zelandalı BT profesyoneli	Katılan işletmelerin yüzde 5'i etkin bir yönetişim ve mahremiyet sağlamak için "çok hazırlıklı" olduklarını söylerken, yüzde 45'i "yeterli hazırlıklı" olduğunu, yüzde 25'i ise "hiç hazır değil" durumda olduğunu söylemiştir.
Voltage Security	InfoSecurtiy Europe kapsamında Nisan 2013	300'den fazla üst düzey BT ve güvenlik uzmanı	Katılanların yüzde 76'sı büyük veri girişimlerinde veri güvenliğinin sağlanamamasından endişe duyduğunu ifade etmiş; yüzde 56'sı güvenlik endişeleri nedeniyle bulut/büyük veri projelerini başlatamayacaklarını veya bitiremeyeceklerini bildirmiştir.
SAP	GSMA Mobil Dünya Kongresi, 2014, Barselona	300 mobil operatör, sabit telekom sağlayıcısı ve diğer yöneticiler	Katılanların yüzde 38'i güvenlik ve mahremiyet kaygıları dolayısıyla kuruluşlarının büyük verinin potansiyelinden tam olarak yararlanamadığını belirtmiştir.
Ovum	2013	500 orta ve büyük ölçekli kuruluş BT yöneticisi (İngiltere, Fransa, Almanya)	Katılanların yüzden 53'ü büyük veri konusunda güvenliğe ilişkin çeşitli endişeleri bulunduğunu ifade etmiştir.
Bireylere yapılan anketler			
Cable Forum (cableforum.co.uk)	2008	Forum ziyaretçileri	Katılanların yüzde 95'i üçüncü bir tarafça çevrimiçi faaliyetlerinin izlenmesini, anonim olarak dahi olsa, istemediğini ifade etmiştir.
Pew Internet & American Life Project	2012	2.254 ABD'li yetişkin arasında yapılan ulusal anket	Akıllı telefon sahiplerinin yüzde 30'u başkalarının bu bilgiye erişebileceği endişeleri nedeniyle yer/konum izleme özelliğini kapattığını söylemiştir.
Boston Consulting Group	2013	12 ülkeden 10.000 tüketici	Katılanların yüzde 75'i için "en önemli sorun" kişisel verilerin gizliliği olarak ifade edilmiş; katılanların sadece yüzde 7'si bilgilerinin başlangıçta toplanan amaçlar dışında da kullanılmasına izin vereceğini ifade etmiştir.
Ovum	2013	11 ülkeden 11.000 kişi	Katılanların yüzde 68'i arama motorunda kolayca sunulan bir hizmet olması durumunda, izlenmeme (do-not-track) özelliğini kullanacağını belirtmiştir; sadece yüzde 14'ü internet şirketlerinin kişisel veri kullanımları konusunda dürüst olduğunu düşündüğünü ifade etmiştir.

Kaynak: Nir Kshetri, 2014.

Voltage Security'nin anketine göre, işletmelerin özellikle yüksek hızlı veri toplamak için tıklama akışı, mobil cihazlardan gelen GPS verileri ve sosyal medya kullanımları, tüketicilerin kişisel verilerinin kötüye kullanımı veya yanlış kullanımı konusundaki endişeleri dolayısıyla sert bir dirençle karşılaşmaktadır. Pew Internet araştırma kuruluşu tarafından 2013 yılında ABD'de yapılan bir ankete göre katılımcıların büyük bir bölümü mahremiyet ve güvenlik kaygılarıyla, örneğin; konum izleme özelliklerini kapamak gibi önlemlere başvurmaktadır. Benzer şekilde, kâr amacı gütmeyen Cable Forum tarafından yapılan araştırmada ankete katılanların yüzde 95'i çevrimiçi faaliyetlerinin üçüncü bir tarafça, anonim bir şekilde olsa dahi, izlenmesini reddedeceklerini ifade etmiştir.

Büyük verinin sunduğu fırsatlardan yararlanmak isteyen işletmelerin ve kuruluşların potansiyel yenilikçi kullanımları keşfedebilmeleri için büyük miktarda kişisel veri depolamaları gerekmektedir. Verinin depolanabildiği ilk zamanlarda kimsenin aklına gelmeyen verinin yenilikçi ikincil kullanımı ise asıl tartışmayı beraberinde getirmektedir. Zira anketlerde de ortaya çıkan genel eğilime göre bireylerin büyük kısmı kişisel verilerinin ikincil kullanımına karşı olduğunu ifade etmektedir.[73]

Özetle, büyük veri kavramının "hacim, hız ve çeşitlilik" özelliklerinin yansıması olarak, veri mahremiyeti konusunda da şu üç temel etki öne çıkmaktadır: (1) kişisel verilerin tutulma ve işlenme maliyetleri önemli ölçüde düşmüştür, (2) büyük miktarda veriyi analiz etmeye yönelik algoritmalar geliştirilmiş (bu anlamda "veri analitiği"nin önemi giderek artmıştır) ve (3) çevrimiçi veri üreten ve toplayan endüstriler kendi geniş veri havuzlarını yaratmıştır. Söz konusu etkiler ise mahremiyet çevrelerinde, büyük veriye ilişkin şu temel endişeleri ortaya çıkarmıştır:

- Anonimleştirildiği veya bulanıklaştırıldığı iddia edilen verilerin yeniden kişiyle ilişkilendirilebilmesi potansiyeli,
- Büyük veri setlerinin temel toplanma amacının ötesine geçilerek farklı amaçlarla yeniden kullanılması,

[73] Mayer-Schönberger ve Cukier, 2013: 153

- Özellikle salt korelasyona dayalı analizin yapıldığı durumlarda bireylere ilişkin elde edilen çıkarımların şeffaflık içerisinde paylaşılmaması ve yanlış çıkarımların ortaya konulması ihtimali,
- Hemen hemen bütün verilerin kapsamlı bir şekilde toplanması eğilimi ve bu doğrultuda, veri koruma hukukunun kabul gören ilkelerinden olan veri minimizasyonundan[74] uzaklaşılması.

AB 29. Madde Çalışma Grubunun da belirttiği üzere, nesnelerin interneti gibi sınırsız veri kaynakları ve söz konusu verilerin analizi sayesinde elde edilen bilgilere dayanarak bir bireyin tüm yaşam ve davranış kalıplarının keşfedilmesi mümkün görünmektedir. Veri analizine dayalı şeffaf olmayan çıkarımların ise toplumda ayrımcılığın ortaya çıkmasına sebep verecek potansiyeli bünyesinde barındırdığına dikkat çekilmektedir. Zira büyük veri uygulamaları sonucu oluşturulan bireysel profiller dolayısıyla, toplumda bazı bireylerle aynı hizmetlere ve olanaklara erişemeyen bir "veri alt sınıfı" oluşturulması tehlikesi hiç de uzak görünmemektedir. Bugün modern bir distopya gibi değerlendirilen söz konusu profilleme yaklaşımı, günümüz gerçekliği içerisinde dahi kolayca örneklerini bulabilmektedir. Bu anlamda, Çin'in vatandaş puanlama uygulaması (bkz. Kutu 2.1) ve e-ticaret firmalarının fiyat farklılaştırması yöntemleri örnek olarak sayılabilmektedir.

[74] Bu kavram 6698 sayılı Kanun bağlamında, kişisel verilerin işleme amaçlarıyla bağlantılı, sınırlı ve ölçülü işlenmesi ilkesine karşılık gelmektedir.

Kutu 2.1. Çin'de Uygulanan "Sosyal Kredi Sistemi"

Çin Devlet Konseyi tarafından Haziran 2014'te "Sosyal Bir Kredi Sisteminin Tesisi İçin Plan Taslağı" başlıklı bir belge yayımlanmıştır. Çalışmalarına 2010 yılında başlanan ve Jiangu bölgesinde pilot proje olarak uygulanmakta olan "Sosyal Kredi Sistemi"nin 2020 yılından itibaren tüm ülkede uygulanması hedeflenmektedir. Hükümet tarafından sekiz özel şirkete sosyal kredi puanı sistemi tasarlaması ve bu amaçla algoritmalar geliştirmesi amacıyla yetki verilmiştir. Hâlihazırda yalnız gönüllü vatandaşların katıldığı sisteme, 2020 yılından itibaren katılım zorunlu hale gelecektir.

Sisteme geçişle birlikte ülkede tüm vatandaşlara kişisel kredi notu verilmeye başlanması öngörülmektedir. Vatandaşların mobil cihazlarına yüklenecek bir uygulama sayesinde vatandaşların davranışlarının anlık olarak denetlenmesi ve böylece bireylerin hem sanal hem de gerçek yaşantılarının devlet takibi altında tutularak puanlanması planlanmaktadır.

Bireyler hakkında büyük miktarlarda verinin özel firmalarca toplanmakta ve işlenmekte olduğu günümüzde bilinen bir gerçektir. Ancak Çin'de uygulanması öngörülen bu sistem söz konusu verilerin pozitif ya da negatif olarak sınıflandırılarak devlet tarafından belirlenen kurallara göre tek bir puana çevrildiği ilk uygulama olarak ortaya çıkmaktadır. Vatandaş hakkında yaratılan tek bir puan, kişinin güvenilir olup olmadığını tüm topluma afişe edecektir.

Puanlama sisteminin vatandaşların gerçek hayattaki davranışları kadar sosyal medya paylaşımları ile de ilişkili olması ve puanına göre sınıflandırılan vatandaşların banka kredisi başvuruları, internet hız kotaları, seyahat hürriyetleri ve evlenme hakları gibi pek çok haklarının devlet tarafından sınırlandırılabilmesi öngörülmektedir. Yüksek puan sahibi vatandaşlar belirli hizmetleri indirimli almak veya hızlı kredi temin edebilmek gibi belirli avantajlara sahip olabilirken; düşük puan sahibi vatandaşların çocuğunu gönderebileceği okuldan başvurabileceği işe kadar pek çok hakkı kısıtlanabilecektir.

Çin Hükümeti, bu sistemin vatandaş güveninin tesis edilmesi için hayata geçirildiğini savunmaktadır. Sistemle kamu yönetiminde, ticari ve toplumsal hayatta samimiyetin ve yargıya güvenin artacağı iddia edilmektedir.[75]

Profillemenin giderek kabul gördüğü bir sistemde, bireyin hayatı doğrudan etkilenmektedir. Örneğin; akıllı bir şehirde, belirli kişilerin veya belirli akıllı araçların bazı caddelere girmesinin yasaklanması; belirli eğlence kompleksi, mekân ya da mağazalara sınırlı sayıda bireyin girişine izin verilmesi gibi ayrımcı sonuçlar çok yakın bir zamanda ortaya çıkabilecektir.[76]

Büyük veriye ilişkin bir diğer endişe, özellikle bireylerin kontrolü dışında üretilen verilerin (nesnelerin interneti, akıllı şehirler gibi) önlenmesi güç hatalarla dolu olması ve bu sebeple bireylere ilişkin "türetilmiş büyük veri" profillerinin oluşmasıdır.

[75] Diab, 2017: 11
[76] Edwards, 2016: 22

Büyük veri kaynaklı mahremiyet ve güvenlik endişelerinin; veriyi işleyen birden fazla tarafın bulunması, üçüncü şahıslarca veriye erişilebilmesi, verilerin toplanması ve saklanması fiilleriyle sıkı bir bağlantısı olduğu değerlendirilmektedir. Söz konusu fiillerin özellikle yeterli farkındalık düzeyinde bulunmayan bireyleri ve teknolojik trendlerden haberdar olmayan tüketicileri olumsuz etkilemesi muhtemeldir. Bu kapsamda, özellikle bireylerin çoklu veri kaynaklarının farkında olması ve etkili arama ve karşılaştırma yapmalarını sağlayan birden fazla veri hizmet sağlayıcısının bilincinde olmaları gerekmektedir.

Ayrıca, üretilen çok miktarda verinin büyük kısmı bulutta depolanmaktadır. Bununla birlikte, bulutta yer alan veriler, çoklu yedeklemeler veya verilerin birden fazla ülkede dağıtılmış olarak işlenme ve çoğaltılması dolayısıyla, bilinmeyen veya değişen depolama alanlarında tutulmakta ve işlenmektedir. Bu durum ise zaten farklı hukuki yaklaşımlara sahip AB ve çoğu büyük bulut hizmet sağlayıcısının yerleşik olduğu ABD arasındaki ayrımın giderek keskinleşmesi riskini pekiştirmektedir.

2.1.2. Güvenlik ve mahremiyetin tesisi için yapılması gerekenler

Büyük veride çoklu veri kaynakları kullanılmakta ve üçüncü taraflara veri aktarımı yapılmaktadır. Verinin üçüncü taraflar ile paylaşılmadan önce anonim hale getirilmesinin imkânsız olduğunu savunan görüşler de bulunmaktadır. Ancak, araştırmacılar, verilerin kişiyi belirlenebilir kılan niteliklerinden sıyrılarak belirli bir kişiyle yeniden ilişkilendirilmesini önleyebilecek çeşitli yöntem ve tekniklerin bulunduğunu da savunmaktadır.[77] Bununla birlikte, büyük veri süreçlerinin, kişisel veriyi kolayca açığa çıkaran ve dolayısıyla anonimleştirmeyi imkânsız kılan öngörü modelleri yaratabildiği gerçeği mahremiyete ilişkin endişeleri artırmaktadır. Bu kapsamda, profilleme, ayrımcılık, fırsat eşitliğinin bozulması gibi sonuçların ortaya çıkması önlenirken hizmet sunan aktörlerin de yenilikçi faaliyetlerinin desteklenmesi gerekmektedir.

Büyük verinin kullanımı, bilhassa hukuki düzenlemeler bakımından bir gri alanı teşkil etmektedir. Büyük veri üzerine çalışmakta olan çoğu kuruluş henüz kişisel verilerin mahremiyetini ve güvenliğini sağlamak için en iyi uygulamaları

[77] Brill, 2012: 2

geliştirememiştir. Ayrıca, bu konuda yeterince uzmanlaşamayan denetleyici veri koruma otoriteleri de dikkate alındığında, tahmini modelleme gibi büyük veri metodlarıyla işlenen kişisel verilerin hassasiyet derecesini dikkate alan, en küçük firmalar düzeyinde dahi büyük veri politikalarına ihtiyaç olduğu değerlendirilmektedir.[78]

Gelecekte büyük veri ile ilgili politika ve mevzuat düzenlemelerinin kurgulanmasında hangi aktörlerin refahı, tercihleri ve görüşlerinin tercih edileceği hususu halen tartışılmaktadır. Ancak, artan bireysel endişelerin muhtemelen daha fazla düzenleyici tepkiyi beraberinde getireceği değerlendirilmektedir. Bu çerçevede, küresel anlamda getirilmeye çalışılan düzenleyici çözümler Bölüm 4.3'te ele alınmaktadır.

2.1.3. Geleceğe ilişkin hukuki senaryolar

Büyük veriyle ilgili hukukî öngörülerin, büyük veri teknolojilerinin beklenti zirvesine ulaşmakta olduğu dönemde hayata geçirilmesinin zor olduğu ifade edilmektedir. Zira doğası gereği statik bir yapıya sahip olan hukukun, dinamik bir sürekli akış eğilimine sahip teknolojik gelişmeleri çoğu zaman geriden takip etmek durumunda kaldığı kabul edilen bir gerçekliktir.[79]

Bugün, hemen her şeyden verinin akmakta olduğu ve söz konusu verilerin aynı hızla analizinin mümkün olduğu teknolojik düzlemde, bireyin özel hayatının gizliliğinin modern hukuki güvencesi olarak değerlendirilen veri mahremiyeti konusunda geleceğe ilişkin iki temel öngörü bulunmaktadır. Mahremiyet alanında geleceğe ilişkin öngörülen ilk senaryo; mahremiyet kavramının modern çağın yeni tabusu haline geleceği ve yeni teknolojilerin doğası gereği göz ardı edilebilir bir alan olarak giderek belirsizleşeceği varsayımıdır.

İkinci senaryoda ise; mahremiyet kavramı hakkında küresel anlamda varılan uzlaşma sayesinde güvenlik ve mahremiyetin geliştirilen her teknolojide başlangıçtan itibaren göz önüne alınan ve uygulanan bir özellik olarak yerini alacağı varsayılmaktadır. Bu yolla bireysel mahremiyetler korunurken teknolojik kaynaklar,

[78] Kshetri, 2014: 1143
[79] Fishleigh, 2014: 149-151

bütün olumlu özellikleriyle gerek bireysel gerekse toplumsal olarak faydaya dönüştürülecektir.

Kutu 2.2. Varsayılan Bir Özellik Olarak Mahremiyet Koruması

İkinci senaryoya ilişkin fütüristik çözüm öngörülerinden biri Hannu Rajaniemi tarafından "The Quantum Thief" adlı eserde ortaya konulmaktadır.[80] Rajaniemi, gelecekte insanların "gevulot" olarak bilinen teknolojik bir kalkan vasıtasıyla her türlü veri toplama ve izleme işlemi için görünmez olmayı seçebileceği bir çözümden bahsetmektedir. Gelecekte tamamıyla akıllı şehirlerde yaşayan insanların başkalarıyla olan tüm etkileşim ve veri açıklamaları, "gevulot" tarafından müzakere edilecektir. Örneğin; iki birey rastgele sokakta karşılaştığında, "gevulot" otomatik olarak mahremiyet tercihlerini gözden geçirecek ve müzakere edecektir. Sonuçta verilen kararda taraflardan biri görülmeyi istemezse, o zaman "gevulot" görsel korteksle etkileşim kurarak karşı tarafı otomatik olarak bulanıklaştıracak/susturacaktır. Şayet taraflar iletişim kurmak istiyorsa, o zaman üretilen içeriğin diğerleriyle paylaşılıp paylaşılamayacağı, ne kadarının hatırlanacağı, kamuya açık veya özel olarak mı konuşulacağı, duygusal tepkilerin paylaşılıp paylaşılmayacağı ya da yüz ifadeleri ve seslerin algoritmik olarak normalize edilip edilmeyeceği üzerinde uzlaşılan bir "gevulot sözleşmesi" ile anlık olarak belirlenecektir.

Bu senaryoda ortaya konulduğu gibi bir "topyekün mahremiyet toplumu" içinde yaşamak istenip istenmediği sorusu bir kenara konursa, hâlihazırda kişisel veriler ile ne yapıldığını kontrol etmeye ve söz konusu verinin izini sürmeye (bulanıklaştırılmış olsa bile) yardımcı olacak, kişisel verilere ilişkin bir dijital haklar yönetimi anlayışının geliştirilmeye çalışıldığı bilinmektedir.[81]

İnsanlığın teknolojik gelişmelerin mahremiyet kurallarının çok ötesine sıçraması karşısında yapılması gerekenin neler olduğuna karar vermek durumunda kalışı ilk değil ve son da olmayacaktır. Bu noktada, toplumların kendilerine sorması gereken temel soru; büyük veri çağında mahremiyetin hâlâ korunmaya değer bulunup bulunmadığı ve bu sorunun cevabının evet olması durumunda bu alanın yeniden nasıl düzenlemesi gerektiği noktasında düğümlenmektedir. Yakın bir gelecekte insan-veri etkileşimini önceleyen yaklaşımın genel kabul göreceği, bu çerçevede insanlığın verilerin akışının merkezinde yer alması ve vatandaşların bu sistemler ve verilerle açıkça etkileşimde bulunması amacıyla teknolojik mekanizmalar geliştirileceği öngörülmektedir. Mevcut gelişmeler ışığında mahremiyete doğrultulan bir namlu muamelesi gören veri teknolojilerinin, bireysel haklar ve toplumsal faydayı mümkün

[80] Rajaniemi, 2010
[81] Pearson veMont, 2011: 60-68

kılacak biçimde tasarlanarak tersine dönebileceği düşünülmektedir. Nitekim, gerek AB tarafından gerçekleştirilen reform çalışmaları gerekse OECD başta olmak üzere diğer uluslararası aktörlerin yaklaşımları teknolojik tasarımdan itibaren mahremiyetin öncelendiği bir hukukî düzenleme alanına doğru gidildiğini göstermektedir.

2.2. Büyük Veri Uygulamalarının Veri Koruma Hukukuna Etkileri

2.2.1. Büyük veri çağında mahremiyet

Büyük verinin veri mahremiyetine ilişkin getirdiği zorlukların ardından, politika yapıcılar tutarlı bir düzenleyici tepki ortaya koymaya çalışmaktadır. 2012 yılından beri OECD, AB ve ABD'nin mahremiyet çerçevelerinde kapsamlı bir gözden geçirme sürecine girmeleri bunun bir yansıması olarak görülmektedir. Bununla birlikte, bu reform çalışmaları kapsamında ortaya konulan yaklaşımın 1970'lerden beri var olan politika çerçevesinden güçlü bir şekilde ayrışmadığı görülmektedir.[82] Ancak, büyük veri özelinde mahremiyete ilişkin sorunların çözümünü sağlayan politika önerileri belirlenemediğinden bu alandaki ikilem varlığını sürdürmektedir.

Kişisel verilerin korunmasına ilişkin yasalar, temelde veri üzerinde bireysel kontrolün esas alındığı veri minimizasyonu ve amaçla sınırlılık gibi ilkelere dayanmaktadır. Kişisel veri toplamanın en aza indirilmesinin büyük veri bağlamında pratik bir yaklaşım olmadığı ortadadır. Daha az veri işlenmesini savunan temel ilkeler büyük verinin doğasına ters düşmektedir. Ayrıca, amaçla sınırlılık ilkesinin uygulama sahası olan rıza kavramı, bireysel mahremiyet ile verinin faydalı yenilikçi kullanımı arasında bir seçim yapılmasını zorlayan etkin olmayan bir mekanizmaya dönüşebilmektedir. Bu çerçevede, örneğin; AB Veri Koruma Reformu ile kabul edilen, kişisel veriye dayalı profillemenin tamamen hukuka aykırı tavsif edilmesi kuralı teknolojik gelişmelerden ve ticari hayatın gereklerinden kopuk görünmektedir.

Büyük veriye ilişkin problemlerin çözümü üzerine ortaya konulan fikirlerin teknolojik ütopyacılık gibi bir uç noktadan, aşırı düzenlemeye sebep olan yoğun bir korkuya kadar uzanması oldukça anlaşılır görünmektedir. Ancak, teknolojik gelişmeler, iş dünyası, sosyal ilişkiler ve etik değerler, modern toplumları büyük

[82] Tene, 2013b: 362

verinin avantajları ile bireysel haklar arasında uzlaşı sağlayan bir yaklaşım benimsemeye zorlamaktadır.

2.2.2. Sınır ötesi mahremiyet

Büyük verinin ortaya çıkmasına zemin hazırlayan temel gelişmelerden biri olan bulut bilişim teknolojilerinden, veride gerçekleşen üstel büyüme karşısında gün geçtikçe daha yoğun faydalanılmaktadır. Bulut bilişim sayesinde kuruluşların coğrafi sınırlara bağlı olmaksızın büyük verilerle çalışabilmesi ise kişisel verilerin işlenmesi alanında uygulanacak hukuk kurallarının belirlenmesini kritik hale getirmektedir.[83]

Nitekim AB Veri Koruma Tüzüğü ile getirilen, verinin aktarılacağı üçüncü ülkelerde AB'de sağlanan veri koruma çerçevesine uygun bir yeterli koruma düzeyinin sağlanması şartı, bu alanda uluslararası mevzuat uyumuna olan ihtiyacı ortaya koymaktadır. Ayrıca, OECD'nin 2017 Sayısal Görünüm Raporu'nda da OECD ülkelerinde hükümetlerin çoğunda kişisel verilerin korunması alanında uluslararası işbirliğine girme eğilimi olmakla birlikte, pek çoğunun hâlâ kendi mahremiyet politikalarını koordine etmekte geciktiği vurgulanmaktadır. Bu kapsamda, mahremiyet düzenlemelerinin koordinasyonu ve uyumlaştırılması yoluyla küresel anlamda birlikte çalışabilirlik, ele alınması gereken önemli bir sorun alanı olarak ortaya çıkmaktadır.

[83] Fishleigh, 2014: 151

3. DÜNYADA VE TÜRKİYE'DE KAMU HİZMETLERİNİN SUNUMUNDA BÜYÜK VERİYE İLİŞKİN TEMEL POLİTİKA VE UYGULAMALAR

Hızla artan büyük veriden ekonomik ve sosyal fayda üretmek amacıyla, ülkeler ve şirketler bu alana büyük ilgi göstermekte ve Ar-Ge çalışmaları başta olmak üzere, yüksek miktarda kaynak ayırmaktadır. Büyük veri araştırma ve uygulamalarının ticari işletmeler tarafından kar ya da verimlilik amaçlı kullanımının uluslararası kuruluşlar ve kamunun oldukça ilerisinde olduğu aşikar olmakla birlikte söz konusu fenomen son yıllarda başta uluslararası örgütler olmak üzere kamu hizmeti veren kuruluşların ve devletlerin de radarına girmiş bulunmaktadır. Zira gelecekte büyük verinin, ekonomik büyümenin bir göstergesi olarak kabul edilmesi ve devletlerarası rekabetin geleneksel konulardan öte büyük veri etrafında şekillenmesi beklenmektedir.[84] "Kalkınma İçin Büyük Veri" temasıyla 2012 yılında Birleşmiş Milletler, 2014 yılında ise Dünya Bankası ilk raporlarını yayımlamıştır.

3.1. Avrupa Birliği

Kamu sektöründeki verimliliği ölçmek çok zor olmasına rağmen ulusal gelişme konusunda büyük veri analizinin kamu sektörüne büyük katkı sağlayabileceği ifade edilmektedir. Yapılan araştırmalarda, büyük verinin etkin kullanımı sonucunda verimliliği artırmak için strateji geliştirecek herhangi bir Avrupa ülkesinin yönetimsel faaliyetlerindeki harcamalarından yıllık yüzde 15 ila 20 oranında tasarruf edebileceği iddia edilmektedir.[85] Verinin kurumların yönetim stratejilerini etkilemenin ötesine geçerek ülkelerin ekonomi politikalarına yansımaya başlamasıyla birlikte büyük veri kavramı Avrupa Komisyonu'nun ve dolayısıyla da Birliğin Dijital Gündem'ine girmiş bulunmaktadır.

2010 yılında yayımlanan Avrupa için Sayısal Gündem, Temmuz 2014'te yayımlanan veriye dayalı ekonomi üzerine kurgulanmış AB stratejisi, Ocak 2017'de yayımlanan Avrupa için Veri Ekonomisi Oluşturulması Belgesi, büyük veri ve açık veri alanlarında araştırma ve yenilik faaliyetlerinin desteklenmesi, veri teknolojilerine ilişkin standartların belirlenmesinin "Avrupa Endüstrisinin Sayısallaştırılması Girişimi" bağlamında beş öncelik alanından biri olarak belirlenmesi, "Bir Avrupa

[84] Jin ve ark., 2015: 60
[85] MGI, 2011: 3

Gigabit Topluluğu için Bağlantı (Connectivity for a European Gigabit Society)" ile bağlanmanın veri ekonomisinin vazgeçilmez bir unsuru olarak belirlenmesi ve açık veri ile açık erişim politikaları AB'de büyük veri konusunda atılmakta olan önemli adımlar olarak dikkat çekmektedir.[86]

Şekil 3.1. Büyük Verinin AB Bakımından Yaratacağı Etki

Kaynak: Avrupa Komisyonu, Sayısal Tek Pazar, Temmuz 2014.

Ayrıca, ifade edilen politika belgeleri dışında uygulamaya yönelik olarak başta Avrupa İçin Büyük Veri platformu olmak üzere kilit önemi haiz sektörlerde (sağlık, tarım, enerji, ulaştırma, iklim, sosyal bilimler ve güvenlik) gelişmeye katkı sağlamak ve bu yolla toplumsal ihtiyaçları karşılamak için büyük veriden fayda yaratmak amacıyla yenilikçi teknolojiler, stratejiler ve yetkinlikler geliştirilmeye çalışılmaktadır (Şekil 1.). Belirlenen sektörler bakımından AB'de önemli sorun alanı oluşturan problemlerin çözümü amacıyla pilot projeler hayata geçirilmekte, sonuçları çeşitli etkinlikler vasıtasıyla (seminerler, çevrimiçi çalıştaylar (webiner), çalıştaylar vb.) kamuoyuyla paylaşılmaktadır.[87]

---

[86]Avrupa Komisyonu resmi internet sitesi, (erişim tarihi: , 20.06.2016), https://ec.europa.eu/digital-single-market/en/big-data

[87] Big Data Europe Girişimi internet sitesi, (erişim tarihi: , 20.06.2016), https://www.big-data-europe.eu/ 20.06.2016

Büyük Veri Kamu-Özel Forumu da AB'nin bu alanda ciddi yatırımlar ve teşvik programları uygulamaya çalıştığı platformlardan biridir.[88] AB'de büyük veri bağlamında kendi kendini sürdürebilir bir endüstrinin ortaya çıkarılması amacıyla; veri toplamak için uygun teknik kanalların oluşturması, karar alıcıların sektörler tarafından doğru yönlendirilebilmesi, büyük veri teknolojisinin getirdiği değişim dalgasının benimsenmesinin teşvik edilmesi ve politika ve mevzuatta yer alan engellerin kaldırılması hedeflenmektedir.

3.2. Birleşmiş Milletler

BM İstatistik Komisyonu, 45'inci oturumunda büyük verinin avantaj ve zorluklarının, sürdürülebilir kalkınma hedeflerinin izleme ve değerlendirilmesi bakımından taşıdığı potansiyel de dahil olmak üzere, daha iyi anlaşılabilmesi amacıyla "Resmi İstatistikler için Büyük Veri Küresel Çalışma Grubu"nun (Global Working Group-GWG) kurulmasına karar vermiştir. Bu çerçevede, GWG'nin, büyük verinin kullanımı alanında fayda ve maliyet analizleri yapmasının yanı sıra metodoloji, kalite, teknoloji, veri erişimi, mevzuat, mahremiyet, yönetim ve finans gibi pekçok konuda çalışma ihtiyacı duyacağı ifade edilmektedir.[89]

"Küresel Nabız", Birleşmiş Milletler Genel Sekreterliğinin büyük veriye ilişkin başlatmış olduğu bir yenilik girişimi olarak ifade edilmektedir. Girişim ile, gelişmekte olan ülkelerdeki ekonomik krizlerle başa çıkmaya yönelik politikaların etkilerini anında algılayıp değerlendirmeye yönelik olarak büyük verinin kullanılması amaçlanmaktadır. Küresel Nabız girişiminin temelinde şu üç eylem alanı bulunmaktadır: ilk olarak, erişilen dijital veriler (internet ve özellikle sosyal ağlar yanında cep telefonlarından toplanan veriler) sayesinde yeni göstergelerin ortaya çıkarılmasıyla toplulukların refahının daha iyi anlaşılması ve uygulanan politikaların geri beslemelerinin anında öğrenilmesi, ikincisi kalkınma uzmanlarının kanıta dayalı kararlara ulaşabilecekleri özgür, açık kaynak kodlu yazılımlara ilişkin teknik altyapının geliştirilmesi ve son olarak her ülkede o ülkedeki uzmanlar tarafından kullanılacak nabız laboratuvarları (merkezler) kurulması ve bu merkezler arasında ağ oluşturulması. Günümüzde bu alanda kullanılan geleneksel veriler, yıllık

---

[88] Big Data Public Private Forum resmi internet sitesi, (erişim tarihi: 20.06.2016), https://www.big-project.eu/

[89] Birleşmiş Milletler Büyük Veri Küresel Çalışma Grubu resmi internet sitesi, (erişim tarihi: 20.06.2016), https://unstats.un.org/bigdata/

ortalamalardan oluşmakta ve söz konusu yıllık ortalamalar üzerinden ülkelerin politika kararlarının sonuçlarının öğrenilmesi uzun döneme yayılmaktadır. Girişim kapsamında, "Endonezya Gıda Fiyat Krizlerini Anlamak için Tweet Madenciliği", "Sosyal Medya Analiziyle İşyerinde Kadınlara Karşı Ayrımcılıkla İlgili Eğilimlerin Belirlenmesi", "El Salvador'da Yakıt Sübvansiyon Politikası Reformuna Kamu Duyarlılığını Analiz Etmek İçin Twitter Verilerinin Kullanılması", "Etkileşimli Görselleştirme Kullanarak Gana'daki Yönetişim ve Barışı Anlamak" ve "Endonezya'daki Profesyonel Eğitimin Oyun Verileri Yoluyla Geliştirilmesi" gibi pek çok pilot proje uygulanmaktadır.[90]

BM'ye bağlı olarak faaliyet gösteren, uzmanlık kuruluşu Uluslararası Telekomünikasyon Birliği (ITU), 2015 yılında büyük veri için ilk uluslararası standardını duyurmuştur. Söz konusu uluslararası standart ile bulut temelli büyük veri uygulamalarının küresel ölçekte başarıyla sürdürülebilmesi için gerekli özellikleri, kullanım alanları ve beklenen faydası ayrıntılarıyla anlatılmaktadır. Ayrıca, bulut bilişim sistemlerinin büyük veri hizmetlerini destekler şekilde nasıl geliştirilebileceği ele alınmaktadır. Kuruluşun tanımladığı standart, teorik olarak faydalı görülmekle birlikte büyük veri konusunda özellikle ticari kuruluşlarda hızla gelişen teknolojik işbirlikleri karşısında (başta teknoloji platformlarının kendi aralarında kurdukları bağlantı vb.) pratikte belirgin bir etki yaratmamaktadır.

ITU tarafından Kolombiya, Gürcistan, Kenya, Filipinler, İsveç ve Birleşik Arap Emirlikleri gibi ülkelerde sürdürülmekte olan "Bilgi Toplumunun Ölçülmesi ve Geliştirilmesi İçin Büyük Veri", "Büyük Veri ve BİT Endüstrisi", "Telekomünikasyon Sektöründe Büyük Veri" ve "Salgın Hastalıklarla Mücadelede Büyük Veri" gibi pilot projelerle belirli alanlarda elde edilen deneyimlerden dersler çıkarılarak, büyük veriden nasıl fayda elde edileceği konuları çalışılmaktadır.[91] Birleşmiş Milletler gibi bir kurumun karar alma mekanizmalarına yeni bir yaklaşımı, büyük veriyi dâhil etmesi önemli bir adım olarak değerlendirilmektedir.

---

[90] Girişim kapsamında yer alan tüm projelere ilişkin liste için bkz. http://www.unglobalpulse.org/projects

[91] Uluslararası Telekomünikasyon Birliği, Big Data for Measuring the Information Society, (erişim tarihi: 14.09.2016), http://www.itu.int/en/ITU-D/Statistics/Pages/bigdata/default.aspx

3.3. Amerika Birleşik Devletleri

Küresel anlamda büyük veri alanında en aktif ülkelerin başında ABD gelmektedir. ABD tarafından büyük veri politikaları konusunda atılmakta olan önemli adımlar aşağıdaki gibidir:

- 2010 yılında Bilim ve Teknoloji Başkan Danışmanları Konseyi tarafından yayımlanan Rapor ile büyük veri stratejisine ilişkin detayların ortaya konulması,
- 2012 yılında Obama Yönetimi tarafından bilim, sağlık, enerji ve savunma ile alakalı birden çok kuruma 200 milyon dolarlık bir yatırımı öngören Büyük Veri Ar-Ge Girişimi'nin başlatılması,
- Merkezi kuruluşların ve yerel yönetimlerin büyük veri projelerine önemli yatırımlar yapmaları (Örneğin; Ulusal Sağlık Enstitüsü yüzlerce terabaytlık genetik verisini kendi süper bilgisayarlarında saklamak yerine Amazon'un bulut ortamına yüklemiştir; ABD Savunma Bakanlığı ise büyük veriyi kullanarak makina öğrenmesi gerçekleştirebilmek amacıyla milyonlarca dolarlık yatırım yapmaktadır),
- 2014 yılında ABD Başkanı Obama'ya sunulan "Büyük Veri: Fırsatları Yakalamak, Değerleri Korumak" raporunda büyük veri uygulamalarının ekonomi ve diğer alanlarda olumlu yönlendirici etkilerine işaret edilirken bireyle devlet arasındaki güç dengesini bozması açısından, büyük veri uygulamalarının özgürlüklere olan potansiyel tehdidine de dikkat çekilmesi.

3.4. Türkiye'de Büyük Veriye İlişkin Mevcut Durum

Türkiye'de büyük veri alanında çalışmalara başlanılmakla beraber, gerçek anlamda büyük veri uygulama örnekleri sınırlı bulunmaktadır. Türkiye'deki haberleşme, perakende, bankacılık gibi müşteri bilgisinin ve müşteri davranışlarının yakından takip edildiği alanlarda faaliyet gösteren büyük özel şirketler, müşterileri ile ilgili toplamış oldukları büyük hacimdeki verileri kullanarak müşteri davranışlarını tahmin etme, müşterilerine sunulan hizmetlerin kalitesini artırma, müşteri memnuniyetini ve bağlılığını artırma, karar alma mekanizmalarına yardımcı olacak öngörüler üretme, ürün tasarımlarını müşteri beklentilerine göre şekillendirme, ürün fiyatlandırmasını optimize etme, detaylı müşteri segmentasyonu yapma ve ürünlerini sundukları kanalların verimliliğini artırma gibi alanlarda "veri madenciliği"

çalışmaları yapmaktadır. Büyük veri uygulamaları, özel sektörün yanı sıra yoğun miktarda veri üreten kamu kurum ve kuruluşları için de önemli potansiyel barındırmaktadır. Bu uygulamalar sayesinde, üretilen veriler kullanılarak detaylı, kapsamlı ve anlık analizlerin yapılması mümkün olmaktadır. Bu çerçevede, kamu kurum ve kuruluşları tarafından büyük veri alanında pilot uygulamaların hayata geçirilmesi önem arz etmektedir.[92]

Türkiye'de büyük veri ilk kez, Onuncu Kalkınma Planı'nın (2014-2018) "Açık kaynak kodlu yazılımlar, büyük veri, bulut bilişim, yeşil bilişim, mobil platform, nesnelerin interneti gibi ürün, hizmet ve yönelimler değerlendirilerek kamu için uygun olabilecek çözümler hayata geçirilecektir." hedefiyle resmi politika belgelerindeki yerini almıştır.

Ardından "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı"nda da büyük verinin ekonomik değere dönüşmesinin sağlanması ve sosyal güvenlik, sağlık, vergi, güvenlik gibi alanlar başta olmak üzere kamuda büyük veri uygulamalarının geliştirilmesi hedefi belirlenmiştir. Bu çerçevede, Eylem Planında yer verilen 49 no'lu "Kamuda Büyük Veri Pilot Uygulaması Gerçekleştirilmesi" eylemi ile, kamu kurum ve kuruluşları tarafından büyük veri alanında pilot uygulamaların hayata geçirilmesi, kamu verisi kullanılarak sosyal güvenlik alanında büyük veri pilot uygulamasının gerçekleştirilmesi ve başarı örneklerinin oluşturulmasıyla bu teknolojilerin Türkiye'de yaygınlaştırılmasına öncülük edilmesi hedeflenmektedir.

Eylem kapsamında Sosyal Güvenlik Kurumu (SGK) toplamış olduğu büyük miktardaki yapılandırılmış ve yapılandırılmamış veriler üzerinde çeşitli analizler yaparak verimliliği artırmak, kayıp-kaçak oranlarını düşürmek ve hizmet kalitesini yükseltmek amacıyla büyük veri alanında çalışmalara başlamıştır.

Onuncu Kalkınma Planında belirlenen hedef doğrultusunda TÜBİTAK-BİLGEM tarafından yürütülmekte olan "Bulut Bilişim ve Büyük Veri Araştırma Laboratuvarı" (B3LAB) Projesi aktif olarak sürdürülmektedir. Söz konusu Projeyle 2013 yılında TÜBİTAK-BİLGEM öncülüğünde ve Yatırım Programı desteğiyle, Bulut Bilişim ve Büyük Veri konularında altyapıların kurulacağı bir araştırma

[92] Kalkınma Bakanlığı, 2015: 154-155

laboratuvarı oluşturulmuştur. Bu laboratuvar bünyesinde bulut bilişim ve büyük veri alanında ileri düzeyde araştırmaların yapılması, ihtiyaç duyulan ürünlerin yerli kaynaklarla geliştirilmesine öncülük edilmesi, bu alanda çalışacak paydaşlar için araştırma yapma ve danışmanlık alma olanaklarının sağlanması hedeflenmektedir. Kamu ihtiyaçlarına yönelik olarak; elde edilen bilgi birikimi, kurulan altyapılar ve kamu kurumlarına verilen danışmanlık hizmetleri ile kurumsal büyük veri analizlerinin yapılması planlanmaktadır.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan "2016-2019 Ulusal e-Devlet Stratejisi ve Eki Eylem Planı"nda Bilim, Sanayi ve Teknoloji Bakanlığı'nın sorumluluğunda yer alan "Kamuda Büyük Veri ve Nesnelerin İnterneti Politikalarının Geliştirilmesi ve Yaygınlaştırılması" eylemi ile bilgiye dayalı politika tasarımı, politika modellemesi ve politikanın uygulanması için kamuya teknik destek sağlanması amaçlanmaktadır. Söz konusu eylemin hayata geçirilmesi amacıyla 2017 yılında TÜBİTAK-BİLGEM tarafından "Kamuda İnovatif Yaklaşımlar: Büyük Veri Politikalarının Geliştirilmesi (KamuV)" Projesine ilişkin çalışmalar başlatılmıştır. Proje kapsamında Türkiye'de ve dünyadaki mevcut durumun analiz edilmesi, kamuda büyük veri çalışmaları için taslak politikaların oluşturulması, büyük veri yöntemleri kullanılarak belirlenen bir kamu hizmetinin iyileştirilmesine ve geliştirilmesine yönelik atölye çalışmaları ile pilot uygulama yapılması ve elde edilen tecrübeler ışığında ve ekosistemde yer alan paydaşların katılımı sağlanarak taslak politikaların nihai olgunluğa ulaştırılmasının hedeflendiği ifade edilmektedir.[93] Ağustos 2017 tarihinde Proje kapsamında kurumlarla bilgi ve tecrübe paylaşımı amacıyla odak grup toplantısı gerçekleştirilmiştir.

2010 yılında IBM ve Orta Doğu Teknik Üniversitesi (ODTÜ) işbirliğiyle çalışmalarına başlanan "Akıllı Kamu Güvenliği Laboratuvarı (Smarter Public Safety Laboratory)" Projesi, büyük veri analizi konusunda Türkiye'de uygulanmaya çalışılan bir diğer örneği teşkil etmektedir. Laboratuvar ile suçla mücadele amacıyla büyük veri teknoloji ve yöntemleri kullanılarak çözümler geliştirilmesi ve acil durumlara cevap verme kapasitesinin artırılması amaçlanmıştır. Multimedya analizi, semantik bilgi

[93] TÜBİTAK Resmi İnternet Sitesi, (erişim tarihi: 09.11.2017), http://yte.bilgem.tubitak.gov.tr/tr/haber/kamuv-projesi-basladi

işleme, veri madenciliği, kablosuz sensör ağları ve dağıtık ortamda veri işleme gibi yöntemler aracılığıyla akıllı kamu güvenliği konusunda araştırma ve uygulamaların hayata geçirilmesi hedeflenmiştir.

4. ULUSLARARASI ALANDA VE KARŞILAŞTIRMALI HUKUKTA VERİ MAHREMİYETİ

4.1. Veri Koruma Hukuku Bağlamında Mahremiyet Hakkı

Büyük veri teknolojileriyle birlikte kaydedilen hızlı gelişme, ilk bölümde de ifade edildiği üzere ticari hayatın aktörlerine, araştırmacılara ve kamu kesimine benzersiz fırsatlar sağlamaktadır. Ancak bu önemli fayda ve fırsatların yanında büyük verinin getirdiği değişim, bireylerin çevrimiçi veya çevrimdışı her türlü faaliyetinin takibi neticesinde elde edilen, çoğunluğu kişisel veriden oluşan, verilerin işlenmesi temeline dayandığından bir mahremiyet sorunsalı teşkil edebilmektedir.

Büyük veri teknolojileri sayesinde, kişisel verilerin derleme, sınıflandırma, saklama işlemlerine tabi tutulması ve istendiğinde hızlıca sunulabilmesi kolaylaşmış, ilgilinin rızası alınmadan başkalarına açıklanması ve bilginin bulunduğu yerden başka bir yere kolayca aktarılması mümkün hale gelmiştir. Kişisel veriler büyük veri teknolojileri sayesinde hiç olmadığı kadar hızlı, etkin ve ucuz bir biçimde işlenerek ekonomik ve sosyal katma değere dönüştürülmektedir. Ancak bu verilerin hukuka uygun olarak nasıl işleneceği ve anayasal ilkelerle korunmaya çalışılan bireyin özel hayatının gizliliği ile kişisel verilerin korunması gibi mahremiyete ilişkin temel haklara halel gelmemesinin nasıl sağlanacağı konuları önemli soru işaretlerini bünyesinde barındırmaktadır. Zira büyük veri setleri kullanılarak ortaya çıkarılacak analiz sonuçlarının öngörülemezliğinin yarattığı yeni durum, veri mahremiyeti hukuku bakımından önemli tartışma alanları ortaya çıkarmaktadır.

Kişisel verilerin korunması hakkı, özel hayatın gizliliği temel ilkesine dayanan negatif statü haklarından biridir. Özel hayatın gizliliği, bütün modern demokratik hukuk devletlerinde benimsenmiş bir anayasa hukuku ilkesidir. Günümüz hukuk devletlerinde, kişi her yönüyle bir bütün olarak kabul edilmekte ve özel hayat da bu bütünün önemli bir parçası olarak görülmektedir. Özel hayatın hukuksal düzenlemelere konu olmasındaki temel amaç; insan kişiliğinin serbestçe gelişmesine imkân vermek, kişiye kendisi ve yakınları ile baş başa kalabileceği, devlet ve başkaları

tarafından rahatsız edilemeyeceği özerk bir alan sağlamaktır. Özel hayatın korunması insan onurunun korunmasında bir araçtır.[94]

Mahremiyet, bireylerin rahatsız edici unsurlardan ârî olduğu fiziksel alan arzusu ile kendisi hakkındaki kişisel bilgileri açıklama zaman ve tarzını kontrol edebilme yetisini ifade etmektedir. Mahremiyet kavramı doğrudan kişilikle ilgilidir ve bireyin kişiliğini, bağımsızlığını, onurunu ve bütünlüğünü korumaktadır.[95]

Mahremiyet hakkı ise sırları gizli tutma hakkını ve onları ancak özel ve bilinçli bir iradeyle paylaşmayı ifade etmektedir. Bireyin kendi seçimiyle kaybolma hakkı olarak da ifade edilen mahremiyet; gizlilik, anonimlik ve yalnızlık olmak üzere üç unsurdan oluşmaktadır. Mahremiyet kavramının, başkasının iletişiminin yasa dışı denetlenmemesi veya kişisel bilgilerinin yasal olmayan yollarla işlenmemesi ya da başka bir kimseyle paylaşılmaması gibi özellikleri bulunmaktadır.[96] Zira hiç kimsenin bireyin hayatına müdahale etmemesi mahremiyet alanında herhangi bir hukukun varlığını gereksiz kılarken, ortaya çıkan müdahalelerden bireyin korunması ihtiyacı mahremiyete ilişkin hukuk kurallarını ortaya çıkarmıştır.

Mahremiyet kavramının mekânsal mahremiyet, kişi mahremiyeti ve veri mahremiyeti olmak üzere üç çeşidi bulunduğu kabul edilmektedir. Mekânsal mahremiyet kişiyi çevreleyen yakın fiziksel alanın korunmasını, kişi mahremiyeti kişiyi haksız müdahalelere karşı korumayı, veri mahremiyeti ise kişisel verilerin toplanma, saklanma, işlenme ve iletiminin nasıl yapılacağının veya yapılmayacağının kontrol edilmesini ifade etmektedir.

Günümüz hukuk sistemleri içerisinde pek çok ülkede veri koruma hukukunun içerisinde ele alınan mahremiyet, Birleşmiş Milletler İnsan Hakları Evrensel Bildirisi, Medeni ve Siyasi Haklar Sözleşmesi ve Avrupa İnsan Hakları Sözleşmesi gibi pek çok önemli bölgesel ve uluslararası insan hakları sözleşmesinde koruma altına alınmaktadır. Ayrıca, Türkiye de dâhil olmak üzere pek çok ülkede anayasal bir hak olarak düzenlenmektedir. Özel hayatın gizliliğiyle yakından ilgili olan mahremiyet,

---

[94] Özbudun, 1997: 265
[95] Kılınç, 2012: 1105
[96] Arslan, "Amerika ile Avrupa Birliği Hukuki Düzenlemelerinin Gizlilik Haklarına Bakış Açısının Karşılaştırılması", X. Türkiye'de İnternet Konferansı, 2005, (erişim tarihi: 21.07.2016), http://inet-tr.org.tr/inetconf10/bildiri/18.doc

dünyada kültürlere ve bölgelere göre çeşitli şekillerde tanımlanmakta olup içinde bulunulan toplum ve çevreye göre değişmektedir. Bu nedenle, mahremiyetin insan hakları kataloğu içerisinde tanımlanması en zor kavramlardan biri olduğu ifade edilmektedir.[97]

Büyük veriyle kişisel verilerin elektronik ortamda saklanması, işlenmesi ve analizi adeta kural haline gelirken, hakkında veri toplanan bireyin kişilik haklarının korunması ve bu alanda güvenin tesis edilmesi gerekmektedir.

4.2. Dünyada Kişisel Verilerin Korunması Alanında Mevcut Hukuki Düzenlemeler

Veri işleme teknolojisindeki hızlı gelişim kişisel verilere bakış açısında bir değişim ihtiyacını doğurmuş, veri koruma politikalarının da bu doğrultuda gelişmesini sağlamıştır. Bu süreç kişisel verilerin korunması sorununun bir hukuki düzenleme alanı olarak ortaya çıkmasını doğal olarak beraberinde getirmiştir. BİT sayesinde hızla gelişen otomatik veri işleme teknolojisinin doğurduğu mahremiyet sorunları ilk kez 1960'lı yılların sonlarında kişisel verilerin korunmasına yönelik kanun çalışmalarının ortaya çıkmasına neden olmuştur. Sanayi toplumundan bilgi toplumuna geçiş sürecini yaşamakta olan ülkelerde, bireysel hak ve özgürlüklerin zarar göreceğine ilişkin endişeler karşısında bu alanda hayata geçirilen hukuki düzenlemeler eliyle kişisel mahremiyetin korunması amaçlanmıştır. Bu çerçevede, bilgi toplumunun en temel sorunlarından biri olan, bireylerin devlet organları ve diğer kişiler karşısında özel yaşam alanına müdahalenin önlenmesi ve kendileri hakkındaki verilerin işlenmesine ilişkin hukuki çerçevenin çizilmesini amaçlayan bir hukuk alanı ortaya çıkmıştır.

Kişisel verilerin korunmasına yönelik ilk ulusal hukuk düzenlemeleri; 1970 yılında Almanya, 1973 yılında İsveç ve 1974 yılında ABD'de yapılan yasa metinleridir.[98] 1970'li yıllarda yapılan bu ulusal düzenlemelere paralel olarak 1980'li yıllardan itibaren, başta OECD'nin kılavuz ilkeleri ve Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşlenme Karşısında Korunması Hakkındaki Sözleşmesi olmak üzere, uluslararası hukuk belgelerinde kişisel verilerin korunması hakkı kabul edilmiştir. 1980'li yılların sonlarında ise kişisel verilerin korunması hakkı özel hayatın

[97] Kılınç, 2012: 1104
[98] Küzeci, 2010: 105-106

gizliliği genel kavramından bağımsız, ayrı ve öne çıkan bir kamu politikası alanı olarak ele alınmaya başlanmıştır. Söz konusu alanın gelişme gösterdiği bu dönemde göze çarpan temel husus, gelişmiş siyasal ve ekonomik yapıya sahip OECD ülkelerinde aynı politika alanında benzer hukuki çözümlerin üretilmesi, başka bir ifadeyle bu alanda sağlanan politika uyuşması olgusudur.[99] 1990'lı yıllarda ortaya çıkan internet teknolojisi ise beraberinde getirdiği geniş ağ bağlantısı imkânı ve elektronik ticarette kişisel verilerin yoğun kullanımı dolayısıyla daha önce sağlanan bu uyumu bozmuş ve farklı veri koruma düzenlemelerine sahip ülkeler bakımından uyuşmazlıklar baş göstermeye başlamıştır. 11 Eylül saldırıları sonrası güvenlik mülahazalarıyla terörle mücadele kapsamında kişisel verilerin toplanması ve işlenmesi hususunda kararlı ve agresif politikalar ortaya koyan ABD yaklaşımı ise bu alandaki dönüm noktalarından biri olmuştur. AB tarafında kişisel veriler kişilik hakkı temelinde bir insan hakkı olarak ele alınıp bağımsız denetçi kurumların gözetimine teslim eden yasalar eliyle düzenlenirken, ABD tarafında bireylere birtakım haklar tanınmakla birlikte uygulamada yeknesaklığı sağlayacak bağımsız bir kurum oluşturulmamış, yalnızca dar kapsamlı sektörel bazı düzenlemelere yer verilmiştir. Kişisel verilerin korunması konusunda dünyadaki düzenlemelere bakıldığında hukuk tekniği bakımından üç temel yaklaşım ön plana çıkmaktadır;

(i) kişisel verinin korunması hakkında genel bir veri koruma kanunu çıkartmak,
(ii) farklı sektörlere yönelik özel hayatın gizliliğine ilişkin kanuni düzenlemeler yapmak
(iii) *"Habeas data[100]"* yaklaşımını benimsemek.[101]

Bu açıdan AB'de ve Türkiye'de ilk yaklaşımın, ABD'de ise ikinci yaklaşımın benimsendiği görülmektedir.

Kişisel verilerin korunması, 1960'lardan beri çalışılan bir konu olmakla birlikte konu tarihsel süreç ve teknolojinin gelişimi karşısında giderek boyut değiştirmekte, küresel BİT hizmetlerinin yaygınlaşması ve ülkeler arasında artan veri trafiği

---

[99] Gür, 2010: 3
[100] Habeas Data: Bireyler tarafından mahkemeye verilen bir dilekçe kanalıyla, görüntüsünün, özel hayatının ve kişisel verilerinin geleceğini belirleme ve bu verilere erişme haklarının korunmasını sağlayan bir bireysel şikâyet yoludur. Brezilya, Peru ve Arjantin başta olmak üzere Latin Amerika ülkelerince anayasal bir hak olarak kabul edilmiştir.
[101] Kaya, 2005: 97

nedeniyle sosyal ve iktisadi açıdan uluslararası önemi haiz bir konuma gelmektedir. Bu çerçevede, son yıllarda ülkelerin veri koruma hukuki altyapılarının uyumlaştırılması çabalarının arttığı dikkat çekmektedir. BİT hizmetleri alanında korumacı yaklaşım güden bazı ülkeler veri koruma düzenlemelerini sıkılaştırarak yabancı şirketlerin yerel pazarlarına erişimini zorlaştırmakta, bu yolla yerel BİT şirketlerine avantaj sağlamaya çalışmaktadır. BİT hizmetleri ihracatçısı ülkeler ise ilişkide olduğu pazarların veri koruma alanındaki gereksinimlerini karşılamaya yönelik tedbirler almaktadır. Yoğun kişisel veri kullanımı olan sağlık, sigorta, finans gibi geleneksel hizmetlerde de yurtdışı pazarlara erişim için veri koruma mevzuatı önem arz etmektedir.[102]

4.2.1. Birleşmiş Milletler

Veri koruma hukukuna ilişkin çeşitli düzenlemeler gerçekleştirmekte olan Birleşmiş Milletler (BM), ilk olarak İnsan Hakları Evrensel Beyannamesinin 12'nci maddesiyle kişilerin mahremiyet, aile ve konut dokunulmazlığının güvence altına alınması ve bu haklara gelecek muhtemel saldırılar karşısında bireylerin hukuki korumadan yararlanmasını hükme bağlamıştır. BM, 1990 yılında kişisel verilerin korunması konusunda kabul edilen "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" ile kişisel verilerin korunmasına ilişkin şu temel prensipleri hüküm altına almıştır: İşlemenin hukuka uygun ve adil olması ilkesi, doğruluk ilkesi, belirli ve meşru amaçlar için işleme ilkesi, ilgili kişilerin erişmesi ilkesi, ayrımcılığın önlenmesi ilkesi, üstün amaçlar için istisna koyabilme ilkesi, güvenlik ilkesi, denetleme ve yaptırım ilkesi ile sınır ötesi veri transferi ilkesi.[103]

4.2.2. Avrupa Konseyi

Mahremiyet hakkı, Avrupa Konseyi Parlamenterler Meclisinin 428 (1970) sayılı Kararı ile "bireyin, hayatını asgari dış müdahaleyle yaşaması hakkı" olarak tanımlanırken, Konseyin 1165 (1998) sayılı Kararında, bu tanıma "kişinin kendisiyle ilgili verileri kontrol hakkı" unsuru da eklenmiştir. 1973 ve 1974 yıllarında Konseyin

[102] Kalkınma Bakanlığı, 2015a: 30
[103] Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği, Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler, 1990, (erişim tarihi: 27.05.2017), http://www.refworld.org/pdfid/3ddcafaac.pdf

Bakanlar Komitesinin özel sektör ve kamuda elektronik veri bankaları karşısında kişilerin mahremiyetinin korunması hakkındaki iki tavsiye kararı, üye ülkelerde verinin toplanması, veri kalitesinin sağlanması ve kişisel verilerin işlenmesi konusunda kişinin bilgi edinme hakkının kabul edilmesini öngörmektedir.[104]

Avrupa Konseyi tarafından 1981 yılında kabul edilen 108 sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme" kişisel verilerin korunması konusunda hukuksal bağlayıcılığı olan ilk belge olarak kabul edilmektedir.[105] Konsey, kişisel verilerin korunması alanında dikkate alınması gereken temel ilkelerin belirlenmesi ve bu alanın ulusal düzeyde çıkarılacak mevzuat eliyle düzenlenmesini teşvik etmeyi amaçlamıştır. Sözleşmenin uygulanmasına yol gösterici olması amacıyla çeşitli tavsiye kararları da yayımlanmıştır. 108 sayılı Sözleşme bir çerçeve düzenleme niteliğindedir. Dolayısıyla, taraf devletlerin, buradaki hükümleri iç hukuklarında kabul edecekleri uygulayıcı düzenlemelerine dercetmeleri gerekmektedir. Bu Sözleşme, kişisel verilerin korunması alanında önemli bir kilometre taşı olmuş ve tüm dünyada bu alanda hayata geçirilen hukukî düzenlemelerde model kabul edilmiştir.

1999 yılında Sözleşmede bir dizi değişiklik ihtiyacı ortaya çıkmış, ardından sözleşmeye ek, 181 sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme Eki Protokol" kabul edilmiştir. Ek Protokol ile veri koruma otoriteleri ve sınır ötesi veri transferine ilişkin hükümler kabul edilmiştir. Sözleşme ile üye ülkelerde uyruğu veya ikametgâhı ne olursa olsun bireylerin, temel hak ve hürriyetleri ile kişisel nitelikteki verilerinin otomatik işlemeye tabi tutulması karşısında mahremiyet haklarının güvence altına alınması amaçlanmaktadır. Bu sözleşmeyle öngörülen korumanın ve kastedilen veri işlemelerinin yalnızca otomatik işlemeler bakımından geçerli olduğu 3'üncü maddesinde ifade edilmektedir.

Sözleşmenin 5'inci maddesinde kişisel verilerin otomatik yollarla işlenmesinde uyulması gereken temel ilkeler sayılmaktadır. İlgili maddeye göre otomatik işleme tabi tutulacak kişisel veriler dürüstlük kurallarına ve hukuka uygun

---

[104] Yüksel Civelek, 2011: 63
[105] Sözleşmenin metni için bkz. http://www2.tbmm.gov.tr/d24/1/1-0966.pdf

olarak elde edilmeli ve işlenmelidir; belirli ve meşru amaçlar için kaydedilmeli ve bu amaçla uyum arz etmeyen bir mahiyette kullanılmamalıdır; kaydetme amaçlarının gerektirdiğinden fazla olmamalı, yeterli ve bağlantılı olmalıdır; doğru olmalı ve gerektiğinde güncellenmelidir; kaydetme amacının gerektirdiğinden daha uzun olmamak koşuluyla, veri sahibinin kimliğini tespite olanak tanıyacak bir formda saklanmalıdır.

Sözleşme'de *hassas kişisel verilere* yönelik özel bir hükme yer verilmekte, hassas kişisel verilerin hangi şartlar altında işlenebileceğine ilişkin temel kural ortaya konulduktan sonra buna ilişkin istisnalar hüküm altına alınmaktadır. Bu alanda, bugünkü modern kanunların hemen hepsinde yer alan temel kriterin bu Sözleşmeden model alındığı görülmektedir. Ayrıca, kaydedilen kişisel nitelikteki verilerin korunması, kazara veya izinsiz olarak imhası veya zayi olması veya bunların elde edilmesi, değiştirilmesi veya izinsiz olarak dağıtılmasının önlenmesi için uygun güvenlik önlemlerinin alınması zorunlu kılınmaktadır.

Bunlara ek olarak 8'inci madde ile kişisel verilerin korunabilmesi için birtakım ilave güvenceler öngörülmektedir. Bu kapsamda, veri sahibi verilerinin otomatik olarak kaydedildiği bir kişisel verinin mevcudiyetini, temel amaçlarını ve dosya yöneticisinin (veri işlemekten sorumlu kişinin) kimliğini, ikametini ve işyerini öğrenebilmek; kendisine ait verilerin kaydedilip kaydedilmediği konusunda makul aralıklarla ve gecikme ya da masraf olmaksızın bilgi edinmek; söz konusu verilerin anlaşılabilir bir biçimde iletilmesini istemek; şayet veriler Sözleşme'de sağlanan güvencelere aykırı biçimde işlenmişse, verilerin düzeltilmesini veya silinmesini talep etmek; bu maddede belirtilen güvencelerin uygulanmaması durumunda hukukî yollara başvurabilmek haklarına sahiptir.

Sözleşmenin 9'uncu maddesiyle, milli güvenliğin korunması, kamu güvenliği, devletin mali menfaatleri veya suçun önlenmesi, verisi işlenen ilgili şahsın korunması ve başkasının hak ve özgürlükleri için zorunlu bir önlem teşkil etmesi, ilgili şahısların özel yaşamlarına açık bir tecavüz tehlikesi teşkil etmedikçe istatistikî veya bilimsel amaçlar için kullanılan kişisel verilerin otomatik yollarla işlenmesi durumlarında sözleşme hükümlerinin ihlal edilmiş olmayacağı belirtilerek söz konusu durumlar kişisel verilerin korunması alanındaki istisnalar olarak düzenlenmiştir.

181 sayılı Ek Protokol ise, taraf ülkelerde kişisel verilerin korunması alanında sorumlu bağımsız ve özerk bir denetleyici otoritenin teşkil edilmesi ve sınır ötesi veri transferinde standartların belirlenmesi konularını düzenlemektedir. Protokole göre Sözleşmeye taraf olmayan ülkelere kişisel veri transfer edilirken, o ülkede yeterli koruma düzeyinin bulunup bulunmadığı değerlendirilmelidir. Protokol bakımından yeterli korumaya sahip olmayan ülkeye sınır ötesi transfere ancak veri sahibinin özel bir yararının bulunması, kamu yararı ya da meşru bir yararın bulunması hallerinde izin verilmelidir.

108 sayılı Sözleşme ve Eki Protokolde düzenlenen temel ilkelerin uygulanmasının temini için taraf ülkelere, iç hukuk düzenlemelerinde gerekli değişiklikleri yapma ve bu Sözleşme'de getirilen hükümlerin ihlali durumunda gerekli yaptırımları uygulayarak hukuki çözüm sağlama görevi verilmiş bulunmaktadır. Ayrıca, Sözleşme ile kurulan ve taraf devletlerin temsilcilerinden oluşan "Danışma Komitesi", gerek veri koruma kurallarını güncellemek gerekse sektörel bazda ortaya çıkan ihtiyaçları karşılamak amacıyla çeşitli tavsiye kararları da kabul etmiştir.

Türkiye'nin 1949 yılında katıldığı Avrupa Konseyi tarafından 1981'de hazırlanan ve Türkiye tarafından da aynı yıl imzalanan 108 sayılı Sözleşme, nihayet 30/01/2016 tarih ve 6669 sayılı Kanun ile TBMM tarafından kabul edilerek yürürlüğe girmiştir. Sözleşmeye ek 181 sayılı Protokol de hazırlandığı yıl olan 2001 tarihinde imzalanmış olup Protokol'ün TBMM'de uygun bulunarak onaylanmasına ilişkin hukuki süreç 20/04/2016 tarihli ve 6705 sayılı Kanun'la kabul edilmesiyle tamamlanmış bulunmaktadır.

4.2.3. İktisadi İşbirliği ve Kalkınma Teşkilatı

Veri teknolojilerinde kaydedilen gelişmeler doğrultusunda veri işlemenin giderek önem kazanması neticesinde birçok OECD üyesi ülke, veri mahremiyeti alanında düzenlemeler yapmış, ancak ülkeler arasındaki mevzuat farklılıkları birtakım sorunlara neden olmuştur. Bu çerçevede, 1978 yılında bir Uzman Grubu kurularak başlatılan çalışmalar neticesinde, 1980 yılında mahremiyetin korunması ve sınır ötesi kişisel veri korumasını tavsiye eden ilk çok uluslu inisiyatif niteliğindeki "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesine İletimi Hakkında Rehber

İlkeler" (Mahremiyet Rehber İlkeleri) kabul edilmiştir. Bu rehber ilkelerin hukukî bağlayıcılığı bulunmayıp uygulanması konusunda devletlere geniş bir takdir yetkisi verilmektedir.

Mahremiyet Rehber İlkeleri, bireylere ilişkin verilerin her türlü yerel bilgisayar ağından, karmaşık ulusal ve uluslararası ağlara kadar geniş bir alanda işlendiği durumlara yönelik bir içeriğe sahip olup, aynı zamanda küresel ağlarda mahremiyeti korumaya ilişkin temel belge olarak görülmektedir. OECD, otomatik veri işleme yöntemlerinin geliştirilmesiyle büyük miktardaki verinin kısa sürede sınır ötesi transferinin mümkün hale gelmesi karşısında kişisel veri mahremiyetinin korunmasına yönelik ilkelerin belirlenmesine ihtiyaç duyulduğunu ifade etmektedir. Bu çerçevede, kişisel verilerin hukuka aykırı olarak kaydedilmesi ve depolanması veya bunların yetkisiz olarak açıklanması yahut kötüye kullanılması gibi durumların insan haklarına aykırı olacağı, son yıllarda geliştirilen yeni bilgisayar ve iletişim teknolojisinin yaygınlaşmasıyla büyük bir hızla artan veri transferleri üzerinde bazı sınırlamalara gidilmesi gerektiği, ancak bu tür sınırlamaların özellikle bankacılık ve sigortacılık gibi ekonomi üzerinde büyük öneme sahip sektörlerde ciddi sorunlara yol açabileceği, bu nedenle kişisel verilerin korunması ile veri transferindeki serbestlik arasındaki dengenin dikkatli kurulması gerektiği vurgulanmaktadır.[106]

Kişisel verilerin toplanması ve yönetilmesi ile ilgili teknolojik gelişmelere ayak uydurabilecek esneklikte kaleme alınan teknoloji tarafsız özelliği ile Mahremiyet Rehber İlkeleri, kişisel verilerin toplanması ve tutulması ile mahremiyetin korunması alanında uluslararası uzlaşıyı temsil etmekte olup şu sekiz temel prensipten oluşmaktadır:[107]

1- Sınırlı veri toplama ilkesi: Kişisel verilerin toplanmasında belirli sınırlamalara uyulması gerektiği ifade edilmektedir. Kişisel veriler hukuka uygun gerekçe ve araçlarla toplanmalı, gerektiğinde veri sahibi bilgilendirilmeli ve rızası alınmalıdır.
2- Veri kalitesi ilkesi: Kişisel veriler, kullanılacakları amaç ile ilgili olmak şartıyla mümkün olduğunca doğru, tam ve güncel olmalıdır.

[106] Kılınç, 2012: 1109
[107] Yüksel Civelek, 2011: 60-62

3- Amaca özgülük ilkesi: Kişisel verilerin toplanma amacı belirlenmeli ve sadece belirlenen amaç için kullanılmalıdır. Veri bu amaç dışında kullanılmamalıdır. Kullanım amacı, sonraki bir tarihte değişirse veya yeni amaca uygun olarak veri işleme faaliyetinin veri sahibine zarar verme ihtimali varsa veri sahibi bilgilendirilmelidir.
4- Kullanım sınırlaması ilkesi: Toplanan veriler, "amaca özgülük" prensibi ile belirlenen amaçlar dışında yayılamaz, bulundurulamaz veya başka amaçlarla kullanılamaz. Bu ilkenin istisnaları veri sahibinin bilinçli rızası ve kanundan kaynaklanan yetki olarak ifade edilmektedir.
5- Güvenlik önlemleri ilkesi: Toplanan veriler kayıp, yetkisiz erişim, zarar görme, değiştirilme, kullanılma veya açıklanma gibi potansiyel tehlikelere karşı makul güvenlik tedbirleri ile güvence altına alınmalıdır.
6- Açıklık (aleniyet) ilkesi: Kişisel verilere ilişkin işlemler, politikalar ve uygulanan önlemler aleniyet politikası çerçevesinde gerçekleştirilmeli; bireylere kendileriyle ilgili veri barındıran kurum ve kuruluşların gizlilik politikalarına kolaylıkla erişebilme hakkı tanınmalıdır.
7- Bireyin katılımı (rıza) ilkesi: Veri sahibinin rızası olmaksızın verileri erişilebilir hale getirilmemeli ve açıklanmamalıdır. Bu ilke çerçevesinde birey, her şeyden önce veri kontrolörünün kendisi ile ilgili veriye sahip olup olmadığı hakkında bilgi alma hakkına sahiptir. Kendisiyle ilgili veri konusunda kontrolör ile makul süre içinde, makul bir ücret mukabilinde, uygun yöntemlerle, açık ve anlaşılabilir araçlarla irtibata geçebilmesi sağlanmalıdır. Bu ilkeyle belirlenen hakların kullanımı amacıyla yapılan başvurunun reddedilmesi durumunda talebin neden reddedildiğinin gerekçe ile bildirilmesini isteme ve ret kararına karşı hukuk yollarına başvurabilme hakkı da düzenlenmiştir. İtirazın kabul edilmesi durumunda verinin silinmesi, değiştirilmesi veya düzeltilmesini isteme hakkı da öngörülmüştür.
8- Hesap verebilirlik ilkesi: Veri sahiplerinin veri toplayanlara karşı yukarıdaki ilkeler çerçevesinde hesap sorabilmeleri mümkün olmalıdır.

Mahremiyet Rehber İlkelerinin ardından, 1985 yılında OECD "Sınır Ötesi Veri Akışları" ile ilgili bildiriyi kabul etmiştir. Bildiri, ticari, bilimsel ve teknolojik veri

değişimi ve şirket içi veri akışı gibi sınır aşan kişisel veri trafiğine ilişkin politika alanlarına değinmektedir. 1998 Ottawa Bakanlar Konferansı'nda ise küresel ağlarda mahremiyetin korunması taahhüdü ile bu alanda yapılması gereken çalışmaları içeren bir bildiri kabul edilmiştir. Bu kapsamda, küresel ağlarda güven tesis edilmesi ve kişisel veri transferinde gerekli olmayan sınırlamaların ortadan kaldırılması amaçlanmaktadır.

Veri mahremiyeti politika ve düzenlemeleri konusundan genel bir yol gösterici olarak kabul edilen Mahremiyet Rehber İlkeleri, son 35 yılda nispeten iyi bir çerçeve çizilmesine yardımcı olmuştur. Bununla birlikte, uygulamada ortaya çıkan yeni durumda, söz konusu ilkelerin olduğu gibi uygulamaya devam edilmesi giderek zorlaşmıştır. 1980 yılından beri veri mahremiyeti konusunda tesis edilmeye çalışılan ekosistem, büyük veri gibi yenilikçi bir gelişme karşısında oldukça değişmiştir. Geleneksel OECD ilkelerinin uygulanmasını güçleştiren faktörler aşağıdaki gibi özetlenebilir:

- Birden çok platformda veri toplamanın giderek yaygınlaşması (büyük verideki dağıtık veri depolama örneğindeki gibi),
- Üretilen ve toplanan verilerin hacmi ve hızı,
- Veri tümleştirme ve potansiyel olarak verilerin anonimliğini ortadan kaldıracak mahiyette veri toplama çalışmaları,
- Bireylerin davranışları, ilgi alanları ve kişisel ilişkileri konularında çıkarımlar yapılmasını ve bilgiye ulaşılmasını sağlayan analitik yöntem ve teknik imkânların çeşitliliği,
- Ardıl (ex-post) veri madenciliği ve başlangıçta tasarlanmamış yöntemlerle verilerin yeniden kullanımı,
- Kişisel verilerin mahremiyetine yönelik tehditlerin giderek artması,
- Kişisel verilerin mahremiyetinden ödün verecek veya onu koruyacak aktörlerin sayısı,
- Kişisel verilerin toplanması ve kullanılması ile ilgili etkileşimlerin karmaşıklığına ilişkin bireylerin yetersiz veya yanlış algısı,
- Kişisel verilere kolayca erişilebilmesi ve söz konusu verilerin küresel ölçekte kullanılabilmesi.

Ayrıca, OECD Mahremiyet Rehber İlkelerinin (ve bu ilkelerden yola çıkılarak hazırlanan tüm düzenleme ve kanunlar) odağında, yalnızca kişisel verilerin; örneğin isim veya kimlik numarası gibi bir kişiyi belirleyen veya adres bilgisi gibi kişiyi belirlenebilir kılmak için yeterli verilerin bu ilkelere göre yönetilmesi gerektiği fikri bulunmaktadır. Bu kapsamda, bir kişiyi belirlemeyen herhangi bir verinin; örneğin kişiyi belirlenebilir kılan tüm unsurların kaldırıldığı veya kişiyi yeniden belirlemeyi makul yollarla mümkün kılmayacak şekilde değiştirilmiş kişisel verilerin bu ilkelerin uygulama kapsamının dışında olduğu kabul edilmektedir. Bununla birlikte, büyük verinin birleştirici özelliğinin, kişisel veriler ile "anonim" veriler arasındaki çizgiyi giderek bulanıklaştırdığı ifade edilmektedir. Zira sonradan elde edilen anonim verilerin önceki anonim veriyle birlikte kullanılması durumunda söz konusu teknik işlemin önceki veriye "belirlenebilir kılma" niteliğini verebileceği ifade edilmektedir.

Yukarıda ifade edilen hususları dikkate alan OECD, 1980 yılında yayımladığı ilkeleri gözden geçirmiş ve 2013 yılında, özellikle hesap verebilirlik ve veri ihlallerinin bildirilmesi alanları başta olmak üzere, yeni "2013 Mahremiyet Çerçevesi"ni duyurmuştur.[108] 2013 Rehber İlkelerinde, büyük veri gibi yeni teknolojik gelişmeler karşısında, bireyin 'rıza'sına ilişkin yeni dinamiklerin, amaçla sınırlılık ilkesinin ve bireyin veri mahremiyeti hususunda kendi rolünün üzerinde çalışılması gerektiği ifade edilmektedir. Bununla birlikte, OECD Konseyi belgesini hazırlayan uzman grup, orijinal sekiz temel ilkenin değiştirilmesi konusunda fikir birliğine varamamış ve bu nedenle ilkelerde değişikliğe gidilememiştir.

2013 yılındaki güncellenme çalışmasının ardından iki özel sektör girişimi düzenleyici çerçeveyi daha da ilerletmek üzere çeşitli çalışmalar başlatmıştır. Microsoft ve Oxford Üniversitesi İnternet Enstitüsü tarafından organize edilen ilk girişim ile "21. Yüzyıl için Veri Koruma İlkeleri" raporu 2014'te yayımlanmıştır.[109] İkinci girişim ise Dünya Ekonomik Forumu (WEF) ile birlikte Boston Consulting Group (BCG) tarafından düzenlenmiş ve "Kişisel Veriden Değer Yaratmak: Toplamadan Kullanıma" adlı raporu 2013'te yayımlamıştır.[110] Her iki girişim de, Rehber İlkelerin 2013 güncellemesinin; veri analizi, toplama ve kullanıma ilişkin hızlı

[108] OECD, 2013: 1-152
[109] Cate ve ark., 2014: 1-23
[110] WEF, 2013: 1-33

ve köklü değişime yeteri kadar değinmemesi dolayısıyla yetersiz olduğu ve çağa uygun olmadığı sonucunu paylaşmaktadır. Bu kapsamda, söz konusu çalışmalar, veri koruma konusunda OECD'nin geleneksel yaklaşımında değişmesini gerekli gördükleri temel hususları ifade etmektedir.

WEF tarafından yayımlanan raporda, veri sahiplerinin kendilerinin de sınırsız birer veri üreticisi haline geldiği mevcut düzlemde, yalnız bir kez alınan ve evet/hayır şeklinde katı bir ikili tercih sunan geleneksel rıza alma metodlarına göre kaleme alınmış 'rıza' ilkesinin yenilikçi veri toplama ve kullanma uygulamaları karşısında yetersiz kalacağı ifade edilmektedir. Bu doğrultuda, söz konusu raporda güncel 2013 Rehber İlkeleri metninde yer alan dört temel eksiklik aşağıdaki gibi özetlemektedir:[111]

- Verinin toplanmasından çok sonra verilerin yeni ve yararlı kullanımlarının keşfedileceği ihtimali hesaba katılmamaktadır.
- Tek parça veriye birden çok kullanıcının erişebildiği, veri toplama, transfer ve işleme maliyetlerini neredeyse sıfıra indiren ağa bağlı veri mimarileri hesaba katılmamaktadır.
- Veri sahiplerinin ürettiği veya onlar hakkında üretilen verilerden oluşan "veri seli" bireylere aşırı bilişsel bir yükü de beraberinde getirmektedir. Zira bireyleri sürekli olarak kendi verilerine ilişkin bildirimlerle bunaltmanın nihai olarak koruma açısından anlamsız ve etkisiz olacağı ifade edilmektedir.
- Pek çok durumda -örneğin işletim sistemine sahip bir araba kullanılırken, aracın M2M yöntemiyle veri toplaması, işlemesi ve iletmesi sırasında- bireylerin rızasını almak için geleneksel yaklaşımların kullanılması artık pratik veya etkili bulunmamaktadır.

Yukarıda ifade edilen eleştirilerin, bu alandaki ABD yaklaşımını yansıttığına ilişkin değerlendirmeler bulunmaktadır. Zira söz konusu raporları hazırlayanlar arasında ABD BİT endüstrisinin önde gelen firmalarının temsil ediliyor olması, AB'nin kişisel verilerin korunması konusundaki yeni yaklaşımına zıt bir görüşün benimsenmesinin ardındaki temel gerekçeyi açıklamaktadır.[112] Hem WEF hem de Oxford/Microsoft raporunda, gerek kişisel verinin sınırları belirlenmesi zor doğası

[111] A.g.e.: 11
[112] OECD-International Transport Forum, 2015: 42

gerekse büyük verilerin toplanması ve analizine ilişkin uygulamalar geliştikçe amaçla sınırlılık ilkesi, kullanım sınırlaması ilkesi ile bildirim ve rızanın alınmasına ilişkin ilkelerin birarada uygulanmasının zorlaşması nedeniyle bazı OECD ilkelerinin yeniden değerlendirilmeye ihtiyacı olduğu vurgulanmaktadır.

Oxford/Microsoft'un '21. Yüzyıl için Veri Koruma İlkeleri' raporunda, en azından kişisel verilerin izin verilen kullanımları konusunda net kural ve yaptırımların ana hatlarıyla ortaya çıkması yolunda ilerleme kaydedilebilmesi için, öncelikle bildirimlerin ve veri sahibinin rızasının nasıl alınması gerektiğine ilişkin uygulamaların birçoğunun yeniden formüle edilmesi gerektiği ifade edilmektedir.

Bu kapsamda, yenilenmiş bir sorumluluk yaklaşımı doğrultusunda, kişilerin rıza verip vermemesine değil, veriyi tutan ve kullananların söz konusu kişisel verileri doğru yönetip yönetmediklerine ilişkin hesap verebilirliklerine dikkat edilmesi gerekmektedir. Böylece, sorumluluklar konusunda eksenin bireylerden veri toplayan ve veri kullananlara doğru kaydırılması gerektiği ifade edilmektedir. Ayrıca, kişisel verinin toplanması aşamasından çok kullanılması aşamasına odaklanmak şeklinde yeni bir yaklaşımın daha faydalı olacağı belirtilmektedir. Zira kişisel verinin sonradan ne tarz katma değer yaratabileceği ve hangi bağlamda kullanılabileceği konusu, verinin toplanması aşamasında çoğunlukla belirsiz olmaktadır.[113] Raporda bu gerekçelerle OECD ilkelerinin gözden geçirmeye ihtiyacı olduğu ifade edilmektedir. Bu gözden geçirmede, veri toplamaya uygulanması gereken ilkeler ile veri kullanımına uygulanması gereken ilkeler arasında bir ayrım yapılması gerektiği belirtilmektedir.

Raporda veri kullanımının sınırlarının oldukça geniş ifade edildiği görülmektedir. Yapılan analizler ve uygulamalar ile kişisel verilerin ortaya çıkmasından kaynaklanabilecek muhtemel zarar ile kişisel verilerin toplanması ve kullanımının sağlayacağı faydaların dengelenmesi gerektiği vurgulanmaktadır. Ayrıca, raporun önermekte olduğu yeni ilkelerin sadece kişisel verilere uygulanabileceği, kişiyi belirlenebilir kılmayan verilere ise uygulanmayacağı vurgulanmaktadır. Sonuç olarak, rapor bir taraftan orijinal OECD ilkelerinde yer alan bildirim ve rıza kavramının korunması gerektiğini ifade ederken diğer taraftan veri toplayanlara "bireylerin, verilerinin toplanacağını makul şekilde tahmin edip

[113] Cate ve ark., 2014: 6

edemeyeceğini değerlendirerek izin alınması gerekip gerekmediğine karar verme" yetkisini vererek aslında bu kavramları yok saymaktadır.

Rıza konusundaki sorumluluğun yukarıda ifade edildiği biçimde eksen değiştirmesi durumunda ortaya çıkması muhtemel hususlar WEF raporunda şu şekilde özetlenmektedir:

- Rıza ilkesinin uygulanmasında, pasif ve evet/hayır biçimindeki onaylama sisteminden kişisel verisine daha çok ilgi gösteren katılımcı bir kullanıcı modeline geçilmesi durumunda verinin kaynağı ve birey hakkında iz sürülmesi ihtiyacı ortaya çıkacaktır. Veri toplama zincirinde mümkün olan en erken aşamada veya sensörlerden elde edilen verinin ham haline, kalıcı ve temizlenemeyen metaverilerin eklenmesi bu alanda çözüm olarak değerlendirilmektedir. Söz konusu çözüm "tasarımdan itibaren mahremiyet" yaklaşımı savunucularının desteklediği bir yöntem olarak kabul edilmektedir.
- Kişisel verilerin kullanımıyla ilgili bireylere daha anlaşılır seçenekler sunulması gerektiği ifade edilmektedir. Bu bağlamda içeriğe özel veri kullanımı seçeneklerinin –örneğin, tıbbi amaçlar veya acil hizmetler için kişisel verilerin kullanılmasına onay verilirken, reklam amaçlı hedeflenmeye konu olmamayı seçebilmek gibi- sunulması anlamlı olabilmektedir. Nitekim kitlesel fayda ortaya çıkaran kişisel veri kullanımları ile -örneğin şehrin trafik akışını düzenlemek amacıyla konum verisi kullanımı- bireye yönelik hizmetler sunmak amacıyla yapılan veri kullanımları arasında bir ayrım yapılması gerektiği ifade edilmektedir.
- Ayrıca, kişisel veriye ilişkin düzenlemeler dışında, kullanıcı odaklı denkleştirilmiş ağlar (peer-network), mahremiyet etiketleri (privacy labels), belirlenmiş mahremiyet profili yöneticileri (designated privacy profile managers) gibi işbirlikleri konuları araştırılmaya değer görülmektedir. Bu türlü işbirlikleri bireylerin kişisel verilerinin kullanımı ve tekrar kullanımı ile ilgili onlara tercih hakkı sunmuş olmaktadır.

Bu noktada, mevcut bildirim ve rıza ilkelerini temel çerçevesinden, verilerin kullanımına odaklanmış bir alana doğru sürüklemenin, mali özerkliğe sahip ve yetkili bir düzenleyici otoritenin varlığını gerektirdiğine dikkat edilmelidir. Bağımsız otorite,

veri kullanımlarını denetleyecek ve bu hususta kovuşturma yaparak uyuşmazlıkları çözecektir. Büyük ve güçlü şirketler ile asimetrik ve zorlu yasal süreçlerin sağlıklı yürütülmesi bakımından söz konusu otoritenin güçlü yetkilerle donatılmış olması gerekmektedir.

4.2.4. Avrupa Birliği

4.2.4.1. 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif

1980'li yıllardan itibaren veri işleme teknolojisinde meydana gelen gelişmeler nedeniyle, AB vatandaşlarının üçüncü kişilere tevdi ettikleri verilerin kontrolü konusundaki tereddütler giderek artarken söz konusu kişisel verilerin ticari amaçlarla kullanımının yaygınlaşması Tek Pazar bakımından üye devletlerde farklı uygulamaların ortaya çıkmasına neden olmuştur. Bu döneme kadar gerek OECD Rehber İlkeleri gerekse Avrupa Konseyi'nin ilgili sözleşmeleri kişisel verilerin korunması bakımından atılması gereken somut adımları sunamamış, dolayısıyla AB üyesi ülkeler bakımından ulusal kanunlar arasında uyum ve standartlaşma sağlanamamıştır. Tüm bu gelişmeler doğrultusunda hazırlanan *"Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 95/46/EC sayılı Direktif"* 20 Şubat 1995 tarihinde kabul edilmiştir.[114] Direktifin kabulünü takiben tüm üyelere ulusal veri koruma düzenlemelerini Direktifle uyumlu hale getirme görevi verilmiştir.

Veri Koruma Direktifi kişisel verilerin korunmasına ilişkin ulusal mevzuatların uyumlaştırılarak kişisel verilerin tüm AB ülkelerinde aynı düzeyde ve benzer ilkeler çerçevesinde korunmasını ve bu yolla kişisel verilerin söz konusu ülkelerde herhangi bir güvenlik riski bulunmaksızın serbest dolaşımını sağlamayı amaçlamıştır. Böylece bireylerin mahremiyetinin yüksek koruma altına alınması ile bilginin serbest dolaşımının sağlanması arasında bir denge oluşturulmaya çalışılmıştır. Bununla birlikte, Direktif'in oluşturulmasında oldukça düşük seviyede kalan ülke katkıları ile ülkeler arası görüş farklılıkları gibi sorunlar, Direktif'in iç hukukla uyumlaştırılması konusunda üye ülkelerde gönülsüzlüğü de beraberinde getirmiştir. AB ülkelerinin Veri

[114] Direktif'in İngilizce tam metni için bkz.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Koruma Direktifi'ni iç hukuklarına uyarlama konusunda yetersiz kaldığı gözlemlenmiştir.[115] Bu durum, ulusal veri koruma düzenlemeleri ve Direktif'in AB genelinde kişisel verilerin korunmasında tek başına yetersiz kalmasına sebep olmuş, bu alanda bir reforma gidilmesi ihtiyacı ortaya çıkmıştır.[116]

4.2.4.2. Avrupa Birliği Genel Veri Koruma Tüzüğü

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

Veri Koruma Reformunun ortaya çıkmasında birden fazla husus etkili olmuştur. Bunlardan en önemlisi, kural koymanın temel doğasından kaynaklanan ihtiyaç doğrultusunda, yeni teknolojik gelişmelere uygun kurallar koyarak temel politika hedefleriyle daha uyumlu ve daha verimli kazanımların sağlanmasıdır. Veri Koruma Direktifi'nin 1995 yılından beri uygulanmakta olduğu düşünüldüğünde, özellikle 90'lı yılların ortalarından itibaren internetin ticarileştirilmesiyle meydana gelen köklü dönüşümler karşısında bu düzenlemenin 'eski' kaldığı değerlendirilmektedir. Zira bu dönüşüm sırasında toplumsal hayata hızla giren yeni teknolojiler bir yandan hayal dahi edilemeyecek yararlar sağlarken öte yandan veri toplama, işleme, depolama ve verinin yeniden kullanımı açısından daha önce akla

[115] Henkoğlu, 2015: 60
[116] 6698 sayılı Kanuna doğrudan kaynaklık eden söz konusu Direktif'e ilişkin ayrıntılı bilgi Ek-2'de yer almaktadır.

gelmeyen mahremiyet risklerini de beraberinde getirmiştir.[117] AB içerisinde en temel çekincelerden biri verinin sınır ötesi transferinin oldukça kolaylaşması olmuştur. Zira bu durum doğal olarak yabancı ülke mahremiyet kurallarının uygulanması zorunluluğunu beraberinde getirmiştir. Bunun sonucunda AB vatandaşlarının mahremiyet haklarının olumsuz etkilenmesi kaygısı giderek yükselmiştir.[118]

Bu çerçevede, mevcut veri koruma kurallarının güncellenmesi ile yeni dijital dünyayla daha uyumlu hale getirilmesi ihtiyacı, Birlik içerisinde ortaya çıkan somut uyuşmazlıklar ve bu değişimi kaçınılmaz kılan siyasi açmazlar sebebiyle giderek zorunlu bir hal almıştır. Bunların başında, 2013 yılında ABD Ulusal Güvenlik Ajansı (NSA) çalışanı Edward Snowden tarafından ortaya çıkarılan mahremiyet ihlalleri gelmektedir. Söz konusu olayda, başta Google, Facebook, Apple ve diğer büyük ABD merkezli internet aktörlerinin kullanıcıları olmak üzere milyonlarca kullanıcının erişim bilgileri de dâhil pek çok kişisel verisi NSA'nın geniş kapsamlı ve derinlikli gözetimlerine konu olmuştur. Bu somut gelişmeler Avrupa Birliği Adalet Divanı'nın (ABAD) mevcut hukuki uygulamalarında önemli bir değişim yaklaşımı benimsenmesine sebep olmasının yanında, Avrupa'da bireyin internetteki haklarının korunması konusundaki genel anlayışın da değişmesine neden olmuş ve mahkeme bu çerçevede bir dizi özgün karara imza atmıştır. Bu kapsamda, ABAD'ın dönüm noktası sayılan kararları şu şekilde sayılabilir:[119]

- *Google-İspanya Kararı:* Hukuk literatürüne "unutulma hakkı" olarak da girecek olan bu uyuşmazlık, bu yönde bir talebin hukuki merciler önüne taşındığı ilk davadır. Söz konusu dava İspanya vatandaşı Mario Costeja Gonzalez tarafından Google İspanya ve Google Inc. şirketine karşı açılmış olup davanın konusu 1998 yılında bir gazetede davacı Gonzalez hakkında yapılan habere ilişkin kısayolun arama motorundan kaldırılması talebidir. Davacı uzun süre önce kendisi hakkında yapılan bu haberin artık "alakasız" bir mahiyette olması gerekçesiyle habere ilişkin bağlantının kaldırılması gerektiğini savunmuştur. Bu kararda büyük miktarda veriyi uzun süre saklayan arama motorlarının ve internet aracı hizmet

[117] Gonçalves, 2015: 6
[118] Akıncı, 2017: 10-11
[119] A.g.e.: 12

sağlayıcılarının veri kontrolörü sayılması gerektiği ifade edilmiştir.[120] Karar bireylerin kişisel verileri konusundaki haklarını savunmaları ve çevrimiçi verileri üzerindeki kontrollerini artırmaları açısından dönüm noktası olmuş, Veri Koruma Tüzüğü'nde yer alan "unutulma hakkı"nın da çıkış noktası kabul edilmiştir.

- *İrlanda Dijital Haklar Kararı:* 2014 tarihli bir diğer ABAD kararında ise 2006/24/EC sayılı Veri Saklama Direktifi geçersiz ilan edilmiştir.[121] Bu Direktif sabit, mobil veya internet telefonu ile e-posta iletişimi verilerinin altı aydan iki yıla kadar saklanmasını düzenlemektedir. Söz konusu kişisel verilerin her üye devlet tarafından muhtemel bir soruşturma, araştırma ve suçun kovuşturulması amacıyla kullanılabilmesini sağlayabilecek şekilde hazır tutulmasının sağlanması amaçlanmıştır. Ancak söz konusu veri saklama faaliyetinin makul suç şüphesi bulunmasına gerek olmaksızın yapılması ve üye devletlerin anayasal düzenlemeleri başta olmak üzere pek çok hukuki gerekliliklerivle çelişmesi, bahse konu Direktif'in yoğun tartışmalara yol açmasına sebep olmuştur. Bu tartışmalar ABAD'ın Direktifi geçersiz ilan eden kararıyla nihayete ermiştir.
- *M.Schrems-Veri Koruma Komisyonu Kararı:* Veri koruma kurallarına ilişkin temel yaklaşımda ve pek çok hukuki düzenlemede değişikliğe gidilmesi ihtiyacının varlığını ortaya çıkaran bir diğer önemli ABAD kararı ise 6 Ekim 2015 tarihinde verilen "Schrems Kararı"dır.[122] Davacı Maximillian Schrems Avusturya vatandaşı olup söz konusu olayda AB'de ikamet eden diğer Facebook kullanıcıları gibi kendisinin de Facebook'a koyduğu bütün verilerin, Facebook'un İrlanda şubesi tarafından Facebook'un ABD'de bulunan sunucularına gönderilerek orada işlendiğini ifade etmektedir. İrlanda Veri Koruma Komisyonu'na şikâyette bulunmuştur. İrlanda Veri Koruma Komisyonu, bu şikâyeti, ABD'nin kendisine gönderilen kişisel verilere Güvenli Liman Anlaşması gereğince yeterli düzeyde koruma sağladığı gerekçesiyle reddetmiştir. Bu gelişmenin ardından İrlanda Yüksek mahkemesi olayı ABAD'a taşımıştır. Davada Schrems tarafından yapılan

[120] Karar C-131/12, Google Spain SL ve Google Inc. v Agencia Española de Protección de Datos (AEPD) ve Mario Costeja González, Adalet Divanı (Grand Chamber) of 13 Mayıs 2014, ECR [2014] 317, parag. 32-41.
[121] Toplu Kararlar C-293 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, ve Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl ve diğerleri yargılaması, 8 Nisan 2014, ECR [2014] I-238.
[122] Karar C-362/14, Maximillian Schrems v. Data Protection Commissioner yargılaması, 6 Ekim 2015, ECLI:EU:C:2015:650.

savunmada, AB ve ABD arasındaki "Güvenli Liman Anlaşması" kapsamında eşdeğer bir kişisel veri koruma seviyesinin bulunmasının zorunlu olmasına rağmen, bir süredir tartışmalara sebep olan NSA gözetimleri de dikkate alındığında ABD tarafından Schrems'in kişisel verilerinin AB için gerekli olan güvence şartları kapsamında korunmadığı iddia edilmiştir. ABAD yaptığı incelemede, Komisyonun üçüncü bir ülkeyi yeterli koruma düzeyini sağlar bulmasının ulusal veri koruma otoritelerinin Veri Koruma Direktifi kapsamında inceleme ve denetleme yapma gücünü azaltmaması gerektiği, Güvenli Liman Anlaşması'nın yalnızca ABD şirketleri bakımından bağlayıcı olup kamu otoritelerini bağlamayacağı, ABD hukuk kurallarının incelenmesi sonucunda AB vatandaşlarının başta kişisel verileri olmak üzere temel hakları bakımından tehlikeli sonuçların ortaya çıkabileceği değerlendirildiğinden Güvenli Liman Anlaşması geçersiz ilan edilmiştir.

4.2.4.2.1. AB Veri Koruma Reformuna İlişkin Genel Bilgiler

AB Veri Koruma Reformu düzenleme paketi içerisinde iki temel hukuki belge yer almaktadır:

- *AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/679 sayılı, 95/46/EC sayılı Direktifi yürürlükten kaldıran, kişisel verilerin işlenmesi karşısında gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin Tüzüğü (General Data Protection Regulation-GDPR),*
- *AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/680 sayılı, Konsey'in 2008/977/JHA sayılı Çerçeve Kararını yürürlükten kaldıran, yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına dair Direktifi.*

14 Nisan 2016 tarihinde Avrupa Parlamentosu tarafından onaylanarak kabul edilen Veri Koruma Tüzüğü, 24 Mayıs 2016 tarihinde yürürlüğe girmiş olmakla birlikte, söz konusu düzenlemenin uygulanmaya başlama tarihi 25 Mayıs 2018 olarak belirlenmiştir. Yine Reform paketinde yer alan Direktif, 5 Mayıs 2016 tarihinde

yürürlüğe girmekle birlikte, AB üye ülkelerince metnin iç hukuklarına dercedilmesi için öngörülen son tarih 6 Mayıs 2018 olarak belirlenmiştir.[123]

Komisyonun kişisel verilerin korunmasına ilişkin genel AB yasal çerçevesini gözden geçirirken temel aldığı politika hedefleri şu şekilde ifade edilmektedir:[124]

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

Bu reform çalışmasında, mahremiyet ve veri korumasını büyük veri, nesnelerin interneti ve bulut bilişim olmak üzere üç temel teknolojinin etkilediği ifade edilmektedir. AB vatandaşlarının kişisel verilerinin değerinin, 2020 yılına kadar yılda yaklaşık 1 trilyon avro artma potansiyeline sahip olduğu tahmin edilmektedir.[125] Bu potansiyeli dikkate alarak; Apple firmasının yeni bir Avrupa Veri Merkezine 1,7 milyar avro yatırım yapacağını açıklaması, bulut bilişim şirketi Salesforce'un İngiltere, Fransa ve Almanya'da üç yeni veri merkezi açarak Avrupa'daki yatırımlarını genişleteceğini açıklaması, IBM ve Amazon'un mahremiyet dostu hizmetler sunabilmek için Almanya'da yeni veri merkezleri açması, Zettabox'un kişisel verileri mümkün olan en üst düzeyde korumak ve yüksek kaliteli hizmet sunmak için operasyonlarını tamamen Avrupa'ya taşıma kararı almaları da bu durumun en bariz göstergeleri olarak kabul edilmektedir.[126]

---

[123] Avrupa Komisyonu Resmi İnternet Sitesi, (erişim tarihi: 15,10.2016), http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[124] Avrupa Komisyonu Resmi İnternet sitesi, Basın Açıklaması, (erişim tarihi: 19.10.2016), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
[125] Avrupa Komisyonu, 2015: 2
[126] A.g.e: 2

4.2.4.2.2. AB Genel Veri Koruma Tüzüğü'nün Getirdiği Temel Değişiklikler

AB Genel Veri Koruma Tüzüğü ile getirilen önemli değişiklikler aşağıda sıralanmaktadır:[127]

- Üye ülkelerde üst seviye mevzuat uyumlaştırması,
- Veri işleyenlerin tamamının veri işlemeden sorumlu tutulması,
- AB Veri Koruma Tüzüğü hükümlerinin küresel ölçekte etkiyi haiz olması,
- Verisi işlenenlere sağlanan tazminat talebi imkânı,
- AB vatandaşlarına ait kişisel verilerin sınır ötesi aktarımının daha sıkı kurallara bağlanması,
- Uyumlaştırılmış kullanıcı hakları,
- Yeni "Unutulma Hakkı" kavramı,
- Kullanıcı haklarına ilişkin bilgilendirme yükümlülüğünün veri kontrolöründe olması,
- Daha sıkı yaptırımların ve elverişli mekanizmaların öngörülmesi,
- Güçlendirilmiş rıza,
- Veri taşınabilirliği hakkı,
- Hassas kişisel verilerin işlenmesi bakımından öngörülen "Veri Koruma Görevlisi",
- Büyük veri analizi ve büyük ölçekli riskli veri işleme faaliyetleri bakımından "Zorunlu Veri Koruma Etki Değerlendirmesi",
- Varsayılan ve Tasarımdan İtibaren Veri Koruması yaklaşımı,
- Veri ihlali riskinin yüksek olması durumunda hem veri koruma otoritesine hem de veri sahibine bildirimde bulunma zorunluluğu,
- Veri kontrolörü bakımından getirilen kurtuluş hakkı.

4.2.4.2.3. AB Genel Veri Koruma Tüzüğü'nün Kapsamı

AB Genel Veri Koruma Tüzüğü'nün getirmiş olduğu yeni düzenlemelere yalnızca veri koruma hukukunun karmaşık ve tartışmalı meseleleri olmaları yönünden değil, aynı zamanda yeni dünya düzeninin ekonomi politikalarına etkisi açısından da

[127] Bu bölümde başlıklar halinde genel olarak ifade edilen, AB Genel Veri Koruma Tüzüğü'nün getirdiği temel değişiklikler çalışmanın Ek-3 bölümünde detaylı olarak yer almaktadır.

bakılması gerekmektedir. Zira söz konusu düzenleme daha oluşturulma aşamasında endüstri ve sivil toplum kuruluşlarının güçlü ve zorlayıcı mücadelesine sahne olurken AB organları Avrupa Komisyonu, Konsey ve Parlamento'nun kendi içindeki çekişmeleri de metnin oluşturulma sürecine yansımıştır. Zira her bir kuruluşun söz konusu Tüzük'ün hayata geçirilmesindeki temel güdüsü birbirinden farklıdır. Örneğin; Komisyon daha çok ekonomik gelişme ve güvenlik gibi kaygılarla hareket ederken Parlamento'nun önceliği temel bireysel hakların korunmasıdır. Nitekim bu gruplar arasında var olan mahremiyetin ne olduğu ve her bir üye devlette nasıl korunması gerektiğine ilişkin görüş ayrılıkları Veri Koruma Tüzüğü'nün hazırlanması ve kabulü süreçlerinin neden uzun sürdüğünü açıklamaktadır.[128]

173 paragraflık giriş bölümü ve 99 maddeden oluşan temel metniyle AB Veri Koruma Tüzüğü oldukça kapsamlı bir veri koruma çerçevesi sunmaktadır. Söz konusu düzenlemenin büyük veriye dayalı dijital ekonomi üzerindeki etkileri bakımından önemli olduğu değerlendirilen ve köklü yenilikler öngördüğü üç temel alan aşağıdaki gibidir:[129]

i) Kişisel verilerin ve veri sahiplerinin daha etkin korunması

Kişisel veri sahiplerinin hakları kapsamına alınan 'unutulma hakkı' Veri Koruma Tüzüğü'nün 17'nci maddesi kapsamında 'silinme hakkı' başlığı altında düzenlenmektedir. Söz konusu madde ile 95/46/EC sayılı Direktif'in 12'nci maddesinin (b) bendinde veri sahibine tanınan hakkın kapsamının genişletildiği görülmektedir. Veri sahipleri, verilerinin artık toplanma amacı ile ilgili olarak tutulmasının gerekli olmadığı, veri sahibinin rızasının bulunmadığı yahut veri sahibinin verisinin işlenmesini istemediği veya kişisel verinin Veri Koruma Tüzüğü'ne aykırı işlendiği durumlarda verilerinin silinmesini veya bundan sonra işlenmemesini talep edebilme hakkına sahiptir. 17'nci maddenin üçüncü fıkrası ve 65 no'lu giriş maddesi birlikte değerlendirildiğinde söz konusu hakkın uygulamasının mutlak olmadığı ve bazı istisnalar tanındığı görülmektedir. Zira bilgi ve ifade hürriyetinin kullanılması için gerekli olması ve belirli yasal istisnalar ile kamu yararı gibi

[128] Akıncı, 2017: 19
[129] A.g.e.: 19-24

gerekliliklerin bulunması (istatistiksel amaçlar, genel sağlık, bilimsel araştırmalar vb.) durumlarında kişisel verilerin tutulması hukuka uygun olarak değerlendirilmektedir.

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

95/46/EC sayılı Veri Koruma Direktifi'nde yer almayan veri taşınabilirliği hakkı ilk kez Veri Koruma Tüzüğü'nün 20'nci maddesiyle tanımlanmıştır. Bu maddeye göre veri sahibi kişisel verisini tutmaya yetkili bir veri kontrolöründen diğerine taşıyabilme yetkisine sahiptir. Maddenin ikinci fıkrasında belirtildiği üzere teknik olarak mümkün olması durumunda veriler bulunduğu veri kontrolöründen diğerine doğrudan iletilebilmektedir. Veri taşınabilirliği, veri sahiplerine verileri

üzerinde oldukça geniş bir hâkimiyet alanı tanıyan etkileyici bir araç gibi gözükmesine karşın kullanımına dikkat edilmesi gerektiği, zira söz konusu hakkın kişisel veriyi gereğinden fazla erişilebilir kılarak ve piyasadaki oyuncuların kendini düzeltme hakkını ortadan kaldırarak inovasyonun gelişimini engelleyebileceği yönünde eleştiriler yapılmaktadır.[130]

Veri işlemeyi hukuka uygun hale getiren veri sahibinin rızasına ilişkin 4'üncü madde hükmünün de veri sahibinin lehine olacak biçimde düzenlendiği görülmektedir. 7'nci maddede yer alan 'rızanın şartları' başlıklı düzenlemeye de uygun olarak, veri sahibine karşı yapılan veri işlemeye ilişkin rıza talebinin anlaşılır ve kolay erişilebilir bir biçimde, açık ve sade bir dille yapılması gerekmektedir. Ayrıca, veri sahibinin söz konusu rızasını geri alma hakkı her zaman bulunmaktadır. Üçüncü fıkrada belirtildiği üzere, usûlde kolaylık sağlanması bakımından rıza nasıl veriliyorsa aynı şekilde geri alınabilecektir. Ancak rıza konusunda getirilen söz konusu düzenleme "kural-uygulama ilişkisi" bağlamında kâğıt üzerinde kalan hakkın uygulamada ne gibi sonuçlar doğuracağının belirsiz olması noktasında eleştirilmektedir. Zira aydınlatılmış veri sahibinin açık rızasını kişisel veri korumasının odağına koymak, zaten uygulamasının çok da etkili olamayacağı öngörüleri varken, giderek daha karmaşık bir hal alan dijital dönüşüm karşısında veri koruma anlamında kifayetsiz kalınacağı yönünde eleştirilmektedir. Nitekim kullanıcıların yalnızca rızalarının olmayışının değil teknolojik ilerleme içerisinde belirli koşullar altında (kuşak, eğitim düzeyi ve finansal durum gibi farklılıkların bu koşulları daha da keskinleştirdiği de göz önüne alındığında) vermiş oldukları her rızanın zaten bu güvenceyi temin edemeyeceği ifade edilmektedir.[131] Tüzük ile getirilen tüm bu geniş hak ve yetkiler veri sahiplerine verilerinin kaderini belirleyebilme konusunda oldukça geniş bir alan sağlarken veri işleyenlere ise oldukça detaylı sorumluluklar yüklemektedir.

ii) Veri işleyenler ile veri kontrolörlerinin artırılmış sorumlulukları

AB Veri Koruma Tüzüğü veri işleyenlerin sorumlulukları konusunda oldukça detaylı hükümler içermektedir. Tüzük kapsamında sorumlulukların yalnızca nitelikleri değişmemiş, sorumlu kişilerin kapsamı da genişletilmiştir. 95/46/EC sayılı Direktif'te

[130] Engels, 2016: 2
[131] Borgesius, 2015: 103–107

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

Veri Koruma Tüzüğü kapsamında veri kontrolörlerinin oldukça geniş bir sorumluluk alanının bulunduğu görülmektedir. Tüzük'ün 5'inci maddesinde sayılan temel prensiplere uygun veri işlemenin gerçekleştirilmesi veri kontrolörünün sorumluluğundadır. Yine Tüzük'ün 25'inci maddesi kapsamında veri kontrolörü bakımından *'Varsayılan olarak ve tasarımdan itibaren veri koruması'* adında yeni bir yükümlülük türünün tanımlandığı görülmektedir. Maddenin birinci fıkrasına göre veri kontrolörü, veri sahiplerinin korunması bakımından Tüzük'te yer alan önemli prensiplerin (veri minimizasyonu gibi) uygulanmasından ve uygun teknik ve organizasyonel önlemleri (bulanıklaştırma gibi) kullanarak veri koruma hukukundan doğan sorumlulukların etkili bir biçimde yerine getirilmesinden sorumludur. Başka bir anlatımla, belirli amaç için gerekli olan veri işleme faaliyeti bakımından veri kontrolörü söz konusu verinin veri koruma mevzuatına uygun olarak işlenmesi için, varsayılan şekilde uygun teknik ve organizasyonel önlemleri almakla yükümlüdür. Söz konusu yükümlülük verinin toplandığı süre ve işlenmesi faaliyeti kapsamında kişisel verinin saklandığı ve veriye erişilebildiği müddetçe geçerlidir. Madde kapsamında öngörülen önlemler bakımından, başlangıçtan itibaren kişisel verilerinin

bireyin herhangi bir girişimi olmaksızın belirsiz sayıda kişinin erişimine açılmadığının temin edilmesi gerekmektedir.

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

Veri Koruma Tüzüğü kapsamında veri işleyenler bakımından ortaya konulan çeşitli çözüm mekanizmaları da bulunmaktadır. Örneğin; 37'nci maddeyle getirilen düzenleme kapsamında bazı veri kontrolörlerinin (hacimsel olarak çok büyük olması veya işlenen verinin hassas veri olması durumlarında) veri koruma görevlisi olarak belirlenmesi mümkündür veya Tüzük'ün 5'inci kitabında yer alan gönüllü davranış kuralları yoluyla veri işleyen işletmelere birtakım imkânlar sağlanmaktadır. Zira AB veri koruma kuralları ile sektör çıkarları arasındaki temel dengenin korunması ihtiyacı bulunmaktadır. Veri koruma otoriteleri bir yandan söz konusu ihlalleri 'sert' müdahale araçlarıyla yaptırıma tabi tutarken diğer yandan geniş kapsamlı soruşturma, düzeltme, yetkilendirme ve danışmanlığı kapsayan araçlarını kullanabilmektedir. Veri koruma

otoriteleri tarafından veri ihlalinin ağırlığına göre değişen oranlarda, yüksek idari para cezaları uygulanabilmektedir. Bu kapsamda, 20 milyon avroya varan para cezalarının yanında, ihlalin teşebbüs aşamasında kalması durumunda, söz konusu şirketin önceki mali yıl küresel cirosunun yüzde 4'üne varan para cezaları öngörülmektedir. Neticede Tüzük, şirketler için Avrupa pazarını daha erişilebilir kılma çabasının yanında öngörmüş olduğu hükümlerle çok daha etkili ve sorunsuz bir izleme sistemi sağlamaya çalışmaktadır. Sayısal Tek Pazar Stratejisi bağlamında Tüzük içerisinde "tek noktadan hizmet" hükmü yerini almıştır. Tüzük'ün 56'ncı maddesinin birinci fıkrası kapsamında veri kontrolörü veya işleyicisinin birden fazla üye devlette faaliyette bulunması durumunda, ana kuruluş merkezinin bulunduğu yer veri koruma otoritesince 'yetkili otorite' olarak adlandırılır ve söz konusu otorite veri kontrolörü veya işleyicisinin tüm üye devletlerde yürüttüğü sınır ötesi veri işleme faaliyetleri bakımından yetkilidir.

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

iii) Mekânsal anlamda daha geniş uygulama alanına sahip olunması

Veri Koruma Tüzüğü'nün uygulama alanı 3'üncü maddesi ile düzenlenmiş olup AB sınırları içerisinde faaliyet gösteren veri kontrolörleri ile işleyicilerinin faaliyetleri kapsamında gerçekleştirdikleri kişisel veri işlemeleri bakımından, işlemenin birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Veri Koruma

Tüzüğü hükümleri uygulanmaktadır. Temel kuralı ifade eden birinci fıkra hükmünün istisnaları ise ikinci fıkrada tanımlanmıştır. Buna göre, Veri Koruma Tüzüğü hükümleri, Birlik içerisindeki veri sahiplerine (ücretsiz olsa dahi) mal veya hizmet sunan yahut (AB içerisinde) söz konusu veri sahiplerinin davranışlarını gözlemleyen veri kontrolörleri ve işleyiciler bakımından uygulama alanı bulmaktadır. Bir veri kontrolörü veya işleyicisinin AB içerisinde mal veya hizmet sunup sunmadığının nasıl belirleneceğine ilişkin detaylar Tüzük'ün 23 no'lu giriş maddesinde belirlenmektedir. AB içerisinde mal veya hizmet sunmak yalnızca bir internet sitesine veya e-posta kutusuna erişimi ifade etmemekte; ayrıca, birden çok AB üyesi ülkede faaliyette bulunulduğunu ortaya koyan dil ve ödeme cinsi/para birimi seçimi ve/veya AB'deki kullanıcı ya da müşterilerin izlenmesini de ifade etmektedir. Bu maddeye göre bir veri kontrolörü veya işleyicisinin bir veya daha fazla AB üyesi ülkede bireylere veri hizmeti sunması durumunda Veri Koruma Tüzüğü'nün uygulanacağı kabul edilmektedir. Tüzük metninde kullanılan 'davranışların izlenmesi' terimiyle, örneğin; bireylerin başta tüketim tercihlerinin ve alışkanlıklarının tespiti amacıyla teknik yöntemlerle internetteki faaliyetlerinin gözetlenmesi ifade edilmektedir. Bu hüküm uygulamada AB dışında faaliyet göstermesine karşın AB tüketicisini hedefleyen şirketlerin Veri Koruma Tüzüğü'ne tâbi olacakları anlamına gelmektedir. Bu madde kapsamında yaratılan yeni durumun Tüzük'ün kapsayıcı mahiyetinin önemli bir uzantısı olduğu ve uygulama bakımından oldukça önemli bir etkiye sebep olacağı değerlendirilmektedir.

Üçüncü bir ülkenin veya uluslararası organizasyonun Avrupa Komisyonu tarafından "yeterli koruma düzeyine sahip" olarak nitelenmesi durumunda Veri Koruma Tüzüğü kurallarının nasıl uygulanacağı hususu tartışılmaktadır (45'inci madde). Komisyon tarafından alınan bu yönde bir karar tüm AB ülkeleri bakımından bağlayıcı olmasının yanında söz konusu üçüncü ülke bakımından kişisel veri aktarımı için herhangi bir ilave yetkilendirmeye gerek bırakmamaktadır. Komisyonun yaptığı söz konusu değerlendirme Schrems Kararı'yla amaçlanan hukuki durumu güçlendirmektedir. Zira 104 nolu giriş maddesinde de belirtildiği üzere Komisyon söz konusu üçüncü ülkede hukukun üstünlüğü, adalete erişim, uluslararası insan hakları norm ve standartlarına uygunluk, temel sektörel iç hukuk düzenlemeleri, kamu

düzenine ilişkin kurallar da dâhil savunma ve ulusal güvenlik ile ceza hukuku mevzuatı bakımından temel bir uygunluk değerlendirmesi yapmak durumundadır. Tüm bu değerlendirme neticesinde üçüncü ülkenin AB'de sağlanan veri koruma çerçevesine uygun yeterli koruma düzeyini sağlayabiliyor olması gerekmektedir. Özellikle veri koruma denetiminin sağlanması bakımından bağımsız bir veri koruma otoritesini haiz bulunulması, üye devletlerin veri koruma otoriteleriyle işbirliği mekanizmalarının hayata geçirilmesi ve bu alanda etkili ve uygulanabilir idari ve hukuki yaptırımların öngörülüyor olması gerekmektedir.

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

4.2.4.2.4. AB Genel Veri Koruma Tüzüğü'ndeki Temel İlkeler

Farklı düzenleme biçimleri şeklinde kabul edilmelerine rağmen temel olarak bakıldığında hem 95/46/EC sayılı Direktif hem de Veri Koruma Tüzüğü aynı amaca hizmet etmektedir. Bu temel amaç; veri işleme ve üye ülkeler arasında verinin serbest dolaşımı faaliyetleri sırasında gerçek kişilerin temel hak ve özgürlüklerinin korunmasıdır. Bu amaca ulaşılmasını temin etmek üzere Tüzük'te bir dizi temel prensibe yer verilmiştir. Tüzük'ün prensipler başlıklı ikinci bölümünde yer alan 5'inci maddesinde verinin işlenmesi sırasında uyulması gereken temel prensipler ifade edilmektedir. Buna göre;

- *Hukukilik, dürüstlük ve şeffaflık ilkesi:* Kişisel verilerin hukuka uygun, dürüstlük kurallarına uygun ve veri öznesine karşı şeffaf işlenmesi gerekmektedir (5/1/a),
- *Amaçla sınırlılık ilkesi:* Kişisel verilerin belirli, açık ve meşru amaçlarla toplanması gerekmektedir (5/1/b),
- *Veri minimizasyonu prensibi:* Kişisel veriler işleme için gerekli olduğu kadar, ilgili ve ölçülü biçimde işlenmelidir (5/1/c),

- *Doğruluk prensibi:* Kişisel verilerin doğru olarak, gerekli hallerde ve güncel tutulması gerekmektedir (5/1/d),
- *Veri saklamanın sınırlandırılması prensibi:* Kişisel verinin işlenmesi amacı için gerekli olandan daha uzun süre tutulmaması gerekmektedir (5/1/e),
- *Bütünlük ve gizlilik prensibi:* Veri işlemenin güvenli olması gerekmektedir (5/1/f),
- *Hesap verebilirlik prensibi:* Veri kontrolörü yukarıda sayılan tüm temel prensiplerden sorumludur (5/2).

AB veri koruma çevrelerinin yeni düzenlemelerle oluşturmaya çalıştığı hukuki çerçevenin, bazı önemli hususların yalnızca düzenlemelerle çözülmesinin imkânsız görülmesi dolayısıyla Silikon Vadisinin "sınır tanımaz yenilikçiliği" ile ortaya koyduğu teknolojik meydan okuma karşısında oldukça cılız kaldığına ve bu veri mücadelesinde AB yaklaşımının giderek daha zorlu bir açmaza girdiğine ilişkin değerlendirmeler de yapılmaktadır.[132] Düzenlemeler eliyle çözülmesi zorlu görülen alanların başında rıza konusu gelmektedir. Yeni teknolojiler karşısında, örneğin akıllı şehirlerde veya akıllı ulaştırma sistemlerinde kullanılan ve genel bir kural olarak toplanan lokasyon verilerinin işlenmesi konusunda, makul bir ön izinle veri sahibinin rızasının nasıl alınacağı hususunun tartışmaya açık olduğu ifade edilmektedir.

Büyük veri ve ondan anlamlı sonuçlar elde etmek üzere kullanılan analizler genelde şeffaf olmayan ve değişken çıkarımlarda bulunmakta iken söz konusu teknolojinin "amaçla sınırlılık" ve "veri minimizasyonu" ilkeleri karşısında nasıl uygulanacağının tartışmalı olduğu ifade edilmektedir. Bu durumun ise, sıradan kullanıcılarda verilerinin kontrolünü ellerinde bulundurmadıkları hissine sebep olacağı öngörülmektedir. Ayrıca, Schrems Kararı'nın ardından Snowden sonrası dünyada, bulut bilişim altyapısını kullanan büyük veri uygulamaları bakımından, verilerin dünyanın herhangi bir yerindeki altyapıya bağımlılığı, AB veri koruma bakış açısıyla oldukça uyumsuz görülmektedir.

Tartışmalar doğrultusunda geleneksel rıza kavramının ve veri işleme konusunda tam anlamıyla bir kontrol yeteneğinin ötesinde bireyin rızası veya

[132] Edwards, 2016: 2

işlemenin gerekçeleri bulunmasına rağmen kısıtlamayı veya yasaklamayı mümkün hale getiren bir modelin hayata geçirilmesi gerektiği ifade edilmektedir.[133]

4.2.4.3. Avrupa Birliği'nde veri korumaya ilişkin diğer düzenlemeler

AB'de kişisel verilerin korunması alanında temel düzenlemeyi oluşturan Veri Koruma Tüzüğü dışında, sektörel bazda birtakım düzenlemelerin hayata geçirildiği de görülmektedir. 2002/58 sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunmasına İlişkin Direktif, Telekomünikasyon Sektöründe Kişisel Verilerin Korunmasına Yönelik 2002/58 sayılı Direktifi değiştiren 2006/24 sayılı Kamu Elektronik Haberleşme Hizmetlerinin Sağlanması veya Kamu Haberleşme Ağları Çerçevesinde Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Direktif, bilgi sistemlerinin güvenliği ile ilgili olarak 31 Mart 1992 tarihinde alınan Konsey Kararı ve Avrupa Komisyonu'nun 2007/228 sayılı Veri Korumanın Mahremiyet Artırıcı Teknolojilerle Desteklenmesi Hakkında Bildirisi veri koruma ile ilgili düzenlemeler kapsamında sayılmaktadır.

4.2.5. Amerika Birleşik Devletleri

ABD'de veri koruma mevzuatı bakımından bütüncül ve yeknesak bir yaklaşım yerine sektörel düzenlemeler ve ilgili hukuk kurallarından oluşan düzenlemelerin uygulanması yoluna gidildiği görülmektedir. Dolayısıyla veri koruma alanında AB ile kıyaslanacak tek, kapsamlı ve çerçeve nitelikte bir veri koruma mevzuatı bulunmamakta, bunun yerine mahremiyete ilişkin düzenlemeler ihtiyaç duyuldukça çıkarılmaktadır. Nitekim ABD, 1981 yılında OECD Rehber İlkelerini imzalayan taraflardan biri olmasına rağmen, bu kuralları halen iç hukukuna yansıtmamıştır.

Gerek Başkan Clinton ve yardımcısı Al Gore'un, "Küresel Elektronik Ticaret Çerçevesi"nde özel sektör ve şirketlerin internet teknolojisi karşısında kendi kurallarını koymalarını açıkça tavsiye etmeleri, gerekse Başkan Obama Yönetiminin hızla büyüyen dijital veri hacminden en iyi şekilde yararlanmayı hedefleyen 2012'de başlattığı "Büyük Veri Araştırma ve Geliştirme Girişimi" ABD'nin kişisel verilerin korunmasına temel haklar penceresinden daha çok veri ekonomisi ve müşteri hakları

[133] Edwards, 2016: 36-37

penceresinden baktığını ortaya koymaktadır. ABD'de uygulanmakta olan yasal düzenlemeler şu şekildedir:

i. *Federal anayasa ve özel hayatın gizliliğine ilişkin temel içtihatlar:* ABD Anayasasında açıkça özel hayatın gizliliğine veya mahremiyete ilişkin bir düzenleme bulunmamaktadır. Bu kapsamda, kişisel verilerin korunması ve özel hayatın gizliliği hakkı yargı kararlarıyla getirilen içtihadî kurallar ile ortaya konulmaktadır.

ii. *Kongre tarafından gerçekleştirilen düzenlemeler:* Bu düzenlemeler, yasama tarafından kamu kurum ve kuruluşlarının veri toplama ve kullanımları için getirilen kurallardan oluşmaktadır. Bu kapsamda, "Bilgi Edinme Özgürlüğü Hakkında Kanun", "Mahremiyet Kanunu", "Kablolu, Elektronik ve Sözlü İletişimin Tespiti Hakkında Kanun" ve Bilgisayar Eşlemesi ve Mahremiyet Kanunu" gibi düzenlemeler yer almaktadır. Bu kanunlarla getirilmekte olan kişisel verilerin korunmasına ilişkin hükümlerin sınırlı bir etki alanı bulunduğu ifade edilmektedir. Zira veri toplama, depolama ve kullanma gibi hukuki önemi haiz işlemlere dair getirilen sınırlamalar yalnızca kamu kurum ve kuruluşlarını bağlamakta, ancak söz konusu kanunlar etkin bir uygulama mekanizması öngörmediğinden bireyler haklarının korunmasını doğrudan talep edememektedir. Yargı mekanizmasına müracaat ise kişisel verilerin korunmasına ilişkin sürecin maliyetli ve uzun sürmesine neden olarak caydırıcı bir etki yaratmaktadır. Ayrıca, söz konusu kanunlarda getirilen geniş istisna hükümleri ABD'deki mevcut sistemin yetersiz kalmasına neden olmaktadır.[134]

iii. *Sektörel düzeyde mahremiyet kuralları:* Kamunun tek başına pek çok özel kuruluştan daha fazla kişisel veriyi elinde bulundurduğuna ilişkin algı özellikle 21'inci yüzyılda ortaya çıkan gelişmelerle birlikte değişmektedir. Günümüzde bir yandan kamu ile özel sektör arasındaki sınırlar bulanıklaşırken diğer yandan özel sektörün sahip olduğu veri hacmi ve işleme kapasitesi her anlamda kamu kurum ve kuruluşlarını gölgede bırakmaktadır. Nitekim BİT altyapısına erişimin kolaylığı ve büyük veri yöntemleri sayesinde dağınık veri tabanlarındaki verilerin kolayca eşleştirilebilmesi, analiz edilmesi ve transferi konusunda ortaya çıkan

[134] Gür, 2010: 128-129

gelişmeler ABD'de sektörlere özgü düzenlemeler yapılması eğilimini güçlendirmiştir. Sektörel anlamda başlıca kanunlar arasında; "Elektronik İletişimin Mahremiyeti Hakkında Kanun", "Video Mahremiyetini Koruma Kanunu", "Ailenin Eğitim Hakları ve Mahremiyeti Hakkında Kanun", "Telekomünikasyon Kanunu", "Çocukların Çevrimiçi Mahremiyetinin Korunması Hakkında Kanun", "Adil Kredi Rapor Edilmesi Hakkında Kanun" ve "Telefon Kullanıcılarının Korunması Hakkında Kanun" yer almaktadır.

ABD'de belirli bir sektörel alanı hedef alan, birden fazla düzenleme yaklaşımı sonuç olarak belirsiz, tutarsız ve genelde rasyonel olmayan bir kişisel veri koruması çerçevesi ortaya çıkarmıştır. Örneğin; AB'de ve Türkiye'de hassas kişisel veri olarak kabul edilen sağlık verileri, ABD'de video film kiralanması hakkındaki verilere nazaran daha düşük bir korumaya sahip bulunmaktadır.[135]

ABD'nin kişisel veriler konusundaki genel yaklaşımı, büyük BİT firmalarının AB pazarındaki etkinliği de dikkate alındığında, AB'nin endişelerini artırmaktadır. Zira doktrinde yeni AB Veri Koruma Tüzüğü ile Brüksel'den Washington'a, ya veri mahremiyeti eğilimlerini değiştirmek ya da kıymetli AB veri pazarını kaybetmek arasında bir seçim yapmak durumunda olduklarına ilişkin üstü kapalı bir diplomatik mesajın verildiği ifade edilmektedir.[136] Söz konusu gelişmeler, ABD mevzuatında köklü bir değişimi getirmese bile özellikle Amerikalı büyük BİT firmalarının tüketicilerinin kişisel verilerine ilişkin tavrını gözden geçirmesine sebep olacaktır.

4.2.6. Çin Halk Cumhuriyeti

Çin'de kişisel verilerin korunması alanında kapsamlı bir hukuki düzenleme bulunmamaktadır. Anayasa'da kişisel verilerin korunması hakkına temel oluşturabilecek belirli haklar dışında Medeni Kanun, Haksız Fiil Sorumluluğu Kanunu, Tüketicinin Korunması Kanunu ve şirketlerin hukuka uygun olarak veri toplamaları ve işlemelerini hedefleyen çeşitli tüzük ve kararlar bulunmaktadır. Kişisel verilerin korunmasına ilişkin kuralların çeşitli sektörlere özgü yasa ve yönetmeliklerde dağınık halde yer aldığı görülmektedir. Eyalet Konseyi bünyesindeki farklı bakanlıklar

[135] A.g.e.: 129
[136] Kulevska, 2013: 1-2

e-ticaret, bankacılık ve BT hizmetleri gibi bir dizi sektöre özgü kurallar yayımlamaktadır.

Son dönemde Çin'de kişisel verilerin korunmasını güçlendirmek için adımlar atıldığı görülmektedir. 2016 yılı sonunda "Ulusal Bilgi Güvenliği Standardizasyon Teknik Komitesi", kişisel verilerin korunmasına yönelik hukuki standartlar taslağı yayımlamıştır. Söz konusu standartların bulut bilişim, endüstriyel kontrol sistemleri, e-devlet uygulamaları ve büyük veri hizmetlerinde geçerli olması öngörülmektedir.[137]

2017 yılında kabul edilen Siber Güvenlik Kanunu kapsamında kişisel verilerin korunmasına ilişkin birtakım düzenlemelere yer verilmektedir. Kanun şebeke işletmecilerinin, kişisel verileri toplaması ve kullanımı sırasında uyması gereken kuralları düzenlemektedir. Kanun ile AB'de olduğu gibi Çin'de de kişisel verilerin ülke dışına aktarımına ilişkin kısıtlamalar getirildiği görülmektedir. Kişisel verilerin yurtdışına çıkarılabilmesi için güvenlik testinden geçmiş olmak şartı getirilmektedir. Söz konusu test sonucunda alınacak sertifikayla kişisel verilerin yurtdışına aktarılabileceği hüküm altına alınmaktadır.

Mevzuatta açık ve temel bir kişisel veri tanımı yapılmamakta, dağınık düzenlemeler arasında birden fazla kişisel veri tanımına yer verilmektedir. Ayrıca, hassas kişisel veri, veri işleme, veri sorumlusu, veri öznesi, bulanıklaştırma gibi temel kavramların da tanımlanmamış olduğu görülmektedir. Veri işlemeye ilişkin temel ilkeler dağınık mevzuat içerisinde yer almakta olup, genel çerçeve ortaya konulmamaktadır. Ayrıca, ülkede büyük veri analizini dikkate alan veri koruma kuralları da bulunmamaktadır.

Çin'de kişisel verilerin korunmasına ilişkin düzenleyici ve denetleyici bir otorite bulunmamaktadır. Kamu kurumları belirli sektörler bakımından denetim görevini üstlenmekte olup, Sanayi ve Bilgi Teknolojileri Bakanlığı baskın bir uygulama alanına sahiptir.[138] Ayrıca, kişisel verilerin korunmasına ilişkin kuralların yalnızca özel sektör bakımından geçerli olması ve kamu kurumlarını bağlamaması ise eleştirilere sebep olmaktadır. Devletin herhangi bir kurala tabi olmaksızın kişisel

---

[137] Chen ve Wong, 2017: 1-2

[138] International Comparative Legal Guides, Data Protection 2018-China, (erişim tarihi: 30.08.2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/china

verileri yönetme konusundaki baskın gücü, etkili bir kişisel veri korumasını zorlaştırmaktadır.[139]

4.3. Büyük Veri Uygulamalarının Etkisiyle Veri Mahremiyeti Alanında Ortaya Çıkan Yeni Hukuki Yaklaşımlar

4.3.1. Avrupa Birliği

Büyük veri, kişisel olmayan verileri kullanarak veri sahiplerinin yeniden belirlenmesini mümkün kılmakta, bu anlamda AB veri koruma hukukunun temellerini zorlamaktadır. Özellikle, anonimleştirmeyi etkili bir strateji olarak tanımlayan ve kişisel veriler ile kişisel olmayan veriler arasındaki temel ayrımı buna dayandıran düzenlemeler bakımından büyük şüpheler ortaya çıkmaktadır. Ayrıca, büyük verinin doğasındaki, bir kişi hakkında yoğun bilgi toplamanın, bir başka ifadeyle veri yığınları oluşturmanın ortaya çıkardığı muhtemel riskler oldukça ağırdır. Yeniden kimliklendirme, veri kontrolörlerinin bir kişinin profili ile daha fazla verinin ilişkilendirilebilmesine olanak tanıyarak veri ihlali riskini artırmaktadır. Büyük veri, kredi derecelendirmesi, kariyer hedefi, sigorta kapsamı veya sosyal yardımlar gibi doğrudan bireyin hayatıyla ilgili kararların, algoritmalar ve yapay zekâya dayalı süreçler kapsamında otomatik olarak alınması sonucunu ortaya çıkarmaktadır.

Büyük veri analizinden elde edilen çıkarımların doğruluk ve kapsamı önemli ölçüde artarak otomatik karar alma mekanizmalarını güçlendirmektedir. Ancak veri madenciliğine dayalı kararlar, söz konusu kararların ardında yatan verilere erişim ile bunların doğruluğu ve güvenilirliği konusundaki önemli sorunlar nedeniyle veri sahipleri bakımından büyük ölçüde öngörülemez olarak nitelenmektedir.

Büyük veri, 95/46/EC sayılı Veri Koruma Direktifi gibi veri koruma düzenlemeleri üzerinde geniş bir etki meydana getirmiştir. AB Veri Koruma Direktifi temelde şeffaflığa ve kullanıcıların kişisel verilerini kuruluşlarla paylaşma konusunda bilinçli seçimlerini ifade eden rızaya dayanmaktadır. Direktifte öngörülen kişisel verilerin işlenmesinde uyulması gerekli objektif kriterlerin etkileri sınırlı kalmaktadır. Çünkü, Direktif ile getirilen işlemeye ilişkin hükümler, temelde kişinin verisinin

[139] Chen ve Wong, 2017: 2

işlendiğine dair farkındalığı kabulüne dayanmaktadır. Büyük veri ve veri madenciliği gibi yenilikçi çözümler ise bu kabulün yanlış olduğunu ortaya koymaktadır. İlk olarak, büyük veri analizinden faydalanan işletmeler veya kuruluşlar, sahip oldukları veri setlerinden neleri keşfedebileceklerini önceden bilemediklerinden bireylerden ön rıza alabilmeleri mümkün olmamaktadır. İkinci olarak, bireyler potansiyel korelasyonlara ilişkin tutarlı bilgiye sahip olmadıklarından büyük veri analizine ilişkin bilinçli bir rıza ortaya koyamamaktadır. Üçüncüsü ise, mahremiyete ilişkin düzenlemeler yalnızca kişisel verilere, bir diğer ifadeyle kimliği belirli veya belirlenebilir gerçek kişilere ilişkin verilere odaklanmaktadır. Ancak, yeni Veri Koruma Tüzüğü'nde korunan şeffaflık, rıza, asgari veri işleme, erişim, unutulma hakkı ve veri taşınabilirliği gibi temel müesseselerin, kişisel verilerden türetilen yeni kişisel olmayan bilgilere uygulanıp uygulanmayacağı belirsizliğini korumaktadır. Özellikle, kişisel olmayan birkaç veri setinin kullanılarak profilleme yapılabildiği hatta yepyeni kişisel bilgilerin ortaya konulabildiği durumlarda nasıl hareket edileceği belirsizliğini korumaktadır.

4.3.1.1. Veri Koruma Hukukunda büyük veriden doğan temel tartışma alanları

Büyük verinin, AB'de uygulanmakta olan mahremiyet yasaları bağlamında uzun süreden beri kabul edilen aşağıdaki üç temel varsayımı sorgulanır hale getirdiği savunulmaktadır:

a) Kişisel veri-kişisel olmayan veri ayrımı

Büyük veri teknolojileriyle birlikte kişisel veri ile kişisel olmayan veri arasındaki ayrımın hala uygulanabilir olup olmadığı sorgulanmaya başlanmıştır. Kişisel verilerin mahremiyet artırıcı teknolojiler vasıtasıyla kişiyi belirlenebilir kılan özelliklerinden sıyrılarak işlenmesi 'kimliksizleştirme' olarak adlandırılmakta ve uzun zamandan beri kabul edilen bir yöntem olarak benimsenmektedir. Bu çerçevede, veri işleyen kuruluşlar başta anonimleştirme, bulanıklaştırma, şifreleme, anahtar kodlama ve veri paylaşımı olmak üzere, pek çok farklı kimliksizleştirme metodu uygulamaktadır. Ancak, son birkaç yılda bilgisayar bilimciler tarafından ortaya konulan çalışmalar göstermiştir ki bu çözümler arasında en köklü olduğu kabul edilen anonimleştirme sonrasında dahi, veri belirli bir kişiyle yeniden ilişkilendirilebilmekte ve bireyi belirlenebilir (yeniden kimliklendirme) kılabilmektedir. Belirleyiciler içeren veri setleriyle anonimleştirilmiş veri setlerini çapraz referanslayarak geliştirilen ve

bireylerin kimliklerinin yeniden belirlenmesine imkân tanıyan bazı büyük veri uygulamaları da bu alandaki şüpheleri artırmaktadır. Bu gelişmeler ise verileri kimliksizleştirmenin, veriyi istikrarlı bir kişisel olmayan veri kategorisine yerleştirmekten ziyade geçici bir çözüm olabildiğini göstermektedir. Sağlık verilerinin işlenmesi (örneğin; klinik araştırmalar), çevrimiçi davranışsal reklamcılık ve bulut bilişim uygulamaları başta gelmek üzere sayısız iş modeli bakımından sağladığı imkânlar nedeniyle kilit bir teknik çözüm haline gelen yeniden kimliklendirmenin, hukuk doktrini tarafından mahremiyet ilkelerinin uygulanmasını imkânsızlaştırdığına dikkat çekilmektedir.

Bireylerin izleme ve profillemeye karşı korunmaları amacıyla kullanılan anonimleştirilme gibi mahremiyet artırıcı teknolojilerin getirdiği çözümün etkin bir çare olup olmayacağı tartışılmaktadır.

Büyük verinin mahremiyete ilişkin ortaya çıkardığı ilk büyük politika sorusu mahremiyet yasasına tabi olacak verilerin kapsamıdır. Bir veri setinin mahremiyet yasalarının kapsamı dışında değerlendirilebilmesi için ne kadar kimliksizleştirilmiş olması gerekecektir? Bu sorunun cevabı belirsiz olmakla birlikte AB hukukçuları arasında, tüm verilerin kişisel veri olarak ele alınması ve düzenleyici çerçeveye tâbi tutulması gerektiği yaklaşımının da bulunduğu görülmektedir. Ancak, tüm verileri kişisel veri kabul eden böyle bir yaklaşım mahremiyet ve veri güvenliği ilkelerinin uygulanamaması gibi riskli sonuçlar doğurabilecektir. Zira bugün dahi uyulması ve uygulanması zor olan mevcut çerçevenin, böyle bir kabul halinde yönetilemez olacağı aşikârdır.

Daha da önemlisi, görünüşte kişisel olmayan bir verinin dahi mahremiyet yasaları gereğince kısıtlamalara tabi tutulması, verinin yararlı kullanımlarının ciddi bir biçimde sınırlandırılması anlamına gelecektir. Bu çerçevede, FTC tarafından yayımlanan "Tüketim Çağında Tüketiciyi Koruma" başlıklı raporda önerilen yaklaşımın AB tarafından da benimsenebileceği savunulmaktadır. FTC, yeniden kimliklendirmenin yapılmaması için hukuki olarak uygulanabilir organizasyonel taahhütlerin yanı sıra, sözleşmeden doğan yükümlülükler ile söz konusu fiilin engellenmesini amaçlayan bir mekanizma öngörmektedir. Buna göre, şu şartların sağlanması durumunda söz konusu kuruluşun mahremiyet kurallarının uygulama

alanından çıkacağı ifade edilmektedir: 1) Veri setinin makul araçlarla kimliklendirilebilir olması mümkün değilse, 2) Kuruluş söz konusu verileri yeniden kimliklendirmeyeceğini kamuoyuna taahhüt etmişse ve 3) Kuruluş alt kullanıcılarına veriyi kimliksizleştirilmiş formatta tutmasını zorunlu kılmışsa. FTC verilerin tek tek incelenmeksizin ve analiz edilmeksizin, amaçlanan kullanımlarının tanımlanmasının ve mahremiyetin tam anlamıyla garanti altına alınmasının neredeyse imkânsız olduğunu kabul etmektedir. Bununla birlikte, FTC mahremiyete ilişkin soruşturmanın temelini, kimliklendirebilirliğin kesin olarak tespitinden veri işleyen kuruluşların yeniden kimliklendirmeyi yasal olarak önleme taahhüt ve niyetlerinin incelenmesine kaydırmaktadır.

Büyük veri setleri toplayan ve kullanan kuruluşların faydalı kullanımlarından ödün vermemeleri bakımından mümkün olduğu ölçüde verileri kimliksizleştirmeleri önem arz etmektedir. Ayrıca, mahremiyet ilkelerinin kimliksizleştirilmiş verilere kısmen uygulanmaya devam edilmesinin faydalı olduğuna; çünkü araştırmacıların hemen hemen her bilgiyi bir kişiyle yeniden ilişkilendirme olanağına sahip olduğuna dikkat çekilmektedir.

Büyük verinin, kişisel ve kişisel olmayan verilerden yeni bilgiler çıkararak yarattığı düzenleyici ikilemde Veri Koruma Tüzüğü'nün aşırı geniş bir kişisel veri tanımı benimsemesi de bu hususu desteklemektedir.

b) Veri minimizasyonu/sınırlı veri toplama ilkesinin uygulanması

Veri minimizasyonu, veri koruma ve mahremiyete ilişkin hukukî düzenlemelerin temel ilkelerinden biri olmaya devam etmektedir. İlkenin temel mantığına göre kuruluşlar kişisel verileri, meşru hedeflerini elde etmek için gereken ölçüyle sınırlı olarak toplamalıdır. Kuruluşların kişisel verilerin yeniden kimliklendirilebilmesini kısıtlayıcı politikalar uygulamaları ve toplama amaçları ortadan kalktığında bu verileri silmeleri gerekmektedir. Bununla birlikte, büyük veriye dayalı iş modelleri bu ilkenin tamamen tersi bir mantıkla çalışmaktadır. Bu iş modellerinde uzun süreler boyunca çok fazla verinin hızla toplanması teşvik edilmektedir. Zira büyük verinin "gizli cevheri"nin verinin beklenmeyen çıkarımlar sağlayan ikincil kullanımları yoluyla elde edileceği düşünülmektedir. Bu doğrultuda, veri minimizasyonu ilkesi, büyük verinin ihtiyaçlarına cevap veremeyeceği ve

muhtemel veri ihlalleri dolayısıyla büyük veriye ilişkin sosyal ve ekonomik faydanın arka planda kalmasına sebep olacağı noktasında eleştirilmektedir.[140]

Hukuk kurallarının teknolojik ve ticari gerçeklerle çarpıştığı bu alanda, kuruluşlar internet, sensörler, videolar, e-postalar ve sosyal ağlar dâhil olmak üzere pek çok kanaldan veri toplamakta ve depolamaktadır. Dolayısıyla günümüz veri piyasasında, veri minimizasyonu katı biçimde uygulanan bir ilke olmaktan çok uzak görünmektedir. Büyük verinin getirdiği toplum sağlığının iyileştirilmesi, ulusal güvenlik, kamu düzeni, çevrenin koruması ve ekonomik verimlilik gibi toplumsal faydaların mahremiyete ilişkin ilkeler karşısında korunarak dengenin tesis edilmesi önem arz etmektedir. Bu kapsamda, belirlenecek çerçevenin potansiyel mahremiyet risklerine karşılık verinin faydasını da göz önünde bulunduran bir risk matrisine dayalı olarak oluşturulması gerektiği savunulmaktadır.[141]

Muhtemel veri kullanımlarının son derece yararlı olduğu ve mahremiyet risklerinin en düşük olduğu durumlarda, bireyler rıza göstermeseler bile veri işlemenin meşru olması gerektiği savunulmaktadır. Örneğin; tüketicilere daha iyi ürün ve hizmetlerin sunulmasını sağlayan ağ analitiği uygulamalarının[142] önemli bir değer yarattığı kabul edilmektedir. Bu yöntemde, doğru uygulandığı durumda, kimliklendirilmemiş istatistikî verilere dayalı olarak analiz yapıldığından mahremiyete ilişkin risklerin de düşük olduğu bilinmektedir.[143] Bu örnekte rızanın şart koşulması analizin uygulanmasını ve verilerin kullanılmasını zorlaştıracaktır.

Bununla birlikte, kişisel verilerin yalnızca faydayı önceleyerek toplanmaması ve birincil amaçlarla toplanan verinin daha sonra keyfî biçimde yeniden işlenmemesi gerektiği kabul edilmektedir.

Sonuç olarak, büyük veri çağında veri minimizasyonu ilkesinin yeniden yorumlanmaya ihtiyaç duyduğu, veri işleyenlerin mümkün olduğunca verileri kimliksizleştirerek işlemesi, makul güvenlik önlemlerini alması ve verilerin yalnızca

---

[140] Rubinstein, 2012: 5
[141] Tene ve Polonetsky, 2013a: 260
[142] Bireylerin ağ (web) hizmetlerini kullanma biçimlerinin anlaşılması ve optimize edilmesi amacıyla internet verilerinin toplanması, ölçülmesi, analizi ve raporlanmasını ifade etmektedir.
[143] McGee, 2011: 1

belirli bir birey bakımından değil toplumsal bir perspektiften kabul edilebilir olduğu durumlarda faydaya dönüştürülmesi gerektiği kabul edilmektedir.

c) Bireyin rızası ve amaçla sınırlılık ilkesinin uygulanması

Başta 95/46/EC sayılı Direktif olmak üzere mahremiyete ilişkin tüm kanunî düzenlemeler, temel bir ilke olarak rıza ve bireysel kontrolü vurgulamaktadır. Gerek ABD'de uygulanmakta olan "bildirim ve rıza" mekanizması, gerekse AB Veri Koruma Tüzüğü'nün rızayı veri işlemeyi meşru kılan bir mekanizma olarak öngörmeye devam etmesi bu yaklaşımın tüm dünyada hâlâ devam ettiğini göstermektedir.

Hukuki düzenlemelerde yer alan rızaya ilişkin bu vurgu, kimi zaman gerek kuruluşlar gerekse bireyler üzerinde gerçekçi olmayan yükler öngörmektedir. Veri işleyen kuruluşların giderek daha da küçülen kutucuklarda meramlarını anlatırken ve genellikle konuya ilgisiz bireylerin rızalarını almaya çalışırken; bireyler ise karmaşık mahremiyet açıklamalarını okumak, anlamak ve "bilgilendirilmiş" bir rıza göstermek durumunda kalmaktadır. Veri akışının yoğun küresel ağlarda ve uygulamalar arasında gittikçe daha da karmaşıklaşan bir zemine kayması karşısında hizmet sağlayıcılar ve diğer aktörlerin rızaya ilişkin uygulamayı nasıl yönetecekleri sorunu ise giderek derinleşmektedir.

Rıza ilkesine göre alınan rızanın amaca özgü (başka bir deyişle belirli bir bağlamda) olması gerekmektedir. Ancak doğası gereği, büyük veri analizi şaşırtıcı korelasyonlar ve kimi zaman tahmin edilmesi imkânsız sonuçlar ortaya koymaktadır. Ayrıca, işletmelerle bireyler arasındaki bilgi asimetrisi ve bilişsel önyargılar bireylerin mahremiyet tercihlerine ilişkin özgünlüklerine gölge düşürebilmektedir. Veri işleyen kuruluşlar kullanıcılara kontrol sahibi oldukları hissini vererek kolayca verilerinin paylaşımını teşvik edebilmektedir.

Aksi bir senaryoda, bireylerin toplumsal olarak faydalı veri işlemelere rıza göstermedikleri durumlarda başkalarının kararlarına kolayca eşlik edilmesi sonucu ortaya çıkan toplu eylemler ise yenilikçi gelişmeleri tehdit etmektedir. Bireylere sunulan seçim menülerinde yer alan ifadelerin kesinliği bu seçimler konusunda veri sahiplerinin orantısız kararlar vermesine sebep olabilmektedir. Örneğin; arama motorlarının sağlık verilerini işleyeceğine dair rıza talebi karşısında olumsuz yanıt

vermesi muhtemel bireyler, arama günlüklerinin analizi sonucu elde edilen zararlı ilaç etkileşimlerinin ortaya çıkarılmasına ilişkin bulguları övgüyle karşılayabilmektedir. Mahremiyete ilişkin rıza konusunda bireylerin hazıra konma, uygulamakta olduğunu devam ettirme eğiliminin belirgin olduğu görülmektedir.

Rızaya dayalı kişisel veri işlemenin teknolojik gelişmeyi yavaşlatmakta olduğu; çünkü bireylerin beklentilerinin deneyimleriyle birlikte düştüğü de savunulmaktadır. Örneğin Facebook, 2006 yılında haber akışı özelliğini doğrudan başlatmamış ve bunun yerine kullanıcıların rızasını beklemiş olsaydı, söz konusu hizmet hiç ortaya çıkmamış olabilirdi. Veriler akmaya başlayınca bireyler de hizmete alışmaktadır. Aynı şekilde Google'ın coğrafi konum hizmetleri için Wi-Fi ağlarının kapsamlı bir haritasını oluşturmak ve dünya çapında tüm şehirlerde saha taraması yapmak amacıyla tek tek rıza talep etmesi durumunda kaç kişinin bunu kabul edeceği tartışmalıdır. Kaldı ki geçmişe dönük yapılan çalışmalarda, söz konusu özelliği devre dışı bırakma imkânının tanınmasının hemen ardından pek çok kullanıcının bu özelliği devre dışı bıraktığı görülmektedir. Bununla birlikte, Google'ın uyuşmazlığa konu olduğu pek çok olayda, denetleyici otoritelerin Google'ın veri kullanımı yoluyla yarattığı faydayı üstü kapalı da olsa takdir ettiği görülmektedir.

Veri mahremiyeti bağlamında kişisel verilerin kullanımı hususunda açık rıza şartının aranmasından sarfınazar edilmemekle birlikte, bireyin hakkı ile verinin kullanımı sonucunda ortaya çıkacak toplumsal faydanın, geniş bir pencereden değerlendirilmesine ihtiyaç bulunmaktadır. Toplumun doğrudan pazarlama, çevrimiçi davranışsal reklamcılık, üçüncü taraf veri acenteleri ve konuma dayalı hizmetler gibi büyük veri uygulamalarını meşru (hatta övgüye değer) modeller olarak mı gördüğü yoksa bu alanda caydırılması gereken aşırı müdahaleler olduğunu mu düşündüğü araştırılmalıdır. Büyük veri bağlamında veri kullanımının faydasının göz ardı edilerek rıza ve veri minimizasyonuna fazla yoğunlaşmak yeniliği ve toplumsal faydayı tehlikeye atabilmektedir.

4.3.1.2. Veri Koruma Tüzüğü ile öngörülen çözüm önerileri

Yukarıda ifade edilen büyük veriye ilişkin sorun alanlarının çözüme kavuşturulması amacıyla AB Veri Koruma Tüzüğünde üç temel çözüm yaklaşımının

ortaya konulduğu görülmektedir. Bu çerçevede; şeffaflık ve rıza ilkelerinin uygulanmasına yönelik hükümler güçlendirilmekte, profillemeye ilişkin hükümler revize edilmekte ve nihayet yeni bireysel haklar tanımlanarak bireyin kişisel verileri üzerindeki kontrolünün artırılması öngörülmektedir. Ayrıca, getirilen yeni hükümlerle veri kontrolörleri ve işleyicilerin sorumlulukları genişletilmektedir. Söz konusu reformların büyük verinin ortaya çıkardığı zorlukları giderip gideremediğine ilişkin değerlendirmeler aşağıda sunulmaktadır.

a) Şeffaflığın artırılması ve rızaya ilişkin hükümler

Veri toplama konusunda şeffaflığın artırılarak bireylerin güçlendirilmesiyle, genelde nadiren okunan ya da hiç okunmayan, anlaşılması güç kurumsal mahremiyet politikaları göz önüne alındığında, bireylerin kendileri hakkında önceden toplanmış verilere ulaşıp bunlardan faydalanmaları, böylece kendi kişisel kullanımları için büyük veriden faydalanmaları da hedeflenmektedir. Ayrıca, bu tür bir şeffaflık, "gizli" veritabanlarının varlığını engelleyecek ve kabul edilemez kullanımların sınırlaması amacıyla toplumsal baskı oluşturulmasını kolaylaştıracaktır.

AB Veri Koruma Tüzüğü ile veri kontrolörleri bakımından şeffaflık artırıcı bir dizi yeni mekanizmanın öngörüldüğü görülmektedir. 12'nci maddede veri kontrolörlerinin, veri sahiplerine ilişkin tuttukları kişisel verilerin "kolayca erişilebilir olması, açık ve anlaşılır bir dille ifade edilmesi" gerektiği hüküm altına alınmaktadır. 13'üncü maddeyle kişisel verilerin doğrudan veri sahibinden toplandığı durumlarda sunulacak bilgiler, 14'üncü maddede ise kişisel bilgilerin veri sahibinin kendisinden temin edilmediği durumlarda sunulması gereken bilgilere ilişkin ayrıntılı bir liste yer almaktadır. Bireylerin daha fazla şeffaflık ve erişim hakkıyla güçlendirilmesinin AB içerisinde etkin bir toplumsal fayda yaratılmasını ve yenilikçiliği destekleyeceği savunulmaktadır. Bireylere ilişkin verilere makinalar tarafından okunabilir formatta erişim sağlanabilmesi, söz konusu verilerden sadece kuruluşların değil aynı zamanda bireylerin de yararlanacağı bir kişisel veri ekosistemi geliştirilmesini sağlamaktadır.

Ayrıca, ticari sırların korunmasına ilişkin kurallar saklı kalmak kaydıyla, işletmelerin kişisel veri analizi ile ilgili olarak karar verme süreçlerinde kullandıkları kriterleri de şeffaf bir biçimde ortaya koymaları gerektiği Avrupalı hukukçular

tarafından savunulmaktadır.[144] Bu sayede, hukuka aykırı olmasa da etik olmayan profillemelere ve algoritma tabanlı makinalar tarafından kendileri hakkında oluşturulan çıkarımlara karşı koyabilmek için uygun bir mekanizma ve süreç sunulmuş olacağı düşünülmektedir.

Tüzük'ün 4'üncü maddesinin on birinci fıkrası ve 7'nci maddesinde yer alan rızaya ilişkin hükümler doğrultusunda, rızanın yalnızca özgürce verilmiş, belirli ve bilgilendirilmiş olması yeterli görülmemiş, aynı zamanda açık olması şartı da getirilmiştir. Böylece, sessiz kalmanın veya herhangi bir tepki vermemenin geçerli bir rıza anlamına gelmeyeceği düzenlenmiştir. Ayrıca, Tüzük ile veri sahibinin rızasının alındığına ilişkin ispat yükü veri kontrolörlerine yüklemektedir. Rızaya ilişkin bu düzenlemelerin tek başına, uzun süredir devam eden tartışmaların üstesinden gelme veya bireylerin haklarını anlamaları ve bu bilinçle hareket etmelerini sağlama yönünde radikal bir değişimi sağlayamayacağı değerlendirilmektedir. Bu alandaki esas değişimin buradaki gibi artırılmış bir rızaya dayanan düzenleyici bakış açısının ötesinde veri pazarını değiştirerek sağlanabileceği de hukuk doktrininde savunulmaktadır.[145]

Nitekim, Tüzük'ün 6'ncı maddesiyle veri işleyenlerin, çatışan menfaatleri dengelemekle sorumlu oldukları ifade edilmektedir. Bu yaklaşıma göre; kişisel verileri işleyenler verinin toplanması esnasında belirtilen amacın, sonradan ortaya çıkan amaçla örtüşüp örtüşmediğini kendiliğinden denetlemekle yükümlü bulunmaktadır. Veri kontrolörleri, verinin toplandığı ve rızanın alındığı sıradaki amaç ile sonradan ortaya çıkan amaç arasındaki her türlü bağlantıyı tespit etmek, veri sahibiyle veri işleyenler arasındaki ilişkiyi dikkate alarak verinin hangi bağlamda toplandığını göz önünde bulundurmak, kişisel verinin niteliğini dikkate almak, sonradan ortaya çıkan amaç değişikliğinin olası sonuçlarını değerlendirmek ve teknik koruma mekanizmalarını göz önünde bulundurmakla sorumlu kılınmaktadır. Bu durum, tamamıyla rızaya dayanan bir sistemden ziyade Tüzük'ün artırılmış sorumluluk ilkesine verdiği önemi göstermektedir.

b) Profilleme

[144] Dwork ve Mulligan, 2013: 1-5
[145] Rubinstein, 2012: 6

Büyük veri analizinden faydalanan birçok aktör, profilleme ve ayrımcılığa varabilen sonuçların, kararların tarafsız, organik ve insan müdahalesi olmadan otomatik olarak oluşturulduğu, tarafsız algoritmaların birer ürünü olduğunu savunmaktadır. Ancak gerçekte, hem veri setleri hem de algoritmalar yoluyla gerçekleştirilen veriye dayalı seçimler, bağlantılar, çıkarımlar ve yorumlar gibi her türlü işlem, belirli bir amaca yönelmiş bilinçli bir teknik ve insan işbirliğinin karmaşık birer tezahürüdür.[146] Örneğin; farklı ihtiyaçları karşılamak amacıyla çeşitli şekillerde hazırlanan farklı türlerdeki haritaların (örneğin; dağcılık, gezi, alışveriş), sınıflandırma sistemleri ne tarafsız ne de objektiftir; amaçlarına yönelik sübjektif bir yargıyı barındırmakta, tasarımcısının gizli veya açık değerlerini yansıtmaktadır. Ancak bugün, söz konusu algoritmaların manevi ve estetik seçimleri içerdiğine ve bu anlamda insan hayatı, kimliği ve onuru üzerinde oynadığı role ilişkin farkındalığın oldukça düşük düzeyde olduğu ifade edilmektedir.[147]

Avrupa'da uygulanan kanunların genellikle, insan incelemesine tabi olmaksızın otomatik olarak kişisel verilerin işlenmesini yasakladığı görülmektedir. Birçok alanda ise otomatik karar verme süreçlerinin insandan kaynaklı ayrımcı ve sezgisel kararlara panzehir gibi görülmesi yaklaşımı hüküm sürmektedir. Buradaki problemi yalnız makinalar ile insan arasındaki mücadele olarak görmek, karmaşık sosyo-teknik sistemlerdeki endişelerin giderilmesine engel olacaktır. Buradaki temel kaygının tehlike altında bulunan bireysel değerlerin en iyi nasıl yönetileceği olması gerekmektedir. Zira büyük veri tartışmaları nihai olarak değerlerle ilişkili olup matematik ve makinalar ikincil seviyede kalmaktadır.

Veriye dayalı profilleme isteğinin uzun yıllardır var olan bir eğilim olduğu kabul edilmektedir. Ancak büyük veri, her yerde ve her konuda sınıflandırma yapılabilmesini sağlamaktadır. Verinin ikincil kullanımları sonucunda gizlenmiş ve yansıyan çıkarımlara daha fazla önem verilmesi ise toplumsal hayatı ve özel hayatın gizliliğini öngörülmesi ve geri dönülmesi oldukça güç biçimde şekillendirecektir.

95/46/EC sayılı AB Direktifi'nin 15'inci maddesinde yer alan düzenlemeye göre; herkes kendisi ile ilgili hukukî sonuçlar doğuran veya kendisini önemli ölçüde

[146] Dwork ve Mulligan, 2013: 2
[147] Bowker ve Star, 2000: 4

etkileyen ve yalnızca verilerin otomatik olarak işlenmesine dayanan çalışma performansı, kredibilitesi, güvenilirliği ve davranışları gibi kendisiyle ilgili kişisel özelliklerinin değerlendirmesini içeren "otomatik bireysel kararlar"a tabi olmama hakkına sahiptir. Söz konusu düzenlemede belirlenen istisna fıkrasıyla, kanunların izin verdiği hallerde veya taraflar arasında bir sözleşme bulunması durumlarında profillemeye izin verildiği görülmektedir. Dolayısıyla, bu hüküm otomatik kararlara tâbi olmayı tamamen yasaklamamakta, yalnızca söz konusu işlemin nasıl yapılacağını ortaya koymaktadır. Hükmün, otomatik kararların bireyleri büyük ölçüde etkileyen sonuçları da dikkate alındığında sınırlı bir kapsamda kaldığı ve sınırlı bir çözüm öngördüğü değerlendirilmektedir. Maddeyle, doğrudan bu kararların alınmasının yasaklanmasından ziyade, bu tür kararlara direnebilmek için bireyin doğrudan müdahale etmesi öngörülmektedir. Burada; bir itiraz hakkı söz konusu olup ancak veri sahibi, otomatik bir karara tabi olduğunun farkındaysa ve itirazda bulunursa söz konusu hüküm uygulama alanı bulmaktadır. Oysa, büyük veriyle ilişkili mahremiyet ihlalleri büyük çoğunlukla veri sahibinin bilgisi veya farkındalığı olmaksızın ortaya çıkmaktadır. Bu durum ise söz konusu hükmün etkisiz bir madde olarak kalmasına sebebiyet vermiştir. Nitekim, madde metninde yer alan çözüm yolu da bu etkisizliği desteklemektedir. Bir veri sahibinin profilleme veya ayrımcılığa maruz kaldığının anlaşılması halinde, veri kontrolörünün otomatik karar mekanizmasının temelini oluşturan faktörleri yeniden gözden geçirmesi gerekmektedir.

AB Veri Koruma Tüzüğü'nün 22'nci maddesiyle söz konusu hükmün revize edildiği görülmektedir. Otomatik karar alma işlemine tabi olmanın istisnaları arasında bireyin rızası da sayılmıştır. Otomatik veri analizi yöntemlerinin yaygın olarak kullanılmasını dikkate alan bu istisna ile bireyler kendi rızaları ile bu işlemin birer parçası olabilecektir. Ancak maddenin dördüncü fıkrasında getirilen hükümle, hassas kişisel verilerin 9'uncu maddenin ikinci fıkrasının (a) ve (g) bentlerinde belirtilen haller dışında hiçbir biçimde otomatik karar alma mekanizmalarıyla işlenemeyeceği hüküm altına alınmaktadır. Otomatik veri işleyen kontrolörlerin, sözleşmeye veya bireyin rızasına dayanarak otomatik kararlar aldığı durumlarda, veri sahibinin hak ve özgürlükleri ile meşru menfaatlerinin korunmasını, bireyin müdahale edebilmesini ve itiraz hakkını kullanabilmesini sağlamak için uygun tedbirleri alması gerekmektedir.

Bu başlık altında ele alınması önem arz eden konulardan biri de kişisel verilerin etik kullanımı hususudur. Bu konu uzun süredir politika yapıcıların gündeminde olup konunun genellikle 'hassas veri' tanımı çevresinde tartışıldığı görülmektedir. Bununla birlikte, kişisel verilerin bağlamsal doğası nedeniyle hassas veri kategorilerini belirleme girişimleri bugüne kadar genellikle başarısızlıkla sonuçlanmıştır.

Kişisel verilerin etik analizinin sağlanabilmesi için veri işleyenlerin yalnızca kullandıkları veritabanları ve veri setlerini değil, aynı zamanda karar verme süreçlerinde kullanılan kriterleri de (ticari sırların korunması ve diğer fikri mülkiyet kurallarına tabi olarak) ortaya koymaları önem arz etmektedir. Uygulamada bu detayda bilginin tüketicilere karşı satıcının mahremiyet politikası kapsamında sunulduğu ve o zaman bile otomatik işlemelerin bazılarının arkasındaki kriterlerin ve mantığın gizli kalmaya devam ettiği bilinmektedir. Veritabanları kamuya açık olduğu ölçüde kişisel verilerin etik dışı ya da sosyal olarak kabul edilemez kullanımlarından kaçınılabileceği değerlendirilmektedir. İşletmeler, bireylerin hayatlarını etkileyen veri işlemeleri sırasında kullandıkları yöntem ve kriterleri açıklamak durumunda kalırsa; cinsiyet, yaş, ırk, cinsel tercihler veya tıbbi veriler gibi hassas kişisel verilerin etik olmayan kullanımlarından kaçınacaklardır.

Kuruluşların veriye dayalı karar kriterlerini ortaya koymaları gerekliliği ABD düzenlemesi olan Adil Veri İşleme Prensipleri'nde (Fair Information Practice Principles-FIPPs) yer alan şeffaflık ve doğruluk ilkeleriyle de hüküm altına alınmıştır. Büyük veride, incelenmesi gereken husus, ham verinin doğruluğu değil, daha ziyade bu verilerden elde edilen çıkarımların doğruluğudur. Zira mükemmel, zararsız ve doğru verilerden hatalı, manipüle edici veya ayrımcı sonuçlar çıkarılabilmektedir. Bir büyük veri uzmanı, tanımladığı veri setiyle, önerdiği hipotezle veya kullandığı algoritma ile araştırmasının sonuçlarını etkileyebilmektedir. Neticede büyük veri analizi, sonuçları ortaya koyan kişinin kimliğinin ve perspektifinin bir yansıması olarak yoruma açık bir mahiyet arz etmekte; hata, yanlışlık ve önyargı barındırabilmektedir.

Veri işleyen işletmelerin karar kriterlerini (algoritmaları değil, daha ziyade dikkate aldıkları faktörleri) açıklaması gerekliliği, hukuk ve teknoloji arasında önemli bir fay hattı teşkil etmektedir. Makinalar tarafından bireylerin hayatlarını etkileyen

kararların temelini oluşturan çıkarımların, kişisel verilerinin hangi kriterlere göre işlenerek elde edildiğinin açıklanması adil veri işleme süreçleri ve temel adalet ilkesi bakımından önem arz etmektedir.

Ayrıca, AB'de son birkaç yıldır mahremiyet koruması alanında geniş toplumsal değerlere ilişkin çatışmalara dikkat çekilmektedir. Örneğin; işverenlerin muhtemel adaylar hakkındaki arka plan araştırmalarını sosyal paylaşım platformları üzerinden yapma eğilimindeki artış, eleştirmenlerin bu tür platformları 'mahremiyet bozucular' olarak adlandırmasına neden olmuştur. Bu olayda sosyal ağ hizmetleri sunanların, işverenlerin yasadışı veya etik olmayan profillemeleri konusunda sorumlu tutulup tutulamayacağı sorusu akla gelmektedir. İşverenlerin adayları ırk, fiziki görünüm veya cinsel eğilimine göre seçmesi gibi (söz konusu veriyi sağlayan tarafsız platform değil) somut bir durumda işverenin sorumlu tutulması gerekecektir. Zira burada önem arz eden husus işlenen kişisel verinin kendisi olmayıp veriyi işleyen aktörlerce sonuca ulaşmada kullanılan karar kriterleri olmaktadır. Bu itibarla, söz konusu kritere ilişkin şeffaflığın sağlanmasına ihtiyaç bulunmaktadır.

c) Kişisel verilere erişimin güçlendirilmesi ve yeni tanımlanan haklar

Bireyin kişisel verilerine erişme ve düzeltilmesini talep etme hakkı, temel bir AB veri koruma hukuku kuralı olmasına rağmen, yeterince etkin olarak kullanılamamaktadır. Bu durumun temel nedeni olarak ise, söz konusu hakkın kullanılmasının zor ve kullanışsız olması gösterilmektedir. Pek çok kuruluş söz konusu talepleri, yorucu kimlik doğrulama işlemleri ve ödemelerin ardından haftalar hatta aylar süren gecikmeyle ve genellikle yalnızca "basılı ortamda" cevaplamaktadır. Ayrıca, çoğu zaman hangi verileri ve kaynakları kullandıkları ile veriyi nerelere ilettiklerine ilişkin detayları vermemek için çabalamakta, bu anlamda kendilerine tanınan kanunî istisnaların arkasına sığınmakta, açıkladıkları verileri de maskelemektedirler. Büyük veriyle birlikte gelişen veri ekosisteminin karmaşıklığı ise bireylerin kişisel verileri konusunda erişim talebini kime ileteceğini belirlemesini güçleştirmektedir. Veri işleyenler veya alt işleyenlerin farklı yabancı ülke hukuklarına tabi olması ise durumu daha da karmaşık hale getirmektedir.

Veri işleyenler lehine hafifletilmiş veri minimizasyonu ilkesi karşılığında veri işleyen kuruluşların kişisel verileri aracılığıyla yaratılan bu serveti bireylerle

paylaşmaya hazır olmaları gerekmektedir. Bu amaçla bireylere, kişisel verilerine "kullanılabilir" bir formatta erişebilme ve kendi verilerinin analizi ile faydalı sonuçlarından yararlanmak için üçüncü taraf uygulamalarından faydalanabilmelerinin mümkün kılınması gerekmektedir.

Büyük verinin kullanım alanlarının artırılması ve özelliklendirilmesinin yenilikçiliği artıracağı ve kişisel veri uygulamaları için bir pazar yaratacağı öngörülmektedir.[148] Nitekim, açık kaynak kodlu yazılımlar ve telif lisansları gibi gelişmeler de bireylerin kişisel verilerine ücretsiz erişimi, faydalanması ve adalet mantığına dayanmaktadır. Kişisel veriye ilişkin mülkiyet yaklaşımının kabul edilip edilmediğine bakılmaksızın bireylerin, verilerinin yararlı kullanımını isteme hakkı adil hukuk kurallarının gereği olarak mevcut olmalıdır.[149] Nitekim, akıllı şebekelere bireyler tarafından tereddütle yaklaşılması sorunun çözümünün tüketicilerin akıllı şebekelerin ürettiği verinin kendilerine olumlu katkısını doğrudan algılamasıyla çözüleceği değerlendirilmektedir. ABD Yönetiminin başlattığı "Yeşil Düğme" girişiminin arkasında da yatan bu temel düşünceye göre, şebekeler üzerinden toplanan büyük verinin faydalı kullanımı için tüketicilere kendi enerji kullanım bilgilerine doğrudan, standart ve kullanımı kolay bir elektronik formatta erişmelerinin sağlanması gerekmektedir. Kullanıcı verilerini halka açık hale getirmenin, enerji yönetimi sistemleri ve bu bilgileri yorumlayıp kullanabilen akıllı telefon uygulamaları gibi yeniliklerin geliştirilmesini sağlayacağı öngörülmüştür. Ayrıca AT&T, Verizon ve Comcast gibi büyük telekomünikasyon firmaları enerji yönetimi ve ev güvenliği üzerine yenilikçi hizmetler başlatmıştır.

Benzer şekilde, Personal.com isimli başlangıç girişimi bireylerin kişisel bilgilerine erişimini, bunlara erişimi kontrol etmesini ve bunlardan yararlanmasını sağlamayı hedeflemektedir. Girişim, bireylere alışveriş alışkanlıkları, seyahatleri, çeşitli sitelerdeki oturum açma kimlik bilgileri ve konum verilerini depolayabilecekleri ve paylaşabilecekleri bir "veri kasası" sunmaktadır. Kullanıcılar bu verileri aileleri, arkadaşları, çalışanları veya iş arkadaşlarıyla paylaşabilmekte ve ticari kuruluşlara satarak kendi verilerinden para kazanabilmektedir. Şirket, kullanıcılarına veri kasası

[148] Robin, 2012: 1-3
[149] Tene ve Polonetsky, 2013a: 264

sunmanın yanı sıra, başka uygulamaların yapılandırılmış kullanıcı bilgilerine erişmesini sağlayan bir platform olmayı amaçladığını ifade etmektedir.

ABD'nin Yeşil Düğme girişimiyle başarmaya çalıştığı hedefin özel sektöre sirayet etmesinin AB bakımından da büyük fayda sağlayacağı savunulmaktadır. Kişisel verileri kendi kullanımları için toplama ve analize odaklanmış özel işletmelerin sahip olduğu büyük veri setlerine dayalı uygulamaların geliştirilmesi önerilmektedir. Yapılan pazar araştırmaları da bireysel kullanıcıların güçlendirilmesine dayalı yenilikçi iş modellerinin uygulanabilirliğini ortaya koymaktadır. Ayrıca, bireylerin erişiminin ve şeffaflığın artırılması çağrısı, veri mahremiyeti düzenlemelerinin temel kaygılarından biri olan gizli veritabanları vasıtasıyla profillemenin önlenmesi amacına da hizmet etmektedir.

Elbette AB'de kişisel verilere erişim hakkına ilişkin çağrı ilk kez yapılmamaktadır. Ancak, veriden değer yaratarak bireylerin kendi kişisel verilerine kullanılabilir biçimde erişmesi, özellikle AB yaklaşımı bağlamında, yepyeni bir vurguyu ifade etmektedir. Mahremiyet düzenlemelerinin başlangıcından itibaren şeffaflık ve erişim tek başına güçlü araçlar olarak ortaya çıkmamıştır. Zira hayatın olağan akışı içinde bireylerin somut bir fayda sağlamak amacıyla doğrudan şeffaflık ve erişim talep etmediği görülmektedir.

Büyük verinin getirdiği yenilikçi değişim içinde erişim hakkının uygulaması, veriyi somut bir biçimde kullanma ve ondan fayda elde etme becerisi olarak ortaya çıkmaktadır. Mahremiyetin 'özelliklendirilmesi' veya 'uyarlanması' yoluyla kişisel verilere faydalı erişim bireylerin ilgisini çekecek, onları işletmelerin kişisel verilerini kullanmalarıyla ilgili incelemeye itecek ve böylece muhtemel kötüye kullanımlar bizzat bireylerin kendisi eliyle ortaya çıkarılacaktır. Mahremiyet yalnızca bireylerin veri uygulamalarından haberdar olmadığı durumlarda değil, aynı zamanda ilgisiz ve etkisiz olduğu durumlarda da zarar görmektedir. Bireylerin ilgisiz ve etkisiz olduğu bir ortam ise, düzenleyici çerçevenin başarı veya başarısızlığından bağımsız olarak, veri toplama ve kullanma konusunda yetersiz bir kontrol sağlamaktadır. Bireylerin verilerine kullanılabilir, faydalı veya katma değer sağlayacak bir şekilde erişebildiği durumda, veri ihlalleri konusunda kontroller doğal olarak birey tarafından yapılacak

ve bu sayede mahremiyet yasalarının uygulanması bakımından bireyler pratik işlevini yerine getirmiş olacaktır.

Ayrıca, bireyler dışında büyük veri kümelerine geniş araştırma topluluklarının erişebilmesi de önem arz etmektedir. Geleneksel olarak, bilim adamları bir araştırma yayımladığında, diğer bilim adamlarının sonuçları doğrulayabilmesi için temel verileri erişime açık tutmaktadır. Ancak, büyük veride analiz edilen ve sonuçları yayımlanan araştırmaya ilişkin veriler açık hale getirilmemekte, çoğunlukla yalnızca belirli kuruluşların çalışanları söz konusu erişimden yararlanmaktadır. Bu gibi durumlarda veri üzerinde çalışan veribilimcilerin, bu verinin özel bir işletmenin mülkiyetinde bulunduğu, hatta müşterilerinin mahremiyetini ihlal edebilecekleri savunmasını getirdikleri görülmektedir. Bu çerçevede, büyük veri setlerine kimlerin erişebileceği, hangi amaçlarla, hangi bağlamlarda ve hangi kısıtlamalarla yararlanabileceği gibi temel sorulara cevap verilmesi gerekmektedir.

Bireylerin kişisel verilerine makinalar tarafından okunabilir ve kullanılabilir bir formatta erişmesi AB hukukunda veri taşınabilirliği hakkını gündeme getirmiştir. Bu çerçevede, Tüzük'ün 20'nci maddesinde düzenlenen veri taşınabilirliği hakkıyla bireylerin kişisel verilerinin (kişisel profilleri, fotoğrafları, iletişim bilgileri vb.) bir uygulama veya hizmetten başka bir uygulama veya hizmete taşınmasına imkân tanınmaktadır. Veri taşınabilirliği hakkı, yeni teknolojik hizmetlerden faydalanılması ve bu alandaki rekabetin teşvik edilmesi bakımından önemli görülmektedir. AB hukuku bakımından yeni olan bu kavram esasında veri koruma hukukunun değil ABD rekabet hukukunun bir parçasıdır. Bu kavrama göre, kişisel veriler bireye ait birer varlığı ifade etmekte olup adil bir fiyatla işlem görmedikleri sürece bireyin kendi kontrolü altında kalmaktadır. AB Veri Koruma Tüzüğü'nde de yer alan veri taşınabilirliği mahremiyet yasasının dokusunun içine yedirilmeye çalışılsa da bu yaklaşımın AB anlayışı bakımından çok ileri gittiği yönünde eleştiriler bulunmaktadır.[150] Ayrıca, veri taşınabilirliği hakkının kişisel veriyi ticari olarak zahmetli yöntemlerle toplamak, düzenlemek ve paylaşmak için önemli beceri ve kaynaklara yatırım yapan yenilikçi işletmelerin sahip olduğu rekabet avantajını ortadan kaldıracağı hususunda eleştiriler bulunmaktadır. Kişisel veriler, ne ticari sır

[150] Eleştiriler için bkz. Tene vePolonetsky, 2013a: 269

alanına ve fikri mülkiyet haklarına engel olacak mahiyette bireylerin münhasır bir varlığı olarak görülmeli ne de bireylerin fayda sağlamalarını engelleyecek şekilde münhasıran işletmelerin mülkiyetine bırakılmalıdır. Kişisel verileri, toplumsal fayda ve yenilikçiliğin desteklenmesi için ortak bir kaynak olarak ele almayı öngören bir politika çerçevesi oluşturulmalıdır.

AB Genel Veri Koruma Tüzüğü ile getirilen unutulma hakkı ve silinme hakkı ise, özellikle sosyal ağlar ve diğer internet hizmetlerinde gönüllü olarak paylaşılan verilerin hızla yayılması, saklanması ve dolayısıyla sürekli analizi ile mevcut kalması dolayısıyla ortaya çıkan mahremiyet ve itibar kaybı gibi zararların daha etkili bir şekilde giderilmesi amacıyla kişisel verilerin silinmesi temeline dayanmaktadır. Tüzüğe göre bir veri sahibinin kendisi ile ilgili daha önce yayınlanmış kişisel verilerinin silinmesini talep etmesi durumunda, veri kontrolörü bu konuda üçüncü taraflara bilgi vermek ve bu alanda gerekli teknik tedbirleri almak durumundadır. Ancak, söz konusu yükümlülüğün büyük veri gibi, veri setlerine birden fazla tarafın erişmekte olduğu durumlarda oldukça külfetli veya imkânsız olabileceği değerlendirilmektedir. Ayrıca bu haklar, kişisel veriler bakımından tanımlanmış olmakla birlikte, büyük verinin merkezinde yer alan analiz yöntemleri sonucunda anonimleştirilmiş verilere dayanarak yapılan ve doğrudan bireyi belirlenebilir kılan tahmini çıkarımlarda bireylerin nasıl korunacağı belirsizlik arz etmektedir.

Sonuç olarak, AB hukukunda şeffaflık, erişim ve doğruluk ilkelerine ilişkin gereksinimler artarken; veri minimizasyonu, rıza ve bireysel kontrol ilkelerinin büyük veriye uyarlanarak gözden geçirildiği görülmektedir. Daha fazla veri, daha çeşitli veri, yeni analitik yöntemler ve daha hızlı bilgisayarlar içeren büyük veri olgusu, AB veri koruma kuralları bakımından ciddi zorlukları beraberinde getirmektedir. Ancak, bu zorluklar ne kadar geniş kapsamlı ve karmaşık olursa olsun tartışma ve önerilerin kaçınılmaz olarak, adil veri işleme ilkelerinin uygulanmasında yoğunlaştığı görülmektedir. Büyük verinin getirdiği hukuki zorluklar karşısında adil veri işleme ilkelerinin uygulanmasının, değişen iş ve teknolojik koşullara uyum adına atılmış önemli bir adım olarak görülmesi gerekmektedir. Zira bu ilkeler sahip oldukları esneklik sayesinde önemli paradigma değişimleri karşısında dirençli kalmakta, bir anlamda zaman zaman bazı ilkeler ön plana çıkarken bazıları geri planda kalmaktadır.

Hukuki metinlerin teknolojik gelişmeler karşısındaki katı duruşunun bu şekilde hafifleyebileceği değerlendirilmektedir. Zira değiştirilmesi güç kurallarla yönetilen bir süreçte sadece teknolojik değişime ayak uyduramamakla kalınmaz; ekonomik ve sosyal fayda da göz ardı edilmiş olur. Bu çerçevede, AB Veri Koruma Tüzüğü'nün de gösterilen çabaya rağmen bu gerçeği değiştiremeyeceği, dolayısıyla yeni yolların aranması gerektiği savunulmaktadır.[151]

4.3.2. Amerika Birleşik Devletleri

Geçtiğimiz kırk yılda, veriye dayalı yenilikçilik ile mahremiyet arasındaki denge, 1980 yılında kabul edilen OECD Mahremiyet İlkelerine dayanan adil veri işleme ilkeleri olarak da adlandırılan bir dizi ilkeye göre düzenlenmiştir. ABD Hükümeti'nin güncel adil veri işleme ilkeleri içerisinde de bu ilkelerle uyumlu; bireysel kontrol, şeffaflık, amaç ile sınırlılık, güvenlik, erişim, doğruluk, odaklanmış veri toplama ve hesap verebilirlik ilkelerinin yer aldığı görülmektedir.

ABD'deki mahremiyete ilişkin sektörel düzenlemelerin hiçbiri doğrudan büyük verinin özel niteliklerine odaklanmamaktadır. ABD düzenlemeleri veri kümesinin boyutu veya kullanılan teknik ne olursa olsun, bütün veri kullanımlarını hüküm altına almaktadır. Zira ABD yaklaşımında büyük verinin tamamen farklı ve bağımsız bir çaba olarak değerlendirilmesi anlayışı kabul görmemektedir. Bununla birlikte, büyük veritabanlarında saklanan bilgilerinin yanlış kullanımından bireylerin büyük zarar görebileceği ve ayrıca gerek özel sektör gerekse kamunun resmi kararlarının giderek artan bir şekilde algoritmalara dayanmasının bu tehdidi artırdığı kabul edilmektedir.[152]

Büyük veri tekniklerinin mevcut mahremiyet düzenlemeleri üzerinde genel bir revizyonu gerektirecek biçimde önemli bir baskı oluşturduğu kabul edilmekle birlikte, ABD hukukunda iki temel hususun değerlendirilmesi gerektiği ifade edilmektedir. İlk olarak, büyük verinin ortaya koyduğu şaşırtıcı ilişkisel sonuçlar, insanların ortaya koyabileceği çıkarımların oldukça ötesinde değerlendirilmektedir. Büyük veri bu özelliği dolayısıyla veri sahiplerinin bilgilendirilmesi ve rızası temeline dayanan

[151] Rubinstein, 2012
[152] Citron, 2007: 241

mahremiyet düzenlemelerini zorlamaktadır. Veri işleyenlerin, bu öngörülemez durum karşısında veri sahibini nasıl bilgilendirebileceği belirsizlik arz etmektedir. Bu durumun FIPPs'te öngörülen amaçla sınırlılık ve kullanım amacı ilkelerinden vazgeçmek anlamına gelebileceği ifade edilmektedir.[153] İkinci olarak büyük veri, mahremiyet artırıcı teknolojiler yoluyla kişisel verilere ilişkin riskleri azaltma girişimlerini zayıflatmaktadır. ABD'de uygulanmakta olan Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Kanunu (Health Insurance Portability and Accountability Act-HIPAA) ve benzeri kanunlar, anonimleştirmeyi ve verilerin gizlenmesine ilişkin diğer teknik yöntemleri teşvik ederken, büyük veri tekniklerinin anonimleştirilen veya gizlenen verileri geri getirebilme özelliği bu çözümlerin etkisini ortadan kaldırmaktadır.

ABD'de mahremiyete ilişkin sorunların çözümü amacıyla, tüm toplumu kapsayan kapsamlı mahremiyet çözümlerinin zorluğu karşısında, uygun hak arama yöntemlerinin belirlenmesi yaklaşımı ortaya çıkmaktadır. Bunun temel nedeni ise daha önce belirtildiği gibi, ülkede çerçeve bir veri koruma düzenlemesinin bulunmaması ve bu alanda bağımsız bir otoritenin olmaması olarak değerlendirilmektedir. Bu kapsamda, ülkede gelişen hukukî yaklaşımların genel olarak tüketicinin korunması ve rekabet hükümleri çevresinde şekil aldığı göz ardı edilmemelidir. ABD hukukunda büyük veri ile veri mahremiyeti arasındaki uyumun geliştirilmesi amacıyla yapılması gerekenler şu şekilde özetlenmektedir:[154]

a) Büyük verinin sağladığı gözetim imkânı karşısında mahremiyete ilişkin düzenlemelerin gözden geçirilmesi gerekmektedir:

ABD hukuk çevrelerinde kabul edilen güçlü görüşe göre bireyin belirli bir davranışının rızası alınmaksızın izlenebilmesi, ancak düzenlemelerde yer alması durumunda mümkün olmalıdır. Ayrıca, kişisel olmayan verileri toplama zorunluluğunun kabulü ile kamusal alanda izleme yoluyla toplanan veri ile belirli bir hizmet sunumunun bir yan ürünü olarak toplanan veri arasında ayrım yapılması

[153] Ohm, 2016: 100
[154] Strandburg, 2016: 32

gerektiği, bu ayrımın büyük veriye ilişkin güncel tartışmaları açıklığa kavuşturacağı savunulmaktadır.

Bu noktada, her izleme bakımından rıza aranmayacağı vurgulanmakla birlikte, izleme faaliyetinin halka açık olarak gerçekleştiği durumlarda rızanın zaten var olduğunun da kabul edilemeyeceği ifade edilmektedir. Bu hususta getirilecek yasalarla, belirli amaçlarla izleme bakımından, vaka bazında yetkilendirme mekanizmalarının sağlanabileceği ifade edilmektedir (örneğin; bir araştırmanın parçası olarak, kurumsal etik kurulları benzeri yapılar veya mahremiyet kurulları tarafından belirli kriterlerin sağlandığının belirlendiği izlemeler bakımından, mahremiyet sorumluluğundan istisna olunması gibi).

Nitekim, Federal Ticaret Komisyonunun 2010 tarihinde yayımladığı "Kişisel Bilgilerin Korunması: İşletmeler İçin Bir Kılavuz" adlı raporda işletmelerin veri toplamasının "yalnızca belirli ve meşru bir iş gereksiniminin yerine getirilmesi için gerekli verilerin toplanması" ile sınırlı olması önerilmektedir. Söz konusu ifade, yukarıda vurgulanan görüşle benzer olmakla birlikte, gerek mevcut mahremiyet yasası gerekse bu yasanın amaçlarıyla uyumlu olarak, izleme ve hizmet sunumu sonucunda elde edilen veriler arasında ayrım yapılmasının yerinde olacağı ifade edilmektedir. Bu anlamda, izleme sonucu elde edilen veri ile hizmet sunumu dolayısıyla ortaya çıkan veri arasında ayrım yapılabilmesi için, veri sorumlularının kendi mahremiyet politikalarında; hangi hizmetleri verdikleri, izleme yoluyla (başka bir ifadeyle hizmet sunumunun bir ürünü olmadan) veri toplayıp toplamadıklarını, hangi verilerin izlenerek elde edildiğini ve bu verilerle ne yaptıklarını belirtmeleri gerekmektedir. Bu kapsamda, hizmet sağlayıcılara, izleme yoluyla veri toplama konusunda hem rıza hem de açık olma gibi gereklilikleri sağlamak gibi önemli bir sorumluluk tanımlanmaktadır.

Ayrıca, ABD'de uygulanmakta olan hukuki çerçeve hükümetin özel kuruluşlar tarafından tutulan tüm verilere erişebilmesini mümkün kılmaktadır. Bu durum ise ABD hükümetinin hizmet sağlayıcılar ve diğer özel kuruluşlar tarafından tutulan kişisel verilere sınırsız erişimi endişesini büyük veri ve mahremiyet bağlamında

artırmaktadır. Bu durum ise ABD'de bu yasanın değiştirilmesi gerektiği yönünde eleştirileri beraberinde getirmektedir.[155]

b) Verileştirme[156] ile bir hizmet dolayısıyla ortaya çıkan verilerin yeniden kullanılması arasında esaslı bir ayrım yapılması gerekmektedir:

FTC'nin 2010 tarihli raporunda[157], ürün ve hizmetin sunumuyla doğrudan alakalı olması, işletmenin iç operasyonları için gerekli olması, suçun önlenmesi, kanunun uygulanması ve kamu yararı amacıyla işleme gibi yaygın olarak kabul edilen uygulamalar bakımından veri toplama ve kullanımında rıza aranmayacağı ifade edilmektedir. Komisyonun söz konusu kabulünün temel mantığı; sayılan veri kullanımlarından bazılarının zaten kullanıcılara açık olması, bazılarının politik nedenlerle gerekli olması ve bazı kullanımlar bakımından 'rıza' aramanın faydasının aramamaktan daha düşük olacağı şeklinde ifade edilmektedir.

Ancak, "işletmenin iç operasyonları için gerekli olmak" veya "yaygın olarak kabul edilen uygulamalar" ifadeleri fazla belirsiz ve esnek olarak değerlendirilmektedir. Dahası, piyasada bildirim ve rıza konusundaki başarısız kısır döngü düşünüldüğünde, işletmelerin yaygın uygulamaları kolayca kabul edilebilir olarak nitelenebilmekte; veri sahipleri verilerinin işlenmesinin mahiyetini anlayamamaktadır.

Raporda aynı zamanda "daha net, daha kısa ve daha standartlaştırılmış" mahremiyet bildirimleri yoluyla veri kullanımlarına ilişkin şeffaflığın artırılması önerilmektedir. Ancak, söz konusu hususun nasıl gerçekleştirileceği netleştirilmemektedir. Ayrıca veri sahiplerinin veri işleyenlerin verileriyle ne yaptığını anlamak için, mahremiyet politikalarının şu anda sağladığından fazla detaya ihtiyacı bulunmaktadır.

---

[155] Ohm, 2016: 105

[156] Verileştirme (datafication) terimi temel olarak, bir bilgiyi ölçülebilir hale getirerek tablolaştırılabilir ve analiz edilebilir kılmak şeklinde tanımlanmaktadır. Daha ayrıntılı bilgi için bkz.: Mayer-Schönberger, and Cukier, K., 2013: 210-242

[157] FTC, "Protecting Consumer Privacy in an Era of Rapid Change: a Proposed Framework for Businesses and Policymakers", 2010, (erişim tarihi: 17.07.2017), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

Verinin hizmet sunumu amacıyla kullanılmasıyla diğer kullanımları arasında veya sadece bilgi edinme amaçlı veri toplama ile verileştirme arasında bir ayrım yapılmasının, mahremiyet bildirimlerini basitleştirip standartlaştırmak açısından iyi bir yol olacağı ifade edilmektedir.

Modern veri mahremiyeti endişeleri, öncelikle bilgi verileştiğinde tetiklenmektedir. Bu sebeple, verileştirme olgusunun bütün ayrıntılarıyla bir hukuki çerçeve ile ortaya konulması gerektiği ifade edilmektedir. Bu çerçevede, kısa ömürlü dosya dolabında saklanan veri ile bir hesaplamanın manipülasyonu için biçimlendirilmiş ve toplanmış veri arasındaki farkın veri sahipleri bakımından önemli olduğu ifade edilmektedir. Çünkü verileştirme, yalnız hizmet sunumu için kullanıldığında bile, belirli mahremiyet risklerini arttırdığından, veri sahiplerinin bu konuda bilgilendirilmeleri gerekmektedir.

Bu çerçevede, hayata geçirilecek düzenlemede şu hususların bulunması gerektiği ifade edilmektedir: 1) Hizmet sunumu sırasında bildirim ve rıza bulunmaksızın veri toplanmasına imkân verilmesi, 2) Hizmet sunumu sırasında bildirimde bulunularak verileştirmeye imkân verilmesi, 3) Bildirim ve açık rızanın bulunmadığı durumlarda ise, verinin kullanımının, verileştirilmesinin veya üçüncü taraflara aktarılmasının yasaklanması. Veri sahibine bildirimin gerekli olduğu durumlarda, kimlik veya kategoriler de dâhil olmak üzere verinin nereye transfer edildiği, hangi bilgilerin tutulduğu ve hangi amaçla kullanıldığının belirtilmesi gerekmektedir.

Burada ifade edilen hukuki rejimin, ABD veri hukukunun özünde yer alan bildirim ve rıza ile ilgili tüm sorunları çözemeyeceği bilinmekle birlikte, veri sahiplerinin veri hazırlama ve yeniden kullanımına ilişkin mahremiyet endişelerini bir nebze de olsa azaltacağı öngörülmektedir. Bildirimler, işletmelerin kişisel bilgileri yalnızca hizmet sunmak için kullandığı durumlarda, kullanıcılara hızlıca bilgi verilmesi anlamında etkili bir çözüm olarak görülmektedir. Dahası, kullanıcıların mahremiyet kaygılarını gidermeleri için işletmelerin ne yaptıkları konusunda doğru ve açık bir şekilde açıklama yapmaları teşvik edilmiş olacaktır.

c) *En azından büyük kuruluşlar için bildirim ve rıza esaslı bir yaklaşımın benimsenmesi gerekmektedir:*

Uygulamada bildirim ve rızaya ilişkin karmaşık ve oldukça uzun beyanlar dikkat çekmektedir. ABD'de yapılan bir araştırmaya göre ortalama bir bireyin internet ortamında kişisel verilerinin işlenmesiyle ilgili bildirim ve rızasını talep eden karşılaştığı her metni okuması durumunda, yılda ortalama 244 saatini harcaması gerektiği ortaya çıkmıştır.[158] Nitekim, WEF'te de açık rıza şartının tamamen terk edilmesi, daha ziyade sorumluluk ilkesine ağırlık verilmesi önerisi getirilmiştir.[159]

Bireyin rızasından tamamıyla vazgeçilmesi fikrine karşın, büyük veri bağlamında bildirim ve rızanın işleyişinin iyileştirilebileceği fikri de savunulmaktadır. Bu amaçla, en azından büyük kuruluşlar üzerinde net ve anlaşılabilir bir bildirimin zorunlu kılınması faydalı görülmektedir. ABD hukuku bakımından makul bir tüketici tarafından anlaşılabilir olduğu kanıtlanamayan bildirimlerin FTC tarafından "haksız ve aldatıcı" kabul edilmesi çözümü öngörülmektedir. Ticaret kanunlarında kullanılan tüketici anketleri ve deneyler gibi tekniklerin, bildirimlerin anlaşılabilirliğini değerlendirmek amacıyla kullanılabileceği savunulmaktadır. Bu yöntem, küçük işletmeler bakımından makul olmayan maliyetlere sebep olabilmekle birlikte, kişisel bilgilerin çoğunu toplayan büyük işletmelere gerekli testlerin uygulanmasının faydalı olacağı ifade edilmektedir.

Ayrıca veri analistlerine, analiz ettikleri dijital verilerin aslında insan hayatını temsil ettiğinin hatırlatılması gerekmektedir. Söz konusu uyarıcılar, verinin hassasiyetiyle ölçeklendirilmeli ve en hassas verilerle çalışanlar, sabit hatırlatıcılarla yüzleşmelidir. Büyük veri tekniklerinin, bireylerin yaşamları ile ilgili geleneksel ve resmi karar alma yöntemlerinin yerini alacağına ilişkin endişeler karşısında; algoritmanın arkasındakilerin -veri bilimciler başta olmak üzere- analiz ettiklerinin gerçek bireylerin hayatı olduğu konusunda düşünmeye zorlanması gerekmektedir.

---

[158] McDonald veCranor, " The cost of reading privacy policies", A Journal of Law and Policy for the Information Society, Privacy Year in Review, pp. 8, 2008, (erişim tarihi: 21.07.2017), http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[159] WEF, Unlocking the Value of Personal Data: From Collection to Usage, 2013, (erişim tarihi: 23.06.2016), http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

4.3.3. İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD)

Büyük veri, nesnelerin interneti ve yapay zekâ gibi algoritmaya dayalı karar mekanizmalarını kullanan yenilikçi dijital teknolojilerin kullanımındaki artış, bireysel mahremiyet ve veri koruması üzerinde bir dizi muhtemel olumsuz etkiyi beraberinde getirmektedir. OECD 2017 Dijital Ekonomik Görünüm Raporu kapsamında 2016 yılında gerçekleştirilen ankete yanıt veren ülkelerin büyük bir kısmı (34 ülkeden 25'i) söz konusu teknolojiler karşısında mevcut düzenlemelerin uygulanmasının önemli zorlukları beraberinde getireceğini ifade etmektedir. Ankete katılan çoğu ülke, söz konusu teknolojilerin toplumsal etkileri ile etik zorluklarının iyi anlaşılması gerektiğini vurgulamış ve yeni bir veri yönetişim politikası ve düzenleme çerçevesi geliştirilmesine ihtiyaç olduğunu ifade etmiştir. Bu çerçevede, örneğin; Fransız veri koruma otoritesi, bu alanda çalışmak üzere yenilikçilik ve dijital teknolojiler üzerine bir çalışma grubu oluşturmuştur. Açık veri bağlamında kişisel verilerin etkin bir biçimde anonimleştirilmesinin veya kişinin belirlenemez kılınmasının teknolojik zorluğu karşısında, birçok ülke yenilikçiliği destekleyen politika önlemlerini hayata geçirmeyi amaçlamaktadır.[160]

Ayrıca, birçok ülkede (34 ülkenin 15'inde) sınır ötesi veri transferine artan bağımlılık da göz önüne alındığında, mahremiyet korumasının uluslararası boyutu itibarıyla önemli bir politika alanı olarak kabul edildiği görülmektedir. Bu bağlamda, mahremiyet düzenlemelerinin koordinasyonu ve uyumlaştırılması yoluyla küresel anlamda birlikte çalışabilirliğin, ele alınması gereken önemli bir zorluk olduğu ifade edilmektedir. Söz konusu uyum ihtiyacının yalnızca uluslararası düzeyde (ulusal mahremiyet rejimleri arasında) değil, aynı zamanda kimi ülkelerde ulusal düzeyde de (bölgesel mahremiyet düzenlemeleri arasındaki fark bakımından) geçerli olduğu görülmektedir.[161]

Yeni AB veri koruma çerçevesinin benimsenmesiyle uyumlaştırılmış bir veri koruma kuralları seti ortaya konulmakta ve ayrıca uluslararası veri transferini kolaylaştırmayı amaçlayan genişletilmiş bir araçlar seti sağlanmaktadır. Bu çerçevede, AB Veri Koruma Tüzüğü'nün üye ülkelerin ötesine geçerek AB pazarında mal ve

[160] OECD, 2017: 92
[161] A.g.e.: 92

hizmet sunan veya AB vatandaşlarının davranışlarını izleme faaliyeti yürüten tüm uluslararası işletmeleri bağladığı ifade edilmektedir. Sonuç olarak, OECD'nin "Kişisel Verilerin Mahremiyetinin ve Sınır Ötesi Transferinin Korunması Hakkında Tavsiye Kararı"nın 6'ncı bölümünde de vurgulandığı üzere, hukuki çerçevede birlikte çalışabilirlik büyük önem taşımaktadır. OECD üyesi ülkelerin, burada yer alan ilkeleri uygulamaya geçirmek amacıyla mahremiyet düzenlemeleri arasında birlikte çalışabilirliği teşvik eden uluslararası mekanizmaların geliştirilmesini teşvik etmesi ve desteklemesi gerekmektedir.

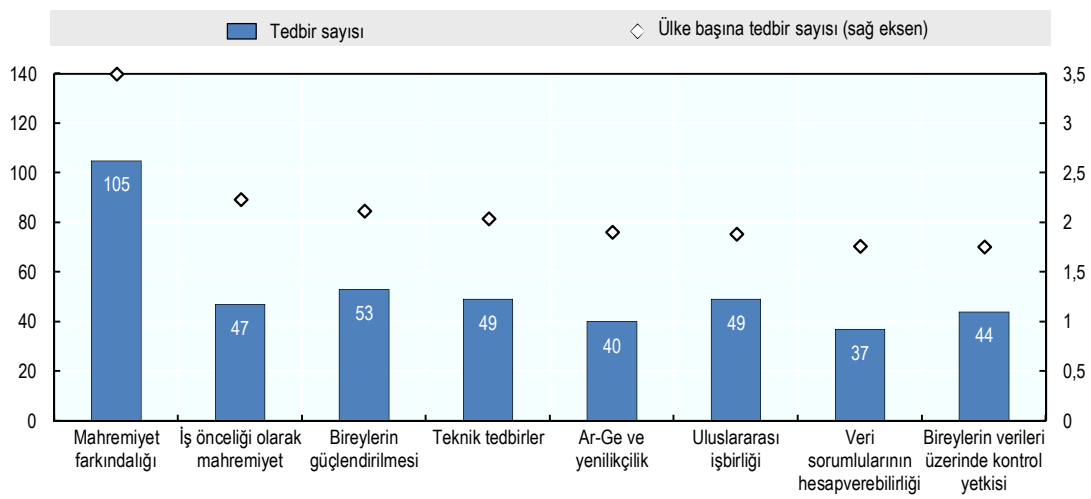
Birçok OECD ülkesinde kamu tarafından büyük verilerin kullanılması, mahremiyet koruması alanında büyük yasal zorlukları da beraberinde getirmektedir. Ankette mahremiyete ilişkin zorluklarla ilgili soruyu yanıtlayan 32 ülkeden 18'i, kamu idarelerinde kişisel verilerin tekrar kullanımının mahremiyet alanında politika zorluğu oluşturduğunu ifade etmiştir. Bu ülkelerin yarıya yakını özellikle kişisel verilerin özel sektörden toplandığı durumlarda, ulusal güvenlik amacıyla toplanan kişisel verilerin en önemli politika zorluklarından birini oluşturduğunu ifade etmiştir. 2016 yılında OECD'nin kilit ortaklarından Brezilya Hükümeti tarafından kabul edilen 8789 sayılı Kararname ile kamu kuruluşları tarafından oluşturulan kişisel verilerin tutulduğu veritabanlarının paylaşımı düzenlenmektedir. Kararname ile devletin kişisel verileri işlemesine, ulusal güvenlik gerekçeleriyle, dinleme kararları da dâhil olmak üzere, kişisel verilere erişimine ve toplamasına imkân verilmektedir. Şebekeler üstü (Over The Top-OTT) hizmetlerin de dâhil edildiği Kararname toplumdaki endişeleri artırmıştır. AB'de bu alanda farklı bir yaklaşım benimsenmektedir. Yeni AB veri koruma yasal çerçevesinin bir parçası olan 2016/680 sayılı Polis Direktifi suçların önlenmesi, soruşturulması, tespiti, kovuşturulması veya cezai yaptırımların uygulanması amacıyla kişisel verilerin yetkili makamlarca işlenmesi alanında da kişisel verilerin korunması hakkını korumayı amaçlamaktadır. Bu bağlamda, AB üyesi ülkelerin kolluk kuvvetleri bu alanda büyük veri teknolojilerini kullanabilmek için söz konusu Direktif'in gerekliliklerine uymakla sorumlu kılınmaktadır.[162]

2016 OECD Dijital Ekonomik Görünüm Politikası Anketi'ne verilen cevaplar hükümetlerin, yukarıda vurgulanan mahremiyet zorlukları ile başa çıkabilmek için

[162] A.g.e.: 93

çeşitli politika tedbirleri benimsediğini ortaya koymaktadır. Bu politika önlemleri arasında, mahremiyet bilincinin artırılması en üst sıralarda yer almaktadır. Ankete katılan ülkelerin sahip olduklarını bildirdikleri mahremiyetle ilgili 424 politika tedbirinin dörtte birinin (105) mahremiyete duyarlılığın artırılması ve eğitim (devlet, işletmeler ve bireylerde) alanlarında olduğu görülmektedir. Söz konusu tedbirlerin dörtte birinin (97) ise hızlı ve kolay telafi mekanizmalarının geliştirilmesi veya kişisel verileri üzerinde bireylerin kontrolünü arttıran imkânların tanınması gibi yollarla bireylerin güçlendirilmesi konusunda olduğu ifade edilmiştir. Ülkelerin gündemlerinde yer alan diğer politika önlemleri arasında; mahremiyeti bir iş önceliği olarak teşvik etmek (47) ve mahremiyet alanında Ar-Ge ve yeniliği destekleyici (40) teknik tedbirlerin (49) alınmasını teşvik etmek (136) ve uluslararası işbirliği ile ülkeler arasındaki mahremiyet mevzuatının koordinasyon ve uyumlaştırılmasının teşvik edilmesi (49) bulunmaktadır (Şekil 3.1).[163]

Şekil 3.1. OECD Ülkelerinde Uygulanan Mahremiyet Politikaları



Kaynak: OECD, 2017.

OECD tarafından dijital ekonomiye ilişkin güvenin ana bileşenleri, güvenlik ve mahremiyet koruması olarak ifade edilmektedir.[164] Güven unsurunun mahremiyet boyutu (kişisel verilerin korunması alanı) ile ortaya çıkan sorunların üstesinden gelmenin oldukça karmaşık ve zorlu olduğu ifade edilmektedir. Veriye dayalı

[163] A.g.e.: 93
[164] A.g.e.: 245

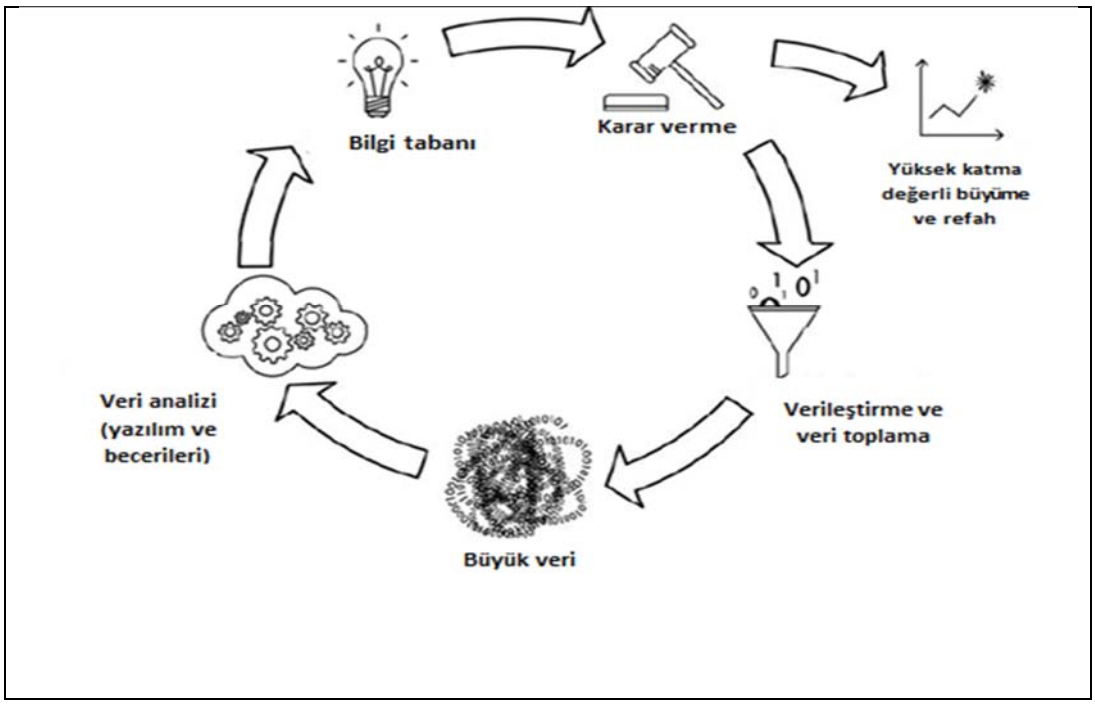
yenilikçilik alanında, verilerinin toplanması ve kullanımı nedeniyle tüketici konumundaki bireylerin korunması ihtiyacı ortaya çıkmakta ve mahremiyete ilişkin daha genel bir analizi gerekmektedir.

4.3.3.1. Veriye dayalı yenilikçiliğin mahremiyetle ilişkili muhtemel etkileri

Büyük veri gibi yenilikçi teknolojiler dolayısıyla ortaya çıkan ve çalışmanın ilk bölümünde de ifade edilen veri toplama, analizi ve kullanımındaki yeni eğilimler, işletmelerin ve kamu kesiminin örgütsel uygulamalarında birtakım dönüşümleri beraberinde getirmektedir. Bu eğilimler ise mevcut politika, kanun ve normların mahremiyeti yeterince koruyup korumadığına dair soruları ortaya çıkarmaktadır. OECD, ortaya koyduğu politika önerilerinin daha önce benzeri görülmemiş öneriler olduğunu iddia etmemekle birlikte, bu alanda henüz belirmeye başlayan önemli ve taze sorunların ancak söz konusu yaklaşımlarla üstesinden gelinebileceğini ifade etmektedir. Zira veriye dayalı yenilikçiliğin dayandığı veri değeri döngüsünün her bir adımının (Şekil 3.2) mahremiyete ilişkin kaygıları artırdığı ifade edilmektedir. Söz konusu kaygılar şu şekilde özetlenmektedir:

i. Kapsamı giderek artan ve bireyin özel alanını azaltarak gelişen bir veri toplama eğilimi,
ii. Kötü niyetli kişilerce veri hırsızlığı yapılması veya verinin yanlış kullanım potansiyeli sonucunda veri ihlalinin olumsuz sonuçlarını artıran büyüklükte verilerin depolanması ve söz konusu büyüklükteki verinin bünyesinde barındırdığı risklerin kolayca öngörülememesi,
iii. Verilerin gömülü olduğu içerik ile organizasyon ve yapısını ortaya çıkaran analizler sayesinde, verinin ilişkili olduğu alanda geniş bilgi elde edilebilmesi ve çıkarımlarda bulunulabilmesi (Zira bu gibi durumların genellikle veri sahibi tarafından bilinçli olarak sağlanan verilerin çok ötesine geçerek, bireyin kontrolünü azalttığı ve bilgi asimetrisi oluşturduğu ifade edilmektedir),
iv. Veriye dayalı kararların bireyler bakımından gerçek dünyada ayrımcı etkilere yol açabilmesi ve diğer zararlar.

Şekil 3.2. Veriye Dayalı Yenilikçilik-Veri Değer Döngüsü



Kaynak: OECD, 2015.

Kişisel verilerin korunması amacıyla sınırlı veri toplama, kriptolama, yeniden tanımlama, bağlantı kurulamayacak işlevsel ayıklama, ayırt edilemez kılmak amacıyla gürültü ekleme ve dezenformasyon gibi çeşitli araçlar kullanılabilmektedir. Nitekim bu araçların temel amacı, koruma tedbiri denince ilk akla gelen kişisel bilgileri saklamak veya gizlemek temeline dayanmaktadır. Bununla birlikte, yeni teknolojilerin her yerde bulunma özelliği, veri analizinde teknolojik ilerlemelerle birleştiğinde, ticari ya da sosyal bağlamda toplanan verilerden, (bireyin kendisi hakkındaki bu veriyi paylaşmasına dahi gerek duymadan) bireyler hakkında çıkarımlar üretmek gittikçe kolaylaşmaktadır.

4.3.3.2. Daha etkin bir mahremiyet koruması için yeni politika yaklaşımı önerileri

Büyük veri gibi veri odaklı yenilikler bağlamında mahremiyet korumasının etkinliğinin artırılması amacıyla çeşitli politika yaklaşımları önerilmektedir. İlk olarak, bireylere şeffaflığın artırılması, verilere erişim ve bireylerin güçlendirilmesi yaklaşımı ön plana çıkmaktadır. İkinci olarak, veri işleyen kuruluşların kişisel verileri daha sorumlu kullanmalarının teşvik edilmesi yaklaşımı tavsiye edilmektedir. Nitekim mahremiyet korumasına hizmet eden teknolojilerde de uzun zamandan beri gelişme

kaydedildiği ifade edilmektedir. Son olarak, risk yönetiminin mahremiyet koruması alanında uygulanması bir başka olası yaklaşım olarak sunulmaktadır.

Burada ifade edilen yaklaşımların hiçbirinin diğerine üstün olamayacağı kabul edildiğinden, birbirini tamamlayıcı biçimde uygulanması önem arz etmektedir. Nitekim, söz konusu yaklaşımların OECD Mahremiyet Rehber İlkelerinde olduğu gibi ülkelerin yürürlükteki mevzuatıyla uyumlu olması gerekmektedir. Ancak bugün, büyük veri gibi yenilikçi uygulamalar nedeniyle veri kullanım ölçeği açısından daha geniş bir çerçeve ortaya çıkmış, bu durum ise birtakım zorluklara sebep olmuştur. Bu çerçevede, OECD Mahremiyet İlkelerine ilişkin revizyon çalışmasına yardımcı olan Uzman Grubu Raporunda rıza, bireyin rolü, amaçla sınırlılık ilkesinin uygulanması ve kişisel veri tanımı üzerinde halen çalışılmaya ihtiyaç bulunduğu ortaya konulmaktadır.

1970'li yıllarda kişisel verilerin veri kontrolörüne, doğrudan veri sahiplerince sağlandığı anlayışın ürünü olan söz konusu Mahremiyet Rehber İlkelerinin bu kapsamda gözden geçirilmeye ihtiyaç duyması şaşırtıcı karşılanmamaktadır. Bugün, bireylerin kendi sağladığı veriden çok daha hızlı büyüyen nesnelerin interneti ve sensör donanımlı akıllı cihazlar sayesinde gözlemlenen veri patlamasına ve bu büyük veri setleri üzerinde (yapılandırılmış veya yapılandırılmamış) analitik çalışabilme kapasitesine odaklanılması gerektiği ifade edilmektedir. Bu çerçevede, kişisel veri kullanım ölçeği, kapsamı ve değeri konusunda böylesi dinamik bir akışın içerisinde, mahremiyet korumasının etkinliğinin artırılması için aşağıda yer alan hususlara dikkat edilmesinin önem arz ettiği ifade edilmektedir:[165]

a) Şeffaflık, veriye erişim ve güçlendirme

Şeffaflığın artırılması, bireyin kişisel verilerine erişimi ve düzeltebilme hakları, ilk kez benimsendikleri 1980'den beri OECD Mahremiyet İlkeleri'nin önemli bir parçası haline gelmiş ve dünyada pek çok ulusal mevzuata dâhil edilmiştir. Söz konusu haklar, veri sahibine, hakkında hangi kararların alındığını tespit edebilme fırsatı sunmasından dolayı ayrımcılık ve profillemeye karşı güçlü mekanizmalar olarak kabul edilmektedir. Bununla birlikte, günümüzde bireyler söz konusu haklarını kullanmayı zor bulmaktadır. Bu kapsamda, bireyler ve veri işleyenler arasındaki bilgi

[165] OECD, 2015: 223-227

asimetrisinin, mevcut teknolojiler ışığında yeniden dengelenmesini amaçlayan bir dizi yeni girişim başlatılmıştır. Bazı ülkelerin, tüketicilere kişisel verilerine (kendi tüketimi ve işlem verileri dâhil) taşınabilir ve elektronik formatta erişmelerini sağlamak üzere çeşitli işletmelerle işbirlikleri kurdukları görülmektedir. Örneğin; ABD'de, 2011 yılında Ulusal Bilim ve Teknoloji Konseyi tarafından Akıllı Bildirim girişimi başlatılmıştır. Girişim kapsamında tüketicilere ürün ve işletmelerle ilgili bilgilerin yanı sıra kendileriyle ilgili kişisel verilere de güvenli, kullanıcı dostu ve taşınabilir elektronik formatta erişebilme hakkı tanınmıştır. Bu alanda önemli bir diğer örnek, Yeşil Düğme girişiminde ise elektrik tüketicilerine enerji kullanım verilerine kullanıcı dostu ve makinalarca okunabilir formatta kolay erişim sağlanması amaçlanmaktadır. Ayrıca, son dönemde veri acentelerinin kendi uygulamaları etrafında şeffaflığı artırma girişimleri de dikkat çekmektedir.

2011 yılında İngiltere hükümeti desteğiyle başlatılan Midata Girişimi kapsamında bireylerin enerji, finans, telekomünikasyon ve perakende sektörlerindeki işlem ve tüketim verilerine kolayca erişmeleri amaçlanmaktadır. Girişim kapsamında geliştirilen programla, işletmelerin tüketim ve işlem verilerini taşınabilir ve tercihen makinalarca okunabilir formatta müşterilerine sunmaları teşvik edilmektedir.

Fransa'da başlatılan FING (Fondation Internet Nouvelle Génération) Girişimi kapsamında, ağ tabanlı bir platform olan MesInfos üzerinden bireylerin işletmeler tarafından tutulan finans, iletişim, sağlık, sigorta ve enerji alanlarındaki verilerine erişmeleri hedeflenmiştir.

Son olarak, AB veri koruma reformu kapsamında yeni Veri Koruma Tüzüğü'nde de yer verilen veri taşınabilirliği hakkıyla, bireylere 'verilerini farklı katma değerli hizmetler sunan üçüncü taraflara iletebilme' hakkı verilmekte ve söz konusu hakkın kişisel verilerin daha verimli ve çeşitlendirilmiş kullanımını sağlayarak yenilikçiliği teşvik edeceği öngörülmektedir. Veri taşınabilirliği hakkı, veri sahiplerinin aktarma maliyetlerini düşürerek veri sorumlularını kolayca değiştirebilmelerine imkân vermekte ve bireylerin kendi verilerine kullanılabilir bir formatta erişerek çıkarları için analiz edebilmelerini mümkün kılmaktadır. Veri taşınabilirliği hakkı, bireylere verinin yenilikçi kullanım alanları konusunda önemli rol

vermiş olmakla kalmamakta, aynı zamanda veri odaklı ürün sağlayıcıları arasındaki rekabetin artmasını da sağlamaktadır.

Yukarıda ifade edilen girişimlerin, bireyleri bilinçli kararlar almaya ve kuruluşları sunmayı amaçladıkları veri yoğun hizmetlerindeki güveni artırmaya teşvik ederek bireylere kişisel verilerinin hukuka uygun işlenmesi konusunda bir denetim imkânı sağlayacağı öngörülmektedir. Bununla birlikte, bu tür girişimlerin gerek gelişmiş veri erişimi mekanizmalarının oluşturulması, gerekse bu alanda çıkarılacak düzenlemelere uyum mekanizmalarının geliştirilmesi ve sürdürülmesi bakımından önemli maliyetler getirebileceği ifade edilmektedir.[166]

Bireylere yönelik şeffaflığın artırılması amacıyla mahremiyet bildirimleri ile desteklenen basit bilgileri sağlayan sadeleştirilmiş bildirimlerin yer aldığı 'çok katmanlı mahremiyet bildirimleri' oluşturma girişimleri de bulunmaktadır. Başka bir örnek, bireylere hizmetin en çok kullanıldığı anda mesaj vermeyi amaçlayan 'zamanında hazır' bildirimleridir. Bu girişimler, bireylere belirli bir sistem içinde gerçekleştirdikleri faaliyetlerin olası sonuçlarını göstermeyi amaçlayan geri bildirim ve farkındalık araçlarının giderek yaygınlaştığını ortaya koymaktadır. Bireylere etkili bir şekilde bilgi sunmak için yeni yolların geliştirilmesinin, yeni teknolojiler karşısında giderek daha karmaşık bir hal alan kişisel veri koruması bulmacasının çözülmesine yardımcı olabileceği öngörülmektedir.

OECD Mahremiyet Rehber İlkeleri içerisinde yer alan açıklık ilkesinde öngörülen şeffaflık anlayışının, bireylerin kişisel verilerine erişimleri ve haklarını doğrudan kullanabilmelerinden çok daha geniş bir amaca hizmet ettiği ifade edilmektedir. Zira söz konusu anlayışın veri işleyenlerin, mahremiyet savunucularının ve tüm kamuoyunun mahremiyet uygulamalarını daha iyi anlamasını ve değerlendirmesini sağlayacağı savunulmaktadır. Nitekim, dijital riskler hakkında daha fazla bilgi sahibi kullanıcılara sahip olan Danimarka, Hollanda ve İsveç gibi ülkelerde veri ihlalleri konusundaki kaygıların daha düşük olduğu, bireylerin söz konusu riskler hakkında daha az bilgi sahibi oldukları Yunanistan, Macaristan, İtalya ve Portekiz gibi ülkelerde ise tam aksine, çevrimiçi bankacılık ve e-ticaret gibi dijital hizmetleri

[166] Fieldfisher, 2012:1

kullanmalarının daha az olduğu, bu kişilerin kişisel bilgilerini internet üzerinden yönetme eğiliminin de daha düşük olduğu ifade edilmektedir. Bu durumun, dijital güvenlik ve mahremiyet riskleri konusunda bilgi sahibi olunması ile mahremiyet ve güvenliğe ilişkin kaygılar arasında negatif bir korelasyon olabileceğini düşündürdüğü ifade edilmektedir.[167]

Bu çerçevede, OECD tarafından güven artırıcı teknolojilerin kullanılması da dâhil olmak üzere, bilgi asimetrilerinin azaltılması, dijital güvenlik ve mahremiyet (risk yönetimi) ile ilgili yetkinliklerin geliştirilmesi konusunda bireylerin ve işletmelerin güçlendirilmesine ilişkin politikalar önerilmektedir.

b) Sorumlu kullanım ve etkili uygulama

Veriyi işleyen ve kullanan işletme ve kuruluşların sorumlu hareket etmelerinin teşvik edilmesinin faydalı bir tamamlayıcı politika olabileceği değerlendirilmektedir. Veri sorumlularının büyük veri analizinin meyvelerini toplamalarının önlenmesine değil, bu alanda sınırların belirlenmesi için daha fazla çabaya ihtiyaç olduğu ifade edilmektedir.

İşletmelerin ve bireylerin sorumluluk sahibi veri kullanımının sınırlarını belirlemenin yolunun, gözden geçirilmiş OECD Mahremiyet İlkelerinin 'tamamlayıcı tedbirler' çağrısında özel olarak tanımlanan, gerek yapılan yaygın hatalar gerekse veri analizinin muhtemel olumsuz etkileri konusunda, eğitim ve farkındalık çalışmalarından geçmekte olduğu savunulmaktadır. Mahremiyet çerçeve ilkeleri, uygulamada en etkili şekilde hayata geçirilmeyi sağlamak için genel üst düzey ilkeler olarak kaleme alınmıştır.

OECD ülkelerindeki politika yapıcıların ve yürütme organlarının, işletmelere uygun sınırları tespit etmek konusunda yardımcı olmaları gerektiği vurgulanmaktadır. Bu çerçevede, örneğin; sigorta firmalarınca genetik bilgilerin kullanılmamasına ilişkin politikalar belirlemek, kredi puanlama rehberleri yayımlamak veya işverenler tarafından sosyal ağ verilerinin kullanılmamasına ilişkin hukuki düzenlemeler yapmak sayılmaktadır.

---

[167] OECD, 2017: 269

OECD Mahremiyet İlkelerinde yer alan hesap verebilirliğe ilişkin yeni hükümlerin yenilikçi teknolojiler dolayısıyla gelişmekte olan kavramlara ve yeni iş konseptlerinin ortaya çıkardığı ihtiyaçlara cevap verdiği ifade edilmektedir. Zira veri işleyen kuruluşların dâhili süreçlerine yapılan sıkı vurgu ve daha güçlü denetimlerin, bu kuruluşların veri işleme riskinin sorumluluğu ve bu riski değerlendirme konusunda daha temkinli davranmalarını sağlayacağı öngörülmektedir. Bu kapsamda, etik bir bakış açısını savunan bazı doktrin görüşleri ise, veri temelli karar verme süreçlerinin veri etiği sorumlusu uzmanların gözetimi altında gerçekleştirilmesi gerektiği fikrini savunmaktadır.[168]

Veri koruma kuruluşları başta olmak üzere veri mahremiyetinin tesisi için çalışan organların, veri işleyenler üzerindeki denetimlerinin etkili olabilmesi için uygulama araçlarının güçlendirilmesi gerekmektedir. Nitekim, gözden geçirilmiş OECD Mahremiyet İlkeleri[169], hükümetlerin yetkilerini yetkili organlarca etkin bir şekilde kullanmaları için kaynak ve teknik uzmanlık ile donatılmaları gerektiğini vurgulamaktadır. Mevcut teknolojik düzlemde kişisel veri kullanımlarını denetlemek gibi büyük bir sorumluluğun büyük bir kaynak ve uzmanlık ihtiyacını da beraberinde getireceği vurgulanmaktadır.

c) Mahremiyet artırıcı teknolojiler

Günümüzde mahremiyeti korumayı amaçlayan, öte taraftan da işlevselliği sürdüren birtakım teknolojiler bulunmaktadır. Söz konusu teknolojiler arasında; mahremiyet koruyucu analizler, farklılaştırılmış mahremiyet veya anonimleştirme sayılabilmektedir. Kimliksizleştirme, genellikle mahremiyet risklerini azaltarak büyük veri analizinden faydalanmayı mümkün kılan pratik yöntem olarak OECD tarafından kabul görmektedir. Bununla birlikte, risklerin tamamen ortadan kaldırılmasının güç olduğu ve yeterli sayıda farklı veri setinin bir araya getirilmesi sonucunda bireyin belirlenebilir kılınabileceği modellerin teknik olarak mümkün olduğu ifade edilmektedir. Nitekim, yeniden kimliklendirme gibi araçların hızla kullanılmasının

[168] Söz konusu yaklaşımın savunucuları için bkz.: Mayer-Schönberger, ve Cukier, K., 2013; Richards ve King, 2014; Johnsonve Henderson-Ross, 2012.
[169] OECD tarafından 2013 yılında gerçekleştirilen güncelleme çalışmasını ifade etmektedir.

mümkün olduğu büyük veri analizinde söz konusu aracın bir politika belirleyicisi olarak etkinliği sorgulanmaktadır.

Yeniden kimliklendirmeye ilişkin riskler, hem veri analizinin gerçekleştirileceği bağlam hem de kimliği yeniden belirlenecek kişilere ilişkin veri kaynakları ve motivasyonla doğrudan ilişkili görülmektedir. Bu kapsamda, yapılacak risk değerlendirmesinde, yeniden kimliklendirmenin gerçekleşmesi durumunda verinin sahibi bakımından oluşacak muhtemel sonuçların dikkate alınması gerekmektedir. Bu çerçevede, yeniden kimliklendirme teknik çözümü ile idari ve yasal önlemleri (örneğin; bireyin yeniden belirlenebilir kılınmaması konusunda alınacak taahhütlere ilişkin düzenlemeler) birleştiren yaklaşımların uygulamaya konulmasının bu alandaki riskleri en aza indirebileceği öngörülmektedir.

Ayrıca, geliştirilen yeni teknik araçlar, bir kuruluşun topladığı kişisel verilerin yaşam döngüsünü kaydedip tanımlayarak kuruluşlara kişisel verilerin yönetiminde yardımcı olabilmekte ve hesap verebilirliği kolaylaştırabilmektedir. Bu kapsamda, gelişmiş veri etiketleme şemaları ile kişisel verilere bağlam ve tercih bilgisi eklenmesi yoluyla kuruluşların gelecekteki veri kullanımlarını yönetebilmesi örnek olarak verilmektedir.

Fonksiyonel ayıklama gibi güvenlik önlemleri, istatistikî veya bilimsel araştırma gibi amaçlarla kullanılan verilerin belirli bir kişiye ilişkin karar alınmasında kullanılamamasının sağlanmasında önemli rol oynayabilmektedir. Söz konusu yöntemin mahremiyete ilişkin sağladığı güvenlik sayesinde toplumsal faydası yüksek önemli çıkarımların ve bilgilerin elde edilmesi mümkün olabilmektedir. Zira politika yapıcıların, büyük veri alanında ortaya çıkan fırsatların değerlendirilmesi adına kamu-özel işbirliklerini teşvik ederek araştırma ve geliştirmeyi teşvik etmeleri gerekmektedir.

Sonuç olarak, ayrımcı etkiler yaratarak bireyleri ve toplumları tehdit eden büyük veri analiz yöntemlerinin yanı sıra bireylere ve toplumlara yönelik ayrımcı uygulamaları tespit eden ve böylece mahremiyet haklarının uygulanmasına ilişkin

değerlendirmeyi yapmaya yardımcı olan analiz yöntemleri de mümkün görülmektedir.[170]

d) Mahremiyet alanında risk yönetimi

Gözden geçirilmiş OECD Mahremiyet İlkelerinde risk yönetimi, özellikle hesap verebilirlik bağlamında mahremiyet koruması için kilit temalardan biri olarak yer almaktadır. Hizmet kullanıcılarına, hissedarlara, çalışanlara ve diğer menfaat sahiplerine göre, kişisel verilerin mahremiyetine ilişkin kaygı ve riskler işletmelerin itibarını, pazardaki gelirlerini ve güven ortamını doğrudan etkileyebilmektedir. Nitekim tüketicilerin, kişisel verilerini koruma konusunda yetersiz kalan işletmelerden hizmet alma konusunda genelde isteksiz oldukları ifade edilmektedir. Bu anlamda kişisel veri ihlallerinin finansal etkilerinin önemli olduğu vurgulanmaktadır. Bir mahremiyet ihlalinin ortaya çıktığı durumda, özellikle hukuki yardım, adli takip, gerekli bildirim mekanizmaları, iyileştirme önlemleri veya hakkında alınan idari, cezai yahut tazminata ilişkin kararlar için ödeme yapacak kaynağa sahip olmayan küçük işletmelerin kendilerini bir anda iş dünyasının dışında bulabilecekleri ifade edilmektedir.[171]

Günümüzde mahremiyetin ekonomik ve sosyal bir risk olarak ele alınması gerektiğinin farkına varılmasına ve pazarda rekabet avantajı sağlayabilecek stratejik bir mesele olarak ele alınması gerekmesine rağmen birçok kuruluş tarafından hâlâ mahremiyet kavramına salt hukuki bir sorumluluk meselesi olarak yaklaşılması eğiliminin olduğu görülmektedir. Birçok KOBİ'nin, mahremiyet korumasının işletmeler için önemli olduğunu fark etse bile, bu konudaki riskleri etkin bir şekilde yönetmek için gerekli kaynak ve uzmanlığa sahip olmadığı görülmektedir. Kaynaklarına sahip oldukları durumlarda da mahremiyet ve güvenlik riski arasındaki farkı anlayamamaktadır. Örneğin; bir işletmenin bireylerin haklarını ihlal edecek bir şekilde kişisel veriyi işlemesi durumunda ortaya çıkan risk mahremiyete ilişkin olup güvenlikle herhangi bir bağlantısı bulunmamaktadır. Zira Kanada Mahremiyet Komiserinin finanse ettiği Kanada'daki ticari uygulamalara ilişkin bir araştırmada da,

---

[170] Executive Office of the President, United States (EOP), "Big data and differential pricing", 2015, (erişim tarihi: 06.09.2016), www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf
[171] OECD, 2017: 279

mahremiyet risk yönetimi konusunun oldukça popüler olduğu, ancak uygulamada gelişme sağlanamadığı bulgusuna erişildiği görülmektedir.[172]

Mahremiyete ilişkin düzenleyici kuralların nasıl uygulanacağı konusunda, özellikle risklerle nasıl başa çıkılacağı ve sorumlulukların tayini konularında örgütsel strateji eksikliğinin bir yansıması olarak hâlâ belirsizlikler olduğu vurgulanmaktadır. Bu görüş, birçok işletmede ve özellikle KOBİ'lerde mahremiyet risklerine yönelik resmi bir politikanın bulunmaması durumuyla tutarlı görünmektedir. OECD ülkelerinde bulunan işletmelerin yalnız yüzde 10 ila 40'ının 2015 yılı itibarıyla resmi bir mahremiyet politikasına sahip olduğu belirtilmektedir. Sonuçta, mahremiyet riskini bir kuruluşun risk yönetim stratejisine entegre etmek, risk türü veya kategorizasyonunu belirlemeyi ve risk yönetim yapısında nerede konumlanması gerektiğini anlamayı gerektirmektedir.[173] Risk yöneticileri genelde mahremiyet korumasını kendi sorumlulukları dâhilinde görmediğinden ve BT yöneticileri de risk yönetimine teknik dijital güvenlik bağlamında yaklaştığından, bu alan belirsizliğini korumaktadır. Veri sorumluları, mahremiyet risk yönetimini doğrudan kendi sorumluluk alanları gibi görmemekte, düzenlemelerle getirilen mahremiyet etki değerlendirmesi gibi mekanizmaları hayata geçirerek üzerlerine düşeni yaptıklarını düşünmektedir. Bu kapsamda, mahremiyet, bir dijital güvenlik meselesi ya da bir uyumluluk sorunu olarak ele alınmaktadır. Dolayısıyla, mahremiyet risk yönetimine genellikle "başkasının sorumluluğu" olarak bakılmaktadır.[174]

Mahremiyet alanında risk yönetimi, kullanım amaçlarının hassasiyeti kadar veri kaynakları ve verinin kalitesini de dikkate almakta; veri ihlallerinin önlenmesinin yanı sıra, veri analiz süreçlerinin incelenerek değerlendirilmesi ile hata ve yanlışlıkların analiz sürecinin neresinde ortaya çıktığının belirlenmesine yardımcı olmaktadır. Rutin ve tutarlı bir şekilde uygulanması basit görünen mahremiyet risk değerlendirmesinin etkili olabilmesi için, muhtemel tüm zarar ve menfaatleri dikkate alacak biçimde geniş ölçekli çalışılması gerekmektedir. Çoğunlukla öznel olan risklerin tanımlanması, şiddetinin belirlenmesi ve sonrasında ortaya çıkaracağı

---

[172] A.g.e.: 281

[173] Greenaway ve ark., "Privacy as a risk management challenge for corporate practice", Ted Rogers School of Management, Ryerson University, Privacy and Cyber Crime Institute, 2012, (erişim tarihi: 10.08.2017), www.ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf

[174] OECD, 2017: 282

muhtemel etkilerin öngörülmesi oldukça zorlu bir görev olarak değerlendirilmektedir. Verilerin yeniden kimliklendirilmesine karşı geliştirilen teknik araçlar (kimliksizleştirme), mahremiyet korumasının tam bir garantisi olamamakla birlikte bu amaçla kullanılabilecek elverişli mekanizmalardan biri olarak öngörülmektedir.[175]

Risk yönetimi odaklı yaklaşım, mahremiyet alanında tamamen yeni bir yaklaşımı ifade etmemektedir. Risk değerlendirmesi yaklaşımı OECD Mahremiyet İlkelerinde yer alan güvenlik önlemleri ilkesiyle örtüşmekte olup veri koruma etki değerlendirmesiyle de yakın bağlantılı bulunmaktadır. Bununla birlikte, kapsamlı bir risk yönetimi yaklaşımının mahremiyet ilkelerinin uygulanmasını ne ölçüde güçlendirebileceği hususunda çalışılmaya devam edilmesi gerektiği ifade edilmektedir.

Dijital güvenlik alanında olduğu gibi, mahremiyet koruması bakımından da başarılı bir risk yönetimi, hem risk kültürünü anlama hem de iyi bir risk yönetimi çerçevesi oluşturmayı gerektirmektedir. Risk yönetimi kültürü, bir varlığın veya çevrenin tehditlere karşı korunmasında belirli bir risk düzeyinin kabul edilmesi gerektiğini kabul ederek faydanın optimizasyonunu gerektirmektedir. Veri mahremiyeti alanında, bireye ilişkin risklere işletmeler ve/veya kuruluşlara ilişkin risklerden bağımsız olarak muamele edilmesi gerekmekte olup bu alanda risk değerlendirmesinin nasıl hayata geçirileceği önemli bir sorun alanı olarak ortaya çıkmaktadır.[176]

Risk yönetimi yaklaşımı, kabul edilebilir risk düzeyini belirlemeyi ve riski buna göre tam bir risk değerlendirmesi temelinde ele almayı gerektirmektedir. Veri mahremiyeti bakımından ise, kabul edilebilir risk seviyesinin nasıl tanımlanacağı ve sorumlulukların nasıl paylaşılacağı gibi karmaşık soruların cevaplanması gerekmektedir. Ayrıca, farkındalık, beceri, sorumluluk ve işbirliğinin önemli rol oynadığı; faaliyetlerin ve çevrenin dinamik doğasını dikkate alarak değerlendirmenin ve çözüm sunmanın süreklilik arz ettiği risk yönetimi çerçevesinde, tam ve devam eden bir risk yönetim döngüsünün oluşturulması gerekmektedir. Ek olarak, işletmenin/kuruluşun risklerinin bireyin risklerinden ayrı tutulması gerekmektedir.

---

[175] OECD, 2015: 358
[176] A.g.e.: 226

Riske dayalı yaklaşımların uygulanmasının iç süreçlerde geçerliliğini sağlamak üzere, bazı durumlarda üçüncü taraf akreditasyonları faydalı bir yol olabilmektedir. Sonuç olarak, bu yaklaşımın mevcut mahremiyet koruma ilkelerini destekler biçimde uygulanabilmesi için daha fazla çalışmaya ihtiyaç bulunduğu ifade edilmektedir.[177]

e) *Güvenlik ve mahremiyete ilişkin beceriler ve yetkinliklerin geliştirilmesi ve bu alandaki talebin karşılanması*

Mahremiyet risklerinin artan önemi ve görünürlüğü, bu alanda çalışan uzmanlar için yeni iş imkânlarını artırmaktadır. Aynı doğrultuda, mahremiyet uzmanlığına olan talep de son yıllarda hızla artmakta, bu alanda kapasitesini güçlendirmek isteyen kuruluşların gerekli beceri ve uzmanlığa sahip profesyonelleri istihdam etme ihtiyacı belirginleşmektedir.

Mahremiyet profesyonelleri alanında gerekli işgücünün temini amacıyla, üye sayısı bakımından bu alandaki en büyük küresel yapılanma olan Uluslararası Mahremiyet Uzmanları Birliği'nin (International Association of Privacy Professionals-IAPP) değerlendirilebileceği ifade edilmektedir. Dünyanın yaklaşık 90 ülkesinden 2012 yılında 10 bin üyesi bulunan birliğin üye sayısı 2016 yılında 26 binin üzerine çıkmıştır. Veri koruma görevlisi bulundurma zorunluluğu öngören hukukî düzenlemelerin de içinde bulunduğu son gelişmeler, bu alanda işgücünün geliştirilmesi ihtiyacını ortaya çıkarmaktadır.

AB Veri Koruma Tüzüğü'nün uygulama alanına giren işletmelerin veri koruma uzmanları konusunda artan talepleri de bu alandaki ihtiyacı ortaya koymaktadır. Bu Tüzük dolayısıyla ortaya çıkan ihtiyaca binaen, özellikle veri kontrolörlerine bir veri koruma görevlisi belirleme zorunluluğunun getirildiği durumlarda, önümüzdeki yıllarda yaklaşık 30 bin ila 75 bin yeni pozisyon oluşturulacağı tahmin edilmektedir.[178] Ayrıca, bu alandaki profesyonellere ilişkin talebi artıran politika ve düzenlemelerin AB ile sınırlı olmadığı; Kanada, Güney Kore ve ABD gibi ülkelerin de bu eğilimde olduğu görülmektedir.

---

[177] A.g.e.: 227
[178] Ashford, 2016: 1

İşletmelerin ve kuruluşların, denetimler ve veri envanterleri de dâhil olmak üzere politika geliştirme, eğitim, belgelendirme ve iletişim gibi mahremiyete ilişkin yatırımlarını önemli ölçüde artırdığı ifade edilmektedir. Bu alandaki yatırımların giderek artacağı öngörülmektedir. Örneğin; IAPP tarafından 2016 yılında yapılan araştırmaya göre; 2015 yılında ankete katılan tüm kuruluşların toplamda 277 bin ABD doları olan mahremiyete ilişkin ortalama yatırımlarının, yaklaşık yüzde 50 artarak 2016 yılında 415 bin ABD dolarına ulaştığı ifade edilmektedir. Kuruluş başına ortalama 1,7 milyon ABD doları tutarındaki yatırımın yüzde 35'i mahremiyet sorumlusu ekibin profesyonellerinin maaşlarına, yüzde 27'si ekip tarafından kullanılan harici kaynaklara, geri kalan yüzde 38'lik kısım ise kuruluşta çalışan diğer personele ödeme olarak ayrılmaktadır. Ayrıca, büyük kuruluşların daha büyük mahremiyet bütçesine sahip olma eğiliminde oldukları ve küçük işletmelerden farklı olarak temel mahremiyet çekirdek ekibi dışında da bu alana yatırım yapma isteğinde oldukları görülmektedir.[179]

Dünyada pek çok kuruluşun bu alandaki profesyonellerde yetkinlik geliştirmek için program, etkinlik ve eğitimler düzenlediği görülmektedir. Bu kuruluşlara örnek olarak; IAPP, Mahremiyet Görevlileri Ağı (Privacy Officers Network), Fransa'da bulunan Kişisel Verilerin Korunması Muhabirleri Derneği (Association Française des Dorrespondants à la Pprotection des Données à Caractère Personnel) ve İspanya'da bulunan Mahremiyet Profesyonelleri Derneği (Asociación Profesional Española de Privacidad) verilebilmektedir.[180]

[179] OECD, 2017: 278
[180] A.g.e.: 278

5. TÜRKİYE'DE VERİ MAHREMİYETİ

5.1. Türk Hukuku Bakımından Kişisel Verilerin Korunmasına İlişkin Düzenlemeler

5.1.1. Türkiye'de kişisel verilerin korunması ile ilgili ulusal politikalar

Sekizinci Kalkınma Planı (2001-2005) Dönemi: Türkiye'de veri koruma hukuku bilgi ve iletişim teknolojilerinin gelişimiyle gündeme gelmiştir. İlk kez Sekizinci Kalkınma Planında (2001-2005) kişilik haklarının korunmasına ilişkin olarak bir hedef belirlenmiştir.[181] Bu Plan döneminde, 58'inci Hükümet tarafından hazırlanan 2003 Acil Eylem Planı'nda yer verilen *e-Dönüşüm Türkiye (e-DTr) Projesi* kapsamında DPT Bilgi Toplumu Dairesi koordinasyonunda yürütülen üç eylem planı ile kişisel verilerin korunmasına ilişkin yasal düzenleme gereksinimi ifade edilmiştir.[182] 2003-2004 Kısa Dönem Eylem Planındaki (KDEP) 73 eylemden ikisi kişisel verilerin korunmasıyla ilgilidir. Bu Eylem Planı ile Adalet Bakanlığı'na Kişisel Verilerin Korunması Kanunu'nun çıkarılması sorumluluğu verilmiştir.[183] 2005 yılı Eylem Plan'nda sağlık kayıtlarının mahremiyetinin korunması eylemine yer verilmiştir.

Dokuzuncu Kalkınma Planı (2007-2013)Dönemi: Bilgi toplumuna dönüşüm vizyonuna sahip olan Dokuzuncu Kalkınma Planı (2007-2013), kişisel verilerin korunmasına ilişkin politika özelinde e-devlet hizmetlerinin gerektirdiği kurumlar arası bilgi paylaşımında, kişisel bilgilerin mahremiyeti ilkesinin gözetilmesi esasını benimsemektedir. Söz konusu Plan döneminde hazırlanan Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010) kapsamında Kişisel Verilerin Korunması Kanunu Tasarısı Taslağının yasalaşması ve Bilgi Güvenliği Kanunu ihtiyacı ifade edilmiştir.[184]

Onuncu Kalkınma Planında (2014-2018) Dönemi: Onuncu Kalkınma Planında, kişisel verilerin korunması, ulusal bilgi güvenliği ve elektronik ticaret alanındaki düzenlemelerin tamamlanması ihtiyacının önemi ifade edilerek, bu alandaki hukuki altyapının tamamlanması hedefi belirlenmiştir.[185] Bu Plan dönemine

---

[181] DPT, 2001: 195
[182] Yüksel Civelek, 2011: 124
[183] Yüksel Civelek, 2011: 125
[184] DPT, 2006: 3
[185] Kalkınma Bakanlığı, 2014: 98

ait programlardan 2015 Yılı Programında yer alan 303 numaralı "Kişisel verilerin korunmasına yönelik yasal düzenleme yapılacaktır." tedbiri aynı yıl hayata geçirilerek tamamlanmıştır.[186] Aynı plan hedefi kapsamında 2015 Yılı Programında 304 numaralı eylemde yer alan "Avrupa Konseyinin kişisel verilerin korunmasına ilişkin 108 ve 181 sayılı sözleşmelerinin onaylanması çalışmaları başlatılacaktır." tedbiri ise 2016 Yılı programında da 355 tedbir numarasıyla yer almış olup aynı yıl içerisinde tamamlanmıştır.[187]

Bu dönemde, Büyüme ve istihdam odağında ve sekiz ana eksende hazırlanan 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı'nda (BTS) ise "Bilgi Güvenliği ve Kullanıcı Güveni" eksenine yer verilmiştir. Bu kapsamında, BİT'in daha yaygın ve güvenli kullanımını temin edebilmek amacıyla bilgi güvenliği, kişisel verilerin korunması, bilişim suçlarıyla mücadele ve güvenli internet alanlarında ulusal bir strateji geliştirilmesi hedeflenmiştir.[188] Nesnelerin interneti, büyük veri, mobil teknolojiler, yakınsama, bulut bilişim ve dış kaynak kullanımı gibi teknolojik gelişme ve eğilimlerin de etkisiyle BİT güvenliği ve kullanıcı güveninin sağlanmasının giderek zorlaştığı ifade edilerek hizmetlerin kesintisiz ve kaliteli sunumu ile hizmetten faydalananların veri mahremiyetinin temini için ülkelerin güçlü bir hukuki, kurumsal ve teknik altyapıya sahip olmalarının önemi vurgulanmıştır.[189] Bu amaçla BTS (2015-2018)'de 38 no'lu "Kişisel Verilerin Korunması Mevzuatının Çıkarılması" eylemi yer almıştır.[190]

5.1.2. Türkiye'de kişisel verilerin koruması ile ilgili mevzuat

5.1.2.1. Anayasa'da kişisel verilerin korunması

Kişisel verilerin korunması konusunun tartışılmaya başlandığı 1970'li yıllardan bu yana mahremiyet hakkı ve kişisel verilerin korunması kavramları, anayasalar ile güvence altına alınan özel hayatın gizliliğinin korunması hakkının uzantıları olarak değerlendirilmiştir.[191]

---

[186] Kalkınma Bakanlığı, 2015: 220
[187] Kalkınma Bakanlığı, 2016: 239
[188] Kalkınma Bakanlığı, 2015: 29
[189] Kalkınma Bakanlığı, 2015: 29
[190] Kalkınma Bakanlığı, 2015:119-120
[191] Yüksel Civelek, 2011: 140-141

Türkiye'de kişisel verilerin korunması temel hakkının doğrudan Anayasa'da tanımlanmasından önce de, bu hakkın temelini oluşturacak çeşitli hükümler mevcut bulunmaktaydı. Söz konusu düzenlemelerin arasında doğrudan kişisel verilerle ilişkili bulunan bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı (m.17) ile özel hayatın gizliliği hakkı (m.20) olduğu gibi, hukuk devleti ilkesi (m.2), konut dokunulmazlığı (m.21), haberleşmenin gizliliği (m.22), dini ve vicdani kanaatleri açıklamaya zorlanamama (m.24) ile düşünce ve kanaatleri açıklamaya zorlanamama (m.25) gibi kişisel verilerin korunmasıyla dolaylı olarak ilgili bulunan anayasal haklar da yer almaktadır.

2010 yılında yapılan değişiklikle Anayasa'nın 20'nci maddesine aşağıdaki hüküm ikinci fıkra olarak eklenmiştir:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

5.1.2.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu

2000'li yılların başından itibaren üzerinde çalışılmaya başlanan, Adalet Bakanlığınca hazırlanan ve uzun süre Adalet Bakanlığı, Başbakanlık ve TBMM arasında sürüncemede kalan Kişisel Verilerin Korunması Kanunu Tasarısı, müteaddit kez kadük kalmış, nihayet 24/03/2016 tarihinde TBMM Genel Kurulu'nda kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu" 07/04/2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Söz konusu Kanun ile kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin koruması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi amaçlanmaktadır. Kanun'un uygulanmasından Kişisel Verileri Korunma Kurumu sorumludur.

Kanun yedi bölümden oluşmaktadır: *Birinci Bölümde;* Kanun'un amaç ve kapsamı belirlenmekte ve Kanun'da kullanılan teknik terimlerin tanımları yapılmaktadır. *İkinci Bölümde;* kişisel verilerin işlenmesi konusundaki temel ilkeler,

verinin ve özel nitelikli verinin işlenme şartları, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi ile kişisel verilerin üçüncü kişilere ve yurtdışına aktarılması konuları düzenlenmektedir. *Üçüncü Bölümde;* veri sorumlusunun yükümlülükleri, ilgililerin hakları ve veri güvenliğine ilişkin yükümlülükler düzenlenmektedir. *Dördüncü Bölümde;* başvuru ve şikâyet mekanizmalarına ilişkin detaylar ile veri sorumluları siciline yer verilmektedir. *Beşinci Bölümde;* kişisel verilere ilişkin suçlar ve kabahatler yer almaktadır. *Altıncı Bölümde;* idari ve mali özerkliğe sahip bağımsız Kişisel Verileri Koruma Kurumu ve teşkilatlanmasına ilişkin hükümler bulunmaktadır. *Yedinci Bölümde;* Kanun'un uygulanmasına ilişkin genel istisnalara yer verilmiş olup Kişisel Verileri Koruma Kurumunun bütçesi ve gelirleri ile kanunun yürürlüğüne ilişkin hükümler de bu bölümde yer almaktadır.

Kanun'un yürürlüğe girmesiyle BİT sektörünün başta AB ülkeleri olmak üzere yurt dışına bilgi toplumu hizmetleri sunabilmesi, kişisel verinin temel girdi olduğu finans, sağlık, sigortacılık gibi sektörlerde Türkiye'nin iş potansiyelinin artması ve sınır ötesi veri paylaşımı ve adli işbirliği kanallarının etkin çalışmasının sağlanması öngörülmüştür. Kanun'la, AB ülkeleri nezdinde veri koruma bakımından güvenilir ülke statüsüne kavuşulması konusunda önemli bir kriter karşılanmış bulunmaktadır. Söz konusu Kanun ile bağımsız ve özerk bir Veri Koruma Otoritesi kurulmuş olup akabinde ikincil mevzuat düzenlemelerinin hazırlanması öngörülmüştür.

5.1.2.2.1. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Kapsamı

Kanun'un kapsam maddesinde belirtildiği üzere, söz konusu düzenlemelerin uygulanması bakımından kamu ve özel sektör ayrımı yapılmamış olup düzenlenen usul ve esaslar her ikisi bakımından da uygulama alanı bulmaktadır. Veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek, ayrıca verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin korunması hakkının kapsamına bakıldığında, hem kapsam maddesi olan 2'nci madde hem de kişisel verinin tanımlandığı 3'üncü maddeden, yalnızca gerçek kişilerle ilişkili verilerin Kanun kapsamında korunduğu anlaşılmaktadır. Söz konusu yaklaşım hem 95/46/EC sayılı AB Direktifi hem de

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

5.1.2.2.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki Temel Kavramlar

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

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

kişisel verilerin işlenmesi, verinin ilk defa elde edilmesinden başlayıp veri üzerinde gerçekleştirilen her türlü faaliyet ve işlemi ifade etmektedir.

iii. *Veri kayıt sistemi:* Bu sistemle kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi kastedilmektedir. Kanunun gerekçesinde de belirtildiği üzere veri kayıt sistemleri gerek elektronik gerekse fiziki ortamda oluşturulabilmektedir.

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

Veri sorumlusu bir veya birkaç gerçek kişi olabileceği gibi şirketler, kamu kurum/kuruluşları veya sivil toplum kuruluşları gibi tüzel kişiler de olabilmektedir.

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

6698 sayılı Kanun'un 18'inci maddesinin ikinci fıkrasında veri sorumlusu ve veri işleyen açısından farklı bir sorumluluk düzeyi belirlenerek idari cezaların uygulaması bakımından yalnızca veri sorumlularına yaptırım uygulanmaktadır. Yine veri sorumluları siciline kaydın yalnız veri sorumluları bakımından gerekli olduğu görülmektedir.

vi. *Açık Rıza:* Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade edilmektedir. Bu çerçevede, söz konusu kavram, ilgili kişinin kendisiyle ilgili verilerin işlenmesine, özgür iradesiyle, konuyla ilgili

yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak vermiş olduğu rıza beyanını ifade etmektedir. Kanunda yer alan birçok hükümde kişisel verilerin toplanması, işlenmesi ve saklanması bakımından kişinin rızasının alınması gerekmekte, başka bir anlatımla veri işleme faaliyetleri bakımından ilgilinin rızası hukuka uygunluk sebebi mahiyetinde bulunmaktadır. Dolayısıyla veri sorumluları bakımından, alınacak rızanın 'açık rıza' tanımıyla uyumluluk arz etmesi elzemdir.

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

Bununla birlikte, bilhassa veri işleme ve analizi konusundaki teknolojik gelişmeler dikkate alındığında, büyük veri uygulamaları, nesnelerin interneti, bulut bilişim vb., kişisel verilerin tamamıyla kişiyi belirlenebilir kılma özelliğinden sıyrılmasının, 6698 sayılı Kanun bağlamında anonimleştirilebilmesinin, giderek zorlaştığı hatta imkânsız hale geldiği değerlendirilmektedir. Giderek gelişen ve değişen söz konusu teknolojilerin izlemekte olduğu mevcut eğilim her türlü veri ile kişi arasındaki bağın kurulmasını hızla kolaylaştırmaktadır. TBMM Komisyon Raporlarında da yer alan söz konusu durum karşısında kişisel veri koruma kurallarının uygulanması konusundaki tekniğe ilişkin sorunların uzun bir süre güncelliğini koruyacağı değerlendirilmektedir.

5.1.2.2.3. 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki Temel İlkeler

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

- Hukuka ve dürüstlük kurallarına uygun olma: Kişisel verilerin korunması hukukunun temel ilkesi olarak değerlendirilen, diğer ilkeleri de kapsayan ve onlara kaynaklık ettiği ifade edilen[192] hukuka ve dürüstlük kurallarına uygun olma ilkesiyle, kişisel verilerin işlenmesinde kanunlara ve diğer hukuki düzenlemelere uygun hareket edilmesi gerektiği ifade edilmektedir.
- Doğru ve gerektiğinde güncel olma: Veri sorumlularınca işlenen kişisel verilerin doğru olması, gerek ilgili kişi gerekse veri işleyen bakımından oldukça önemli olup verilerin doğruluğu hususunda veri sorumlusuna bir sorumluluk yüklenmektedir. Ayrıca, verilerin güncelliğinin sağlanması bakımından veri sahibi ile birlikte hareket etmesi beklenmektedir.
- Belirli, açık ve meşru amaçlar için işlenme: Kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi ilkesiyle, veri sorumlusunun kişisel verileri işleme amacını açık ve kesin olarak belirlemesi ve söz konusu amacın meşru olması amaçlanmaktadır. Amacın meşru olması, veri sorumlusunun işlediği verilerin yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma: Veri sorumlularının kişisel verileri toplamadan önce amaçlarıyla bağlantılı olarak verileri mutlaka kullanıp kullanmaması gerektiğini araştırması, söz konusu kişisel verilerden amacına ulaşmak için yeterli miktarını toplaması ve işlemesi, gereğinden fazla veri toplamaması ve işlememesi gerektiği kuralını ifade etmektedir. Bu çerçevede, belirlenen amacı gerçekleştirmeye elverişli olmayan kişisel verilerin işlenmemesi gerektiği ifade edilmektedir. Ayrıca, kişisel verilerin sonradan ortaya çıkması muhtemel ihtiyaçların karşılanması amacıyla işlenebilmesi için, işlemeye ilk kez

[192] KÜZECİ, 2010: 212

başlanıyormuş gibi, 5'inci maddede yer alan işlenme şartlarından birinin gerçekleşmesi gerekmektedir.

- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme: Kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiğini ifade eden ilkedir.

Tablo 5.1. Kişisel Verileri Koruma İlkeleri Bakımından 6698 sayılı Kanun ile AB Genel Veri Koruma Tüzüğü'nün Karşılaştırılması

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

Tablo 4.1.'de görüldüğü üzere temel özellikleri itibarıyla örtüşen 6698 sayılı Kanun'daki temel ilkelerle AB Genel Veri Koruma Tüzüğü'nde yer alan ilkeler kişisel verilerin işlenmesi alanındaki teknolojik gelişmelerle uyumlu esneklikte kaleme alınmıştır. AB Genel Veri Koruma Tüzüğü ile, söz konusu ilkelerin uygulanmasından sorumlu olan süjenin açıkça belirlenmesi kaydıyla veri kontrolörünün hesap verebilirliği artırılmıştır. AB Genel Veri Koruma Tüzüğü'nün temel yaklaşımında yer alan artırılmış kişisel veri koruması eğilimine paralel olarak, Tüzük'te yer alan ilkelerin uygulanmasından sorumlu olan veri kontrolörü doğrudan temel ilkeler başlıklı 5'inci maddede düzenlenirken 6698 sayılı Kanun'da ise doğrudan genel ilkeler başlıklı 4'üncü maddede böyle bir yaklaşım yer almamakta, ancak 12'nci maddede veri sorumlusunun yükümlü olduğuna ilişkin düzenleme yer almaktadır.

5.1.2.2.4. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun AB Reformunun Getirdiği Yenilikler Bağlamında Değerlendirilmesi

Türk hukukunda kişisel verilere ilişkin anayasal düzenlemelerde ve 6698 sayılı Kanunu'nda AB hukukunun mehaz teşkil ettiği bilinmektedir. 6698 sayılı Kanun'da doğrudan 95/46/EC sayılı Direktif hükümlerinin yer aldığı görülmektedir. Bu doğrultuda, mer'i hukuk düzenlemelerine kaynaklık eden AB güncel düzenlemelerinin uygulanmakta olan 6698 sayılı Kanun bağlamında kısaca değerlendirilmesi faydalı görülmektedir.

a) Veri İşleyen Tarafların Sorumluluğu

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

Yukarıda ifade edildiği üzere, AB Genel Veri Koruma Tüzüğü veri koruma hukukundan doğan sorumluluk bağlamında veri kontrolörü ve veri işleyen ayrımını ortadan kaldırarak kişisel veri ihlallerine ilişkin durumlarda hem veri kontrolörünün hem de veri işleyicisinin sorumlu olduğunu hüküm altına almaktadır. Ancak 6698 sayılı Kanun'un 18'inci maddesinin ikinci fıkrasında veri sorumlusu ve veri işleyen açısından farklı bir sorumluluk düzeyi belirlenerek idari cezaların uygulaması bakımından yalnızca veri sorumlularına yaptırım uygulanmaktadır. Veri işleyenlerin

sorumlulukları noktasında benimsenen bu yaklaşım AB Veri Koruma Tüzüğü'nde benimsenen geniş sorumluluk alanı yaklaşımıyla farklılık arz etmektedir.

b) Unutulma Hakkı

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

AB Veri Koruma Tüzüğü kapsamında kabul edilen unutulma hakkına benzer bir hak, münferit olarak 6698 sayılı Kanunda yer almamaktadır. Bununla birlikte, Tüzük'te yer alan unutulma hakkına benzer bir kavram ilk kez Yargıtay 4. Hukuk Dairesi'nin 03.07.2013 tarih ve 2013/6256 esaslı kararında tartışılmıştır.[193] Unutulma

[193] Akgül, 2015

hakkı kavramının ilk kez açıkça yer aldığı yargı kararı ise Anayasa Mahkemesi (AYM) tarafından 2016 yılında verilmiştir. AYM'nin 03/03/2016 tarih ve B.2013/5653 no'lu kararı kapsamında, hakkındaki haberin internet ortamından silinmesi amacıyla başvuran kişi haklı bulunmuştur. Karar kapsamında *"Bireyin kişisel şeref ve itibarı, Anayasa'nın 17'nci maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devlet, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfi olarak müdahale etmemek ve üçüncü kişilerin saldırılarını önlemekle yükümlüdür."* ifadesine yer verilmiştir. AYM, internet ortamının sağladığı kolaylıklar gözetildiğinde başvuranın şeref ve itibarının korunması için söz konusu habere erişimin engellenmesi gerektiğine karar vermiştir.[194] AYM'nin söz konusu kararı Türk hukuku bakımından unutulma hakkının uygulaması bağlamında emsal niteliğindedir.

c) Yaptırımlar

AB Veri Koruma Tüzüğü ile getirilen en önemli düzenlemelerin başında veri ihlalleri karşısında öngörülen yaptırımlara ilişkin hükümler gelmektedir. Zira veri koruma kurallarına ilişkin ihlaller karşısında 95/46/EC sayılı Direktif'e göre çok daha ağır tazmin yaptırımları (20 milyon avro veya hizmet sağlayıcının küresel gelirinin yüzde dördü gibi önemli miktarlar) öngörülmektedir. 6698 sayılı Kanun'da ise söz konusu idari para cezalarının daha düşük miktarlarla sınırlı olduğu (en düşük 5 bin Türk Lirasından en yüksek 1 milyon Türk Lirasına kadar) görülmektedir.

d) Veri Taşınabilirliği ve Veri Koruma Etki Değerlendirmesi

AB Veri Koruma Tüzüğü'nün 20'nci maddesiyle ilk kez tanımlanan "*veri taşınabilirliği hakkı"* kapsamında veri sahibi, kişisel verisini, bu veriyi tutmaya yetkili bir veri kontrolöründen diğerine taşıyabilme yetkisine sahiptir. Ayrıca, 37'nci madde kapsamında hassas verilerin işlenmesi bakımından "*veri koruma görevlisi"*nin belirlenmesi ve 35'inci madde kapsamında riskli veri işleme faaliyetleri bakımından *"zorunlu veri koruma etki değerlendirmesi"* öngörülmektedir. 6698 sayılı Kanun'da ise bu kapsamda ayrıca tanımlanmış hükümler bulunmamaktadır.

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

e) Veri Koruma tedbirleri

AB Veri Koruma Tüzüğü kapsamında kişisel verilerin işlenmesi bağlamında gerçek kişilerin hak ve özgürlüklerinin korunması amacıyla gerekli teknik ve organizasyonel önlemlerin alınması gerektiği ifade edilerek "*varsayılan veri koruması" ve "tasarımdan itibaren veri koruması"* yaklaşımlarına yer verilmektedir. Bilhassa teknolojik gelişmeler dikkate alındığında bu yaklaşımların, 6698 sayılı Kanun'da doğrudan yer almasa dahi özellikle Kişisel Verileri Koruma Kurulunca hayata geçirilecek ikincil düzenlemelerde dikkate alınması önem arz etmektedir.

5.1.2.3. Kişisel verilerin korunmasına ilişkin diğer düzenlemeler

6698 sayılı Kanun'un kabulünden önce kişisel verilere ilişkin düzenlemeler çoğunlukla ilgili oldukları sektör ve kuruluşların uygulamalarına yön vermek üzere çeşitli kanunlarda dağınık halde bulunmaktaydı. Anayasa'da yer alan 20'nci madde hükmünün çerçeveyi oluşturduğu bu kanunlar hem özel hukukta hem de kamu hukukunda yer almakta idi. Söz konusu kanun ve yönetmelikler, 6698 sayılı Kanun'a uyum bakış açısıyla kapsamlı bir gözden geçirme süreci gerçekleşmemiş olup, aşağıdaki gibi listelenebilir:

Türk Medeni Kanunu, Türk Ceza Kanunu, Ceza Muhakemesi Kanunu, Vergi Usul Kanunu, İş Kanunu, Elektronik Haberleşme Kanunu, Bilgi Edinme Kanunu, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Elektronik İmza Kanunu, Nüfus Hizmetleri Kanunu, Polis Vazife ve Salahiyet Kanunu, Jandarma Teşkilat, Görev ve Yetkileri Hakkında Kanun, Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik, Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

5.2. Türkiye'de Büyük Veri Uygulamalarının Veri Mahremiyeti Düzenlemelerine Etkileri

Türkiye'de veri koruma hukuku alanında temel düzenleme sayılan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun büyük verinin getirdiği değişim bağlamında değerlendirilmesine ihtiyaç bulunmaktadır. Kanun'un büyük verinin getirmekte olduğu riskler ile sosyal ve ekonomik faydayı dikkate alır mahiyette bulunup bulunmadığı bakış açısıyla ve büyük veriye ilişkin müesseseler bağlamında yapılan değerlendirmeler aşağıda yer almaktadır.

5.2.1. Kişisel veri tanımı ve verinin işlenmesi bakımından değerlendirme

Kanun'un 3'üncü maddesine göre, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" kişisel veri olarak kabul edilirken, 6'ncı maddeye göre "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"nin özel nitelikli kişisel veri olduğu ifade edilmektedir. Bu iki hükme göre mevzuatta kişisel veri kavramının çok geniş bir uygulama alanına sahip olduğu görülmektedir. Bu tanıma giren bütün veriler, öngörülen korumadan faydalanmakta ve ancak Kanun'da öngörülen hallerde işlenebilmektedir. Kanun koyucu, söz konusu mutlak hakkın derecesine göre bir ayrıma giderek "basit" kişisel verilerin işlenme şartlarıyla, "hassas" kişisel verilerin işlenme şartlarını ayrı ayrı düzenlemekte, özel nitelikli kişisel veriler bakımından daha sıkı şartlar aramaktadır. Ancak, yukarıda da ifade edildiği üzere, büyük veri setlerinin kullanılmasıyla alelade verilerden hassas kişisel verilere erişilebilmesi, hatta kişisel olmayan verilerden kişiyi belirlenebilir kılan verilerin kolayca elde edilmesi mümkün olmaktadır.

Büyük verinin karakteristik özelliklerinden biri verilerin çokluğudur. Büyük hacimli veri setleri sayesinde yeni ve faydalı sonuçların elde edilmesi mümkün olmaktadır. Bu bağlamda, büyük veride olabildiğince fazla verinin toplanması ve işlenmesi kural iken, 6698 sayılı Kanun ile getirilen temel kural kişisel verilerin işlenmemesidir. Kanuna göre kişisel veriler ancak kişinin rızası ya da bir hukuka uygunluk sebebinin bulunması (örneğin; bu alanda belirlenmiş başka bir kanun,

uluslararası sözleşmelerden doğan bir yükümlülük gibi) durumunda işlenebilmektedir. Kanun'un kişisel verilerin işlenmesini kural olarak yasaklamasının uygulamada veri işleyen kuruluşları kanunla getirilen istisna hükümlerinden yararlanmayı bir çıkış noktası olarak görmeye itebileceği değerlendirilmektedir. 5'inci maddenin ikinci fıkrasının (b) ve (c) bentlerinde düzenlenen, rıza aranmaksızın kişisel verilerin işlenebileceği istisnai haller bu bağlamda ele alınabilir. Hükme göre "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" ve "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hallerinde rıza aranmaksızın kişisel verilerin işlenebileceği düzenlenmektedir.

Kanun'un 11'inci maddesi gereğince herkes, ilgili veri sorumlusuna başvurarak kendisiyle alakalı kişisel verilerin işlenip işlenmediği konusunda bilgi alma hakkına sahiptir. Bireyler, işlenme amaçlarını, verilerin bu amaca uygun şekilde işlenip işlenmediğini, verilerin üçüncü kişilere aktarılıp aktarılmadığını sorma ve bunların düzeltilmesini talep etme hakkına sahiptir. Maddenin (g) bendinde işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması halinde bireye itiraz hakkı tanınmakta, (ğ) bendinde ise, kanuna aykırı olarak işlenen kişisel veriler sebebiyle zarar meydana geldiğinde zararın giderilmesi talep edilebilmektedir. Ancak, bu maddeyle getirilen otomatik sistemler vasıtasıyla analiz suretiyle ortaya çıkacak aleyhe sonuçtan bireyin nasıl haberdar olacağı ve buna itiraz edeceği hususu belirsiz bulunmaktadır. Ayrıca, ilgililerin veri sorumlusuna başvuru ve Kurul'a şikâyet haklarını düzenleyen 13 ve 14'üncü madde hükümlerine göre taleplerin yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle iletileceği düzenlenmektedir. Söz konusu hükümlerin veri sorumlularının şeffaflığını ön plana çıkarmaktan ziyade, verisi işlenen ilgililerin tam bir farkındalık içerisinde bulunduğu kabulüyle kaleme alındığı görülmektedir. Ancak, çoğunlukla büyük veri uygulamaları bakımından veri sahiplerinde bu düzeyde bir farkındalığın mevcut olmasının teknik olarak mümkün olmadığı değerlendirilmektedir. Ayrıca, Kanun ile getirilen koruma ve tazminat müesseseleri ihlal ortaya çıkıp zarar oluşmadan ilgilinin müdahalesine imkân vermemektedir. İlgili

ancak sonradan telafi mekanizmalarını işletebilmektedir. Büyük veri gibi birey hakkında kapsamı ve sonuçları öngörülmesi güç veri işleme faaliyetleri bakımından ilgili hükümlerin yetersiz kalacağı değerlendirilmektedir. İlgilinin süreçlere aktif katılımını sağlayan ve teşvik eden mekanizmaların öngörülmesi gerekmektedir.

Son olarak, 6698 sayılı Kanun'da yer alan veri siciline kaydı düzenleyen 16'ıncı maddede yer alan bildirime ilişkin hükümde büyük kapsamlı veri işleme faaliyetleri bakımından farklı bir düzenlemeye gidilmediği görülmektedir. Eski AB düzenlemesi 95/46/EC sayılı Direktif'in getirdiği veri siciline kayıt ve bildirime ilişkin genel hükmün, pek çok idari ve mali yük getirirken kişisel verilerin korunması konusunda köklü bir çözümü sağlamadığı ifade edilmektedir. Bu çerçevede, ayrım gözetmeksizin tanımlanan bu genel bildirim yükümlülüğü yerine yeni Tüzük büyük ve riskli veri işleme faaliyetleri bakımından yeni bir yaklaşım ortaya koymaktadır. 6698 sayılı Kanun'da ise bu amaca hizmet eden bir hüküm bulunmamaktadır.

5.2.2. İlgilinin açık rızası, amaçla sınırlılık ve sınırlı veri işleme ilkeleri bakımından değerlendirme

Kanun açık rızayı "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" olarak tanımlamaktadır. Kanunun uygulanması bakımından rıza, verilerin işlenmesinde temel hukukî gereklilik olarak vücut bulmaktadır. Ayrıca, kişisel verilerin aktarımını düzenleyen 8'inci madde ile kişisel verilerin yurtdışına aktarımını düzenleyen 9'uncu maddelerde de açık rıza şartı aranmaktadır.

Kişisel verilerin hukuka uygun olarak işlenmesinde 6698 sayılı Kanunla verinin ilgilisinden talep edilen rıza alelade bir rıza olmayıp açıkça, belirli bir konuyla bağlantılı ve aydınlatılmış bir iradeye dayanan özgür bir rıza olarak tezahür etmelidir. Rızayı açıklayan kişi, kişisel verisinin hangi amaçlarla işleneceğine ilişkin tam bir bilgi sahibi olmalıdır. Bununla birlikte, uygulamada işletmelerin önceden hazırlanmış, uzun ve karmaşık bilgilendirme formları yoluyla rıza almaya çalıştıkları bilinmektedir. Ayrıca, pek çok uygulama ve hizmetten faydalanmak için kullanıcının bu formları onaylaması talep edilmekte, aksi halde hizmetten faydalanmak mümkün olamamaktadır. Bu gibi durumlarda kullanıcılar uzun ve karmaşık formları okuyup

değerlendirmeden onaylamakta, hizmetten bir an önce faydalanmak isteği, mahremiyetin ve veri güvenliğinin önüne geçebilmektedir.

Kişisel verilerin rızaya dayalı olarak işlenmesi, Kanun'un 4'üncü maddesinde sayılan temel ilkelerinden biri olan amaçla sınırlılık ilkesinin uygulamaya yansıması olarak kabul edilmektedir. Bu ilkeye göre, belirli bir amaç için elde edilen kişisel veri ancak o amaçla bağlantılı, sınırlı ve ölçülü olarak işlenebilecektir. Bu bağlamda, verinin ikincil kullanımı gibi durumlarda, söz konusu işlenme başlangıçta alınan rızanın kapsamı dışında bir işlemi içeriyorsa, bireyin yeniden açık rızasının talep edilmesi gerekecektir. Zira yukarıda da ifade edildiği üzere, verilerin toplandığı ve rızanın açıklandığı sırada bütün işlenme amaçlarının kapsamlı bir biçimde öngörülmesi mümkün görülmemektedir. Sınırlı ve ölçülü veri işlemeyi gerektiren bu ilke AB hukukundaki veri minimizasyonu ilkesine karşılık gelmekte ve büyük verinin doğasıyla uyumsuzluk arz etmektedir.

5.2.3. Verinin sınır ötesi aktarımı bakımından değerlendirme

Kişisel verilerin yurt dışına aktarılması Kanun'un 9'uncu maddesiyle hüküm altına alınmakta, bu kapsamda kişisel verilerin ilgilinin açık rızası olmaksızın yurt dışına aktarılamayacağı düzenlenmektedir. Ancak, Kanun'un 5'inci maddesinin ikinci fıkrası ile 6'ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması veya ülkede yeterli koruma bulunmamakla birlikte, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri halinde Kişisel Verileri Koruma Kurulu, verilerin aktarımına izin verebilmektedir.

Ayrıca, Türkiye'nin taraf olduğu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin (108 no'lu Sözleşme) 12'nci maddesiyle, sözleşmeye taraf devletlerden birine yapılacak veri aktarımlarının münhasıran özel yaşam gerekçesiyle yasaklanamayacağı veya özel bir izne tabi kılınamayacağı düzenlenmektedir. Daha sonra kabul edilen, bu sözleşmenin eki 181 no'lu Protokol'ün 2'nci maddesinde ise Sözleşmeye taraf olmayan bir ülkeye veri aktarımları bakımından, muhatap kuruluş veya ülkenin "yeterli seviyede koruma" şartını karşılaması gerektiği ifade edilmektedir.

Gerek 6698 sayılı Kanun'da yer alan hüküm, gerekse mehaz AB düzenlemesinin temelinde veri aktarımının sınırlandırılması yaklaşımının mevcut olduğu görülmektedir. Ancak, büyük veri teknolojisinin dağıtık yapısı ve veri depolama amacıyla çoğunlukla bulut hizmetlerinden faydalanıldığı mevcut düzlemde bu yaklaşım eleştirilmektedir.[195] Verinin saklandığı veya işlendiği mekânsal konumun güvenlik ve mahremiyetin tesisinde tek belirleyici kriter olamayacağı, bu katı yaklaşım yerine, veri nereye aktarılırsa aktarılsın veya nerede işlenirse işlensin güvenlik, hesap verebilirlik ve şeffaflığın sağlanmasının hedeflenmesinin doğru olacağı değerlendirilmektedir.

5.2.4. Kanun'un geneline ilişkin hususlar

Dünyada büyük veriden fayda elde etme eğilimi belirginleştikçe toplumsal yaklaşım ve kurallar da aynı etkiyle değişime uğramaktadır. Nitekim çalışmanın birinci bölümünde anlatıldığı üzere büyük veri hâlihazırda birçok sektörü ve hatta bireysel olarak düşünme yöntemini derinden etkilemekte ve dönüştürmektedir. Bu durum ise fayda ve maliyet arasında bir denge tesis edilmesi ihtiyacını ortaya koymaktadır. Ancak dünyanın bugüne kadar yaşadığı büyük dönüşüm ve reformların aksine bu çabaların hayata geçirilmesi için önümüzde uzun yüzyıllar değil, oldukça kısa bir sürenin olduğu öngörülmektedir. Ayrıca, hukuki düzenlemelerde yapılan basit değişikliklerin büyük veri çağında hüküm vermek ve getirdiği riskleri önlemek için yeterli olamayacağı da savunulmaktadır.[196] Zira parametrik bir değişimden ziyade, bir paradigma değişiminin gerektiği değerlendirilmektedir. Bu çok yönlü değişim ihtiyacı, bu alanda izlenmesi gereken politikaların belirlenmesi konusunda mevcut kurumların yetersiz kalmasına neden olmuştur. OECD Bilim, Teknoloji ve Yenilikçilik Genel Müdürü'nünde belirttiği üzere; bu alanda ihtiyaç duyulan politikalar geleneksel bakanlıkların ötesinde, tüm hükümeti kapsayan ve hatta uluslararası işbirliğini gerektiren bir mahiyettedir. Verinin adeta sel olup aktığı bir ortamda, devletler her türlü politikasını veri mahremiyeti, güvenlik, erişim ve sorumluluk konularını dikkate alarak tasarlamak zorundadır.[197]

---

[195] Bozkurt-Yüksel, 2016: 173
[196] Mayer-Schönberger veCukier, 2013: 371
[197] Wyckoff, 2017: 1

Bu bağlamda, devletlerin büyük veri çağının doğuşunu nasıl ele aldıkları önem arz etmektedir. Her ne kadar bu hızlı değişim ve belirsizlik karşısında karar almak giderek daha zorlayıcı olsa da, alınan kararlar geleceği önemli ölçüde şekillendirecektir.

Mevcut 6698 sayılı Kanun'a kaynaklık eden AB hukukundaki yeni yaklaşımın, veri koruma alanındaki ilkelerin reaktif değil proaktif bir şekilde uygulanması şeklinde olduğu görülmektedir. Tüzük'ün 23'üncü maddesinde de belirtildiği üzere veri kontrolörü, kişisel verilerin korunmasına dair ilkelerin uygulanabilmesi için gerekli ve uygun teknik ve organizasyonel önlemleri almakla yükümlü kılınmıştır. Veri kontrolörünün elde ettiği kişisel verileri ancak belirlenen amaç doğrultusunda kullanması gerektiği ve bu çerçevede yükümlülüğünün verinin hacmi, işleme kapsamı, saklama süresi ve erişilebilirliği hususlarını da kapsadığı belirtilmektedir. Tüzük ile öngörülen bu artırılmış sorumluluk rejimi sayesinde özellikle bireyin haberi ve müdahalesi olmaksızın kişisel verilerinin işlenmesinin önlenmesi amaçlanmaktadır. Bireyi sürekli kontrol etme durumunda bırakmak yerine, bu alanda veri işleyenlerin de sorumluluklarını artırmak bir taraftan güçlü yaptırımların uygulanabilmesini ve ihlal durumunda müeyyideyi kati surette uygulayan bir kurumsal mekanizmayı gerektirmektedir. Nitekim büyük verinin temelini oluşturan karmaşık algoritmaları yorumlamak ve zarar görebilecek bireyleri savunmak için güçlü kurumlar ve profesyonellerin ortaya çıkması gerekmektedir. "Küçük veri çağında esas olan mahremiyet iken, büyük veri çağında özellikle güçlendirilmiş özgür iradenin ve ahlaki seçimde bulunabilme hürriyetinin bütün tehditlere karşı savunulması gerekmektedir."[198]

Gerek mehaz düzenleme olarak kabul edilen AB veri koruma hukukunun yeni düzenlemesi Veri Koruma Tüzüğü'yle getirilen sorumluluk artırıcı müesseselerin 6698 sayılı Kanun'da öngörülmemiş olması, gerekse Kişisel Verileri Koruma Kurumu'nun kurumsal yapılanmasının hala tamamlanamamış olması bir dizi zorluğu beraberinde getirmektedir.

[198] Cukier veMayer-Schönberger, 2013: 2

6. TÜRKİYE İÇİN DEĞERLENDİRME VE ÖNERİLER

Büyük verinin veri mahremiyetine ilişkin ortaya çıkardığı zorlukların giderilerek başarılı bir şekilde uygulanabilmesini sağlamak amacıyla, incelenen uluslararası örnekler ile Türkiye'deki mevcut durum, sorun alanları ve gelişmeler çerçevesinde geliştirilen politika tercihi, mevzuat düzenlemeleri ve idari faaliyetler kapsamındaki öneriler aşağıda yer almaktadır.

1. **Büyük verinin faydaları ile kişisel verilerin korunması hakkı başta olmak üzere mahremiyete ilişkin kişi hak ve hürriyetlerinin korunması arasında uzlaşmayı sağlayan temel bir politika yaklaşımı benimsenmelidir.**

Büyük veri, bünyesinde barındırdığı teknik imkânlarla mahremiyetin hâlâ korunabilir olup olmadığını sorgulanır hale getirmiştir. Modern toplumların mahremiyete ilişkin değerler ile büyük verinin getirdiği fayda arasında bir denge tesis etmesi gerekmektedir. Dolayısıyla Türkiye bakımından bu alanın nasıl düzenlenmesi gerektiği hususu; kişisel verilerin işlenmesini göz ardı ederek büyük veriden değer yaratan bir ülke olmak mı, yoksa büyük verinin fırsatlarını faydaya dönüştüremeden mahremiyete ilişkin kaygıların öncelenmesi mi noktasında düğümlenmektedir. AB'nin uzun süredir uygulamakta olduğu veri koruma mevzuatını, ABD yaklaşımını ve yeniliklerini dikkate alarak daha önce görülmemiş bir kapsamda yenilemesi, bu alandaki küresel yakınsamanın en önemli göstergesidir. Veriden değer yaratan küresel ABD şirketleri karşısında güçlü AB pazarı hızlı bir biçimde pozisyonunu almaya çalışmış, köklü bir mevzuat değişimine gitmiştir. Öte yandan Çin, kişisel veri pazarını güçlü küresel şirketlere bırakmamak adına gerek devlete gerekse yerli firmalara sağladığı ayrıcalıklı pozisyon ve verinin sınır ötesi aktarımı hususunda kabul ettiği sınırlandırıcı düzenlemelerle bu alanda ayrıksı bir yaklaşımı göstermektedir.

Küresel anlamda süregelen bu mücadele karşısında büyük verinin faydaları ile kişi hak ve hürriyetlerinin korunması arasında uzlaşmayı hedefleyen bir yaklaşımın benimsenmesi gerekmektedir. Nitekim, AB'de de, veri mahremiyeti konusunda büyük veri öncesindeki aşırı korumacı eğilimden vazgeçilmiş, büyük verinin sağladığı ekonomik ve sosyal faydayı kullanabilmek için veri işleyen sektörleri destekleyen düzenlemelerin benimsenmesi yönünde gelişmeler ortaya çıkmıştır.

Bu kapsamda, Türk hukukunda benimsenen adil veri işleme ilkelerinin temel olarak önemli yenilikçi değişimler karşısında uygulanabilirliğini sürdürdüğü değerlendirilmektedir. Ancak, zaman zaman bazı ilkeler öne çıkarken bazılarının geri planda kalması gerekmektedir. Bu çerçevede, değiştirilmesi güç katı hukuki metinler yerine, yenilikçi teknolojilerden yararlanılmasını kolaylaştıran, temel ilkelerin yorumlanmasını ve yol göstericiliğini güçlendiren yeni düzenleme ve politikaların belirlenmesi gerekmektedir.

2. Veri koruma hukukunun temelinde yer alan rıza kavramının uygulanmasına ilişkin düzenlemelerde, büyük verinin getirdiği değişimi dikkate alan güncellemeler hayata geçirilmelidir.

Kişisel verilerin işlenmesi konusunda incelenen bütün hukuk sistemlerinde temel bir ilke olarak bireyin rızasının arandığı görülmektedir. Ancak, büyük veri hizmetleri gibi veriye dayalı iş modellerinin etkin bir biçimde sürdürülmesinin temini açısından gerek ABD'de gerekse AB'de kişisel verilerin kullanılması sırasında veri sahibinin rızasının nasıl alınması gerektiğine ilişkin uygulamaların yeniden formüle edilmesi gerektiği kabul edilmiştir. Yeni hukuki yaklaşımda rızaya ilişkin sorumluluğun bireyden veri işleyenlere kayması gerektiği, veri toplama ve veri kullanımı süreçlerinin ayrı ayrı değerlendirilmesi gerektiği tespit edilmiştir.

Kişisel verinin toplanması sırasında alınan tek taraflı rızaya dayalı bir sistemden ziyade, veri işleyenlerin bilhassa ikincil kullanımlar dolayısıyla ortaya çıkan yeni kullanımlarda da bireyin onayını aldığı artırılmış bir sorumluluk rejimi çözüm olarak faydalı görülmektedir. AB Veri Koruma Tüzüğü'nde benimsenen tasarımdan itibaren mahremiyet ilkesinin Türk mevzuatına kazandırılması faydalı görülmektedir. Zira rızaya ilişkin mevzuatla getirilen sıkı şartların tek başına büyük verinin getirdiği zorlukları gideremeyeceği kabul edilmektedir. Bu alandaki esas değişimin veri pazarının aktörlerinin uygulamalarını değiştirerek sağlanabileceği görülmektedir. Bu çerçevede, 6698 sayılı Kanun'da yer almayan tasarımdan itibaren güvenlik ilkesinin mevzuata kazandırılması ve söz konusu ilkenin veri sorumlularınca nasıl uygulanması gerektiğine ilişkin rehberlerin Kişisel Verileri Koruma Kurumu tarafından yayımlanması gerekmektedir.

3. **Büyük veriyle birlikte uygulanması giderek zorlaşan şeffaflık ilkesinin hayata geçirilmesini kolaylaştırıcı yeni düzenlemeler uygulamaya geçirilmelidir.**

Giderek belirsizleşen kişisel veri kullanım süreçlerinde şeffaflığın artırılması amacıyla, veri işleyenlerin ilgilileri daha aktif olarak bilgilendirmekle ve sahip oldukları yasal haklar konusunda gerekli hatırlatmaları yapmakla yükümlü kılınması yaklaşımı ortaya çıkmıştır. 6698 sayılı Kanun ile veri sorumluları bakımından getirilen aydınlatma yükümlülüğünde ise yalnızca verilerin elde edilmesi sırasında bilgi verilmesi düzenlenmiş, daha sonraki ikincil kullanımlar bakımından herhangi bir bilgilendirme mekanizması öngörülmemiştir. Kanun'un temel ilkeler bölümünde de şeffaflığa vurgu yapılmış olmakla birlikte, verinin ikincil kullanımları alanında ortaya çıkacak yeni durumların ilgililere bildirilmesini öngören hükümlerin Kanun'a eklenmesinin faydalı olacağı değerlendirilmektedir.

Yeni hukuki düzenlemelerde, en önemli şeffaflık artırıcı mekanizmalardan biri olarak, bireylerin kişisel verilerine makinalar tarafından okunabilir formatta erişim sağlanabilmesi yaklaşımı öne çıkmıştır. Kişisel verilerden sadece veri işleyen kuruluşların değil, aynı zamanda bireyin bizzat kendisinin yararlanacağı bir ekosistemin geliştirilmesi gerekmektedir. Bu kapsamda, bireylerin kişisel verilerine makinalar tarafından okunabilir formatta erişim sağlama hakkının tanınması, büyük veri ekosisteminin gelişmesi açısından faydalı olacaktır.

Ayrıca, veri sorumlularının, ABD hukukunda olduğu gibi farklı kaynaklardan elde ettikleri veriler ile sundukları hizmet dolayısıyla ortaya çıkan veri arasında ayrım yapılabilmesi amacıyla kendi mahremiyet politikalarında; hangi hizmetleri verdikleri, izleme yoluyla veri toplayıp toplamadıklarını, hangi verileri izleyerek elde ettikleri ve bu verilerle ne yaptıklarını belirtmelerinin sağlanması faydalı görülmektedir. Kişisel Verileri Koruma Kurumu tarafından çıkarılacak ikincil düzenlemelerde bu hususun dikkate alınması önem arz etmektedir.

Küresel anlamda öne çıkan bir diğer önemli husus ise büyük veri analizinde karar verme süreçlerinde kullanılan algoritmaların temel aldıkları kriterlerin de şeffaf olmasıdır. Algoritmalara dayalı karar alma eğilimindeki artış dikkate alınarak,

Türkiye'de kişisel veri işleyen aktörlerce sonuca ulaşmada kullanılan kriterlerin kamuoyuna açıklanması zorunluluğu getirilmesi gerekmektedir. Bu çerçevede, bireylere haklarında oluşturulan çıkarımlara karşı koyabilmeleri için uygun mekanizmaların ve süreçlerin veri sorumluları tarafından sunulması gerekmektedir.

4. **Büyük kapsamlı ve kritik veri işleme faaliyetleri bakımından veri koruma görevlisi belirlenmesine ilişkin kanunî düzenlemeler hayata geçirilmelidir.**

OECD çalışmalarında, veri temelli karar verme süreçlerinin veri etiği sorumlusu uzmanlar tarafından gözetim altında gerçekleştirilmesi önerisi getirilmiştir. AB'de benimsenen zorunlu veri koruma görevlisine ilişkin kanun hükümleri de bu yaklaşımın bir tezahürüdür. Bu çerçevede, Türkiye'de de büyük kapsamlı veri işlemeler bakımından veri koruma görevlisi belirlenmesine ilişkin kanuni seviyede çalışma yapılması faydalı olacaktır.

5. **Veri işleyenlerin kişisel veri ihlallerinin önlenmesine ilişkin verdikleri taahhütlere yönelik sorumluluklarının artırılması yaklaşımı kabul edilmelidir.**

Verileri kimliksizleştirmeyi sağlayan mahremiyet artırıcı teknolojilerin, büyük veri bağlamında veriyi istikrarlı bir kişisel olmayan veri kategorisine yerleştirmekten ziyade, geçici bir çözüm olabildiği tespit edilmiştir. Mahremiyet artırıcı teknolojiler karşısında yeniden kimliklendirmeyi mümkün kılan araçların hızla kullanılmasının mümkün olduğu büyük veri analizinde, söz konusu araçların tek başına politika belirleyicisi olarak etkin olamayacakları değerlendirilmektedir. AB'nin yeni düzenlemesinde olduğu gibi veri işleyenlerin gerekli teknik önlemleri almakla yükümlü kılındığı artırılmış bir sorumluluk rejiminin bu alanda faydalı olacağı değerlendirilmektedir. Bu çerçevede, teknik çözümlerin idari ve yasal önlemlerle birleştirilerek iç hukukta da uygulanmasının teşviki gerekmektedir.

Ayrıca, büyük veride mahremiyete ilişkin hangi teknik çözüm mekanizmalarının uygulanabileceğine yönelik güncel rehberlerin Kişisel Verileri Koruma Kurumu tarafından yayımlanması faydalı olacaktır. Bu rehberlerde, geliştirilen yeni teknolojik araçların, toplanan kişisel verilerin yaşam döngüsünü kaydedip tanımlayarak kuruluşlara kişisel verilerin yönetiminde yardımcı olabilecek

ve hesap verebilirliği kolaylaştıracak imkânları da sunabileceği değerlendirilmektedir. Böylece, gelişmiş veri etiketleme şemaları ile kişisel verilere bağlam ve tercih bilgisi eklenmesi yoluyla kuruluşların gelecekteki veri kullanımlarını yönetebilmesi teşvik edilmiş olacaktır.

6. **Kişisel verilerin işlendiği büyük veri uygulamalarında, algoritmaları oluşturanların insan hakları ve etik değerler konusunda farkındalıklarını artırıcı mekanizmalar geliştirilmelidir.**

Büyük veri tekniklerinin, bireylerin yaşamları ile ilgili geleneksel ve resmi karar alma yöntemlerinin yerini alacağına ilişkin endişeler bulunduğu görülmüştür. Veri bilimciler başta olmak üzere algoritmaların arkasındaki aktörlerin analiz ettiklerinin gerçek bireylerin hayatı olduğu konusunda düşünmeye zorlanması gerekmektedir. Veri sorumlularının kişisel verilerin güvenliğinin temini için gerekli teknik önlemleri almakla yükümlü bulunması Türk hukukunda da kabul edilmiştir. Ancak, OECD ve ABD tarafından da önerilen; veri analistlerine, analiz ettikleri dijital verilerin aslında insan hayatını temsil ettiğinin defaatle hatırlatılması ihtiyacına yönelik bir düzenleme bulunmamaktadır. İşlenen verinin hassasiyetiyle doğru orantılı olarak, en hassas verilerle çalışan kuruluşların sürekli ve sabit hatırlatıcılarla yüzleşmelerinin sağlanması gerekmektedir. Bu çerçevede, büyük çapta veri işleyen kuruluşlarda bu ihtiyaca yönelik iç denetim mekanizmalarının kurulması amacıyla ikincil düzenlemelerin hayata geçirilmesi gerekmektedir.

7. **Otomatik veri sistemlerinin kullanıldığı büyük ölçekli kişisel veri işleme faaliyetleri bakımından veri koruma etki değerlendirmesi (VKED) yapılması şartı getirilmelidir.**

Özellikle otomatik veri sistemlerinin kullanıldığı büyük ölçekli işleme faaliyetleri AB Veri Koruma Tüzüğü ile riskli veri işleme faaliyeti olarak değerlendirilmektedir. Bu kapsamda, kaleme alınan zorunlu VKED'e ilişkin hükümle, özellikle yeni teknolojik veri işleme metodlarının kullanıldığı veri işleme faaliyetlerinin gerçek kişilerin hak ve özgürlükleri bakımından yüksek bir risk içermesinin muhtemel olduğu durumlarda, söz konusu işlemenin kapsamı, niteliği, bağlam ve amacı da dikkate alınarak veri kontrolörünün, öncelikle bir VKED yapması

şartı getirilmiştir. 6698 sayılı Kanun'da da aynen yer alan eski AB düzenlemesi 95/46/EC sayılı Direktif'in getirdiği veri siciline kayıt ve bildirime ilişkin genel hükmün, pek çok idari ve mali yük getirirken kişisel verilerin korunması konusunda köklü bir çözüm sağlamadığı görülmüştür. Bu çerçevede, ayrım gözetmeksizin tanımlanan bu genel bildirim yükümlülüğü yerine, VKED'nin yapılmasının çok daha amaca matuf olacağı değerlendirilmektedir.

Bu çerçevede, Kişisel Verilerin Korunması Kanunu'na bu yönde bir düzenlemenin konulması ve veri sorumlularının kişisel veri sicil kaydına ilişkin hazırlanacak yönetmelikte de bu hususun dikkate alınması gerekmektedir.

Ayrıca, AB Genel Veri Koruma Tüzüğü'nde VKED kurumsal anlamda uygulanması zorunlu bir yöntem olarak öngörülmüştür. Dolayısıyla, Kişisel Verileri Koruma Kurumu tarafından VKED'ye tabi veri işleme faaliyetlerinin bir listesinin oluşturularak güncel şekilde yayımlanması gerekmektedir. Böylece, yüksek risk taşıyan büyük veri analizlerinde söz konusu listede yüksek riskli olarak değerlendirilen veri işleme faaliyetleri bakımından veri sorumlularının Kurum'dan görüş alabilme imkânı ortaya çıkmış olacaktır.

8. Bireylerin kişisel verilerine kolayca erişebilmesi ve taşıyabilmesine ilişkin hukuki düzenlemeler hayata geçirilmelidir.

ABD'nin Yeşil Düğme Girişimi, İngiltere hükümetinin başlattığı Midata Girişimi ve Fransa'da başlatılan FING Girişimi örnekleri bireylere kendileriyle ilgili kişisel verilerine güvenli, kullanıcı dostu ve makinalar tarafından okunabilir formatta erişebilme hakkının tanınmasının önemini ortaya koymaktadır. Bu çerçevede, Türkiye'de de kişisel verileri, toplumsal fayda ve yenilikçiliğin desteklenmesi için ortak bir kaynak olarak ele almayı öngören bir politika bakış açısının geliştirilmesi gerekmektedir.

Kişisel verilere makinalar tarafından okunabilir ve kullanılabilir bir formatta erişilmesi düşüncesi AB hukukunda ABD veri aktörlerinin derin etkisini ortaya koymaktadır. Veriyi bir kez elde ettikten sonra, söz konusu kaynağın her türlü faydasının büyük ABD BİT firmalarında kalmasının engellenmesi amaçlanmıştır. Diğer taraftan, AB hukukunda gündeme gelen veri taşınabilirliği hakkının mevzuata

dercedilmesinin önem arz ettiği değerlendirilmektedir. Özellikle özel sektör işletmelerinin tüketim ve işlem verilerini taşınabilir ve tercihen makinalarca okunabilir formatta müşterilerine sunmaları teşvik edilmelidir.

9. Unutulma hakkı mevzuatta açıkça tanımlanmalıdır.

Büyük miktarda veriyi uzun süre saklayan arama motorlarının ve hizmet sağlayıcıların veri kontrolörü sayılması gerektiğini ortaya koyan ve bireyin kişisel verileri konusundaki haklarını savunmaları ve çevrimiçi verileri üzerindeki kontrollerini artırmaları açısından dönüm noktası olan "unutulma hakkı" dünyada ilk kez AB Veri Koruma Tüzüğü ile kabul edilmiştir. Türkiye'de yargı kararlarında da yer almaya başlayan söz konusu hakkın 6698 sayılı Kanun ile düzenlenmesinin faydalı olacağı değerlendirilmektedir.

10. Gelişmekte olan yenilikçi teknolojiler karşısında mahremiyet bilinci ve farkındalığını artırıcı çalışmalar hayata geçirilmelidir.

Gözden geçirilmiş OECD Mahremiyet İlkelerinin "tamamlayıcı tedbirler" çağrısında işletmelerin ve bireylerin sorumluluk sahibi veri kullanımlarını sağlamanın temel yolunun, gerek yapılan yaygın hatalar gerekse veri analizinin muhtemel olumsuz etkileri konusunda eğitim ve farkındalık çalışmalarının hayata geçirilmesi olduğu ifade edilmiştir. OECD ülkelerinin mahremiyet zorluklarıyla başa çıkabilmek için benimsediği politika önlemleri arasında, mahremiyet bilincinin artırılması en üst sıralarda yer almıştır. Mahremiyet duyarlılığının artırılması ve kamu, özel sektör ve bireylerin bu konuda eğitilmeleri hususunda somut adımlar atılması gerekmektedir. Bu çerçevede, Türkiye'de de büyük veri alanında mahremiyet risklerinin önlenmesi amacıyla, Kişisel Verileri Koruma Kurumu tarafından eğitim ve farkındalık çalışmalarının hayata geçirilmesi gerekmektedir.

11. Kişisel verilerin korunması alanındaki düzenleme ve denetleme görevinin etkili ve hızlı uygulanması sağlanmalıdır.

Büyük veri karşısında hakları güçlendirilmiş bireyler ve sorumlulukları artırılmış veri sorumlularına ilişkin hukuki düzenlemelerin küresel ölçekte güçlü veri aktörlerine karşı uygulanabilmesi için, gözden geçirilmiş OECD Mahremiyet İlkelerinde de belirtildiği üzere etkili kaynaklara ve teknik uzmanlığa sahip olunması gerekmektedir. 2016 yılında yayımlanan 6698 sayılı Kanun'un yürürlüğe girmesinin üzerinden uzun bir süre geçmesine rağmen Kişisel Verileri Koruma Kurumu'nun halen kurumsal yapılanmasını tamamlayamadığı görülmüştür. Bu alanda güçlü yetkilerle ve yaptırım gücüyle donatılmasının yanında Kişisel Verileri Koruma Kurumu'nun nitelikli teknik ve hukuki personel ihtiyacının en kısa sürede karşılanması gerekmektedir.

Ayrıca, başta büyük veri olmak üzere yenilikçi teknolojilerin toplumsal etkileri ile etik zorluklarının iyi anlaşılması ve yeni bir kişisel veri yönetişim politikası ve düzenleme çerçevesi geliştirilmesi ihtiyacını karşılamak üzere, Fransa veri koruma otoritesi veya 29. Madde Çalışma Grubu örneğinde olduğu gibi Kişisel Verileri Koruma Kurumu uhdesinde bir çalışma grubu oluşturulmasının faydalı olacağı öngörülmektedir.

12. Yenilikçi teknolojiler karşısında mahremiyetin korunmasına ilişkin profesyonellere yönelik program, etkinlik ve eğitimler düzenlenmeli, bu alanda işbirlikleri geliştirilmelidir.

OECD tarafından ortaya konulan çalışmada yenilikçi teknolojiler dolayısıyla mahremiyet risklerinin artan önemi ve görünürlüğü, bu alanda çalışan uzmanların potansiyel yeni iş imkânlarının ve onlara olan talebin arttığını göstermiştir. AB tarafından öngörülen zorunlu veri koruma görevlisi bulundurmaya ilişkin hukuki düzenlemeler de ülkelerin bu alanda işgücünü geliştirme ihtiyacını ortaya çıkarmıştır. Nitekim AB pazarıyla iş yapmakta olan yerli BİT firmaları bakımından da bu ihtiyacın artacağı öngörülmektedir.

Bu kapsamda, dünyadaki pek çok kuruluşun profesyonellerde yetkinlik geliştirmek için attığı adımların incelenmesi ve Türkiye'de de büyük veri gibi yenilikçi teknolojilerde mahremiyetin korunmasına ilişkin profesyonellere yönelik program, etkinlik ve eğitimler düzenlenmesi ve Kişisel Verileri Koruma Kurumu tarafından işbirlikleri geliştirilmesi gerekmektedir.

13. Sınır ötesi veri aktarımı konusunda uluslararası işbirliği mekanizmaları geliştirilmeli ve 6698 sayılı Kanun'da öngörülen sistemin etkin bir şekilde hayata geçirilmesi sağlanmalıdır.

OECD ülkelerinin büyük bir bölümünde, veri depolama amacıyla çoğunlukla bulut hizmetlerinden faydalanılması ve büyük verinin dağıtık yapısı gibi sebeplerle sınır ötesi veri aktarımına olan bağımlılığın arttığı, bu nedenle mahremiyet korumasının uluslararası boyutunun önemli bir politika alanı olarak kabul edilmeye başlandığı görülmüştür. Uluslararası işbirliğiyle ülkeler arasındaki mahremiyet mevzuatının koordinasyonu ve uyumlaştırılması teşvik edilmektedir. Nitekim AB Genel Veri Koruma Tüzüğü'yle getirilen geniş uygulama alanı da, AB ülkelerinin kendi aralarında sağlamaya çalıştığı üst seviye uyum çabasının sonucudur. AB ülkeleriyle iş yapan yerli BİT firmalarının "yeterli ülke" konumunun sağlamlaştırılması açısından Türkiye'de de AB standartlarına uyumun yakalanması gerektiği değerlendirilmektedir. Bu çerçevede, mevzuat anlamında üst seviye uyumu kendi içinde sağlayan AB'nin yeni Tüzüğü'nün güvenlik, hesap verebilirlik ve şeffaflığın sağlanmasına ilişkin temel gerekliliklerinin karşılanması gerekmektedir. Ayrıca, Tüzük'ün sınır ötesi uygulanmasında, yeterli ülke kriteri belirlenirken komisyonun veri otoriteleri arasında işbirliği araması nedeniyle Kişisel Verileri Koruma Kurumu'nun biran önce AB ülkeleriyle işbirliği yolunda harekete geçmesi önem arz etmektedir.

Ayrıca, Kurum'un, 6698 sayılı Kanun'un verilerin yurtdışına aktarılmasına ilişkin hükümlerinin etkili bir şekilde uygulanabilmesi için kurulması önerilen 29. Madde Çalışma Grubu gibi etkin bir mekanizma tesis ederek yurt dışına aktarım şartlarını doğru bir şekilde ortaya koyması önem arz etmektedir.

SONUÇ

Büyük verinin kullanım alanlarının artması yenilikçiliği artırmakta, toplum sağlığının iyileştirilmesinden ulusal güvenliğe, kamu düzeninin korunmasından ekonomik verimliliğin artırılmasına kadar birçok toplumsal fayda açığa çıkarmaktadır. Belirlenen öncelikli sektörlerde kalkınmaya katkı sağlamak için büyük veriden fayda yaratmak amacıyla yenilikçi uygulamalar, stratejiler ve yetkinlikler geliştirilmesini destekleyen Avrupa İçin Büyük Veri Platformu girişimi ve gelişmekte olan ülkelerdeki ekonomik krizlerle başa çıkmaya yönelik politikaların belirlenmesi amacıyla BM Genel Sekreterliğince başlatılan "Küresel Nabız" girişimi bu alanda öne çıkan çalışmalar olmaktadır. Büyük verinin getirdiği faydaların mahremiyete ilişkin kurallar karşısında korunarak dengenin tesis edilmesinin önem arz ettiği görülmektedir. Nitekim, büyük veride kişisel olmayan birkaç veri setinin kullanılarak profilleme yapılabilmesi, hatta kişisel olmayan verilerden yepyeni kişisel bilgilerin ortaya çıkarılabilmesi, kişisel veriler ile kişisel olmayan veriler arasında ayrım öngören modern mahremiyet düzenlemelerinin hâlâ uygulanabilir olup olmadığını sorgulanır hale getirmiştir. Söz konusu düzenlemelerin temel ilkelerinden biri olmaya devam eden kişisel verilerin bireyin rızasına dayanan, amaçla bağlantılı, sınırlı ve ölçülü işlenmesi temel kabulünün büyük veri çağında uygulanmasının oldukça güçleştiği görülmüştür. Zira büyük veriye dayalı iş modellerinde uzun süreler boyunca büyük miktar ve çeşitlilikte verinin hızla toplanması gerektiği görülmüştür. Bu doğrultuda, büyük veri tekniklerinin mevcut mahremiyet düzenlemeleri üzerinde genel bir revizyonu gerektirecek biçimde önemli bir baskı oluşturduğu görülmüş, büyük veri çağında kişisel veri işleme kurallarının yeniden yorumlanması ihtiyacına binaen Türkiye'de bu alanda yapılması gerekenler tespit edilmiştir.

Bu çalışma kapsamında, büyük veri kavramı ile bileşenleri açıklanmış, büyük veri analizini mümkün kılan teknolojik çözümler ele alınmış, ardından büyük verinin uygulama alanları, zorlukları ve riskleri değerlendirilmiştir. Ayrıca, büyük verinin ekonomik etkilerine ilişkin yaklaşımlar da ele alınmıştır. Büyük veri uygulamalarının veri mahremiyeti kurallarına etkilerinin değerlendirilmesi amacıyla, dijital çağda güvenlik ve mahremiyet alanında ortaya çıkan yeni ihtiyaçlar ile güvenlik ve mahremiyete ilişkin kaygılar ele alınarak bu alanda atılması gereken adımlar ve

geleceğe ilişkin hukukî öngörüler değerlendirilmiştir. Bu çerçevede, uluslararası örneklerden yola çıkılarak Türkiye'de büyük veri uygulamalarının veri koruma hukukuna etkileri bakımından bir değerlendirme yapılmış; mevcut düzenlemelerin söz konusu sorunları çözmede yeterli olmadığı tespit edilmiştir.

Kişisel verilerin büyük veri gibi yenilikçi teknolojiler karşısında korunması için değiştirilmesi güç katı hukuki metinler yerine, bu teknolojilerden yararlanılmasını kolaylaştıran temel ilkelerin yorumlanmasını ve yol göstericiliğini güçlendiren yeni düzenleme ve politikaların belirlenmesi önem arz etmektedir.

6698 sayılı Kanun'da yer alan rızaya ilişkin sorumluluğun bireyden veri işleyenlere kayması gerektiği, veri toplama ve veri kullanımı süreçlerinin ayrı ayrı değerlendirilmesi gerektiği tespit edilmiştir. Ayrıca Kanun'da yer almayan tasarımdan itibaren güvenlik ilkesinin mevzuata kazandırılması ve söz konusu ilkenin veri sorumlularınca nasıl uygulanması gerektiğine ilişkin rehberlerin yayımlanması önem arz etmektedir.

Büyük veriyle giderek yaygınlaşan verinin ikincil kullanımları alanında ortaya çıkacak yeni durumların ilgililere bildirilmesini öngören düzenlemelerin hayata geçirilmesi gerektiği görülmüştür. Bu kapsamda şeffaflık artırıcı mekanizmalardan biri olan, bireylerin kişisel verilerine makinalar tarafından okunabilir formatta erişim sağlama imkânının tanınması gerektiği değerlendirilmektedir.

Algoritmalara dayalı karar alma eğilimindeki artış dikkate alınarak, Türkiye'de kişisel veri işleyen aktörlerce sonuca ulaşmada kullanılan kriterlerin kamuoyuna açıklanması zorunluluğu getirilmesi, bu çerçevede, bireylere haklarında oluşturulan çıkarımlara karşı koyabilmeleri için uygun mekanizmaların ve süreçlerin veri sorumluları tarafından sunulması gerektiği tespit edilmiştir.

Büyük veri temelli karar verme süreçlerinin giderek yaygınlaşması dikkate alınarak, Türkiye'de büyük kapsamlı veri işleme faaliyetleribakımından veri koruma görevlisi belirlenmesine ilişkin kanuni düzenleme yapılması gerekmektedir.

Büyük veri işleyenlerin gerekli teknik önlemleri almakla yükümlü kılındığı artırılmış bir sorumluluk rejiminin bu alanda faydalı olduğu değerlendirilmiştir. Bu çerçevede, teknik çözümleri idari ve yasal önlemlerle birleştiren yaklaşımların

mevzuata yansıtılması önem arz etmektedir. Ayrıca, büyük çapta veri işleyen kuruluşlarda analiz ettikleri dijital verilerin aslında insan hayatını temsil ettiğinin hatırlatılması ihtiyacına yönelik düzenlemelerin hayata geçirilmesi faydalı görülmektedir.

Türkiye'de de büyük veri alanında mahremiyet risklerinin önlenmesi amacıyla, eğitim ve farkındalık çalışmalarının hayata geçirilmesi gerekmektedir.

Türk yargı kararlarında da yer alan "unutulma hakkı"nın 6698 sayılı Kanun ile düzenlenmesi önem arz etmektedir.

Büyük veri işleyen küresel ölçekte güçlü veri aktörlerine karşı mevzuatın güçlü bir biçimde uygulanabilmesi için, Kişisel Verileri Koruma Kurumu'nun nitelikli teknik ve hukuki personel ihtiyacının en kısa sürede tamamlanması gerekmektedir.

Sınır ötesi veri aktarımının giderek arttığı mevcut durumda, uluslararası işbirliğiyle ülkeler arasındaki mahremiyet mevzuatının koordinasyonu ve uyumlaştırılmasının teşvik edildiği görülmüştür. Bu çerçevede, Türkiye'de uluslararası işbirliğinin tesisi amacıyla gerekli mekanizmaların düzenlenmesi ve AB'deki 29. Madde Çalışma Grubu gibi etkin bir mekanizma tesis edilerek yurt dışına aktarım şartlarının doğru bir şekilde ortaya konulması önem arz etmektedir.

EKLER

EK-1: AB'nin 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktifi

1. Veri Koruma Direktifi'nin Kapsamı

Direktif'in kapsamını belirleyen 3'üncü maddesine göre bu Direktif bir dosyalama sisteminin parçasını oluşturan ya da oluşturması istenen gerçek kişilere ait kişisel verilerin, otomatik veya otomatik olmayan araçlarla işlenmesi durumunda uygulama alanı bulmaktadır. Bu kapsamda, gerek elektronik ortamda tutulan veriler gerekse elle işlenen kişisel veriler bakımından söz konusu verilerin özel kriterlere göre erişilebilir ve yapılandırılmış olması gerektiği anlaşılmaktadır. Direktifin özellikle "yapılandırılmış kişisel veri seti" ifadesine olan vurgusu, yapılandırılmamış veri yığınlarının işlenerek anlamlı sonuçlar elde edildiği ve sonucunda kişinin belirlenebilir kılınmasını sağlayan yapılandırılmış verilere dönüştürülebildiği büyük veri teknolojileri ve analizi bakımından dikkat çekici bir hususdur.

Direktif'in koruma konusu yalnızca gerçek kişilere ilişkin kişisel veriler olup söz konusu hükümlerin tüzel kişiler bakımından koruma etkisi bulunmamaktadır. Söz konusu kurallar ile getirilen sorumluluk ve kuralların uygulanışı bakımından ise hiçbir fark gözetilmeksizin kamu, bireyler ve özel sektör bakımından uygulama alanı ortaya çıkmaktadır.

Direktif, kişisel verilerin işlenmesi hususunda oldukça kapsamlı bir yaklaşımı yansıtmakla birlikte, 3'üncü maddesinin ikinci fıkrasında bu Direktif hükümlerinin uygulama alanı bulamayacağı iki istisnai durum belirlenmiştir. Bunlardan ilki kamu güvenliği, savunma ve devletin güvenliğine ilişkin veri işlemelerinde ve devletin ceza hukuku alanındaki faaliyetleri gibi AB hukukunun uygulama alanı dışında kalan faaliyetlerinde Direktif hükümleri uygulanmayacaktır. İkinci istisnai durum ise gerçek bir kişinin tamamen kişisel veya evi ve ailesiyle ilgili olan veri işlemelerinde Direktif hükümleri uygulanmayacaktır.

Veri Koruma Direktifi'nin teknoloji tarafsız, kişisel verinin işlendiği her tür durumda uygulanma imkânına sahip olduğu ifade edilmektedir.[199]

2. Veri Koruma Direktifi'ndeki Temel Kavramlar

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

i. *Kişisel Veri*: Direktif'in 2/a maddesinde; *"kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri"* olarak tanımlanmaktadır. Direktif'te belirlenen kişisel veri kapsamı oldukça geniş olmakla birlikte sınırsız değildir. Yalnızca isim, adres veya kimlik numarası gibi doğrudan bireyin kimliğine atfedilen bilgiler değil elektronik ticaret sırasında gerçekleştirdiği işlem kayıtları, tıkladığı kısayollar, konumunun belirlenmesine yarayan görüntü kayıtları gibi kişisel tercih belirten ve bireye ulaşılmasını sağlayan hemen her türden veri kişisel veri sayılmaktadır.

ii. *Kişisel verilerin işlenmesi (işleme):* Kişisel verilerin otomatik ya da otomatik olmayan araçlarla toplanması, saklanması, elde edilmesi, değiştirilmesi, okunması, sorulması, kullanılması, üçüncü taraflara aktarılması, yayılması ya da hazır bulundurulması için yapılan işlemlerle verilerin kombinasyonu, bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü müdahale *"işleme"* kabul edilmektedir. Bu çerçeveden bakıldığında kişisel verilerin işlenmesi tanımı, kişisel verilerin hemen hemen her türlü kullanımını içeren, verinin kayıt altına alınmasından yok edilmesine kadar birçok işlemi ifade etmektedir.

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

---

[199] Yüksel Civelek, 2011: 75

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

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

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

3. Veri Koruma Direktifi'ndeki Temel İlkeler

Mahremiyet hakkının korunması ve bireyin özel hayatına müdahaleleri önleme ihtiyacıyla ortaya çıkan veri koruma ilkeleri Veri Koruma Direktifi'nin temelini

oluşturmaktadır. Söz konusu ilkelerle veri kontrolörünün kişisel verileri işlerken uyması gereken yükümlülükler belirlenmekte, işleme sırasında veri kontrolörüyle veri sahipleri arasında ortaya çıkan çıkar çatışması dengelenmeye çalışılmaktadır. Direktif'e göre üye devletler, kişisel verileri ancak aşağıdaki temel ilkelere uygun olarak işleyebilecektir:

i. *Adil ve Yasal İşleme:* Kişisel veriler adil ve yasalara uygun şekilde işlenecektir.
ii. *Amaç ile Sınırlılık:* Kişisel veriler; kesin, belirlenmiş ve hukuka uygun amaçlara göre toplanmış olacak ve ilk toplandıkları amaca aykırı olarak daha sonradan işlemeye konu olmayacaktır. Üye devletin gerekli önlemleri alması şartıyla, bu verilerin ilk toplandıkları amacın dışında tarihsel, istatistiksel ve bilimsel amaçlarla daha sonradan işlemeye konu olmaları durumu saklıdır.
iii. *İlgililik ve Orantılılık:* Kişisel veriler, toplama ve/veya müteakip olarak işleme amaçları için yeterli ve bu işlemlerle ilgili olacak, aşırı olmayacaktır.
iv. *Doğruluk ve Güncellik:* Söz konusu veriler güncel ve doğru olarak tutulacak; böylece veri kalitesi korunacaktır. Toplanma amaçları veya daha sonraki işleme için yanlış veya eksik olan verinin silinmesi veya düzeltilebilmesi için gerekli tüm makul adımlar atılacaktır.
v. *Süreyle Sınırlılık:* Kişisel veriler, toplama amacının veya daha sonraki işlemenin gerektirdiğinden daha uzun süre saklanmayacaktır. Veriler, veriye konu olan kişilerin kimliğinin belirlenmesine müsaade eder biçimde muhafaza edilecektir. Tarihsel, istatistiksel veya bilimsel amaçlarla daha uzun süreli muhafaza edilmesi gereken veriler bakımından uygun koruma önlemleri belirlenecektir.

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

Pek çok hukuk sisteminde kişilerin sağlık durumları, cinsel yaşamlarına ilişkin verileri, dini ve felsefi inançları, ırk veya etnik kökenlerini belirten kişisel verileri ve siyasi görüşleri daha üst seviyede bir korunmayı gerekli kıldığından "hassas kişisel

veri" olarak tanımlanmaktadır. Direktif'in 8/1'inci maddesiyle hassas kişisel veri niteliğini haiz verilerin işlenmesinin üye devletler tarafından yasaklanması gerektiği ifade edilmektedir. Söz konusu işleme yasağına ilişkin istisna hükmü ise (veri sahibinin açık rızasının olması durumu gibi) aynı maddenin ikinci fıkrasında düzenlenmektedir. Hassas kişisel verilerin, mahiyetleri itibarıyla, bireylerin toplum içerisinde ayrımcılık veya bir takım mağduriyetlere uğramasına yol açabilmeleri bakımından bu hüküm yüksek önemi haizdir.

Veri Koruma Direktifi'nin kişisel verilerin korunması hukuku bağlamında sahip olduğu en önemli unsurlarından biri de 28'inci maddesiyle getirmiş olduğu etkin denetim sistemidir. Söz konusu maddeye göre her üye devlet Direktif'te yer alan hükümlerin kendi ülkesindeki uygulamasını izlemek ve bu konuda en az bir kamu kurumunu (Veri Koruma Otoritesi) görevli kılmak zorundadır. Bu kapsamda, üye ülkelere, kişisel verilerin işlenmesi ve bu anlamda bireysel hakların korunması konusunda ikincil düzenlemelerini yaparken veya idari tedbir alırken, Veri Koruma Otoritesine danışılmasını temin etme yükümlülüğü getirilmektedir. Veri Koruma Otoritelerinin görevlerini yerine getirirken gerekli tüm bilgilere erişim, bu bilgilerin silinmesini veya yok edilmesini isteme, uyarma ve iç hukuk hükümlerinin ihlali halinde bu ihlalleri yargı aşamasına taşımak üzere kovuşturmaya başlama yetkileri de Direktif'te yer almaktadır.

EK-2: Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Temel Değişiklikler

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

Veri İşleyenlerin (data-proccesors) Tamamının Veri İşlemeden Sorumlu Tutulması: 95/46/EC sayılı Direktif'te "kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri"nin işlenmesine ilişkin kurallara uymakla yükümlü olan ve hukuka aykırı olarak yapılan iş ve işlemlerden sorumlu olan tek kişi "veri kontrolörü (data-controller)", başka bir ifadeyle veri işlemeye ilişkin tam yetkiyi elinde bulunduran kişi olarak düzenlenmekteydi. Veri Koruma Tüzüğü ile getirilen düzenleme kapsamında, veri kontrolörü olmamakla birlikte bu verileri işleyen herhangi bir şirket ya da birey de (bulut veya büyük veri analizi hizmet sağlayıcıları gibi alt hizmet sağlayan üçüncü taraflar da dâhil olmak üzere) verinin hukuka uygun işlenmesinden sorumlu tutulacaklardır. Bu hüküm veri işleme sayılan fiillerin sayıldığı madde hükmüyle birlikte değerlendirildiğinde; kişisel veriye ilişkin gerçekleştirilen

her türlü işleme faaliyetinin tüm faillerinin söz konusu işlemeden kaynaklı her türlü veri ihlali ve hukuka aykırılıktan sorumlu olduğu görülmektedir. Bu hükmün uygulanmasının yansımaları oldukça geniş olacağından hem veri kontrolörleri hem de veri kontrolörünün talebiyle veriyi işleyen üçüncü kişiler bakımından hukuki sorumluluk ortaya çıkmaktadır. Bu kapsamda, Veri Koruma Tüzüğü hükümlerinin, özellikle büyük veri alanında sunucuları AB dışında yerleşik bulunan ve işleme faaliyetlerini Birlik ülkeleri dışından sürdüren örneğin bulut hizmet sağlayıcıları bakımından da bağlayıcı olduğu görülmektedir. Tüzük ile getirilen yüksek oranlı para cezaları bu işleyiciler bakımından da bağlayıcıdır.

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

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

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

Uyumlaştırılmış Kullanıcı Hakları: Veri koruma hukuku kurallarının tanımış olduğu haklar bakımından üye ülke uygulamalarında ortaya çıkan bazı farklılıklar

giderilmektedir. Örneğin 95/46/EC sayılı Direktif hükümleri kapsamında da kullanıcılar kendileri hakkında hangi verilerin tutulduğuna ilişkin bilgi edinme hakkına sahiptiler. Ancak mevcut durumda üye ülke mevzuatları veri kontrolörüne bu konuda farklı uygulama seçenekleri sağlamaktadır. Örneğin; İngiltere'de bu bilgilerin sağlanması için gereken süre 40 gün olarak tespit edilmiştir. Veri Koruma Tüzüğü ile bu farklılık ortadan kaldırılarak söz konusu bilgilerin 20 gün içerisinde kullanıcılara sağlanması gerektiği düzenlenmiştir.

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

Kullanıcı Haklarına İlişkin Bilgilendirme Yükümlülüğünün Veri Kontrolöründe Olması: Veri Koruma Tüzüğü kapsamında veri kontrolörleri, kullanıcılarını bilgilendirmek ve sahip oldukları yasal haklar konusunda gerekli hatırlatmaları yapmakla yükümlü olup aynı zamanda söz konusu yükümlülüklerini gerçekleştirdiklerini belgelemekle de yükümlü tutulmaktadırlar. Tüzük'te ayrıca kullanıcılara ilişkin kişisel verilerin kontrolörün sistemlerinde yer almasına/kullanılmasına ilişkin olarak opt-out değil opt-in yaklaşımının tercih edildiği görülmektedir.[200] Bu kuralın ihlal edilmesi durumunda yeni Veri Koruma Tüzüğü 95/46/EC sayılı Direktif'e göre çok daha ağır tazminatlar öngörmektedir.

Daha Sıkı Yaptırımların ve Elverişli Mekanizmaların Öngörülmesi: Veri Koruma Tüzüğü ile getirilen en önemli düzenlemelerin başında veri ihlalleri karşısında öngörülen yaptırımlara ilişkin hükümler gelmektedir. Zira veri koruma kurallarına ilişkin ihlaller karşısında çok daha ağır tazmin yaptırımları ve elverişli sorun çözme

---

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

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

mekanizmaları öngörülmektedir. Hâlihazırda, örneğin İngiltere'de veri ihlalleri neticesinde verilebilecek en yüksek para cezası 500 bin Pound iken Tüzük ile bu rakam 20 milyon avro veya hizmet sağlayıcının küresel gelirinin yüzde dördü gibi önemli miktarlara ulaşabilmektedir. Ayrıca, mevcut iç hukuk düzenlemeleri bakımından veri ihlallerinin kullanıcılara veya veri koruma otoritelerine bildirimleri konusunda birbirinden farklı hukuki yaklaşımlar ve uygulamalar bulunmaktadır. Veri Koruma Tüzüğü ile bu konudaki belirsizliğin ve üye ülkeler arası farklılığın ortadan kaldırılması amacıyla söz konusu bildirimin en geç 72 saat içerisinde veri koruma otoritelerine yapılması gerektiği düzenlenmektedir (33'üncü madde). Bununla birlikte, veri ihlali konusunda kullanıcının ne kadar süre içerisinde bilgilendirileceğine ilişkin bir süre öngörülmemiş olup bu konu belirsiz bulunmaktadır.

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

Veri Taşınabilirliği Hakkı: Bu hak ilk kez Veri Koruma Tüzüğü'nün 20'nci maddesiyle tanımlanmış olup madde ile veri sahibi, kişisel verisini tutmaya yetkili bir veri kontrolöründen diğerine taşıyabilme yetkisine sahiptir.

Hassas Verilerin İşlenmesi Bakımından Öngörülen Zorunlu Veri Koruma Görevlisi: Veri Koruma Tüzüğü'nün 37'nci maddesi gereğince aşağıdaki koşulların varlığı halinde veri kontrolörleri ve işleyicileri veri koruma görevlisi olarak belirlenir:

a) İşleme faaliyeti, yargı faaliyetinin yürütülmesi durumu hariç, bir kamu kurum veya kuruluşunca gerçekleştiriliyorsa,

b) Yapmış oldukları işin doğası gereğince büyük ölçüde veriyi düzenli ve sistematik izlemeyi gerektiren veri işleyicisi veya veri kontrolörlerinin temel faaliyetlerini veri işleme oluşturuyorsa,
c) Veri kontrolörü veya işleyicisinin temel faaliyetlerini 9'uncu maddede sayılan özel nitelikli hassas verilerin işlenmesi veya 10'uncu maddede ifade edilen ceza mahkûmiyeti veya suça ilişkin kişisel bilgilerin işlenmesi durumunda.

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

Riskli Veri İşleme Faaliyetleri Bakımından Zorunlu Veri Koruma Etki Değerlendirmesi (VKED): Veri Koruma Tüzüğü'nün 35'inci maddesiyle getirilen bu yeni düzenlemede, özellikle yeni teknolojik veri işleme metodlarının kullanıldığı veri işleme faaliyetlerinin gerçek kişilerin hak ve özgürlükleri bakımından yüksek bir risk içermesinin muhtemel olduğu durumlarda, söz konusu işlemenin kapsamı, niteliği, bağlam ve amacı da dikkate alınarak Tüzük hükümlerine uyumun arttırılması amacıyla veri kontrolörü, öncelikle bir VKED yapılmasından sorumlu tutulmaktadır. Maddenin ikinci fıkrasında özellikle hangi durumlarda VKED yapılması gerektiği (otomatik veri işleme sistemlerinin kullanılması, hassas verilerin işlenmesi veya ceza mahkûmiyeti ve suçlara ilişkin veriler gibi) detaylı olarak açıklanmaktadır. Bu kapsamda, 86 no'lu giriş maddesinde kişisel veri işleme faaliyetlerinin Veri Koruma Tüzüğü hükümlerine uygun olarak gerçekleştirilmesine yönelik alınacak önlemlerin belirlenmesinde söz konusu VKED sonuçlarının dikkate alınacağı ifade edilmektedir. VKED'nin özellikle büyük ölçekli işleme faaliyetlerinde gerekli olduğu vurgulanmaktadır. Ayrıca, bir VKED sonucunda, işleme faaliyetlerinin kontrolörün mevcut teknoloji ve uygulama maliyetleri açısından uygun tedbirlerle hafifletemeyeceği yüksek bir riski içerdiğinin ortaya çıkması durumunda, veri işleme faaliyetinden önce veri koruma otoritesine danışılması gerekmektedir.

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

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

Varsayılan ve Tasarımdan İtibaren Veri Koruması yaklaşımı: Tüzüğün giriş bölümünde kişisel verilerin işlenmesi bağlamında gerçek kişilerin hak ve özgürlüklerinin korunması amacıyla gerekli teknik ve organizasyonel önlemlerin alınması gerektiği ifade edilmektedir. Bu kapsamda, veri kontrolörü iç işleyişi ile alakalı politikalarını belirleyerek varsayılan ve tasarımdan itibaren veri koruması ilkelerini karşılamaya yönelik gerekli tedbirleri almalıdır. Bu ilkeye göre veri kontrolörü, gerek veri işleme vasıtalarının belirlenmesi sırasında gerekse veri işleme anında Tüzük'te öngörülen veri koruma kurallarının etkili bir biçimde uygulanması için gerekli araçları kullanarak, örneğin bulanıklaştırma (pseudonymisation)[201] veya asgari veri işleme gibi, uygun teknik ve organizasyonel önlemleri almalıdır. Söz konusu önlemlerin belirlenmesine ilişkin temel hususlar Veri Koruma Tüzüğü'nün 25'inci maddesinde yer almaktadır.

Kanada Ryerson Üniversitesi Mahremiyet ve Büyük Veri Enstitüsü Genel Müdürü Ann Cavoukian tarafından geliştirilen bir yaklaşım olan tasarımdan itibaren mahremiyet, veri toplama ve analizi konusundaki güçlü ön-mahremiyet önlemlerinin daha tasarım aşamasında dikkate alınması ilkesine dayanmaktadır. Söz konusu yaklaşım şu yedi temel ilkeden oluşmaktadır: reaktif değil proaktif- iyileştirici değil önleyici olma ilkesi, varsayılan ayar olarak mahremiyet ilkesi, tasarıma gömülü

[201] AB Veri Koruma Tüzüğü kapsamında "pseudonymisation" terimiyle ifade edilen kavramın Türkçede karşılığı bulunmaması dolayısıyla çalışma kapsamında "bulanıklaştırma" teriminin kullanımı tercih edilmiştir.

mahremiyet ilkesi, tam işlevsellik ilkesi, uçtan uca güvenlik ilkesi, tam yaşam döngüsü koruması, görünürlük ve şeffaflık ilkesi ve son olarak kullanıcı odaklı tutum-kullanıcı mahremiyetine saygı ilkesi.

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

Veri Kontrolörüne Kurtuluş Hakkı: Veri Koruma Tüzüğü ile veri kontrolörü bakımından getirilen sorumluluğun sınırlarını belirlemek amacıyla kullanılan temel kavram "kullanıcıların makul beklentisi" olarak ifade edilmektedir. Şifreleme veya bulanıklaştırmayı dahi yetersiz bulan bir yaklaşımı ortaya koyan Veri Koruma Tüzüğü bakımından bu hüküm dikkat çekicidir. Veri kontrolörünün veriyi bulut hizmet sağlayıcısına vermeden önce şifrelemesi veya bulanıklaştırması, onu sorumluluktan kurtulabileceği anlamına gelmektedir. Zira herhangi bir veri ihlali durumunda şirketlerin kendi şifreleme anahtarlarını tutarak bireylerin veri gizliliği konusundaki "makul beklentilerini" karşılama konusunda gerekli adımları atmış olduklarını veri koruma otoritesine savunma olarak sunabilecekleri değerlendirilmektedir.

KAYNAKLAR

AKGÜL, A., "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın Google Kararı", *Türkiye Barolar Birliği Dergisi*, 2015, Sayı:116, ss. 11-39.

AKINCI, A. N., *Kişisel Veri Koruma Hukukunda Reform Hareketi: AB Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*, Kalkınma Bakanlığı Çalışma Raporu, Ankara, 2017.

ALTUNIŞIK, R., "Büyük Veri: Fırsatlar Kaynağı mı Yoksa Yeni Sorunlar Yumağı mı?", *Yıldız Social Science Review*, 2015, Vol.: 1, pp. 45-76.

ANDERSON, C., "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete", 2008, (çevrimiçi) https://www.wired.com/science/discoveries/magazine/16-07/pb_theory, 12.07.2016.

ARSLAN, H., "Amerika ile Avrupa Birliği Hukuki Düzenlemelerinin Gizlilik Haklarına Bakış Açısının Karşılaştırılması", *X. Türkiye'de İnternet Konferansı*, 2005, (çevrimiçi) http://inet-tr.org.tr/inetconf10/bildiri/18.doc, 21.07.2016.

ASHFORD, W., "GDPR will require 75.000 DPOs worldwide, study shows", *Computer Weekly*, 2016, (çevirimiçi) http://www.computerweekly.com/news/450402719/GDPR-will-require-75000-DPOs-worldwide-study-shows, 21.07.2017.

AT KEARNEY, "Big Data and the Creative Destruction of Today's Business Models", 2013'ten, SCHUMPETER, J.A., *Capitalism, Socialism and Democracy*, Taylor & Francis e-Library Edition (2003), 1943.

ATKINSON, G. M., D. J. WALD, ""Did you feel it?" Intensity data: A surprisingly good measure of earthquake ground motion", *Seismological Research Letters*, Vol.: 78(3), 2007, pp. 362-368.

AVRUPA BİRLİĞİ VERİ KORUMA KOMİSERLİĞİ, "Opinion on Privacy and Competitiveness in the Age of Big Data", 2014, (çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf, 05.05.2016 .

AVRUPA KOMİSYONU, *The EU Data Protection Reform and Big Data-Factsheet*, 2015.

BİRLEŞMİŞ MİLLETLER İNSAN HAKLARI YÜKSEK KOMİSERLİĞİ, *Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler, 1990, (çevrimiçi)* http://www.refworld.org/pdfid/3ddcafaac.pdf, 27.05.2017.

BORGESIUS, F. J. Z., 'Informed Consent: We Can Do Better to Defend Privacy', *IEEE Security and Privacy*, 2015, Vol.: 13, pp. 103-107.

BOWKER, G. C., S. L. STAR, *Sorting Things Out: Classification and Its Consequences*, The MIT Press, 2000.

BOZKURT YÜKSEL, A. E., *Bulut Bilişimde Kişisel Verilerin Korunması*, Yetkin Kitabevi, Ankara, 2016.

BRILL, J., “Big data, big issues”, *Fordham University School of Law*, 2012, (çevrimiçi) http://www.ftc.gov/public-statements/2012/03/big-data-big-issues, 20.05.2016.

BRUMLEY, J., “Google just became a real problem for online travel agents”, 2014, (çevrimiçi) http://investorplace.com/2014/04/goog-stock-google-travel-booking/#.VCPn_Pl_veg, 25.07.2017.

BRYNJOLFSSON, E., L. M. HITT, H. H. KIM, “Strength in Numbers: How Does Data Driven Decisionmaking Affect Firm Performance?”, 2011, (çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486, 20.01.2017.

CATE, F. H., P. CULLEN, V. MAYER-SCHÖNBERGER, “Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines”, *Oxford University*, Oxford, 2014.

CHEN, G. G., T. G. WONG, “August Waiting for China’s Data Protection Law:The lack of a unified legal framework may hamper China’s ongoing digitalization drive”, 2017, (çevrimiçi) https://thediplomat.com/2017/08/waiting-for-chinas-data-protection-law, 29.08.2017.

CHEN, M., S. MAO, Y. ZHANG, V. C. M. LEUNG, “Big Data: A Survey”, *Mobile Networks and Applications*, April 2014, Vol.: 19, Issue 2, pp. 171-209.

CHEN, R., M. LAZER, *Sentiment analysis of twitter feeds for the prediction of stock market movement*, Stanford, 2013.

CITRON, D. K., “Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age”, *Southern California Law Review*, Vol.: 80(2), 2007, pp. 241-297.

CRAIG, T., M.E. LUDLOFF, *Privacy and Big Data: The Players, Regulators, and Stakeholders*, O'Reilly Media, 2011.

CUKIER, K. N., "Data, data everywhere: A special report on managing information", *The Economist Newspaper*, 2010.

CUKIER, K. N., V. MAYER-SCHÖNBERGER, “The Rise of Big Data: How It’s Changing the Way We Think About the World”, *Foreign Affairs*, 2013, (çevrimiçi) http://www.foreignaffairs.com/articles/2013-04-03/rise-big-data, 21.08.2016.

ÇİĞDEM, Ş., H. İ. SEYREK, “İşletmelerde Büyük Veri Uygulamaları: Bir Literatür Taraması”, *2. Ulusal Yönetim Bilişim Sistemleri Kongresi*, Kongre Bildirisi, Erzurum, 2015.

DALTON, A., “Google and Facebook Team Up on a Direct Connection to Asia”, 2016, (çevrimiçi) https://www.engadget.com/2016/10/12/google-facebook-direct-connection-to-asia, 30.10.2016.

DANIELS, B. L., “Big data, big trouble? Privacy and legal concerns with big data”, *Pillsbury Winthrop Shaw Pittman LLP*, 2013, (çevrimiçi), http://www.lexology.com/library/detail.aspx?g=027d46af-e621-4714-8da4-27c07f7ee6e0, 21.06.2016.

DAVENPORT, T., *Big Data @Work*, Türk Hava Yolları Yayınları, İstanbul, 2014.

DAVENPORT, T. H., P. BARTH, R. BEAN, "How "big data" is different", *MIT Sloan Management Review*, 2012, Vol.: 54(1), pp. 43-46.

DEBATIN. B.. J. P. LOVEJOY, M. A. ANNE-KATHRIN HORN, B. N. HUGHES, "Facebook and Online Privacy: Attitudes. Behaviors and Unintended Consequences", *Journal of Computer-Mediated Communicatio*, 2009, Vol.: 15(1), pp. 83-108.

DEMCHENKO, Y., "Addressing Big Data Issues in the Scientific Data Infrastructure", 2013, (çevrimiçi) https://tnc2013.terena.org/includes/tnc2013/documents/bigdata-nren.pdf, 12.07.2016.

DEVLET PLANLAMA TEŞKİLATI, Sekizinci Beş Yıllık Kalkınma Planı (2001-2005), Ankara, 2001.

DEVLET PLANLAMA TEŞKİLATI, e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003-2004), Ankara, 2003.

DEVLET PLANLAMA TEŞKİLATI, Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010), Ankara, 2006.

DIAB, R. S., "Becoming-Infrastructure: Datafication, Deactivation, and the Social Credit System.", *Journal of Critical Library and Information Studies,* 2017, Vol.:1(1), pp. 1-23.

DIGITALEUROPE, *Energy Big Data Analytics "Unlocking the benefits of Smart metering and Smart Grid Technologies",* Brüksel, 2015.

DRIDI, A., S. SASSI, A. TISSAOUI, *Big Data in Complex Systems: Challenges and Opportunities,* Springer International Publishing, 2015.

DRUM, K., "Privacy is dead. Long live transparency!", 2013, (çevrimiçi) http://www.motherjones.com/politics/2013/10/future-of-privacy-nsa-snowden, 11.07.2017.

DWORK, C., D. K. MULLIGAN, "It's Not Privacy, and It's Not Fair", 2013, (çevrimiçi) https://www.stanfordlawreview.org/online/privacy-and-big-data-its-not-privacy-and-its-not-fair, 11.07.2017.

EDWARDS, L., "Privacy, security and data protection in smart cities: a critical EU law perspective", *European Data Protection Law Review (Lexxion)*, 2016, pp. 1-37.

ENGELS, B., "Data Portability among Online Platforms", *Internet Policy Review*, Vol.: 5(2), 2016, pp. 1-5.

ERL, T., KHATTAK, W., BUHLER, P., "Big Data Fundamentals: Concepts, Drivers & Techniques", Prentice Hall PTG, 2016.

EXECUTIVE OFFICE OF THE PRESIDENT, UNITED STATES (EOP), "Big data and differential pricing", 2015, (çevrimiçi) www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf, 06.09.2016.

FIELDFISHER, "Will access to midata work?", 2012, (çevrimiçi) http://www.fieldfisher.com/publications/2012/12/tech-bytes-technology-law-newsletter#sthash.UrY4J0ao.PzZLwmaB.dpbs, 08.08.2017.

FISHLEIGH, J., "A Non-Technical Journey into the World of Big Data: an Introduction", *Legal Information Management*, 2014, pp. 149-151.

FRIEDMAN, U., "Big data: A short history", 2012, (çevrimiçi) http://foreignpolicy.com/2012/10/08/big-data-a-short-history, 11.07.2016.

FEDERAL TRADE COMISSION, "Protecting Consumer Privacy in an Era of Rapid Change: a Proposed Framework for Businesses and Policymakers", 2010, (çevrimiçi) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf, 17.07.2017.

GANZ, J., D. REINSEL, "Extracting Value from Chaos", *IDC iView*, 2011, pp. 1-12.

GONÇALVES, A. S. S., "The Cross Border Regulation of Online Data Privacy and the Judicial Cooperation", *Jusletter IT*, 2015, pp. 6-10.

GREENAWAY, K., S. ZABOLOTNIUK, A. LEVIN, "Privacy as a risk management challenge for corporate practice", *Ted Rogers School of Management, Ryerson University, Privacy and Cyber Crime Institute*, 2012, (çevrimiçi) www.ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf, 10.08.2017.

GRILL, A., "Using Big Data to Fight Crime and Predict What Products Consumers Might Purchase in the Future", 2013, (çevrimiçi) https://londoncalling.co/2013/04/using-big-data-to-fight-crime-and-predict-what-products-consumers-might-purchase-in-the-future, 21.11.2016.

GÜR, İ., *Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları*, Ankara, Turhan Kitabevi, 2010.

GÜRSAKAL, N., *Büyük Veri*, Dora Yayın, 2. Baskı, Bursa, 2014.

HENKOĞLU, T., *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Yetkin Yayınları, Ankara, 2015.

IDC, *Worldwide Semiannual Big Data and Analytics Spending Guide*, 2016, (çevrimiçi) https://www.idc.com/getdoc.jsp?containerId=IDC_P33195, 21.07.2017.

IDC, *Data Age 2025: The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big*, IDC White Paper, 2017, (çevrimiçi) https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf, 21.03.2017.

JIN, X., B. W. WAH, X.CHENG, Y. WANG, "Significance and Challenges of Big Data Research", *Big Data Research*, 2015, Vol.: 2, pp. 59-64.

JOHNSON, D., J. HENDERSON-ROSS, "The new data values", 2012, (çevrimiçi) www.aimia.com/content/dam/aimiawebsite/CaseStudiesWhitepapersResearch/english/WhitepaperUKDataValuesFINAL.pdf, 08.08.2017.

KALKINMA BAKANLIĞI, Bilgi Toplumu Stratejisi'nin Hazırlanması Projesi İhtiyaç Tespiti ve Öneriler Raporu, Ankara, 2013.

KALKINMA BAKANLIĞI, Onuncu Kalkınma Planı (2014-2018), Ankara, 2014.

KALKINMA BAKANLIĞI, Bilgi Toplumu Stratejisi ve Eylem Planı (2015-2018), Ankara, 2015a.

KALKINMA BAKANLIĞI, 2015 Yılı Programı, Ankara, 2015b.

KALKINMA BAKANLIĞI, 2016 Yılı Programı, Ankara, 2016.

KAYA, C., *İdare Hukukunda Bilgi Edinme Hakkı*, Seçkin Yayınları, Ankara, 2005.

KAYABAY, K. , M. O. GÖKALP, M. A. AKYOL, P. E. EREN, A. KOÇYİĞİT, "Geleceğin Kuruluşları İçin Büyük Veri: Mevcut Durum ve Eğilimler", *METU Informatics Institute*, 2016, (çevrimiçi) https://www.researchgate.net/profile/Kerem_Kayabay/publication/309635166_Big_Data_for_Future_Enterprises_Current_State_and_Trends/links/581afda608aeffb29414489b/Big-Data-for-Future-Enterprises-Current-State-and-Trends.pdf, 12.12.2016.

KILINÇ, D., "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *AÜHFD*, 2012, Sayı: 61 (3), Ankara, ss. 1089-1169.

KRISHNAMURTHY, B., K. NARYSHKIN, C. E. WILLS, "Privacy leakage vs. Protection measures: the growing disconnect", *AT&T Labs and Worcester Polytechnic Institute*, 2011, pp.1-10.

KSHETRI, N., "Big data's impact on privacy, security and consumer welfare", *Telecommunications Policy*, 2014, Vol.: 38, pp. 1134-1145.

KULEVSKA, S., "The Future of Your Past: A Right to be Forgotten Online?", 2013, (çevrimiçi) https://lumendatabase.org/blog_entries/521, 10.07.2017.

KÜZECİ, E., *Kişisel Verilerin Korunması*, Ankara, Turhan Kitabevi, 2010.

MARR, B., "3 Massive Big Data Problems Everyone Should Know About", 2017, https://www.forbes.com/sites/bernardmarr/2017/06/15/3-massive-big-data-problems-everyone-should-know-about/2/#39d5dfe75fcf, 21.06.2017.

MAYER-SCHÖNBERGER, V., *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2011.

MAYER-SCHÖNBERGER V., K.CUKIER, *"Big Data (A Revolution That Will Transform How We Live, Work and Think)"*, Houghton Mifflin Harcourt Publishing, New York, 2013.

McAFEE, A., E. BRYNJOLFSSON, "Big Data: The Management Revolution", *Harvard Business Review*, 2012, Vol.: 90 (10), pp. 60-68.

McDONALD, A. M., L. F. CRANOR, " The cost of reading privacy policies", *A Journal of Law and Policy for the Information Society*, Privacy Year in Review, 2008, (çevrimiçi) http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf, 21.07.2017.

McGEE, M., "German Government Says Google Analytics Now Verboten", *Search Engine Land*, 2011, (çevrimiçi) http://searchengineland.com/german-govt-says-google-analytics-now-verboten-61109, 26.07.2016.

McKINSEY GLOBAL INSTITUTE, *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, 2011.

MORABITO, V., *Big Data and Analytics: Strategic and Organizational Impacts*, Springer, 2015.

NARAYANAN, A., V. SHMATIKOV, "How To Break Anonymity of the Netflix Prize Dataset", *The University of Texas at Austin*, 2007, (çevrimiçi) https://archive.org/stream/arxiv-cs0610105/cs0610105_djvu.txt, 05.06.2016.

OECD, *The OECD Privacy Framework*, OECD Publications, Paris, 2013.

OECD-International Transport Forum, *Big Data and Transport: Understanding and assessing options*, 2015.

OECD*, Digital Economy Outlook*, 2017.

OFFICE OF SCIENCE AND TECHNOLOGY POLICY, *Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*, 2010, (çevrimiçi) https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-health-it-release.pdf, 10.12.2016.

OFFSEY, S., "Micro-segmentation in the age of big data", 2014, (çevrimiçi) http://marketbuildr.com/blog/segmentationin-the-age-of-big-data, 11.12.2016.

OHM, P., "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review*, 2009, Vol.: 57, 1701-1777.

OHM, P., "Changing Rules: General Principles for Data Use and Analysis", *Privacy, Big Data and the Public Good,* Cambridge University Press, 2016.

ÖZBİLGİN, İ. G., "Kamuda Büyük Veri ve Uygulamaları", Anadolu Üniversitesi, *Akademik Bilişim Konferansı*, 2015, (çevrimiçi) http://ab.org.tr/ab15/bildiri/483.pdf, 20.01.2017.

ÖZBUDUN, E., "Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği", *Ankara Hukuk Fakültesi Ellinci Yıl Armağanı*, Sevinç Matbaası, Ankara, 1997.

PEARSON, S., M. C. MONT, "Sticky Policies: An Approach for Managing Privacy across Multiple Parties", *IEEE*, 2011, Vol.: 44(9), pp. 60-68.

PROVOST, F., T. FAWCETT, "Data science and its relationship to big data and data driven decision making", *Data Sci. Big Data.*, 2013, pp. 51-59.

RAJANIEMI, H., *The Quantum Thief*, Orion Publishing, London, 2010.

RICHARDS, N. M., J. H. KING, "Big Data Ethics", *Wake Forest Law Review*, 2014, pp.1-40.

ROBIN, F., "The Emerging Market that Could Kill the iPhone", *Fortune*, 2012, (çevrimiçi) http://fortune.com/2012/08/01/the-emerging-market-that-could-kill-the-iphone, 29.07.2016.

RUBINSTEIN, I. S., "Big Data: The End of Privacy or a New Beginning?", *New York University School of Law, Public Law & Legal Theory Research Paper Series*, Working Paper No: 12-56, 2012.

SCHULTZ, T., "Turning healthcare challenges into big data opportunities: a use-case review across the pharmaceutical development lifecycle", *Bull. Am. Soc. Inf. Sci. Technol*., 2013, Vol.: 39(5), pp. 34-40.

STEVENS H., L. FEARNLEY, S. SUN, S. WATSON, "Big Data in Asian Society: Provocations and Potentials", *Nanyang Technical University*, 2016, (çevrimiçi) http://bigdatasoc.blogspot.com.tr/p/essays-and-provocations.html, 01.04.2017.

STRANDBURG, K. J., "Monitoring, Datafication, and Consent: Legal Approches to Privacy in the Big Data Context", *Privacy, Big Data and the Public Good,* Cambridge University Press, 2016.

TENE, O., J., POLONETSKY, "Big Data for All: Privacy and User Control in the Age of Analytics", *Northwestern Journal of Technology and Intellectual Property*, 2013, Vol.: 11(5), pp. 240-272. (2013a)

TENE, O., J., POLONETSKY, "Judged by The Tin Man: Individual Rights in The Age of Big Data", *J. on Telecomm. & High Tech. L.,* 2013, pp. 351-368. (2013b)

TUFEKCI, Z., "Engineering the Public: Big Data, Surveillance and Computational Politics", *First Monday*, 2014, Vol.: 19(7), pp. 1-39, (çevrimiçi) http://firstmonday.org/article/view/4901/4097, 20.09.2016.

ÜNAL, F., *Büyük Veri ve Semantik*, Abaküs Yayın, İstanbul, 2015.

VASHIST, R., "Cloud Computing Infrastructure for Massive Data: A Gigantic Task Ahead", *Springer Studies in Big Data*, 2015, Vol.: 9, pp. 1-29.

VERGANTI, R., *Design Driven Innovation*, Harvard Bussiness Press*,* 2009.

WATSON, S. M., "Data is the new '___'", 2016, (çevrimiçi) http://dismagazine.com/discussion/73298/sara-m-watson-metaphors-of-big-data, 21.06.2016.

WORLD ECONOMIC FORUM, *Unlocking the Value of Personal Data: From Collection to Usage*, Geneva, 2013, (çevrimiçi) http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf, 23.06.2016

WYCKOFF, A., "Re-booting government as a bridge to the digital age", 2017, (çevrimiçi) http://www.oecd.org/internet/re-booting-government-as-a-bridge-to-the-digital-age.htm, 21.10.2017.

YÜKSEL CİVELEK, D., *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, DPT Uzmanlık Tezi, Ankara, 2011.

Mevzuat

Türkiye Cumhuriyeti Anayasası (09/11/1982 tarih, 17863 sayılı T.C. Resmi Gazete)

4721 sayılı Türk Medeni Kanunu (8/12/2001 tarih, 24607 sayılı T.C. Resmi Gazete)

4982 sayılı Bilgi Edinme Kanunu (24/10/2003 tarih, 25269 sayılı T.C. Resmi Gazete)

5070 sayılı Elektronik İmza Kanunu (23/1/2004 tarih, 25355 sayılı T.C. Resmi Gazete)

5237 sayılı Türk Ceza Kanunu (12/10/2004 tarih, 25611sayılı T.C. Resmi Gazete)

5271 sayılı Ceza Muhakemesi Kanunu (7/12/2004 tarih, 25673 sayılı T.C. Resmi Gazete)

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (23/05/2007 tarih, 26530 sayılı T.C. Resmi Gazete)

5809 sayılı Elektronik Haberleşme Kanunu (10/11/2008 tarih, 27050 sayılı T.C. Resmi Gazete)

6698 sayılı Kişisel Verilerin Korunması Kanunu (7/4/2016 tarih, 29677 sayılı T.C. Resmi Gazete)

Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik, (01/06/2005 tarih, 25832 sayılı T.C. Resmi Gazete)

Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik (14/02/2007 tarih, 26434 sayılı T.C. Resmi Gazete)

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (28/10/2017 tarih, 30224 sayılı T.C. Resmi Gazete)

Yararlanılan Yargı Kararları

Avrupa Birliği Adalet Divanı, Karar C-131/12, Google Spain SL ve Google Inc. v Agencia Española de Protección de Datos (AEPD) ve Mario Costeja González, Adalet Divanı (Grand Chamber) of 13 Mayıs 2014, ECR [2014] 317, parag. 32-41

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

Avrupa Birliği Adalet Divanı, Karar C-362/14, Maximillian Schrems v. Data Protection Commissioner yargılaması, 6 Ekim 2015, ECLI:EU:C:2015:650

Yararlanılan diğer çevrimiçi kaynaklar

http://www.tbmm.gov.tr

http://www.anayasa.gov.tr

http://yte.bilgem.tubitak.gov.tr

http://eur-lex.europa.eu

http://www.unicode.org/standard/WhatIsUnicode.html

http://www.cognizant.com

http://ec.europa.eu

http://europa.eu

https://ec.europa.eu/digital-single-market/

https://www.big-data-europe.eu

https://www.big-project.eu/

https://www.statista.com

https://iclg.com

https://gizmodo.com

https://www.big-project.eu

https://unstats.un.org/bigdata

http://www.unglobalpulse.org/projects

http://www.itu.int/en

DİZİN

A

AB · xii, 1, 2, 3, 36, 42, 44, 47, 48, 49, 50, 51, 59, 68, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 82, 83, 84, 85, 86, 87, 89, 90, 91, 92, 93, 96, 97, 98, 100, 101, 103, 105, 106, 107, 114, 115, 120, 128, 133, 135, 138, 139, 140, 141, 142, 145, 146, 147, 148, 149, 150, 152, 153, 154, 155, 156, 157, 159, 160, 161, 162, 166, 167, 168, 171, 173, 176
ABD · xii, 1, 2, 10, 16, 19, 23, 24, 29, 30, 31, 37, 41, 44, 47, 53, 58, 68, 73, 74, 87, 88, 89, 96, 102, 105, 106, 108, 109, 110, 112, 113, 120, 128, 129, 149, 150, 151, 153, 154, 168, 176
algoritma · ii, 18, 99, 102
anayasa · 56, 88, 141, 181
anonim · xv, 36, 41, 44, 67, 133, 136
Avrupa İnsan Hakları Sözleşmesi · xii, 57
Avrupa Konseyi · 3, 58, 60, 61, 63, 71

B

bağımsız · xv, xvi, 59, 63, 85, 105, 108, 109, 127, 133, 166
bilgi güvenliği · 130, 131
Bilgi Toplumu · i, xii, 54, 130, 177
bilgi ve iletişim teknolojileri · ii
Birleşmiş Milletler · xii, xiii, 49, 51, 52, 57, 60
BİT · xii, 1, 13, 22, 25, 27, 32, 52, 58, 60, 68, 88, 89, 131, 133, 154, 156, 157
bulanıklaştırma · xv, 81, 90, 92, 171

D

dijital · ii, 1, 2, 4, 6, 17, 35, 46, 51, 73, 78, 80, 87, 113, 114, 116, 121, 122, 126, 153, 160, 166

E

e-devlet · 90, 130
e-ticaret · 15, 18, 42, 90, 121

H

hassas kişisel veri · 34, 89, 90, 165

K

Kişisel Verilerin Korunması Kanunu · 130, 132, 133, 134, 137, 138, 139, 143, 154, 180

M

M2M · xiii, 30, 68
mahremiyet artırıcı teknolojiler · xv, 92, 109

N

nesnelerin interneti · 6, 12, 42, 43, 54, 76, 114, 119, 136

O

OECD · 2, 3, 36, 37, 47, 48, 58, 63, 64, 66, 67, 69, 70, 71, 87, 108, 114,

115, 116, 117, 118, 119, 121, 122, 123, 125, 126, 127, 129, 147, 152, 153, 155, 156, 157, 174, 178
otomatik · 7, 46, 58, 61, 62, 64, 79, 91, 100, 101, 102, 134, 144, 153, 161, 162, 170

S

sınır ötesi · 3, 60, 61, 63, 83, 114, 133, 146, 157

V

veri ekonomisi · 87
Veri Koruma Direktifi · 71, 72, 75, 79, 91, 161, 162, 163, 165
Veri Koruma Tüzüğü · xiii, 48, 72, 74, 75, 77, 78, 79, 80, 81, 82, 83, 84, 85, 87, 89, 92, 94, 96, 97, 98, 101, 106, 107, 108, 120, 128, 134, 138, 139, 140, 141, 142, 148, 150, 153, 155, 166, 167, 168, 169, 170, 171, 172, 173
veri madenciliği · 11, 12, 36, 53, 56, 66, 92
veri mahremiyeti · ii, 2, 3, 22, 41, 45, 56, 57, 63, 66, 67, 89, 105, 109, 112, 147, 149
veri sorumlusu · 90, 135, 139

Y

yazılım · 5