

İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

BÜYÜK VERİ ÇAĞINDA KİŞİSEL VERİLERİN KORUNMASI: AVRUPA
BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ'NDE PROFİLLEME VE
OTOMATİK KARAR ALMA DÜZENLEMELERİ

İrem YALÇINKAYA ÖZDAMAR
117692023

Prof. Dr. Leyla KESER BERBER

İSTANBUL
2022

Büyük Veri Çağında Kişisel Verilerin Korunması: Avrupa Birliği Genel Veri
Koruma Tüzüğü'nde Profilleme ve Otomatik Karar Alma Düzenlemeleri

Protection of Personal Data in the Age of Big Data: Profiling and Automated
Decision Making Under the European Union General Data Protection Regulation

İrem YALÇINKAYA ÖZDAMAR

117692023

Tez Danışmanı : **Prof. Dr. Leyla KESER BERBER**
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Dr. Öğr. Üyesi Mehmet Bedii KAYA**
İstanbul Bilgi Üniversitesi

Dr. Öğr. Üyesi Sezen KAMA IŞIK
İstanbul Medeniyet Üniversitesi

Tezin Onaylandığı Tarih : 26.07.2022

Toplam Sayfa Sayısı : 303

Anahtar Kelimeler (Türkçe)

- 1) Kişisel Veri
- 2) Genel Veri Koruma Tüzüğü
- 3) Profilleme
- 4) Otomatik Karar Alma
- 5) Kişisel Verilerin Korunması

Anahtar Kelimeler (İngilizce)

- 1) Personal Data
- 2) GDPR
- 3) Profiling
- 4) Automated Decision-Making
- 5) Personal Data Protection

ÖNSÖZ

2017 yılında başladığım Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, farklı disiplinlere ilişkin konular hakkındaki dersleriyle gerçek anlamda ufkumu açan bir deneyimdi. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün uygulanmaya başladığı bu dönemde, Tüzüğün profillemeye ve otomatik karar alma düzenlemelerinin uygulanabilirliği ve yeterliliğine ilişkin Avrupa'daki tartışmalar tez konumu belirlememde önemli bir etken oldu. Kişisel Verilerin Korunması Kanunu ile Tüzük arasında özellikle profillemeye ve otomatik karar alma düzenlemeleri açısından önemli farklılıklar bulunduğunu ve 95/46 Sayılı Direktif esas alınarak hazırlanan Kanun'un Tüzük ile uyumlaştırılma ihtiyacına ilişkin eleştirileri göz önüne alarak, bu alandaki çalışma ihtiyacına katkı sağlama motivasyonu ile profillemeye ve otomatik karar alma faaliyetlerini incelemeye karar verdim. Çalışmanın gerçekleştirilmesindeki cesaretlendirici yaklaşımı, ilgisi ve yönlendirmeleri için tez danışmanım Prof. Dr. Leyla Keser Berber'e, değerli eleştirileri ile tezime katkı sağlayan Dr. Sezen Kama Işık ve Dr. Mehmet Bedii Kaya'ya, manevi desteklerini sadece bu süreçte değil tüm hayatım boyunca hiçbir zaman esirgemeyen aileme, anlayışı ve sevgisiyle her daim yanımda olduğunu hissettiren eşim Alper Özdamar'a ve tüm bu süreçteki destekleyici tutumları için Akbank T.A.Ş. Hukuk Müşavirliğindeki yöneticilerime ve meslektaşlarıma en içten teşekkürlerimi sunarım. Çalışmanın tüm okuyuculara faydalı olması dileğiyle.

Av. İrem Yalçinkaya Özdamar

İÇİNDEKİLER

ÖNSÖZ	iii
İÇİNDEKİLER	iv
KISALTMALAR	viii
ÖZET.....	x
ABSTRACT.....	xi
GİRİŞ	1
1. PROFİLLEME VE OTOMATİK KARAR ALMA UYGULAMALARI AÇISINDAN KİŞİSEL VERİLERİN KORUNMASI	5
1.1. BÜYÜK VERİ	5
1.1.1. Büyük Veri Analitiği	6
1.1.2. Büyük Veri Analitiğinde Kullanılan Teknolojiler	7
1.1.3. Büyük Veri Analitiğinin Sağladığı Yarar	8
1.1.4. Büyük Veri Analitiğinde Kişisel Verilerin Kullanılması	10
1.1.5. Büyük Veri Analitiğinin Kişisel Verilerin Korunması Açısından Risk Oluşturan Özellikleri	12
1.2. YAPAY ZEKA	15
1.2.1. Yapay Zeka Nedir?	15
1.2.2. Yapay Öğrenme	17
1.2.3. Derin Öğrenme ve Yapay Sinir Ağları	20
1.2.4. Veri Madenciliği	21

1.3. PROFİLLEME VE OTOMATİK KARAR ALMA UYGULAMALARI	23
1.3.1. Grup Profillemeye ve Bireysel Profillemeye Ayrımı	25
1.3.1.1. Çevrimiçi İzleme Teknolojileri	31
1.3.2. Profillemeye ve Otomatik Karar Alma Uygulamalarının Kullanım Alanları	35
1.3.3. Profillemeye ve Otomatik Karar Alma Uygulamaları ile Edinilen Çıkarımların Kişisel Veri Kavramı Açısından Değerlendirilmesi	37
1.3.3.1. Kişisel Verilerin Korunması Mevzuatında “Kişisel Veri” Kavramı	37
1.3.3.2. Profillemeye ve Otomatik Karar Alma Uygulamaları ile Edinilen Çıkarımların Hukuki Niteliği	38
1.3.4. Avrupa Birliği Genel Veri Koruma Tüzüğü’ndeki Özel Tanımlar ve Düzenlemeler	48
1.3.5. Profillemeye ve Otomatik Karar Alma Uygulamalarının Birey Üzerindeki Olumsuz Etkileri	51
1.3.5.1. Kişisel Verilerin Korunması ve Mahremiyet Hakkına İlişkin Riskler	52
1.3.5.2. Algoritmik Önyargı ve Ayrımcılık	54
1.3.5.3. Caydırıcı Etki	60
1.3.5.4. Filtre Balonu Etkisi	62

2. KİŞİSEL VERİLERİN İŞLENMESİNE HAKİM OLAN İLKELER	65
2.1. PROFİLLEME VE OTOMATİK KARAR ALMA FAALİYETLERİ KAPSAMINDA KİŞİSEL VERİLERİN İŞLENMESİNE HAKİM OLAN İLKELER	65
2.1.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma	67
2.1.2. Doğru ve Gerekğinde Güncel Tutulma	70
2.1.3. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Edilme	77
2.1.4. Belirli, Açık ve Meşru Amaçlar için Toplanma ve İşlenme	83
2.1.5. Amaçla Bağlantılı, Sınırlı ve Ölçülü Veri İşleme	90
2.2. GENEL VERİ KORUMA TÜZÜĞÜ'NDE YER VERİLEN ÖZEL İLKELER	95
2.2.1. Hesap Verebilirlik İlkesi	95
2.2.2. Hesap Verebilirlik İlkesine Uyum Araçları	104
2.2.2.1. Veri Koruma Etki Değerlendirmesi	104
2.2.2.2. Veri Koruma Görevlisi	111
2.2.2.3. Tasarımdan İtibaren Veri Koruma ve Varsayılan Ayarlarla Veri Koruma İlkeleri	113
2.2.3. Şeffaflık İlkesi	122
2.2.3.1. Algoritmik Şeffaflık	123
3. ÖZEL DÜZENLEMELER, HUKUKA UYGUNLUK SEBEPLERİ, İLGİLİ KİŞİNİN HAKLARI	134

3.1. GENEL VERİ KORUMA TÜZÜĞÜ'NDE PROFİLLEME VE OTOMATİK KARAR ALMAYA İLİŞKİN ÖZEL DÜZENLEMELER	134
3.1.1. Profilleme de Dahil Olmak Üzere Tamamen Otomatik İşlemeye Dayalı Karar Alma	134
3.1.1.1. Tamamen Otomatik İşlemeye Dayalı Olma	140
3.1.1.2. Hukuki veya Benzer Şekilde Önemli Sonuçlar Doğurma	144
3.1.1.3. Çevrimçi Davranışsal Reklamcılık Faaliyetleri	148
3.1.1.4. Otomatik Karar Alma Faaliyetlerine İzin Verilen İstisnai Haller	152
3.1.1.5. Özel Nitelikli Kişisel Veriler	152
3.1.1.6. Uygun Tedbirler	153
3.1.1.7. Çocukların Profillenmesi	160
3.1.1.8. Güncel Mahkeme Kararları	164
3.2. HUKUKA UYGUNLUK NEDENLERİ	171
3.2.1. İlgili Kişinin Rızası	172
3.2.1.1. Açık Rıza	175
3.2.1.2. Profilleme ve Otomatik Karar Alma Faaliyetlerinde Rıza Şartlarının Uygulanabilirliği	178
3.2.2. Bir Sözleşmenin Kurulması veya İfası İçin Gerekli Olma	186
3.2.3. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Veri İşlemenin Zorunlu Olması	192

3.2.4. Veri Sahibinin veya Üçüncü Bir Gerçek Kişinin Hayati Menfaatlerinin Korunması İçin İşleme Faaliyetinin Gerekli Olması	194
3.2.5. Kamu Yararı İçin Gerçekleştirilen Bir Görevin Yerine Getirilmesi veya Veri Sorumlusunun Resmi Yetkisini Kullanması İçin Veri İşlemenin Gerekli Olması	195
3.2.6. Kişisel Verilerin İşlenmesinin Veri Sorumlusunun veya Üçüncü Bir Kişinin Meşru Menfaati için Gerekli Olması	196
3.3. İLGİLİ KİŞİNİN HAKLARI	204
3.3.1. İlgili Kişinin Bilgilendirilme Hakkı	205
3.3.2. İlgili Kişinin Erişim Hakkı	213
3.3.3. İlgili Kişinin Otomatik Kararların Açıklanmasını Talep Etme Hakkı	219
3.3.4. İlgili Kişinin Düzeltme Hakkı	234
3.3.5. İlgili Kişinin Kişisel Verilerin Silinmesini Talep Etme Hakkı	236
3.3.6. İlgili Kişinin İşlemeyi Kısıtlama Hakkı	240
3.3.7. İlgili Kişinin Veri Taşınabilirliği Hakkı	242
3.3.8. İlgili Kişinin İtiraz Hakkı	244
3.4. KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDA İLGİLİ DÜZENLEMELER	246
SONUÇ	254
KAYNAKÇA	267

KISALTMALAR

108 No'lu Sözleşme

108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması Sözleşmesi

(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)

95/46 Sayılı Direktif

95/46 Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korumasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data)

AB

Avrupa Birliği

ABAD

Avrupa Birliği Adalet Divanı

Bkz.

Bakınız

Direktif

95/46 Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korumasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

Divan

Avrupa Birliği Adalet Divanı

EDPB

European Data Protection Board
(Avrupa Veri Koruma Kurulu)

EDPS

European Data Protection Supervisor
(Avrupa Veri Koruma Gözetmeni)

EPRS	European Parliamentary Research Service (Avrupa Parlamentosu Arařtırma Servisi)
GVK Tüzüğü	Avrupa Birlięi Genel Veri Koruma Tüzüğü (<i>EU General Data Protection Regulation</i>)
ICO	Information Commissioner's Office (Birleşik Krallık Bilgi Komisyoneri Ofisi)
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
KVK Kanunu	6698 sayılı Kişisel Verilerin Korunması Kanunu
m.	Madde
OECD	Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
OECD Rehber ilkeleri	OECD'nin 1980 yılında yayınladığı Özel Yaşamın Gizliliğinin ve Sınır Ötesi Veri Akışının Korunmasına İlişkin Rehber İlkeler (<i>OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data</i>)
s.	Sayfa
Tüzük	Avrupa Birlięi Genel Veri Koruma Tüzüğü (<i>EU General Data Protection Regulation</i>)
vb.	Ve benzeri
vd.	Ve devamı

ÖZET

Yapay öğrenme algoritmaları günümüzde eğitim, sağlık, bankacılık ve öngörücü polislik gibi birçok farklı alanda profillemeye ve otomatik karar almada kullanılmaktadır. Yapay zeka tabanlı profillemeye ve otomatik karar sistemleri, gücünü yüksek oranda kişisel veri içeren büyük veriden alır. İşlenebilir verinin olağanüstü şekilde artması ve gelişmiş yapay öğrenme algoritmalarının ortaya çıkması bireylerin profillerinin çıkarılmasında ve bazı önemli kararların bu profillere dayanarak kayda değer bir insan müdahalesi olmaksızın tamamen otomatik bir şekilde alınmasına imkan tanımaktadır. Veri miktarındaki ve veri işleme kapasitesindeki artışın ekonomik büyümeye olan katkısı göz ardı edilemeyecek düzeydedir. Buna karşın, profillemeye ve otomatik karar alma faaliyetlerinin birey açısından olumsuz sonuçlarını ortaya koyan vakalar da son yıllarda hızla artmaktadır. Bu durum ise bireylerin, hayatları ile ilgili önemli konularda hatalı, önyargılı, ayrımcı sonuçlar doğuran profillemeye ve otomatik karar alma faaliyetlerine karşı korunmasına olan ihtiyacı artırmıştır. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde bu ihtiyaç gözetilerek, profillemeye ve otomatik karar alma da dahil olmak üzere veri işleme faaliyetlerinin şeffaf ve hesap verebilir olmasını sağlamak amacıyla, bazı özel düzenlemelere yer verilmiştir. Ancak Tüzüğün yürürlüğe girişi, bu düzenlemelerin profillemeye ve otomatik karar alma faaliyetleri açısından uygulanabilirliğine ilişkin tartışmaları da beraberinde getirmiştir. Çalışmada profillemeye ve otomatik karar alma faaliyetleri kişisel verilerin korunması hukuku perspektifinden değerlendirilmiştir. Bu kapsamda, 6098 Sayılı Kişisel Verilerin Korunması Kanunu'nun Tüzük ile uyumlaştırılması için yapılması gereken değişikliklere yön göstermesi amacıyla, Avrupa Birliği Genel Veri Koruma Tüzüğü esas alınarak, ilgili düzenlemelerin uygulanabilirliği ve yeterliliği incelenmiştir.

Anahtar Kelimeler: Kişisel Veri, Genel Veri Koruma Tüzüğü, Profillemeye, Otomatik Karar Alma, Kişisel Verilerin Korunması

ABSTRACT

Nowadays machine learning algorithms are used for profiling and automated decision making in many different fields such as education, health, banking and predictive policing. Artificial intelligence-based profiling and automated decision making systems are powered by big data which contain a high percentage of personal information. The enormous increase in usable data and the emergence of advanced machine learning algorithms allow for the profiling of individuals and important decisions being made based on these profiles in a fully automated manner without any meaningful human intervention. The contribution of the increase in the amount of data and data processing capacity to economic growth cannot be ignored. On the other hand, the number of cases revealing the negative consequences of profiling and automated decision-making activities in which big data are processed with artificial intelligence techniques has been increasing rapidly in recent years. This situation has increased the individuals' need to be protected against profiling and automated decision-making activities that create erroneous, biased and discriminatory results regarding important matters in their life. As a response to this need, EU General Data Protection Regulation has introduced specific provisions in order to ensure that data processing activities, including profiling and automated decision-making, are transparent and accountable. However, the entry into force of this regulation has brought with it debates on its applicability in terms of profiling and automated decision-making activities. In this thesis, profiling and automated decision-making activities are evaluated from the perspective of personal data protection law. In this context, the applicability and adequacy of the EU General Data Protection Regulation have been examined in order to guide the changes that need to be made to the Turkish Personal Data Protection Law No. 6098 to establish consistency between the two regulations.

Keywords: Personal Data, GDPR, Profiling, Automated Decision Making, Personal Data Protection

GİRİŞ

Teknolojik inovasyonların ekonomik büyümenin itici gücünü oluşturduğu bulunduğumuz yüzyılda, her hareketimiz bir dijital iz bırakmaktadır. Telekomünikasyon cihazlarının cep boyutuna gelerek kullanımının yaygınlaşması, “Nesnelerin İnterneti” kavramının doğması ve bulut bilişim teknolojisinin gelişmesi, dijital izlerimizi ciddi ölçüde artırarak “Büyük Veri” çağına girilmesi ile sonuçlanmıştır. Son yıllarda “Veri yeni petroldür” deyimini oldukça sık duyduğumuz popüler bir tabir haline gelmiştir. Öte yandan büyük veri uygun tekniklerle işlenerek içgörüyeye dönüştürülebildiği, diğer bir ifadeyle anlamlandırılabilirdiği ölçüde ekonomik değeri yaratabilmektedir. Ancak büyük verinin insan beyninin muhakeme kapasitesi ile anlamlandırılması mümkün değildir. Verinin katlanarak artmasıyla birlikte bilgi işlem gücünde hızlanma ve depolama maliyetlerindeki düşüş, veri analitiği teknolojilerinin gelişmesine zemin hazırlamıştır. Böylece günümüzde büyük veri yığınları, gelişmiş veri analitiği yöntemleri ve yapay öğrenme algoritmaları ile analiz edilebilmektedir. Yapay öğrenme algoritmaları ile insan zekası ile gerçekleştirilemeyecek şekilde, büyük miktarda verinin analiz edilmesi, bu veri kümelerindeki korelasyonların tespit edilmesi ve çıkarımlarda bulunabilmesi mümkün hale gelmiştir. Günümüzde otomatik veri işleme teknikleri ve algoritmalar, internet kullanıcılarının bilgiye ulaşmasını sağlamanın yanı sıra her geçen gün artan bir şekilde, önceden sadece insanlar tarafından karar verilen birçok konuda karar alınmasında kullanılmaktadır. Karar süreçlerinin algoritmalar ile desteklenmesiyle, eskiden insan zekasına dayanan kararlar yerini yapay zeka sistemleri ile verilen kararlara bırakmaya başlamıştır. Finans sektöründe bireylerin kredi puanının belirlenmesinde, insan kaynakları alanında işe alım süreçlerinde başvuruvcuların değerlendirilmesinde, sigorta risk priminin hesaplanmasında, tıp ve sağlık hizmetlerinde hastalıkların teşhisinde sıklıkla yapay zeka tabanlı sistemler kullanılmaktadır.

Algoritmalarla dayanan profillemeler ve otomatik karar alma faaliyetleri şirketlere, kamu kurumlarına ve bireylere birçok fayda sağlamakla birlikte, son yıllarda artan şekilde tartışma konusu edilen çeşitli sorunlara neden olmaktadır. Profillemeler ve otomatik karar alma faaliyetlerinde kullanılan yapay öğrenme algoritmalarının yakıtı büyük veri kümeleridir. Büyük veri ise çoğunlukla kişisel verilerden oluşur. Profillemeler ve otomatik karar alma sistemlerinin dayandığı algoritmalar genellikle, ilgili kişi tarafından sağlanan ya da ilgili kişi hakkında gözlemlenen kişisel verilerle eğitilir. Algoritmanın eğitildiği girdi verilerinin doğruyu ve gerçeği yansıtmaması, algoritmanın ürettiği çıktıları ciddi şekilde etkilemektedir. Buradaki esas endişe ise, bireylerin yanlış ve içinden çıkılması zor profiller altında kategorilendirilmesidir. Bireylerin doğruluğu veya güncelliği teyit ve kontrol edilemeyen çıkarımlara göre kategorize edilmesi, ayrımcılık ve sosyal eşitsizliğin artmasına neden olabilmektedir. Nitekim profillemeler ve otomatik karar alma sistemlerinin bireylerin ırk, etnik köken, cinsiyet, yaş, sosyo-ekonomik düzey gibi özellikleri üzerinden ayrımcılığa uğramalarına neden olduğunu gösteren sayısız vaka mevcuttur. Algoritmaların insan zihninin anlamlandıramayacağı şekilde karmaşık ve opak yapısı, profillemeler ve otomatik karar alma faaliyetleri gerçekleştirenler ile bu faaliyetlerden etkilenen bireyler arasında bir güç dengesizliği yaratmaktadır. Bu durum bireylerin kişisel verileri ve verilerinin işlendiği algoritmik sistemler üzerinde kontrol ve denetim imkanını kaybetmelerine, bu sistemlerin nasıl çalıştığını, kendileri hakkındaki çıkarımların nasıl gerçekleştirildiğini tam anlamıyla kavrayamamalarına neden olmaktadır. Bireyin yaşam hakkı, adil yargılanma hakkı, mahremiyet hakkı, ifade özgürlüğünün yanı sıra masumiyet karinesi, hukukun üstünlüğü ve insan onuru da profillemeler ve otomatik karar alma sistemlerinden olumsuz etkilenmektedir. Bu zararların tamamen ortadan kaldırılamasa bile nasıl en az seviyeye indirilebileceği en çok tartışılan konulardan biri olmuştur. Bireyler hakkında yapılan çıkarımların önyargılı, ayrımcı, adaletsiz veya herhangi bir şekilde yanlış olması, kişi hakkında verilen tek bir kararı etkileme potansiyelinin yanı sıra, bu çıkarımların yapay zeka sistemine girdi olarak kullanılarak kişi hakkında ileride verilecek farklı kararları etkileyebilme ihtimali sebebiyle de oldukça önemli bir problem haline gelmiştir.

Profilleme ve otomatik karar alma faaliyetlerinin yarattığı etik sorunların yanı sıra bu faaliyetlerin bireyin mahremiyeti, temel hak ve özgürlükleri ve kişisel verilerin korunması açısından olumsuz etkileri karşısında korunması için bu alanda yapılacak hukuki düzenlemeler oldukça önemli bir role sahiptir.

Kişisel verilerin korunması hukuku, büyük verinin, teknolojinin ve inovasyonun yarattığı katma değer ile bireyin temel hak ve özgürlükleri arasındaki dengeyi gözeterek, teknolojik inovasyonun ekonomik büyümeye olan faydasını engellemeden veri işleme faaliyetlerinin taraflarının hak ve yükümlülüklerinin belirlenmesini amaçlamaktadır. Profilleme ve otomatik karar alma faaliyetlerinin bugünkü kadar yaygın olmadığı dönemde yürürlükte olan 95/24 Sayılı Direktif'te profilleme ile ilgili açık bir tanım veya hükme yer verilmemiş olmakla birlikte, Direktif'in 15. maddesinde kişi üzerinde önemli etkisi olan otomatik işlemeye dayalı kararlara ilişkin bir düzenlemeye yer verilmiştir. Dijitalleşme ile birlikte üretilen verinin hızla artması ve teknolojik gelişmeler, profilleme ve otomatik karar alma faaliyetlerini de ciddi şekilde artırmıştır. GVK Tüzüğü'nde, büyük veri ve yapay zeka sistemlerinin bireyler açısından teşkil ettiği riskler gözetilerek, bireyin mahremiyet haklarının güçlendirilmesi amacıyla, profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetlerine yönelik bazı yeni düzenlemelere ve tanımlara yer verilmiştir. Ancak yapay zeka sistemlerinin doğasından ileri gelen özellikleri, kişisel verilerin korunmasına ilişkin düzenlemelerin uygulanabilirliği açısından çeşitli sorunlara neden olmaktadır. Bu bağlamda GVK Tüzüğü düzenlemelerinin, profilleme ve otomatik karar alma faaliyetleri açısından pratikte uygulanabilirliği ve bireylere yeterli koruma sağlayıp sağlamadığı konusunda süregelen tartışmalar bulunmaktadır. Türkiye'de ise kişisel verilerin korunmasına ilişkin ilk metin olan KVK Kanunu'nda ilgili kişiye "İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı" tanınmış olup, bu hak tamamen otomatik işlemeye dayalı karar almaya atıf yapılan tek düzenlemedir.

Çalışmanın birinci bölümünde, çalışmanın temelini oluşturan profilleme ve otomatik karar alma uygulamaları ile ilgili kavramsal çerçevenin çizilmesi

amacıyla, büyük veri analitiği, yapay zeka ve alt kavramları, profillemeye türleri, ilgili mevzuattaki özel tanımlar, veri türleri ve bu uygulamaların kişisel veri kavramı ile ilişkisi incelenmiştir. Bu bölümde ayrıca profillemeye ve otomatik karar alma uygulamalarının kullanım alanları, sağladığı yarar ve bireyler açısından olumsuz etkileri ele alınmıştır. Çalışmanın ikinci bölümünde kişisel verilerin işlenmesine hakim olan ilkeler, hesap verebilirlik ilkesine uyum araçları ve şeffaflık ilkesi profillemeye ve otomatik karar faaliyetleri bağlamında, öncelikli olarak GVK Tüzüğü düzenlemeleri ve ilgili noktalarda KVK Kanunu düzenlemelerine atıf yapılarak büyük verinin teşkil ettiği sorunlar ekseninde değerlendirilmiştir. Üçüncü bölümde ise GVK Tüzüğü'nün profillemeye ve otomatik karar alma faaliyetlerine ilişkin özel düzenleme niteliğindeki 22. maddesi incelenerek maddenin Avrupa'da farklı açılardan tartışmaya konu edilen belirsizlik ve boşlukları ele alınmıştır. Kişisel verilerin işlenmesinde hukuka uygunluk nedenleri ve ilgili kişinin hakları profillemeye ve otomatik karar alma faaliyetleri bağlamında incelenmiştir. Son olarak, Kişisel Verilerin Korunması Kanunu düzenlemeleri profillemeye ve otomatik karar alma faaliyetleri açısından ilişkin düzenlemeleri Tüzük hükümleri ile karşılaştırıldıktan sonra Kanun'da değişiklik önerisi sunulmuştur.

BİRİNCİ BÖLÜM

1. PROFİLLEME VE OTOMATİK KARAR ALMAUYGULAMALARI AÇISINDAN KİŞİSEL VERİLERİN KORUNMASI

1.1. BÜYÜK VERİ

1990'lı yılların sonu ile 2000'li yılların başlarında, internet teknolojisinin hızla gelişmesi ve maliyetlerin düşmesiyle dünya nüfusunun oldukça büyük bir kesimi internete erişim imkanına sahip hale gelmiştir. Dijital devrim, insanlığın tecrübe ettiği en büyük değişimi başlatmıştır. İnternete erişimin kolaylaşması ile eş zamanlı olarak bilgi ve iletişim teknolojilerinde yaşanan dönüşüm ve gelişim, dünya çapında üretilen verinin olağanüstü seviyede artmasıyla sonuçlanmıştır. Üretilen verinin artmasıyla eş zamanlı olarak bulut bilişim teknolojisinin gelişmesi, kayıt altında tutulan verinin katlanarak artmasını beraberinde getirmiştir. Böylece “Büyük Veri” kavramı hayatımıza girmiştir. Genel anlamda büyük veri, günümüzde daha önce mümkün olmayan yeni yöntemlerle verilerin toplanarak depolanabilmesi ve analiz edilebilmesini ifade eder¹. Bu bağlamda, büyük veri kavramının, teknik nitelikli bir ifadeden ziyade, veri işlemeye yönelik özel bir yaklaşım olduğu söylenebilir².

Büyük verinin en genel ve ilk kabul gören tanımı olan Gartner'in “3V” tanımı³, aslında üç ana öğeden oluşan büyük veri kavramının sadece bir bölümünü teşkil etmektedir. Büyük verinin tam anlamıyla kavranabilmesi, bu tanımın 3V (*volume-velocity-variety*) dışındaki diğer iki bölümünün de incelenmesi ile mümkündür. Bu bağlamda büyük veri kavramı, (i) büyük verinin üstün hacim, hız ve çeşitliliğe sahip veri yığınlarından oluşması, (ii) büyük veri kullanılarak

¹ Bernard MARR, Büyük Veri İş Başında (Çeviri: Başak GÜNDÜZ), İstanbul, 2019, s.11-12.

² Sezen KAMA IŞIK, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, On İki Levha Yayıncılık, 1. Baskı, İstanbul, 2018, s.178.

³ Gartner analisti Doug Laney'nin büyük veri tanımına atfettiği, “3 V/Three V's” ifadesi, büyük verinin en temel üç niteliğini betimleyen hacim (*volume*), hız (*velocity*) ve çeşitlilik (*variety*) özelliklerini belirtmektedir.

ulaşılmak istenen nihai hedefin, herhangi bir konuya ilişkin olarak iç görü edinmek ve karar almak olması, (iii) bu amaca yönelik olarak günümüzde büyük verinin uygun maliyetli ve yenilikçi veri işleme yöntemleri ile analiz edilebiliyor olması özelliklerinden oluşmaktadır⁴.

1.1.1. Büyük Veri Analitiği

Büyük verinin potansiyel değeri, herhangi bir konuda veriye dayalı karar alınmasına hizmet ettiği noktada ortaya çıkmaktadır. Büyük veriden katma değer yaratabilmek ve fayda sağlayabilmek, toplanan veriyi analiz edebilme becerisine bağlıdır. Bunun için, büyük verinin analiz edilerek bilgi dağarcığına kazandırılması, yani içgörüye (*insight*) dönüştürülmesi gerekir. Veri yığınlarının içgörüye dönüştürülmesi çeşitli süreçlerden geçirilmesini gerektirmektedir. Bu süreçler, veri yönetimi (*data management*) ve veri analitiği (*data analytics*) olmak üzere iki ana başlık altında incelenebilir⁵. Veri yönetimi, verinin toplanması, saklanması ve analize hazır hale getirilmesine hizmet eden süreç ve teknolojileri ifade eder⁶. Veri analitiği ise, büyük verinin analiz edilerek anlamlı bir bilgi ve içgörü edinilmesi için kullanılan birçok teknik ve yöntemi betimleyen genel bir ifade olarak tanımlanmaktadır⁷.

Veriden içgörü edinme süreci, verinin toplanması, verinin saklanması, verinin analiz edilmesi ve veriden elde edilen analiz sonuçlarının hedeflenen nihai amaç için kullanılması aşamalarından oluşur⁸. Verinin toplanması aşamasında,

⁴ Svetlana SICULAR, Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s, <https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/?sh=2c470e9b42f6>.

⁵ Amir GANDOMI & Murtaza HAIDER, Beyond the hype: Big data concepts, methods, and analytics, *International Journal of Information Management* 35(2):137-144, s.140, <https://doi.org/10.1016/j.ijinfomgt.2014.10.007>.

⁶ Gandomi & Haider, s.140.

⁷ Gandomi & Haider, s.140.

⁸ Ruben CASADO & Muhammed YOUNAS, "Emerging Trends and Technologies in Big Data Processing", *Concurrency and Computation Practice and Experience*, 27(8), 2014, s.9, https://www.researchgate.net/publication/266373455_Emerging_trends_and_technologies_in_big_data_processing.

dağıtık veri tabanları da dahil ancak bununla sınırlı olmamak üzere çeşitli kaynaklardan veriler toplanmaktadır⁹. İkinci aşama ise, toplanan verilerin ilerleyen aşamada işlenmesi veya analiz edilmesi için saklanmasıdır¹⁰. Saklanan bu veriler, çeşitli model, teknoloji ve algoritmaların kullanılması ile farklı sektörlerde farklı amaca yönelik analiz edilmektedir¹¹. Son aşama ise, veri yığınlarının analiz edilmesi aşamasında elde edilen sonuçlar ve yapılan gözlemler aracılığıyla içgörü edinilmesi, diğer bir ifadeyle veriden katma değer yaratılmasıdır. Bu aşamalar her zaman birbirini izleyen bir sırada gerçekleşmek zorunda değildir¹². Veri analizi, büyük veri ile ilgili çalışmaların en önemli aşamasını oluşturur. Veri analizi, toplanan veriden doğru, yararlı ve kullanılabilir olarak değerlendirilenleri ayıklandıktan sonra edinilen ham veriden, bir sonuç çıkarmak, tahminde bulunmak veya bir konuda karar almak suretiyle katma değer elde edilmesini ifade eder¹³. Veri analizi tür ve şekilden bağımsız olarak her çeşit veri üzerinde gerçekleştirilebilir. Veri, analiz sürecinde, ayrıştırma, temizleme, değiştirme ve görselleştirme gibi işlemlerden geçirilir¹⁴.

1.1.2. Büyük Veri Analitiğinde Kullanılan Teknolojiler

Büyük verinin oldukça büyük hacimli ve karmaşık yapıdaki yapılandırılmış, yarı-yapılandırılmış ve yapılandırılmamış veri yığınlarından oluşması, geleneksel veri analiz yöntemlerimin yetersiz kalmasına neden olmuştur. Büyük verinin çalışmanın ilgili bölümde açıklanan özellikleri, bu özelliklere uygun yeni metod, teknik ve teknolojilerin geliştirilmesini gerektirmiştir¹⁵. Günümüzde büyük veri analizinde, ulaşılmak istenen nihai amaca göre, farklı yapay zeka yöntem ve

⁹ Casado & Younas, s.9.

¹⁰ Casado & Younas, s.9.

¹¹ Casado & Younas, s.9.

¹² Casado & Younas, s.9.

¹³ Murat ÖZBAYOĞLU, “Derin Öğrenme ile Büyük ve Açık Veri Analizi”, Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar (Editörler: Şeref Sağıroğlu & Orhan Koç), 1.Baskı, Ankara, 2017, s.122, https://bigdatacenter.gazi.edu.tr/wp-content/uploads/buyuk_veri_ve_acik_veri_analitigi.pdf.

¹⁴ Rohit SHARMA, Data Mining vs. Data Analytics: Difference between Data Mining&Data Analytics, 15 Eylül 2020, <https://www.upgrad.com/blog/data-mining-vs-data-analytics/>.

¹⁵ Casado & Younas, s.4.

teknikleri kullanılmaktadır. Bunlar Metin Analitiği/Metin Madenciliği (*Text Analytics/ Text Mining*), Yapay Öğrenme (*Machine Learning*), Veri Madenciliği (*Data Mining*) Tahmine Dayalı Analitik (*Predictive Analytics*), Doğal Dil İşleme (*Natural Language Processing*), İstatistiksel Analiz (*Statistical Analysis*), Sosyal Ağ Analizi (*Social Network Analysis*), Görüntü İşleme (*Image Processing*), Örüntü Tanıma (*Pattern Recognition*) olarak sıralanabilir¹⁶. Büyük veri analiz edilmediği sürece herhangi bir faydaya sahip değildir. Bu teknolojilerin kullanılması suretiyle, büyük veri yığınlarının analiz edilip içgörüye dönüştürülerek değer yaratması sağlanmaktadır¹⁷. Bunların yanı sıra, Bulut Bilişim (*Cloud Computing*)¹⁸ ve Nesnelerin İnterneti (*Internet of Things*)¹⁹ teknolojileri de büyük verinin özelliklerine uygun veri toplama ve depolama imkanları sunarak büyük verinin gelişimine olanak sağlamıştır.

1.1.3. Büyük Veri Analitiğinin Sağladığı Yarar

Büyük veri, devletlere, kamu ve özel sektördeki farklı kurum ve kuruluşlara, farklı alanlarda faaliyet gösteren şirketlere, her geçen gün artan nispette fayda sağlamaktadır. Büyük veri yaşadığımız dünya ile ilgili birçok konuyu anlamlandırabilme imkanı sağlamaktadır²⁰. Büyük verinin en öne çıkan avantajı

¹⁶ Özbayoğlu, s.122

¹⁷ Ann CAVOUKIAN & Jeff JONAS, Privacy by Design in the Age of Big Data, 8 Haziran 2012, s.3, <https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf>.

¹⁸ Bulut bilişim (*cloud computing*), 3. kişilerce devasa çevrimiçi sunucuları aracılığıyla internet ortamında sunulan bir veri depolama hizmetidir. Günümüzde bulut bilişim altyapılı sistemleri, daha fazla depolama alanına erişim imkanı sağlamakla birlikte, veri transferini de hızlandırmaktadır. Bu bağlamda bulut tabanlı depolama çözümlerinin büyük veri ekosistemine en önemli faydası, depolama maliyetlerinde, iş gücünde ve zamanda tasarruf sağlamaktır. Diğer yandan, bulut tabanlı yazılımlar ile kullanıcılara güvenlik ihtiyaçlarına göre farklı depolama seçenekleri sunulmaktadır. Bunlar, genel bulut (*public cloud*), özel bulut (*private cloud*), topluluk bulut (*community cloud*) ve hibrit bulut (*hybrid cloud*) olarak sıralanabilir.

¹⁹ Nesnelerin interneti, akıllı cihaz ve sensörlerin internet aracılığıyla birbirleriyle bilgi paylaşacak şekilde ağlararası çalışmasını tanımlayan yeni bir paradigmayı ifade eder. Ethem ALPAYDIN, Yapay Öğrenme: Yeni Yapay Zeka (Çeviri: Aylin Ağar), Tellekt, 1.Baskı, Aralık 2020, İstanbul, s.23 (Kısaltılmışı “Yapay Öğrenme: Yeni Yapay Zeka”).

²⁰ Viktor MAYER-SCHÖNBERGER & Kenneth CUKIER, Büyük Veri-Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim, 1. Baskı, İstanbul, 2013, s.15.

ise hemen her sektörde sağladığı ekonomik menfaattir²¹. Zira büyük veri yığınlarının analizi, şirketlere müşterilerine, tüketicilere, organizasyon yapılarına, ürün ve hizmetlerine, faaliyet gösterdikleri sektöre ilişkin detaylı çıkarımlar edinilmesini sağlayarak ekonomik katma değer yaratır. Bu bağlamda büyük veri şirketler açısından önemli bir rekabet avantajı aracıdır²².

Bankacılık, finans, e-ticaret, havacılık, reklamcılık, enerji, lojistik, sigorta, sağlık gibi verinin anlık olarak analiz edilmesinin önem arz ettiği sektörlerde faaliyet gösteren şirket ve kuruluşlarca, büyük verinin analiz edilmesi suretiyle edinilen içgörü ve çıkarımları gözetilerek, “veriye dayalı” kararlar alınması mümkün hale gelmiştir. Günümüzde büyük veri yığınlarını gerçek zamanlı olarak analiz edebilen ve veriye dayalı kararlar alabilen şirket ve işletmeler veriden ekonomik değer yaratabilmektedir. Veriye dayalı kararlar, verimliliğinin artırılması, işletme maliyetlerindeki verimsizliklerinin tespit edilerek maliyet optimizasyonun sağlanması, müşteri memnuniyetinin ve sadakatının artırılması, veriye dayalı stratejiler geliştirilerek işletme performansının iyileştirilmesi, yeni ürün ve hizmetler ile yeni iş modellerinin geliştirilmesi, müşteri deneyiminin kişiselleştirilerek müşteri davranışlarının analiz edilebilmesi, müşteri sayısının artırılması, maliyetlerin azaltılması, karın artırılması, veri tabanlı pazarlama yapılması ve organizasyona bütüncül yaklaşım oluşturulması gibi birçok fayda sağlamaktadır²³.

Büyük verinin ekonomik faydasının yanında, devletlerin vatandaşlarına sağlık, toplu taşıma, eğitim, ulaşım gibi kamu hizmetlerini sağlamasına ilişkin de önemli faydaları bulunmaktadır. Farklı kaynaklardan elde edilen verilerin doğru şekilde analiz edilmesiyle, kamu hizmetlerinin vatandaşların ihtiyaçları gözetilerek bu ihtiyaçlardaki değişimlere cevap verecek şekilde tasarlanması ve böylece

²¹ Büyük verinin farklı sektörlerde faaliyet gösteren şirketlerdeki uygulamalarına ve sağladığı faydalara ilişkin detaylı bir çalışma için bkz. Bernard MARR, Büyük Veri İş Başında (Çeviri: Başak Gündüz), MediaCat Kitapları, Ekim 2019.

²² Mayer-Schönberger & Cukier, s.152-153.

²³ Fernando L.E. ALMEIDA, Benefits, Challenges and Tools of Big Data Management, Journal of Systems Integration, 2017/4, s.16, DOI:10.20470/jsi.v8i4.311.

vatandaşların eşit şekilde kamu hizmetlerinden faydalanması mümkün kılınmaktadır²⁴. Örneğin, açık hükümet (*open government*) politikasını benimseyen ülkelerde, vatandaşlara kurumlarla ilgili bilgilere açık erişim imkanı tanınarak vatandaş ile devlet ilişkisinde güven ve şeffaflığın tesis edilmesi sağlanmaktadır²⁵. Diğer yandan, sensör verilerinin analiz edilmesiyle şehirlerdeki trafik yoğunluğunu, hava ve çevre kirliliğini, belediye vasıtalarının lokasyon ve güzergahını, çöp kutularının kullanım oranını, asayiş bozacak davranışları tespit etmeyi sağlayan akıllı şehir (*smart city*) ve nesnelerin interneti uygulamaları, etkin kent yönetiminin sağlanmasının yanı sıra, vatandaşların hayat kalitesi ve güvenliğinin artırılmasında da olumlu etkiye sahiptir²⁶. Büyük veri ayrıca, politika belirleyici ve karar verici mercilere, geleneksel medyanın yanı sıra internet siteleri, bloglar, sosyal medya hesapları gibi yeni medya araçlarından edinilen verileri analiz ederek, vatandaşların ilgi alanlarını ve düşüncelerini dikkate alarak hangi kamu hizmetlerinin önceliklendirileceğine daha etkin bir şekilde karar verebilmelerine olanak sağlar²⁷.

1.1.4. Büyük Veri Analitiğinde Kişisel Verilerin Kullanılması

Büyük veri analitiğinin yakıtı olan veri yığınları, şirketlere ait ticari sır niteliğindeki veriler, kamu tüzel kişiliklerine ait veriler, istatistiki veriler, anonim veriler ve kamuya açık verilerin yanı sıra gerçek kişilere ait kişisel veriler de içerir. Bu bağlamda, bir veri analitiği faaliyeti kişisel verilerin işlenmesi ile ilgili olabileceği gibi, herhangi bir kişisel veri kullanılmadan da gerçekleştirilebilir. Günümüzde internetin, mobil cihazların, yeni medya araçlarının, sensörlerin, çevrimiçi alışveriş sitelerinin, video oyunlarının ve diğer çeşitli teknolojilerin

²⁴ Mehmet Bedii KAYA, “Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge”, Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku (Editörler: Keser Berber & Bilgili), 1.Baskı, İstanbul, 2020, s.53 (Kısaltılmışı “Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge”).

²⁵ Ricard Munne, “Big Data in the Public Sector”, New Horizons for a Data Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe (Editörler: José María Cavanillas, Edward Curry, Wolfgang Wahlster), Springer Open, 2016, s.195, <https://link.springer.com/content/pdf/10.1007%2F978-3-319-21569-3.pdf>.

²⁶ Munne, s.196.

²⁷ Munne, s.195.

dünya nüfusunun önemli bir kısmı tarafından yoğun şekilde kullanılması, büyük veri yığınlarındaki kişisel veri oranını her geçen gün artırmaktadır. Büyük veri yığınları kişisel veriden ne kadar arındırılırsa, araştırma ve analitik faaliyetleri ile hedeflenen yararın da bir o kadar azaldığı belirtilmektedir²⁸. Diğer yandan, büyük veri, kişilerle ilgili bilgi edinmek ve onlar hakkında kararlar almak için gerçekleştirilen analitik uygulamalarının yanı sıra, sadece bazı genel eğilimlerin belirlenmesi için de kullanılabilir²⁹. Şehirlerdeki toplu taşıma güzergahlarının planlanabilmesi için, metro ve otobüslere binmek için kullanılan kartlardan edinilen ilgili kişilere ait seyahat ve ulaşım verilerinin, trafik verileri ile eşleştirilmesi buna örnek olarak gösterilebilir³⁰.

Büyük veri yığınlarını oluşturan veriler, kaynağından ilk edinilme anında kişisel veri niteliğinde olabileceği gibi, ilk edinilme anında anonim veri veya istatistiksel veri niteliğinde olmasına rağmen, yapay zeka teknikleri kullanılarak başka veriler ile eşleştirilmek veya desteklenmek suretiyle de kişisel veri niteliği kazanabilmektedir³¹. Bu bağlamda, büyük veri uygulamaları ile işleme tabi tutulan verilerin veya edinilen sonuçların kişisel verilerin korunması kapsamına girip girmediğinin tespiti için yapılacak değerlendirmede, ilgili bölümdeki kişisel veri kavramı ve unsurları ile ilgili açıklamalarımız dikkate alınmalıdır³². Öte yandan, örneğin, bir kimsenin sosyal medya hesaplarından toplanan veriler, kişinin yaşam tarzı hakkında bilgi edinmek ve bu bilgi çerçevesinde kişinin kredi notunu belirlemek veya gelecekteki sağlık durumu hakkında bir tahminde bulunmak için kullanılabilir³³. Kişisel verilerin kullanıldığı büyük veri analitiği çalışmaları

²⁸ Matthew STEWART, Data Privacy in the Age of Big Data, 28 Şubat 2020, <https://towardsdatascience.com/data-privacy-in-the-age-of-big-data-c28405e15508>.

²⁹ Information Commissioner's Office (ICO), Big Data, Artificial Intelligence, Machine Learning and Data Protection, 20170904, Version:2.2, s.17, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> (Kısaltılmışı "Big Data, Artificial Intelligence, Machine Learning and Data Protection").

³⁰ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.17.

³¹ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.12.

³² Çalışmanın "1.3.3.1. Kişisel Verilerin Korunması Mevzuatında "Kişisel Veri" Kavramı" başlıklı bölümü için bkz. s. 36 vd.

³³ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.11, s.32.

sonucunda kiři hakkında edinilen yeni bilgilerin de kiřisel veri olduėunu savunan g r řler olduėu gibi, aksi y nde de g r řler mevcuttur³⁴.

1.1.5. B y k Veri Analitiėinin Kiřisel Verilerin Korunması Aısından Risk Oluřturan  zellikleri

B y k veri analitiėini geleneksel veri analizi y ntemlerinden ayıran kendine has  zellikleri bulunmaktadır. Bu  zellikler, aslında yapay  ėrenme ve derin  ėrenme gibi yeni teknolojilerin teknik iřleyiřinden kaynaklanmaktadır. Bu  zelliklerin incelenmesi, profilleme ve otomatik karar alma faaliyetlerinin, kiřisel verilerin korunması ve mahremiyet aısından teřkil ettiėi risklerin de anlařılmasına yardımcı olacaktır. alıřmanın ilgili b l mlerinde bu  zelliklere atıfta bulunularak kiřisel verilerin korunması aısından deėerlendirmelere yer verildiėinden, bu b l mde sadece genel bilgi verilecektir.

Birleřik Krallık Bilgi Komisyoneri Ofisi'ne g re, b y k veri analitiėinde

- Algoritmaların kullanılması,
- Veri iřleme s recinin řeffaf deėil “opak” bir řekilde gerekleřmesi,
- Olabildiėince fazla veri toplanması,
- Verilerin toplanma amacından farklı amalar iin iřlenmesi ve
- Farklı t rdeki verilerin kullanılması

b y k veri analitiėinin kiřisel verilerin korunması, veri kalitesi ve mahremiyet aısından risk oluřturan ayırt edici  zelliklerini teřkil etmektedir³⁵.

Belirtilmelidir ki, bilgisayarda bir problemin  z lmesi iin her zaman bir algoritmaya ihtiya vardır³⁶. Yazılımın temel yapı taşı oluřturan algoritma,  zellikle bilgisayarlar tarafından hesaplamalarda veya bir problemin  z m nde

³⁴ alıřmanın, “1.3.3.2. Profilleme ve Otomatik Karar Alma Uygulamaları İle Edinilen ıkarımların Hukuki Niteliėi” bařlıklı b l m  iin bkz. s.38 vd.

³⁵ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.9.

³⁶ Alpaydın, Yapay  ėrenme: Yeni Yapay Zeka, s.27.

girdiyi çıktıya dönüştürmek için izlenen süreç veya komutlar dizisidir. Geleneksel veri analizinde programcının, bilgisayara belirli bir görevi yerine getirmek için ne yapması gerektiğini bir programlama dilinde program yazarak tanımlaması gerekir³⁷. Diğer bir ifadeyle, veriden ne öğrenmek istenildiğine göre ilgili veriler tanımlanmalı ve öğrenilmek istenen şeye göre bir sorgu oluşturulmalıdır³⁸. Büyük veri analitiğinde ise, program yazmak yerine, ne yapılması gerektiğine ilişkin örnekler içeren veriler toplanır³⁹. Geleneksel veri analizinin aksine, büyük veri analitiğinde belli bir hipotezi test etmek için önceden bir sorgu oluşturulmaz; veri setleri arasındaki korelasyonlar algoritmalar ile keşfedilir⁴⁰. Yapay öğrenme teknolojisinin işleyişinin bir özelliği olan bu keşif süreci büyük veri analitiğinde “belirsizlik” sorununa neden olur⁴¹.

Yapay öğrenme sistemlerinin kişisel verilerin korunması açısından risk teşkil eden en önemli sorunlardan biri de bu sistemlerin opak bir işleyiş yapısına sahip olmalarıdır. Özellikle derin öğrenme uygulamalarının karmaşık algoritmik yapılar olması ve büyük veri setlerini gelişmiş istatistiksel hesaplamalar ile analiz edebilmesi, bu sistemlerin opak bir işleyişe sahip olmasına neden olur. Dolayısıyla da ilgili modelin çıktılarını nasıl ürettiği, ilgili varsayım ve tahminin neye dayandığı gibi hususlar insanlar tarafından yeterince anlaşılamamaktadır⁴². Örneğin, yapay sinir ağı algoritmalarının kullanıldığı modellerde, modele bir girdi verildiğinde bir çıktı hesaplanır, ancak ağın ara katmanlarındaki işleyişin ne şekilde gerçekleştiğini kavramak zordur⁴³. Algoritma ne kadar karmaşık ise, tecrübeli bir mühendis

³⁷ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.11.

³⁸ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.10.

³⁹ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.11.

⁴⁰ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.10.

⁴¹ Reihaneh H. HARIRI & Erik M. FREDERICKS & Kate M. BOWERS, Uncertainty in Big Data Analytics: Survey, Opportunities, and Challenges, Journal of Big Data (2019) 6:44, Survey Paper, <https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-019-0206-3.pdf>.

⁴² ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.10.

⁴³ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.27.

tarafından dahi anlaşılması o kadar zorlaşır⁴⁴. Bu durum literatürde, “kara kutu problemi” (*black box problem*) olarak ifade edilmiştir⁴⁵.

Büyük veri analitiğininolabildiğince fazla verinin toplanarak analiz edilmesi yaklaşımına dayanması veri kalitesi ilkesi açısından risk oluşturmaktadır. İnternetin ortaya çıkmasından sonra çevrimiçi bağlanabilirlik (*online connectivity*) da hızla artmış, akıllı cihazların keşfiyle birlikte Nesnelerin İnterneti uygulamaları hayatımıza girmiştir⁴⁶. Nesnelerin İnterneti uygulamalarının yanı sıra büyük veri analitiğinde kullanılan yapay zeka teknolojileri, olabildiğince fazla verinin toplanmasını mümkün kılmıştır⁴⁷. Büyük veri analitiğinde artık sadece bireylerin bilinçli olarak paylaştıkları veriler değil, çevrimiçi davranışlarının izlenmesi suretiyle otomatik olarak oluşturulan veriler de kullanılmaktadır. Bu durum, veri kalitesi ve büyük veri analitiği ile ulaşılan çıktıların doğruluğu ile ilgili sorunları beraberinde getirmektedir. Büyük veri analitiğinde mümkün olan tüm verinin toplanması ve veri çeşitliliğinin artmış olmasının bir diğer sonucu da toplanan verilerin sıklıkla toplandıkları amaçtan farklı bir amaç için işlenmesidir. Bunun nedeni büyük veri analitiği ile çeşitli kaynaklardan edinilen ve görünürde farklı olan veri setleri arasındaki korelasyonların keşfedilebilmesidir. Böylece kişilerin hayatları ile ilgili hemen her konuda ve hatta kendilerinin dahi farkında olmadığı hususlara ilişkin içgörü ve çıkarımlar edinilebilmektedir. Bu da verilerin toplandığı amaçtan farklı bir amaç için işlenmesi anlamına gelir⁴⁸.

⁴⁴ Robyn CAPLAN & Joan DONOVAN & Lauren HANSON & Jenna MATTHEWS, Algorithmic Accountability: A Primer, Data & Society, s.15, https://datasociety.net/wp-content/uploads/2019/09/DandS_Algorithmic_Accountability.pdf.

⁴⁵ Carlos ZEDNIK, Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence, s.1, <https://arxiv.org/pdf/1903.04361v2.pdf>.

⁴⁶ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.20-24.

⁴⁷ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.11.

⁴⁸ Bart CUSTERS & Helena U VRABEC, Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection, International Data Privacy Law, 2016, s.8, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046774.

1.2. YAPAY ZEKA

Çalışmanın ilk bölümünde büyük veri analitiği ile yapay zeka teknolojilerinin ilişkisi açıklanmıştı. Çalışmanın bu bölümünde ise, profillemeye ve otomatik karar alma uygulamalarının veri işleme süreçlerinde kullanılabilecek yapay öğrenme, veri madenciliği ve yapay sinir ağları gibi farklı yapay zeka teknolojilerine ilişkin genel bilgi verilecektir.

1.2.1. Yapay Zeka Nedir?

Yapay zekanın bilim dünyasında kabul edilmiş genel geçer bir tanımı bulunmamakla birlikte, tanımlanması zor bir kavram olduğu belirtilmektedir⁴⁹. Yapay zeka, genel anlamda, insanlar için zeka gerektiren görevleri yerine getirebilen ve problemleri çözebilen bilgisayar sistemlerini tanımlamaktadır⁵⁰. Öte yandan, bir dönemde o günkü koşullarda yapay zeka olarak kabul gören bir teknolojinin, toplum o teknolojiye alıştıkça teknolojinin niteliğine yönelik algısının değiştiği ve bu teknolojinin artık yapay zeka olarak adlandırılmasının sona erdiği göz önüne alındığında, yapay zekanın tüm dünyada kabul göreceği belirli bir tanımı üzerinde uzlaşılmasının mümkün görünmediğini söylemek yanlış olmayacaktır⁵¹.

Avrupa Konseyi Yapay Zeka Ad Hoc Komitesi'nin (CAHAI), ilgili fizibilite çalışmasında,

- “AI” teriminin, yaygın olarak ve şu anda insan zekası ile ilişkili yetenekler sergileyen, farklı tekniklere dayalı çeşitli bilgisayar uygulamaları için “kapsamlı bir terim” olarak kullanıldığı,

⁴⁹ Shlomit YANISKY-RAVID, Generating Rembrandt: Artificial Intelligence, Copyright, And Accountability In The 3A Era-The Human-Like Authors Are Already Here-A New Model”, Michigan State Law Review, 2017, s.673.

⁵⁰ Intellectual Property Office, Artificial Intelligence, A worldwide overview of AI patents and patenting by the UK AI sector, s.2.

⁵¹ Bu durum “yapay zeka etkisi” (*artificial intelligence effect*) olarak adlandırılmaktadır. Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence, 2016, s.12, https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.

- Bu tekniklerin, resmi modellerin (veya sembolik sistemlerin) yanı sıra, örneğin denetimli öğrenme, denetimsiz öğrenme ve pekiştirmeli öğrenme dahil olmak üzere tipik olarak istatistiksel yaklaşımlara dayanan veriye dayalı modellerden, diğer bir ifadeyle öğrenmeye dayalı sistemlerden oluşabileceği,
- Yapay zeka sistemlerinin, veri toplamak suretiyle çevrelerini kayıt altına alarak, yapılandırılmış veya yapılandırılmamış verileri analiz ederek, verilerden elde edilen bilgi üzerinde akıl yürüterek veya işleyerek fiziksel veya dijital boyutta hareket ettiği ve bu bağlamda bir sonuca ulaşabilmek için en iyi eylem planına karar verdiği sonucuna varılabileceği ifade edilmiştir⁵².

Belirtmek gerekir ki insan zekasının en temel ve önemli unsuru öğrenme kabiliyetidir. Yapay zekanın insan beyninin çalışma mekanizmasından ve insan zekasından ilham aldığı göz önüne alındığında, sürekli değişen bir çevreye ve koşullara tıpkı bir insan gibi adapte olması beklenen bir sistemin mutlaka öğrenme yeteneğine sahip olması gerekir⁵³. Zira zeki bir sistem ancak hatalarını tekrar etmemeyi ve başarılarını tekrar etmeyi öğrenebildiği ölçüde çevresine uyum sağlayacaktır⁵⁴. Dolayısıyla yapay zeka sistemlerinin, bireyler hakkında çeşitli konularda çıkarımlarda bulunabilmek gibi belirli bir görevi gerçekleştirebilmeleri için yapay öğrenme algoritmaları (*machine learning algorithms*)⁵⁵ ile eğitilmeleri gerekmektedir⁵⁶. Günümüzde gündelik dilin bir parçası haline gelen “yapay zeka”

⁵² Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study, CAHAI (2020) 23, 17 Kasım 2020, s.4, <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> (Kısaltılmışı “Feasability Study”).

⁵³ Pedro DOMINGOS, Master Algoritma- Yapay Öğrenme Hayatımızı Nasıl Değiştirecek? 3.Baskı, İstanbul, 2019, s.28.

⁵⁴ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.13.

⁵⁵ Yapay öğrenme algoritması, yapay öğrenmede kullanılan, çıktıları tahmin etmek üzere girdileri analiz eden programlanmış algoritmalarıdır. Sisteme yeni veriler girildikçe, bu algoritmalar daha iyi bir performans gösterebilmek için işlevişlerini optimize ederler. Böylece, zamanla “öğrenme kabiliyeti” ve “zeka” geliştirirler.

⁵⁶ Bernhard ANRIG & Will BROWNE & Mark GASSON, “The Role of Algorithms in Profiling”, Profiling the European Citizen (Editörler: Mireille Hildebrandt, Serge Gutwirth), Springer, 2010, s.70; European Parliamentary Research Service (EPRS), The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA), Haziran 2020, s.10-12,

kavramı, bu teknolojiden kaynaklanan herhangi bir otomasyonun yanı sıra, sinir ağlarına dayalı yapay öğrenme veya derin öğrenme gibi makineye insanın bilişsel kapasitesini taklit ettirme misyonuna sahip yeni teknolojileri de kapsamaktadır⁵⁷.

1.2.2. Yapay Öğrenme

Yapay öğrenme, veri setlerinden bir çıkarımda bulunmak üzere çeşitli istatistiksel yöntemlerin kullanıldığı bir yapay zeka çalışma alanıdır. Çalışmada da yapay zeka ile yapay öğrenme kavramları zaman zaman birbirinin yerine kullanılmıştır. Yapay öğrenmede, bilgisayarların geleneksel yöntemlerle programlanması yerine bilgisayarın neyi nasıl yapması gerektiğine ilişkin örnekler içeren veriler toplanır⁵⁸. Toplanan veriler yapay öğrenme algoritmaları ile matematiksel tekniklerle analiz edilir. Böylece analiz edilen verilerden “öğrenmek” suretiyle birtakım çıkarımlarda bulunulur. Bu öğrenilmiş çıkarımlardan yararlanılarak da daha doğru tahminlerde bulunulabilir⁵⁹. Yapay öğrenme algoritmaları açık bir şekilde programlanmadan veriye dayalı bir girdi-çıkı modeli oluşturur. Bu model gelecekte yeni vakalarda karar almak ya da tahminde bulunmak amacıyla kullanılır⁶⁰.

Yapay öğrenme, genel olarak, doğru girdi-çıkı örneklerinin algoritmaya sunulup sunulmadığına bağlı olarak, denetimli/gözetimli öğrenme (*supervised learning*), ve denetimsiz/gözetimsiz öğrenme (*unsupervised learning*) olarak iki ana başlık altında incelenebilir⁶¹. Bunların dışındaki yapay öğrenme teknikleri, yarı gözetimli/denetimli (*semi-supervised learning*), pekiştirmeli öğrenme

[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU\(2019\)624261_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf) (Kısaltılmışı “The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence”).

⁵⁷CAHAI, Feasability Study, s.3.

⁵⁸ Ethem ALPAYDIN, Introduction to Machine Learning, The MIT Press, Second Edition, Cambridge, Massachusetts, s.11 (Kısaltılmışı “Introduction to Machine Learning”).

⁵⁹ European Commission, “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe”, Communication, 2018, s.11.

⁶⁰ Alpaydın, Introduction to Machine Learning, s.11.

⁶¹ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.14-15; ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.11.

(*reinforcement learning*) ve federe öğrenmedir (*federated learning*). Denetimli öğrenmede eldeki her bir girdi için arzu edilen çıktı da önceden bilinmektedir. Yapay öğrenme algoritması eğitim verilerini (*training data*) analiz ederek girdi ile çıktı arasında ilişki kuran fonksiyonu ortaya çıkarır⁶². Denetimsiz öğrenmede ise arzu edilen çıktılar önceden bilinmemektedir. Algoritmalar, önceden etiketlenmiş girdi ve çıktılar olmadan, eldeki verilerden birbirleri ile benzerlik gösterenleri eşleştirip gruplara ayırır. Yeni gelen veriler bu gruplar altında tasnif edilerek girdi ile çıktı arasındaki örüntü (*pattern*) ortaya çıkarılır⁶³. Her iki durumda da yapay öğrenme algoritmaları yeni verileri işlemek için karar alma kuralları (*decision-making rules*) geliştirir⁶⁴. Böylece yapay öğrenme ile bilgisayar yazılımları, insanların komutları ile programlanan ve son sözü programcının söylediği sistemler olmaktan uzaklaşmıştır. Bu yazılımlar otonom şekilde öğrenme yeteneği geliştirmiş, veri setlerinin altında yatan örüntüleri tespit edebilen yapay zeka sistemleri haline gelmiştir⁶⁵. Yarı denetimli öğrenme, denetimli öğrenme ile denetimsiz öğrenme arasında yer alır ve bir modelin öğrenmesi ve yeni örnekler üzerinden tahminde bulunması gereken az miktarda etiketlenmiş veri ile çok fazla etiketlenmemiş verinin birlikte kullanılması yaklaşımına dayanır⁶⁶. Pekiştirmeli öğrenme ise, istenilen davranışların ödüllendirildiği ve/veya istenilmeyen davranışların cezalandırıldığı, algoritmanın bu kapsamda sonraki denemelerde en yüksek ödülü getirecek eylemleri üretmeyi öğrenmesine dayanan bir yapay öğrenme tekniğidir⁶⁷. Satranç oyununda yaptığı hamlelere göre oyunu kazanan veya kaybeden oyuncunun ödül (kazanma) veya ceza (kaybetme) ile sonuçlanan hamlenin hangisi olduğunun öğrenerek sonuca göre o hamleyi tekrarlama olasılığını artırması veya azaltması pekiştirmeli öğrenmeye örnek olarak gösterilebilecektir⁶⁸.

⁶² John D. KELLEHER & Brendan TIERNEY, Veri Bilimi (Çeviri: Onur Öztürk), Tellekt, 1. Baskı, İstanbul, 2020, s.76.

⁶³ Alpaydın, Introduction to Machine Learning, s.11.

⁶⁴ Brent MITTELSTADT & Patrick ALLO & Mariarosaria TADDEO & Sandra WACHTER & Luciano FLORIDI, The Ethics of Algorithms: Mapping the Debate, Big Data & Society, 2017, s.3, <https://ssrn.com/abstract=2909885>.

⁶⁵ Onur KOÇ & Mustafa KASAP, Daha İyi Bir Dünya İçin Yapay Zeka, İstanbul, 2018, s.47.

⁶⁶ Jason BROWNLEE, What is Semi-Supervised Learning, 9 Nisan 2021, <https://machinelearningmastery.com/what-is-semi-supervised-learning/>.

⁶⁷ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.139.

⁶⁸ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.139

Yapay öğrenme tekniklerinden biri de “federe öğrenme” dir. Standart (klasik) yapay öğrenme tekniklerinin dışında, görece yeni bir yapay öğrenme tekniğini ifade eden “federe öğrenme” (*federated learning*) kavramı ilk kez 2016 yılında Google araştırmacıları tarafından yazılan bir makalede kullanılmıştır⁶⁹. Federe öğrenme standart yapay öğrenme tekniklerinden farklı olarak modelin merkezi olmayan/dağıtılmış (*decentralized*) veri ile eğitilmesi yaklaşımına dayanmaktadır. Standart yapay öğrenmede, eğitim verileri bir makinede veya veri merkezinde toplanmak suretiyle merkezileştirilirken, federe öğrenmede kişisel veriler kullanıcılara ait cihazlarda kalmaktadır⁷⁰.

Google tarafından açıklandığı üzere federe öğrenmenin işleyiş prensibi ve öngörülen faydaları şu şekildedir⁷¹:

- Kullanıcıya ait telefon mevcut modeli indirir, telefondaki verilerden öğrenerek modeli geliştirir ve ardından değişiklikleri bir güncelleme olarak özetler.
- Modele ilişkin bu güncelleme, paylaşılan modeli geliştirmek amacıyla şifreli iletişim kullanılarak diğer kullanıcı güncellemeleriyle ortalaması alınarak buluta gönderilir.
- Tüm eğitim verileri kullanıcının cihazında kalır ve bulutta hiçbir bireysel güncelleme depolanmaz.
- Federe öğrenme, eğitim verilerinin tamamını cihazda tutarak cep telefonlarının ortak bir tahmin modelini iş birliği ile öğrenmesini

⁶⁹ İlgili makale için bkz. H. Brendan MCMAHAN & Eider MOORE & Daniel RAMAGE & Seth HAMPSON & Blaise AGÜERA Y ARCAZ, Communication-Efficient Learning of Deep Networks from Decentralized Data, Proceedings of the 20 th International Conference on Artificial Intelligence and Statistics (AISTATS) 2017. JMLR: W&CP volume 54, 17 Şubat 2016, <https://arxiv.org/abs/1602.05629>.

⁷⁰ Google AI Blog, Federated Learning: Collaborative Machine Learning without Centralized Training Data, 6 Nisan 2017. Google AI’ın federe öğrenmeyi anlatan karikatür öyküsü için bkz. <https://federated.withgoogle.com>.

⁷¹ Google AI Blog, Federated Learning: Collaborative Machine Learning without Centralized Training Data, 6 Nisan 2017, <https://ai.googleblog.com/2017/04/federated-learning-collaborative.html>.

sağlarken verilerin bulutta depolanması ihtiyacı ile yapay öğrenme yeteneğini ayırır.

- Federe öğrenme ile mahremiyet garanti edilir, daha az güç tüketimi ile daha akıllı modeller yaratılır.
- Paylaşılan modele bir güncelleme sağlanırken, kullanıcının telefonundaki geliştirilmiş model de hemen kullanılabilir. Böylece kullanıcının telefonu kullanma şekline göre kişiselleştirilen deneyimleri güçlendirilir.

1.2.3. Derin Öğrenme ve Yapay Sinir Ağları

Derin öğrenme büyük veriden yararlanarak özellik çıkarma, sınıflandırma ve dönüştürme gibi çeşitli işlemleri yerine getirebilen bir yapay öğrenme tekniğidir⁷². Derin öğrenme algoritmaları (*deep learning algorithms*), insan beynindeki sinir ağlarının yapısı ve çalışma şeklini çok daha basit bir modele indirgeyen yapay sinir ağlarına (*artificial neural networks*) dayanır⁷³. Yapay sinir ağları insan beyninin karmaşık görevleri yerine getirme ve problemleri çözmek için kullandığı yöntemlerden ilham alarak geliştirilmiştir⁷⁴. İnsan beyninin en temel özelliği olan öğrenme yeteneğini bilgisayarlar açısından hayata geçirmek üzere tasarlanan yapay sinir ağları, genellikle, birkaç katman ve bu katmanlar arasındaki bağlantılardan oluşur⁷⁵. Öğrenme sürecinde veriler ilk katman vasıtasıyla yapay sinir ağına girilir⁷⁶. Bundan sonra gelen her bir katmanda girdiler matematiksel fonksiyonlardan geçirilerek bir sonraki katmana iletilir⁷⁷. Yapay sinir ağının ürettiği sonuç son katmanın çıktısıdır⁷⁸. Bu sistemin ürettiği çıktılar her bir katmanda geriye doğru iletilerek öğrenme süreci işletilir⁷⁹. Yapay sinir ağlarının belirtilen

⁷² Gülçin BÜYÜKÖZKAN FEYZİOĞLU, “Dijitalleşen Dünyada Yapay Zeka”, Gelişen Teknolojiler ve Hukuk II: Yapay Zeka (Editörler: Eylem Aksoy Retornaz, Osman Gazi Güçlütürk), 1. Baskı, İstanbul, 2021, s.7.

⁷³ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.77.

⁷⁴ Büyükoçkan Feyzioğlu, s.8.

⁷⁵ Büyükoçkan Feyzioğlu, s.8.

⁷⁶ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.77-80;

⁷⁷ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.77-80;

⁷⁸ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.77-80;

⁷⁹ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.77-80;

işleyiş yapısı, yapay sinir ağı öğrenme algoritmaları ile büyük veri setlerindeki örüntülerin tespit edilebilmesini mümkün kılar⁸⁰. Geleneksel yapay öğrenme ile derin öğrenme arasındaki en temel fark, derin öğrenmede çok daha fazla katman ve alt öge içeren karmaşık modeller kullanılmasıdır. Bu modellerin doğru şekilde çalışabilmesi için çok büyük veri kümelerine ihtiyaç duyulur⁸¹. Ayrıca derin öğrenmede kullanılan sofistike modeller, büyük veri içinde yer alan ve geleneksel yapay öğrenme ile ortaya çıkarılamayan örüntüleri tespit edebilmektedir⁸². Buna karşın, derin öğrenme modellerinin belirtilen karmaşık yapısı, elde edilen sonuçlara tam olarak nasıl ulaşıldığının modeli kullanan uzmanlar tarafından dahi çözümlenmesini neredeyse imkansız hale getirir⁸³. Kara kutu problemi olarak ifade edilen bu durum, çalışmanın ilgili bölümlerinde inceleneceği üzere şeffaflık ve hesap verebilirlik ilkelerinin uygulanabilirliği açısından sorun teşkil etmektedir.

1.2.4. Veri Madenciliği

Veri madenciliği, büyük veri kümelerindeki örüntü ve ilişkilerin analiz edilmesi suretiyle, gizli ve daha önce bilinmeyen ancak faydalı olabilecek bilgiye dayalı çıkarımlar edinilmesi sürecidir⁸⁴. Nitekim veri madenciliği için “Bilgi Keşif Süreci” (*Knowledge Discovery Process*) kavramı da kullanılmaktadır⁸⁵. Veri madenciliği algoritmaları, veri setlerindeki anormalliklerin tespit edilmesi, veriler arasındaki bağlantıların tespit edilmesi, kümeleme ve sınıflandırma gibi çeşitli görevleri gerçekleştirebilir⁸⁶. Konuyla ilgili çalışmalarda, veri analitiği ve veri

⁸⁰ Alpaydın, Yapay Öğrenme: Yeni Yapay Zeka, s.77-80;

⁸¹ Büyüközkan Feyzioğlu, s.7.

⁸² Maryam M NAJAFABADI & Flavio VILLANUSTRE & Taghi M KHOSHGOFTAAR & Naeem SALIYA & Randall WALD & Edin MUHAREMAGIC, Deep Learning Applications and Challenges in Big Data Analytics, Journal of Big Data (2015) 2:1, s.3, <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-014-0007-7>.

⁸³ Najafabadi & Diğerleri, s.14-15.

⁸⁴ Padhy NEELAMAHDAB & Mishra PRAGNYABAN & Panigrahi RASHMITA, The Survey of Data Mining Applications And Feature Scope, International Journal of Computer Science, Engineering and Information Technology (IJCEIT), Vol.2, No.3, Haziran 2012, s.44.

⁸⁵ Bart CUSTERS, Data Mining and Group Profiling on the Internet, 2001, s.3-4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047161.

⁸⁶ Shikha AGRAWAL & Jitendra AGRAWAL, Survey on Anomaly Detection Using Data Mining Techniques, Procedia Computer Science 60 (2015) 708 – 713, s.709, <https://doi.org/10.1016/j.procs.2015.08.220>.

madenciliği kavramlarının sıklıkla birbirlerinin yerine kullanıldığı görülmektedir. Bu iki kavram tam olarak aynı şeyi ifade etmiyor olmakla birlikte, veri madenciliğinin, büyük veri analitiği sürecindeki adımlardan biri olduğu söylenebilir.

Benzer şekilde, veri madenciliği ile yapay öğrenme sıklıkla birbirinin yerine kullanılmaktadır. Yapay öğrenme algoritmalarının görevi, yukarıda açıklandığı üzere, girdilerden eğitim aşamasında öğrendiklerine dayalı tahmin ve çıkarımlar oluşturmaktır. Veri madenciliği algoritmaları ise, bilinmeyen örüntü ve bağlantıların tespit edilmesi için mevcut veri setlerinin analiz edilmesini hedefler. Veri madenciliği ve yapay öğrenme farklı kavramlar olmakla birlikte, her ikisi de veri analitiği yöntemi olarak kabul edilir. Veri madenciliği ve yapay öğrenmenin ortak noktası, büyük veri yığınlarındaki örüntü ve ilişkilerin tespitine ve veriden bilgi sağlayarak daha iyi kararlar alınmasını sağlamaya hizmet eden teknolojiler olmalarıdır. Diğer yandan, yapay öğrenmede, daha iyi tahminlerde bulunmak için örüntüleri tespit etmek ve model oluşturmak amacıyla veri madenciliği teknikleri kullanılırken, veri madenciliğinde de benzer şekilde daha net analiz sonuçları çıkarabilmek için yapay öğrenmeden faydalanılmaktadır⁸⁷.

⁸⁷ Bernard MARR, What is the Difference Between Data Mining and Machine Learning?, <https://bernardmarr.com/default.asp?contentID=1741>.

1.3. PROFİLLEME VE OTOMATİK KARAR ALMA UYGULAMALARI

Profilleme (*profiling*), bir çeşit veri madenciliği yöntemidir⁸⁸. Veri madenciliği ile bireyler veya topluluklar ile ilgili profiller oluşturulabilmektedir. Profillemeye, genel olarak, bir kimsenin kişiliği, davranışları, yaşam tarzı, ilgi alanları, alışkanlıkları ve tercihlerine ilişkin kişisel verilerinin analiz edilmesi suretiyle kategorilendirilmesi ve bu kategorinin genel özellikleri çerçevesinde kişi hakkında bir tahminde bulunulması veya bir karar alınmasını ifade etmektedir⁸⁹. Mendoza ve Bygrave, profillemenin “(i) tek bir kişi veya kişi grubu hakkında bir dizi özellik çıkarma (yani, profil çıkarma) ve/veya (ii) bu kişi veya gruba (veya diğer kişilere/gruplara) bu özellikler ışığında muamelede bulunma (yani bir profilin uygulanması süreci) sürecini” ifade ettiğini belirtmiştir⁹⁰. Hildebrandt, profillemenin veriyle değil, tümevarsımsal bilgi (*inductive knowledge*) ile ilgili olduğunu ifade etmektedir. Buna göre profillemeye, ortam zekasını (*ambient intelligence*) etkinleştirecek bir teknolojidir ve esas amacı, veriler arasında bağlantı kurarak insan zihni ile fark edilmesi mümkün olmayan örüntüleri ortaya çıkarmaktır⁹¹.

Otomatik bireysel karar alma (*automated individual decision making*), belirli bir kişi hakkında, insan müdahalesi olmaksızın otomatik araçlar aracılığıyla herhangi bir konuda bir karar verilmesini ifade eder⁹². Burada bahsi geçen “otomatik araçlar”, çoğunlukla derin öğrenme ve yapay sinir ağları algoritmalarını kullanan yapay öğrenme sistemleridir. Nitekim literatürde otomatik karar alma faaliyetini tanımlamak üzere “algoritmik karar alma” (*algorithmic decision*

⁸⁸ Liane COLONNA, Legal Implications of Data Mining, Stockholm Faculty of Law Research Paper Series, 2016, s.86 vd, <https://dx.doi.org/10.2139/ssrn.2924541>.

⁸⁹ Article 29 Working Party, Guidelines on Automated Individual Decision Making and Profiling for the Purposes of Regulation 2016/679, (WP251rev.01), 3 Ekim 2017, s.6-7, <https://ec.europa.eu/newsroom/article29/items/612053>(Kısaltılmışı “Automated Individual Decision Making and Profiling”).

⁹⁰ Isak MENDOZA & Lee BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, 2017, s.1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855.

⁹¹ Mireille HILDEBRANDT, Profiling: From Data to Knowledge The Challenges of a Crucial Technology, *Datenschutz und Datensicherheit*, Cilt:30, Sayı:9, 2006, s.548-549, https://www.researchgate.net/publication/242181840_Profiling_From_data_to_knowledge.

⁹² ICO, Guide to the General Data Protection Regulation, s.161.

making) ifadesi de kullanılmaktadır⁹³. Otomatik karar süreçlerinde doğrudan ilgili kişiler tarafından ibraz edilen veriler (bir ankette alınan cevaplar gibi), kişiler hakkında toplanan veriler (bir mobil uygulama aracılığıyla edinilen lokasyon verisi gibi) veya kişinin daha önce oluşturulmuş profili gibi bazı verilerden türetilen veriler (kredi puanı gibi) gibi her türlü veri kullanılabilir⁹⁴.

GVK Tüzüğü m. 22 tahtında düzenlenen “tamamen otomatik işlemeye dayalı karar alma” (*solely automated decision making*) faaliyetinden bahsedilebilmesi için, söz konusu karar “anlamlı” bir insan değerlendirmesi bulunmaksızın verilmiş olmalıdır⁹⁵. Profillemeye dayalı karar alma (*decision making based on profiling*) ile tamamen otomatik işlemeye dayalı karar alma arasındaki fark, kredi örneği üzerinden somutlaştırılabilir⁹⁶. Bankaların çevrimiçi uygulamaları üzerinden başvurulabilen tüketici kredilerinde, değerlendirme saniyeler içinde algoritmalar aracılığıyla gerçekleştirilerek sonucu yine çevrimiçi olarak başvuru bildirildiğinde, karar sürecinin herhangi bir aşamasında anlamlı bir insan müdahalesi veya değerlendirmesi bulunmadığından tamamen otomatik işlemeye dayalı karar alma söz konusudur⁹⁷. Diğer yandan, kişiye kredi verilip verilmeyeceğine ve verilecekse hangi tutarda verileceğine ilişkin nihai kararın, kişinin kredi notu ve diğer verilerinin otomatik araçlarla işlenmesi suretiyle çıkarılan finansal profiline bakılarak bir banka yetkilisi tarafından verilmesi durumunda, profillemeye dayalı karar alma gerçekleştirilmektedir⁹⁸. Otomatik karar alma faaliyetleri çoğunlukla profillemeye içermekle birlikte⁹⁹, karar sürecinin tamamen otomatik işlemeye dayalı olup olmadığından bağımsız olarak, profillemeye

⁹³ Çalışmada da algoritmik karar alma” ifadesi “otomatik karar alma” ile eş anlamlı olarak kullanılmıştır.

⁹⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8.

⁹⁵ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.9.

⁹⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.9.

⁹⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.9.

⁹⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8-9.

⁹⁹ ICO, Guide to the General Data Protection Regulation, s.161. Kredi başvurusunun banka yetkilisi tarafından başvuranın kredi notunun göz önüne alınarak değerlendirilmesi profillemeye içeren bir otomatik karar alma örneğidir.

içermeden de gerçekleştirilebilir¹⁰⁰. Belirtilmelidir ki, profillemeye faaliyetinin de her zaman bir otomatik karar ile sonuçlanması gerekmez¹⁰¹. Öte yandan otomatik karar alma ve profillemenin birbirinden bağımsız şekilde gerçekleşmesi de gerekmez¹⁰². Profillemeye içermeyecek şekilde başlayan bir otomatik karar süreci verinin kullanım şekline göre profillemeye dayalı bir karara dönüşebilmektedir¹⁰³.

1.3.1. Grup Profillemeye ve Bireysel Profillemeye Ayrımı

Profillemeye faaliyeti genel olarak, belirli bir kişinin veya bir grup kişinin hedeflenmesine göre grup profillemeye ve bireysel profillemeye olarak sınıflandırılmaktadır. Grup profillemeye doğrudan veya dolaylı olarak gerçekleşmesine ve dağıtımsal olup olmamasına göre de kategorize edilmektedir. Çalışmanın bu bölümünde, öncelikle grup profillemeye (*group profiling*) ve bireysel profillemeye (*individual profiling*), ardından doğrudan profillemeye (*direct profiling*) ve dolaylı profillemeye (*indirect profiling*), son olarak ise dağıtımsal profillemeye (*distributive profiling*) ve dağıtımsal olmayan profillemeye (*non-distributive profiling*) ayrımları incelenecektir.

Bireysel profillemeye, belirli bir kişi hakkında toplanan kişisel verilerin analiz edilmesi suretiyle, bu kişinin bilinmeyen özellikleri ve gelecekteki davranışları ile ilgili çıkarımda veya tahminde bulunulmasını ifade eder. Bireysel profillemeye, bir

¹⁰⁰ Bir sınav değerlendirme kurulunun çoktan seçmeli sınav kağıtlarını değerlendirmek için kullandığı otomatik sistemde, başarılı ve başarısız notlar için gereken doğru cevapların sayısı ile önceden programlanır. Adayların doğru cevap sayısına göre otomatik olarak hesaplanan puanlar adaylara otomatik olarak atfedilir ve sonuçlar çevrimiçi olarak açıklanır. Belirtilen otomatik karar alma sürecinin herhangi bir aşamasında profillemeye söz konusu değildir. Bilgi Komisyoneri Ofisi'nin ilgili örneği ve açıklamaları için bkz. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>. 29. Madde Çalışma Grubu, profillemeye içermeyen otomatik karar alma faaliyetine örnek olarak, şehir kameralarından elde edilen kanıtlara dayanılarak otomatik olarak kesilen hız cezaları göstermiştir. Öte yandan, ilgili sürücünün sürüş alışkanlıklarının zaman içinde izlenmesi ve yakın zamanda başka trafik ihlallerinde bulunup bulunmadığı veya tekrarlayan şekilde hız aşımı gerçekleştirip gerçekleştirmediği değerlendirilerek ceza tutarının belirlenmesi halinde, profillemeye dayalı bir karar söz konusu olacaktır. Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8.

¹⁰¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8.

¹⁰² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8.

¹⁰³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8.

kişinin belli özelliklerini keşfetmek veya kişiselleştirilmiş hizmetler sunabilmek için tercih edilen bir yöntemdir¹⁰⁴. Öte yandan, kişiselleştirilmiş hizmetler aynı zamanda ve çoğunlukla grup profillemeye dayalı olarak gerçekleştirilmektedir¹⁰⁵. Grup profillemeye ise, belirli ortak özelliklere veya davranış biçimlerine sahip bir insan grubuyla ilgilenir¹⁰⁶. Grup profillemeye, bir kişinin profilinin çok fazla sayıda kişiyle ilgili çok fazla verinin analiz edilmesiyle oluşturulan bir profile eşleştirilmesi sonucu, ilgili kişinin belirli bir kategori altında tanımlanmasını sağlayan bir veri madenciliği yöntemidir¹⁰⁷. Grup profillemeye önceden tanımlanmış (bilinen) bir topluluğun (bir siyasi partiye üye, belirli bir üniversitede öğrenci veya mezun olan, belirli bir dine mensup kişilerin oluşturduğu topluluk gibi) üyeleri arasında paylaşılan önceden tanımlanmamış (bilinmeyen) ortak özelliklerin keşfedilmesi veya halihazırda bazı ortak özellikleri paylaşan bireylerin kategorilendirilmesi amaçlanmaktadır¹⁰⁸. Grup profillemeye bazen de bilinen bir topluluğun üyeleri olarak tanımlanmayan bir grup insanın, bilinmeyen bazı ortak özellikleri paylaştığını ve bu özelliklerin ilişkili olduğu diğer olguları (sağlık riskleri, finansal risk, akademik başarılilik oranı vb.) da ortaya çıkarabilmektedir¹⁰⁹. Örneğin, belirli bir semtte yaşayan 35 yaş altındaki erkeklerin ortalama olarak haftada iki kez mobil yemek uygulaması üzerinden eve yemek siparişi verdikleri sonucunun çıkarıldığı bir analizde, aynı davranış kalıplarını paylaşan belirli bir insan grubu “belirli bir semtte yaşayan 35 yaş altı erkekler”; keşfedilen korelasyon ise, “yemek siparişi alışkanlıkları”dır¹¹⁰.

¹⁰⁴ V. FERRARIS & F. BOSCO & G. CAFIERO & E. D’ANGELO & Y. SULOYEVA, Defining Profiling, Working Paper, Version 1.0, s.7, <https://ssrn.com/abstract=2366564>; David OLIVIER & Jaquet CHIFFELLE, “Reply: Direct and Indirect Profiling in the Light of Virtual Persons”, Profiling the European Citizen-Cross Disciplinary Perspectives (Eds: Mireille Hildebrandt & Serge Gurwith), Springer, 2008, s.35.

¹⁰⁵ Ferraris & Diğerleri, s.6.

¹⁰⁶ Ferraris & Diğerleri, s.6.

¹⁰⁷ Ferraris & Diğerleri, s.6-7.

¹⁰⁸ Ferraris & Diğerleri, s.6-7; E. Gil GONZALEZ & Paul DE HERT, Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data- An Analysis of GDPR Provisions and Principles, ERA Forum, 2019 (4), 597-621, s.608, <https://doi.org/10.1007/s12027-018-0546-z>.

¹⁰⁹ Gonzalez & De Hert, s.608.

¹¹⁰ Gonzalez & De Hert, s.608.

Grup profillemenin teknik anlamda üç aşaması bulunur¹¹¹. İlk aşamada, bireylerin kişisel özellikleri, alışkanlıkları, tercihleri ve davranışlarına ilişkin farklı kaynaklardan geniş ölçekli veri toplanır. Bunlar kişilerin internet alışverişlerinde satın aldıkları, seyahat bilgileri, sosyal medya platformlarındaki beğenileri, sağlık verileri, beslenme alışkanlıkları, nesnelerin interneti uygulamaları ile edinilen veriler gibi birçok farklı veriden oluşur¹¹². İlgili kişi hakkında toplanan bu veriler, kişisel veri niteliğinde olabileceği gibi kişisel özelliklerden arındırılmış (anonim) veya şifreli (*coded*) halde olabilir¹¹³. İkinci aşamada, toplanan bu veriler veri madenciliği ve büyük veri analitiği teknikleriyle analiz edilerek davranışlar, alışkanlıklar, tercihleri arasındaki korelasyonlar tespit edilir¹¹⁴. Yapay öğrenme algoritmaları ve istatistiksel analiz metodlarının kullanılmasıyla insan beyni ve muhakemesi ile gerçekleştirilmesi mümkün olmayan şekilde, farklı veri setleri arasındaki döngü ve örüntülerin ortaya çıkarılır ve bunların gerçekleşme olasılığının hesaplanır. Bu aşama aynı zamanda farklı davranış ve özellikler arasındaki korelasyon ve örüntülerin analiz edilmesi suretiyle profillerin oluşturulduğu aşamadır¹¹⁵. Çıkarılan profil, ilgili kişi hakkında bir “çıkarım” (*inference*) teşkil eder¹¹⁶. Son aşamada ise bu profiller diğer kişileri profilelemek için kullanılır. Böylece ilgili kişinin gelecekteki tercihleri, özellikleri veya davranışlarına ilişkin bir tahminde bulunulmak suretiyle kişi hakkında bir karar verilir¹¹⁷.

¹¹¹ Gonzalez & De Hert, s.608; Council of Europe, The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, Recommendation CM/Rec (2010)13 and Explanatory Memorandum, 23 Kasım 2010, s.25, <https://rm.coe.int/16807096c3> (Kısaltılmışı “The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling”); Information Commissioner’s Office (ICO), Guide to the General Data Protection Regulation, s.162, <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>. (Kısaltılmışı “Guide to the General Data Protection Regulation”).

¹¹² ICO, Guide to the General Data Protection Regulation, s.162,

¹¹³ Council of Europe, The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, s.25.

¹¹⁴ Gonzalez & De Hert, s.609.

¹¹⁵ Gonzalez & De Hert, s.609.

¹¹⁶ Gonzalez & De Hert, s.609.

¹¹⁷ Mireille HILDEBRANDT, “Defining Profiling: A New Type of Knowledge”, Profiling the European Citizen (Editörler: Mireille Hildebrandt & Serge Gutwirth), Springer, 2010, s.19.

Bankalar, müşteri riskini değerlendirmek yaygın şekilde profillemeye ve veri analitiği yöntemlerini kullanırlar. Analitik yöntemleri ile çıkarılan bir kredi puanı ile ölçülen müşteri riski, gelecekteki bir davranışa atıfta bulunur¹¹⁸. Kredi puanının oluşturulması, banka ve finansal kuruluşlarca müşteri verilerinin ve ödeme geçmişinin analiz edilerek, kimin borcunu geri ödediğini ve kimin ödemediğine ilişkin belirli korelasyonların çıkarılmasını gerektirir¹¹⁹. Bu puan, müşterinin daha önce diğer müşterilerde gözlemelenen ödeme ve ödememeye ilişkin belirli özellikleri taşıma olasılığını yansıtır¹²⁰. Buna göre, örneğin, belirli bir semtte yaşayan, haftada en az iki kez yemek siparişi veren ve aylık kirası belirli bir tutarın altında olan bir kişi, “35 yaş altı kadın/erkek” profilinde sınıflandırılacaktır¹²¹. İlgili verilerin bu profildeki kişilerin %27 oranında ödemelerinde gecikmeye düşme ihtimalinin bulunduğunu gösterdiği bir senaryoda, bu profil altında sınıflandırılan kişiler hakkında verilecek kredi kararında “ödemede %27 oranında gecikme ihtimalinin bulunduğu” varsayımı dikkate alınacaktır¹²². Belirtmek gerekir ki bu şekilde gerçekleştirilen profillemeye faaliyetleri, her zaman, kişinin daha önce temerrüde düşüp düşmediği veya kredi talebinin olumlu sonuçlanmasını sağlayacak faktörlerden (bankada birikim hesabında belli bir tutarda mevduat bulunması gibi) bağımsız olarak, ait olmadığı bir profil altında sınıflandırılması ve böylece onu gerçek şekilde tanımlamayan davranış ve özellikler ile eşleştirilmesi konusunda bir hata payı içerir¹²³.

Bireysel profillemeye de grup profillemeye de doğrudan veya dolaylı olarak gerçekleştirilebilir¹²⁴. Doğrudan profillemeye belirli bir kişi ya da gruptan edinilen veya bu kişi ya da grup hakkında gözlemlenen verilerin analiz edilmesiyle oluşturulan çıkarımlar, yine aynı kişi veya grup ile eşleştirilir. Bir kişi hakkındaki profilin yine bu kişinin bizzat kendisine uygulanması halinde, “doğrudan bireysel

¹¹⁸ Gonzalez & De Hert, s.609-610.

¹¹⁹ Gonzalez & De Hert, s.609-610.

¹²⁰ Gonzalez & De Hert, s.609-610.

¹²¹ Gonzalez & De Hert, s.609.

¹²² Gonzalez & De Hert, s.609.

¹²³ Gonzalez & De Hert, s.609-610.

¹²⁴ Olivier & Chiffelle, s.40-43.

profilleme” söz konusudur. Bir grup hakkında oluşturulan profilin yine bu gruba uygulanması halinde ise “doğrudan grup profilleme” gerçekleştirilmektedir. Bu bağlamda, doğrudan profilleme ile ilgili kişi veya grubun daha iyi tanınması sağlanarak bu sayede bu kişilerin gelecekteki davranışları, tercihleri ve alışkanlıkları hakkında çıkarımda bulunulması hedeflenmektedir¹²⁵.

Öte yandan dolaylı profillemeye, daha geniş bir kitleden veri toplanır. Kişisel verileri, bu verinin analiz edilmesi ile çıkarılan profile uyuşan bireyler veya gruplara, bu grup profili uygulandığında dolaylı profilleme gerçekleştirilmektedir¹²⁶. Bir kişiye ait verilerin bir gruba ait profile uyuşması sonucu bu grup profilinin ilgili kişiye uygulanması halinde dolaylı bireysel profillemeye bahsedilebilecektir¹²⁷. Eğer bir grup profili, yine bu grubun üyesi olan kişilere uygulanmakta ise bu durumda dolaylı grup profilleme söz konusudur¹²⁸. Dolaylı profillemeye örnek olarak, e-ticaret sitelerinde ve çevrimiçi platformlarda kullanılan tavsiye sistemleri gösterilebilir. Netflix’in bazı kullanıcıların izledikleri film ve dizilere göre diğer kullanıcılara yaptığı tavsiyeler ve Amazon’un diğer kişilerin yaptıkları kitap alışverişlerini esas alarak yaptığı kitap tavsiyeleri, dolaylı bireysel profillemeye gerçekleştirilen örneklerdir¹²⁹.

Grup profillemeye, profillemenin grubun tüm üyeleri için geçerli olup olmadığına göre dağıtımsal ve dağıtımsal olmayan profillemeye olmak üzere ikiye ayrılır¹³⁰. Bir gruba ait profile ilişkin özelliklerin grubun tüm üyeleri için geçerli olduğu durumda dağıtımsal profillemeye gerçekleştirilmektedir¹³¹. Örneğin, bir üniversitesinin mezunlar derneği üyelerinin (grup) tamamı ilgili üniversitenin mezunu olup, bu üniversitenin mezunu olmak tüm grup ve ayrıca her bir grup üyesi için doğru ve geçerli bir olgudur¹³². Belirli bir gruba sahip tüm kişilerin %80

¹²⁵ Olivier & Chiffelle, s.40-41.

¹²⁶ Ferraris & Diğerleri, s.6-7.

¹²⁷ Ferraris & Diğerleri, s.6-7.

¹²⁸ Ferraris & Diğerleri, s.6-7.

¹²⁹ Ferraris & Diğerleri, s.7.

¹³⁰ Anton VEDDER, KDD: The Challenge to Individualism, Ethics and Information Technology 1 (4): 275-281, 1999, s.277, DOI:10.1023/A:1010016102284.

¹³¹ Ferraris & Diğerleri, s.6.

¹³² Ferraris & Diğerleri, s.6.

oranında belirli bir hastalığı geliştirme riskinin bulunduğuna ilişkin bir çıkarım da dağıtımsal grup profillemeye örnek olarak gösterilebilir. Öte yandan, dağıtımsal olmayan grup profillemeye ise, bir gruba ait profile ilişkin özellikler grubun tüm üyeleri için her zaman geçerli değildir¹³³. Belirtmek gerekir ki, algoritmalar aracılığıyla gerçekleştirilen profillemeye çoğunlukla bu kategoridedir¹³⁴. Bu bağlamda dağıtımsal olmayan grup profillemenin önyargılı, ayrımcı, adil olmayan sonuçlar üretme potansiyelinin dağıtımsal grup profillemeye göre daha yüksek olduğu kabul edilir¹³⁵. Örneğin, bazı kişiler stresli yaşam tarzı, genetik faktör, sigara kullanımı gibi belirli risk faktörlerin göz önüne alınarak kardiyovasküler hastalık geliştirme ihtimali daha yüksek bireyler olarak profillemektedir. Ancak bu faktörleri karşılamayan, diğer bir ifadeyle bu profile sahip kişilerle aynı özellikleri göstermeyen biri de kardiyovasküler hastalık geliştirme riski yüksek kişilerle aynı grubun üyesi olabilir¹³⁶. Benzer şekilde, örneğin, bir kişi, kredi ödemelerinde hiç gecikme yaşamamış veya ödemede başarısız olmamış olsa dahi, kredi puanının düşük hesaplanmasına neden olan bazı kriterlere sahip olduğu için (yaş, yaşanan semt, meslek vb.) kişiye düşük bir puan verilebilmektedir. Bu durumda, bu kişi her ne kadar bu düşük kredi puanlı grup açısından bir istisna da olsa, bu husus değerlendirilmeden kişinin sadece kredi puanına bakılarak kredi talebi reddedilebilecektir¹³⁷.

¹³³ Hans LAMMERANT & Paul DE HERT, “Predictive Profiling and Its Legal Limits: Effectiveness Gone Forever?”, Exploring the Boundaries of Big Data (Eds: B. van der Sloot, D. Broeders, & E. Schrijvers), 2016, s.148; Ferraris & Diğerleri, s.6-7.

¹³⁴ Ferraris & Diğerleri, s.7.

¹³⁵ Vedder, s.277; Ferraris & Diğerleri, s.7; Lammerant & De Hert, s.148; Gonzalez & De Hert, s.610.

¹³⁶ Ferraris & Diğerleri, s.6-7.

¹³⁷ Vedder, s.277.

1.3.1.1. Çevrimiçi İzleme Teknolojileri

Profilleme faaliyetlerinde özellikle de çevrimiçi davranışsal reklamcılıkta çeşitli teknolojiler ile kullanıcıların izlenmesi suretiyle toplanan kişisel veriler analiz edilir ve kullanıcıların bu analiz sonucunda bir profili oluşturulur. Çevrimiçi izleme, kullanıcıların çevrimiçi faaliyetlerinin tarayıcı çerezleri (*cookies*), javascript dosyaları (*javascript files*), süperçerezler (*supercookies*), cihaz parmak izi (*device fingerprinting*), konum izleme (*location tracking*), izleme pikselleri (*tracking pixels*)¹³⁸, yazılım geliştirme kitleri (*software development kits*), kanonik isim gizleme (*canonical name cloaking*) gibi çevrimiçi izleme teknolojileri kullanılarak izlenmesini ifade etmektedir¹³⁹. Çevrimiçi izleme, mobil uygulamalar, internet siteleri veya cep telefonları, tabletler ve akıllı TV'ler gibi akıllı cihazlar tarafından toplanan kişisel verilerin işlenmesine (birinci taraf izleme) dayanabileceği gibi, üçüncü kişiler adına veri toplanması şeklinde (üçüncü taraf izleme) de gerçekleşebilmektedir¹⁴⁰. Birinci taraf izleme (*first-party tracking*), kullanıcının ziyaret ettiği bir internet sitesi veya kullandığı bir mobil uygulama tarafından, kişisel verileri üçüncü bir taraf ile paylaşılmadan izlenmelerini ifade etmektedir¹⁴¹. Üçüncü taraf izlemede ise, ilk taraf izlemeden farklı olarak kullanıcı verileri farklı araçlarla (Google Ad Exchange gibi) üçüncü taraflarla paylaşılmaktadır¹⁴². Kullanıcıya ait kişisel verilerin kullanıcının bilmediği birçok üçüncü tarafla kullanıcının kontrol sahibi olmadığı bir şekilde paylaşılması ve GVK Tüzüğü'nün özellikle rızaya ilişkin gerekliliklerinin karşılanmasını zorlaştırması nedeniyle, üçüncü taraf izleme birinci taraf izlemeye kıyasla bireyin mahremiyeti

¹³⁸ İzleme pikselleri, bir internet sitesi, mobil uygulama veya e-postaya yerleştirilen görünmez resim dosyalarıdır. Bu şekilde ilgili internet sitesinde gezinen, uygulamayı kullanan veya e-postayı alan kişinin reklam ve pazarlama kampanyaları ile amaçlanan etkileşimleri ölçülmektedir.

¹³⁹ Leyla KESER BERBER, Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ocak 2014, s.23-25.

¹⁴⁰ Leyla KESER BERBER & Ayça ATABEY & Ezgi EREN, E-Privacy Report: Lessons learned from the European Experience & Reflections for e-Privacy Laws in Turkey, İstanbul Bilgi University IT Law Institute, Eylül 2020, s.36-48, <https://itlaw.bilgi.edu.tr/tr/haberler/e-privacy-raporumuz-yayinlandi-145/>.

¹⁴¹ Keser Berber & Atabey & Eren, s.52.

¹⁴² Keser Berber & Atabey & Eren, s.52.

ve bilgilerin geleceğini belirleme hakkı açısından çok daha riskli kabul edilmektedir¹⁴³.

Çevrimiçi izleme teknolojilerinden en sık ve yaygın kullanılanı çerezlerdir. Çerezler, internet sitelerinin kullanıcıların bilgisayarlarına gönderdiği, kullanıcının bilgisayarında bilgi depolanmasına ve kullanıcının sonraki ziyaretlerinde kullanıcının ve tarayıcının tanınmasına imkan tanıyan küçük metin dosyalarıdır¹⁴⁴. Oturum çerezleri (*session cookies*), kalıcı çerezler (*persistent cookies*), süperçerezler (*supercookies*) ve zombi çerezler (*zombie cookies*) gibi farklı çerez türleri bulunmaktadır¹⁴⁵. Özellikle üçüncü taraf çerezleri (*third party cookies*) aracılığıyla gerçekleştirilen çevrimiçi izleme faaliyetlerinin internet kullanıcılarının mahremiyeti üzerindeki olumsuz etkileri, uzun süredir birçok tartışmaya konu olmuştur. Üçüncü taraf çerezlerinin mahremiyet üzerindeki olumsuz etkilerine ilişkin tartışmaların yanı sıra Safari ve Firefox'un geliştirdiği teknolojiler ile üçüncü kişi çerezlerin engellenebilmesi sonucunda, üçüncü taraf izleyiciler bazı yeni izleme teknikleri geliştirmişlerdir¹⁴⁶. Safari ve Firefox'tan sonra üçüncü taraf çerezlerin devre dışı bırakılması konusunda girişimde bulunan bir diğer şirket de Google olmuştur. En yaygın olarak kullanılan tarayıcı olarak kabul edilen Chrome'un sahibi Google, 2019 yılında üçüncü taraf çerezlerinin kullanımdan kaldırılması suretiyle kullanıcıların mahremiyetinin daha iyi bir şekilde korunmasını amaçlayan standartların geliştirilmesi planı kapsamında "Privacy Sandbox" adlı girişimini açıklamıştır¹⁴⁷. Girişimin üçüncü taraf çerezlerini devre dışı bırakmak amacıyla geliştirilmiş teknolojilerinden biri de "Federe Öğrenme Kümeleri" (*FLoC-Federated Learning of Cohorts*) yazılımıdır¹⁴⁸.

¹⁴³ Keser Berber & Atabey & Eren, s.52.

¹⁴⁴ Keser Berber & Atabey & Eren, s.39.

¹⁴⁵ Keser Berber & Atabey & Eren, s.39; Keser Berber, s.23-24.

¹⁴⁶ Keser Berber & Atabey & Eren, s.53.

¹⁴⁷ Bkz. <https://privacysandbox.com/>.

¹⁴⁸ Brendan McMAHAN&Daniel RAMAGE, Federated Learning:Collaborative Machine Learning without Centralized Training Data, Google AI Blog, 6 Nisan 2017, <https://ai.googleblog.com/2017/04/federated-learning-collaborative.html>.

FLoC, algoritmalar aracılığı ile grup profillemeye gerçekleştirilen bir çevrimiçi izleme teknolojisidir¹⁴⁹. FLoC algoritmasıyla kullanıcıların tarayıcıdaki çevrimiçi aktivitelerinin analiz edilmesi suretiyle benzer içeriklere erişenlerin bir “kohort kimliği” (*cohort ID*) altında gruplandırılmakta, reklam verenler de API’ler aracılığıyla sadece bu kohort kimliklerine erişerek belli ortak özelliklere sahip insanlardan oluşan “ilgi kümelerine” (kohortlara) benzer reklamlar gösterilebilmektedir¹⁵⁰. Her bir kohortun en az birkaç bin kullanıcıdan oluşması ve kullanıcıların her hafta farklı bir grup altına konması suretiyle kohortların güncellenmesi, kullanıcıların kimliğinin tespit edilmesini zorlaştırmaktadır. Bu bağlamda, FLoC ile üçüncü taraf çerezlerinin kullanılmasıyla mümkün olan kadar net bir hedefleme yapılamamakla birlikte, yine de kullanıcıların kişisel verilerinin işlenmesi üzerine kurulu bir teknolojidir. FLoC, yalnızca GVK Tüzüğü ve e-Gizlilik Direktifinin yürürlükte olmadığı ülkelerde test edilebilmiş, Avrupa Birliği’nde ise GVK Tüzüğü ve E-Gizlilik Direktifi ile uyumlu olmadığı gerekçesiyle kullanımı askıya alınmıştır¹⁵¹. Zaman içerisinde FLoC’un, Google’ın iddia ettiği kadar mahremiyet dostu olmadığı, rekabeti bozucu uygulamalara neden olduğu ve GVK Tüzüğü ile E-Gizlilik Direktifi düzenlemelerine uyumlu olmadığı yönünde çeşitli eleştirilere konu olmuştur¹⁵². Google, 2021’de FLoC’un kullanımını askıya almış, 2022 başında ise FLoC API’lerinin geliştirmesine son verdiğini resmi olarak açıklamıştır¹⁵³.

¹⁴⁹<https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/>.

¹⁵⁰David NIELD, What’s Google FLoC? And How Does It Affect Your Privacy? 9 Mayıs 2021, <https://www.wired.com/story/google-floc-privacy-ad-tracking-explainer/>.

¹⁵¹Data Secure, Google’s FLoC & It’s Impact on Privacy, 17 Temmuz 2021, <https://www.datasecure.ind.in/googles-floc-its-impact-on-privacy/>.

¹⁵²Allison SCHIFF, Google Will Not Run FLoC Origin Tests in Europe due to GDPR Concerns (At Least for Now), 23 Mart 2021, <https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/>; Competition and Markets Authority, Investigation into Google’s ‘Privacy Sandbox’ Browser Changes, 8 Ocak 2021, <https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes>; Emily BIRNBAUM, The DOJ Sues Google for Monopoly Practices- And Says There’s More to Come, 20 Ekim 2020, <https://www.protocol.com/google-justice-department-lawsuit-antitrust>.

¹⁵³Vinay GOEL, Get to Know the New Topic API for Privacy Sandbox, 25 Ocak 2022, <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/>.

Grup profillemeye içeren bir diğer hedeflemeörneği de adreslenebilir televizyon reklamcılığı (*addressable TV advertising*) uygulamalarıdır. Adreslenebilir televizyon reklamları, geleneksel televizyon reklamcılığından oldukça farklı bir işleyişe sahiptir. Geleneksel reklamcılıkta reklam verenler reklamlarının gösterilmesi için bir yayın ağı (*network*) veya televizyon programı seçerken, adreslenebilir televizyon reklamcılığında reklamın hangi haneye gösterileceği seçilmektedir. Adreslenebilir reklamcılığı modelinde, ilk olarak TV içerik sağlayıcıları tarafından toplanan lokasyon verisi, demografik veriler, izleme alışkanlıkları, ziyaret edilen internet siteleri gibi tüketici verilerinin analiz edilmesiyle hane profilleri oluşturulmaktadır¹⁵⁴. Bu profillerin uydu, kablo ve IPTV dağıtım sistemleri aracılığıyla eşleştirilmesiyle, aynı programı izleyen farklı hanelere, hane profili esas alınarak farklı reklam gösterilmesi mümkün hale gelmektedir. Öte yandan, adreslenebilir televizyon reklamcılığı ile reklamın gösterileceği kitle hane düzeyinde hedeflenebilmekle birlikte, aynı haneyi paylaşan farklı bireylere de farklı reklamlar sunulabilmektedir¹⁵⁵.

Adreslenebilir TV reklamcılığı ile reklamcılar ve pazarlamacılar, belirli reklamları ihtiyaçlarına göre filtreledikleri belirli kitlelere sunarak reklam ile amaçlanan etkileşimi iyileştirme imkanına erişebilmektedir. Adreslenebilir televizyon reklamcılığının tüketiciler ve reklamcılar açısından çeşitli faydaları bulunmakla birlikte, tüketici verisine dayalı bir hedefleme teknolojisi olması itibarıyla kişisel verilerin korunmasına ilişkin tartışmalara neden olmuştur. Zira adreslenebilir televizyon reklamcılığı, profillemeye, lokalizasyon ve pazarlama faaliyetleri içerdiğinden, kişisel verilerin ilgili kişinin açık rızasının bulunması halinde işlenebileceği kabul edilmektedir. Ancak televizyonun çoğu aile veya ev

¹⁵⁴Theviewpoint, Why You Should Look Into Addressable TV Advertising, 10 Haziran 2021, <https://theviewpoint.com/insights/blog/why-you-should-look-into-addressable-tv-advertising/>.

¹⁵⁵ Dentons, The Market's View: Interview with Andrea d'Agostino on How Digital Advertising Players are Creating a New Era in the TV Market, 4 Mayıs 2020, <https://www.dentons.com/en/insights/articles/2020/may/4/how-digital-advertising-players-are-creating-a-new-era-in-the-tv-market>.

halkı açısından bireysel değil ortak kullanılan bir cihaz olması, geçerli bir rızanın nasıl alınacağına ilişkin sorunları da beraberinde getirmektedir¹⁵⁶.

1.3.2. Profillemeye ve Otomatik Karar Alma Uygulamalarının Kullanım Alanları

Profillemeye ve otomatik karar alma sistemleri günümüzde hem kamu tarafından hem de özel sektör tarafından kullanılmaktadır. Bu sistemleringerek tüketiciler gerekse de özel şirketler vekurumlar açısından birçok faydası bulunmaktadır. Profillemeye faaliyetleri amaç bakımından farklılık göstermektedir. Profillemeye, kamu veya özel sektörde faaliyet gösteren çeşitli aktörler tarafından, (i) bir kişi hakkında toplanan kişisel verilerden kişinin kimliği, kişiliği, davranışları, ilgi alanları ve yetenekleri ile ilgili tahminde veya çıkarımda bulunmak, (ii) kişileri puanlandırmak, derecelendirmek, değerlendirmek, (iii) bir kişi hakkında belirli bir konuda karar almak veya kişi hakkında verilecek bir karara dayanak oluşturmak, (iv) kişiye özel kişiselleştirilmiş reklam ve içeriklerin gösterilmesi amacıyla yapılabilmektedir. Özellikle çok büyük veri setlerinin analiz edilmesini ve hızlı kararlar alınmasını gerektiren konulardabu sistemler sayesinde daha önce bilinmeyen korelasyonlar keşfedilmekte ve kararlar veriye dayalı olarak daha hızlı ve tutarlı şekilde alınabilmektedir¹⁵⁷.

Günümüzde pazarlama, bankacılık, finans hizmetleri, e-ticaret, bilgi işlem, sağlık, eğitim, hukuk, sigorta, kolluk hizmetleri, medya, reklamcılık gibi birçok farklı sektörde kredi derecelendirme, çevrimiçi davranışsal reklamcılık, dolandırıcılığın önlenmesi, hastalıkların teşhisi ve önlenmesi, iş başvurularının filtrelenmesi, suçların ve terörün önlenmesi gibi farklı alanda otomatik şekilde

¹⁵⁶Leyla KESER & Ayça ATABEY, Addressable TV and Consent Sequencing, Global Privacy Law Review, Volume 1, Issue 1 (2020), s.14-38.

¹⁵⁷ European Parliamentary Research Service (EPRS), Understanding Algorithmic Decision-Making: Opportunities and Challenges, Panel for the Future of Science and Technology, Mart 2019, s.3,[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU\(2019\)624261_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf) (Kısaltılmışı “Understanding Algorithmic Decision-Making: Opportunities and Challenges”).

gerçekleştirilen profillemeden faydalanılmaktadır. Bankaların kullandığı yapay öğrenme tabanlı kredi derecelendirme (*credit scoring*) sistemlerinde, kişinin finansal geçmişine ilişkin veriler, sosyo ekonomik durumuna gösterge teşkil eden veriler, kredi kayıt kurumları tarafından kredi geçmişleri esas alınarak yapılan değerlendirmeler gibi farklı verilerin analiz edilmesiyle bir profil oluşturulmakta ve bu profile bakılarak kimin kredi başvurusunun onaylanacağına ve hangi tutarda kredi kullandırılacağına karar verilmektedir. Pazarlama sektöründe ise, doğru ürün ve hizmet için doğru kişinin hedeflenmesi müşteri segmentasyonu ile sağlanabilmektedir. Müşteri segmentasyonu, hedef müşteri kitlesinin belirli özelliklere göre gruplandırıldığı bir bölümlere ayırma yöntemidir. Müşteri ilgi alanları, sosyo ekonomik durumu ve alışveriş geçmişi ile ilgili bilgilerin analiz edilmesi suretiyle belirli bir segment altında profillendiğinde, müşteriye sunulacak ürün ve hizmetler de bu profile göre belirlenebilmektedir. Böylece doğru müşteriye doğru ürünün pazarlaması yapılarak satışlar artırılmakta ve ekonomik fayda sağlanmaktadır¹⁵⁸. Profilleme, yapay öğrenme tabanlı öngörücü polislik (*predictive policing*) uygulamalarında da sıklıkla kullanılmaktadır. Bu uygulamalar, kişinin şüpheli davranışlarının veya suç işleme niyetinin çeşitli analitik teknikleri kullanarak tahmin edilmesi suretiyle suçun gerçekleşme riskinin öngörülmesini sağlar. Günümüzde birçok ülkede kolluk kuvvetlerince IBM, Microsoft, PredPol, Palantir, Hitachi gibi teknoloji firmalarınca bu amaçla üretilen yazılımlar kullanılmaktadır¹⁵⁹.

¹⁵⁸National Public Research, Market Profiling and Segmentation, <https://nationalpublicresearch.com/survey-types/market-profiling-segmentation/>.

¹⁵⁹Walter L. PERRY & Diğerleri, Predictive Policing: The Role of Crime Forecasting In Law Enforcement Operations, Rand Safety and Justice Program, 2013, s.1. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

1.3.3. Profillem ve Otomatik Karar Alma Uygulamaları ile Edinilen Çıkarımların Kişisel Veri Kavramı Açısından Değerlendirilmesi

Büyük veri dünyasında kişisel verilerin korunması ve mahremiyet bağlamında endişelere yol açan verilerden ziyade onlardan elde edilen çıkarımlardır. Kişisel verilerin korunmasına ilişkin hukuki düzenlemeler, profillem ve otomatik karar alma faaliyetleri de dahil olmak üzere herhangi bir veri işleme faaliyeti kapsamında işlenen verinin “kişisel veri” niteliğini haiz olması halinde uygulama alanı bulur. Bu çerçevede, ilgili kişilerin, kişisel verilerin korunması düzenlemeleri ile tanınan haklarını, profillem ve otomatik karar alma uygulamaları ile edinilen çıkarımlar açısından da kullanabilmeleri için bu çıkarımların kişisel veri niteliğine sahip olması gerekir. Çalışmanın bu bölümünde kişisel verilerin korunması düzenlemeleri tahtında kişisel veri kavramı ve çıkarımların hukuki niteliği incelenecektir.

1.3.3.1. Kişisel Verilerin Korunması Mevzuatında “Kişisel Veri” Kavramı

Kişisel veri, GVK Tüzüğü’nde ve KVK Kanunu’nda birbirine paralel şekilde, “kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanmıştır¹⁶⁰. Gerek uluslararası gerek ulusal mevzuat ve öğretide genel kabul gören kişisel veri kavramı tanımı uyarınca, kişisel veri bir kişinin kimliğini belirlemeye yarayan o kişi ile ilintili her türlü bilgiyi ifade etmektedir. Buna göre, kişisel verilerin korunması kapsamına giren bir veri işleme faaliyetinden söz edilebilmesi için, işlenen verinin (i) “bir gerçek kişiye ilişkin” olması ve (ii) bu kişinin kimliğinin “belirli ya da belirlenebilir” nitelikte olması gerekmektedir¹⁶¹. Gerek GVK Tüzüğü’nde gerekse KVK Kanunu’nda bazı verilerin özel nitelikli (hassas) kişisel veri olarak sınıflandırılarak, diğerler verilere göre daha fazla koruma altına alındığı görülür. İlgili düzenlemeler uyarınca, kişinin ırkı veya etnik kökeni, siyasi görüşleri, dini veya felsefi inancı, dernek, vakıf veya sendika

¹⁶⁰ Bkz. GVK Tüzüğü, m.4; KVK Kanunu, m.3/d.

¹⁶¹ Elif KÜZECİ, Kişisel Verilerin Korunması, 3. Baskı, Ankara, 2019, s.9.

üyeliğiliği, genetik verileri, biyometrik verileri, sağlığı ve cinsel hayatıyla ilgili veriler, özel nitelikli kişisel verilerdir¹⁶². Özel nitelikli kişisel veriler üzerinde gerçekleştirilecek veri işleme faaliyetleri birtakım kısıtlamalara ve özel güvenlik tedbirlerine tabi tutulmuştur. Özel nitelikli kişisel verilerin işlenebilmesi ancak ilgili düzenlemelerde öngörülen özel nitelikli kişisel verilerin işleme şartlarının gerçekleşmesi ve yeterli önlemlerin alınması ile mümkün kılınmıştır¹⁶³.

1.3.3.2. Profillemeye ve Otomatik Karar Alma Uygulamaları İle Ulaşılan Çıkarımların Hukuki Niteliği

İnsan beyninin bilgi edinme ve bilgiyi kullanma sürecine benzer şekilde, veriyle eğitilen yapay öğrenme algoritmaları da bu verilerin analiz edilmesi suretiyle bazı sonuçlar çıkarmakta veya diğer bir ifadeyle çıkarımlarda bulunmaktadır. Profillemeye ve otomatik karar alma mekanizmaları ile büyük veri setleri analiz edilerek, insan beyni ve mantığıyla tespit edilemeyecek ve hatta bazen kişinin kendisinin dahi farkında olmadığı olgulara ilişkin çıkarımlara ulaşılmaktadır. Bu çıkarımların bireyler üzerinde uygulanması suretiyle kişiler hakkında tahminde bulunma veya karar alma faaliyetleri gerçekleştirilmektedir. Bu bağlamda yapay öğrenme algoritmalarının kullandığı profillemeye ve otomatik karar alma mekanizmaları ile büyük verinin bir araya gelmesinin, kişisel veri kavramına önemli etki ve sonuçları bulunmaktadır. Yapay öğrenme algoritmaları ile geliştirilen modellerde, modelin geliştirilmesi için kullanılan veri setlerinde bulunan veriler kişisel veri niteliğine sahip olabileceği gibi, bu modele girdi (*input*) olarak sunulan veriler de kişisel veri olabilmektedir¹⁶⁴. Modelin uygulanması sonucunda ortaya çıkan veri, modelin geliştirilmesinde kullanılan ve modele girdi olarak verilen verilerden bağımsız olarak, kişisel veri olabilir veya olmayabilir¹⁶⁵.

¹⁶² Bkz. GVK Tüzüğü, m.9/1; KVK Kanunu, m.6/1.

¹⁶³ Bkz. GVK Tüzüğü, m.9/2-4; KVK Kanunu, m.6/4.

¹⁶⁴ Eylem AKSOY RETORNAZ & Osman Gazi GÜÇLÜTÜRK, “Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi”, Gelişen Teknolojiler ve Hukuk II: Yapay Zeka (Editörler: E. Eylem Aksoy Retornaz/Osman Gazi Güçlütürk), 1.Baskı, İstanbul Nisan 2021, s.285.

¹⁶⁵ Aksoy-Retornaz & Güçlütürk, s. 285.

Çalışmanın bu bölümünde, modelin uygulanması sonucu ulaşılan çıkarımların, yani çıktının (*output*) kişisel veri niteliğine sahip olup olmadığı incelenecektir.

29. Madde Çalışma Grubu'na göre, 4 tür veri söz konusudur. Bunlar genel olarak, ilgili kişi tarafından sağlanan veriler ve üçüncü kişilerce ilgili kişi hakkında oluşturulan veriler olmak üzere iki grup altında incelenebilir. İlgili kişi tarafından sağlanan veriler, doğrudan ilgili kişi tarafınca sağlanan veriler (*provided data*) ve dolaylı olarak ilgili kişi tarafından sağlanan veriler, diğer bir ifadeyle ilgili kişi hakkında gözlemlenen veriler (*observed data*) olmak üzere bir grubu; üçüncü kişilerce ilgili kişi hakkında oluşturulan verileri ise türetilen veriler (*derived data*) ve çıkarılan veriler (*inferred data*) olarak başka bir grubu oluşturur¹⁶⁶.

Doğrudan ilgili kişi tarafından sağlanan veriler, ilgili kişinin bizzat, bir bilgi formuna kişisel verilerini girmesi gibi bilinçli bir hareketi sonucunda paylaştığı kimlik bilgileri, adres bilgisi ve benzeri kişisel verileri ifade eder¹⁶⁷. Gözlemlenen veriler ise, ilgili kişinin bir hizmet veya cihazı kullanımı sonucu, örneğin sanal platformlardaki davranış ve hareketlerinin, konum verisinin, trafik verisinin veya bir sağlık uygulaması ile edinilen kalp atış verisinin gözlemlenmesi sonucu edinilen verilerdir¹⁶⁸. Bu bağlamda gözlemlenen veri de ilgili kişi tarafından sağlanan ancak doğrudan ilgili kişi tarafından sağlanan verilerden farklı olarak dolaylı veya pasif bir şekilde paylaşılan verilerdir¹⁶⁹.

İlgili kişi tarafından sağlanan verilerin aksine, türetilen ve çıkarılan veriler, doğrudan veya dolaylı olarak ilgili kişi tarafından sağlanmazlar. Bunlar, veri sorumlusu veya üçüncü kişilerin, ilgili kişi tarafından sağlanan verilerden yarattıkları verilerdir. Veri sorumlusunca ilgili kişinin halihazırda mevcut verilerinden türetilen verilere örnek olarak, her hafta aynı marketin çevrimiçi uygulamasından alışveriş yapan bir tüketicinin haftalık ortalama harcama tutarının

¹⁶⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8; Article 29 Working Party, Guideline on the Right to Data Portability, 16/EN WP 242 rev.01, 13 Aralık 2016, s.9, <https://ec.europa.eu/newsroom/article29/items/611233> (Kısaltılmışı “Data Portability”).

¹⁶⁷ Article 29 Working Party, Data Portability, s.9.

¹⁶⁸ Article 29 Working Party, Data Portability, s.9.

¹⁶⁹ Article 29 Working Party, Data Portability, s.10.

hesaplanması veya kişinin posta kodundan ikamet ettiği ülkenin belirlenmesi gösterilebilir¹⁷⁰. Çıkarılan veriler ise, diğer verilerin işlenmesiyle geliştirilir ve kişinin doğrudan veya dolaylı bir eylemi olmaksızın, örneğin tahminde bulunmak için veri kümelerindeki korelasyonları tespit etmek amacıyla gerçekleştirilen analitik bir sürecin sonucu olarak tanımlanabilir¹⁷¹. Kredi puanı, kişiselleştirilmiş hizmetler veya tavsiye mekanizmalarındaki veri işleme süreci sonucunda edinilen çıkarımlar, kişinin sağlık verilerinin analizi sonucunda belirli bir hastalığı geliştirme riskine yönelik değerlendirmelerin hepsi çıkarılan veri kategorisine girer¹⁷². Wachter ve Mittelstadt, çıkarılan verileri, “salt gözlem veya ilgili kişiden toplama yerine, çıkarım veya muhakeme yoluyla oluşturulan kimliği belirli veya belirlenebilir gerçek kişiyle ilgili bilgiler” olarak tanımlanmışlardır¹⁷³. Bu verilerin, ilgili kişinin doğrudan veya dolaylı bir eylemi ile sağlanmamasının doğal bir sonucu olarak ilgili kişinin kendisi hakkındaki bu verilerden haberdar olmaması söz konusu olabilmektedir¹⁷⁴. Öte yandan, çıkarılan veriler, bir veri analizinin sonucu olmakla birlikte, kişi hakkında bir tahminde bulunulması veya karar alınması gibi yeni veri oluşturma sürecinde de kaynak olarak kullanılmaktadır¹⁷⁵. İlgili kişinin doğrudan katılımının bulunmadığı ve yeterli bir farkındalığa sahip olmadığı analitik faaliyetleri sonucunda devamlı olarak daha çok yeni veri geliştirilmektedir¹⁷⁶.

Kişisel verilerin korunması mevzuatında “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanan kişisel veri kavramının üç ana unsuru bulunmaktadır. Bunlar, “kimliği belirli veya belirlenebilir bir gerçek

¹⁷⁰ Article 29 Working Party, Data Portability, s.9.

¹⁷¹ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.13,

¹⁷² Sandra WACHTER & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, s.22, <https://ssrn.com/abstract=3248829>(Kısaltılmışı “A Right to Reasonable Inferences”).

¹⁷³ Wachter & Mittelstadt, A Right to Reasonable Inferences, s.24.

¹⁷⁴ Wachter & Mittelstadt, A Right to Reasonable Inferences, s.22.

¹⁷⁵ Wachter & Mittelstadt, A Right to Reasonable Inferences, s.17.

¹⁷⁶ Bart CUSTERS, “Profiling As Inferred Data Amplifier Effects and Positive Feedback Loops”, Being Profiled: Cogitas Ergo Sum 10 Years of Profiling the European Citizen (Editörler: Emre Bayramlıoğlu, Irina Baraluic, Liisa Janssens, Mireille Hildebrandt), Amsterdam University Press, 2018, s.112-115.

¹⁷⁶ Custers, s.112-115.

kişi”, “her türlü bilgi” ve “bilginin kişiye ilişkin olması”dır. Verinin “kişisel veri” olarak kabul edilebilmesi için bu unsurların hepsini taşıyor olması gerekir. 29. Madde Çalışma Grubu, kişisel verilerin korunmasına ilişkin düzenlemelerdeki “kişisel veri” tanımını göz önüne alarak, herhangi bir verinin “kişisel veri” niteliğine sahip olup olmadığının tespiti için üç aşamalı bir değerlendirme modeli oluşturmuştur. Buna göre, bir verinin “kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin” olması için; (i) “amaç”, (ii) “içerik” veya (iii) “sonuç” unsurlarından en az birinin bulunması gerekmektedir¹⁷⁷. Çıkarımların “kişisel veri” niteliğine sahip olup olmadığı da bu unsurlar üzerinden değerlendirilmelidir. Bu unsurlardan birinin bulunması halinde, çıkarım ile ilgili kişi arasında bağlantı bulunduğu, diğer bir ifadeyle çıkarımın ilgili kişiye ilişkin olduğu kabul edilebilecektir¹⁷⁸.

İçerik unsuru, verinin “kimliği belirli veya belirlenebilir bir kişi hakkında” olmasını ifade eder¹⁷⁹. Amaç unsuru, “kimliği belirli veya belirlenebilir bir kişinin, davranışlarını, herhangi bir konudaki durumunu, performansını ve benzeri özelliklerini değerlendirmek amacıyla toplanan her türü verinin o kişiye ilişkin olduğunu” belirtir¹⁸⁰. Sonuç unsuru ise, kişisel verilerin işlenmesinin, “kimliği belirli veya belirlenebilir bir kişinin hakları ve menfaatleri üzerinde etkiye sahip olması halinde, işlenen verinin o kişiye ilişkin olduğunu” ifade eder¹⁸¹. Belirtmek gerekir ki, bu etkinin varlığının kabulü için, işlenen verinin ilgili kişinin diğer kişilerden farklı bir muamele görmesine yol açması yeterlidir¹⁸². 29. Madde Çalışma Grubu, işlemeye konu edilen verinin, kimliği belirli veya belirlenebilir bir gerçek kişinin hakları ve menfaatleri üzerinde bir etkiye sahip olmasının, “kişisel veri” olarak kabul edilmesi için yeterli olduğunu belirtmektedir¹⁸³. Bu çerçevede, verinin kimliği belirli veya belirlenebilir bir kişi hakkında olmaması veya kişinin

¹⁷⁷ Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP136, 20 Haziran 2007, s.11, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (Kısaltılmışı “Personal Data”).

¹⁷⁸ Article 29 Working Party, Personal Data, s.10-11.

¹⁷⁹ Article 29 Working Party, Personal Data, s.10.

¹⁸⁰ Article 29 Working Party, Personal Data, s.10.

¹⁸¹ Article 29 Working Party, Personal Data, s.11.

¹⁸² Article 29 Working Party, Personal Data, s.11.

¹⁸³ Article 29 Working Party, Personal Data, s.10-11.

davranışlarını, performansını, durumunu değerlendirmek amacıyla toplanmadığı durumlarda dahi, söz konusu verilerin işlenmesi kimliği belirli veya belirlenebilir bir kişinin hak ve menfaatleri üzerinde bir etki oluşturma potansiyeline sahipse, bu veriler kişisel veri olarak kabul edilecektir¹⁸⁴. Wachter ve Mittelstadt, 29. Madde Çalışma Grubu’nun 3 aşamalı değerlendirme modelinden yola çıkarak, ilgili kişiden ilk elden veya dolaylı olarak toplanan verilerin analiz edilmesiyle doğrudan açığa vurulamayan ancak bu verilerden “çıkarılan” veya “türetilen” verilerin, kişisel veri olduğu sonucuna varmışlardır¹⁸⁵. Wachter ve Mittelstadt, çıkarımların hukuki niteliğinin belirlenmesinde sonuç unsurunun “kilit unsur” olduğunu ileri sürmüştür¹⁸⁶.

Öte yandan çıkarımlar sadece sonuç unsuru bakımından değil, amaç ve içerik bakımından da ilgili kişi ile ilişkilendirilebilir¹⁸⁷. Buna göre, kişiye belirli bir şekilde muamele etmek amacıyla gerçekleştirilen profillemeye ve otomatik karar alma faaliyetlerinde, ulaşılan çıkarımlar amacı gereği ilgili kişiyle ilişkilendirilebilmektedir. İçerik bakımından kişiyle ilişkilendirilebilen çıkarımlara örnek olarak, 29. Madde Çalışma Grubu’nun örneği üzerinden, kişinin sağlık durumunun tespiti için tıbbi kayıtlarının algoritmalar ile analiz edilmesi gösterilebilir¹⁸⁸. Bu örnekte, kişinin sağlık durumuna ilişkin çıkarımlar, sağlık kayıtlarının içerik itibarıyla doğrudan ilgili kişi hakkında olması sebebiyle, kişisel veri olarak kabul edilecektir. Öte yandan, bu analiz sonuçlarının, bir sigorta şirketi tarafından kişinin sigorta poliçesi başvurusuna ilişkin kabul veya ret kararı verilmesi veya sigorta primlerinin belirlenmesi amacıyla kullanılması halinde, içerik unsurunun yanı sıra sonuç unsurunun da karşılanmış olacaktır¹⁸⁹.

¹⁸⁴ Article 29 Working Party, Personal Data, s.10-11.

¹⁸⁵ Wachter & Mittelstadt, A Right to Reasonable Inferences, s.26.

¹⁸⁶ Wachter & Mittelstadt, A Right to Reasonable Inferences, s.25.

¹⁸⁷ Article 29 Working Party, Personal Data, s.9-10.

¹⁸⁸ Article 29 Working Party, Personal Data, s.10.

¹⁸⁹ Günümüzde sigorta şirketleri sağlık kayıtlarının yanı sıra kişinin hayat tarzına ilişkin birçok farklı veriyi de analiz etmektedir. Kişinin neler satın aldığı, neler yediğinin ve günde kaç saat TV izlediğinin ödeyeceği sigorta primini belirlediği tespit edilmiştir. ProPublica’nın ilgili araştırması için bkz. Marshall ALLEN, Health Insurers Are Vacuuming Up Details About You- And It Could

Profilleme ve otomatik karar alma modelleri ile ulaşılan çıkarımların kişisel veri niteliğine sahip olduğu görüşünü destekleyen bir diğer olgu da kişisel veri tanımındaki “her türlü bilgi” ifadesidir¹⁹⁰. Kişisel veri, “kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi” yi ifade etmekle birlikte, bu ifade geniş bir kapsama sahiptir. Buna göre, bir kişiye ilişkin gizli bilgilerin yanı sıra gizli olmayan bilgiler, nesnel (objektif) bilgilerin yanı sıra düşünce, değerlendirme ve tahminler gibi öznel (subjektif) bilgiler ve hatta yanlış bilgiler kişisel verilerin korunması kapsamındadır¹⁹¹. Nitekim Avrupa Birliği Adalet Divanı, 20 Aralık 2017 tarihli ve C-434/16 sayılı Nowak kararında, kişisel veri tanımında “her türlü bilgi” ifadesinin kullanılmış olmasının AB yasama organının, kişisel veri kavramına geniş bir kapsam tanıma iradesini yansıttığından bahisle, kişisel verilerin özel nitelikli bilgilerle sınırlı olmadığı, belirli veya belirlenebilir bir gerçek kişiye “ilişkin” olması şartıyla, nesnel bilgilerin yanı sıra öznel görüş ve değerlendirmelerin de kişisel veri kapsamında olduğunu hüküm altına alınmıştır¹⁹². Nowak kararının, çalışmanın konusu açısından önemi, öznel görüş ve değerlendirmelerin de kişisel veri olarak kabul edilmiş olmasıdır. Zira çıkarımların veri setlerinin analiz edilmesiyle gerçekleştirilen değerlendirmelerin sonucu olduğu düşünüldüğünde, Nowak kararı çıkarımların kişisel veri niteliğine sahip olduğu görüşünü desteklemektedir. Ancak algoritmaların opak yapısının neden olduğu “kara kutu” özelliği sebebiyle, profillemeye ve otomatik karar alma uygulamaları ile ulaşılan çıkarımların gerçeği yansıttığını ve önyargı veya ayrımcılık içermediğini kanıtlayabilmek her zaman kolay değildir. Bu bağlamda, doğruluğu kanıtlanmamış bilgilerin de kişisel veri tanımındaki “her türlü bilgi” ifadesinin geniş kapsamına dahil olduğu göz önüne alındığında, profillemeye ve otomatik karar mekanizmaları ile ulaşılan çıkarımların kişisel veri olarak kabul edileceği sonucu doğmaktadır.

Raise Your Rates, ProPublica, 17 Temmuz 2018, <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>.

¹⁹⁰ Wachter & Mittelstadt, A Right to Reasonable Inferences, s.26.

¹⁹¹ Article 29 Working Party, Personal Data, s.6.

¹⁹² Avrupa Birliği Adalet Divanı’nın 20 Aralık 2017 tarihli ve C-434/16 sayılı Peter Nowak v. Data Protection Commissioner kararı için bkz. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=539376>.

Belirtmek gerekir ki Avrupa Birliği Adalet Divanı'nın bu konuda farklı kararları bulunmaktadır. Adalet Divanı Nowak kararından önceki bir kararında, görüşlerin dayandığı unsurların (*facts*) kişisel veri olduğuna ancak görüşlerin kişisel veri olarak kabul edilemeyeceğine hükmetmiştir¹⁹³.

Büyük veri setlerindeki çeşitli teknikler kullanılarak anonimleştirilmiş, yani kişisel verilerden arındırılmış veriler yapay zeka sistemleri ile analiz edilerek ilgili kişinin kimliğinin tespit edilmesi mümkün hale gelmiştir¹⁹⁴. Bu bağlamda büyük veri analitiğinin, kişisel veri kavramının “kimliği belirlenebilir bir gerçek kişiye ilişkin olma” unsurunu anlamsız kıldığını söylemek yanlış olmayacaktır¹⁹⁵. Öte yandan, büyük veri setlerinin analiz edilmesiyle üretilen çıkarımlar ile de ilgili kişi hakkında yeni kişisel verilere ulaşılabilmektedir. 29. Madde Çalışma Grubu'nun profillemeye ve otomatik karar alma sistemleri ile ilgili rehberinde de büyük veri setlerinin güncel teknolojiler ile analiz edilmesiyle edinilen yeni verilerin kişisel veri olduğu ifade edilmiştir¹⁹⁶. Bu durum kişisel veri kavramının genişlemesine neden olmaktadır¹⁹⁷. Purtova, kişisel veri kavramının genişlemesine ilişkin olarak, “Avrupa veri koruma hukukunun, her ne kadar en üst düzey hukuki koruma sağlamayı amaçlasa da pratikte uyulması imansız olan, mantıksız ve hakların kötüye kullanılmasına neden olduğu için göz ardı edilen veya itibarsızlaştırılan bir

¹⁹³ Avrupa Birliği Adalate Divanı'nın 17 Temmuz 2014 tarihli Y.S. v Minister voor Immigratie, Integratie en Asiel, Minister voor Immigraite, Integratie en Asiel v.M (in joined cases C-141/12 and C-372/12 C-141/12) kararı için bkz. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=155114&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6466149>.

¹⁹⁴ Kişisel verilerden arındırılmış haldeki veri setlerinin, gelişmiş yapay zeka teknolojileri ve büyük veri analizi yöntemleri ile günümüzde sıklıkla gerçek kişiler ile ilişkilendirildiği olaylar yaşanmaktadır. Görünüşte anonim olan verilerin bir gerçek kişiyle ilişkilendirilmesi halinde (İng. *reidentification*) bu veriler artık kişisel veri niteliği kazanmaktadır.

¹⁹⁵ Omer TENE & Jules POLONETSKY, Big Data for All: Privacy and User Control in the Age of Analytics, *Northwestern Journal of Technology and Intellectual Property*, (11:5), 2013, s. 258, <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip>.

¹⁹⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8.

¹⁹⁷ E. Eylem AKSOY RETORNAZ & Osman Gazi GÜÇLÜTÜRK, “Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi”, *Gelişen Teknolojiler ve Hukuk II: Yapay Zeka* (Editörler: E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk), 1.Baskı, İstanbul, 2021, s.280.

“her şeyin kanunu” (“*law of everything*”) haline gelme riskiyle karşı karşıya olduğunu” ileri sürmüştür¹⁹⁸.

Çıkarımlar, bazı durumlarda ise özel nitelikli kişisel veri oluşturur. GVK Tüzüğü’nün 9. maddesinde özel nitelikli kişisel verinin tanımı yapılmıştır. Bu tanım uyarınca, kişinin “ırk veya etnik kökenini, siyasi görüşlerini, dini veya felsefi inançlarını ya da sendika üyeliğini açığa çıkaran” veriler özel nitelikli kişisel veri olarak kabul edilir. 29. Madde Çalışma Grubu, çeşitli tavsiye ve görüşlerinde, çıkarımların özel nitelikli kişisel veri oluşturma olasılığı bulunduğunu kabul eden değerlendirmelerde bulunmuştur. 29. Madde Çalışma Grubu, GVK Tüzüğü’nün 9. maddesindeki “özel nitelikli kişisel veri” tanımına atıf yaparak, tanımdaki “açığa çıkaran” ibaresinden, sadece doğası gereği hassas bilgiler içeren verilerin yanı sıra bir kimseye ilişkin hassas bilgilere ulaşılmasını sağlayan verilerin de özel nitelikli kişisel veri kapsamında olduğu sonucunun doğduğuna işaret etmiştir¹⁹⁹. Çalışma Grubu’nun profillemeye ve otomatik karar alma ile ilgili rehberinde de profillemeye faaliyeti ile ulaşılan çıkarımların “özel nitelikli kişisel veri” oluşturabileceği belirtilmektedir²⁰⁰. Kişinin sosyal medya hesaplarındaki beğenilerinden ve takip ettiği kişi ve sayfalardan siyasal görüşüne ilişkin bir çıkarımda bulunulması buna örnek olarak gösterilebilir. Benzer şekilde, çevrimiçi yemek siparişi ve market alışverişlerine ilişkin veriler ile sipariş edilen yemek veya yiyeceklerin besin değerleri ile ilgili verilerin birlikte değerlendirilmesi sonucu kişinin sağlık durumuna ilişkin çıkarımlarda bulunulabilecektir²⁰¹.

Büyük veri ile algoritmaların bir araya gelmesi, bireylerin mahremiyet hakkını ihlal eden şekilde gerçekleştirilen algoritmik çıkarımlarda da artışa neden olmuştur. Örneğin Facebook algoritmalarının, kullanıcıların çevrimiçi

¹⁹⁸ Nadezdha PURTOVA, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 2018 Law, Innovation and Technology 10(1), 9 Eylül 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355.

¹⁹⁹ Article 29 Working Party, Advice Paper on Special Categories of Data (“Sensitive Data”), 20 Nisan 2011, s.4, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (Kısaltılmışı “Special Categories of Data”).

²⁰⁰ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.15.

²⁰¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.15.

davranışlarının izlenmesi suretiyle cinsel yönelimlerine, siyasi görüşlerine, ırkçı düşünce ve eğilimlerine, ruhsal durumlarına ve hatta intihara eğilimlerine ilişkin çıkarımlarda bulunduğu bilinmektedir²⁰². Avrupa Birliği Veri Koruma Kurumu, Facebook kullanıcılarının ABD’deki başkanlık seçimleri sürecinde siyasi amaçlar için manipüle edildiğini ortaya çıkaran Cambridge Analytica skandalına²⁰³ atıfta bulunarak, bireyin politik düşüncelerini açığa çıkaran verilerin “özel nitelikli kişisel veri” olarak kabul edilmesi gerektiğine ilişkin bir beyanname yayınlamıştır²⁰⁴. Öte yandan, veri sorumlusunun profillemeye faaliyetini, ilgili kişi hakkında özel nitelikli veri niteliğinde çıkarımlarda bulunma niyetiyle gerçekleştirmiş olup olmadığı, söz konusu işleme faaliyetinin özel nitelikli kişisel verilerin işleme şartlarına tabi olup olmayacağını belirlemektedir.

Birleşik Krallık Bilgi Komisyonu Ofisi, çıkarımların özel nitelikli kişisel veri kategorisinde ve Tüzüğün 9. maddesinin uygulama alanı kapsamında kabul edilebilmesini, (i) ilgili çıkarımın ne derece doğru ve kesin bir bilgiyi ifade ettiğine ve (ii) veri sorumlusunun bu çıkarımı bilerek gerçekleştirip gerçekleştirmediğine bağlı olduğunu belirtmiştir²⁰⁵. Bilgi Komisyonu Ofisi’nin görüşüne göre, ilgili çıkarım “makul bir kesinlik derecesi” ne sahipse, özel nitelikli kişisel veri kategorisinde olması muhtemeldir. Öte yandan, ulaşılan çıkarımlar, yalnızca

²⁰² Annie PALMER, Facebook may be Developing a System to Automatically Detect How Rich or Poor You are: Patent Reveals How the Site Could Track Your Socioeconomic Status, 2 Şubat 2018, <https://www.dailymail.co.uk/sciencetech/article-5346733/Facebook-patent-uses-track-socioeconomic-status.html>; Julia ANGWIN & Madeleine VARNER & Ariana TOBIN, Facebook Enables Advertisers to Reach Jew Haters, 14 Eylül 2017, <https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters>; Benjamin GOGGIN, Inside Facebook’s Suicide Algorithm: Here’s How the Company Uses Artificial Intelligence to Predict Your Mental Health, 6 Ocak 2019, <https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12>; Teo ARMUS, Facebook Can Tell Whether You’re Gay Based on a Few ‘Likes’, Study Says, 23 Kasım 2017, <https://www.nbcnews.com/feature/nbc-out/facebook-can-tell-if-you-re-gay-based-few-likes-n823416>.

²⁰³ Hannes GRASSEGER & Mikael KROGERUS, The Data That Turned the World Upside Down, 28 Ocak 2017, <https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win>.

²⁰⁴ European Data Protection Board, Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns, 13 Mart 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

²⁰⁵ Information Commissioner’s Office, Guide to Data Protection, What is Special Category Data?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>.

doğruluğu “muhtemel” bir bilgiyi ifade ediyor ise, bu çıkarımın doğru olduğu ortaya çıksa dahi, eğer veri sorumlusu bu çıkarım temelinde bir kimseye farklı muamelede bulunmak amacı gütmüyorsa, özel nitelikli veri kategorisinde kabul edilmemelidir. Birleşik Krallık Bilgi Komisyonu Ofisi’nin örneği üzerinden konu somutlaştırılabilecektir. İş başvurusunda bulunan kişinin özgeçmişine göre işitme engelli kişilere destek amaçlı kurulmuş bir derneğin yöneticisi olarak çalışmış olmasından kişinin işitme engelli olması gerektiği çıkarılamaz. Ancak eğer başvuruyu alan şirket, başvuran kişi hakkında farklı kaynaklardan topladığı verilerle bu bilgiyi beraber değerlendirerek kişinin işitme engelli olduğunu doğrulayabiliyorsa, bu durumda özel nitelikli kişisel verilerin işlenmesi için gereken şartlara tabi olacaktır²⁰⁶.

Bilgi Komisyonu Ofisi’nin aynı görüşünde belirttiği üzere, kişinin dini veya etnik kökeni gibi özel nitelikli kişisel verilerinin, isim veya resim gibi verilerinden çıkarılması mümkündür. Zira birçok soyadı belirli bir etnik kökene veya dine işaret eder. Ancak bu durum kişinin ad-soyad bilgisinin her durumda özel nitelikli kişisel veri kategorisinde işlenebileceği anlamına gelmemektedir. Kişinin ad soyad bilgisinin sadece bir müşteri veritabanında tutulması suretiyle işlenmesi halinde, özel nitelikli kişisel verilerin işlenmesine ilişkin şartların varlığı aranmaz. Öte yandan, soyad bilgisinin, örneğin çevrimiçi davranışsal reklamcılık faaliyetleri kapsamında özellikle etnik köken veya din bilgisine göre hedefleme gerçekleştirilmesi amacıyla işlenmesi durumunda, özel nitelikli kişisel veri işlendiği kabul edilir. Aynı şekilde, kişinin etnik kökeni, dini inancı, siyasi görüşleri, sağlık durumu, cinsel yönelimi gibi özel nitelikli kişisel verileri hakkında çıkarımda bulunan bir profillemeye faaliyeti gerçekleştirildiğinde, özel nitelikli kişisel verilerin işlenmesine ilişkin şartlar uygulanacaktır. Kişisel verilerin işlenmesine ilişkin şartların uygulanabilirliği açısından çıkarımların doğru olup olmadığı değil, özel nitelikli kişisel veri kategorilerinden biriyle ilgili bir çıkarımın,

²⁰⁶Information Commissioner’s Office, Guide to Data Protection, What is Special Category Data?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>.

işletmenin karar ve faaliyetlerine etki edecek şekilde kullanılıyor olması belirleyici olacaktır²⁰⁷.

1.3.4. Avrupa Birliği Genel Veri Koruma Tüzüğü’ndeki Özel Tanımlar ve Düzenlemeler

Profilleme için veri toplanması, profilin kişiye uygulanması ve profillemeye veya otomatik işlemeye dayalı bir karar alınması faaliyetleri kapsamındaki tüm veri işleme süreçleri, veri koruma düzenlemelerine uygun şekilde gerçekleştirilmelidir. Çalışmanın bu bölümünde, profilleme ve otomatik karar alma kavramlarına ilişkin GVK Tüzüğü’ndeki tanımlayıcı düzenlemeler ile birlikte, profilleme, otomatik karar alma ve profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma (“*solely automated decision making including profiling*”) kavramlarının birbiriyle ilişkisi incelenecek ve değerlendirilecektir.

GVK Tüzüğü’ndeki düzenlemelerden profillemenin kullanılabileceği üç muhtemel veri işleme faaliyeti ortaya çıkmaktadır:

- (i) Genel profilleme;
- (ii) Profillemeye dayalı karar alma; ve
- (iii) “İlgili kişi hakkında hukuki veya benzer derecede önemli şekilde etki doğuran, profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma” (GVK Tüzüğü, m.22)²⁰⁸.

GVK Tüzüğü’nün 4.maddesinde profilleme, “kişinin iş yerindeki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya davranışlarına ilişkin bilgilerin analiz edilmesi ya da tahmin edilmesi başta olmak üzere, ilgili kişiye ait belirli kişisel

²⁰⁷ Information Commissioner’s Office, Guide to Data Protection, What is Special Category Data?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>.

²⁰⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8.

özelliklerin değerlendirilmesine yönelik kişisel verilerin kullanılmasını gerektiren her türlü otomatik kişisel veri işleme biçimi”²⁰⁹ olarak tanımlanmıştır²¹⁰. Tanımdaki “otomatik işleme”, bilgisayar, cep telefonu, tablet gibi işlemciye sahip cihazlar tarafından, algoritmalar aracılığıyla, insan müdahalesi olmadan kendiğinden gerçekleşen işleme faaliyetini ifade eder²¹¹. Bu bağlamda, GVK Tüzüğü hükümlerinin uygulama kapsamına giren bir profillemenin mutlaka herhangi bir otomatik işleme biçimi içermesi gerekmele birlikte, sürece bir insanın katılımı her zaman faaliyeti tanımın kapsamı dışına çıkarmaz²¹². Profillemeye faaliyetinin, (i) bir kişi veya grup hakkında veri toplanması, (ii) toplanan verilerin çeşitli korelasyonların tespit edilmesi amacıyla analiz edilmesi, (iii) tespit edilen korelasyonların kişinin halihazırdaki veya gelecekteki davranışlarına ilişkin özelliklerin belirlenmesi amacıyla ilgili kişiye uygulanması aşamalarının tamamında, veri sorumluları, veri koruma düzenlemelerinin gerekliliklerini yerine getirmekle yükümlüdür²¹³.

Profillemeye kişinin birtakım bireysel özelliklerinin tespit edilmesi amacıyla verilerin analiz edilmesini gerektirmektedir. Bu analiz, kişi hakkında bir karar alınması ile sonuçlanabileceği gibi, herhangi bir karara varılmadan sadece profillemeye işlemi olarak da kalabilir. Öte yandan, profillemenin ardından kişi hakkında bir karar alınması halinde, bu karar sürecinde bir insan müdahalesi olabileceği gibi, tamamen otomatik ve insan müdahalesinden bağımsız şekilde de gerçekleştirilebilir. Herhangi bir şekilde bir insan müdahalesi bulunmaksızın, tamamen algoritmalar aracılığıyla verilerin kararlar, çalışmanın ilgili bölümünde incelendiği üzere, toplumsal açıdan olumsuz etkilere neden olabilmektedir²¹⁴. Algoritmik karar mekanizmalarının şeffaf olmayan veri işleme süreçleri ve birey

²⁰⁹ GVK Tüzüğü’nün Avrupa Birliği Bakanlığı tarafından yapılan Türkçe çevirisi için bkz. <https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-Türkçe-Çeviri-AB-Bakanlığı.pdf>.

²¹⁰ Bkz. GVK Tüzüğü, m.4/4.

²¹¹ Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, s.22.

²¹² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.7.

²¹³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.7.

²¹⁴ Çalışmanın “1.3.5. Profillemeye ve Otomatik Karar Alma Uygulamalarının Bireyler Üzerindeki Olumsuz Etkileri” başlıklı bölümü için bkz. s.50.

hakkında ayrımcı, önyargılı, adil olmayan kararlar alınmasına neden olma potansiyeli göz önüne alınarak, bireyin karar alıcı karşısındaki konumunu güçlendirmek amacıyla GVK Tüzüğü'nün 22. maddesinde özel bir düzenlemeye yer verilmiştir. Tüzüğün 22. maddesi ile ilgili kişinin kendisi hakkında hukuki veya benzer şekilde önemli sonuçlar doğuran, “profilleme de dahil olmak üzere üzere tamamen otomatik işlemeye dayalı” kararların konusu olmamayı talep edebilmesi mümkün kılınmıştır²¹⁵. Bu düzenleme ile ilgili kişiye tamamen otomatik işlemeye dayalı gerçekleşen, diğer bir ifadeyle hiçbir şekilde insan müdahalesi bulunmayan karar alma faaliyetlerinin konusu olmama seçeneği sunulmaktadır. Tüzüğün 22. maddesiyle getirilen bu düzenleme kişisel verilerin korunması düşüncesinin temelinde yatan bireysel özerklik ve bilgilerin geleceğini belirleme hakkı kavramları ile doğrudan ilgilidir²¹⁶.

Konuyu, bireysel kredi başvurusu örneği üzerinden somutlaştırmak faydalı olacaktır. Bir kişinin bir bankaya tüketici kredisi başvurusunda bulunması örneğinde, kredi talebinin onaylanıp onaylanmayacağı kararı, kişi hakkında algoritmalar aracılığıyla hesaplanan ve kişinin kredi profilini temsil eden kredi puanına bakılarak bir banka temsilcisi tarafından veriliyor ise, bu durumda profillemeye dayalı bir karar alma söz konusudur. Ancak bu karar “tamamen otomatik işlemeye dayalı” bir karar değildir. Öte yandan, eğer bu karar bir insan tarafından değerlendirmeye tabi tutulmaksızın tamamıyla bir algoritma tarafından verilir ve başvurucuya da otomatik olarak bildirilirse, bu durumda GVK Tüzüğü tahtında 22.maddede hüküm altına alınan “profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma” söz konusudur²¹⁷.

KVK Kanunu'nda, Tüzüğün 4. maddesindeki gibi bir profilleme tanımı yapılmamış olmakla birlikte, Kanun'un ilgili kişinin haklarının düzenlendiği 11. maddesinde, ilgili kişinin “kendisi hakkında verilerinin otomatik sistemler aracılığıyla analiz edilmesi halinde kendisi aleyhine bir sonucun ortaya çıkmasına

²¹⁵ Bkz GVK Tüzüğü, m.22/1.

²¹⁶ Küzeci, s.230.

²¹⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.8-9.

itiraz edebileceği” düzenlenmiştir²¹⁸. KVK Kanunu’nun 11/g maddesi, Kanun’daki profillemeye ve otomatik karar alma faaliyetlerine atıf yapılan tek düzenlemedir.

1.3.5. Profillemeye ve Otomatik Karar Alma Uygulamalarının Bireyler Üzerindeki Olumsuz Etkileri

Profillemeye ve otomatik karar alma uygulamaları, kurum ve şirketlere ekonomik verimliliğin ve kaynak tasarrufunun artırılması gibi birçok fayda sağlamakla birlikte, kişisel verilerin korunması ve mahremiyet açısından birçok sorunu da beraberinde getirmiştir. Birleşmiş Milletler İnsan Hakları Konseyi, 23 Mart 2017 tarihli ilgili kararında, profillemeye ve otomatik karar alma uygulamalarının ayrımcılığa neden olma ve ekonomik, sosyal ve kültürel haklar da dahil olmak üzere insan haklarının kullanılmasını olumsuz şekilde etkileme potansiyeline sahip kararlara yol açabileceğinden endişe duyulduğunu vurgulamıştır²¹⁹. Aşağıda detaylı olarak inceleneceği üzere, kişisel verilerin opak bir süreçte işlendiği profillemeye ve otomatik karar alma uygulamaları bireyler hakkında ayrımcı, önyargılı, hatalı, mahremiyeti ihlal eden çıkarımlar üretilmesine neden olmaktadır. Öte yandan bireyler çoğunlukla profillemeye ve otomatik karar alma faaliyetlerinin farkında dahi değildir. Farkında olsalar bile bu sürecin nasıl gerçekleştiğini anlamaları oldukça zordur. Bu durum, bireyin mahremiyetinin, kişisel verilerin korunması hakkının, ifade özgürlüğünün ve bilgilerin geleceğini belirleme hakkının zarar görmesine neden olmaktadır²²⁰.

²¹⁸ Bkz. KVK Kanunu, m.11/g.

²¹⁹ UN General Assembly Human Rights Council, Resolution adopted by the Human Rights Council on 23 March 2017, A/HRC/RES/34/7, s.3, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement>.

²²⁰ Kaya, Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge, s.53; Wachter & Mittelstadt, A Right to Reasonable Inferences, s.17-19.

1.3.5.1. Kişisel Verilerin Korunması ve Mahremiyet Hakkına İlişkin Riskler

Günümüzde büyük veri kavramının doğmasını sağlayan gelişmeler, yapay zeka teknolojilerindeki gelişmelere de ivme kazandırmıştır. Büyük veri analitiği teknolojilerindeki hızlı gelişmeler de sunduğu kolaylık ve avantajların yanında, bireyin temel hak ve özgürlükleri açısından tehlikeler barındırmaktadır. Büyük veri analitiği teknolojilerinde algoritmaların kullanılması, algoritmaların otonom özelliği, veri işleme sürecinin opak bir şekilde gerçekleşmesi, bu sistemlerin gerektiği kadar değil tüm veriyi toplama ve toplama amacıyla farklı bir amaç için işleme eğilimi, doğruluğu kesin olmayan, belirli bir olasılık hesabının sonuçlarını yansıtan çıktılar üretmesi, bireyin kişisel verilerin korunması ve mahremiyet hakkı açısından çeşitli riskler doğurmaktadır²²¹.

Tüm veri işleme faaliyetleri gibi, profillemeye ve otomatik karar alma faaliyetleri de veri koruma ilkelerine uygun gerçekleştirilmelidir. Ancak, büyük veri analitiği uygulamalarının belirtilen özellikleri, kişisel verilerin korunmasına hakim olan temel ilkelerin profillemeye ve otomatik karar alma uygulamaları açısından uygulanabilirliği ile ilgili sorunların doğmasına neden olmaktadır. Yapay zeka sistemlerinin doğasından kaynaklanan “kara kutu problemi”, özellikle kişisel verilerin hukuka uygun olarak işlenmesi, şeffaflık ve hesap verebilirlik ilkelerinin uygulanabilirliği, veri sorumlusunun aydınlatma yükümlülüğü ve ilgili kişinin bilgilendirilme hakkı bakımından çeşitli sorunlara neden olmaktadır. Öte yandan, kara kutu problemi, profillemeye ve otomatik karar alma sistemlerinin güvenilirliği ve açıklanabilirliği ile ilgili tartışmaları da beraberinde getirmiştir²²².

²²¹ Information Commissioner’s Office, Big Data, Artificial Intelligence, Machine Learning and Data Protection, 20170904, Version 2.2, s.9; Aksoy Retornaz & Güçlütürk, s. 279; Matthew U. SCHERER, Regulating Artificial Intelligence Systems: Risks, Challenges Competencies, and Strategies, Harvard Journal of Law & Technology, Vol.29, No.2, 2016, s. 363, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609777.

²²² Gerek yapay zeka konusunda çalışmalar yürüten uluslararası girişim ve kuruluşlar gerekse de çeşitli ülkelerdeki ulusal aktörler tarafından güvenilir yapay zeka (*trustworthy artificial intelligence*) ve açıklanabilir yapay zeka (*explainable artificial intelligence*) konularında birçok çalışma mevcuttur. İlgili çalışmaların listesi için bkz. European Parliamentary Research Service (EPRS), The Ethics of Artificial Intelligence Issues and Initiatives, Panel for the Future of Science and Technology, Mart 2020, s.37-42, [https://www.europarl.europa.eu/stoa/en/document/EPRS_STU\(2020\)634452](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)634452) (Kısaltılmışı “The

Kişisel verilerin korunmasının çıkış noktası olan mahremiyetin korunması, insan onurunun ve kişiliğin geliştirilmesine hizmet eder²²³. Mahremiyet ve kişisel verilerin korunması hakkının bireysel özerklik, bütünlük ve kendi kaderini tayin hakkı gibi unsurları, temelde insan onuruna dayanmaktadır²²⁴. Bireyin mahremiyetinin ve kişisel verilerin korunması hakkının korunmasını amaçlayan hukuki düzenlemelerin, profillemeye ve otomatik karar alma faaliyetleri açısından etkin bir şekilde uygulanabilir olup olmadığı ile ilgili çeşitli sorunlar mevcuttur. Yapay zekanın doğasından ileri gelen özelliklerinin sebep olduğu bu sorunlar, demokratik bir toplumun temel gerekliliklerinden olan eşit insan onuru anlayışı ve bireyin kendi kaderini belirleyebilme gücüne duyulan ihtiyaç açısından endişeler yaratmaktadır.

Çalışmanın ilerleyen bölümlerinde, kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin, profillemeye ve otomatik karar alma uygulamaları bağlamında, bireylerin mahremiyet ve kişisel verilerin korunması haklarını güvence altına alarak hukuka uygun, adil ve şeffaf bir şekilde gerçekleştirilmesi için yeterli ve etkili bir koruma sağlayıp sağlamadığı konuyla ilgili görüş ve tartışmalar çerçevesinde incelenecektir.

Ethics of Artificial Intelligence Issues and Initiatives”). Avrupa Komisyonu Yapay Zeka Üst Düzey Uzman Grubu’nun güvenilir yapay zekaya ilişkin etik rehberi için bkz. European Commission High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

²²³ Kama Işık, s.40.

²²⁴ Kama Işık, s.19-40.

1.3.5.2. Algoritmik Önyargı ve Ayrımcılık

Günümüzde satın alacağımız üründen, dinleyeceğimiz şarkıya, sosyal medyada kimle arkadaş olacağımızdan hangi filmi izleyeceğimize kadar farklı tavsiyelerde bulunan farklı algoritmalar mevcuttur. Ancak algoritmalar sadece tavsiye sistemlerinde değil, insan hayatına etkisi oldukça ciddi olabilecek önemli kararların alınması için de kullanılmaktadır. Kimin bankadan kredi alabileceğine, kimin özgeçmişinin bir insan kaynakları yöneticisi tarafından incelenmeye değer olduğuna, kimin ne kadar süre tutuklu kalacağına artık algoritmalar ile karar verilebilmektedir. Ancak profilleme ve otomatik karar alma mekanizmaları, bireyler hakkında adil olmayan, ayrımcı veya önyargılı kararların alınmasına neden olabilmektedir²²⁵. Algoritmik karar mekanizmalarının kullanılması çeşitli faydalar sağlamakla birlikte, bu kararlar sonucunda bireyler adil olmayan bir şekilde bazı fırsatlardan mahrum kalabilmekte, bazı hizmetlere erişimleri sınırlandırılabilen ve hatta haksız ve hukuka aykırı bir şekilde özgürlüklerinin kısıtlanabilmektedir.

Algoritmik karar mekanizmalarında önyargı, farklı gruplar arasında bir grup aleyhine karar alınmasını haklı gösterecek herhangi bir ayrım bulunmamasına rağmen, sistematik olarak belirli bir gruptaki insanlar aleyhine sonuçlar üretilmesini ifade eder²²⁶. Algoritmik önyargı ve ayrımcılığın birçok farklı sebebi bulunur. Öncelikle, algoritmaların her zaman bir insan tarafından tasarlandığı göz önüne alındığında, programcının önyargıları, algoritmanın ayrımcı ve önyargılı çıktılar üretmesine neden olabilir²²⁷. Eğitim verisinin doğruluğu kesin olmayan, eksik veya tarihsel önyargı veya adaletsizlikleri yansıtan verilerden oluşması halinde, bu verilerin analiz edilmesi ile oluşturulan profiller, yine ayrımcı ve önyargılı kararlara neden olabilmektedir. Bu bağlamda, önyargılı algoritmaların, programcı önyargılı

²²⁵ Claire CAIN MILLER, Algorithms and Bias: Q. and A. With Cynthia Dwork, NY Times, 10 Ağustos 2015, <https://www.nytimes.com/2015/08/11/upshot/algorithms-and-bias-q-and-a-with-cynthia-dwork.html>.

²²⁶ Nicol Turner LEE & Paul RESNICK & Genie Barton, Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms, Brookings Institute, 22 Mayıs 2019, <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>.

²²⁷ The Civil Liberties Union for Europe (Liberties), Algorithmic Bias: Why And How Do Computers Make Unfair Decisions?, 2021, <https://www.liberties.eu/en/stories/algorithmic-bias-17052021/43528>.

olmasa veya ayrımcılık yapma niyetinde olma dahi, belirli gruplar açısından adil olmayan, önyargılı ve ayrımcı sonuçlar üretme riski bulunmaktadır²²⁸. Öte yandan, programcının sahip olduğu önyargı veya eğitim verisinin barındırdığı önyargıdan bağımsız olarak algoritmanın kendisi de önyargılı olabilir²²⁹. Algoritmik sistemlerin beslendikleri verilerin herhangi bir gerçeğe aykırılık veya önyargı içermediği hallerde dahi, yapay öğrenme sürecinde verilerin birbirleriyle olan etkileşimi de ayrımcı ve önyargılı sonuçlar üretebilmektedir²³⁰. Algoritmik karar sistemlerinde önyargı ve ayrımcılığın en yaygın sebeplerinden bir diğeri ise, yapay öğrenme uygulamalarının sadece belirli demografik grupları veya kalıplaşmış toplumsal önyargıları yansıtan veriler ile eğitilmesidir. Yapay öğrenme algoritmalarını eğitmek için kullanılan veriler, belirli insan gruplarını, diğerlerine nispeten daha fazla yansıtıyor ise, üretilen çıkarımlar eğitim verisinde temsil edilmeyen ya da yeterince temsil edilmeyen gruplar açısından haksız ve ayrımcı etkilere neden olabilmektedir²³¹.

Her ne kadar veri analitiğinin sayılara dayandığından bahisle insan kararlarında önemli bir etkiye sahip olan önyargılı düşünceleri kodlamadığı ve dolayısıyla da nesnel çıktılar ürettiği ileri sürülse de algoritmaların dikkatli kullanılmaması halinde önyargıları sürdürdüğü ve önyargıların güçlenmesine neden olduğu ortaya çıkmıştır²³². Verideki örüntüleri çıkaran yapay öğrenme algoritmaları, veride toplumdaki önyargılı bir yaklaşımın kodlanmış olması halinde, çoğunlukla bu önyargılı örüntüyü üreteceği çıktılarda esas almaktadır²³³. Herhangi bir konudaki önyargılı bir yaklaşım veya ilişki toplumsal hayatta ne kadar

²²⁸ EPRS, The Ethics of Artificial Intelligence: Issues and Initiatives, s.15.

²²⁹ David DANKS & Alex John LONDON, Algorithmic Bias in Autonomous Systems, Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17) 2017, s.4693, https://www.researchgate.net/publication/318830422_Algorithmic_Bias_in_Autonomous_Systems.

²³⁰ Frederik Zuiderveen BORGESIU, Discrimination, Artificial Intelligence And Algorithmic Decision Making, s.21, <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>.

²³¹ Nicole TURNER LEE & Paul RESNICK & Genle BARTON, Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms, 2019, <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>.

²³² Kelleher & Tierney, s.135.

²³³ Kelleher & Tierney, s.135.

yerleşmişse, veri setlerindeki önyargılı örüntünün görünürlüğü de o derece kuvvetlenmekte, bu ise algoritmaların bu önyargı örüntüsünü kopyalama ihtimalini artırmaktadır²³⁴.

Günümüzde çevrimiçi istihdam platformlarında, dijital reklamlarda, sınav değerlendirme algoritmalarında, yüz tanıma teknolojilerinde ve ceza yargılama algortimalarında algoritmik önyargı (*algorithmic bias*) ve algoritmik ayrımcılık (*algorithmic discrimination*) ile karşılaşıldığına dair birçok örnek mevcuttur. Aşağıda sırasıyla yakın tarihli örneklerle yer verilmiştir.

2020 yılında İngiltere’de üniversiteye geçiş puanının hesaplanması için yapılan lise bitirme sınavlarının COVID-19 pandemisi sebebiyle iptal edilmesinden sonra öğrencilerin üniversiteye giriş puanlarını belirlemek için geliştirilen bir algoritma kullanılmıştır. Liseden üniversiteye geçmeye hazırlanan öğrenciler, üniversiteye geçiş sınavlarından aldıkları puanlar yerine, sınav puanlarını ve yerleştirme sonuçlarını düzenleyen yetkili kurum olan Ofqual (*The Office of Qualifications and Examinations*) tarafından geliştirilen ve öğrencilerin okul dönemi boyunca aldıkları notların ve bireysel başarılarının yanında, okudukları okulun tarihsel başarısına göre her öğrenci için bir puan tahmininde bulunan algoritmanın çıkardığı sonuçlara göre üniversite tercihlerini yapmak durumunda kalmışlardır. Algoritma, özel okullardaki öğrenciler için tahmin edilen puanları olması gerekenden yüksek, çoğunlukla daha dar gelirli ailelerden gelen Afrika kökenlilerin, Asyalıların ve etnik azınlıkların okuduğu büyük devlet okullarındaki öğrenciler için tahmin edilen puanları olması gerekenden düşük hesaplamıştır. Diğer tüm algoritmik karar alma mekanizmaları gibi, Ofqual algoritması da geçmiş tarihli veri setlerindeki örüntüleri tespit ederek geleceğe yönelik tahminde bulunmak için tasarlanmıştır. Buna bağlı olarak ise derslerinde aldıkları iyi notlara

²³⁴ Kelleher & Tierney, s.135.

rağmen okudukları okulun tarihsel başarısının düşük olması sebebiyle algoritma tarafından puanı düşürülen binlerce öğrenci mağdur olmuştur²³⁵.

Harvard Üniversitesi profesörlerinden Latanya Sweeney'in yürüttüğü bir araştırmada, arama motorlarında Afro-Amerikalı kişilere ait isimlerin aratılması halinde, arama sonuçlarında bu isimlerle ilişkilendirilen tutuklama haberlerinin gösterilme ihtimalinin beyaz Amerikalı kişilere ait isimlerle ilgili sorgulamalara nazaran daha yüksek olduğu tespit edilmiştir. Öte yandan aynı araştırmada, yüksek faizli kredi kartları ve diğer bazı finansal ürünlere ilişkin gerçekleştirilen hedefleme ve pazarlama faaliyetlerinde, Afro-Amerikalı kişilerle beyaz Amerikalı kişiler arasında ayrımcılık yapıldığı ifade edilmiştir²³⁶.

Düyanın en büyük elektronik ticaret şirketlerinden biri olan Amazon, kullandığı işe alım algoritmasının cinsiyet ayrımcılığı içeren kararlar aldığını tespit ederek algoritmanın kullanımına son vermiştir. Algoritmayı yaratan mühendisler, algoritmayı oluştururken Amazon'a son 10 yıl içinde yapılan ve ağırlıklı olarak beyaz erkeklere ait iş başvurularına ait verileri kullanmışlardır. Algoritma, ilgili iş için gerekli beceriler yerine özgeçmişlerdeki kelime örüntüsünü tanımayı öğrenmiş ve girdi olarak kullanılan veri erkeklere ait olduğundan erkek başvuruların daha uygun olduğu çıkarımında bulunmuştur. Sonuç olarak yapay öğrenme algoritmaları üzerine kurulu işe alım yazılımının kullanılması, sadece kadınların kabul edildiği üniversitelere giden kadınlara ait özgeçmişler ile herhangi bir şekilde içinde "kadın" kelimesi geçen özgeçmişlerin değerlendirmede dikkate alınmaması suretiyle cinsiyet ayrımcılığına neden olmuştur²³⁷.

²³⁵ Jon PORTER, UK Ditches Exam Results Generated By Biased Algorithm After Student Protests, The Verge, 17 Ağustos 2020, <https://www.theverge.com/2020/8/17/21372045/uk-a-level-results-algorithm-biased-coronavirus-covid-19-pandemic-university-applications>.

²³⁶ Latanya SWEENEY, Discrimination in Online Ad Delivery, 28 Ocak 2013, <https://arxiv.org/pdf/1301.6822.pdf>.

²³⁷ Isobel Asher HAMILTON, Why It's Totally Unsurprising That Amazon's Recruitment AI Was Biased Against Women, Business Insider, 13 Ekim 2018, <https://www.businessinsider.com/amazon-ai-biased-against-women-no-surprise-sandra-wachter-2018-10>; Vincent JAMES, Amazon Reportedly Scraps Internal AI Recruiting Tool That Was Biased Against Women, The Verge, 10 Ekim 2018, <https://www.theverge.com/2018/10/10/17958784/ai-recruiting-tool-bias-amazon-report>.

Massachusetts Institute of Technology (MIT) Üniversitesi'nde araştırmacı olan Joy Boulamwini, piyasada halihazırda kullanılmakta olan üç farklı yüz tanıma yazılımındaki algoritmanın daha koyu tenli kişileri tanımakta başarısız olduğunu keşfetmiştir. Genel olarak, yüz tanıma algoritmalarında kullanılan eğitim veri setlerinin %75'ten fazlası erkek ve %80'den fazlası beyazlara ait yüz görüntüleridir. Görüntüdeki kişinin beyaz erkek olması halinde, yazılımın doğru tahminde bulunma ihtimali %99 oranındadır. Boulamwini'nin araştırmasına göre, bu üç farklı yüz tanıma yazılımında hata oranı %1'den az olmakla birlikte, fotoğraftaki kişi koyu tenli bir kadın olduğunda yazılımlardan birinin hata oranı %20'nin üzerine, diğer ikisinde ise %34'in üzerine çıkmaktadır. Bu araştırma sonuçları üzerine, IBM ve Microsoft yüz tanıma yazılımlarının koyu tenli kadınları tanımada doğru kararlar verebilmesini sağlamak için geliştirme girişimlerinde bulunmuşlardır²³⁸.

ABD'de mahkemelerde sanığın tutuklanacağına mı yoksa kefaletle serbest mi bırakılacağına karar almak amacıyla yargıçlar tarafından kullanılan ve sanığın gelecekte tekrar suç işleme ihtimalini hesaplayan COMPAS (*Correctional Offender Managemenet Profiling for Alternative Sanctions*) isimli yazılımda Afrikalı-Amerikalı kişilere karşı ayrımcılık yapıldığı tespit edilmiştir. COMPAS algoritması, tutuklama kayıtları, suçlulara ilişkin demografik bilgiler ve diğer bilgilerden oluşan verilere dayanarak her bir sanığın gelecekte suç işleme ihtimaline ilişkin bir risk puanı belirler. Bu algoritmanın kullanılması, tekrar suç işleme ihtimali Afrikalı-Amerikalı kişilerle eşit olan beyazlarla karşılaştırıldığında, Afrikalı-Amerikalı kişilerin risk puanlarının daha yüksek olmasına ve dolayısıyla da bu sanıkların duruşmayı tutuklu olarak beklemelerine neden olmaktadır²³⁹.

²³⁸Larry HARDESTY, Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems, MIT News, 11 Şubat 2018, <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>.

²³⁹ Julia ANGWIN & Jeff LARSON & Surya MATTU & Lauren KIRCHNER, Machine Bias, ProPublica, 23 Mayıs 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

Suçun nerede ve ne zaman ortaya çıkmasının daha muhtemel olduğunu tahmin etmek için tasarlanan, İngiltere’de ve ABD’deki polis merkezlerinde kullanılan öngörücü polislik uygulaması PredPol, kullanıldığı şehirde harita üzerindeki suç oluşma olasılığı bulunan sorunlu bölgeleri çıkaran günlük bir rapor üretir ve bu bölgelere suçun oluşacağı inanılan süre boyunca polis vardiyası tayin eder²⁴⁰. Her ne kadar bu uygulamanın potansiyel olarak suçun etkili bir şekilde önlenmesini ve polislik hizmetlerinin maliyetinin azaltılmasını sağladığı iddia edilebilecekse de bu tür önleyici polislik uygulamalarının etkililiğine yönelik birçok tartışma gündeme gelmiştir²⁴¹. Daha da önemlisi, bu uygulamaların ırksal ve sınıfsal ayrımcılığa neden olduğu iddialarını güçlendiren birçok vaka yaşanmıştır²⁴². Algoritmanın söz konusu raporu üretirken geçmiş verilerden yararlanması sebebiyle, ekonomik açıdan dezavantajlı konumdaki bölgeler ve benzeri bölgelerde daha fazla polisin görevlendirilmesine, bu durum ise ilgili bölgelerde bildirilen suçların daha yüksek seyretmesine neden olabilecektir²⁴³. Bu bağlamda önleyici polislik uygulamaları suçun öngörülerek önlenmesi yerine suçun üretilmesine sebep olarak “kendi kendini gerçekleştirme kehanet” (*self fulfilling prophecy*) halinin ortaya çıkması ile sonuçlanabilecektir²⁴⁴. Bu döngüye girilmesi, şehirlerdeki belirli bölgelerin orantısız şekilde polis gözetimine maruz kalmasına, bu da o bölgelerde yaşayanlar ile kolluk kuvvetleri arasında bir güven sorunu yaşanmasına neden olacaktır²⁴⁵.

²⁴⁰ Kelleher & Tierney, s.135.

²⁴¹ Kelleher & Tierney, s.136.

²⁴² Uluslararası Af Örgütü’nün Hollanda’da önleyici polisliğin neden olduğu ayrımcı uygulamalara ilişkin tespitleri de içeren raporu için bkz. Amnesty International, We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands, 29 Eylül 2020, <https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR3529712020ENGLISH.pdf>. Ayrıca bkz. Alexander BABUTA & Marion OSWALD, Data Analytics and Algorithmic Bias in Policing, Royal United Services Institute for Defence and Security Studies Briefing Paper, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf.

²⁴³ Kelleher & Tierney, s.136.

²⁴⁴ Kelleher & Tierney, s.136; Jasmin LIU, Big Data and the Creation of a Self-Fulfilling Prophecy, 5 Nisan 2017, <https://stanforddaily.com/2017/04/05/big-data-and-the-creation-of-a-self-fulfilling-prophecy/>.

²⁴⁵ Kelleher & Tierney, s.136.

1.3.5.3. Caydırıcı Etki

Yapay öğrenme algoritmalarının opak yapısı ve otonom özelliği nedeniyle, profillenen bireyler çoğunlukla profillemeye faaliyetinin kendileri hakkında ne gibi çıkarımlar üretebileceğinin ve bu çıkarımların nasıl gerçekleştirildiğinin farkında değildir²⁴⁶. Profillendiğinin farkında olmayan birey ile profillemeyi gerçekleştiren arasında ortaya çıkan ve “bilgi asimetrisi” (*information asymmetry*) olarak tarif edilen bu durum, sözleşmeye dayalı veya ticari ilişkilerde, taraflardan birinin diğerinden daha çok bilgi ve farkındalık sahibi olmasını ifade eder²⁴⁷. Bilgi asimetrisi, profillenen birey ile profillemeyi gerçekleştiren arasında güç dengesizliğine neden olur. Veri madenciliğinin avantajlarını elinde bulunduran taraf, bireye göre daha güçlü durumdadır. Öte yandan, profillemeye uygulamaları kişileri değerlendirir, sınıflandırır, kategorize eder, derecelendirir ve puanlandırır. Profillemeye ve otomatik karar sistemlerinin yaygınlaşması, insan hayatının ve kişiliğinin bir puandan ibaret anlama sahip dijital bir profile indirgenmesi tehlikesini de beraberinde getirmektedir. Bankacılık, sigorta, işe alım ve birçok alanda kullanılan puanlama sistemleri, “puanlanan toplum” yapısına doğru gidildiğine işaret etmektedir²⁴⁸.

²⁴⁶ Brent MITTELDADT & Luciano FLORIDI, The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts, *The Ethics of Biomedical Big Data* (445-480), 2016, s.466, https://www.researchgate.net/publication/305813620_The_Ethics_of_Big_Data_Current_and_Foreseeable_Issues_in_Biomedical_Contexts; Andrew D. SELBST & Solon BAROCAS, The Intuitive Appeal of Explainable Machines, *Fordham Law Review* (87:3), 2018, s.1091-1092, <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5569&context=fllr>. İngiltere’de faaliyette bulunan bilim topluluğu The Royal Society of London for the Improvement of Natural Knowledge tarafından yapay öğrenmeye yönelik toplumsal farkındalığının araştırıldığı bir proje (*machine learning project*) gerçekleştirilmiştir. Proje değerlendirmeleri için bkz. The Royal Society, *Machine Learning: The Power and Promise of Computers that Learn by Example*, s.18 vd, <https://royalsociety.org/~media/policy/projects/machine-learning/publications/machine-learning-report.pdf>.

²⁴⁷ Peter J. VAN DE WAERDT, Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market, *Computer Law & Security Review*, Volume 38, 2020, 105436, s.2, <https://doi.org/10.1016/j.clsr.2020.105436>.

²⁴⁸ EPRS, *Understanding Algorithmic Decision-Making: Opportunities and Challenges*, s.27.

Algoritmik sistemlerin dikkatli şekilde kullanılmamasının en önemli risklerinden biri “dijital panoptikon”²⁴⁹ yaratılmasına neden olmasıdır. Veri madenciliğinin imkanlarını kullanan şirket ve kuruluşlarca profillemeye ve otomatik karar faaliyetleri gerçekleştirilmek suretiyle kişinin hayatıyla ilgili önemli bir konuda aleyhine bir karar verildiğinde, kişi otosansür mekanizması geliştirerek çevrimiçi platformlardaki davranışlarını kendi iradesiyle kısıtlayabilir; diğer bir ifadeyle kişi kendi kendine disipline edebilir. Algoritmik karar sistemlerinin bireyler üzerinde yarattığı bu etki “caydırıcı etki” (*chilling effect*)²⁵⁰ olarak ifade edilmektedir. Sosyal medya profillerinin, internetteki görüntülerinin, ziyaret ettikleri sitelerin, arkadaş çevrelerinin, ilgili alanlarının, ne okuduklarının işe alımda, kredi başvurusunda ve hatta artık ev kiralama da dahi değerlendirmeye konu edildiğinin farkında olan birey, hayatının her alanında gerçek düşünce ve kişiliğini gizleme eğilimi geliştirebilecektir²⁵¹. Kişi, kendisine göre daha güçlü olan tarafa karşı geliştirdiği korku sebebiyle, örneğin izlenme endişesiyle siyasi faaliyetlere katılmaktan kaçınma refleksi geliştirebilir²⁵². Günümüzde birçok ülke klasik (zarfla) oy kullanma sisteminden dijital oy sistemine geçmiş, birçok ülke de bu sisteme geçmeyi değerlendirmektedir. Ancak dijital oy sistemlerinde anonimliğine sağlanabilirliğine ilişkin kaygılar, özellikle demokratikleşme sürecini tamamlayamamış ülkelerde bireylerin fişlenme korkusuyla oy kullanma haklarını

²⁴⁹ “Bütünü gözlemlemek” anlamına gelen “panoptikon” kavramı, İngiliz filozof, hukukçu ve toplum bilimcisi Jeremy Bentham tarafından geliştirilen bir hapisane modeline atıfta bulunan bir metafor olarak kullanılmaktadır. Tam ortasında bir gözetleme kulesi bulunan sekizgen yapıdaki bölümlerde yer alan hücrelerden oluşan bir bina olarak tasarlanan hapisanede, kuleden bütün hücreler görülebilirken hücrelerden kule görülememektedir. Hapishanenin bu şekilde tasarlanmasındaki amaç, mahkumların izlenmeler bile izlendiklerini veya her an izlenebileceklerini düşünmelerine neden olarak oto kontrol mekanizması geliştirmelerini sağlamaktır. Zira gözlemlenen her bir yanlış davranışı sebebiyleceza alacağını bilen ancak tam olarak ne zaman gözlemlendiğini bilmeyen mahkumlar, her zaman gözlemleniyormuş gibi davranmak zorunda kalacaktır.

²⁵⁰ Council of Europe, Algorithms and Human Rights, s.24, <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

²⁵¹ Başak Ozan ÖZPARLAK, “İşe Alımda Ayrımcılık ve Yapay Zeka Sistemleri”, Gelişen Teknolojiler ve Hukuk II: Yapay Zeka (Editörler: Eylem Aksoy Retornaz & Osman Gazi Güçlütürk), On İki Levha Yayıncılık, 1.Baskı, İstanbul, 2020, s. 240.

²⁵² Bart H.M. CUSTERS & Bart W. SCHERMER, "Responsibly Innovationg Data Mining and Profiling Tools: A New Approach to Discrimination Sensitive and Privacy Sensitive Attributes", Responsible Innovation 1: Innovative 335 Solutions for Global Issues (Editörler: J. Van den Hoven& Diğerleri), Springer Science+Business Media, Dordrecht, 2014, s. 339-340.

kullanmaktan kaçınmalarına sebep olabilecektir²⁵³. Otomatik karar alma ve profillemeye faaliyetlerinin neden olduğu bu ve benzeri caydırıcı etkiler, bireyin kendi kaderini tayin hakkı, bilgilerin geleceğini belirleme hakkı ve ifade özgürlüğüne zarar vermektedir²⁵⁴. Zira birey kendi hayatını kontrol edebildiği ve karar ve tercihlerinde özgür olabildiği müddetçe insan ourunun varlığından bahsedilebilecektir²⁵⁵. Kişinin düşüncelerini ifade etme özgürlüğünden gönüllü olarak vazgeçmesi, demokratik toplumun temellerinin sarsılmasıyla totaliter devlet tehlikesini doğuracaktır²⁵⁶.

1.3.5.4. Filtre Balonu Etkisi

Yapay öğrenme algoritmaları ile çalışan kişiselleştirilmiş çevrimiçi hizmetlerin bireyler açısından barındırdığı risklerden biri de birbirine oldukça yakın anlamlara sahip olan “filtre balonu” (*filter bubble*) ve “yankı odası” (*echo chamber*) etkisidir²⁵⁷. Yankı odası etkisi ile ilgili endişelerini ilk kez dile getiren Cass Sunstein olmuştur²⁵⁸. Sunstein, bireylerin internetteki haber kaynaklarını giderek daha fazla özelleştirerek, içinde sadece “kendi seslerinin daha yüksek yankılarını” duydukları bir çember yaratacaklarından endişlendiğini belirtmiştir²⁵⁹. Zira insanlar kendileri ile aynı veya benzer görüşteki kişilerle ilişki kurmaya eğilimli olduklarından, çevrimiçi etkileşimleri bu kapsamda olmaktadır. Sosyal medya

²⁵³ Martin RUSSELL & Ionel ZAMFIR, Digital Technology in Elections: Efficiency Versus Credibility?, European Parliamentary Research Service (EPRS) Briefing, 2018, s.6.

²⁵⁴ Custers & Schermer, s.340; Wachter & Mittedstadt, A Right to Reasonable Inferences, s.102.

²⁵⁵ Luciano FLORIDI, On Human Dignity as a Foundation for the Right to Privacy; Philosophy & Technology, 2016, <https://link.springer.com/article/10.1007/s13347-016-0220-8>.

²⁵⁶ Özparlak, s.240. Anayasa Mahkemesi’nin 14/8/2015 tarihli 29445 sayılı Resmi Gazete’de yayınlanan, 7/7/2015 tarihli 2014/6128 numaralı Tansel Çölaşan Bireysel Başvurusu Kararı’nda, kamusal tartışmalara katılan bireylerin, hafif dahi olsa bir yaptırımla karşılaşma endişesi taşımalarının, ifade özgürlüğü üzerinde “caydırıcı etki” ye neden olacağı belirtilerek, bireylerin böyle bir etki altında ileride düşüncelerini ifade etmekten sakınma riski bulunduğu hüküm altına alınmıştır. Karar için bkz. <https://www.resmigazete.gov.tr/eskiler/2015/08/20150814-21.pdf>.

²⁵⁷ EPRS, Understanding Algorithmic Decision-Making: Opportunities and Challenges, s.27.

²⁵⁸ Brent KITCHENS & Steven L. JOHNSON & Peter GRAY, Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption, MIS Quarterly (44:4), 1619-1649, 2020, s.1621.

²⁵⁹ Michael TAGER, Cass Sunstein’s Republic.com, Journal of the Association for History and Computing (6:1), Nisan 2003, <https://quod.lib.umich.edu/j/jahc/3310410.0006.109/--cass-sunsteins-republiccom?rgn=main;view=fulltext>.

platformlarında kullanıcıların kendileriyle aynı fikirde olmadıkları kişilerle etkileşimi kesebilmeleri son derece kolaydır. Bu durum kullanıcıları “yankı odaları” olarak adlandırılan kendi görüşleri ile aynı görüşte olan kişilerden oluşan homojen topluluklar içinde kalmalarına neden olur. Sunstein’a göre, diğer görüşlerden izole edilen aynı veya benzer düşüncelere sahip insanlarda bu durumun neden olduğu dar bakış açısı, sosyal ayrılmaya neden olabilecektir²⁶⁰.

Profilleme ve otomatik karar faaliyetleri bireyleri belirli bir şekilde kategorize eder ve kişiselleştirilmiş öneriler ile kısıtlar. Bu durum “filtre balonu” kavramı ile ifade edilmektedir. Filtre balonu kavramı ilk kez internet aktivisti Eli Praiser tarafından kullanılmıştır²⁶¹. Praiser, çevrimiçi hizmetlerin kişiselleştirilmesinin, kullanıcıların maruz kaldığı içeriğin çeşitliliğini kısıtlayarak, bireyin yaratıcılığını ve düşünme yeteneğini engellediği görüşündedir²⁶². Örneğin, öneri motorları ile kişinin ilgi alanlarına ve beğenilerine uygun içerik veya ürünler sunulması suretiyle, kişinin bunları daha uzun süre izlemesi, daha çok tıklaması, yorum yapması ve paylaşması, böylece dijital etkileşimin en üst seviyeye taşınması hedeflenir. Bunun nedeni, dünyanın en büyük şirketlerinden olan Facebook, Twitter, Google, Youtube, Instagram gibi dijital platformların yanı sıra Amazon gibi çevrimiçi alışveriş sitelerinin en önemli gelir kaynağının bu platformlarda gösterilen reklamlar olmasıdır. Çevrimiçi platformlar, öneri motorları sayesinde, reklam veren şirketlere reklamların hedef kitleye en etkili şekilde gösterilmesi imkanı sunar. Ancak bu şekilde bir kişiselleştirme hizmeti neticesinde sürekli olarak kendi ilgi alanları, beğenileri ve görüşlerine uygun içeriklere maruz kalan kişiler, filtre balonlarına hapsolür. Filtre balonuna hapsolan kişi, balonun içinde ne olduğunun farkında olsa da hangi bilgi ve içeriklerden mahrum kaldığının farkında

²⁶⁰ Cass R. SUNSTEIN, The Law of Group Polarization, The Journal of Political Philosophy (10:2), 175-195, s.186.

²⁶¹ Zoe SCHIFFER, ‘Filter Bubble’ Author Eli Praiser On Why We Need Publicly Owned Social Networks, The Verge, 12 Kasım 2019, <https://www.theverge.com/interface/2019/11/12/20959479/eli-pariser-civic-signals-filter-bubble-q-a>.

²⁶² EPRS, Understanding Algorithmic Decision-Making: Opportunities and Challenges, s.13-14. Eli Praiser’ın konuya ilişkin açıklamaları için bkz. Eli PRAISER, Beware Online ‘Filter Bubbles’, TED Talk, Şubat 2011, <https://ed.ted.com/lessons/beware-online-filter-bubbles-eli-pariser>.

değildir. Bu durum, sadece seçme özgürlüğünü kısıtlamakla kalmayıp, kişinin dijital platformlardaki karşıt fikir ve görüşlerden soyutlanmasına da neden olmaktadır²⁶³. Kişinin kendi fikir ve düşünceleri ile uyuşan, diğer bir ifadeyle onayladığı içerikleri daha sık görmesi, kişinin bakış açısını daralttığı gibi, sorgulama yeteneğini de köreltecektir. Filtre balonları ile kullanıcıların ilgi alanlarının sık sık değişmemesi önlenerek, hedeflemenin etkin bir şekilde yapılması sağlanmaktadır. Ancak yapay öğrenme tabanlı profillemeye ve otomatik karar mekanizmalarının kullanılmasıyla gerçekleştirilen çevrimiçi kişiselleştirme uygulamaları, bilgiyi, ürünleri ve deneyimleri kişiselleştirmekle birlikte, bireylerin farklı bakış açıları ve içeriklerden etkili bir biçimde izole edilerek seçme özgürlüklerinin sarsılması riskini barındırmaktadır. Dijital platformların kişinin zevklerini ve tercihlerini önceden bildiği veya tahmin ettiği bir çevre, bireysel özerklik ve bu tür manipülatif uygulamaların etikliği ile ilgili sorunları da beraberinde getirmektedir²⁶⁴.

²⁶³ Farnam Street, How Filter Bubbles Distort Reality: Everything You Need To Know, <https://fs.blog/filter-bubbles/>.

²⁶⁴ EPRS, Understanding Algorithmic Decision-Making: Opportunities and Challenges, s.14. Ayrıca bkz. Eli PRASER, Beware Online ‘Filter Bubbles’, TED Talk.

İKİNCİ BÖLÜM

2. KİŞİSEL VERİLERİN İŞLENMESİNE HAKİM OLAN İLKELER

2.1. PROFİLLEME VE OTOMATİK KARAR ALMA FAALİYETLERİ KAPSAMINDA KİŞİSEL VERİLERİN İŞLENMESİNE HAKİM OLAN İLKELERİN DEĞERLENDİRİLMESİ

Kişisel verilerin korunması hukuku, kişisel verilerin işlenmesine hakim olan birkaç genel ilkenin üzerine inşa edilmiştir. Kişisel verilerin korunmasını düzenleyen ulusal ve uluslararası mevzuat ve yasal belgelerde, kişisel verilerin işlenmesine hakim olan ilkelerin temelde aynı olmakla birlikte birtakım farklılıklar barındıracak şekilde düzenlendiği görülmektedir. 108 No’lu Sözleşme, OECD Rehber İlkeleri, BM İlkeleri, 95/46 sayılı Direktif ve Tüzük’te birbirine benzer şekilde düzenlenen ilkelerin iç hukukumuzda adaptasyonu da Kişisel Verilerin Korunması Kanunu’nun 4. maddesi ile sağlanmıştır.

Kişisel verilerin işlenmesine hakim olan ilkelerin amacı, kişisel verilerin toplandığı andan itibaren başlayarak veriler üzerinde gerçekleştirilecek her türlü işlem sırasında uyulması gereken yeknesak kuralların belirlenmesidir. Önemle belirtilmelidir ki, kişisel verilerin işlenmesine hakim olan ilkeler, her türlü veri işleme faaliyetinde, verinin toplanmasından tamamen yok edildiği ana kadar tüm süreç boyunca gözetilmelidir. Bu bağlamda, kişisel veriler üzerindeki tüm işleme faaliyetlerinin bu ilkelerin hepsine uygun gerçekleştirilmesi gerekmektedir²⁶⁵. Aksi durumda veri işleme faaliyeti hukuka aykırı hale gelecektir.

²⁶⁵Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Hakkında Sıkça Sorulan Sorular, Aralık 2019, s.41, <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular>. Hukuka uyum bir veri işleme faaliyetinden bahsedilebilmesi için bu ilkelerden sadece bir veya birkaçının varlığı yeterli olmayıp hepsine birlikte uyum gösterilmesi gerekmektedir. Bu bağlamda, örneğin, ilgili kişinin açık rızası bulunsa dahi, işleme amacının gerektirdiğinden fazla veri toplanmış olması veya bu verilerin gereğinden fazla süre depolanarak silme yükümlülüğünün yerine getirilmemiş olması hainde veri işleme faaliyetinin hukuka aykırı olduğu kabul edilecektir. Murat Volkan DÜLGER, Kişisel Verilerin Korunması Hukuku, 1. Baskı, İstanbul, 2009, s.6.

Kişisel verilerin korunmasına hakim olan ilkelerin birbirinden net bir şekilde ayrılması son derece zordur. İlkelerle ilişkin açıklamalarımız değerlendirilirken, bu ilkelerin pek çoğunun birbirleri ile yakın ilişkide olduğu ve birbirini tamamladığı, bazılarının ise diğerlerine kaynaklık eden genel bir niteliğe sahip olduğu unutulmamalıdır²⁶⁶. Çalışmanın konusu olan profillemeye ve otomatik karar alma faaliyetleri de kişisel veri işlenmesini gerektirdiği sürece kişisel verilerin korunması mevzuatı kapsamında sayılacağından, bu ilkelerin tamamı profillemeye ve otomatik karar alma için de geçerlidir.

Kanun'un 4. maddesinde, "Kişisel Verilerin Korunmasına İlişkin İlkeler" başlığı altında işleme faaliyetlerine uygulanacak ilkeler düzenlenmiştir. Tüzük'te Kanun'dan farklı olarak, "Hesap Verilebilirlik"²⁶⁷ (*accountability*) ile "Şeffaflık" (*transparency*) ilkeleri ayrıca düzenlenmiştir. Bu iki ilke, çalışma konumuz ile ilgisinin önemine binaen ayrı başlıklar altında incelenmiştir. Bu bölümde, kişisel verilerin işlenmesine hakim olan ilkeler, Kanun ve Tüzük hükümlerinin benzer ve ayrışan yönlerine ve yapay öğrenme algoritmaları ile çalışan profillemeye ve otomatik karar mekanizmaları aracılığı ile gerçekleşen kişisel veri işleme faaliyetleri ile ilişkisine değinilerek ele alınacaktır.

²⁶⁶ Küzeci, s.199.

²⁶⁷ Bkz. GVK Tüzüğü, m.5/2. GVK Tüzüğü'nden önceki Avrupa Birliği düzenlemeleri olan 108 No'lu Sözleşme ve 95/46 sayılı Direktifte açık şekilde "hesap verilebilirlik" adı altında bir düzenlemeye yer verilmemiştir. Diğer yandan, ilk defa GVK Tüzüğü'nde düzenlenen bu ilkenin, önceki AB düzenlemelerinde yer alan ilgili kişinin haklarını düzenleyen hükümlerin doğal bir sonucu olduğu söylenebilir. Furkan Güven TAŞTAN, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, On İki Levha Yayıncılık, 2. Baskı, İstanbul, 2017, s.48.

2.1.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma

KVK Kanunu'ndaki "hukuka ve dürüstlük kurallarına uygun olma"²⁶⁸ ilkesi, GVK Tüzüğü'nde "hukuka uygunluk, adalet ve şeffaflık"²⁶⁹ olarak, düzenlenmiştir. Şeffaflık ilkesi ayrı bir başlık altında incelendiğinden bu bölümde sadece doğruluk ve dürüstlük kurallarına uygunluk ile ilgili açıklamalara yer verilmiştir²⁷⁰. Kişisel verilerin "hukuka ve dürüstlük kurallarına uygun" şekilde işlenmesi, kişisel veri işleme faaliyetinin kanunlarla ve diğer hukuki düzenlemeler ile getirilen ilkelere uygun bir şekilde gerçekleştirilmesi zorunluluğunu ifade eder²⁷¹. Kişisel verilerin genel hukuk kurallarına uygun olarak işlenmesi, kişisel verilerin "hukuka ve dürüstlük kurallarına uygun" kabul edilmesinde tek başına yeterli olmayacak, ilgili işleme faaliyeti dürüstlük kuralına uygun gerçekleştirilmediği takdirde hukuka aykırı kabul edilecektir. Bu bağlamda, hukuka ve dürüstlük kurallarına uygun olma, kişisel verilerin işlenmesine hakim olan diğer ilkeleri de kapsayan genel bir ilke niteliğindedir²⁷². Dolayısıyla, kişisel verilerin kullanıldığı tüm veri işleme faaliyetlerinin, kişisel verilerin işlenmesine hakim olan ilkelere uygun olduğunun kabul edilmesi ilgili işleme faaliyetinin hukuka uygun, adil ve şeffaf olmasına bağlıdır²⁷³.

Profilleme ve otomatik karar faaliyetlerinin hukuka ve dürüstlük kurallarına uygun gerçekleştirildiğinin kabul edilebilmesi için, öncelikle söz konusu veri işleme faaliyetinin Tüzük veya Kanun'da düzenlenen hukuka uygunluk sebeplerinden biri tahtında "gerekli" olması ve kişisel verilerin işlenmesine hakim olan diğer ilkelere uygun şekilde gerçekleştirilmesi gerekir. Öte yandan, profilleme sürecinin her aşamasında GVK Tüzüğü'nde açıkça veri işleme ilkelerinden biri

²⁶⁸ Bkz. KVK Kanunu, m.4/2(a)

²⁶⁹ Bkz. GVK Tüzüğü m. 5/1(a)'da "lawfulness, fairness and transparency" olarak ifade edilmiştir.

²⁷⁰ Çalışmanın "2.2.3. Şeffaflık" başlıklı bölümü için bkz. s.124.

²⁷¹ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s.2.

²⁷² Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, s.42.

²⁷³ Dülger, s.109. KVK Kanunu'nda ve diğer düzenlemelerde yer verilen diğer ilkeler, hukuka uygun işlemenin doğal bileşenlerini oluşturmaktadır. Küzeci, s.201.

olarak düzenlenmiş olmakla birlikte, KVK Kanunu'nda açıkça düzenlenmeyen ancak Kurum kararlarında atıfta bulunulan şeffaflık ilkesinin de gözetilmesi elzemdir²⁷⁴. Kişisel verilerin adil şekilde işlenmesi, şeffaflık ilkesine sıkı sıkıya bağlıdır. Profillemeye ve otomatik karar alma faaliyetleri kapsamında kişisel verileri adil bir biçimde işlenmesi, ilgili kişilerin kişisel verilerinin işlenmesi konusunda aldatılmamasını, yanlış yönlendirilmemesini, profillemenin varlığı ve sonuçları hakkında bilgilendirilmesini gerektirir²⁷⁵. Kişisel verilerin adil şekilde işlenmesi, hesap verebilirlik ilkesi ile de yakından ilgilidir. Ancak büyük veri analitiği yöntemlerinin ve algoritmaların karmaşık ve opak yapısı, işleme amaçlarının başlangıçta belirli olmaması gibi nedenlerin sebep olduğu sorunlar, şeffaflık ve hesap verebilirlik ilkelerinin profillemeye ve otomatik karar alma faaliyetleri bakımından uygulanabilirliğine ilişkin tartışmaları beraberinde getirmiştir²⁷⁶. Hukuka uygun ve adil bir biçimde işleme ilkesinin şeffaflık ve hesap verebilirlik ile ilişkisi göz önüne alındığında, profillemeye ve otomatik karar alma faaliyetlerinin hukuka ve dürüstlük kurallarına uygunluğunun da sorunlu olduğu sonucu ortaya çıkmaktadır.

Veri sorumlusu profillemeye ve otomatik karar alma faaliyeti kapsamında gerçekleştirilen çıkarımların veya kararların içerik anlamında da adil olmasını sağlamakla yükümlüdür. Örneğin, çalışmanın ilgili bölümünde²⁷⁷ açıklandığı üzere, Amazon tarafından işe alım sürecinde kullanılmak üzere geliştirilen yapay öğrenme modeli, veriden öğrenme aşamasında cinsiyet verisi kullandığında, cinsiyete dayalı ayrımcı kararlar alınmasına neden olduğundan, işleme faaliyeti “belirli, açık ve meşru amaçlar” için gerçekleştiriliyor olsa dahi, bu şekilde bir veri işlemenin hukuka ve dürüstlük kuralına uygunluğundan söz edilemeyecektir. Zira profillemeye ve otomatik karar sistemlerinin, yapay öğrenme algoritmalarının teknik özelliklerinin yol açtığı riskler nedeniyle, işleme faaliyetinin hukuka ve dürüstlük

²⁷⁴ Küzeci, s.228; Dülger, s.236; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi, s.2.

²⁷⁵ Bkz. GVK Tüzüğü, Giriş Bölümü, 60.Paragraf.

²⁷⁶ Çalışmanın ilgili bölümleri için bkz. s. 96-135.

²⁷⁷ Bkz. s.59.

kuralına aykırı olmadığının işleme öncesinde tespit edilebilmesi her zaman mümkün değildir. Dolayısıyla bu tespitin, yapay öğrenme algoritmalarının ürettiği sonuçlara bakılarak her bir veri işleme faaliyeti özelinde yapılması gerekmektedir.

Veri sorumlusu, profillemeye ve otomatik karar faaliyetlerinin önyargılı, ayrımcı ve haksız çıkarımlar veya kararlar ile sonuçlanmaması, özellikle kişisel verilerde hatalara neden olan faktörlerin düzeltilmesini ve hata riskinin en aza indirgenmesi için gerekli tedbirleri almakla yükümlüdür. Bu bağlamda, veri sorumlusu profillemeye ve otomatik karar alma uygulamalarının, birey açısından “ırk ve etnik köken, siyasi görüş, din veya inançlar, sendika üyeliği, genetik veya sağlık durumu veya cinsel yönelim” gibi faktörler üzerinden muhtemel ayrımcı etkilerini önleyecek uygun matematiksel veya istatistiksel prosedürleri takip etmeli, teknik ve organizasyonel önlemleri almalıdır²⁷⁸.

Wachter ve Mittelstadt, profillemeye ve otomatik karar alma uygulamaları ile ulaşılan çıkarımların, “makul ve mantıklı” (*reasonable*), diğer bir ifadeyle “adil” kabul edilebilmesinin, üç kriterin karşılanmasına bağlı olduğunu ifade etmiştir. Bunlar, kabul edilebilirlik (*acceptability*), uygunluk (*relevance*) ve güvenilirliktir (*reliability*). Bu kriterlere göre, ilk olarak çıkarımların makul ve adil olduğunun kabul edilebilmesi için, sisteme girdi olarak sunulan veriler bireyler hakkında ulaşılan çıkarımlara bir temel oluşturabilmek için normatif olarak kabul edilebilir olmalıdır. İkincisi, söz konusu çıkarım otomatik karar alma faaliyetinin amacı ile ilgili ve bu bağlamda kabul edilebilir olmalıdır. Son olarak eğitim verisi de dahil olmak üzere hem girdilerin hem de kullanılan analitik yöntemlerinin doğru ve istatistiksel olarak güvenilir olması gerekir²⁷⁹.

²⁷⁸ Bkz. GVK Tüzüğü, Giriş Bölümü, 71.Paragraf.

²⁷⁹ Wachter & Mittelstadt, A Right to Reasonable Inferences, s.90 vd.

2.1.2. Doğru ve Gerekliğinde Güncel Tutulma

Kişisel verilerin “doğru ve gerektiğinde güncel tutulması” ilkesi²⁸⁰, “kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin” verilerin kişisel veri olarak kabul edilmesinin doğal bir sonucu olarak ortaya çıkmıştır. Çalışmanın ilgili bölümünde açıklandığı üzere, kişisel verilerin “kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin olma” niteliğini kaybetmesi halinde hukuki korumadan faydalanılması mümkün olmayacaktır. Bu bağlamda verilerin “doğru ve gerektiğinde güncel” olması önem arz etmektedir. Doğru ve güncel olmayan kişisel verilerin işlenmesi, ilgili kişi açısından birçok olumsuz sonuç doğurabilecek olmakla birlikte²⁸¹, veri sorumlusunun işleme faaliyeti ile edinmeyi amaçladığı faydayı da sağlayamayacaktır²⁸². Bu ilke büyük veri analitiği kapsamında bilgi yönetimi açısından bir nevi “iyi uygulama” (*good practice*) teşkil etmekle birlikte, kişisel verilerin korunması açısından da bireyin kendisi hakkında yanlış verileri düzeltme hakkıyla doğrudan ilgilidir²⁸³. Kişisel verilerin “doğru ve gerektiğinde güncel tutulması” gerekliliği, “veri kalitesi” (*data quality*) kavramı ile de ifade edilmektedir. Zira bireylerin profillemeye ve otomatik karar alma faaliyetleri sonucu ortaya çıkabilecek herhangi bir yanlışlığı veya haksızlığı düzeltme imkanına sahip olmaları, veri kalitesinin iyileştirilmesine hizmet edecektir. Bu bağlamda veri sorumlularının ilgili kişileri hangi kişisel verilerinin işlendiği ve işlenen verilerini düzeltme hakkına sahip oldukları hususunda açıkça bilgilendirmeleri doğru ve

²⁸⁰ GVK Tüzüğü’nün 5/1(d) maddesinde, “doğruluk” (*accuracy*) başlığı altında “kişisel verilerin doğru ve gerektiği durumlarda güncel tutulması, işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeksizin silinmesi veya düzeltilmesi için makul tüm adımların atılması gerektiği” düzenlenmiştir. Aynı şekilde 95/46 Sayılı Direktif’in 6/1-d maddesinde ve 108 No’lu Sözleşme’nin 5/d maddelerinde de kişisel verilerin “doğru ve gerektiği durumlarda güncel olması” gerektiği belirtilmiştir. Diğer yandan OECD Rehber İlkeleri’nin 8.maddesinde “doğruluk” ve “güncellik” ifadelerinin yanında kişisel verilerin tam olması gerekliliğine (“*completeness*”) de değinilmiştir. Bu maddeye KVK Kanunu’ndaki karşılık gelen hüküm, m.4/2-b’de düzenlenen “doğru ve gerektiğinde güncel olma” ilkesidir.

²⁸¹ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s.6; Colonna, s.162.

²⁸² Colonna, s.162.

²⁸³ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.43; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s.5.

gerektiğinde güncel tutulma ilkesinin uygulanabilirliği açısından önem teşkil etmektedir²⁸⁴

Profilleme ve otomatik karar alma faaliyetleri gerçekleştiren veri sorumluları, verilerin toplanması, analiz edilmesi, ilgili kişinin profilinin çıkarılması ve bu profilin ilgili kişi hakkında bir karar almak üzere ilgili kişiye uygulanması aşamalarının tamamında kişisel verilerin “doğru ve güncel olmasını” sağlamakla yükümlüdür²⁸⁵. Profilleme ve otomatik karar alma süreçlerinde girdi olarak kullanılan verinin doğru ve güncel olmaması, bu verinin analiz edilmesi sonucunda ilgili kişi hakkındaki tahmin veya çıkarımın, dolayısıyla da oluşturulacak profilin ve verilecek kararın da yanlış olmasına neden olacaktır²⁸⁶. Örneğin, bankalar ve finansal kuruluşlar, kredi talebinde bulunan kişiye kredi verilip verilmeyeceğine karar almak için kredi puanlarını dikkate almaktadır. Kredi puanı ilgili kişinin kredi raporundaki geçmiş finansal bilgilerinin analiz edilmesi suretiyle kişiye kredi verilmesi halinde geç ödeme veya ödememe hallerinin ortaya çıkmasına ilişkin risk tahminine atfedilen sayısal bir değerdir. Dolayısıyla kredi puanının, ilgili kişi hakkında sübjektif bir değerlendirmeden ziyade olgulara dayalı bir analize dayandığı göz önüne alındığında, kredi puanının doğruyu yansıtması ancak bu puanın hesaplanmasında esas alınan verilerin doğru ve yeterli olması halinde mümkün olacaktır²⁸⁷. Öte yandan, kişinin kredi geçmişine ilişkin doğru olmayan veriler, kredi puanının yanlış hesaplanmasına ve kişinin kredi talebinin reddedilmesine neden olabilecektir²⁸⁸.

Kişiler hakkındaki çıkarımların dayandığı olguların, diğer bir ifadeyle yapay öğrenme sistemlerine girdi olarak sunulan verilerin, doğru ve gerektiğinde güncel olmaları gerektiği açıktır. Öte yandan, bu ilkenin büyük veri analitiği

²⁸⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.12.

²⁸⁵ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.12.

²⁸⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.12.

²⁸⁷ ICO, Guide to the General Data Protection Regulation, s.35.

²⁸⁸ European Union Agency for Fundamental Rights & Council of Europe, Handbook on European Data Protection Law, 2018 Edition, s.128, https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf; Colonna, s.162.

uygulamaları ile edinilen çıkarımlara uygulanabilirliği, doktrinde farklı görüşlere konu olmuştur. Hallinan ve Borgesius, literatürde çıkarımların doğruluk ilkesinin uygulama alanına girdiğini savunan görüşler olduğu gibi, aksi yönde de görüşler olduğunu ancak bunlardan hiçbirinin görüşlerini destekleyecek detaylı bir argüman ortaya koyamadığını, bu konuya ışık tutacak yeterli bir içtihatın da bulunmadığını ifade etmiştir²⁸⁹. Öte yandan, bu konuya yeterli bir şekilde değinen aydınlatıcı bir içtihat da bulunmadığı gibi, üye devletlerin veri koruma otoritelerince de konuya kesin bir açıklama getirilememiştir²⁹⁰. Hallinan ve Borgesius’a göre, GVK Tüzüğü’nün uygulanabilir olduğu her durumda, doğruluk ilkesi de geçerli ve uygulanabilir olacaktır. Zira Adalet Divanı da Nowak kararı ile çıkarımların kişisel veri niteliğini haiz olduğunu kabul etmiştir²⁹¹. Dolayısıyla, çıkarımların GVK Tüzüğü’nün temel uygulanabilirlik kriterlerini karşılayabileceği noktasında bir tereddüt söz konusu değildir²⁹². Bu bağlamda Hallinan ve Borgesius, doğruluk ilkesinin pozitif hukuk açısından çıkarımlara uygulanabilir olduğu, normatif açıdan da uygulanabilir olması gerektiği görüşündedir²⁹³.

Denetimli yapay öğrenme süreci, her ne kadar girdilerin kalitesini artırmak üzere bir ön işleme aşaması içerse de eğitim veri kümesinin insan eliyle etiketlenmesi, önyargı ve ayrımcı çıkarımların oluşması açısından başka bir risk faktörü teşkil edebilmektedir²⁹⁴. Öte yandan, büyük veri analitiğinin, işlenen veri hacmi çok yüksek olduğundan belirli bir oranda, doğru olmayan veriyi tolere edebileceğini ileri süren görüşler de vardır²⁹⁵. Bu çerçevede, örneğin, bir konuda genel eğilimleri tespit etmek üzere gerçekleştirilen analitik faaliyetlerinde, isim veya adres verisinin yanlış olması sorun yaratmayacaktır²⁹⁶. Ancak, kişisel verilerin

²⁸⁹ Dara HALLINAN & Frederik ZUIDERVEEN BORGESIOUS, Opinions can be incorrect (in our opinion)! On data protection law’s accuracy principle, *International Data Privacy Law*, 2020, Vol.10, No.1, s.5, <https://doi.org/10.1093/idpl/ipz025>.

²⁹⁰ Hallinan & Borgesius, s.5.

²⁹¹ Hallinan & Borgesius, s.5.

²⁹² Hallinan & Borgesius, s.5.

²⁹³ Hallinan & Borgesius, s.8-10.

²⁹⁴ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.44.

²⁹⁵ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.43.

²⁹⁶ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.43.

belirli bir kişiyi profillemeye amacıyla işlendiği senaryoda, bu verilerin doğru olmaması profilin de yanlış olmasına sebep olabilecektir²⁹⁷.

Yapay öğrenme algoritmalarının kullanıldığı profillemeye ve otomatik karar alma mekanizmalarında, farklı kaynaklardan farklı yapıda çok fazla veri toplanmaktadır. Bu durum toplanan ve işlenen verinin ilgili kişi hakkında doğru bir bilgiyi yansıtmaması veya güncel bir bilgi olmaması ihtimalini kuvvetlendirmektedir. Dolayısıyla veri sorumlularının, verinin toplanması, analiz edilmesi, ilgili kişinin profilinin çıkarılması ve karar alma aşamalarının tamamında, yeniden kullanılan veya dolaylı olarak elde edilen verilerin “doğru ve güncel olmasını” temin edecek gerekli tedbirleri almaları gerekir²⁹⁸.

Büyük veri analitiği yöntemleri, büyük hacimli veri setlerinin analiz edilerek veri setleri arasındaki korelasyonların tespit edilebilmesine imkan tanır. Ancak büyük veri analitiğinin sağladığı bu imkan, her zaman daha doğru tahmin ve çıkarımlarda bulunulacağı anlamına gelmez²⁹⁹. Zira yapay zeka uygulamaları “ihtimallere dayalı, kesin olmayan ve belirli bir olasılık dağılımını yansıtan sonuçlar” üretmektedir³⁰⁰. Aynı verilerin farklı algoritmalar aracılığı ile veya farklı amaçlar için analiz edilmesi, farklı çıktıların üretilmesi ile sonuçlanabilmektedir³⁰¹. Dolayısıyla ilgili kişinin kendisinden veya üçüncü bir kişiden edinilen kişisel veriler, doğru olarak kayıt altında tutulsa dahi, bu verilerin analiz edilmesiyle ulaşılabilecek çıkarımlar her zaman mutlak suretle doğru ve kesin bir bilgi ifade etmeyebilecektir³⁰².

²⁹⁷ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.43.

²⁹⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.12.

²⁹⁹ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.43.

³⁰⁰ Osman Gazi GÜÇLÜTÜRK & Yasin Murat KADIOĞLU, “Yapay Zeka ve Regülasyon”, Gelişen Teknolojiler ve Hukuk II: Yapay Zeka (Editörler: Eylem Aksoy Retornaz & Osman Gazi Güçlütürk), On İki Levha Yayıncılık, 1.Baskı, İstanbul, 2021, s.89.

³⁰¹ Güçlütürk & Kadioğlu, s.90.

³⁰² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.12.

Veri setinin, ilgili kişiyi ne derece doğru şekilde temsil ettiği ve analitik sürecinde gizli önyargı ve ayrımcılık olup olmadığı hususunda da belirsizlikler söz konusu olabilir. Dengesiz veri setlerini, önyargı içeren girdileri veya ayrımcı faktörleri de hesaba katacak şekilde önyargılı olarak tasarlanmış algoritmalar, yapay öğrenme sistemlerinin ayrımcı uygulamalara neden olabilecek çıkarımlarda bulunmasına neden olabilmektedir³⁰³. Diğer yandan, büyük veri analitiğinde veri setlerinin birçok farklı kaynaktan edinilen verilerden oluşması da veri sorumlusunun veri analitiği sürecinin her aşamasında işlenen kişisel verilerin “doğru ve gerektiğinde güncel olmasını” sağlamasını zorlaştırmaktadır³⁰⁴. Bu nedenle, profillemeye ve otomatik karar alma uygulamalarının kullanılması suretiyle kendisi hakkında yanlış çıkarımlarda bulunulduğundan endişe duyan bireylerin, bu çıkarımların dayandığı girdileri ve çıkarımları düzeltme veya silme imkanına sahip olmaları, hatalı çıkarımların olumsuz etkilerinin en aza indirgenmesi açısından oldukça önemlidir.

Kişisel verilerin potansiyel olarak birden çok kişi tarafından kullanılacak nesnelerin interneti uygulamaları ile toplandığı göz önüne alındığında, bu cihazlardaki kullanıcı kimliğinin doğrulanmasını sağlayan mekanizmaların da kişisel verilerin doğru ve gerektiğinde güncel olması gerekliliğine hizmet ettiği söylenebilecektir³⁰⁵. Kimlik doğrulaması birden fazla kullanıcı tarafından veri oluşturulabilecek cihazlarda kişisel verilerin doğruluğunun sağlanması açısından kritik öneme sahiptir³⁰⁶. Zira doğrulama yapılmadığı takdirde, farklı kullanıcıların cihazı kullanmak suretiyle oluşturdukları veriler, tek bir kullanıcının profili altında gruplanır ve böylece hatalı bir veri işleme meydana gelir³⁰⁷.

³⁰³ Çalışmanın “1.3.5.2. Algoritmik Önyargı ve Ayrımcılık” başlıklı bölümü için bkz. s. 56.

³⁰⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.12, s.17.

³⁰⁵ Sandra WACHTER, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.11, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130392 (Kısaltılmışı “The GDPR and the Internet of Things: A Three-Step Transparency Model”).

³⁰⁶ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.11.

³⁰⁷ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.11.

Avrupa Konseyi Bakanlar Komitesi'nin profillemeye faaliyetleri karşısında bireyin korunmasına ilişkin tavsiye metninde, veri ve algoritma kalitesinin sağlanması için,

- Verinin yanlış olmasına ilişkin faktörlerin düzeltilmesi ve profillemenin doğasında bulunan hata ve önyargı risklerinin sınırlandırılması için veri sorumluları ve uygun olan hallerde veri işleyenler tarafından uygun önemlerin alınması,
- Veri sorumlularının ve uygun olan hallerde veri işleyenlerin periyodik olarak ve makul süreler içinde profillemeye için kullanılan verilerin ve istatistiksel çıkarımların kalitesini ve ayrıca profillemeye faaliyetinin ilgili kişinin hakları üzerindeki etkisini yeniden değerlendirmeleri,
- Veri sorumlusu veya veri işleyenlerin, veri veya algoritmaları üçüncü kişilerden edindikleri hallerde, verilerin ve algoritmaların kalitesini ve bunların işleme amacına uygunluğunu kontrol etmek için gerekli belgeleri de ilgili üçüncü kişilerden temin etmeleri gerektiği belirtilmiştir³⁰⁸.

Doğruluk ilkesi, ilgili kişinin hatalı kişisel verilerin işlenmesini kısıtlama³⁰⁹ ve hatalı kişisel verilerin düzeltilmesini talep etme³¹⁰ haklarının uygulanabilirliği açısından bir kriter işlevi görür³¹¹. GVK Tüzüğü m.15/3 kapsamında ilgili kişinin erişim hakkını kullandığında ilgili kişiye işlenen verilerinin bir kopyası sağlanmalıdır. İlgili kişi kişisel verilerinin yanlış olduğu kanaatine varırsa, kısıtlama ve düzeltme hakları devreye girer. İlgili kişi işlemeyi kısıtlama hakkını kullanarak, veri sorumlusu verilerin doğruluğunu onaylayıncaya kadar, potansiyel

³⁰⁸ Council of Europe, Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 3 Kasım 2021, <https://www.coe.int/en/web/human-rights-rule-of-law/-/data-protection-committee-of-ministers-updates-recommendation-on-profiling>.

³⁰⁹ Bkz. GVK Tüzüğü, m.18. KVK Kanunu'nda böyle bir hakka ilişkin açık bir düzenleme bulunmamaktadır.

³¹⁰ Bkz. GVK Tüzüğü, m. 15/3; KVK Kanunu, m.11/d.

³¹¹ Hallinan & Borgesius, s.3.

olarak yanlış olan kişisel verilerin işlenmesini geçici olarak kısıtlayabilecektir³¹². Kişisel verilerin yanlış olduğu tespit edilirse, bu defa ilgili kişi düzeltme hakkını kullanarak veri sorumlusundan yanlış kişisel verilerin düzeltilmesini veya güncellenmesini talep edebilir³¹³.

Hallinan ve Borgesijs, kişisel verilerin düzeltilmesinin hukuken veya uygulamada sorun yaratacağı bazı istisnai durumlarda, söz konusu kişisel verilere eklenecek bir açıklama ile yükümlülüğün ortadan kaldırılacağı görüşündedir³¹⁴. Buna göre, kişinin kredi raporunda cep telefonu faturasını zamanında ödemediğine ilişkin bir kayda yer verildiği bir örnekte, ilgili kişi mücbir sebepler nedeniyle operatör sağlayıcısına ödeme yapamadıysa, bu bilginin geç ödemeye ilişkin kayda eklenmesi gerekebilir. Doğruluk ilkesinin dayanak oluşturduğu bir diğer hak ise, ilgili kişinin kendisi hakkında otomatik kararlara itiraz etme hakkıdır. İlgili kişi, GVK Tüzüğü'nün 22/2 (a) ve (c) bentlerinde atıfta bulunulan hallerde, “profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma” faaliyetinin doğruluk ilkesine uygun gerçekleştirilmediğini düşünüyor ise, 22. maddenin 3.fıkrası ile kendisine tanınan otomatik kararlara itiraz etme hakkını kullanabilecektir³¹⁵.

³¹² Bkz. GVK Tüzüğü, m.18.

³¹³ Bkz. GVK Tüzüğü, m. 15/3; KVK Kanunu, m.11/d.

³¹⁴ Hallinan & Borgesijs, s.3.

³¹⁵ Bkz. GVK Tüzüğü, m.22/3.

2.1.3. İlgili Mevzuatta Öngörülen Veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

GVK Tüzüğü m.5/1(e)'de veri sorumlularının kişisel verileri, işleme amaçlarının gerektirdiği sürece ilgili kişinin kimliğinin tespit edilmesini sağlayacak şekilde tutmakla yükümlü olduğu düzenlenmiştir³¹⁶. Tüzük'te bu ilke için, “saklama süresinin sınırlandırılması” (“*storage limitation*”) ifadesi kullanılmaktadır. Bu ilkenin KVK Kanunu'ndaki karşılığı olan m.4/2(d)'de, GVK Tüzüğü ile paralel şekilde, kişisel verilerin “ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi” gerektiği belirtilmektedir.

Kişisel verilerin korunmasına ilişkin birçok düzenlemede³¹⁷ kabul edilmiş olan bu ilke, Avrupa'daki kişisel verilerin bir insan hakkı olarak korunması yaklaşımının bir yansımasıdır. Kişisel verilerin ne kadar süre tutulduğunun belli olmadığı bir ortamda, kişisel verileri bir kez edinilen bir kişi verilerinin süresiz şekilde kayıt altında tutulacağı ve ihtiyaç duyulan her an kullanılmak üzere saklanacağı fikrine kapılabilecektir³¹⁸. Büyük veri analitiğinin ve profillemeye uygulamalarının bu derece yaygınlaştığı günümüz dünyasında dijitalleşmenin boyutu göz önüne alındığında, bireyin kişisel verilerinin süresiz olarak kayıt altında tutulması halinde, kişisel verilerin korunmasının temelini oluşturan, bilgilerin geleceğini belirleme hakkı, kişinin maddi ve manevi bütünlüğü ve özel hayatın gizliliği gibi değerlerin zarar görmesi kaçınılmazdır³¹⁹.

³¹⁶ Tüzükte kişisel verilerin muhafaza edilme süresinin işlendikleri amaç için gerekli olan süre ile (“*strict minimum*”) sınırlı tutulması gerektiği belirtilmiştir. Bkz. GVK Tüzüğü, Giriş Bölümü, 39. Paragraf; Paul VOIGT & Axel VON DEM BUSSCHE, The EU General Data Protection Regulation (GDPR), Springer e-Book, 2017, s.179, <https://link.springer.com/book/10.1007%2F978-3-319-57959-7>.

³¹⁷ Bkz. 108 No'lu Sözleşme, m.5/e; OECD Rehber İlkeleri, 8. Paragraf; 95/46 Sayılı Direktif, m.6/1-e.

³¹⁸ Küzeci, s.215.

³¹⁹ Küzeci, s.215.

Profilleme ve otomatik karar alma uygulamaları bakımından elde edilmek istenen menfaat için kişisel verilerin saklanması ve işlenmesinin mutlaka gerekli olup olmadığı değerlendirilmelidir³²⁰. İlgili menfaati elde etmek için anonim verinin yeterli olması halinde kişisel veriler anonimleştirilmelidir³²¹. Veri sorumlusunun, profillemeye ve otomatik karar faaliyetlerinde bu ilkenin gerekliliklerini yerine getirmek üzere, kişisel verileri ileride faydalı olabileceği düşüncesiyle ayırım yapmaksızın saklamaktan ziyade işleme amacına uygun, güncel ve gerekli verileri tutması, kişisel verilerin korunmasına hizmet etmekle birlikte, veri kalitesinin artırarak analitik süreçlerine de fayda sağlayacaktır³²².

Öte yandan bu ilkenin profillemeye ve otomatik karar alma uygulamaları bakımından uygulanabilirliğine ilişkin bazı sorunlar söz konusudur. Yapay öğrenme algoritmalarının büyük veriden beslendiği ve işlenen veri miktarı arttıkça çıkarımların da o ölçüde isabetli hale geldiği göz önüne alındığında, kişisel verilerin saklanma sürelerinin sınırlandırılması, büyük veri ve yapay zeka uygulamalarının çalışma prensibi ile örtüşmemektedir. Zira büyük veri analitiği yöntemlerinin olağanüstü hacme sahip veri yığınlarını işleyebilme kapasitesi ve depolama maliyetlerinin düşmesi, veri sorumlularını kişisel verileri ticari amaçlarının gerektirdiğinden daha uzun süre saklamaya teşvik edebilmektedir³²³.

Her ne kadar ticari hedefleri kapsamında büyük veri analitiğinden faydalanan şirketler için olabildiğince fazla verinin olabildiğince uzun süre saklanması, algoritmaların daha iyi sonuçlar üretmesini sağlayabilecek ise de, veri sorumluları profillemeye faaliyetinin tüm aşamalarında veri minimizasyonu ve amaçla sınırlılık ilkelerini gözetmekle ve profillemeye faaliyetinin amacı için gerekli olan süre kadar saklamakla yükümlüdür. Bu nedenle, veri sorumlularının, hangi veri setine neden ihtiyacı olduğunu ve analiz etmesi gerektiğini, profillemeye faaliyeti

³²⁰ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.42.

³²¹ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.47, s.58.

³²² ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.42.

³²³ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.40.

gerçekleştirilmeden önce belirlemeleri gerekir³²⁴. Büyük veri analitiği yöntemleri ve yapay öğrenme algoritmalarının doğası ve çalışma özellikleri göz önüne alındığında, buradaki asıl zorluk işlemenin amaçlarını tanımlamak ve hangi verilerin bu amaç ile ilgili olacağını belirlemektedir³²⁵.

Veri sorumluların profillemeye ve otomatik karar alma faaliyetini bu ilkeye uygun bir şekilde yerine getirebilmelerini sağlayacak yöntemlerden biri de “veri saklama ve imha politikası” (*retention policy*) oluşturmaktır³²⁶. Saklama ve imha politikası, tutulan kişisel verilerin türlerini listeler ve bunların ne için kullanılacağını ve ne kadar süre tutulacağını ortaya koyar³²⁷. Saklama ve imha politikası, ilgili kişinin temel hak ve özgürlükleri ile kişisel verilerin korunmasına hakim olan ilkeler gözetilerek hazırlanmalıdır³²⁸. Açık ve anlaşılır veri saklama ve imha politikalarının oluşturulması, verilerin “işlendikleri amaç için gerekli olan süre kadar” muhafaza edilmesini sağlayarak veri sorumlularının yetkili kurum ve kuruluşlardan gelecek saklama ve imha ile ilgili sorgulamalar ve ilgili kişilerin kişisel verilerinin silinmesine ilişkin talepleri ile karşılaşma ihtimalini de azaltacaktır³²⁹.

Profillemeye ve otomatik karar alma faaliyetleri açısından önem teşkil eden bir diğer husus ise, GVK Tüzüğü’nde “kamu yararına arşivleme, bilimsel, tarihi veya istatistiksel amaçlarla” gerçekleştirilen veri işleme faaliyetlerinin, hukuka uygunluk sebeplerinden birinin uygulanabilir olması ve uygun teknik ve idari

³²⁴ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.41.

³²⁵ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.41.

³²⁶ Küzeci, s.215.

³²⁷ ICO, Guide to the General Data Protection Regulation, s.44. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliğinin 3.maddesinde kişisel veri saklama ve imha politikasının tanımı yapılmış, 5.maddesinin 1.fikrasında, veri sorumlularının kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlü oldukları hüküm altına alınmış ve 6. maddesinde ise kişisel veri saklama ve imha politikasının kapsamına ayrıntılı olarak yer verilmiştir. Kişisel Verilerin Korunması Kurumu tarafından hazırlanarak yürürlüğe girmiş ve Sicile kayıtlı yükümlü olan veri sorumlularına kişisel veri saklama ve imha politikası hazırlama konusunda örnek ve yardımcı olmak üzere Kurul tarafından, Kurum internet sayfasında yayınlanmasına karar verilmiş olan KVKK Kişisel Veri Saklama ve İmha Politikası için bkz. <https://kvkk.gov.tr/Icerik/5383/Diger-Dokumanlar>.

³²⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.12.

³²⁹ ICO, Guide to the General Data Protection Regulation, s.44.

tedbirlerin alınması şartıyla, m.5/1(b) ile düzenlenen “amaçla sınırlılık” ve m.5/1(e) ile düzenlenen “saklama süresinin sınırlandırılması” ilkelerinden muaf tutulmuş olmasıdır³³⁰. Tüzük’teki ilgili düzenlemeler uyarınca, hukuka uygunluk sebeplerinden birine dayanılarak toplandığı ve uygun tedbirler alındığı sürece, kişisel verilerin daha sonra istatistiksel amaçlar için işlenmesi halinde ayrıca bir hukuka uygunluk sebebi aranmamaktadır³³¹. GVK Tüzüğü’nün bu düzenlemesi ile bilim ve sanat özgürlüğü ile kişisel verilerin korunması arasında denge kurulmaya çalışılmıştır³³². Öte yandan, Tüzük’te istatistiksel amaçlarla veri işleme faaliyetlerine ayrıcalık tanınması, büyük veri analitiği yöntemleri ile gerçekleştirilen çıkarımların, diğer bir ifadeyle profillemeye faaliyetlerinin hangi hallerde bu muafiyetlerden yararlanabileceği konusunda farklı görüşlerin ortaya çıkmasına neden olmuştur³³³.

Mayer-Schönberger ve Padova, büyük veri analitiğinin, ağırlıklı olarak istatistiksel yöntemlere dayandığı gerekçesiyle “istatistiksel amaçlar için işleme” olarak değerlendirilebileceğini ileri sürmüştür³³⁴. Zarsky ise, büyük veri analitiğinin belirtilen muafiyetler kapsamına girebilmesinin önünde önemli zorluklar bulunduğunu ifade etmiştir³³⁵. Wachter ve Mittelstadt, Tüzük kapsamındaki bu muafiyetlerin büyük veri analitiği ile gerçekleştirilen çıkarımlar açısından iki sonucu olacağını öngörmektedir. İlk olarak, bu muafiyetler, büyük veri analitiği uygulamaları açısından kişisel verilerin korunmasına ilişkin gereksinimleri ve şartları hafifletmek suretiyle istatistiksel modelleme ve profillemeye uygulamalarının yaygınlaşmasını teşvik edecektir. İkinci olarak, Tüzüğün tanıdığı bu muafiyetler sebebiyle, kişisel verilerin istatistiksel amaçlarla işlendiği hallerde, ilgili kişiler Tüzük ile tanınan hakları kullanamayacak ve dolayısıyla da kişisel

³³⁰ Bkz. GVK Tüzüğü, m.5/1(b), m.5/1(e), m.89/1.

³³¹ Wachter & Mittelstadt, s.102.

³³² Küzeci, s.216.

³³³ Wachter & Mittelstadt, s.102-108.

³³⁴ Viktor MAYER-SCHÖNBERGER & Yann PADOVA, Regime Change? Enabling Big Data Through Europe’s New Data Protection Regulation, The Columbia Science & Technology Law Review, 2016, s.315-335, <https://journals.library.columbia.edu/index.php/stlr/article/view/4007>.

³³⁵ Tal Z. ZARSKY, Incompatible: The GDPR in the Age of Big Data, Seton Hall Law Review, Vol.47, No.4(2), 2017, s.1007-1008, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (Kısaltılmışı “Incompatible: The GDPR in the Age of Big Data”).

verilerinin istatistiksel amaçlarla işlenmesini engelleyebilecek bir imkana sahip olamayacaklardır. Öte yandan, ilgili kişiler, kendi kişisel verilerinin analiz edilmesiyle oluşturulan, Tüzük m.89/1 tahtında “istatistiksel sonuç” niteliğindeki profillerine ilişkin olarak da herhangi bir hak iddia edemeyeceklerdir³³⁶.

Bu muafiyetlerin devlet kurumları ve üniversiteler gibi kamu ve araştırma kurumlarının yanı sıra ticari kazanç sağlayan özel şirketler için de geçerli olup olmadığı ayrı bir tartışmanın konusu olmuştur³³⁷. GVK Tüzüğü’nün giriş bölümünün 162. paragrafında, kişisel verilerin istatistiksel amaçlarla işlenmesi, “istatistiksel araştırmalar veya istatistiksel sonuçların üretilmesi için gerekli olan herhangi bir kişisel veri toplama ve işleme faaliyeti” olarak tanımlanmıştır³³⁸. Öte yandan, aynı paragrafta, kişisel verilerin istatistiksel amaçlarla işlenmesi suretiyle edinilen çıktıların, gerçek bir kişi ile ilgili herhangi bir tedbir veya karar alınmasında kullanılamayacağı belirtilmiştir³³⁹. Mayer-Schönberger ve Padova, “istatistiksel amaçlar” kavramının geniş yorumlanabileceğini ve Tüzük kapsamındaki muafiyetlerin sadece kamu menfaati için gerçekleştirilen işleme faaliyetleri açısından değil, ticari kazanç amacı güden özel şirketler için de uygulanabilir olduğunu ileri sürmüştür³⁴⁰. Yeterli bir hukuki dayanak sunulmamakla birlikte, muafiyetlerin ticari çıkarlar için kullanılamayacağını ve bu muafiyetler kapsamında oluşturulan istatistiksel sonuçların daha sonra ticari çıkarlar için kullanılacak olması halinde, işleme faaliyetinin kişisel verilerin korunmasına ilişkin genel ilkeler ve hukuka uygunluk sebeplerine dayandırılması gerekeceğini ileri süren görüşler de bulunmaktadır³⁴¹.

Önemle belirtmek gerekir ki, “kamu yararına arşivleme, bilimsel, tarihi veya istatistiksel amaçlarla” gerçekleştirilen veri işleme faaliyetlerinin, Tüzük m.5/1(b) ile düzenlenen “amaçla sınırlılık” ve m.5/1(e) ile düzenlenen “saklama süresinin

³³⁶ Wachter & Mittelstadt, s.103.

³³⁷ Wachter & Mittelstadt, s.104.

³³⁸ Bkz. GVK Tüzüğü, Giriş Bölümü, 162.Paragraf.

³³⁹ Bkz. GVK Tüzüğü, Giriş Bölümü, 162.Paragraf.

³⁴⁰ Mayer-Schönberger & Padova, s.326.

³⁴¹ Wachter & Mittelstadt, s.104-105.

sınırlandırılması” ilkelerinden muaf tutulabilmesi uygun idari ve teknik tedbirlerin alınmasına bağlıdır. Bu tedbirlerden biri de anonimleştirmedir. Öte yandan, veri sorumlusu profillemeye ve otomatik karar alma faaliyeti kapsamında topladığı ve işlediği verileri, işleme amacı ortadan kalktığında silmek veya anonim hale getirmekle yükümlüdür. Gerek kamu yararına arşivleme, bilimsel, tarihi veya istatistiksel amaçlarla gerçekleştirilen veri işleme faaliyetlerinde idari ve teknik tedbirler kapsamında verilerin anonimleştirilmesi, gerek işleme amacı ortadan kalktığında verilerin silinmesi veya anonim hale getirilmesi zorunluluğu, verilerin işleme amacı ile alakasız, ölçsüz ve yanlış ya da güncelliğini yitirmiş hale gelmesini engelleyerek, profillemeye faaliyetinin veri minimizasyonu (*data minimisation*) ve doğru ve gerektiğinde güncel olma (*accuracy*) ilkelerine uygun şekilde gerçekleştirilmesini sağlar. Profillemeye ve otomatik karar alma faaliyetlerinden doğabilecek kişisel verilerin korunmasına yönelik risklerin minimum seviyeye indirilmesi açısından, verilerin anonimleştirilmesi veri sorumlularına tanınan önemli bir imkandır. GVK Tüzüğü’nde anonim verilerin, kişiyi belirli veya belirlenebilir kılma ihtimali taşımadığından bahisle kişisel verilerin korunması kapsamına girmediği açıkça düzenlenmiştir³⁴². Ancak, içinde bulunduğumuz büyük veri çağında, verinin miktarı ve çeşitliliği arttıkça, daha çok verinin birbiriyle eşleştirilebilme ihtimali de artmakta, bu da bireylerin kimliklerinin belirlenebilmesini kolaylaştırmaktadır³⁴³. Nitekim günümüzde büyük veri teknolojileri ve teknikleri ile farklı veri kümeleri birbirleriyle eşleştirilmesi suretiyle anonimleştirilmiş veri³⁴⁴ kümelerinden kişilerin kimliklerinin tespit

³⁴² Bkz. GVK Tüzüğü, Giriş Bölümü, 26. Paragraf.

³⁴³ Mesut Serdar ÇEKİN, 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha Yayıncılık, 1. Baskı, İstanbul, 2008, s.95; Viktor MAYER-SCHÖNBERGER & Kenneth CUKIER, Büyük Veri- Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim, 1. Baskı, İstanbul, 2013, s. 161.

³⁴⁴ Anonim veri, “başka verilerle eşleştirilse dahi hiçbir şekilde kimliği belirli veya belirlenebilir bir gerçek kişi ile ilişkilendirilemeyecek hale dönüştürülmüş, kişiyle ilişkisi tamamen kesilmiş” veridir. Article 29 Working Party, Personal Data, s.21. Diğer bir ifadeyle, anonimleştirme veri kümelerinden isim, kimlik numarası, doğum tarihi, adres ve benzeri kişinin kimliğinin belirlenmesini sağlayan her türlü veriden arındırılmasıdır. Mayer-Schönberger & Cukier, s. 161-162. KVK Kanunu m. 3/b’de “anonim hale getirme”, “kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi” olarak tanımlanmıştır. Ulusal mevzuatta kişisel verilerin anonimleştirilmesine ilişkin usul ve esaslar, “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik” te düzenlenmiştir.

edilebildiği hadiseler yaşanmaktadır³⁴⁵. Bu durum, anonimleştirme ile ilgili tartışmaları beraberinde getirmektedir. Zira her ne kadar büyük veri setlerindeki verilerin anonimleştirildiği iddia ediliyor olsa da veri miktarının artması ve veri analiz yöntemlerinin gelişmesiyle, veri setlerinin gerçek anlamda anonimleştirilmesi neredeyse imkansız hale gelmektedir³⁴⁶.

2.1.4. Belirli, Açık ve Meşru Amaçlar için Toplanma ve İşlenme

GVK Tüzüğü'nde “amaçla sınırlılık” (“*purpose limitation*”) ³⁴⁷olarak ifade edilen kişisel verilerin “belirli, açık ve meşru amaçlar için toplanması ve işlenmesi” ilkesi ilgili kişilerin, kişisel verilerinin nasıl kullanılabileceğini anlamalarına ve kişisel verilerinin işlenmesinin sınırlarını belirlemelerine imkan tanıyarak profillemeye faaliyetlerinin şeffaf ve öngörülebilir olmasına hizmet eder³⁴⁸. Bu ilke gereği, veri sorumlusu, en geç verilerin toplanma anında ilgili kişiyi kişisel verilerinin profillemeye ve otomatik karar alma uygulamaları kapsamında kullanılma amacı

³⁴⁵ Bu hadiselerden başlıcaları ve konuyla ilgili çalışmalarda en sık örnek gösterilenler, AOL ve Netflix vakalarıdır. 2006 yılında ABD merkezli web portalı ve çevrimiçi hizmet sağlayıcısı AOL (America Online), eski arama sorgularını anonim hale getirerek kamuya açıklaması ve New York Times gazetesi çalışanlarınca bu aramaların eşleştirilmesiyle Thelma Arnold isimli kullanıcının tespit edilmesi üzerine, başka kullanıcıların da kimliklerinin tespit edilebildiği ortaya çıkmıştır. Aynı sene, teknoloji ve medya hizmetleri sağlayıcı Netflix'in, kullanıcıların kiralama kayıtlarını anonimleştirerek kamuya açıklamış; Texas Üniversitesi'nden bazı araştırmacılar bu verileri diğer kamuya açık veri setleriyle eşleştirerek, bir filme değerlendirme notu vermenin bir Netflix müşterisini %84 oranında tespit edebilmesini sağlığını, değerlendirme notunun verildiği tarih bilgisinin bilinmesi halinde müşteri kimliğinin tespit edilebilirliğinin %99'a çıktığını ortaya koymuştur. Mayer-Schönberger & Cukier, s. 161-162. Benzer şekilde, 2014 yılında New York City Taksi ve Limuzin Komisyonu (*Taxi and Limousine Commission*), o yıl içinde New York şehrinde yapılan tüm taksi yolculuklarına ilişkin bilgileri içeren veri setlerini, plaka ve taksi kimlik numarası bilgilerini gizlemek suretiyle anonimleştirerek kamuya paylaşmış; ancak anonimleştirmeişleminin hatalı yapılması sonucu, taksi kimlik numaralarının tamamının eski haline getirilmesiyle taksi sürücülerinin gelir bilgisine ulaşılması mümkün hale gelmiştir. O sırada Neustar şirketinde stajyer olarak çalışan bir veri bilimci, internetteki ünlü kişilerin taksiye binerken veya inerken çekilmiş bazı fotoğraflarında taksilerin kimlik numaralarının görüldüğünü tespit ettikten sonra, kilik numarası, tarih ve saat bilgilerini kullanarak veri setindeki yolculuklara ilişkin başlangıç ve varış noktalarını, yolculuk ücretini ve hatta bahşiş tutarını tespit etmiştir. Boris LUBARSKY, Re-Identification of “Anonymized Data”, Georgia Law Technology Review, 2017, s.211, <https://perma.cc/86RR-JUFT>.

³⁴⁶ Paul OHM, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010), s.1704-1706.

³⁴⁷ Bkz.GVK Tüzüğü, m. 5/1(b).

³⁴⁸ Article 29 Working Party, Opinion 03/2013 on Purpose Limitation (WP203), s.17 (Kısaltılmışı “Purpose Limitation”).

hususunda şeffaf ve yeterince anlaşılır bir şekilde bilgilendirmeli ve profillemeye faaliyetini hukuka uygunluk sebeplerinden birine dayandırabilmelidir. Profillemeye ve otomatik karar faaliyetleri kapsamında toplanacak kişisel veriler, öncelikle, “belirli, açık ve meşru amaçlar için” toplanmalı, ikinci olarak ise, bu verilerin toplanma amacı ile sonraki kullanım amaçları uyumlu olmalıdır.

İlkenin profillemeye açısından uygulanabilirliğine ilişkin sorunlardan ilki, profillemeye faaliyetinin hangi amaçla gerçekleştirildiği verilerin toplanma anında belirli olmaması ile ilgilidir. Profillemeye ve otomatik karar uygulamalarında kullanılan büyük veri analitiği yöntemleri ve nesnelerin interneti uygulamaları aracılığıyla belirsiz veya geniş bir şekilde tanımlanmış amaçlar için geniş ölçekte veri toplanmaktadır. Kişisel verilerin nasıl kullanıldığını yeterince şeffaf bir şekilde ortaya koyamayan günümüzde oldukça yaygın şekilde veri toplayan nesnelerin interneti uygulamaları ve bunların topladığı verileri birbiri ile ilişkilendirebilen kimlik tanıma teknolojileri, kişinin önceden öngöremeyeceği şekilde profilinin çıkarılmasını mümkün kılmakla birlikte bireyin mahremiyet ve kişilik hakları üzerindeki kontrolüne de zarar vermektedir³⁴⁹. Çalışmanın ilgili bölümünde de açıklandığı üzere, profillemeye faaliyeti, veri sorumlusunun verilerin toplanma aşamasında keşfetmeyi amaçlamadığı verilerdeki gizli örüntü ve korelasyonların tanımlanmasını sağlamaktadır. Zarsky profillemeye faaliyetinin bu özelliğini, profillemeye sürecinin sadece veri sorumlusunun verilerin toplanma anında mevcut sorularına değil, aynı zamanda veri sorumlusunun verileri toplamadan önce sormayı düşünemediği sorulara da cevap verme kapasitesine sahip olduğunu belirterek tanımlamaktadır³⁵⁰. Mayer-Schönberger ve Padova, büyük veri analitiğinde, verilerin gerçek değerinin toplanma anında değil analiz anında ortaya çıktığından bahisle, kişisel verilerin toplanmasının bir amaçtan ziyade çıkara yönelik olarak gerçekleştiğini ifade etmiştir³⁵¹. Bu bağlamda, profillemenin

³⁴⁹ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.10.

³⁵⁰ Tal Z. ZARSKY, “Mine Your Own Business!”: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion, Yale Journal of Law & Technology, Vol.5, 2002-2003, s.4, <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1008&context=yjolt>.

³⁵¹ Mayer-Schönberger & Padova, s.320.

amaçları ilk etapta bilinse bile, analitik yöntemleri ile veri setleri arasındaki örüntülerin tespit edilmesiyle verilerin toplanma anında öngörülemeyen yeni işleme amaçları ortaya çıkabilmekte ve başlangıçtaki amaçların verilerin analiz edilmesinden sonra değişmesi söz konusu olabilmektedir³⁵².

Bu noktada, sorunu, 29. Madde Veri Çalışma Grubu'nun ilgili örneği üzerinden somutlaştırmak faydalı olacaktır. Bu örnekte, bir mağaza, müşterilerinden sadakat kartı başvurusunda topladığı verilerini (isim, doğum tarihi, cinsiyet, iletişim bilgileri, çalışma durumu gibi bilgiler), müşterilerinin satın alma alışkanlıklarını analiz etmek, pazarlama trendlerini belirlemek, müşterilere özel tekliflerde bulunmak, hesaplarına indirim kuponları tanımlamak için analiz etmektedir. Mağaza, verilerin toplanma anında ilgili kişilere sunduğu aydınlatma metninde (*terms & conditions*) sadece “verilerin müşterilere özel teklifler ve indirim kuponları sağlamak da dahil olmak üzere pazarlama amaçlarıyla” kullanılabileceğini belirtmiştir. Öte yandan, mağazanın bu verilerin analizinde kullandığı yenilikçi analitik yazılımı bir kadın müşterinin hamile olduğunu ve hamileliğinin kaçınıcı ayında olduğunu yüksek olasılıkla tahmin edebilmektedir. İlgili kişinin hamileliğine ilişkin bu bilgiler, kişiye özel pazarlama tekliflerinin kişinin profiline uyarlamak için kullanılır ve ilgili kişinin ailesiyle yaşadığı evin posta kutusuna hamilelikle ilgili reklamlar gönderilir. Bu örnekte, her ne kadar ilgili kişinin kişisel verilerinin toplanma anında hamile olduğunu tespit edilmesi amaçlanmıyor olsa da pek çok müşterinin öngöremeyeceği, sakıncalı ve uygunsuz bulacağı ve rahatsız olacağı bir şekilde, hamileliği tahmin etmek için geliştirilmiş gizli algoritmaların kullanılması suretiyle ilgili kişinin profili çıkarılmıştır. Bu bağlamda, kişisel verilerin toplanma amacından farklı olan sonraki işleme amacının ilgili kişinin “makul beklentisi” dahilinde olduğunu söylemek mümkün olmayacaktır. 29. Madde Veri Çalışma Grubu'na göre, burada sorun toplanan verilerin niteliğinden ziyade, bu verilerin daha sonra toplanma amacından farklı bir

³⁵² Arnold ROOSENDAL, Digital Personae and Profiles in Law Protecting Individuals' Rights in Online Contexts, Wolf Legal Publishers (WLP), s.48-50, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2313576.

amaçla işlenmesi, diğer verilerle eşleştirilme şekli, ilgili kişinin verilerin toplanma anında yeterince şeffaf bir şekilde bilgilendirilmemesi ve ilgili kişinin itirazına konu olabilecek gizli bir algoritma ile kişinin hamileliği ile ilgili hamileliğinin kaçınıcı ayında olduğu bilgisini de içeren genel profilinin çıkarılması ile ilgilidir³⁵³.

GVK Tüzüğü'nde, kişisel verilerin toplanma amacından farklı bir amaç için işlenmesi mutlak şekilde yasaklanmamış, toplama amacı ile sonraki işleme amacının birbiri ile uyumu olması gerektiğini hüküm altına alınmıştır³⁵⁴. Belirtilmelidir ki, kişisel verilerin toplandıktan sonra farklı bir amaç için işlenmesi, sonraki amacı direkt olarak uyumsuz hale getirmemekte, her işleme faaliyeti özelinde değerlendirme yapılması gerekir³⁵⁵. Buna göre, ilk amaçla sonraki amacın uyumluluğu değerlendirilirken, iki amaç arasındaki herhangi bir bağlantının, ilgili kişilerin makul beklentilerinin, verilerin niteliğinin ve sonraki işleme faaliyetlerinin olası sonuçlarının ve gerekli tedbirlerin alınıp alınmadığı dikkate alınmalıdır³⁵⁶. Birleşik Krallık Bilgi Komisyonu Ofisi ise, sonraki işleme amacının ilk amaçla uyumlu olup olmadığına karar almadaki rol oynayan esas faktörün sonraki işleme amacının adil olup olmadığı ile ilgili olduğu görüşündedir. Buna göre, sonraki işleme amacının adil olup olmadığına ilişkin yapılacak değerlendirmede, söz konusu yeni işleme amacının ilgili kişilerin mahremiyetini nasıl etkilediği ve ilgili kişinin makul beklentisi içinde kabul edilip edilemeyeceği önem teşkil etmektedir³⁵⁷.

Bu bağlamda, sonraki işleme amacının verilerin toplanma amacı ile uyumlu olması halinde, kişisel verilerin profillemeye faaliyetinde kullanılması mümkündür. Ancak, sonradan ortaya çıkan profillemeye amacı ile verilerin toplanma amacının uyumlu olmaması halinde, profillemenin hukuka uygunluk sebeplerinden birine dayanması aranacaktır. Bu noktada, ilk amaç ile sonraki amacın uyumlu olup

³⁵³ Article 29 Working Party, Purpose Limitation, s.61.

³⁵⁴ Article 29 Working Party, Purpose Limitation, s.12-13.

³⁵⁵ Article 29 Working Party, Purpose Limitation, s.21.

³⁵⁶ Bkz. GVK Tüzüğü, Giriş Bölümü, 50.Paragraf.

³⁵⁷ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.38.

olmadığının neye göre değerlendirileceği sorunu gündeme gelmektedir. 29. Madde Çalışma Grubu tarafından bu değerlendirmede esas alınmak üzere belirlenen temel faktörler şu şekildedir: (i) kişisel verilerin toplanma amaçları ile sonraki işleme amaçları arasındaki ilişki; (ii) kişisel verilerin hangi bağlamda toplandığı ve ilgili kişilerin sonraki kullanımlarına ilişkin makul beklentileri, (iii) kişisel verilerin niteliği ve sonraki işleme faaliyetinin ilgili kişiler üzerindeki etkisi, (iv) adil işlemeyi sağlamak ve ilgili kişiler üzerinde herhangi bir uygunsuz etkiyi önlemek için veri sorumlusu tarafından alınan tedbirler³⁵⁸.

29.Madde Çalışma Grubu’nun öngördüğü uyumluluk değerlendirmesinde esas alınması gereken faktörler, yukarıdaki örnek üzerinden somutlaştırılabilecektir. Bir perakende satış mağazasının sadakat kartına başvuru sırasında kişisel verilerini paylaşan ilgili kişinin bu verilerin mağazanın pazarlama stratejisi için kullanılacağına ilişkin makul bir beklenti içinde olması muhtemeldir. Dolayısıyla sadakat kartı için toplanan verilerin, ilgili kişiye satın alma tercihlerine uygun indirim kuponu tanımlanması için kullanılması halinde, verilerin toplanma amacı ile sonraki kullanım amacı arasında ilişki olduğu ve kişinin makul beklentileri dahilinde olduğu kabul edilebilecektir. Ancak, yukarıdaki örnekteki gibi, sadakat kartı için toplanan verilerin kullanılmasıyla kadın kullanıcıların hamileliğine ilişkin tahminlerde bulunulması ve kişinin hamilelik bilgilerinin kişiye yönelik pazarlama stratejisi belirlenmesinde kullanılması halinde, veriler toplandıktan sonra gerçekleştirilen hamileliğe ilişkin profillemeye faaliyeti, ilgili kişinin makul beklentisi kapsamında değerlendirilemeyecektir. Farklı bir örnek olarak, sosyal medya kullanıcılarının sosyal medya hesaplarında paylaştıkları bilgilerin, sağlık riskleri veya kredibilitelerinin değerlendirilmesinde veya belirli ürünlerin pazarlamasının yapılması için kullanıldığı bir durumda, ilgili kişilerin belirtilen sonraki işleme faaliyetlerine yönelik açık rızaları alınmadığı takdirde, sonraki işleme amacının verilerin toplanması amacıyla uyumluluğundan veya adillikinden bahsedilemeyecektir³⁵⁹. Bir şirket veya kuruluşun, büyük veri analitiği

³⁵⁸ Article 29 Working Party, Purpose Limitation, s.40.

³⁵⁹ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.38.

için veri simsarlarından (*data brokers*) kişisel veri satın aldığı durumlarda ise, veri sorumlularınca mutlaka gerçekleştirilecek analitik faaliyetlerinin verilerinin ilgili kişilerden ilk toplanma amacı ile uyumlu olup olmadığına bakılarak, ilgili kişilerden tekrar rıza alınması veya yeni işleme amaçlarına ilişkin yeniden bilgilendirme yapılmasını değerlendirilmelidir³⁶⁰.

29. Madde Çalışma Grubu, kişisel verilerin toplandıkları amaçtan farklı bir amaç için işlenmesi sorununu büyük veri analitiği ve profillemeye bağlamında değerlendirmiştir. Buna göre, kişisel verilerin toplandıkları amaçla uyumlu olarak işlenebileceği iki tür işleme faaliyeti mevcuttur. Bunlar, (i) genel trendler hakkında tahminde bulunmak veya korelasyonları tespit etmek amacıyla gerçekleştirilen profillemeye ve (ii) ilgili kişinin davranışları, tercihleri ve kişiliği hakkında analiz yapmak veya tahminde bulunmak ve ilgili kişi hakkında kararlar almak için gerçekleştirilen profillemeye faaliyetleridir. Çalışma grubunca, kişisel verilerin, ilgili kişiden toplandıktan sonra, toplanma amacından farklı olarak, genel eğilimlere ilişkin tahminde bulunmak veya korelasyonları tespit etmek amacıyla, ilgili kişinin profilinin çıkarılmasında kullanılması halinde, veri sorumlusunun veri güvenliğini temin etmeye yönelik gerekli idari ve teknik önlemleri almakla yükümlü olduğu belirtilmiştir. Öte yandan, kişisel verilerin toplanma amacından farklı olarak, ilgili kişi hakkında bir karar alınması amacıyla işlenecek olması halinde, ilgili kişinin “özgür iradeyle açıklanmış, tereddüte yer vermeyecek açıklıkta, bilgilendirmeye dayalı rızası” alınmış olmalıdır. Çalışma grubunun ilgili değerlendirmesinde, şeffaflık ilkesinin de önemine değinilmiş ve ilgili kişilere profillerini düzeltme ve güncelleme imkanı ile kişisel verilerine, taşınabilir, kullanıcı-dostu ve bilgisayar aracılığıyla okunabilir bir formatta erişime imkanı tanınması gerektiği belirtilmiştir³⁶¹.

Profillemeye faaliyetleri ile bireyin geçmiş veya mevcut durumu ile ilgili bilgi edinilmesini sağlamakla birlikte, gelecekteki durumu ile ilgili de çıkarımlarda

³⁶⁰ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.39.

³⁶¹ Article 29 Working Party, Purpose Limitation, s.46.

bulunur. Örneğin, herhangi bir banka veya finans kuruluşunca kredi kartı ve fatura borcu ödeme geçmişi gibi finansal durumuna ilişkin gösterge teşkil eden bilgilerinin analiz edilmesi suretiyle çıkarılan profili, kişinin gelecekte farklı banka veya finans kuruluşları nezdinde gerçekleştirebileceği kredi başvurularında değerlendirmeye esas teşkil edebilmektedir. Bu ve benzeri hallerde yine verilerin toplanma amacı ile gelecekteki işleme amacının birbiri ile uyumlu olup olmadığının değerlendirilmesi gerekecektir.

KVK Kanunu’nda sonradan ortaya çıkan amaçlarla ilgili bir düzenlemeye açıkça yer verilmemiştir. Kurumun, kanunun uygulamasına ilişkin rehberinde de veri sorumlularının ilgili kişiye bildirdikleri amaçlardan farklı amaçlarla veri işlemleri halinde sorumluluklarının doğacağı ifade edilmiştir. Dolayısıyla kişisel verilerin işlenmesinde amaç değişikliği halinde, GVK Tüzüğü’nden farklı olarak Türk hukukunda, baştaki işleme amacıyla uyumlu olsa dahi kişisel verilerin işlenemeyeceği sonucuna varılmaktadır. Uygulamada çeşitli sorunlara sebebiyet vermesi ve uzun süredir tartışma konusu olmasına rağmen Kanun’da açık bir düzenlemeye yer verilmemesi bazı yazarlarca bir eksiklik olarak değerlendirilmiştir³⁶².

Profilleme ve otomatik karar uygulamaları, kişisel verilerin “meşru amaçlar için toplanması ve işlenmesi” gerekliliği açısından da sorun teşkil edebilmektedir. Kişisel verilerin toplanma ve işlenme amacının meşru olması geniş bir kavramdır. Kişisel verilerin toplanma amacının “meşru” kabul edilebilmesi için, kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin yanı sıra bütün hukuki düzenlemeler ve gereklilikler ile uyumlu olması gerekir³⁶³. Öte yandan, verilerin toplanma amacı ile verilerin işlenmesi ile hedeflenen menfaat dengeli olmalıdır³⁶⁴. Bu ilke, kişisel verilerin ayrımcı ve önyargılı uygulamalara yol açacak şekilde işlenmesini de yasaklar. 29. Madde Çalışma Grubu, meşru olmayan amaçlar için

³⁶² Çekin, s.49; Dülger, s.122.

³⁶³ Küzeci, s.203.

³⁶⁴ Küzeci, s.203

gerçekleştirilen profillemeye bir mağazanın müşterilerini etnik kökenlerine göre profillemesini örnek olarak göstermiştir³⁶⁵. İlgili örnekte, Asyalı soyadına sahip müşterilere gönderilen kuponlara farklı oranlarda kişiselleştirilmiş indirimler uygulamak suretiyle, “Asyalı” müşterilere “beyaz” müşterilere göre daha düşük ücret uygulanır. Müşterilere “sadakat kartı için toplanan bilgilerin pazarlama amacıyla işlenebileceği” dışında bir bilgilendirme yapılmamıştır. Örnekte şeffaf bir şekilde gerçekleşmeyen veri işleme faaliyeti, ayrımcı ve adil olmayan bir uygulama ile sonuçlanmıştır. 29. Madde Çalışma Grubu, bu örnek üzerinden, kişisel verilerin meşru amaçlar için işlenmesinde şeffaflığın da önemli bir rol oynadığını vurgulamıştır. Zira mağaza Asyalı müşterilere indirim yapılacağını açık bir şekilde bildirmiş olsaydı, tüm müşteriler bu ayrımcı uygulamanın farkında olur ve mağazadan alışveriş yapıp yapmayacaklarını bu kapsamda değerlendirebilirlerdi³⁶⁶.

2.1.5. Amaçla Bağlantılı, Sınırlı ve Ölçülü Veri İşleme

Kişisel verilerin işlenmesi faaliyetlerinin “amaçla bağlantılı, sınırlı ve ölçülü” olması gerekliliğini ifade eden bu ilke kişisel verilerin miktarı, niteliği ve belirlenen amaca uygunluğu ile ilgilidir³⁶⁷. Bu ilke ile toplanacak verilerin işleme amaçları ve miktarı sınırlandırılmış, işlenecek veri miktarının işleme amacı ölçülü olması öngörülmüştür. Bu bağlamda, veri işleme amacının gerçekleştirilmesine hizmet etmeyen veri işleme faaliyetlerinden kaçınılması gerekmektedir. İlke ile amaçlanan hukuki yarar, gelecekte kullanılmak üzere gereğinden fazla veri toplanmasını engellemek ve ilgili işleme faaliyeti ile hedeflenen amacın gerçekleşmesi için gereken minimum verinin kullanılmasını sağlamaktır. Veri sorumlusu, işleme faaliyeti için belirlediği amaca ulaşması için kişisel verilerin işlenmesinin zorunlu olması halinde, bu amaca ulaşmak için olanaklı olan en az veriyi kullanmalıdır³⁶⁸. Belirtilmelidir ki, bu ilke ile işlenen veri miktarının mutlak bir asgari seviyeye indirilmesinden ziyade işleme amacına uygun bir seviyeye

³⁶⁵ Article 29 Working Party, Purpose Limitation, s.54-55.

³⁶⁶ Article 29 Working Party, Purpose Limitation, s.54-55.

³⁶⁷ Dülger, s.117.

³⁶⁸ Küzeci, s.208.

indirilmesi hedeflenmektedir³⁶⁹. Dolayısıyla, belirtilen amaca ulaşılması için kişisel verilerin işlenmesi zorunlu değilse, bireyin korunması hedeflenen temel hak ve özgürlüklerine “daha az ya da hiç” müdahale edilmemesini sağlayan diğer yöntemler tercih edilmelidir³⁷⁰.

Kişisel verilerin “amaçla bağlantılı, sınırlı ve ölçülü işlenmesi”, GVK Tüzüğü m.5/1(c)’de “veri minimizasyonu” (“*data minimisation*”) olarak ifade edilmiştir³⁷¹. Veri minimizasyonu ilkesi, amaçla sınırlılık ilkesinin olağan bir sonucu olarak değerlendirilmektedir³⁷². Zira veri sorumlusu işleme amacını belirledikten sonra, kişisel verilerin toplanmasının ve/veya işlenmesinin, ilgili amaç için gerekli olup olmadığını değerlendirmekle yükümlüdür³⁷³. Tıpkı amaçla sınırlılık gibi, veri minimizasyonu da risk yönetimi sağlayan önleyici bir

³⁶⁹ Voigt & Von Dem Bussche, s.241.

³⁷⁰ Küzeci, s.208; Çekin, s. 53.

³⁷¹ KVKK’da veri minimizasyonu açık bir şekilde düzenlenmemiştir. Ancak kanunda münferit bir düzenlemeye yer verilmemiş olmakla birlikte, gerek kanunda veri işlemenin amaçla sınırlı ve ölçülü olması ilkesi ve dürüstlük kuralına uygunluk ilkesine yer verilmiş olması, gerekse de Kurul kararları ve ve duyurularında veri minimizasyonuna atıf yapılmış olması, Türk hukukunda da veri minimizasyonunun uygulama alanı bulduğunu göstermektedir duyurularında veri minimizasyonuna atıf yapılmış olması, Türk hukukunda da veri minimizasyonunun uygulama alanı bulunduğunu göstermektedir. Kurul mahkemece veri sorumlusundan ilgili kişinin kişisel verilerinin talep edilmesi halinde, veri sorumlusunun talep edilenden fazla veri paylaşmasını açıkça “veri minimizasyonu ilkesine aykırılık” olarak değerlendirilmiştir. Bkz. <https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik->. Kurul, yine başka bir kararında “spor salonu hizmeti veren veri sorumlusunun salona giriş çıkışların kontrol edilmesi kapsamında üyelerinin biyometrik verilerini işlemesinin, ilgili kişilerin açık rızası bulunsa dahi, ilgili kişiden minimum düzeyde veri talep etme ilkesine aykırılık teşkil ettiğine” hükmetmiştir. İlgili karar için bkz. Kişisel Verileri Koruma Kurulu’nun 2020/167 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6738/2020-167>. Kurum, internet sitesinde yayınladığı 27.03.2020 tarihli duyuruda veri minimizasyonu ilkesinden açıkça bahsedilerek, Covid-19 virüsü ile mücadeleye yönelik gerçekleştirilecek veri işleme faaliyetlerinin, diğer tüm veri işleme faaliyetlerinde olduğu gibi amaçla bağlantılı ve sınırlı olarak gerçekleştirilmesi, gereğinden fazla kişisel veri işlenmesinden kaçınılması ve hedeflenen amaca ulaşmak için “imkan dahilindeki en müdahaleci olmayan” yolun tercih edilmesi gerektiği belirtilmiştir. İlgili duyuru için bkz. Kişisel Verileri Koruma Kurumu, “Covid -19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler”, Kamuoyu Duyurusu, 27.03.2020, <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler->.

³⁷² Asia BIEGA & Michele FINCK, Reviving Pupose Limitation and Data Minimisation in Data Driven Systems, Technology and Regulation, 2021, 44-61, s.55, <https://arxiv.org/pdf/2101.06203.pdf>.

³⁷³ Nikolaus FORGÓ & Stefanie HÄNOLD & Benjamin SCHÜTZE, “The Principle of Purpose Limitation and Big Data”, New Technology, Big Data and the Law (Eds: Marcelo Corrales, Mark Fenwick, Nikolaus Forgó), Springer Nature Singapore Pte Ltd. 2017, s.68.

yaklaşımıdır. Nitekim gereğinden fazla verinin işlenmesi hacklenme riskinden, yanlış, hatalı ve potansiyel olarak tehlikeli kararlarla sonuçlanabilecek güvenilir olmayan çıkarımlar oluşturulmasına kadar gereksiz risk yaratma ihtimali barındırır³⁷⁴. Tüzüğün giriş bölümünün 78. paragrafında, tasarımdan itibaren ve varsayılan ayarlarla veri koruması için organizasyonel bir önlem olarak 'kişisel verilerin en aza indirilmesi' gerektiği belirtilmiştir³⁷⁵.

Amaçla sınırlılık ilkesi gibi, veri minimizasyonu ilkesinin de profillemeye ve otomatik karar alma faaliyetleri açısından uygulanabilirliği tartışma konusu olmuştur³⁷⁶. Algoritmik karar mekanizmaları, ayrımcılık ve önyargı içeren çıktılar üretmenin yanı sıra veri minimizasyonu ilkesinin uygulanabilirliği açısından da risk barındırır. Veri minimizasyonu ilkesi ile veri madenciliğinin çalışma prensibinin bağdaştırılmasının oldukça zor olduğunu söylemek yanlış olmayacaktır. Zira veri madenciliğinin öne çıkan özelliği, çok büyük hacimli karmaşık ve çok boyutlu verileri, yararlı iç görüler oluşturabilecek örüntü ve korelasyonların keşfedilmesi suretiyle, anlamlandırabilmesidir. Yaygın varsayım, algoritmaları eğitmek için ne kadar çok veri kullanılırsa ne yapmak için eğitildiklerini tahmin etmede daha başarılı oldukları yönündedir. Bunun için, halihazırda bilinmeyen ancak gelecekte ortaya çıkabilecek faydalı kullanımlar için daha fazla veri toplanmaktadır. Bu “veri maksimizasyonu” yaklaşımı, büyük ve muhtemelen yasa dışı veri toplama ve verilerin daha fazla işlenmesi için bir teşvik ortamı yaratır³⁷⁷. Özellikle algoritmalar aracılığı ile düzenli olarak yeni korelasyonların keşfedildiği profillemeye araçlarını kullanan şirket ve kuruluşlar, ileride yararlı olacağı düşüncesiyle bireyler hakkında mümkün olduğunca fazla bilgi toplamaya eğilim gösterebilmektedir. Ancak her koşulda, bu şirket ve kuruluşlar da diğer tüm veri sorumluları gibi, sadece ilgili işleme amacını karşılamak için gerekli olan kadar veri işlendiğini ispat

³⁷⁴ Mireille HILDEBRANDT, Primitives of Legal Protection in the Era of Data-Driven Platforms, Georgetown Law Technology Review, 2018, s.267, <https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Hildebrandt-pp-252-73.pdf>.

³⁷⁵ Bkz. GVK Tüzüğü, Giriş Bölümü, 78.Paragraf.

³⁷⁶ Biega & Finck, s.45.

³⁷⁷ European Data Protection Board, Letter Out Ref. 2020-0004, 29 Ocak 2020, Brüksel, s.2-3, https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intvoldalgorithms_en.pdf.

edebilmelidir³⁷⁸. Bunun için ise, önce kişisel verilerin “belirli, açık ve meşru amaçlar için” işlendiği ortaya konulabilmelidir. Zira amacın ne olduğu açıkça belirlenemiyorsa, işlenen veri miktarının da amaçla ölçülü olduğunun gösterilmesi zorlaşacaktır. Birleşik Krallık Bilgi Komisyonu Ofisi’nin yapay zeka, yapay öğrenme ve büyük veri ile ilgili raporunda ifade edildiği üzere, veri analitiği sürecindeki bazı verilerin, ilerde çeşitli tahmin ve çıkarımlar için faydalı bulunabilecek olması, bu verilerin işleme amacı için gerekli olduğu sonucuna varmak için tek başına yeterli olmamakla birlikte, bu verilerin toplanması, kullanılması ve saklanması açısından da geçmişe dönük olarak da haklı bir gerekçe oluşturmamaktadır³⁷⁹. Veri sorumluları, kişisel verilerin toplanması ve saklanmasına ilişkin ihtiyacın sebebini şüpheye yer bırakmayacak şekilde açıklayabilmeli veya profillemeye süreçlerinde anonimleştirilmiş veya takma adlandırılmış veri kullanmayı değerlendirmelidir³⁸⁰.

Öte yandan, veri madenciliği uygulamasında sadece büyük miktarda veri toplanması değil, toplanan verilerin ileride faydalı olabileceği düşüncesiyle belirsiz bir süre için saklanması da veri minimizasyonu ve saklama süresinin sınırlandırılması (*storage limitation*) ilkesi açısından sorun teşkil etmektedir. Profillemeye ve otomatik karar uygulamalarının bu özelliği, veri minimizasyonu ilkesinin gerçekte ne ölçüde uygulama alanı bulabildiğinin değerlendirilmesinde önemli bir test kriteri oluşturmaktadır³⁸¹.

Hildebrandt, profillemeye ve otomatik karar faaliyetlerinin çoğunlukla birden fazla cihaz ve makine arası bilgi alışverişine, yüksek katmanlı sinir ağlarına ve etkileşimli sistemler arasındaki öngörülemez dinamiklere dayandığından bahisle, algoritmaların gerekli olmayan veriler ile eğitilmesini önlemenin daha iyi sonuçlar doğuracağı görüşündedir³⁸². Yapay öğrenme teknolojisi açısından, işleme amacıyla

³⁷⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.11.

³⁷⁹ Information Commissioner’s Office, Big Data, Machine Learning and Artificial Intelligence, s.40-41.

³⁸⁰ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.11.

³⁸¹ Biega & Finck, s.45.

³⁸² Hildebrandt, Primitives of Legal Protection in the Era of Data-Driven Platforms, s.267.

ilgisi olmayan, yanlış ve eksik veriler, “gereksiz” olmakla birlikte, hatalı sonuçlara da neden olur. Hildebrandt’a göre, bu durum, veri minimizasyonunun sadece bir veri koruma ilkesi değil, aynı zamanda yapay öğrenme algoritmalarının güvenilir bir çıkarımda bulunabilmesine ilişkin bir ön koşul niteliğinde olduğunu doğrulamaktadır. Veri minimizasyonu, verilerin düzenlenme ve ayıklanma ihtiyacını azaltacak ve veri işleme amacıyla alakalı olmayan verilerle zaman kaybedilmesini de önleyecektir³⁸³.

Kişisel verilerin işlenmesi sürecinde alınması gereken teknik ve organizasyonel önemler de veri işleme faaliyetinin bu ilkeye uygun şekilde gerçekleşmesine hizmet etmelidir³⁸⁴. Nitekim GVK Tüzüğü m.25/1’de, veri sorumlusunun hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, verilerin asgarileştirilmesi ilkesinin etkili bir şekilde uygulanmasına yönelik teknik ve düzenlemeye ilişkin tedbirleri almakla yükümlü olduğu düzenlenmiştir³⁸⁵. Bu kapsamda, toplanan verilerin amaca uygun bir seviyeye indirgenmesi için, anonimleştirme (*anonymisation*), takma adlandırma (*pseudonymisation*), tasarımdan itibaren veri koruma (*privacy by design*) ve varsayılan ayarlarla veri koruma (*privacy by default*) tedbirlerinin uygulanması gerektiği kabul edilmiştir³⁸⁶.

³⁸³ Hildebrandt, Primitives of Legal Protection in the Era of Data-Driven Platforms, s.267-268.

³⁸⁴ Voigt & Von Dem Bussche, s. 242.

³⁸⁵ KVK Kanunu’nda bu ilkeyi bu şekilde somutlaştıran bir hükmeye verilmemiştir. Çekin, s.53.

³⁸⁶ Voigt & Von Dem Bussche, s.242; Dülger, s.124; Çekin, s.53; Küzeci, s.212.

2.2. GENEL VERİ KORUMA TÜZÜĞÜ'NDE YER VERİLEN ÖZEL İLKELER

2.2.1. Hesap Verebilirlik

Gerek kamuda gerek özel sektörde çeşitli alanlarda, yaygın şekilde, bireyin hayatına ilişkin önemli kararların alınmasında kullanılan profillemeye ve algoritmik karar sistemleri, çalışmanın ilgili bölümünde incelendiği üzere birey hakkında adil olmayan, ayrımcı, önyargılı kararlar ile sonuçlanabilmektedir. Helen Nissenbaum, 1996 tarihli çalışmasında bilgisayara bağlı hale gelmiş toplumumuzda hesap verebilirliğin ve sorumluluğun sınırlarının belirsizleşmesine neden olan dört faktöre değinmiştir³⁸⁷. Nissenbaum'un bu çalışmasının üzerinden geçen zaman diliminde, bilgisayar teknolojisinde yaşanan dönüşümle birlikte, hesap verebilirlik ve sorumluluk kavramlarının sınırlarının belirsizleşmesine neden olan yeni faktörler ortaya çıkmıştır.

Hesap verebilirlik ilkesinin ve bu ilkeyle doğrudan ilgili olan şeffaflık ilkesinin bu sistemler açısından uygulanabilirliğine ilişkin başlıca sorunlardan biri ise, karar sürecinin tamamen opak bir işleyişe sahip olmasıdır. Burrell, ilgili çalışmasında, algoritmik hesap verebilirlik ve şeffaflığın önünde engel teşkil eden yapay öğrenme sistemlerindeki opaklık sorununun üç nedenine değinmiştir. Bunlar, (i) şirket, kurum ve kuruluşların kurumsal gizliliğin veya ticari sırların korunmasını sağlamak amacıyla bilinçli olarak yaratılan opaklık, (ii) kod yazmanın ve okumanın bir uzmanlık becerisi gerektirmesi ve ilgili programlama dilleri ve yapay öğrenme sistemleri konusunda yeterince bilgili kişinin az olması ve (iii)

³⁸⁷ Nissenbaum' göre, ilk olarak, bilgisayar sistemleri genellikle birden çok kişi tarafından tasarlanır ve çalıştırılır. Bunun sonucu olarak, sorumluluk birden fazla taraf arasında dağılır ve kimin veya hangi kurumların sorumlu tutulabileceğine dair bir tespit yapılması zorlaşır. İkinci olarak, yazılımlarda hataların kaçınılmaz olduğu yönündeki genel geçer inanış, yazılımlardaki hataların ortadan kaldırılmasına yönelik yatırımlar yapılmasına engel olmaktadır. Üçüncüsü, bilgisayar sistemlerinde ve yazılımlarda herhangi bir sorun yaşandığında, insanlar yerine bilgisayarı çok kolay suçlama eğiliminde olunmasıdır. Sonuncusu ise, yazılım geliştirenlerin kendi ürettikleri ürünün sorumluluğunu almayı reddetmeleridir. Helen NISSENBAUM, Accountability in a Computerized Society, Science and Engineering Ethics (1996) 2, s. 25-42, <https://nissenbaum.tech.cornell.edu/papers/AccountabilityinaComputerizedSociety.pdf>.

yapay öğrenme sistemlerindeki matematiksel optimizasyon süreçlerinin karmaşıklığı ve çok boyutlu oluşuna bağlı olarak, otomatik sistemler ile verilen kararların insan zihninin izin verdiği ölçekteki akıl yürütmeye anlaşılmasının güç olmasıdır³⁸⁸.

Bu durum, kişisel verilerin korunması açısından oldukça önemli olan şeffaflık ilkesinin tesis edilmesini zorlaştırmakta, bireyin kendisi hakkında karar süreçlerinin farkında olmamasına veya farkında olsa dahi anlamlandıramamasına neden olmaktadır. Otomatik karar sistemlerinin toplum üzerindeki önemli etkisi göz önüne alındığında, bu sistemleri kullananlara sistemlerin tasarlanması ve uygulanmasında kamusal hesap verme sorumluluğu yüklenmesi, günümüzde hiç olmadığı kadar önem arz etmektedir.

Hesap verebilirlik (“*accountability*”) ilkesi, ilk kez GVK Tüzüğü’nün 5.maddesinin ikinci fıkrasında açıkça düzenlenmek suretiyle hukuki çerçeveye kavuşturulmuştur. 29. Madde Çalışma Grubu’na göre hesap verebilirlik, en genel anlamda, sorumluluğun nasıl yerine getirildiğinin gösterilmesi ve bunun doğrulanabilmesini ifade etmektedir. Çalışma Grubu, sorumluluk ve hesap verebilirliğin bir madalyonun iki yüzü olduğunu ve sorumluluğun etkili bir şekilde yerine getirildiğinin gösterilebildiği müddetçe veri sorumlularına karşı yeterli bir güvenin tesis edilebileceğini belirtmiştir³⁸⁹. Belirtilmelidir ki, hesap verebilirlik ilkesinin kapsamı, GVK Tüzüğü’nde açıkça belirtilenlerle sınırlı değildir; kişisel verileri içeren veri işleme faaliyetlerinin tüm yönlerini kapsar³⁹⁰. Veri sorumlularının, kişisel verilerin korunması düzenlemeleri tahtında hesap verebilir veya sorumlu olabilmeleri, veri işleme faaliyetlerinin kişisel verilerin işlenmesine hakim olan genel ilkelere uyumlu olduğunun gösterebilmesini gerektirir³⁹¹. Bu

³⁸⁸ Jenna BURRELL, How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms, Big Data & Society, January-June 2016: 1-12, s. 1-2, <https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512>.

³⁸⁹ Article 29 Working Party, Opinion 3/2010 on the Principle of Accountability (WP 173), 13 Temmuz 2010, s.7, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (Kısaltılmışı “Principle of Accountability”).

³⁹⁰ Information Commissioner’s Office, Big Data, Machine Learning and Artificial Intelligence, s.52.

³⁹¹ Bkz. GVK Tüzüğü, m.5/2.

bağlamda hesap verebilirlik, kişisel verilerin korunmasına ilişkin diğer ilkelerle doğrudan ilişkilidir. Nitekim 29. Madde Çalışma Grubu da hesap verebilirlik ilkesinin, mevcut ilkelerin etkinliğini *de facto* olarak artırdığı, her türlü veri işleme faaliyetine ve türüne bu ilkenin uygulanması suretiyle kişisel verilere daha etkin bir koruma sağlanacağını belirtmiştir³⁹².

Tüzük m.30'da 250'den fazla çalışana sahip olan ve/veya 250'den az çalışana sahip olan ancak bireylerin temel hak ve özgürlükleri açısından risk teşkil eden veri işleme faaliyetleri yürüten şirket ve kuruluşların, kayıt tutmakla yükümlü olduğu belirtilmiştir³⁹³. Kayıt tutma yükümlülüğünün kapsamına kişisel verilerin işlenme amaçları da dahildir. Büyük veri analitiği alanında faaliyet gösteren şirketlerin 250'den fazla çalışana sahip olması veya bu şirketlerin veri işleme faaliyetlerinin doğası gereği bireylerin hak ve özgürlükleri açısından risk teşkil etmesi oldukça muhtemeldir. Öte yandan, büyük veri analitiğinde verilerin işlenme amacı çoğunlukla başlangıçta belirli değildir. Başlangıçta belirlenen ve kayıt altına alınan amaç, veri setleri arasındaki yeni korelasyonlar keşfedildikçe değişebilir. Birleşik Krallık Bilgi Komisyoneri Ofisi, bu durumun, büyük veri analitiği şirketlerinin hesap verebilirlik düzenlemelerine uyum sağlamaları açısından sorun teşkil edebileceği görüşündedir³⁹⁴.

Büyük veri analitiği ve algoritmik karar mekanizmaları bağlamında hesap verebilirlik, "algoritmik hesap verebilirlik" (*algorithmic accountability*) olarak ifade edilmektedir. Algoritmik hesap verebilirlik, yapay öğrenme sistemleri tarafından kullanılan ve geliştirilen algoritmaların, gerçekten de düşünülen şekilde veri işleyip işlemediği ve ayrımcı, hatalı veya adil olmayan çıkarımlar üretmediğinin kontrol edilebilmesine imkan tanıyan bir sorumluluk mekanizmasını ifade eder³⁹⁵.

³⁹² Article 29 Working Party, Principle of Accountability, s.9-10.

³⁹³ Bkz. GVK Tüzüğü, m.30/5.

³⁹⁴ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.51.

³⁹⁵ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.52.

Dünyanın en geniş bilgisayar topluluğu olduğu belirtilen Bilgi İşlem Makineleri Derneği (*Association for Computing Machinery- Kısaltılmışı “ACM”*) sponsorluğunda “Adil Olma, Hesap Verebilirlik ve Şeffaflık” (*Fairness, Accountability, Transparency- Kısaltılmışı “FAccT”*) alanında her sene dünyanın farklı yerlerinde konferans düzenlenmektedir. Kısaca “ACM FAccT” olarak anılan konferans, etik, yapay öğrenme, algoritmalar ve yapay zekanın kesiştiği alanda yapılacak araştırmalar için önde gelen ve disiplinlerarası bir forum haline gelmiştir. “Adil, şeffaf ve hesap verebilir yapay öğrenme” konusu üzerine çalışan seçkin araştırmacılar ve teknoloji şirketlerinde çalışan profesyonllerinden oluşan bir araştırma topluluğu da bu konferans ile özdeşleşmiştir. Araştırma topluluğu, veri sorumlusunun profileme ve otomatik karar alma faaliyetleri açısından hesap verme sorumluluğunu yerine getirebilmesinin, ilgili kişiyi bilgilendirme, kararları açıklama, otomatik karar alma mekanizması ile alınan kararın haklı dayanaklarını ortaya koyabilme ve bu sistemlerin olumsuz toplumsal etkilerini ve potansiyel zararlarını azaltma yükümlülüklerini etkin bir şekilde yerine getirebilmesine bağlı olduğu görüşündedir³⁹⁶. Araştırma topluluğunun ve ACM FAccT konferansının çalışmaları sonucunda “FAT-ML (*Fair, Accountable, Transparent Machine Learning*) ilkeleri” olarak anılan beş ilke belirlenmiştir. Buna göre, algoritmik hesap verebilirlik, profileme ve otomatik karar alma faaliyetlerinin sorumluluk (*responsibility*), doğruluk (*accuracy*), açıklanabilirlik (*explainability*), denetlenebilirlik (*auditability*) ve adil olma (*fairness*) ilkelerine uygun şekilde gerçekleştirilmesini hedeflemektedir³⁹⁷. Profileme ve otomatik karar sistemleri bağlamında algoritmik hesap verebilirlik kavramının anlaşılması açısından bu ilkelerin incelenmesi önemlidir. Sorumluluk ilkesi, profileme ve otomatik karar sistemlerinin, bireysel ve toplumsal ölçekteki muhtemel olumsuz etkilerinin ortadan kaldırılmasını sağlamaya yönelik somut düzeltme ve başvuru yollarının düzenlenmesi ve söz konusu olumsuz etkilerin vaktinde ortadan kaldırılmasından

³⁹⁶ Nicholas DIAKOPOULOS & Diğerleri, “Principles for Accountable Algorithms and a Social Impact Statement for Algorithms”, Fairness Accountability and Transparency in Machine Learning (FAT/ML), 18 Kasım 2016, <https://www.fatml.org/resources/principles-for-accountable-algorithms>.

³⁹⁷ Diakopoulos & Diğerleri, Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, <https://www.fatml.org/resources/principles-for-accountable-algorithms>.

sorumlu kişileri sürece dahil edilmesini ifade etmektedir. Açıklanabilirlik ilkesi uyarınca, veri sorumlusu yapay öğrenme algoritmaları ile alınan kararların ve ilgili kararın alınmasında rol oynayan verilerin teknik kavramlar içermeyen, anlaşılır, yalın bir dille ilgili kişiye anlatılabilmesini sağlamalıdır. Doğruluk ilkesine uyum sağlanmasıyla, algoritmaların işleyişi ve veri kaynaklarına ilişkin hata ve belirsizliklerin belirlenmesi, kayıt altına alınması ve ifade edilmesi surtiyle oluşması muhtemel ve oluşabilecek en kötü senaryonun etkileri önceden anlaşılabilir ve böylece bu etkilerin azaltılmasına yönelik işletilecek prosedürler belirlenebilecektir. Denetlenebilirlik, ilgili üçüncü kişilerin, ayrıntılı belgeler, kullanım koşulları (*terms of use*), teknik açıdan uygun uygulama programlama arayüzleri (*application programming interface-API*) de dahil olmak üzere, izleme, kontrol ve denetlemeye imkan tanıyan bilgilerin açıklanmasıyla otomatik karar sistemlerinin işleyişini incelemelerine ve sorgulamalarına izin verilmesini ifade eder. Son olarak, adil olma, profillemeye ve otomatik karar sistemleri ile bireyin cinsiyet, ırk, sosyo-ekonomik durumu gibi kişisel verilerini dikkate alarak belirli gruplar aleyhine ayrımcı veya adaletsiz çıkarım veya kararlara ulaşılmasının önlenmesini ifade eder³⁹⁸.

Algoritmik hesap verebilirliğin gerçekleştirilmesini sağlamak üzere geliştirilen fikirlerden biri de algoritmaların denetlenmesidir. Yapay zekanın insan ve toplum yararına gelişmesini sağlama misyonuyla Birleşik Krallık'ta kurulan bağımsız araştırma kurumu Ada Lovelace Enstitüsü ve DataKind UK tarafından hazırlanan raporda, “algoritmik denetim” (*algorithmic audit*), “belirli bir algoritmik sistemin işleyişini anlamak ve önceden belirlenmiş bazı normatif standartlara göre değerlendirmek amacıyla, sistemin çalışmasını denetlemeye yönelik bir dizi uygulama” olarak ifade edilmiştir³⁹⁹. Yine aynı raporda, algoritmik sistemlere ilişkin iki farklı denetim türüne yer verilmiştir. Bunlar, güvenilirliği

³⁹⁸ Diakopoulos & Diğerleri, Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, <https://www.fatml.org/resources/principles-for-accountable-algorithms>.

³⁹⁹ Ada Lovelace Institute & DataKind UK, Examining the Black Box: Tools for Assessing Algorithmic Systems, Nisan 2020, s.8-14, <https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/>.

değerlendirmek ve ulaşılan çıkarımların ayrımcılığa neden olabilecek önyargı unsurları içerip içermediğini tespit edebilmek amacıyla teknik unsurların (girdiler, çıktılar, eğitim verileri ve algoritmalar) incelendiği “önyargı denetimi” (*bias audit*) ve algoritmik karar sistemlerinin işleyişinin teknik unsurlarının yanında bazı normatif standartların (kalite güvencesi, hukuka uygunluk vb.) da değerlendirildiği “düzenleyici denetim” (*regulatory inspection*) olarak ifade edilmiştir⁴⁰⁰.

Algoritmik karar mekanizmaları özel sektör tarafından olduğu kadar kamu tarafından da yaygın şekilde kullanılmaktadır. Ada Lovelace Enstitüsü, AI Now Enstitüsü ve Açık Yönetim Ortaklığı⁴⁰¹ (*Open Government Partnership*) tarafından hazırlanan ve algoritmik hesap verebilirliğin kamu sektörü açısından değerlendirildiği raporda, algoritmaların denetiminin, hesap verebilirlik ilkesi ve algoritmik karar sistemlerinin olumsuz etkilerinin ortadan kaldırılmasına yönelik umut vaat eden bir araç olmasına rağmen, devlet politikalarıyla desteklenerek resmi olarak hayata geçirilmediği belirtilmiştir⁴⁰². Raporda belirtildiği üzere, kamuda algoritmik denetim, algoritmik hesap verebilirliğe ilişkin sistematik bir politika veya düzenleme kapsamında değil, belirli bir amaca özel (*ad-hoc*) uygulamalar ile gerçekleştirilmektedir. Üye devletlerin bazılarında algoritmik denetim, devletin hesap verme yükümlülüğü çerçevesinde, devlet faaliyetlerini denetlemekle görevli yüksek denetim kurumları tarafınca amaca özgü düzenleyici denetim faaliyeti olarak gerçekleştirilmektedir. Öte yandan, kamuda kullanılan algoritmik karar sistemlerinin denetlenmesine yönelik ihtiyaçlar farklılık göstermektedir⁴⁰³.

⁴⁰⁰ Ada Lovelace Institute & DataKind UK, s.8.

⁴⁰¹ Uluslararası alanda Open Government Partnership olarak bilinen Açık Yönetim Ortaklığı, kamusal kararların şeffaf ve hesap verebilir olmasının sağlanması, yolsuzlukla etkili bir şekilde mücadele edilmesi, vatandaşların ve sivil toplum örgütlerinin karar alma süreçlerine katılımının güçlendirilmesi, şeffaf ve etkin bir kamu yönetimi için yeni teknolojilerin teşvik edilmesi ve vatandaşların devlet karşısında daha güçlü bir konuma getirilmesi amacıyla 2011 yılında kurulmuş çok taraflı bir girişimdir. 2022 yılı itibarıyla 78 ülke üyedir. Girişime 2011’de katılmış olan Türkiye’nin üyeliği, ilk eylem planına ilişkin taahhütlerini yerine getiremediği gerekçesiyle 2016’da pasif hale getirilmiştir. Organizasyon deklarasyonu için bkz. <https://www.opengovpartnership.org/process/joining-ogp/open-government-declaration/>.

⁴⁰² Ada Lovelace Institute & AI Now Institute & Open Government Partnership, Algorithmic Accountability for the Public Sector, 2021, s.26, <https://www.opengovpartnership.org/wp-content/uploads/2021/08/algorithmic-accountability-public-sector.pdf>.

⁴⁰³ Ada Lovelace Institute & AI Now Institute & Open Government Partnership, Algorithmic Accountability for the Public Sector, s.26.

Algoritmik denetimlerde bazen algoritmik sistemlerin amacına uygun şekilde çalışıp çalışmadığının araştırılması hedeflenirken, bazen de ilgili sistemlerin kullanılmasına bağlı olarak ortaya çıkması muhtemel, kamu güveni üzerinde olumsuz etki doğurabilecek ayrımcılık riskleri de dahil olmak üzere toplumsal risklerin tespit edilmesine odaklanılmaktadır⁴⁰⁴.

Mayer-Schönberger ve Cukier, bireylerin hak ve özgürlükleri üzerinde önemli etki doğurabilecek kararlarda büyük veri analitiği yöntemlerinin kullanılması halinde, bazı tedbirlerin alınmasını tavsiye etmiştir. İlk olarak kişiyi etkileyen çıkarımların dayandığı veriler ve algoritma herkese açık ve herkesçe ulaşılabilir olmalıdır. İkincisi, ilgili algoritmanın bu şekilde hassas kararlarda kullanımının makul, akla yatkın ve kabul edilebilir olduğu uzman bir üçüncü tarafça onaylanmasıdır. Son olarak, ilgili kişinin kendisi hakkındaki bir çıkarımı çürütebileceği somut yollar belirlenmelidir⁴⁰⁵. Mayer-Schönberger ve Cukier ayrıca, profillemeye ve otomatik karar mekanizmalarının kara kutu özelliğinden doğabilecek risklerin minimize edilmesi açısından, “algoritmist” adı altında yeni aktörlerin süreçte oynayacakları rolün önemine değinmiş ve bu mesleğin nasıl icra edileceğine ilişkin tavsiyelerde bulunmuştur⁴⁰⁶. Buna göre, bilgisayar bilimleri, matematik ve istatistik alanlarında uzman algoritmistler, büyük veri analitiği ile gerçekleştirilen çıkarımları inceleyecek ve bu çıkarımların yanıltıcı olduğunu düşünen kişilere bunların düzeltilmesini talep etmeleri konusunda destek sağlayacaklardır⁴⁰⁷. Algoritmistler, veri kaynaklarını ve veri analitiği yöntemlerinin

⁴⁰⁴ Ada Lovelace Enstitüsü ilgili raporunda çeşitli örneklerle yer vermiştir. İsveç Ulusal Denetim Ofisi (*The National Audit Office of Sweden*), ilk kez, İsveç hükümeti tarafından kullanılan üç farklı otomatik karar sistemini denetlemiş ve otomatik karar sistemlerinin kullanımının etkili ve yeterli olup olmadığının yanı sıra karar alma faaliyetinde “hukuki kesinlik” ilkesinin tehlikeye atıp atmadığı da araştırılmıştır. Hollanda Sayıştay (The Netherlands Court of Audit), devlet kararları üzerinde önemli bir etkiye sahip olan tahmine dayalı algoritmaları vaka çalışmaları aracılığıyla denetleyerek, söz konusu denetimde uygulanan süreci belgelemiştir. Birleşik Krallık’ta bakanlık bünyesinde kurulmuş ve faaliyet gösteren Birleşik Krallık Veri Etiği ve Yenilik Merkezi (*The UK Centre for Data Ethics and Innovation*) ise, ülkedeki yerel yönetim otoriteleri tarafından kullanılan algoritmik karar sistemlerindeki tarafsızlığa ilişkin gerçekleştirdiği denetim kapsamında algoritmik sistemlerde önyargı ve ayrımcılık içeren çıktıları incelemiştir.

⁴⁰⁵ Mayer-Schönberger & Cukier, s.184.

⁴⁰⁶ Mayer-Schönberger & Cukier, s.186-189.

⁴⁰⁷ Mayer-Schönberger & Cukier, s.187.

seçimini ve çıkarımları değerlendirecek, bir uyumsuzluk olması halinde ise uyumsuzluğa konu kararı üreten algoritmalara, istatistiki metodlara ve kullanılan veri setlerine erişebileceklerdir. Bu bağlamda bir nevi “büyük veri analizlerinin ve tahminlerinin eleştirmeni” görevi görecekları belirtilmektedir. Öte yandan, algoritmistlerin birçok profesyonel meslekte olduğu gibi tarafsızlık ve güvenilirlik yemini etmeleri tavsiye edilmiştir. Algoritmistler, şirketlerin muhasebe kayıtlarının hem kendi bünyelerindeki muhasebeciler hem de bağımsız denetçiler tarafından incelenmesinde olduğu gibi, “iç algoritmist” ve “dış algoritmist” olarak iki şekilde görev alabileceklerdir⁴⁰⁸. Dış algoritmistler, mahkeme emri veya kanun yoluyla gelen inceleme taleplerinde, büyük veri tahminlerinin doğruluğunu ya da kabul edilebilirliğini değerlendirmekle görevli bağımsız aktörlerdir⁴⁰⁹. Dış algoritmistlerin tarafsız, güvenilir, alanında uzman ve profesyonel olmaları katı sorumluluk ve mesleki ahlak kurallarıyla zorunlu kılınmalıdır. Bu yeni profesyonellerin, algoritmalarla ilgili kompleks davalarda teknik konularda uzman bilirkişi olarak da görev almaları istenebilecektir. Ayrıca, profillemeye ve otomatik karar uygulamalarından zarar gördüklerini düşünen kişilerin, bu kararları anlamak ve bu kararlara karşı hukuki yollara başvurabilmek için avukatların yanı sıra algoritmistlere de başvurabilmeleri önerilmiştir. İç algoritmist ise, büyük veri analitiği faaliyetlerini izlemek üzere, şirket, kurum ve kuruluşların bünyesinde çalışır, sadece ilgili organizasyonun değil aynı zamanda bu organizasyonun analitik faaliyetlerinden olumsuz etkilenen kişilerin menfaatlerini de gözetir, analitik faaliyetlerini denetler, büyük veri analizlerini hayata geçirilmeden önce bütünlük ve doğruluk açısından inceler ve bu faaliyetlerden zarar gördüğüne inanan herkesin ilk iletişim noktası olarak görev yapar. Bu bağlamda iç algoritmistin görevlerinin, GVK Tüzüğü’nde düzenlenen “veri koruma görevlisi” nin görevleri ile benzer olduğu söylenebilecektir⁴¹⁰.

⁴⁰⁸ Mayer-Schönberger & Cukier, s.186-189.

⁴⁰⁹ Mayer-Schönberger & Cukier, s.188.

⁴¹⁰ Mayer-Schönberger & Cukier, s.188-189.

GVK Tüzüğü'nde algoritmaların denetimine ilişkin açık bir düzenleme bulunmamakla birlikte, veri koruma denetimi (*data protection audit*) bağlamında çeşitli atıflar yer almaktadır⁴¹¹. Öte yandan, Tüzük'teki farklı düzenlemelerin de algoritmaların denetimini dolaylı olarak öngördüğü değerlendirilmektedir. Bunlardan ilki, GVK Tüzüğü'nün 24. maddesinde düzenlenen veri koruma etki değerlendirmesidir. Veri koruma etki değerlendirmesi, veri sorumlularının, veri işleme faaliyetleri sebebiyle ortaya çıkması muhtemel “gerçek kişilerin hak ve özgürlüklerine yönelik değişen olasılık ve şiddetteki riskleri” değerlendirmelerini ve “veri işlemenin GVK Tüzüğü'ne uygun gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve organizasyonel tedbirleri uygulamalarını” gerektirir. Tüzüğün 40. maddesinde, üye devletlerin, denetim organlarının ve belirtilen diğer kurum ve kuruluşların, adil ve şeffaf veri işlemenin sağlanması ve veri sorumlusunun, işleme faaliyetinin Tüzük uyarınca gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve organizasyonel tedbirlerin belirlenmesine yönelik olarak davranış kuralları (*codes of conduct*) oluşturmaya teşvik edildiği düzenlenmiştir. Yine Tüzüğün 42. maddesinde, üye devletlerin, denetim organlarının ve belirtilen diğer kurum ve kuruluşların, kişisel veri işleme faaliyetlerinin Tüzük'le uyumluluğunun gösterilebilmesi amacıyla, şeffaf bir süreç vasıtasıyla sağlanması ve periyodik incelemeye tabi olması öngörülen, veri koruma sertifika mekanizmalarının ve veri koruma mühürlerinin ve işaretlerinin oluşturulmasının teşvik edildiği düzenlenmiştir⁴¹².

FAT-ML ilkelerinden biri olarak ifade edilen “açıklanabilirlik”, şeffaflık ilkesi ile doğrudan ilgilidir. Hesap verebilirlik ilkesi gereği, profillemeye ve otomatik karar mekanizmalarını kullanan veri sorumlusunun, tüm veri işleme süreçlerinin adil ve şeffaf bir şekilde gerçekleştirildiğini ilgili kişiye gösterebiliyor olması gerekir. Bunun için de profillemeye ve otomatik karar alma faaliyetlerinin şeffaf ve adil bir şekilde gerçekleştirildiğinin ilgili kişiye açıklanabilir olması gerekir. Diğer

⁴¹¹ Bkz. GVK Tüzüğü, m.28/3(h), m.39/1(b), m.47/2(j), m.58/1(b).

⁴¹² Bkz. GVK Tüzüğü, m.42.

bir ifadeyle, veri sorumlusu profillemeye ve otomatik karar alma faaliyetlerinden etkilenen ilgili kişilere bu kararları açıklayabilmelidir. Bu bağlamda profillemeye ve otomatik karar alma faaliyetlerinde şeffaflığın sağlanması, veri sorumlusunun hesap verme sorumluluğunun yerine getirilmesine hizmet etmektedir. Yapay öğrenme tabanlı profillemeye ve otomatik karar alma faaliyetlerinin şeffaf şekilde gerçekleştirildiğinin kabulü için, neden böyle bir karar verildiği, karar sürecinin nasıl gerçekleştiği, kişisel verilerin bir yapay öğrenme destekli profillemeye ve otomatik karar alma sisteminin eğitilmesi ve test edilmesi aşamalarında nasıl kullanıldığı hususlarında ilgili kişi açık bir şekilde bilgilendirilmelidir⁴¹³. Çalışmanın ilerleyen bölümlerinde şeffaflık ve algoritmik şeffaflık kavramları detaylı şekilde inceleneceğinden, buradaki açıklamalarımız sınırlı tutulmuştur.

2.2.2. Hesap Verebilirlik İlkesine Uyum Araçları

Çalışmanın bu bölümünde hesap verebilirlik ilkesine uyum araçları olan “veri koruma etki değerlendirmesi”, “veri koruma görevlisi” ve “tasarımdan itibaren veri koruma” ile “varsayılan ayarlarla veri koruma” ilkeleleri incelenecektir.

2.2.2.1. Veri Koruma Etki Değerlendirmesi

Veri koruma etki değerlendirmesi (*data protection impact assessment*), kişisel verilerin korunması hukukunda ilk kez GVK Tüzüğü ile düzenlenen hesap verebilirlik ilkesine uyum araçlarından biridir. Veri sorumlusu, özellikle yapay öğrenme, yapay zeka, derin öğrenme nesnelerin interneti uygulamaları ve benzeri yeni teknolojilerin kullanıldığı işleme faaliyetlerinde, işlemenin mahiyeti, kapsamı, bağlamı ve amaçları göz önüne alındığında, belirtilen yeni teknolojilerin ilgili kişilerin temel hak ve özgürlüklerine yüksek seviyede zarar verme riski taşıdığı gerekçesiyle, işleme faaliyeti gerçekleştirilmeden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisiyle ilgili bir değerlendirme

⁴¹³ Bkz. GVK Tüzüğü, m.13, m.14; GVK Tüzüğü, Giriş Bölümü, 60.Paragraf.

yapmakla yükümlü tutulmuştur⁴¹⁴. Veri koruma etki değerlendirmesi, esas olarak veri sorumlusunun yükümlülüğü olmakla birlikte, bir veri koruma görevlisinin atandığı hallerde, veri sorumlusu veri koruma görevlisinin de görüşünü almalı; bu görüşe veri koruma etki değerlendirmesinde yer verilmelidir⁴¹⁵. İşlemenin kısmen veya tamamen bir veri işleyen (*data processor*) tarafından gerçekleştirilmesi halinde, veri işleyen veri koruma etki değerlendirmesinde veri sorumlusuna yardımcı olmalı ve gerekli bilgileri sağlamalıdır⁴¹⁶. Veri koruma etki değerlendirmesi, veri işleme faaliyetinden önce gerçekleştirilmektedir⁴¹⁷. Böylece proaktif bir yaklaşım benimsenerek, mevzuata aykırılık oluşturabilecek potansiyel risklerin kaynağı, doğası, özelliği ve ciddiyeti değerlendirilerek risk ortaya çıkmadan önlenmesi amaçlanmaktadır⁴¹⁸. Bu bağlamda bir nevi “erken uyarı mekanizması” işlevine sahip bu araç ile belirli veri işleme faaliyetinin GVK Tüzüğü’ne uyumu denetlenmektedir⁴¹⁹.

Birleşik Krallık Bilgi Komisyoneri Ofisi, büyük veri analitiği teknikleri kullanılan profillemeye ve otomatik karar alma faaliyetlerinin veri koruma etki değerlendirmesi yapılmasını gerektirip gerektirmediğine ilişkin şu üç soruya verilecek cevapların belirleyici olacağını belirtmiştir⁴²⁰:

- i. Profillemeye faaliyeti kapsamında işlenen kişisel veriler, elde edilme amacından farklı bir amaç için veya farklı bir yolla kullanılmakta mıdır?
- ii. Söz konusu profillemeye faaliyeti kapsamında özel hayatın gizliliğine etki edebilecek yeni bir teknoloji kullanılmakta mıdır?

⁴¹⁴ Bkz. GVK Tüzüğü, m.35/1.

⁴¹⁵ Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purpose of Regulation 2016/679, 4 Nisan 2017, s.15, <https://ec.europa.eu/newsroom/article29/items/611236/en> (Kısaltılmışı “Data Protection Impact Assessment”).

⁴¹⁶ Article 29 Working Party, Data Protection Impact Assessment, s.15.

⁴¹⁷ Article 29 Working Party, Data Protection Impact Assessment, s.14.

⁴¹⁸ Voigt & Von Dem Bussche, s.129.

⁴¹⁹ Çekin, s.116.

⁴²⁰ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.101.

- iii. Profilleme faaliyeti neticesinde alınan kararlar ya da alınan aksiyonlar bireyleri ciddi ölçüde etkilemekte midir?

29. Madde Veri Çalışma Grubu, GVK Tüzüğü'nün ilgili düzenlemeleri göz önünde bulundurarak, yüksek risk ihtiva etmesi sebebiyle veri koruma etki değerlendirmesi yapılmasını gerektiren işleme faaliyetlerinin belirlenmesinde esas alınmak üzere dokuz kriter belirlemiştir. Buna göre, (i) değerlendirme veya puanlama, (ii) hukuki veya benzeri şekilde önemli etkiye sahip otomatik karar alma, (iii) sistematik izleme, (iv) hassas veya özel nitelikli kişisel verilerin işlenmesi, (v) büyük ölçekte veri işleme, (vi) veri kümelerini eşleştirme veya birleştirme, (vii) korunmasız kişilere ilişkin veriler, (viii) yeni teknolojik veya organizasyonel çözümler uygulama, (ix) ilgili kişilerin bir hakkı kullanmasını veya bir hizmet veya sözleşmeden yararlanmasını engelleme kriterlerinden birini içeren bir veri işleme faaliyeti, veri koruma etki değerlendirmesi yapılmasını gerektirecektir⁴²¹.

Tüzüğü'nün 35. maddesi uyarınca, “bireyin hak ve özgürlüklerine yönelik yüksek risk doğurması muhtemel” işleme faaliyetlerinde veri koruma etki değerlendirmesi yapılması zorunludur⁴²². Öte yandan, 29. Madde Veri Çalışma Grubu veri sorumlularının veri işleme faaliyetlerini veri koruma düzenlemelerine uygun şekilde gerçekleştirebilmeleri açısından faydalı olacağından bahisle, veri koruma etki değerlendirmesi yapılmasının zorunlu olup olmadığının belirgin olmadığı durumlarda da veri koruma etki değerlendirmesi yapılmasını tavsiye etmektedir⁴²³. Zira büyük veri analitiği, kişisel verilerin yeni, karmaşık ve bazen beklenmedik kullanımlarını içerebilir. Veri koruma etki değerlendirmesi yapılması, işleme başlamadan önce, işlemenin verileri kullanılan bireyleri ne ölçüde etkileyebileceğinin değerlendirilmesini ve olası etkileri hafifletme önlemlerinin belirlenmesini sağlayacaktır⁴²⁴.

⁴²¹ Article 29 Working Party, Data Protection Impact Assessment, s.9-11.

⁴²² Bkz. GVK Tüzüğü, m.35/1.

⁴²³ Article 29 Working Party, Data Protection Impact Assessment, s.8.

⁴²⁴ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.70.

GVK Tüzüğü'nde, kişinin kişisel özellikleri ile ilgili olarak, sistematik ve kapsamlı bir değerlendirmenin ardından profillemeye dayalı kararlar alınması için kişisel verilerin işlendiği hallerde veri koruma etki değerlendirmesinin yapılması gerektiği belirtilmektedir⁴²⁵. Özellikle ilgili kişinin “işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri veya ilgi alanları, güvenilirliği veya davranışı, konumu veya hareketleri” bakımından bir profilinin çıkarılması ve hakkında bir tahminde bulunulması halinde veri koruma etki değerlendirmesi yapılması zorunluluk teşkil etmektedir⁴²⁶. GVK Tüzüğü m.35/3(a) uyarınca “yüksek risk doğurması muhtemel” işleme faaliyetlerinden biri de bireylerin kişisel özelliklerinin, profillemeye de dahil olmak üzere otomatik işleme faaliyetleri ile sistematik ve kapsamlı olarak değerlendirilmesi ve bu değerlendirmeye göre bireyler üzerinde hukuki etki yaratan veya benzer derecede önemli şekilde etki doğuran kararlar alınmasıdır⁴²⁷. Dolayısıyla, GVK Tüzüğü m. 22'nin uygulama alanına giren profillemeye ve otomatik karar alma faaliyetleri, veri koruma etki değerlendirmesi yapılmasını gerektirmektedir.

Belirtmek gerekir ki, veri sorumlusu, sadece GVK Tüzüğü'nün 22. maddesinde düzenlenen ilgili kişi hakkında hukuki veya benzer derecede önemli etkiler doğuran profillemeye de dahil olmak üzere tamamen otomatik karar alma faaliyetleri için değil, m.22'nin uygulama alanına girmeyen (tamamen otomatik işlemeye dayalı olmayan) ancak ilgili kişi hakkında hukuki veya benzer derecede önemli etkiler doğuran profillemeye ve otomatik karar alma faaliyetleri için de veri koruma etki değerlendirmesi yapılmakla yükümlüdür⁴²⁸. Öte yandan ilgili kişi üzerinde herhangi bir etki doğurmayan veya etkisi oldukça sınırlı olan profillemeye ve otomatik karar alma faaliyetleri, bu kriteri karşılamamaktadır⁴²⁹. Bu bağlamda, örneğin, bir e-ticaret şirketinin, müşterilerinin şirketin online satış platformunu kullanırken oluşturdukları verileri analiz etmek suretiyle davranışsal veya

⁴²⁵ Bkz. GVK Tüzüğü, Giriş Bölümü, 91.Paragraf.

⁴²⁶ Bkz. GVK Tüzüğü, Giriş Bölümü, 71.Paragraf ve 91.Paragraf.

⁴²⁷ Bkz. GVK Tüzüğü m.35/3(a); Article 29 Working Party, Data Protection Impact Assessment, s.8.

⁴²⁸ Article 29 Working Party, Automated Decision Making and Profiling, s.29.

⁴²⁹ Article 29 Working Party, Data Protection Impact Assessment, s.9.

pazarlama profillerinin çıkarması durumunda veri koruma etki değerlendirmesi yapılması gerekmektedir. Benzer şekilde, kişinin profilinin çıkarılması amacıyla kamuya açık sosyal medya verilerinin toplanması veya ulusal düzeyde bir kredi puanı veya dolandırıcılık veri tabanı oluşturmak için gerçekleştirilecek işleme faaliyetlerinde veri koruma etki değerlendirmesi yapılması zorunlu kabul edilecektir⁴³⁰. Öte yandan, bir e-ticaret sitesinde bu sitede görüntülenen veya satın alınan şeyler baz alınarak gerçekleştirilen sınırlı bir profillemeye dayalı olarak kullanıcılara reklam gösterilmesi durumunda veri koruma etki değerlendirmesine gerek bulunmadığı sonucuna varılabilecektir⁴³¹.

Wachter'e göre, profillemeye ve otomatik karar alma uygulamalarının, bireyin bilgilerinin geleceğini belirleme hakkı (*informational self-determination*) ve kişisel verilerinin korunması açısından barındırdığı riskler göz önüne alındığında, profillemeye uygulamalarının ilgili kişiler açısından taşıdığı risklerin şeffaf bir şekilde paylaşılması, taraflar arasındaki güvenin artırılması açısından önemlidir⁴³². Veri koruma etki değerlendirmesinin hukuken zorunlu olmadığı veya gereksiz görüldüğü hallerde dahi, veri sorumlularının profillemeye ve otomatik karar uygulamalarını gözden geçirmeleri ve bunun gerçekleştirilmesinin arkasındaki nedenleri kamuya açıklamaları, veri sorumlularının kullanıcıların mahremiyetini sağlamak için hukuken zorunlu tutulmanın ötesinde bir çaba sarf ettiğini göstereceğinden, kullanıcıların profillemeye ve otomatik karar uygulamalarına olan güvenin artmasına yardımcı olabilecektir⁴³³.

GVK Tüzüğü'nün 35/7 maddesi ile giriş bölümünün 84. ve 90. paragraflarında, düzenleyici kuruma sunulacak veri koruma etki değerlendirmesi raporunun asgari içeriği düzenlenmiştir. Bu düzenlemeler veri koruma etki

⁴³⁰ Article 29 Working Party, Data Protection Impact Assessment, s.11.

⁴³¹ Article 29 Working Party, Data Protection Impact Assessment, s.11.

⁴³² Sandra WACHTER, Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR, Computer Law & Security Review 34 (2018) 436-449, s.447, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083554 (Kısaltılmışı "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR").

⁴³³ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.16.

değerlendirmesinde izlenecek metodolojiye ilişkin yön gösterir. Buna göre, profillemeye faaliyeti için gerçekleştirilecek bir veri koruma etki değerlendirmesi kapsamında düzenleyici kuruma sunulacak raporda, “ (i) uygulanabilir olan hallerde, veri sorumlusunun meşru menfaati de dahil olmak üzere, öngörülen işleme faaliyeti ve işleme amaçlarına ilişkin sistematik bir açıklamaya, (ii) profillemeye faaliyetinin işleme amacına göre gerekliliği ve ölçülülüğüne ilişkin değerlendirmeye, (iii) profillemeye faaliyetinin ilgili kişilerin temel hak ve hürriyetleri bağlamındaki risk değerlendirmesine; (iv) ilgili kişilerin ve diğer kişilerin hakları ve meşru menfaatleri göz önüne alınarak, kişisel verilerin korunması ve GVK Tüzüğü’ne uygun hareket edildiğini gösterilmesini sağlayacak güvenceler, güvenlik tedbirleri ve mekanizmalar da dâhil olmak üzere, risklerin ele alınmasına yönelik tedbirlere” yer verilmelidir⁴³⁴.

Birleşik Krallık Bilgi Komisyonu Ofisi’ne göre büyük veri analitiğinin doğasına ilişkin özellikleri, Tüzük ile öngörülen bu metodolojiyi takip etmeyi zorlaştırabilmektedir⁴³⁵. Örneğin, GVK Tüzüğü kapsamındaki veri koruma etki değerlendirmelerinin erken aşamalarından biri, işleme faaliyetlerinin ve işlemenin amaçlarının tanımlanmasıdır. Öte yandan, büyük veri analitiği sürecinde veri setleri arasında yeni ve öngörülme korelasyonlar keşfedildikçe veriden değer yaratılabilmektedir. Dolayısıyla hangi verilerin yararlı olacağı veya hangi verilerin nasıl kullanılacağı işlemenin ilk aşamasında net olmayabilir. Bu durum öngörülen işleme faaliyetindeki veri akışının ne şekilde olacağını ve kişisel verilerin hangi amaçlar için işleneceğinin tanımlanmasını zorlaştırmaktadır⁴³⁶.

29. Madde Çalışma Grubu, veri koruma etki analizi konulu rehberinde, veri koruma etki değerlendirmelerinin “en azından kısmen kamuya açık olması ve 'sürekli olarak gözden geçirilmesi ve düzenli olarak yeniden değerlendirilmesi” gerektiğini belirtmişse de çalışma grubunun görüş ve rehberlerinin hukuken bir

⁴³⁴ Bkz. GVK Tüzüğü, m.35/7; GVK Tüzüğü, Giriş Bölümü, 84. ve 90. Paragraflar.

⁴³⁵ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.71.

⁴³⁶ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.71.

bağlayıcılığı bulunmamaktadır⁴³⁷. GVK Tüzüğü'nde ise veri koruma etki değerlendirmelerinin kamuya açık olması veya gözden geçirilmesi konusunda bir düzenlememeye yer verilmemiştir. Bununla birlikte, veri sorumlularının, veri koruma etki değerlendirmelerinin sonuçlarını ve yöntemlerini yayınlamayı değerlendirmeleri ve veri koruma etki değerlendirmesi raporunu, düzenleyicilerin ve ulusal denetim kurumlarının, riskleri ortaya etkin bir şekilde ele alarak bunlara yanıt vermelerine yardımcı olmak için düzenli olarak gözden geçirmeleri tavsiye edilmektedir⁴³⁸.

29. Madde Çalışma Grubu'na göre profillemeye ve otomatik karar alma faaliyetleri kapsamında gerçekleştirilecek veri koruma etki değerlendirmesi, veri sorumlusunun profillemeye faaliyetinden önce muhtemel riskleri belirlemesini, bunları değerlendirmesini ve GVK Tüzüğü'ne uyum sağlanması için gerekli tedbirleri aldığını gösterebilmesini amaçlar⁴³⁹. Veri koruma etki değerlendirmesi, veri sorumlusunun işleme faaliyetindeki risklerin tespiti için alınması gereken tedbirleri belirlemesi açısından faydalı bir araçtır⁴⁴⁰. Çalışma Grubu, Tüzüğün 13/2(f), 14/2(g) ve 22/3 maddelerindeki gereklilikleri gözeterek, alınacak tedbirler kapsamında,

- İlgili kişinin otomatik karar alma faaliyetinin varlığı ve bu süreçte izlenen mantık hakkında bilgilendirilmesi,
- İşleme faaliyetinin ilgili kişi açısından önemini ve öngörülen sonuçlarının açıklanması,
- İlgili kişiye karara itiraz edebileceği imkanların sağlanması ve
- İlgili kişinin kendi bakış açısını açıklamasına imkan tanınması gerektiğini belirtmiştir⁴⁴¹.

⁴³⁷ Article 29 Working Party, Data Protection Impact Assessment, s.14.

⁴³⁸ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.15-16.

⁴³⁹ Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.29.

⁴⁴⁰ Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.29.

⁴⁴¹ Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.30.

2.2.2.2. Veri Koruma Görevlisi

Veri koruma görevlisi kavramına, ilk kez GVK Tüzüğü'nde yer verilmiştir. 95/46 Sayılı Direktif'te veri sorumlularının veri koruma görevlisi ataması şeklinde bir yükümlülüğe yer verilmemiş olmakla birlikte, seneler içerisinde birçok üye ülkede veri koruma görevlisi atanmasına yönelik bir uygulama benimsenmiştir⁴⁴². GVK Tüzüğü ile veri koruma görevlisinin atanması, konumu ve görevleri düzenlenmek suretiyle bu aktörün hukuki bir çerçeveye kavuşması ve kurumsallaşması sağlanmıştır⁴⁴³.

GVK Tüzüğü'nün veri koruma görevlisinin görevlerini düzenleyen 39. maddesi uyarınca veri koruma görevlisi, “(i) veri sorumlusu veya veri işleyen ile işleme faaliyetleri gerçekleştiren çalışanları, GVK Tüzüğü ve Avrupa Birliği'nin veya üye ülkelerin diğer veri koruma düzenlemelerine ilişkin bilgilendirmek ve onlara tavsiyede bulunmak; (ii) GVK Tüzüğü'ne, Avrupa Birliği'nin veya üye ülkelerin diğer veri koruma düzenlemeleri tahtındaki yükümlülüklerine ve işleme faaliyetlerine müdahil personelin sorumluluklarının belirlenmesi, bilinçlendirilmesi ve eğitimi ile ilgili denetimler de dahil, veri sorumlusu veya veri işleyenin kişisel verilerin korunmasına ilişkin politikalarına uyumluluğunu denetlemek; (iii) talep edilmesi halinde veri koruma etki değerlendirmesine ilişkin tavsiyede bulunmak ve değerlendirmenin yeterliliğini denetlemek; (iv) düzenleyici kurum ile işbirliği yapmak; (v) GVK Tüzüğü'nün 36. maddesinde atıfta bulunulan ön istişare de dahil olmak üzere işleme faaliyetine ilişkin konularda düzenleyici kuruma yönelik bir irtibat noktası olarak hareket etmek ve uygun olduğu hallerde, diğer her türlü konu ile ilgili danışmak” ile görevlidir⁴⁴⁴.

GVK Tüzüğü m.37 uyarınca, “(i) mahkemeler hariç olmak üzere veri işleme faaliyetinin kamu kurum ve kuruluşları tarafından gerçekleştirilmesi; (ii) veri

⁴⁴²Article 29 Working Party, Guidelines on Data Protection Officers (DPOs), 13 Aralık 2016, <https://ec.europa.eu/newsroom/article29/items/612048/en> (Kısaltılmışı “Data Protection Officers”).

⁴⁴³ Mehmet Bedii KAYA, Kişisel Verilerin Korunmasına Yeni Paradigma: Hesap Verebilirlik İlkesi, İstanbul Hukuk Mecmuası, 78(4), 1859-1897, s.1886, <https://dergipark.org.tr/en/download/article-file/1573623>.

⁴⁴⁴ Bkz. GVK Tüzüğü, m.39.

sorumlusu veya veri işleyen ana faaliyet konusunun, ilgili kişilerin büyük ölçekli olarak düzenli ve sistematik bir şekilde izlenmesini gerektiren veri işleme veya özel nitelikli kişisel veriler üzerinde işleme faaliyeti içermesi; (iii) veri sorumlusu veya veri işleyen ana faaliyet konusunun, büyük ölçekli olarak özel nitelikli kişisel veri veya ceza ya da suça ilişkin verilerin işlenmesini içermesi” halinde veri koruma görevlisi atanması zorunludur⁴⁴⁵. Öte yandan, GVK Tüzüğü’nde özellikle bir veri koruma görevlisinin atanmasını gerektirmeyen hallerde dahi, şirket ve kuruluşlar gerekli gördükleri takdirde gönüllü olarak veri koruma görevlisi atayabilirler⁴⁴⁶.

GVK Tüzüğü’nün 37/1 (b) maddesinde belirtilen “ilgili kişilerin büyük ölçekli olarak düzenli ve sistematik bir şekilde izlenmesi” kavramının açık bir tanımı yapılmamıştır. Ancak Tüzüğün giriş bölümünün 24. paragrafında, “ilgili kişilerin davranışlarının izlenmesi” kavramına atıf yapılmış; özellikle ilgili kişi hakkında bir karar almak veya kişisel tercihleri ve davranışlarını analiz etmek veya bunlar hakkında tahminde bulunmak amacıyla, çevrimiçi davranışsal reklamcılık amacıyla gerçekleştirilenler de dahil olmak üzere internet ortamındaki her türlü izleme ve profillemeye faaliyetlerinin, ilgili kişinin davranışlarının izlenmesi kapsamında olduğu açıkça ifade edilmiştir⁴⁴⁷.

29. Madde Çalışma Grubu’nun ilgili rehberinde, ilgili kişinin “düzenli” olarak izlenmesinin (i) belirli bir süre için belirli aralıklarla devam eden veya meydana gelen ve/veya (ii) belirli zamanlarda yinelenen veya tekrarlanan ve/veya (iii) sürekli veya periyodik olarak gerçekleşen izleme faaliyetlerini ifade ettiği belirtilmiştir. Öte yandan, ilgili kişinin “sistematik” şekilde izlenmesi, (i) belirli bir sistem çerçevesinde ve/veya (ii) önceden düzenlenmiş, organize edilmiş veya metodik şekilde ve/veya (iii) genel bir veri toplama planının parçası olarak ve/veya (iv) belirli bir stratejinin parçası olarak gerçekleştirilen izleme faaliyetlerini ifade etmektedir⁴⁴⁸. 29. Madde Çalışma Grubu, risk değerlendirmesi amacıyla kredi

⁴⁴⁵ Bkz. GVK Tüzüğü, m.37.

⁴⁴⁶ Article 29 Working Party, Data Protection Officers, s.4.

⁴⁴⁷ Bkz. GVK Tüzüğü, Giriş Bölümü, 24.Paragraf.

⁴⁴⁸ Article 29 Working Party, Data Protection Officers, s.8-9.

puanlaması, sigorta primlerinin belirlenmesi, dolandırıcılığın ve kara para aklamanın tespiti ve önlenmesi için gerçekleştirilen profil oluşturmayı, veriye dayalı pazarlama ve davranışsal reklamcılık faaliyetlerini, mobil uygulamalar tarafından gerçekleştirilen konum takibini, sadakat programlarını, giyilebilir cihazlar aracılığıyla sağlık verilerinin toplanmasını ilgili kişinin düzenli ve sistematik şekilde izlenmesine örnek olarak göstermiştir⁴⁴⁹. Bu bağlamda, veri sorumlusunun, ana faaliyet konusunun ilgili kişilerin büyük ölçekli olarak düzenli ve sistematik şekilde izlenmesini gerektiren profillemeye ve/veya otomatik karar alma faaliyetleri olması halinde, hesap verebilirlik ilkesinin bir gerekliliği olarak veri koruma görevlisi ataması gerekecektir⁴⁵⁰.

2.2.2.3. Tasarımdan İtibaren Veri Koruma ve Varsayılan Ayarlarla Veri Koruma İlkeleri

Çalışmanın ilgili bölümlerinde açıklandığı üzere, büyük veri analitiği ve yapay öğrenme algoritmalarının bireyin temel hak ve özgürlükleri ile mahremiyetine ilişkin barındırdığı riskler sebebiyle, büyük veri ile mahremiyet birbirleri ile çelişen kavramlardır. Bireyler (ilgili kişiler/kullanıcılar) ile hizmet sağlayıcılar arasındaki güvenin, bireyin kişisel verilerin korunması hakkının ve mahremiyetinin yeterince gözetilmemesi nedeniyle zedelenmesi, hizmet sağlayıcılara da zarar vermektedir. Örneğin, çevrimiçi davranışsal reklamcılık şirketleri ve ağları, veri işleme süreçlerine kullanıcı-dostu rıza mekanizmaları entegre edemediklerinden, kullanıcıların reklamları engelleyici yazılım (*ad-blocking software*) kullanma eğiliminde artış yaşanmıştır⁴⁵¹. Mahremiyet konusundaki sorun ve engeller, eğer doğru şekilde ele alınabilirse, taraflar arasında güven tesisi sağlanabilecek, böylece büyük veri ekosisteminde hem kullanıcılar hem de hizmet sağlayıcılar fayda sağlayabilecektir.

⁴⁴⁹ Article 29 Working Party, Data Protection Officers, s.9.

⁴⁵⁰ Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.30.

⁴⁵¹ ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In the Era of Big Data Analytics, Aralık 2015, s.19, <https://www.enisa.europa.eu/publications/big-data-protection> (Kısaltılmışı “Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In the Era of Big Data Analytics”).

Tasarımdan itibaren veri koruma (*data protection by design*)⁴⁵² ve varsayılan ayarlarla veri koruma (*data protection by default*) ilkelerinin ilk kez GVK Tüzüğü'nde hukuki çerçeveye kavuşturulması kişisel verilerin korunması açısından önemli bir mihenk taşı niteliğindedir. Tasarımdan itibaren veri koruma veya diğer adıyla tasarımdan itibaren mahremiyet (*privacy by design*), kuruluş ve şirketlerin kişisel verilerin korunması için gerekli idari ve teknik tedbirleri; teknolojinin tasarımına, iş politikalarına ve fiziki altyapılarına entegre etmelerini ifade eder⁴⁵³. Bu da bir ürün veya hizmetin tasarım aşamasından itibaren kişisel verilerin korunması ve mahremiyetin gözetilmesini gerektirir. Varsayılan ayarlarla veri koruma ilkesi ise, veri sorumlularının Tüzük'te düzenlenen bu yükümlülüklerini yerine getirmeleri halinde kullanıcıların, bir ürün veya hizmet aldıklarında kişisel verilerinin korunması için başka herhangi bir ayar yapmaya ihtiyaç duymadıkları bir veri koruma düzeni sağlamayı amaçlamaktadır⁴⁵⁴. Öte

⁴⁵² Tasarımla veri koruma (*data protection by design*) yerine sıklıkla tasarımdan itibaren/tasarımla gizlilik (*privacy by design*) kavramı kullanılmaktadır. “*Privacy by design*” kavramının Türkçe karşılığı olarak mahremiyet tabanlı tasarım, tasarım ile gizlilik, tasarımdan itibaren gizlilik gibi farklı ifadelerin kullanıldığı görülmektedir. 2009 yılında Kanada'nın Ontario eyaletinde Bilgi ve Gizlilik Komisyoneri olan Dr. Ann Cavoukian, tasarımdan itibaren gizliliğin korunmasına ilişkin 7 ilke yayınlamıştır. Bunlar genel olarak, proaktif ve önleyici olma, gizliliğin standart ayar olması, gizliliğin tasarıma entegre edilmesi, pozitif toplam yaklaşımının benimsenmesi, uçtan uca güvenlik, şeffaflık ve görünebilirlik, kullanıcıya saygı olarak sıralanabilir. Detaylı bilgi için bkz. Ann CAVOUKIAN, *Privacy by Design: The 7 Foundational Principles*, Ağustos 2009, <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Bu ilkelerin pratikte uygulamasının nasıl gerçekleşeceği belirsiz olmakla birlikte, tasarımla veri koruma ilkesinin GVK Tüzüğü ile hüküm altına alınması ile beraber bu ilkelerin pratiğe nasıl döküleceğine ilişkin farklı kurumlarca çeşitli dokümanlar yayınlamaktadır. Tasarımla veri koruma ilkesinin pratikteki uygulamasına ilişkin olarak Norveç Veri Koruma Gözetmeni'nin tasarımdan itibaren ve varsayılan ayarlarla veri koruma yoluyla yazılım geliştirme rehberi ve Avrupa Veri Koruma Denetçisi'nin ön görüş niteliğindeki raporu önemli rehberlerdir. Datatilsynet, *Software Development with Data Protection by Design and by Default*, <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true>; European Data Protection Supervisor, *Opinion 5/2018 Preliminary Opinion on Privacy by Design*, 31 Mayıs 2018, https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en.

⁴⁵³ Article 29 Working Party, *Opinion 3/2012 on Developments in Biometric Technologies*, 27 Nisan 2012, s.28, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

⁴⁵⁴ European Digital Rights (EDRi), *An Introduction to Data Protection, The EDRi Papers*, Issue 06, s.13, http://www.edri.org/files/paper06_datap.pdf. Bu çerçevede, örneğin sosyal medya platformları, kullanıcılarının üyelik kayıtlarını tamamladıkları andan itibaren profil ayarlarını en gizlilik-dostu (*privacy-friendly*) şekilde ayarlamak suretiyle, profillere erişimi kısıtlanmasını ve sınırsız sayıda kullanıcıya açık olmamasını sağlamakla yükümlüdürler. Dolayısıyla, bir sosyal medya sitesinde hesap oluşturan bir kişinin hesabının oluşturulduğu andan itibaren, sosyal medya sitesinin halihazırdaki ayarları sebebiyle kişinin yaşı ve yaşadığı şehir gibi bilgilerinin herkese açık şekilde

yandan, her ne kadar 29. Madde Veri Çalışma Grubu'nun görüşüne⁴⁵⁵ göre GVK Tüzüğü'nde düzenlenen bu ilkelerin ne anlatmak istediği açık olsa da, ilgili sektörlerde bu ilkelerin pratikte nasıl hayata geçirileceği ile ilgili belirsizlikler ve soru işaretleri bulunduğu belirtilmektedir⁴⁵⁶.

Tasarımdan itibaren veri koruma ve varsayılan ayarlarla veri koruma ilkeleriyle veri sorumlusu, gelişmiş teknoloji, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, içeriği ve amaçları ve gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği riskleri dikkate alarak, GVK Tüzüğü'nün gerekliliklerini yerine getirmek ve ilgili kişilerin haklarını korumak amacıyla, gerek işleme faaliyetinde kullanılacak araç ve yöntemler belirlenirken gerekse işleme faaliyeti sırasında, veri minimizasyonu (*data minimisation*) ve amaçla sınırlılık (*purpose limitation*) gibi kişisel verilerin işlenmesine hakim olan ilkelerin etkili bir şekilde hayata geçirilmesi için tasarlanmış uygun teknik ve idari tedbirleri etkili bir şekilde uygulamak ve gerekli önlemleri almakla yükümlü tutulmaktadır⁴⁵⁷. Veri minimizasyonu ve amaçla sınırlılık ilkelerinin özümsemesi suretiyle tasarlanacak teknik çözümler, iş yapma süreçleri, işletim sistemleri ve iş modelleri; “veri koruma dostu ürün ve hizmetler” in geliştirilmesini sağlayacaktır⁴⁵⁸. Veri koruma dostu ürün ve hizmetler için “Mahremiyeti Artıran Teknolojiler” (*Privacy Enhancing Technologies*) ifadesi de kullanılmaktadır. Bu bağlamda, tasarımdan itibaren veri

profilinde gösteriliyor olması, varsayılan ayarlarla veri koruma ilkesine aykırılık teşkil edecektir. Ancak hesap sahibinin, kendi rızasıyla gizlilik ayarlarını değiştirmesi halinde artık varsayılan ayarlarla veri koruma ilkesinin ihlalden bahsedilemez. European Commission, What Does Data Protection ‘By Design’ and ‘By Default’ Mean?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en; EDRI, s. 13; Taştan, s. 21.

⁴⁵⁵ Article 29 Working Party, Opinion 08/2012 Providing Further Input on the Data Protection Reform Discussions, 5 Aralık 2012, s.28, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.

⁴⁵⁶ Nilgün BAŞALP, Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 21, Sayı 1, 77-106, 2015, s.92; ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics, s. 21.

⁴⁵⁷ Bkz. GVK Tüzüğü, m. 25, Giriş Bölümü, 78. Paragraf.

⁴⁵⁸ İpek Çimen BULUT, Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları, Anadolu Üniversitesi Sosyal Bilimler Dergisi, Cilt 20, Sayı 2 (127-142), <https://dergipark.org.tr/tr/download/article-file/1169283>, s. 132.

koruma, mahremiyet ve veri koruma ilkelerini hayata geçiren mahremiyeti artıran teknolojilerin geliştirilmesine ve kullanılmasına zemin hazırlayan, çeşitli teknolojik ve organizasyonel bileşenleri içeren bir süreci ifade etmektedir⁴⁵⁹.

Tasarımdan itibaren veri korumanın sağlanması için kullanılabilecek mahremiyeti artıran teknolojiler arasında, kimlik doğrulama, güvenli özel iletişim, anonimleştirme ve takma adlandırma, veri tabanlarında gizliliğin sağlanması, gizliliği koruyan veri madenciliği, verilerin saklanması gizliliğin sağlanması, analitik faaliyetlerinde gizliliğin korunması ve şeffaflığın artırılması, ilgili kişinin veri işleme sürecine müdahale edebilmesine imkan tanıyan teknolojiler yer almaktadır⁴⁶⁰. Wachter'e göre, GVK Tüzüğü'nün tasarımdan itibaren ve varsayılan ayarlarla veri koruma, anonimleştirme, takma adlandırma, şifreleme ve diğer mahremiyeti artıran teknolojilerin kullanılmasını hüküm altına alan ilgili düzenlemeleri, bireyin kimliğinin ortaya çıkarılmasını sağlayan teknolojilere karşı kullanıcı güveninin ve toplumsal kabulün artırılması ve aynı zamanda kullanıcı mahremiyetinin iyileştirilmesine yardımcı olmalıdır⁴⁶¹. Öte yandan, mahremiyeti artıran teknolojiler çoğu zaman kusurludur ve kişinin kimliğinin tespit edilmesini engellemek neredeyse imkansızdır⁴⁶².

Büyük veri analitiği uygulamalarının bireyin temel ve hak özgürlükleri ile kişisel verilerin korunması açısından barındırdığı riskler göz önüne alındığında, profillemeye ve otomatik karar alma uygulamalarında tasarımdan itibaren veri koruma ilkesinin uygulanması, belirli teknik ve idari tedbirlerin alınması suretiyle, kişisel verilerin korunmasını sağlamaya yönelik proaktif bir yaklaşım benimsenmesini sağlayacaktır. Kişisel verilerin korunmasına hakim olan ilkelerin hayata geçirilmesini sağlayacak mekanizmaların algoritmaların geliştirilmesi aşamasından itibaren sürece entegre edilmesi, ilgili kişiler ile veri sorumluları

⁴⁵⁹ ENISA, Privacy and Data Protection by Design-From Policy to Engineering, Aralık 2014, s. 3, <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> (Kısaltılmışı "Privacy and Data Protection by Design-From Policy to Engineering").

⁴⁶⁰ ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics, s. 22.

⁴⁶¹ Wachter, The GDPR and the Internet of Things: A Three Step Transparency Model, s. 23.

⁴⁶² Wachter, The GDPR and the Internet of Things: A Three Step Transparency Model, s. 23.

arasında mahremiyet ve kişisel verilerin korunmasına ilişkin yaşanabilecek çatışmaların gerçekleşmeden önlenmesi ve güven ortamının sağlanabilmesi açısından önemlidir⁴⁶³.

Profilleme ve otomatik karar uygulamalarında tasarımdan itibaren gizliliğin korunması ilkesinin uygulanması, genel olarak, veri koruma ilkelerinin etkin bir şekilde uygulanmasını ve bireysel hakların korunmasını sağlayacak uygun teknik ve idari tedbirlerin ve mahremiyeti artıran teknolojilerin, büyük veri analitiği süreçlerine entegre edilerek uygulanmasını, bireylerin kişisel verilerinin işlendiği profilleme ve otomatik karar faaliyetleri karşısında sahip oldukları hakları etkin bir şekilde kullanabilmeleri için yeterli kontrol imkanı ve seçeneğe sahip olmasını, veri sorumlularının profilleme ve otomatik karar faaliyetinin amacının gerektirdiği kadar ve bu amaçla sınırlı olarak veri işlemesini, büyük veri analitiği süreçlerinde şeffaflığın etkin bir şekilde sağlanmasını, ilgili kişilerin bu hususta izni bulunmadıkça ilave veri işlenmemesini, ilgili kişilere işleme sürecine müdahale imkanı tanınmasını gerektirir⁴⁶⁴.

Profilleme ve otomatik karar alma uygulamalarında anonimleştirme, takma adlandırma (*pseudonymization*) ve fonksiyonel ayırma (*functional separation*) yöntemleri, kişisel verilerin korunması ve veri güvenliğini sağlanması amacıyla, tasarımdan itibaren sürece entegre edilmelidir. Anonimleştirmenin büyük veri analitiğinin ve gelişmiş bilgisayar teknolojilerinin doğasına bağlı olarak tam anlamıyla mümkün olmadığı hallerde, en azından takma-adlandırma, şifreleme ve kimliğin doğrudan belirlenmesini sağlayan faktörlerden arındırma kısmi anonimleştirme yöntemleri uygulanmalı ve ilave tedbirler alınmalıdır⁴⁶⁵. Özellikle, fonksiyonel ayırma yöntemi, çalışmanın konusunu teşkil eden otomatik karar alma faaliyetleri açısından önemlidir. Yenilikçi mühendislik çözümlerinin teşvik edildiği fonksiyonel ayırma yönteminin amacı, istatistiksel veya diğer araştırma amaçları

⁴⁶³ EDRI, s.12; ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics, s. 21-23.

⁴⁶⁴ ICO, Guide to the General Data Protection Regulation, s.187-192.

⁴⁶⁵ Article 29 Working Party, Purpose Limitation, s.31.

için işlenen kişisel verilerin ilgili kişiler hakkında bir önlem veya karar almada değerlendirmeye esas teşkil etmemesini sağlamaktır⁴⁶⁶. Veri sorumlusunun büyük veri analitiği yöntemleriyle elde ettiği içgörülerini veya çıkarımları ilgili kişilere doğrudan uygulamak yerine yalnızca işlemeye konu verilerdeki eğilimleri ve korelasyonları tespit etmek istemesi halinde, fonksiyonel ayırma yöntemi potansiyel olarak işleme faaliyetinin bireylerin hakları üzerindeki olumsuz etkisini azaltmaya yardımcı olmakla birlikte veri sorumlusunun veriyi elde edilme amacından farklı bir amaç için kullanabilmesine imkan tanıdığı belirtilmektedir⁴⁶⁷. Öte yandan, ulusal istatistik ofisleri ve araştırma kurumları dışında fonksiyonel ayırma yönteminin etkin bir şekilde uygulandığına nadiren rastlanmaktadır⁴⁶⁸.

Önemle belirtmek gerekir ki, yapay öğrenme teknikleri ile gerçekleştirilen profillemeye ve otomatik karar uygulamaları, tasarımdan itibaren veri koruma anlayışının veri işleme sürecine etkin şekilde tesir edebilmesi belirtilen tedbirlerin haricinde birçok farklı idari ve teknik tedbirlerin alınmasını gerektirir. Verilerin kötüye kullanılmasının önlenmesi amacıyla erişim kontrolleri, şifreleme ve denetim kayıtları gibi güvenlik tedbirleri; sadece gerekli olan değerlendirme ve işlemler kapsamında gerekli olduğu ölçüde verilerin işlenmesini sağlamak üzere veri sadeleştirilmesine ilişkin önlemler; kişisel verilerin genel eğilimleri ve korelasyonlar tespit etmek amacıyla işlenen verilerden ayrı tutmak için amaçla sınırlılık ilkesi ve veri ayırımına yönelik tedbirler bunlardan bazılarıdır⁴⁶⁹.

Tasarımdan itibaren veri koruma yaklaşımının tasarım odaklı ve teknik içeriğe sahip ilkelere dönüşmesi göz önüne alındığında, geliştirilecek olan uygulama, ürün ya da hizmetin mimarisinden ve tasarımından sorumlu mühendisler, yazılımcılar ve ilgili diğer iş birimleri tarafından bu yaklaşımın içselleştirilmesi önem teşkil etmektedir. Bu birimlerin proje yönetim metodolojilerinde bu ilkeyi bir öz denetim unsuru olarak dikkate almaları, hukukçuların ise bu birim ve/veya

⁴⁶⁶ Article 29 Working Party, Purpose Limitation, s.30.

⁴⁶⁷ European Data Protection Supervisor, Opinion 7/2015, Meeting the Challenges, s.15.

⁴⁶⁸ European Data Protection Supervisor, Opinion 7/2015, Meeting the Challenges, s.21, Dipnot 42.

⁴⁶⁹ ICO, Big Data, Artificial Intelligence, Machine Learning And Data Protection, s.73.

kişilere muğlak noktalarda yol gösterici veya onaylayıcı rolünde olmaları önerilmektedir⁴⁷⁰.

Wachter, tasarımdan itibaren veri koruma ve varsayılan ayarlarla veri koruma ilkelerinin, açık rızanın kriterlerinin karşılanması açısından da faydalı bir yaklaşım olacağını belirtmiştir. Zira kullanıcı, özel hayatının gizliliğinin varsayılan ayarlarla korunacağından emin olduğunda ve ilgili hizmeti kullandığında bunun sonuçlarının öngörülebilir hale geldiğinde, bilinçli bir seçim yapabilecektir. Bu bağlamda, veri sorumlularının IoT hizmetlerini, varsayılan ayarları gereği, mümkün olduğunca az veri gerektirerek çalışacak şekilde tasarlamayı değerlendirmeleri tavsiye edilmektedir⁴⁷¹.

Veri sorumluları, otomatik karar sürecinde kişisel verilerin işlenmesine bağlı olarak oluşabilecek, hataları, yanlışlıkları veya ayrımcılığı önlemek üzere uygun prosedür ve tedbirler geliştirmelidir. Zira veri sorumlusunca toplanan veya ilgili kişi tarafından paylaşılan verilerdeki ya da otomatik kararalma sürecindeki hatalar veya önyargılar, yanlış sınıflandırmalara neden olabilmekte, doğruluğu kesin olmayan çıkarımlara dayalı değerlendirmeler bireyler üzerinde olumsuz etkiler doğurabilmektedir⁴⁷². Veri sorumluları, karar sürecinde herhangi bir önyargı olup olmadığını kontrol etmek adına, işledikleri veri setleri üzerinde rutin değerlendirmeler yapmalı ve tespit edilen korelasyonlara ilgili kişi hakkındaki karara esas teşkil etmesi bağlamında aşırı güvenilmesi de dahil olmak üzere önyargı içerebilecek tüm unsurları tespit edilmesini sağlayacak yöntemleri geliştirmelidir⁴⁷³. Bu tedbirler, sadece tasarım aşamasında değil, profillemeye ve otomatik karar faaliyetindeki tüm veri işleme süreci boyunca, devamlı ve döngüsel

⁴⁷⁰ Yaşar K. CANPOLAT, Privacy by Design- Şirketlerin rekabet avantajı yaratması için yeni formül, 10 Haziran 2019, <https://medium.com/canpolat-legal/privacy-by-design-%C5%9Firketlerin-rekabet-avantaj%C4%B1-yaratmas%C4%B1-i%C3%A7in-yeni-form%C3%BCI-99cfe0133aa>.

⁴⁷¹ Wachter, Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR, s.466.

⁴⁷² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.27.

⁴⁷³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

olarak uygulanmalıdır⁴⁷⁴. Bu tedbirlerin uygulanmasından edinilen sonuçlar, yine, sistemin tasarımında kullanılmalıdır⁴⁷⁵.

Hildebrandt, algoritmaları denetleyen sistemlerin geliştirilmesi ve kullanılması ile profillemeye de dahil olmak üzere otomatik karar alma faaliyetinin doğruluğu ve uygunluğunun rutin olarak gözden geçirilmesinin yararlı olacağını belirtilmektedir⁴⁷⁶. Bu tür tedbirler, tasarımdan itibaren veri koruma ilkesinin, kişisel verilerin işlendiği sistemlerin tasarımına rehberlik eden, veri koruma hukukunun yersiz ihlallerini ortadan kaldıran ve teknik altyapı bağlamında pratik ve etkili bir koruma sağlayan operasyonel bir gerekliliğe nasıl dönüştürülebileceğinin örneklerini teşkil etmektedir⁴⁷⁷.

Sosyal medya kullanıcıları, bu hizmetlerden yararlanabilmek için, hizmet sağlayıcıların kullanıcıların kişisel verilerinin korunmasını gözetip gözetmediklerini göz ardı ederek, çoğunlukla gereğinden fazla kişisel veri paylaşma eğilimindedirler⁴⁷⁸. Büyük veri analitiği yöntemlerinin karmaşık yapısı ve kendine özgü özellikleri göz önüne alındığında, kişisel veriler bilgilendirme ve rıza alma süreçlerinden sonra toplanıp analiz edilse dahi, kullanıcılar hizmet sağlayıcıların kendileri hakkında hangi verileri topladığı ve toplanan verilerden kendileri hakkında hangi çıkarımlarda bulunduğu konusunda çoğunlukla yeterli bir farkındalığa sahip değildir. Mahremiyeti artıran teknolojiler, kullanıcılara kişisel verilerinin korunmasını sağlamak adına önemli olanaklar tanısa da özellikle çevrimiçi davranışsal reklamcılık uygulamaları kapsamında gerçekleştirilen

⁴⁷⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

⁴⁷⁵ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

⁴⁷⁶ Mireille HILDEBRANDT, 10. 'Legal by Design' or 'Legal Protection by Design?', Law for Computer Scientists, <https://lawforcomputerscientists.pubpub.org/pub/gfzd6k0g/release/12>.

⁴⁷⁷ Hildebrandt, 10. 'Legal by Design' or 'Legal Protection by Design?', <https://lawforcomputerscientists.pubpub.org/pub/gfzd6k0g/release/12>.

⁴⁷⁸ Alessandro ACQUISTI & Ralph GROSS, Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook, Privacy Enhancing Technology Workshop (PET), 2006, s.1-2, <https://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf>.

profilleme faaliyetleri karşısında kullanıcılara yeterli şeffaflık sağlamadığı yönünde tereddütler oluşmuştur⁴⁷⁹.

Tasarımdan itibaren veri koruma ilkesinin şeffaflığı sağlamada yetersiz kaldığı yönündeki iddialar sonucunda, “Tasarımdan İtibaren Şeffaflık” (*Transparency by Design*) yaklaşımı geliştirilmiştir. Kullanıcılar ile hizmet sağlayanlar arasında şeffaflığı artırıp bilgi asimetrisini azaltmak suretiyle, kullanıcılara daha güçlü bir koruma sağlamak için çeşitli araçlar önerilmiş ve bunlar “Şeffaflığı Artıran Teknolojiler” (*Transparency Enhancing Technologies*) olarak adlandırılmıştır⁴⁸⁰. Şeffaflığı artıran teknolojiler, kullanıcılara, hizmet sağlayıcıların kişisel verileri toplama, analiz etme ve kullanımına ilişkin bilgiler sağlayarak taraflar arasındaki bilgi asimetrisini azaltmayı amaçlar⁴⁸¹. Diğer bir ifadeyle, şeffaflığı artıran teknolojiler, veri minimizasyonu ve amaçla sınırlılığın sağlanmasından ziyade, kullanıcıların veri sorumlusunun kişisel verileri hangi amaçla topladığı ve gerçekte hangi amaçla işlediği konusunda fikir edinmesini hedefler⁴⁸². Bu bağlamda, şeffaflığı artıran teknolojilerin, mahremiyeti artıran teknolojileri tamamlayıcı bir role sahip olduğu ifade edilmektedir⁴⁸³.

⁴⁷⁹ Christian ZIMMERMANN, A Categorization of Transparency-Enhancing Technologies, 17 Temmuz 2015, s.1, <https://arxiv.org/abs/1507.04914v2>.

⁴⁸⁰ ENISA, Privacy and Data Protection by Design-From Policy to Engineering, s. 44-45; Emre BAYRAMLIOĞLU, Transparency of Automated Decisions in the GDPR, An Attempt for Systemisation, s. 22, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097653.

⁴⁸¹ Zimmermann, s.1.

⁴⁸² Zimmermann, s.1.

⁴⁸³ Zimmermann, s.1.

2.2.3. Şeffaflık İlkesi

GVK Tüzüğü'nde, KVK Kanunu'ndan farklı olarak şeffaflık ilkesi açık bir şekilde hüküm altına alınmıştır⁴⁸⁴. KVK Kanunu'nda şeffaflık ilkesi açık bir şekilde düzenlenmemiş olmakla birlikte, şeffaflık ilkesine atıf yapılan bazı kurul kararları bulunmaktadır⁴⁸⁵. Şeffaflık ilkesi GVK Tüzüğü'nde temel ve kapsayıcı bir ilke olarak düzenlenmiştir. Bu ilke kişisel verilerin işlenmesi faaliyetlerinde ilgili kişiye tanınan haklar, tasarımla veri koruma ve varsayılan ayarlarla veri koruma yaklaşımları ile başta hesap verilebilirlik ilkesi olmak üzere kişisel verilerin işlenmesine hakim olan diğer ilkelerle yakından ilişkilidir. Şeffaflık en genel anlamda, kişisel verilerinin ne için ve nasıl işlendiğine ilişkin olarak, kişisel verileri işlenen kişilere karşı açık ve dürüst olunmasını ifade eder⁴⁸⁶. Kişisel verilerin hukuka uygun ve adil bir şekilde işlendiğinin kabul edilebilmesi için, veri sorumluları, veri işleme faaliyetlerini şeffaflık ilkesinin gerekliliklerine uygun şekilde gerçekleştirmekle yükümlüdür. Bu ilke gereği, ilgili kişilerin kendileri üzerinde sonuç doğuran veri işleme süreçleri hakkında bilgilendirilmeleri suretiyle bu sürecin nasıl işlediğini anlamaları ve gerektiği durumlarda bu sürece ilişkin itirazlarını ileri sürebilmeleri sağlanmalıdır⁴⁸⁷.

⁴⁸⁴ Bkz. GVK Tüzüğü, m.5/1(a)

⁴⁸⁵ Kurul, petrol piyasasında faaliyet gösteren veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri, meşru menfaat çerçevesinde kullanma talebiyle Kişisel Verileri Koruma Kurumu'na yapmış olduğu başvuruya ilişkin gerçekleştirdiği incelemede, KVK Kanunu'nun 5/2(f) maddesi kapsamında meşru menfaatinin bulunup bulunmadığı değerlendirilmesi yapılırken KVK Kanunu'nda açıkça düzenlenmemiş olan şeffaflık ve hesap verilebilirlik ilkelerinin esas alınması gerektiğine karar vermiştir. Bkz. Kişisel Verilerin Korunması Kurulu'nun 25.03. 2019 tarihli ve 2019/78 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/5434/2019-78>. Kurul başka bir kararında ise veri sorumlusunun sunduğu sadakat programı kapsamında şifre değişikliği kimlik görüntüsü talep edilen ilgili kişinin yaptığı başvuruda, veri sorumlusunun kimlik görüntüsünü kaydetmesine rağmen ilgili kişiye aksi şekilde bilgi verilmesinden dolayı şeffaf olmadığını, dolayısıyla da dürüstlük kuralına aykırı veri işlediğini değerlendirmiştir. Bkz. Kişisel Verilerin Korunması Kurulu'nun 01.10.2019 tarihli ve 209/294 sayılı kararı, <https://www.kvkk.gov.tr/Icerik/6556/2019-294>.

⁴⁸⁶ Information Commissioner's Office & The Alan Turing Institute, Explaining Decisions Made With AI, 2020, s.13. https://iapp.org/media/pdf/resource_center/ico_explaining_decisions_with_ai.pdf.

⁴⁸⁷ Article 29 Working Party, Guidelines on Transparency Under Regulation 2016/679, 17/EN WP260 rev.01, s.4, <https://ec.europa.eu/newsroom/article29/items/622227/en> (Kısaltılmışı "Transparency").

2.2.3.1. Algoritmik Şeffaflık

Avrupa Parlamentosu Bilim ve Teknolojinin Geleceği Heyeti, profillemeye ve otomatik karar sistemlerinin barındırdığı risklerin azaltılması için bu sistemlerin sahip olması gereken temel özellikleri, (i) tüm algoritmik sistemler açısından gerekli özellikler ve (ii) algoritmik karar sistemlerine özgü özellikler olmak üzere iki grup altında incelemiştir⁴⁸⁸. Tüm algoritmik sistemler için gerekli temel özellikler, güvenlik (*safety*) ve mahremiyet (*privacy*) iken; algoritmik karar sistemlerine özgü özellikler ise, adil olma (*fairness*), önyargısız olma (*absence of bias*), ayrımcı olmama (*non-discrimination*) ve anlaşılabilirlik (*understandability*) olarak sayılmıştır. Anlaşılabilirlik, algoritmik karar sistemlerindeki girdi ile çıktı arasındaki bağlantıya ilişkin anlaşılabilir bilgi sunulabilmesini ifade etmektedir. Algoritmik kararların anlaşılabilir olabilmesinin iki boyutu bulunur. Bunlar, şeffaflık (*transparency*) ve açıklanabilir olma (*explainability*) özellikleridir. Literatürde, şeffaflık ilkesini algoritmik karar sistemleri bağlamında betimlemek üzere kullanılan “algoritmik şeffaflık” (*algorithmic transparency*), algoritmik karar sistemlerinde bu özelliklerin uygulanabilirliğini amaç edinen kapsayıcı bir ilke niteliğindedir.

GVK Tüzüğü uyarınca veri sorumlusu, profillemeye ve otomatik karar faaliyetlerinde sürecin tüm aşamalarında kişisel verilerin işlenmesinin şeffaflık ilkesine uygun şekilde gerçekleştirildiğini ispat edebilmelidir. Profillemeye ve otomatik karar faaliyetlerinde hesap verebilirliğin sağlanması veri işlemenin şeffaf bir şekilde gerçekleştirilmesini gerektirir⁴⁸⁹. Bu bağlamda algoritmik şeffaflığın sağlanması, algoritmik kararlarda sorumluluğun tesis edilebilmesini amaçlayan algoritmik hesap verebilirlik ilkesinin uygulanabilmesine hizmet eder. Zira şirket, kurum ve kuruluşların hukuki düzenlemelere uymakla yükümlü tutulabilmeleri ve uymadıkları takdirde sorumluluklarına gidilebilmesi, öncelikle faaliyetlerinin şeffaf bir şekilde bilinmesine bağlıdır. Öte yandan, kişisel verilerin adil bir şekilde

⁴⁸⁸ EPRS, Understanding Algorithmic Decision-Making: Opportunities and Challenges, s.25-26.

⁴⁸⁹ Article 29 Working Party, Transparency, s.5.

işlenmesi için de şeffaflık ilkesi kritik önem taşır. Kişisel verilerin adil bir şekilde işlenmesi açıkça tanımlanmamıştır. 29. Madde Çalışma Grubu’nun ilgili görüşünde, kişisel verilerin adil bir şekilde işlenmesinin, ilgili kişilerin kişisel verilerinin işlenmesine ilişkin farkındalığı ile bağlantılı olduğu belirtilmektedir⁴⁹⁰. Bu çerçevede, algoritmik şeffaflık için, ilgili kişilerin, kişisel verilerinin profillemeye ve otomatik karar faaliyetleri kapsamında hangi amaçla işleneceğinin ve işleme faaliyetinin kapsamının farkında olmaları gerekir. İlgili kişilerin belirtilen çerçevede bir farkındalığa sahip olabilmeleri, ancak yeterince açık, anlaşılır ve kapsamlı bir bilgilendirme (aydınlatma) ve ile mümkündür.

Şeffaflık ilkesi GVK Tüzüğü’nün 13 ve 14. maddelerinde düzenlenmiş olan ilgili kişinin bilgilendirilme hakkıyla doğrudan ilgilidir⁴⁹¹. Şeffaflık ilkesine uyum, profillemeye ve otomatik karar faaliyetinin hangi amaçlarla gerçekleştirildiğinin, kişisel verilerin toplanması sırasında açık, meşru ve belirli olmasını gerektirir⁴⁹². Profillemeye ve otomatik karar alma faaliyetlerinin şeffaflık ilkesine uygun şekilde gerçekleştirilmesi, ilgili kişinin, veri sorumlusunun kimliği, profillemeye ve otomatik karar alma faaliyetinin amacı, riskleri, bu kapsamda alınan tedbirler, bu faaliyetlere karşı sahip olduğu haklar ve bu hakları nasıl kullanabileceğine ilişkin bilgilendirilmesini gerektirir⁴⁹³. Öte yandan veri sorumlusu GVK Tüzüğü’nün 22. maddesi tahtında düzenlenen ilgili kişinin kendisi hakkında hukuki sonuçlar doğuran veya benzer biçimde önemli şekilde kendisini etkileyen profil çıkarma da dahil olmak üzere tamamen otomatik işlemeye dayalı karar almanın varlığı ve söz konusu işleme faaliyetinin ilgili kişi açısından önemli ve öngörülen sonuçları

⁴⁹⁰ Article 29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 Eylül 2014, s.16, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (Kısaltılmışı “Recent Developments on the Internet of Things”).

⁴⁹¹ Bilgilendirilme hakkı, “*right to be informed*” ifadesinin karşılığı olarak kullanılmıştır. KVK Kanunu’nda “bilgilendirilme hakkı” yerine veri sorumlusunun “aydınlatma yükümlülüğü” hüküm altına alınmıştır.

⁴⁹² Bkz. GVK Tüzüğü, Giriş Bölümü, 39.Paragraf; Voigt&Von Dem Bussche, s.236.

⁴⁹³ Voigt & Von Dem Bussche, s.173-174.

hakkında ilgili kişiyi bilgilendirmek ve ilgili kişiye karar sürecinde yürütülen mantığa ilişkin anlamlı bilgiler sağlamakla yükümlüdür⁴⁹⁴.

Bu bilgilendirmenin kısa, kolay erişilebilir ve anlaşılabilir olması, açık ve sade bir dil ve uygun olan hallerde görselleştirme kullanılması gerekir; bilgilendirme, bir internet sitesi aracılığıyla dijital ortamda da yapılabilir⁴⁹⁵. İlgili kişilerin şeffaflık ilkesine uygun şekilde bilgilendirilmelerinde hedeflenen hukuki yarar, ilgili kişilerin kişisel verilerinin işlendiği hususunda bilgi sahibi olmalarının yanı sıra, otomatik karar alma faaliyetleri kapsamında bu kararlardan etkilenen taraf olarak kişisel verileri üzerinde kontrol sahibi olmalarını sağlamaktır⁴⁹⁶. Wachter, kullanıcıların, bir otomatik sisteme güvenip güvenmeme ve sistemi kullanma konusunda bilinçli bir karar verebilmeleri, anlaşılır ve kapsamlı bir bilgilendirme gerektirdiğini ve bu sayede sistemi geliştirenler ve kullananlar arasında oluşacak diyalogun, otomatik sistemlerin opak yapısından kaynaklanan öngörülemez ayrımcılığın yarattığı risklerin önlenmesi açısından önemli olduğunu belirtmiştir⁴⁹⁷. Öte yandan, kullanıcıların otomatik sistemleri kullanma olasılığı, hizmet sağlayıcıların ve uygulamaların “güvenilir” olarak algılanmaması halinde düşmektedir⁴⁹⁸. Bu durum ilgili otomatik sistemden beklenen faydaların gerçekleşmeyeceği anlamına geleceğinden, veri sorumluları açısından da sorun teşkil eder⁴⁹⁹.

Profilleme ve otomatik karar uygulamaları, olabildiğince gerçeğe yakın sonuçlar elde edebilmek için, kamuya açık (alenileştirilmiş) verilerin yanı sıra, üçüncü kişilerce geliştirilmiş uygulamalar, nesnelerin interneti, RFID ve sensörler gibi çeşitli teknolojiler aracılığıyla çeşitli ve farklı kaynaklardan veri

⁴⁹⁴ Bkz. GVK Tüzüğü, m.13/2(f), 14/2(g).

⁴⁹⁵ GVK Tüzüğü, Giriş Bölümü, 39 ve 58.Paragraflar; Voigt & Von Dem Bussche, s.236.

⁴⁹⁶ Lilian EDWARDS & Michael VEALE, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, Duke Law & Technology Review, 23 Mayıs 2017, s. 41, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855# (Kısaltılmışı “Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for”); Article 29 Working Party, Recent Developments on the Internet of Things, s.17.

⁴⁹⁷ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.12.

⁴⁹⁸ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.12.

⁴⁹⁹ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.12.

toplamaktadır⁵⁰⁰. Bu veriler insan zihninin takip etmekte ve anlamakta zorlanacağı derecede karmaşık model ve algoritmalar ile analiz edilir. Algoritmaların “kara kutu” olarak nitelendirilen karmaşık ve opak yapısı, ilgili kişilerin profillemeye ve otomatik karar alma sürecinin nasıl işlediğini, kendileri hakkında bu kararın neye dayanılarak verildiğini, bu kararın alınmasında hangi verilerinin etkili olduğunu anlayabilmelerini neredeyse imkansız hale getirir⁵⁰¹. Öte yandan, profillemeye ve otomatik karar uygulamalarında verinin en “inovatif ikincil kullanımları” verinin ilgili kişiden toplanma anında henüz bilinmemektedir⁵⁰². Mayer-Schönberger ve Cukier henüz bilinmeyen bir amaç için veri sorumlusunun bilgilendirme yükümlülüğünü yerine getiremeyeceğini ve ilgili kişinin de bilinmeyen bir amaç için rıza gösteremeyeceğini ifade etmiştir. Mayer-Schönberger ve Cukier’e göre, ilgili kişinin rızasının bulunmaması, her bir büyük veri analizi faaliyetinde ilgili kişiden yeni rıza alınmasını gerektirir; ancak bu mümkün olsa dahi yaratacağı maliyet sebebiyle hiçbir şirket tarafından tercih edilmeyecektir. Kullanıcılardan kişisel verilerinin “ilerde olası her türlü kullanımı” için rıza talep edilmesi de GVK Tüzüğü’nün “bilgilendirmeye dayalı rıza” (“*informed consent*”) kriterlerini karşılamayacaktır⁵⁰³. Belirtilen durumlar, ilgili kişilere yapılacak bilgilendirmeleri işlevsiz kılmakla birlikte, profillemeye ve otomatik karar faaliyetlerinde şeffaflık ve hesap verebilirlik ilkesinin uygulanabilirliği konusunda soru işaretleri yaratır. Açıklanan nedenlerle, GVK Tüzüğü otomatik karar uygulamalarında kişisel verilerin şeffaf ve hesap verebilir şekilde işlenmesini yeterli şekilde garanti edemediği gerekçesiyle eleştiri konusu olmuştur⁵⁰⁴.

Şeffaflık ilkesi, ilgili kişinin bilgilendirilme hakkının yanı sıra GVK Tüzüğü’nün 15.maddesinde düzenlenen erişim hakkı (*right of access*) ile de

⁵⁰⁰Şehriban İpek AŞIKOĞLU, Veri Sorumlularının Aydınlatma Yükümlülüğü, Kişisel Verileri Koruma Dergisi 1 (2), 2019, s.51, <https://dergipark.org.tr/tr/pub/kvkd/issue/50609/639205>.

⁵⁰¹Article 29 Working Party, Automated Individual Decision Making and Profiling, s.9.

⁵⁰² Mayer & Schönberger & Cukier, s.160.

⁵⁰³ Mayer & Schönberger & Cukier, s.161.

⁵⁰⁴Sandra WACHTER & Brent MITTELSTADT & Luciano FLORIDI, Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation, International Data Privacy Law, 2017, s.47, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469.

doğrudan ilgilidir. İlgili kişi, erişim hakkını kullanarak veri sorumlusundan kişisel verilerinin profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyeti kapsamında işlenip işlenmediği, yürütülen mantığa ilişkin anlamlı bilgi ve söz konusu işleme faaliyetinin kendisi açısından önemi ve öngörülen sonuçları hakkında bilgi talep edebilmektedir⁵⁰⁵. Erişim hakkı kullanılmadan, silme ve düzeltme ile Tüzüğün 21. maddesinde düzenlenen itiraz hakları etkili bir şekilde kullanılamayacağından, erişim hakkı ilgili kişinin hakları içinde önemli bir role sahiptir. Ancak, bu hak mutlak bir hak değildir. Tüzük'te, ilgili kişinin erişim hakkının, üçüncü kişilerin hak ve özgürlüklerini olumsuz etkileyemeyeceği, bu bağlamda veri sorumlusunun bilgi taleplerini kısıtlayabileceği hüküm altına alınmıştır⁵⁰⁶. Bu bağlamda, üçüncü kişilerin mahremiyet haklarının yanı sıra veri sorumlularının ticari sır niteliğindeki ve fikri mülkiyet haklarının konusunu oluşturan bilgiler, ilgili kişinin erişim hakkını etkin bir şekilde kullanabilmesinin önünde engel teşkil etmektedir⁵⁰⁷. Özellikle, profillemeye de dahil tamamen otomatik işlemeye dayalı karar alma faaliyetlerine ilişkin bilgi taleplerinde, belirtilen istisna sorun yaratmaktadır. Konuyla ilgili daha detaylı incelemeye çalışmanın ilgili kişinin erişim hakkına ilişkin bölümünde yer verilecektir.

Wachter, GVK Tüzüğü'nün bağlayıcı hükümlerinin bireyin mahremiyetini ve kimliğini korumada yeterli korumayı sağlayamadığından bahisle, bireylerin nesnelerin interneti uygulamalarında kişisel verilerinin nasıl toplandığı, işlendiği ve aktarıldığı ve bu kapsamda oluşabilecek muhtemel risklerin neler olduğunu daha iyi anlamalarını sağlamayı amaçlayan üç aşamalı bir şeffaflık modeli öne sürmüştür⁵⁰⁸. Wachter, bu modelin uygulanmasıyla, nesnelerin interneti cihazlarının ve hizmetlerinin kullanıcılarının, kendilerine sağlanacak bilgiler sayesinde bu cihaz ve hizmetleri kullanıp kullanmama konusunda daha bilinçli tercihler yapma ve kişisel verilerinin nasıl toplandığını, işlendiğini ve aktarıldığını

⁵⁰⁵ Bkz. GVK Tüzüğü, m. 15/2(h).

⁵⁰⁶ Bkz. GVK Tüzüğü, m. 15/4; GVK Tüzüğü, Giriş Bölümü, 63.Paragraf.

⁵⁰⁷ Wachter, The GDPR and the Internet of Things: A Three Step Transparency Model, s.18.

⁵⁰⁸ İlgili çalışma için bkz. Sandra WACHTER, The GDPR and the Internet of Things: A Three-Step Transparency Model, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130392.

daha etkin bir şekilde kontrol etme konusunda mevcuttaki durumlarına göre daha iyi bir konuma sahip olacakları görüşündedir. Wachter'in üç aşamalı modelinin ikinci aşamasında, yanlış veya öngörülemeyen tahmin ve varsayımları ve bu bağlamda profillemeye dayalı ayrımcılığı sınırlamak için şeffaflığı sağlayacak mekanizmalara yer verilmiştir. Bunlar, (i) ayrımcılığı önleyici araç ve prosedürlerin geliştirilmesi, (ii) kullanıcıların kendileri hakkındaki varsayım ve çıkarımlar hakkında bilgilendirilmeleri, (iii) kişisel verilerin aktarılmasına ilişkin etik uygulamalarının geliştirilmesi, (iv) ilgili kişilerin bilinçli tercihler yapmalarını sağlamak için işleme faaliyetine göre özelleştirilmiş rıza modellerinin geliştirilmesi ve (v) izlemeyi önlemek üzere itiraz opsiyonlarının sunulması şeklinde dört ana başlık altında incelenmiştir. Wachter'in şeffaflık modelinde, ayrımcı uygulamaların ortaya çıkarılması için algoritmalar üzerinde "etik denetimi" gerçekleştirilmesine yönelik araçların kullanılması, bireyleri ayrımcı profillemeye ve otomatik karar uygulamalarına karşı koruyacak iç denetim planlarının oluşturulması, kullanıcılara işlenen verilerinin kapsamı ve bunlardan ulaşılan çıkarımlar hakkında anlamlı bilgiler sağlayacak "Google Ad Manager" ve benzeri araçların kullanılması ve kullanıcıların kişisel verilerinin üçüncü kişilerle paylaşılacak olması halinde, paylaşımından önce, paylaşılan veri kümelerinin farklı işleme amaçları için farklı veri kümeleri ile eşleştirilmesi suretiyle çıkarılacak yeni bilgilerin ilgili kişi açısından doğurabileceği ayrımcılık risklerine ilişkin bir değerlendirme yapılması tavsiye edilmektedir⁵⁰⁹.

Profillemeye ve otomatik karar alma sistemlerinde algoritmik şeffaflığı sağlayama yönelik ileri sürülen yaklaşımlardan biri de görselleştirme ve etkileşimin birleştirilmesidir⁵¹⁰. Araştırmalar, TalkExplorer ve SetFusion gibi etkileşimli görselleştirme araçlarının, özellikle büyük veri analitiği yöntemlerinin kullanıldığı tavsiye sistemlerinde, bireylerin kendilerine neden ilgili tavsiyede bulunulduğunu daha iyi anlamalarını ve kendileri için daha isabetli tavsiyeler oluşturmalarına

⁵⁰⁹ Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, s.19-22.

⁵¹⁰ ICO, Big Data, Artificial Intelligence, Machine Learning And Data Protection, s.87.

olanak tanıdığını tespit etmiştir⁵¹¹. Bu araçlardaki görselleştirme ve etkileşim, tablolar ve venn şemaları gibi araçlarla sağlanmaktadır. Öte yandan, bazı büyük veri analitiği yöntemleri açısından etkileşimli görselleştirme sistemlerinin uygulanmasının zor olduğu durumlarda, ilgili kişilere yapay öğrenme algoritmalarının gerçekleştirdiği çıkarımları kontrol etme ve gerektiğinde düzeltme imkanı veren, daha basitleştirilmiş bir yaklaşım benimsenebilecektir⁵¹². Bu bağlamda, örneğin, bir bankanın kredi risk değerlendirmesi için müşterilerinin profillerini çıkardığı durumda, müşterilerine bu profilleri inceleme ve kendilerine atfedilen hatalı çıkarımları düzeltme imkanı tanınması, profillemeye faaliyetinin şeffaflık ilkesine ve kişisel verilerin doğru ve güncel olması gerekliliğine uygun olmasını sağlamakla birlikte, yapay öğrenme algoritmalarının oluşturduğu çıkarımların da kesinliğinde genel bir iyileşme sağlayacaktır⁵¹³.

GVK Tüzüğü'nün, "ilgili kişinin profillemeye de dahil tamamen otomatik işlemeye dayalı karar almanın varlığı, yürütülen mantığa ilişkin anlamlı bilgi ve söz konusu işleme faaliyetinin ilgili kişi açısından önemi ve öngörülen sonuçları" hakkında bilgilendirilmesini düzenleyen 13/2(f) ve 14/2(g) maddelerinin uygulanabilirliğine ilişkin tartışmalar, temelde yapay zeka sistemleri ve bu sistemlerin ürettiği çıkarımların açıklanabilirlik sorunu ile ilişkilidir⁵¹⁴. Açıklanabilirlik (*explainability*), yapay zekanın gelişiminde kişisel verilerin korunmasının sağlanması açısından önemli bir ilke olarak kabul edilmektedir. Belirtmek gerekir ki, GVK Tüzüğü'ndeki şeffaflık ilkesi ile "şeffaf ve açıklanabilir yapay zeka" kavramı birbiri ile ilişkili olmakla birlikte birbirinden farklı kavramlardır⁵¹⁵. Zira şeffaf ve açıklanabilir yapay zeka ilgili kişilerin kendilerine

⁵¹¹ ICO, Big Data, Artificial Intelligence, Machine Learning And Data Protection, s.88; Katrien VERBERT & Denis PARRA & Peter BRUSILOVSKY, The Effect of Different Set-based Visualizations on User Exploration of Recommendations, 2014, https://www.researchgate.net/publication/280888821_The_Effect_of_Different_Set-based_Visualizations_on_User_Exploration_of_Recommendations.

⁵¹² ICO, Big Data, Artificial Intelligence, Machine Learning And Data Protection, s.88.

⁵¹³ ICO, Big Data, Artificial Intelligence, Machine Learning And Data Protection, s.88.

⁵¹⁴ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.54.

⁵¹⁵ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.44.

ilişkin veri işleme faaliyetleri ile ilgili olarak yeterli şekilde bilgilendirilmesinden ziyade, yapay zeka sistemlerinin işleyişine ilişkin bir model geliştirilmesini ifade etmektedir⁵¹⁶. Bilgisayar bilimcileri teknoloji alanında uzmanlara yönelik yapay zeka sistemlerinin açıklanabilirliği sağlayacak ve sisteme erişim sağlayacak teknikler ve modeller geliştirmektedir⁵¹⁷. Bu teknik ve modellerin geliştirilmesinde, bilgisayar bilimcileri, özellikle derin sinir ağları gibi opak yapay zeka sistemlerinin, bilgisayar bilimleri ve teknoloji alanındaki uzmanlarının bu sistemlerin işleyişine hakimiyetini sağlayacak derecede açıklanabilir bir modelini geliştirmenin teknik olasılığına odaklanmışlardır⁵¹⁸.

Avrupa Parlamentosu Bilim ve Teknolojinin Geleceği Heyeti'nin çalışmasında açıklanabilir yapay zeka ile ilgili araştırmaların farklı açıklama türleri etrafında şekillendiği belirtilmektedir⁵¹⁹. Bunlar, modelin açıklanması (*model explanation*), modelin denetlenmesi (*model inspection*) ve sonuçların açıklanması (*outcome explanation*) olarak sıralanmıştır. Çalışmada belirtildiği üzere, modelin açıklanması, opak bir yapay zeka sisteminin, bu sistemin mantığını tam olarak kavrayabilen yorumlanabilir ve şeffaf bir model üzerinden açıklanmasını ifade etmektedir. Modelin denetlenmesinin, opak bir yapay zeka modelinin veya bu model ile gerçekleştirilen tahminlerin bazı belli özelliklerinin anlaşılabilmesine imkan tanıyacağı belirtilmektedir. Modelin denetlenmesi ile örneğin, başvuranın gelirindeki veya yaşındaki bir değişikliğin bir kredi başvurusunun sonucuna nasıl etki ettiği tespit edilebilir⁵²⁰. Sonuçların açıklanması ise, opak bir yapay zeka sisteminin belirli bir duruma ilişkin çıkarımlarının hesaplanması ile ilgilidir⁵²¹.

⁵¹⁶ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.44.

⁵¹⁷ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.54.

⁵¹⁸ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.54.

⁵¹⁹ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.54.

⁵²⁰ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.54.

⁵²¹ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.55.

Örneğin herhangi bir konudaki (kredi, sigorta, eğitim vb.) kişisel verilerin otomatik yollarla işlenmesiyle verilen karar, bu karara yol açan etkenlerin (başvuranın geliri, yaşı, malvarlığı gibi konulardaki spesifik bilgiler) listelenmesi suretiyle açıklanabilecektir⁵²².

Avrupa Parlamentosu Bilim ve Teknolojinin Geleceği Heyeti, ilgili çalışmasında, şeffaflığı, gerek algoritmik karar sistemlerinin kullanımında insan haklarının ve toplumsal yararın en üst seviyede gözetilmesini, gerek hesap verebilirlik ilkesi kapsamında kimin sorumlu olduğunun tespitine yönelik mekanizmaların kurularak bazı sosyal hedeflere ulaşılması açısından son derece önemli bir araç olarak nitelendirmiştir⁵²³. Çalışmada, algoritmik karar sistemlerinin şeffaflık gerektiren unsurları, veri (*data*), algoritmalar (*algorithms*), hedefler (*goals*), sonuçlar (*outcomes*), uyum (*compliance*), etki (*influence*), kullanım şekli (*usage*) olarak tespit etmiştir. Çalışmada şeffaflığın bu unsurlardan her biri açısından farklı bir anlama sahip olduğu, dolayısıyla tüm algoritmik karar sistemlerinin her unsuruna aynı şekilde uygulanabilecek tek bir özellikten ibaret olmadığı belirtilmiştir. Bu bağlamda şeffaflığın algoritmik sistemin doğasına, yönetim ihtiyacına yol açan karmaşık koşullara ve bu yönetişimin amaçlarına bağlı olarak her bir sisteme farklı şekilde uygulanması gerekir.

Çalışmadaki tespitler uyarınca,

⇒ Algoritmik karar sisteminde kullanılan veri ve algoritmaların incelenmesi,

- Veri ve algoritmalarda sistemin adillliğini etkileyecek bir önyargı olup olmadığının kontrol edilmesi,

⁵²² EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.55.

⁵²³ European Parliamentary Research Service (EPRS), A Governance Framework for Algorithmic Accountability and Transparency, Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA), PE624.262 Nisan 2019, s.6, [https://www.europarl.europa.eu/stoa/en/document/EPRS_STU\(2019\)624262](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)624262) (Kısaltılmışı “A Governance Framework For Algorithmic Accountability And Transparency”).

- Sistemin söz konusu çıkarımları işleme amacı ile ilgili verilerden yapıp yapmadığının kontrol edilmesi,
- Sistemin verileri ilişkilendirme ve ağırlıklandırma yönteminden öğrenilebilecek bir şey olup olmadığının tespit edilmesi,
- Sistemdeki hataların bulunması ve düzeltilmesi,
- Kötücül verilerin (*malicious data*) sisteme girişinin önlenmesi açısından gerekli ve önemlidir.

⇒ Algoritmik karar sisteminin hedef ve sonuçlarının şeffaf olması,

- Söz konusu hedef ve sonuçların tartışılabilmesi ve düzenlenebilmesi,
- Düzenleyicilerin ve halkın, algoritmik bir sistemin hedeflerine göre ve yerine geçtiği veya tamamladığı önceki sistemle karşılaştırıldığında ne ölçüde bir performans gösterdiğini değerlendirebilmeleri açısından önemlidir.

⇒ Bir kuruluşun ilgili düzenlemelere uyum sağladığının kamuya açık olması,

- Düzenleyicilerin, ilgili düzenlemelere uyum sağlanmadığı takdirde şirket, kurum ve kuruluşları sorumlu tutabilmesi,
- Halkın ilgili kuruluşun güvenilirliğini değerlendirebilmesi ve böylece insanların kendilerine sunulan hizmetler hakkında kullanıcılar olarak bilinçli kararlar verebilmesi ve vatandaşların yapay zeka tabanlı hizmetlerin faydaları ve riskleri hakkında daha iyi bilgi sahibi olabilmeleri açısından gerekli ve önemlidir⁵²⁴.

Öte yandan yukarıda belirtilen kapsamda bir şeffaflığın, bazı olumsuz sonuçlar doğurma ihtimali de söz konusu olabilir: Düzenleyici kurumların, şeffaflık ilkesi ile uyumluluğunu denetleyebilmek için yeterli personele sahip olmaları gerekir. İşletmeler ve diğer kuruluşlar, düzenleyici kurumların talep ettiği süreçleri,

⁵²⁴ EPRS, A Governance Framework for Algorithmic Accountability and Transparency, s.6-7.

kuralları ve yasal gözetimi oluşturmali ve sürdürmelidir. Şeffaflık, ticari sırları riske atabilir. Zararsız görünen verilere bilgisayar korsanlarınca erişilmesi, kişisel gizliliğin ihlal edilmesine yol açabilir. Şeffaflık gerekliliği, ciddi zararların ortaya çıkmasıyla sonuçlanabilecek amacına uygun olmayan algoritmaların kullanılmasına neden olabilir. Algoritmaların artan derecede şeffaflaşması, bilgisayar korsanlarının kötü amaçlı erişimlerini kolaylaştırabilir⁵²⁵.



⁵²⁵ EPRS, A Governance Framework for Algorithmic Accountability and Transparency, s.7.

ÜÇÜNCÜ BÖLÜM

3. ÖZEL DÜZENLEMELER, HUKUKA UYGUNLUK SEBEPLERİ, İLGİLİ KİŞİNİN HAKLARI

3.1. GENEL VERİ KORUMA TÜZÜĞÜ'NDE PROFİLLEME VE OTOMATİK KARAR ALMAYA İLİŞKİN ÖZEL DÜZENLEMELER

GVK Tüzüğü'nün 22. maddesi ile bireyler üzerinde hukuki veya benzer şekilde önemli bir etkiye sahip olan, profillemeye dayalı olanlar da dahil olmak üzere, tamamen otomatik işlemeye dayalı olarak gerçekleştirilen karar alma faaliyetleri belirli bir çerçevede sınırlandırılmıştır. Tüzüğün 22. maddesinin uygulama alanına girdiği kabul edilen bir otomatik karar alma faaliyeti, profillemeye de içerebileceği gibi, kararın mutlaka profillemeye dayanması da zorunlu değildir⁵²⁶. Belirtilmelidir ki, Tüzüğün 22. maddesi, sadece profillemeye içeren veri işleme faaliyetlerinden ziyade, profillemeye dayalı olanlar da dahil olmak üzere, ilgili kişiyi hukuki veya benzer şekilde önemli bir biçimde etkileyen tamamen otomatik işlemeye dayalı kararlarla ilgilidir. İlgili kişi üzerinde hukuki veya benzer şekilde önemli bir etkisi olmayan tamamen otomatik işlemeye dayalı karar alma faaliyetleri ile tamamen otomatik işlemeye dayalı olmayan karar alma faaliyetleri Tüzüğün 22. maddesinin uygulama alanına girmemektedir.

3.1.1. Genel Veri Koruma Tüzüğü'nde Profillemeye de Dahil Olmak Üzere Tamamen Otomatik İşlemeye Dayalı Karar Almaya İlişkin Düzenlemeler

GVK Tüzüğü'nün 22. maddesinin birinci fıkrasında yer verilen düzenleme ile ilgili kişiye, “kendisi ile ilgili hukuki sonuçlar doğuran veya kendisini benzer şekilde önemli derecede etkileyen profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı bir karara tabi olmama hakkı” (“*right not to be subject to*

⁵²⁶ Bkz. s.24-25.

a decision based solely on automated processing, including profiling”) tanınmıştır⁵²⁷. Çalışmanın ilerleyen bölümlerinde de 22. maddeye sıklıkla atıf yapılacağı göz önüne alınarak maddenin Türkçe’ye tercüme edilmiş metnine aşağıda yer verilmiştir:

“Madde 22 (Profilleme de dahil olmak üzere otomatik bireysel karar alma):

1. İlgili kişi kendisi ile ilgili hukuki sonuçlar doğuran veya benzer şekilde önemli derecede kendisini etkileyen profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı bir karara tabi olmama hakkına sahiptir.

2. Kararın,

(a) ilgili kişi ile veri sorumlusu arasında bir sözleşmenin akdedilmesi veya ifası için gerekli olması;

(b) veri sorumlusunun tabi olduğu ve ilgili kişinin hak ve özgürlükleri ile meşru menfaatinin güvence altına alınması amacıyla uygun tedbirlerin de hüküm altına alındığı Birlik veya üye devley hukukunda izin verilmesi,

(c) ilgili kişinin açık rızasına dayanması

halinde 1.paragraf uygulanmaz.

3. 2. paragrafın (a) ve (c) bentlerinde atıfta bulunulan hallerde, veri sorumlusu, ilgili kişinin hak ve özgürlükleri ile meşru menfaatlerinin güvence altına alınması için, ilgili kişiye en azından, insan müdahalesinin sağlanmasını talep etme hakkı, kendi görüşünü ifade etme hakkı ve karara itiraz etme hakkı sağlamak suretiyle uygun tedbirleri alacaktır.

⁵²⁷ Bkz. GVK Tüzüğü, m.22/1.

4. 9(2) maddesinin (a) veya (g) bendinin geçerli olmaması ve ilgili kişinin hak ve özgürlükleri ile meşru menfaatlerinin güvence altına alınması amacı ile uygun tedbirlerin alınmamış olması halinde, 2. paragrafta atıfta bulunulan kararlar 9(1) maddesinde atıfta bulunulan özel nitelikli kişisel verilerin işlenmesine dayanamaz.”

Tüzüğün 22. maddesi kapsamında ilgili kişiye tanınan bu hak, kişisel verilerin korunmasındaki temel düşünce olan bireysel özerklik ve bilgilerin geleceğini belirleme hakkı ile yakından ilişkilidir⁵²⁸. Hükmün lafzındaki “karara tabi olmama hakkı” ifadesi, m.22/1’in bir “yasak” mı yoksa “itiraz hakkı” olarak mı yorumlanacağına ilişkin tartışmaları beraberinde getirmiştir⁵²⁹.

GVK Tüzüğü m.22/1, itiraz hakkı veya yasak olarak yorumlamasına göre, ilgili kişi ve veri sorumlularının hak ve menfaatleri açısından farklı şekilde koruma sağlamaktadır⁵³⁰. Hükmün bir yasak olarak yorumlanması halinde, veri sorumlusunun m.22/2’nin a, b ve c bentlerindeki hukuka uygunluk sebeplerinden birine dayanmadığı takdirde otomatik karar alma faaliyetleri gerçekleştirmemekle yükümlü olacağı sonucu ortaya çıkmaktadır⁵³¹. Hükmün ilgili kişiye bir itiraz hakkı tanıdığı şeklinde yorumlanması halinde ise, m.22/2’nin a, b, c bentlerindeki durumlardan biri gerçekleştiği takdirde ilgili kişi kendisi hakkındaki otomatik kararlara itiraz edemeyecektir⁵³². Hükmün belirtilen iki yorumu, ilgili kişinin

⁵²⁸ Küzeci, s.230. GVK Tüzüğü’nden önceki düzenleme olan 95/46 Sayılı Direktif’in 15. maddesinin birinci fıkrasında, herkesin, kendisiyle ilgili hukuki sonuçlar doğuran, kendisini önemli şekilde etkileyen ve işindeki performansı, kredibilitesi, güvenilirliği gibi kişisel durumları ile ilgili bir değerlendirmede bulunmak amacıyla yalnızca otomatikleştirilmiş veri işlemesine dayanan bir karara tabi olmama hakkına sahip olduğu hüküm altına alınmıştır. 1978 tarihli eski Fransız Veri Koruma Yasası’nın 39. maddesinden Direktif’e aktarılan bu hüküm Üye Devletlerin tamamı tarafından kabul edilmiştir. Küzeci, s.230. 1978 tarihli eski Fransız Veri Koruma Yasası’nın İngilizce metni için bkz. <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>.

⁵²⁹ Wachter & Mittelstadt & Floridi, s.94.

⁵³⁰ Frederike KALTHEUNER & Elettra BIETTI, Data is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR, Journal of Information Rights Policy and Practice 2(2), Ocak 2018, s.10, <http://doi.org/10.21039/irpandp.v2i2.45>.

⁵³¹ Wachter & Mittelstadt & Floridi, s.94; Kaltheuner & Bietti, s.10.

⁵³² Wachter & Mittelstadt & Floridi, s.94; Kaltheuner & Bietti, s.10.

otomatik karar alma faaliyetlerini kısıtlamak için aktif bir eyleminin gerekip gerekmediği noktasında ayrılmaktadır⁵³³.

İlgili kişinin tamamen otomatik işlemeye dayalı bir kararın konusu olmama hakkının bir itiraz hakkı olarak yorumlanması halinde, ilgili kişinin bu hakkını aktif bir eylemiyle kullanması gerekecektir. Öte yandan bir yasak olarak yorumlanması halinde, m. 22 kapsamında bir otomatik karar alma gerçekleştiren veri sorumlusu, ilgili kişinin açıkça bir talebi olmadan, veri işleme faaliyetlerini bizzat gözetmekle yükümlü olacaktır⁵³⁴. İlgili kişinin aktif eylemini gerektiren itiraz hakkının kullanılması, hem ilgili kişinin otomatik bir kararın varlığının farkında olmasını, hem de sürece müdahil olmaya istekli olmasını, her iki durumda da ilgili kişinin bilinçli bir çabasını gerektirir⁵³⁵.

Bu bağlamda GVK Tüzüğü m. 22/1'deki hakkın ilgili kişi tarafından aktif şekilde kullanılması gereken bir hak olarak kabul edilmesi halinde, hakkın kullanılması ilgili kişinin özgür iradesine ve seçimine bağlı olacaktır⁵³⁶. Brkan'a göre bu durum, ilgili kişinin bu hakkı kullanmayı seçmediği senaryoda, m. 22/1 tahtındaki otomatik karar alma faaliyetlerinin hukuka uygun kabul edilmesine ve veri sorumlusunun ilgili hükmün 3. paragrafında belirtilen tedbirleri sağlamadan, ilgili kişi açısından hukuki ya da benzer şekilde önemli sonuçları olan tamamen otomatik işlemeye dayalı bir karar alabilmesi olasılığına yol açacaktır⁵³⁷. Öte yandan, ilgili kişinin hakkını kullanmaması veya kullanamaması sonucunda, kendisi hakkındaki böyle bir kararın hukuki sonuçları, ilgili kişi açısından oldukça zararlı olabilecektir⁵³⁸. Tüzük m.22/1'in, ilgili kişiye fiilen kullanması gereken bir hak verdiği şeklinde yorumlanması, ilgili kişi üzerinde zararlı etkilere yol açarak,

⁵³³ Wachter & Mittelstadt & Floridi, s.94.

⁵³⁴ Maja BRKAN, Do Algorithms Rule the World? Algorithmic Decision- Making in the Framework of the GDPR and Beyond, 1 Ağustos 2017, s.7, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901.

⁵³⁵ Wachter & Mittelstadt & Floridi, s.94.

⁵³⁶ Brkan, s.7.

⁵³⁷ Brkan, s.7.

⁵³⁸ Brkan, s.7.

bireyi tamamen otomatik şekilde gerçekleşen bir karar alma faaliyetine konu edilme olasılığına karşı korumayı amaçlayan hükmün amacına aykırı sonuç doğurabilecektir⁵³⁹. Brkan, ilgili kişinin bu hakkı kullanma tercihinin doğuracağı hukuki sonuçların da belirsiz olduğunu vurgulamıştır. Buna göre bu hakkın, otomatik kararın tamamen engellenmesini sağlayan bir itiraz hakkı niteliğinde mi olduğu veya karar sürecine insan müdahalesi talebi olarak mı kabul edileceği belli değildir⁵⁴⁰.

Wachter, Mittelstadt ve Floridi'ye göre, hükmün ilgili kişiye tanınan bir itiraz hakkı olarak yorumlanması halinde, otomatik karar alma faaliyetleri ilgili kişinin fiili olarak itirazda bulunduğu hallerle sınırlandırılmaktadır⁵⁴¹. Buna göre, ilgili kişi itirazda bulunduğu anda, ilgili otomatik karar alma faaliyetinin m. 22/2'nin a, b ve c bentlerinde belirtilen hukuka uygunluk sebeplerinden birine dayanması aranacaktır. Öte yandan, Tüzük m. 22/2'nin a, b ve c bentlerindeki hukuka uygunluk hallerinden birine dayanan bir otomatik karar söz konusu ise, ilgili kişi otomatik karar faaliyetine itiraz edemeyecek ise de m.22/3 kapsamında insan müdahalesinin sağlanmasını talep etme, kendi görüşünü ifade etme ve karara itiraz haklarını kullanabilecektir⁵⁴². Wachter ve diğerlerine göre, hükmün bir itiraz hakkı olarak yorumlanması, ilgili kişilere kendileri hakkındaki otomatik kararları değerlendirmek ve itiraz etmek suretiyle profillemeye ve otomatik karar faaliyetleri karşısında hak ve menfaatlerini etkin bir şekilde savunma yükümlülüğünü getirir⁵⁴³. Bu bağlamda, lafzı itibarıyla bir yasak veya hak olarak yorumlanmaya açık şekilde kaleme alınan 22. maddenin, otomatik karar alma faaliyetlerine ilişkin bir yasak hükmünde kabul edilmesini sağlayacak şekilde revize edilmesi tavsiye edilmiştir⁵⁴⁴.

⁵³⁹ Brkan, s.7.

⁵⁴⁰ Brkan, s.7.

⁵⁴¹ Wachter & Mittelstadt & Floridi, s.39.

⁵⁴² Wachter & Mittelstadt & Floridi, s.39.

⁵⁴³ Wachter & Mittelstadt & Floridi, s.39.

⁵⁴⁴ Wachter & Mittelstadt & Floridi, s.46.

22. maddenin bir yasak olarak yorumlanması halinde, m.22/2'deki hukuka uygunluk hallerinden biri gerçekleşmediği müddetçe veri sorumlusu otomatik karar alma faaliyeti gerçekleştirmemekle yükümlü olacaktır. Tüzüğün 22. maddesinin, veri sorumlularının uymak zorunda olduğu otomatik karar alma yasağı olarak yorumlanması ve uygulanması halinde ilgili kişinin hak ve çıkarlarının daha fazla korunacağı yönünde çeşitli görüşler bulunmaktadır⁵⁴⁵. Maddenin bir yasak olarak yorumlanması ve uygulanması halinde ilgili kişiler hukuki düzenlemelerle halihazırda korunduklarından, kendileri hakkında tamamen otomatik bir karar alınmasını önlemek için fiilen bir eylemde bulunmaları gerekmeyecektir⁵⁴⁶. Denetleyici makamlar da otomatik karar uygulamalarının hukuka aykırı şekilde gerçekleşmesi halinde veri sorumlularına para cezası da dahil olmak üzere gerekli yaptırımları uygulayarak otomatik kararların hukuka uygun şekilde alınmasını sağlamak suretiyle 22. maddenin uygulanmasında önemli bir role sahiptir⁵⁴⁷. Bu bağlamda 22. maddenin bir yasak olarak yorumlanması ilgili kişinin hak ve çıkarları açısından daha fazla koruma sağlamaktadır⁵⁴⁸. Nitekim profillemeye ve otomatik karar faaliyetlerinin çoğunlukla bu kararlardan etkilenenler farkında olmadan gerçekleştiği dikkate alındığında, ilgili kişilerin itiraz haklarını etkin bir şekilde kullanamamaları ihtimali göz ardı edilemeyecektir⁵⁴⁹. Öte yandan, otomatik karar alma süreçleri, büyük veri ve algoritmalarının kullanımı ve yapay öğrenme dahil olmak üzere giderek daha fazla gelişmiş karmaşık işleme yöntemlerine dayandığından, yanlış ve adil olmayan kararların yorumlanması veya denetlenmesi oldukça zor olabilmektedir. Bu bağlamda, ilgili hükmün bir itiraz hakkından ziyade yasak olarak yorumlanması ve uygulanması yerinde olacaktır⁵⁵⁰.

⁵⁴⁵ Bu yöndeki görüşler için bkz. Mendoza & Bygrave, s.9; Kaltheuner & Bietti, s.11; Wachter & Mittelstadt & Floridi, s.95.

⁵⁴⁶ Wachter & Mittelstadt & Floridi, s.39.

⁵⁴⁷ Wachter & Mittelstadt & Floridi, s.39.

⁵⁴⁸ Wachter & Mittelstadt & Floridi, s.39.

⁵⁴⁹ Kaltheuner & Bietti, s.11

⁵⁵⁰ Kaltheuner & Bietti, s.11

3.1.1.1.Tamamen Otomatik İşlemeye Dayalı Olma

Tamamen otomatik işlemeye dayalı bir karardan söz edilebilmesi ve ilgili kişinin Tüzük m.22/1 ile tanınan korumadan faydalanabilmesi için, değerlendirme ve nihai karar sürecinde bir insan müdahalesinin bulunmaması gerekmektedir. GVK Tüzüğü'nün 22. maddesinin birinci fıkrasında, “tamamen otomatik işlemeye dayalı kararlar” (“*decisions based solely on automated processing*”) ifadesi kullanılmış olmakla birlikte, bu şartın neyi ifade ettiği ile ilgili bir açıklama yapılmamıştır. Dolayısıyla bu ifadenin pratikte uygulamasının ne şekilde olacağına ilişkin bir belirsizlik söz konusudur. Maddedeki “tamamen” (“*solely*”) ifadesi nedeniyle, asgari düzeyde bir insan müdahalesi bulunan otomatik kararların maddenin uygulama alanının dışında kaldığını ileri süren görüşler bulunmaktadır⁵⁵¹. Bu durum, Tüzüğün 22. maddesinin birinci fıkrasının, günümüzde etkin şekilde kullanılan ve ilgili kişiyi önemli şekilde etkileyen ve hatta temel hak ve özgürlüklerine zarar veren birçok otomatik karar alma faaliyetine uygulanamamasına neden olan tehlikeli bir boşluk yaratmaktadır⁵⁵². Örneğin, bankalarda ve sigorta şirketlerinde kullanılan ve algoritmalar aracılığı ile gerçekleştirilen veri analiziyle potansiyel müşterilerin güvenilirlikleri, kredibiliteleri gibi özellikleri üzerinden puanlandıkları puanlama sistemlerinde, ilgili kişiye bir puan verildikten sonra genellikle önceden belirlenmiş kurallara göre her bir puan için belirli koşulların uygulanması kararı alınması veya başvurunun (kredi veya sigorta başvurusu) reddedilmesi suretiyle pasif bir insan müdahalesi gerçekleşmektedir⁵⁵³. Ancak önceden belirlenmiş kuralların uygulanması, herhangi bir muhakeme çabasını gerektirmemektedir⁵⁵⁴. Dolayısıyla, Tüzüm m.22/1'in dar şekilde yorumlanması, ilgili kişi hakkında önemli sonuçları olan otomatik

⁵⁵¹Wachter & Mittelstadt & Floridi, s.33; Mireille HILDEBRANDT, The Dawn of a Critical Transparency Right for the Profiling Era, Haziran 2012, s.50-51, https://www.researchgate.net/publication/254898221_The_Dawn_of_a_Critical_Transparency_Right_for_the_Profiling_Era.

⁵⁵²Kaltheuner & Bietti, s.13; Gianclaudio MALGIERI & Giovanni COMANDÉ, Why a Right to Legibility of Automated Decision-making Exists in the General Data Protection Regulation, 13 Kasım 2017, s.13, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088976.

⁵⁵³ Malgieri & Comandé, s.13.

⁵⁵⁴ Malgieri & Comandé, s.13.

kararların, süreçte pasif de olsa bir insan müdahalesi içerdiği gerekçesiyle maddenin uygulama alanı dışında kalmasına yol açacaktır⁵⁵⁵.

29. Madde Çalışma Grubu'nun ilgili rehberinde belirtildiği üzere, burada insan müdahalesi ile kastedilen, ilgili otomatik kararın şekli bir incelemeden ziyade anlamlı bir inceleme ve değerlendirmeye tabi tutulmasıdır⁵⁵⁶. Bu da, veri sorumlusunun, sürece insan katılımı varmış gibi göstererek ilgili kişinin GVK Tüzüğü m.22 tahtında kendisine tanınan korumadan faydalanmasını önleyemeyeceği anlamına gelir⁵⁵⁷. Söz konusu inceleme ve değerlendirme, bu karara müdahale ederek değiştirebilme yetki ve becerisine sahip bir kişi tarafından gerçekleştirilmeli ve inceleme kapsamında ilgili tüm veriler dikkate alınmalıdır⁵⁵⁸. Bu görüşe paralel şekilde, Birleşik Krallık Bilgi Komisyoneri Ofisi'nin, profileme ve otomatik karar alma faaliyetlerine ilişkin görüşünde, kararın sonucu üzerinde gerçek bir etkiye sahip olmayan minimal düzeyde insan müdahalesi bulunan otomatik kararların m.22/1'in kapsamı dışında bırakılamayacağı belirtilmiştir⁵⁵⁹. Öte yandan, 29. Madde Çalışma Grubu'nun mevcut tüm girdi ve çıktı verilerinin dikkate alınması yönündeki bu görüşü, Kaltheuner ve Bietti tarafından, bu işlemin büyük veri analitiği ve yapay öğrenme algoritmaları bağlamında her zaman mümkün olmadığı ve anlamlı insan müdahalesinin varlığını kanıtlamak için de yeterli olmadığı gerekçesiyle eleştirilmiştir⁵⁶⁰. Kaltheuner ve Bietti'nin 29. Madde Çalışma Grubu'nun ilgili rehberine yönelik eleştirilerinden biri de rehberde insan müdahalesinin kriterlerine ilişkin açıklamalara yer verilmiş olmasına rağmen özellikle profileme amacıyla gerçekleştirilen karmaşık veri işleme faaliyetlerindeki şeffaflık sorunları sebebiyle bu açıklamaların “anlamlı bir bir

⁵⁵⁵ Malgieri & Comandé, s.13.

⁵⁵⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.21.

⁵⁵⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.21.

⁵⁵⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.21.

⁵⁵⁹ Information Commissioner's Office, Feedback request-profiling and automated decision making, 2017, s.19, <https://ico.org.uk/media/about-the-ico/consultations/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>.

⁵⁶⁰ Kaltheuner & Bietti, s.14.

insan müdahalesi” nin nasıl olması gerektiğine yönelik yeterli bir bilgi sağlamadığına ilişkindir⁵⁶¹.

Kaltheuner ve Bietti, büyük veri analitiği, yapay öğrenme ve algoritmik karar mekanizmalarındaki kara kutu problemi ve bu sistemlerdeki işleme sürecinin şeffaf bir şekilde gerçekleşmediği göz önüne alındığında insan müdahalesi ve gözetiminin bir anlam ifade etmeyebileceği görüşündedir⁵⁶². Zira bu sistemlerde veri işleme faaliyetleri oldukça karmaşık ve insan aklının kavrayamayacağı şekilde gerçekleşebildiğinden, kararlarını bu sistemlerin çıkarımlarına dayandıran kişiler bu sistemlerin kara kutu özelliğinden ileri gelen eksikliklerinin her zaman farkında olmayabilirler⁵⁶³. Buna göre, karar sürecindeki insan müdahalesinin “anamlı insan müdahalesi” olarak nitelendirilebilmesi için, bu kararı veren kişilerin, kararlarına esas aldıkları profilin doğru, adil olduğunu ve ayrımcılık içermediğini tespit edebilecek yeterlilikte teknik bilginin yanı sıra profillemeye ve otomatik karar alma faaliyetlerinin adil olmayan ve ayrımcı sonuçlara yol açabilme potansiyelinin sebepleri hakkında da öngörüye sahip olması gerekir⁵⁶⁴. Dolayısıyla, bu gibi hallerde, nihai karar bir insan tarafından verilse dahi, karar veren kişi bu kararı etkili bir şekilde sorgulama kapasitesine sahip olmadığında otomatik bir sistem onun yerine karar vermiş olacaktır⁵⁶⁵. Örneğin COMPAS risk değerlendirme sisteminin⁵⁶⁶ kullanıldığı mahkemelerde, bu yazılımın ayrımcı veya haksız kararlar verdiğinin daha önce tespit edilmediği ve davaya bakan yargıcın bu hususta bilgi sahibi olmadığı bir senaryoda yargıcın nihai kararına hükmederken sadece yazılımın çıktısını esas alması halinde, her ne kadar nihai kararın resmi olarak yargıç tarafından veriliyor olması karar sürecinde bir insan müdahalesinin varlığına

⁵⁶¹ Kaltheuner & Bietti, s.13.

⁵⁶² Kaltheuner & Bietti, s.13-14. Benzer yönde Ben Green tarafından kaleme alınan ve algoritmik karar alma faaliyetlerinde insan müdahalesi öngören 41 farklı düzenlemenin incelenerek bu düzenlemelerin barındırdığı hata ve eksikliklerin incelendiği çalışma için bkz. Ben GREEN, The Flaws of policies requiring human oversight of government algorithms, Computer Law & Security Review, Volume 45, 2022, <https://doi.org/10.1016/j.clsr.2022.105681>.

⁵⁶³ Kaltheuner & Bietti, s.14.

⁵⁶⁴ Kaltheuner & Bietti, s.14.

⁵⁶⁵ Kaltheuner & Bietti, s.14.

⁵⁶⁶ Çalışmanın COMPAS ile ilgili açıklamalar içeren bölümü için bkz. s.60 vd.

işaret etse de, bir yazılım tarafından verilen otomatik karar davanın sonucuna ilişkin belirleyici rol oynayabilecektir⁵⁶⁷. Bununla beraber, otomatik karar alma sisteminin denetlenebilir ve açıklanabilir olması da insan müdahalesinin pratikte bir anlam ifade edebilmesi açısından kritik öneme sahiptir⁵⁶⁸.

Brkan, karar prosedürünün gerekli bir öznesi olarak insanı sürece dahil eden ancak nihai olarak karar alma yetkisini otomatik bir sisteme bırakan şekli bir değerlendirmenin, ilgili kişiye yeterli düzeyde bir koruma sağlayamayacağını belirtmiştir⁵⁶⁹. Brkan’a göre, kararın tamamen otomatik işlemeye dayanmadığının kabul edilebilmesi için, süreçteki insan müdahalesinin, “algoritmik sistemler aracılığı ile oluşturulan kararın esasının değerlendirilmesi ve doğrulanması” şeklinde gerçekleşmesi gerekir⁵⁷⁰. Bu bağlamda, algoritmik sisteme sadece bir destek aracı olarak başvurularak, nihai kararın bir insan tarafından alınması halinde, bu karar GVK Tüzüğü m.22’nin uygulama alanı dışında kalacaktır⁵⁷¹.

Wachter, Mittelstadt ve Floridi, Avrupa Parlamentosu Medeni Haklar, Adalet ve İç İşleri Komitesi tarafından teklif edildiği üzere, maddenin ilgili kısmının “tamamen veya ağırlıklı olarak otomatik işlemeye dayalı kararlar” (*solely or predominantly based on automated processing*) şeklinde değiştirilmesi ya da tamamen veya ağırlıklı olarak otomatik işlemeye dayalı karar almaya ilişkin belirli örnekler verilmesiyle bu belirsizliğin ortadan kaldırılabilceğini belirtmiştir⁵⁷².

29. Madde Çalışma Grubu ilgili rehberinde, veri sorumlularının, veri koruma etki değerlendirmesinde karar alma sürecinde hangi aşamada ve ne ölçüde bir insan müdahalesinin gerçekleştiğini belirtmeleri ve kayıt altına almaları gerektiğini ifade etmiştir⁵⁷³. Kaltheuner ve Bietti ise, kararları veren kişinin

⁵⁶⁷ Kaltheuner & Bietti, s.14.

⁵⁶⁸ Kaltheuner & Bietti, s.13-14.

⁵⁶⁹ Brkan, s.10.

⁵⁷⁰ Brkan, s.10.

⁵⁷¹ Brkan, s.10.

⁵⁷² Wachter & Mittelstadt & Floridi, s.44-45.

⁵⁷³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.21.

kararlara gerçekte ne ölçüde müdahale edebildiğini ve müdahalesinin kararın sonucunu değiştirip değiştirmediğini kayıt altına almanın, veri sorumlusu için karar sürecinde anlamlı bir insan müdahalesi ve gözetimine yer verildiğini göstermenin etkili bir yolu olduğu görüşündedir⁵⁷⁴.

Edwards ve Veale ise, 29. Madde Çalışma Grubu’nun otomatik karar almaya ilişkin rehberini “tamamen otomatik işlemeye dayalı olma” kriterine ilişkin yeterli açıklıkta bilgiye yer verilmediği gerekçesiyle eleştirmiş, Veri Koruma Etki Değerlendirmesi’ne etkili bir araç olarak başvurulabileceğini ancak 29. Madde Çalışma Grubu’nun 2017 yılında yayınlanan ve geçerli bir veri koruma etki değerlendirmesi için kriter sunan ilgili rehberinde 22. madde tahtındaki hak ve yükümlülöklere herhangi bir atıf yapılmamış olmasının bu konuda belirsizliğe neden olduğunu belirtmiştir⁵⁷⁵.

3.1.1.2. Hukuki Veya Benzer Şekilde Önemli Sonuçlar Doğurma

İlgili kişinin 22. madde ile kendisine tanınan korumadan faydalanabilmesi için, söz konusu kararın hukuki ya da benzer şekilde önemli bir etki doğurması gerekmektedir. GVK Tüzüğü’nde hukuki etkinin tanımı yapılmamıştır. Hukuki etki doğuran haller genel olarak, ilgili kişinin hukuki statüsünün değiştirildiği veya hukuki görevlerin yaratıldığı durumlar ile tanımlanabilecektir⁵⁷⁶. İlgili kişi üzerinde bir hukuki etkinin varlığının kabulü için ilgili kişinin hukuki durumu üzerinde, örneğin ilgili kişinin haklarının kısıtlanması gibi bir etkinin varlığı aranacaktır⁵⁷⁷. Kişinin hukuki statüsünü, özgürlük, vatandaşlık ve sosyal güvenlik gibi kamu

⁵⁷⁴ Kaltheuner ve Bietti, s.13.

⁵⁷⁵ Michael VEALE & Lilian EDWARDS, Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, Computer Law & Security Review 34 (2018) 398-404, s.401, <https://www.sciencedirect.com/science/article/pii/S026736491730376X> (Kısaltılmışı “Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling”)

⁵⁷⁶ Veale & Edwards, Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, s.401.

⁵⁷⁷ Wachter & Mittelstadt & Floridi, s.34.

haklarını, sözleşmeden doğan haklarını, özel mülkiyet hakkını etkileyen kararlar bu kapsamda kabul edilebilecektir⁵⁷⁸. 29. Madde Çalışma Grubu’nun ilgili rehberinde, otomatik kararın ilgili kişi hakkında hukuki bir etki doğurduğunun kabulü için, kişinin başkalarıyla ilişki kurma özgürlüğü, bir seçimde oy kullanma veya hukuki işlem başlatma gibi yasal hakları üzerinde veya kişinin hukuki statüsü ya da bir sözleşme tahtındaki hakları üzerinde etki doğurması gerektiği belirtilmiştir. Bu kapsamda kişinin taraf olduğu bir sözleşmenin feshedilmesine, bir seçimde oy kullanamamasına, vatandaşlık başvurusunun reddedilmesine ve sosyal yardım ve hizmetleri alamamasına neden olan kararlar örnek olarak gösterilmiştir⁵⁷⁹.

Otomatik karar alma faaliyeti, ilgili kişi hakkında hukuki etki doğurmasa dahi, “hukuki etkiye benzer şekilde önemli” bir etki doğurması halinde de m.22/1’in alanına girecektir⁵⁸⁰. Maddenin uygulama alanı, ilgili kişi üzerinde “hukuki etkiye benzer şekilde önemli” etki doğuran otomatik kararların da kapsama alınmasıyla genişletilmiştir⁵⁸¹. Kararın ilgili kişi üzerinde doğuracağı etkinin önem derecesine ilişkin öngörülen eşik, “hukuki etkiye benzer şekilde önemli” bir etkidir. İlgili kişi hakkındaki bir karar, kişinin temel haklarını doğrudan etkilemese de diğer menfaatlerini “hukuki etkiye benzer şekilde önemli derecede” etkilediği takdirde 22.maddenin kapsamına girecektir⁵⁸². Ancak hukuki etki doğuran kararların neler olabileceği açıkça tespit edilebilmekteyken, hukuki etkiye benzer şekilde önemli etki doğuran kararların neler olduğunu kesin şekilde belirlemek aynı şekilde kolay değildir⁵⁸³.

⁵⁷⁸ Centre for Information Policy Leadership, Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party’s Guidelines on Automated Individual Decision-Making and Profiling adopted on 3 October 2017, s.6, 1 Aralık 2017, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp_29_guidelines_on_automated_individual_decision-making_and_profiling.pdf.

⁵⁷⁹ Article 29 Working Party, Automated Data is Power and Profiling, s.21.

⁵⁸⁰ Article 29 Working Party, Automated Data is Power and Profiling, s.21.

⁵⁸¹ Malgieri & Comandé, s.16.

⁵⁸² Malgieri & Comandé, s.16.

⁵⁸³ Brkan, s.10; Veale & Edwards, Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, s.401.

GVK Tüzüğü'nün giriş bölümünün 71.paragrafında, kişinin meşru menfaatinin bulunduğu kabul edilebileceği haller genel olarak belirtilmiştir. İlgili kişinin “işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri veya ilgi alanları, güvenilirliği veya davranışları, konumu veya hareketleri ile ilgili hususların analiz edilmesi veya tahmin edilmesini içeren ve ilgili kişi üzerinde hukuki veya benzer şekilde önemli etkiye sahip” otomatik kararların konusu olmama hakkı vardır⁵⁸⁴. Giriş bölümünün 71. paragrafında, “kişinin kredi veya iş başvurusunun insan müdahalesi olmaksızın tamamen otomatik sistemler aracılığıyla değerlendirildikten sonra ret kararı verilmesi” kişinin hayatında önemli etkiye sebep olan kararlara örnek olarak gösterilmiştir⁵⁸⁵. İlgili kişinin bir kredi başvurusunun onaylanması veya bir iş pozisyonuna kabul edilme konusunda yasal bir hakkı söz konusu değildir; ancak kişinin başvurusunun hukuka uygun ve adil bir şekilde değerlendirilmesi ve ayrımcı bir uygulamaya konu edilmemesine ilişkin meşru menfaati bulunur⁵⁸⁶. Dolayısıyla kişinin iş veya kredi başvurusunun olumsuz sonuçlandığı bir otomatik karar, “hukuki etki” kapsamında olmasa bile “hukuki etkiye benzer şekilde önemli etki” doğuran bir karar olarak 22. maddenin kapsamında değerlendirilecektir⁵⁸⁷. Benzer şekilde, kişinin “kişiselleştirilmiş reklam almama hakkı” veya “nöropazarlamaya maruz kalmama hakkı”ndan bahsedilemeyecek olmakla birlikte, kişinin meşru menfaati haksız ticari uygulamaların veya bilişsel manipülasyona konusu olmamayı talep etmesini gerektirebilmektedir⁵⁸⁸.

Kaltheuner ve Bietti, Tüzüğün giriş bölümünün 71. paragrafında “benzer şekilde önemli etki” ye sahip otomatik kararlara ilişkin sınırlı örneğe yer verildiğini, dolayısıyla da söz konusu “önemli etki” nin, ilgili kişinin veya veri sorumlusunun öznel algısına mı bağlı olduğu veya doğası gereği önemli etkiler üreten otomatik karar alma biçimlerini belirlemek için bazı nesnel standartların oluşturulup

⁵⁸⁴ Bkz. GVK Tüzüğü, Giriş Bölümü, 71.Paragraf.

⁵⁸⁵ Bkz. GVK Tüzüğü, Giriş Bölümü, 71.Paragraf.

⁵⁸⁶ Malgieri & Comandé, s.16.

⁵⁸⁷ Wachter & Mittelstadt & Floridi, s.34.

⁵⁸⁸ Malgieri & Comandé, s.16.

oluşturulamayacağını belirsiz olduğunu ifade etmiştir⁵⁸⁹. Wachter, Mittelstadt ve Floridi, 22. maddedeki bu ifadenin kapsamının açıklığa kavuşturulmasını, en azından “önemli etki” nin ilgili kişinin öznel bakış açısından mı yoksa bazı objektif standartlara göre mi belirleneceğinin tanımlanmasını tavsiye etmiştir⁵⁹⁰.

29. Madde Veri Çalışma Grubu’nun ilgili rehberinde belirttiği üzere, ilgili kişiyi bu derece önemli bir şekilde etkilemiş bir otomatik karar faaliyetinden bahsedilebilmesi için, kararın etkilerinin dikkate değer derecede büyük veya önemli olması gerekir⁵⁹¹. Bu çerçevede, ilgili kişinin hayat koşullarını, davranışlarını veya seçimlerini önemli ölçüde etkileyebilecek, ilgili kişi üzerinde uzun süreli veya kalıcı bir etki oluşturabilecek, ilgili kişinin dışlanmasına veya ayrımcılığa maruz kalmasına yol açabilecek kararlar bu kapsamda değerlendirilebilecektir⁵⁹². Çalışma Grubu, neyin “önemli etki” eşiğini karşılamaya yeterli derecede önemli olduğunun kesin kriterler ile belirlenmesinin zor olduğunu ancak aşağıda belirtilen konulardaki otomatik kararların bu kapsamda değerlendirilebileceğini belirtmiştir:

- Kişinin kredi kullanmaya uygunluğu gibi finansal durumunu etkileyen kararlar;
- Sağlık hizmetlerine erişimini etkileyen kararlar;
- Üniversiteye kabul ve benzeri eğitime erişim ile ilgili kararlar;
- Kişinin bir iş imkanından mahrum bırakılması veya ciddi ölçüde dezavantajlı durumda kalmasına neden olan kararlar⁵⁹³.

Benzer şekilde, kişiye vize verilmesi veya bir ülkeye giriş hakkı tanınması, ikamet, vatandaşlık hakkı tanınması, kişinin vergi indirimi için belirli bir vergi diliminde sınıflandırılması, kişinin ikramiye ödemesine hak kazanması veya terfi ettirilmesi,

⁵⁸⁹ Kaltheuner & Bietti, s.11.

⁵⁹⁰ Wachter & Mittelstadt & Floridi, s.45.

⁵⁹¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.21.

⁵⁹² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.21.

⁵⁹³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.22.

enerji hizmetlerine erişimi ve tarifelerin belirlenmesine ilişkin otomatik kararlar da bu kapsamda kabul edilebilecektir⁵⁹⁴.

3.1.1.3. Çevrimiçi Davranışsal Reklamcılık Faaliyetleri

Çevrimiçi davranışsal reklamcılık alanında, reklamların olabildiğince belirli bir hedef kitleye ulaşmasını sağlamak için tasarlanan hedefleme teknolojileri kullanılmaktadır. Çeşitli izleme teknolojileri ile farklı kaynaklardan toplanan veriler ile bizzat kullanıcı tarafından sağlanan verilerin analiz edilmesi suretiyle tahmine dayalı profiller oluşturulmaktadır. Böylece belirli ürünlerin bazı kişileri hariç tutarak hedef kitleye sunulması veya aynı ürünün farklı kişilere farklı fiyattan sunulması mümkün hale gelmektedir. Bu modern reklamcılık teknikleri, bireyin mahremiyetini ihlal etme potansiyeline sahip olmakla birlikte, yeterli yasal korumaya sahip olmayan savunmasız gruplara karşı hukuka aykırı şekilde ayrımcılık yapılmasına neden olmaktadır⁵⁹⁵. Giderek daha fazla otomatikleştirilmiş veri işleme süreçlerine dayanan ve tamamen otomatik işlemeye dayalı karar alma içeren çevrimiçi davranışsal reklamcılık faaliyetleri karşısında ilgili kişinin GVK Tüzüğü'nün 22. maddesi kapsamında kendisine tanınan korumadan faydalanıp faydalanamayacağı konusunda farklı görüşler bulunmaktadır.

29. Madde Veri Çalışma Grubu, kişiyi önemli derecede etkileyen kararların değerlendirmesinde, ilgili kişinin özel durumunun da dikkate alınması gerektiği, bazı kişilerin üzerinde önemli bir etkiye sahip olmayan otomatik karar alma faaliyetlerinin, azınlık grupları veya savunmasız veya korumasız kişiler gibi toplumun belirli grupları üzerinde önemli etkilere neden olabileceği görüşündedir⁵⁹⁶. Çalışma Grubu'nun verdiği örnek üzerinden somutlaştırmak gerekirse, finansal sıkıntı içinde olan kişiler sürekli olarak yüksek faizli kredi

⁵⁹⁴ Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Automated Individual Decision – Making and Profiling adopted on 3 October 2017, s.6,

⁵⁹⁵ Sandra WACHTER, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising, Berkeley Technology Law Journal, Vol. 35:2, s. 4-5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639.

⁵⁹⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.22.

tekliflerine yönelik reklamlara maruz kalmaları sonucunda bu kredi tekliflerine başvurarak daha da borçlanabileceklerdir⁵⁹⁷. Kaltheuner ve Bietti, Çalışma Grubu'nun rehberindeki bu açıklamalarının otomatik karar alma faaliyeti ile hedeflenen ilgili kişinin, savunmasız veya korumasız olduğuna kim tarafından ve hangi kıstasa göre karar verileceği sorularını gündeme getirdiğini, profillemeye faaliyetlerinin bireyleri önemli ölçüde etkilememesini sağlamak üzere nesnel bir standart belirlenmesinin veri sorumlusunun yükümlülüğü olduğunu belirtmiştir⁵⁹⁸. Nesnel bir standart belirlemenin zorluğu göz önüne alındığında, davranışsal reklamlardan olumsuz etkilenen kişi ve gruplara ilişkin örnekler çoğaltılabilecektir⁵⁹⁹. Görünüşleri hakkında kaygı duyan ve sürekli diyet ya da estetik operasyonlar ile ilgili reklamların hedefinde olan kadınların da finansal sıkıntı içinde olan kişiler gibi bu reklamlara karşı savunmasız durumda olduğu savunulabilecektir⁶⁰⁰.

Brkan, davranışsal reklamcılık faaliyetlerinin hangi hallerde ilgili kişi üzerinde önemli etkiler doğurduğunun belirlenebilmesinin neredeyse imkansız olduğunu belirtmiştir. Zira ilgili kişi bu tür reklamları görmezden gelir ve takip etmezse, söz konusu reklamın ilgili kişiyi önemli ölçüde etkilediğini iddia etmek zordur. Öte yandan, bu reklamlar ilgili kişinin satın alma kararlarının sistematik şekilde şekillendirilmesinde rol oynadığı takdirde, önemli etkinin varlığından bahsedilebilecektir. Bu noktada, önemli etki kriterinin yerine getirilmesi için, profillemeye ile ilgili kişinin eylemi arasında bir neden sonuç ilişkisi gerekli olup olmadığı sorusu gündeme gelmektedir. Brkan'a göre, bir nedensel ilişkinin gerekliliği, sadece belirli davranışsal reklam faaliyetlerinin ilgili kişi üzerinde önemli bir etkiye neden olduğunun kabul edilmesine neden olacak ve önemli etki değerlendirmesini oldukça karmaşık bir hale getirecektir. Brkan, bu gibi durumlarda önemli etkinin değerlendirmesinde alternatif olarak, ilgili reklamın

⁵⁹⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.22.

⁵⁹⁸ Kaltheuner & Bietti, s.11.

⁵⁹⁹ Kaltheuner & Bietti, s.11.

⁶⁰⁰ Kaltheuner & Bietti, s.11.

hedef aldığı gerçek tüketici yerine ortalama bir tüketicinin dikkate alınmasını önermektedir⁶⁰¹.

29. Madde Çalışma Grubu'nun ilgili rehberinde, pek çok tipik çevrimiçi davranışsal reklamcılık faaliyetinde, profilemeye dayalı reklamcılık faaliyetlerin bireyler üzerinde hukuki etkiye benzer şekilde önemli bir etki doğurmayacağı belirtilmiş, internet üzerinden satış yapan bir moda markasının, belirli bir bölgede belirli yaş aralığındaki modaya ve belirli giyim eşyalarına ilgi duyması muhtemel kişileri hedefleyerek göstereceği reklamlar buna örnek olarak gösterilmiştir⁶⁰². Öte yandan rehberde, çevrimiçi davranışsal reklamcılık faaliyetlerinin her bir olay özelinde, farklı internet siteleri, cihazlar ve hizmetler üzerinden kişinin izlenmesi de dahil olmak üzere profileme faaliyetinin bireyin hayatına ne ölçüde müdahale ettiği, ilgili kişinin beklenti ve istekleri, reklamın ilgili kişiye ulaşma şekli veya kişilerin zayıflıklarının reklam hedeflemesinde kullanılması gibi belirli şartlarçerçevesinde yapılacak değerlendirmeye göre söz konusu reklamların ilgili kişinin hayatında önemli şekilde etkiye sahip olduğu sonucuna varılabileceği ifade edilmiştir⁶⁰³. Kaltheuner ve Bietti, bu kriterlere bakıldığında, Çalışma Grubu'nun davranışsal reklamların çoğunlukla bireyler üzerinde önemli bir etkiye sahip olmadığı yönündeki değerlendirmesine katılmadıklarını belirterek, Çalışma Grubu'nun açıklamalarını, rehberdeki örneğin günümüzdeki davranışsal reklamcılık uygulamalarını doğru şekilde yansıtmadığı gerekçesiyle eleştirmiştir⁶⁰⁴. Kaltheuner ve Bietti bu eleştirisini üç farklı gerekçeye dayandırmıştır⁶⁰⁵. İlk olarak, çevrimiçi davranışsal reklamcılık çoğunlukla bireyin hayatına son derece müdahaleci şekilde gerçekleştirilen profileme faaliyetlerine dayanmaktadır⁶⁰⁶. Facebook reklamlarının etkililiğinin, reklam verenin hedef kitlesini tek bir kişiye kadar indirgeyebilmesi için, reklam hedefleme seçeneklerinin, davranış, demografik bilgi ve coğrafi konum verilerinin

⁶⁰¹ Brkan, s.10-11.

⁶⁰² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.22.

⁶⁰³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.22.

⁶⁰⁴ Kaltheuner & Bietti, s.11-12.

⁶⁰⁵ Kaltheuner & Bietti, s.11-12.

⁶⁰⁶ Kaltheuner & Bietti, s.12.

kombinasyonlarını kullanma imkanı sağlamasına bağlı olduğu belirtilmektedir⁶⁰⁷. 2017 yılında yayınlanan bir araştırma ise, insan psikolojisi esas alınarak gerçekleştirilen hedefli reklamcılığın, “bireylerin psikolojik özelliklerine göre gösterilen cezbedici içeriklerin, tıklamalar ve satın almalarla ölçülebilen davranışlarını önemli ölçüde değiştirdiğini” ortaya koymuştur⁶⁰⁸. Nitekim Kaliforniya Üniversitesi tarafından yürütülen bir araştırmada, bilgisayarların kişinin kişiliğini değerlendirmede aile üyelerinden ve arkadaşlarından daha iyi olduğu keşfedilmiştir⁶⁰⁹. İkincisi, tüketicilerin büyük çoğunluğu, profillemenin nasıl gerçekleştiği ve profillemeye sonucu yeni kişisel verilerin ortaya çıkabileceğine ilişkin oldukça az bilgi sahibidir ve genellikle de profilinin çıkarıldığının farkında dahi değildir⁶¹⁰. Dolayısıyla, tüketiciler belirli bir reklamın neden kendilerini hedef aldığını çoğunlukla anlayamazlar. Öte yandan, davranışsal reklamcılık faaliyetlerinin bireylerin ayrımcılığa uğramasına yol açma potansiyeline sahip olduğunu ortaya koyan birçok çalışma mevcuttur⁶¹¹. Profilinin çıkarıldığından ve bu profile dayanılarak belirli reklamlara maruz kaldığından haberi olmayan ve bu konuda bir farkındalığa sahip olmayan bireylerin, ayrımcılığa uğradıklarını tespit edebilmeleri de mümkün olmayacaktır⁶¹². Kaltheuner ve Bietti, belirtilen

⁶⁰⁷Larry KIM, 5 Ridiculously Powerful Facebook Ad Targeting Strategies, <https://www.wordstream.com/blog/ws/2015/01/28/facebook-ad-targeting>.

⁶⁰⁸ Kaltheuner & Bietti, s.12. İlgili araştırma için bkz. S. C. MATZ & M. KOSINSKI & G. NAVE & D.J. STILLWELL, Psychological Targeting as an Effective Approach to Digital Mass Persuasion, Proceedings of the National Academy of Sciences (PNAS), 28 Kasım 2017, Vol.114, No.48, <https://www.pnas.org/doi/pdf/10.1073/pnas.1710966114>.

⁶⁰⁹ Wu YOUYOU & Michal KOSINSKI & David STILLWELL, Computer-based Personality judgements are more accurate than those made by humans, Proceedings of the National Academy of Sciences (PNAS), 12 Ocak 2015, Vol.112, No.4.

⁶¹⁰ Kaltheuner & Bietti, s.12.

⁶¹¹ 2015 yılında Carnegie Mellon Üniversitesi tarafından yapılan bir araştırmada, Google’ın çevrimiçi reklamcılık sisteminin, yüksek gelirli işler ile ilgili reklamları kadınlara gösterdiğinden çok daha sık bir şekilde erkeklere gösterdiği tespit edilmiştir. Privacy International, s. 12. İlgili araştırma için bkz. Amit DATTA & Michael Carl TSCHANTZ & Anupam DATTA, Automated Experiments on Ad Privacy Settings, <https://arxiv.org/abs/1408.6491>. Son çalışmalarda, tarafsızlık ve önyargı içermeyecek şekilde tasarlanan, bilim, teknoloji, mühendislik ve matematik gibi alanlardaki iş ilanlarının Facebook Ads, Google Ads, Instagram ve Twitter gibi büyük platformlarda, kadınlara kıyasla erkeklere daha fazla gösterildiği ortaya çıkmıştır. L. Elisa CELIS & Anay MEHROTRA & Nisheeth K. VISHNOI, Toward Controlling Discrimination in Online Ad Auctions, s.3, <https://www.semanticscholar.org/paper/Toward-Controlling-Discrimination-in-Online-Ad-Celis-Mehrotra/3dd26b108eb2d246219e9a69e0ce36cd0e5e8dfb>.

⁶¹² Kaltheuner & Bietti, s.12.

gerekçelerle, “hukuki” veya “benzer şekilde önemli” etkiler hakkında öznel değerlendirmelerden kaçınılması gerektiğini ifade etmiştir⁶¹³.

3.1.1.4. Tamamen Otomatik İşlemeye Dayalı Karar Alma Faaliyetlerine İzin Verilen İstisnai Haller

GVK Tüzüğü’nün 22. maddesinin ikinci fıkrasında, 22. madde kapsamına giren tamamen otomatik işlemeye dayalı karar alma faaliyetlerine izin verilen haller düzenlenmiştir. Buna göre, “(i) otomatik karar alma faaliyetinin, ilgili kişi ve veri sorumlusu arasında bir sözleşmenin ifası için gerekli olması; (ii) veri sorumlusunun tabi olduğu ve ilgili kişinin hak ve özgürlükleri ile meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de hüküm altına alındığı Avrupa Birliği veya üye devlet mevzuatında otomatik karar alma faaliyetine izin verilmesi; (iii) kararın ilgili kişinin açık rızasına dayanması” hallerinden birinin geçerli olması durumunda, veri sorumlusu ilgili kişi hakkında profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma gerçekleştirebilecektir⁶¹⁴. Bununla beraber, veri işleme faaliyeti GVK Tüzüğü’nün 22/2(a) veya 22/2(c) maddelerinde düzenlenen istisnai hallerden birine dayandığı takdirde dahi, veri sorumlusu ilgili kişilerin hak ve özgürlüklerini ve meşru menfaatlerini korumak için uygun tedbirleri almakla yükümlüdür⁶¹⁵. Belirtilen istisnai haller ilgili çalışmanın “Hukuka Uygunluk Sebepleri” başlıklı bölümünde incelenecektir.

3.1.1.5. Özel Nitelikli Kişisel Veriler

GVK Tüzüğü’nün 22. maddesi tahtında düzenlenen profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyeti kapsamında özel nitelikli kişisel verilerin işlenebilmesi, ancak işlemenin GVK Tüzüğü’nün 22. maddesinin ikinci fıkrasında belirtilen hallerden birine dayanması, Tüzüğün 9. maddesinin (a) veya (g) bendinin uygulanabilir olması ve veri sorumlusunun ilgili

⁶¹³ Kaltheuner & Bietti, s.13.

⁶¹⁴ Bkz. GVK Tüzüğü, m.22/2.

⁶¹⁵ Bkz. GVK Tüzüğü, m.22/3.

kişinin hak ve özgürlükleri ile meşru menfaatlerini korumak için uygun tedbirleri alması halinde mümkündür⁶¹⁶. Belirtilen düzenlemeler uyarınca, (i) ilgili kişinin açık rızasının bulunması veya (ii) gözetilen amaçla orantılı, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hak ve menfaatlerinin güvence altına alınmasını sağlayacak belirli tedbirleri hüküm altına almış Birlik veya üye devlet hukuku gereğince kayda değer şekilde kamu yararı ile ilişkili nedenlerden ötürü işleme faaliyetinin gerekmesi halinde profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetleri kapsamında özel nitelikli kişisel veriler işlenebilecektir⁶¹⁷. Bu şartların karşılanmadığı hallerde, GVK Tüzüğü m.22 kapsamına giren profillemeye de dahil tamamen otomatik işlemeye dayalı karar alma faaliyetleri kapsamında özel nitelikli kişisel verilerin işlenmesi yasaktır. Belirtilmelidir ki, özel nitelikli kişisel verilerin işlenmesine ilişkin düzenlemeler sadece doğrudan ilgili kişiden edinilen özel nitelikli kişisel verilere değil, aynı zamanda türetilen veya çıkarılan veriler açısından da geçerlidir. Zira profillemeye ve otomatik karar alma faaliyetlerinde, özel nitelikli olmayan kişisel verilerin işlenmesi suretiyle, kişinin sağlığı, siyasi görüşü, dini inancı ve cinsel yönelimi gibi özel nitelikli kişisel verileri çıkarılabilmektedir.

3.1.1.6. Uygun Tedbirler

Tüzüğün 22. maddesinin üçüncü fıkrası uyarınca, otomatik karar alma faaliyetinin ilgili kişinin açık rızasına dayanması veya bir sözleşmenin kurulması veya ifası için gerekli olması halinde veri sorumlusu, ilgili kişinin hakları, özgürlükleri ve meşru menfaatlerini korumak için uygun tedbirleri almakla; bu kapsamda ilgili kişiye en azından “(i) karar alma sürecine insan müdahalesi talep etme (*“right to obtain human intervention”*) , (ii) karara ilişkin kendi görüş ve bakış açısını beyan etme (*“right to express his or her point of view”*) ve (iii) ilgili karara itiraz etme (*“right to contest the decision”*) hakkı” tanımakla yükümlüdür⁶¹⁸.

⁶¹⁶ Bkz. GVK Tüzüğü, m.22/4.

⁶¹⁷ Bkz. GVK Tüzüğü, m.9/2 (a), m.9/2(g).

⁶¹⁸ Bkz. GVK Tüzüğü, m.22/3.

Tüzük m.22/3'e paralel şekilde Tüzüğün giriş bölümünün 71. paragrafında, bu tür bir işleme halinde veri sorumlusunun ilgili kişiye, işleme faaliyeti ile ilgili belirli bilgilerin sağlanması, insan müdahalesi talep etme, kendi bakış açısını beyan etme, karara ilişkin bir açıklama yapılmasını talep etme haklarının tanınması da dahil olmak üzere uygun tedbirleri almakla yükümlü olduğu belirtilmiştir⁶¹⁹. Tüzüğün bu düzenlemesiyle tamamen otomatik işlemeye dayalı karar alma faaliyetlerine izin verilen hallerde, veri sorumlularının uygun tedbirleri almalarını sağlamak suretiyle, hatalı, ayrımcı veya ilgili kişinin hak ve çıkarlarına aykırı kararların önlenmesi amaçlanmaktadır⁶²⁰. 29. Madde Çalışma Grubu, bu düzenlemenin, kişisel verilerin GVK Tüzüğü'nün genel yapılanması üzerinde önemli bir etkisi bulunan şeffaflık ilkesine uygun şekilde işlenmesine olan ihtiyacı vurguladığını belirtmiştir. Zira ilgili kişi, söz konusu kararın ne şekilde ve neye dayanılarak alındığını tam olarak anlayabildiği müddetçe bu karara itiraz edebilecek ve karara karşı görüşlerini ifade edebilecektir⁶²¹. Wachter ve Mittelstadt, Tüzük ile hüküm altına alınan bu hakların, ilgili kişilerin tamamen otomatik işlemeye dayalı kararları incelemelerine ve sorgulamalarına imkan tanımak için, sadece prosedürel veri kontrolü ve yönetiminin ötesine geçildiğine işaret ettiği ve ayrıca, Tüzüğün 22. maddesinin, ilgili kişinin kendisi hakkındaki çıkarımlara ilişkin çıkarlarının gözetildiği bir hüküm olması itibarıyla, girdi verilerinin yönetimine odaklanan diğer düzenlemelerden ayrıldığı görüşündedir⁶²².

Brkan'a göre, ilgili kişiye karar sürecine insan müdahalesi talep etme hakkı sunularak, sürece bir insan dahil edilmek suretiyle ilgili kararın "otomatik" olma özelliğinin ortadan kaldırılması amaçlanmaktadır⁶²³. Bireysel kredi başvurusunun dijital bankacılık kanallarıyla iletildiği ve başvurunun anlık olarak algoritmalar aracılığı ile değerlendirilerek sonucunun müşteriye iletildiği durumda, başvurunun reddedilmesi halinde müşterinin başvurusunun bu sefer bir banka yetkilisi

⁶¹⁹ GVK Tüzüğü, Giriş Bölümü, 71.Paragraf.

⁶²⁰ Brkan, s.13.

⁶²¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.27.

⁶²² Wachter & Mittelstadt, s.78-79.

⁶²³ Brkan, s.13.

tarafından tekrar değerlendirilmesini talep etmesi bu hakkın kullanımına bir örnek olarak gösterilebilecektir. Öte yandan veri sorumlusu, ilgili kişinin bu hakkını kullanabilmesi için elverişli bir ortam sağlamalıdır⁶²⁴. Karar sürecine insan müdahalesinin sağlanması ile ilgili olarak, müdahalenin kararı değiştirmek için uygun yetki ve yeteneğe sahip bir kişi tarafından gerçekleştirilmesi ve bu kişi tarafından ilgili kişinin sağladığı tüm ek bilgiler de dahil olmak üzere otomatik karar alma faaliyetine esas alınan tüm verilerin kapsamlı şekilde değerlendirilmesi önem teşkil etmektedir⁶²⁵. Tüzük'te ilgili kişiye karara ilişkin kendi görüş ve bakış açısını beyan etme hakkı tanınmış olmakla birlikte, ilgili kişinin kendi görüşünü beyan etmesinin hukuki sonuçlarının ne olacağına ilişkin bir düzenlemeye yer verilmemiştir⁶²⁶.

İlgili kişiye tanınan bir diğer hak ise karara itiraz etme hakkıdır. Brkan'a göre, ilgili kişinin karara itiraz etmesi halinde, itirazı kimin değerlendireceği ve karar vereceği belirsizdir⁶²⁷. Wachter, Mittelstadt ve Russell tarafından ileri sürüldüğü üzere, itiraz hakkının nasıl kullanılacağı, Tüzüğün 22/3 maddesinin nasıl yorumlandığına göre farklılık arz edecektir⁶²⁸. Zira Tüzük m.22/3, ilgili kişinin bu madde ile hüküm altına alınan hakların hepsini birlikte kullanması gerektiği şeklinde yorumlanabileceği gibi, bu hakların ayrı ayrı kullanılmasına izin verecek şekilde de yorumlanabilecektir⁶²⁹. Wachter ve diğerleri, bu çerçevede, itiraz hakkının dört farklı şekilde kullanılabileceği görüşündedir⁶³⁰. Buna göre, hakların hepsinin birlikte kullanılması gerektiği senaryoda, yeni bir kararın alınması için insan müdahalesi gerekecektir⁶³¹. Bu durumda, algoritma desteği olmaksızın tamamıyla bir insan tarafından yeni bir karar alınması halinde artık Tüzüğün 22.

⁶²⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.27.

⁶²⁵ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.27.

⁶²⁶ Brkan, s.13.

⁶²⁷ Brkan, s.13.

⁶²⁸ Sandra WACHTER & Brent MITTELSTADT & Chris RUSSELL, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, Harvard Journal of Law & Technology Volume 31, Number 2 Spring 2018, 842-887, s.873, <https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>.

⁶²⁹ Wachter & Mittelstadt & Russell, s.873.

⁶³⁰ Wachter & Mittelstadt & Russell, s.873.

⁶³¹ Wachter & Mittelstadt & Russell, s.873.

maddesi kapsamına giren bir otomatik kararın varlığından söz edilemeyecektir⁶³². Alternatif olarak, ilgili kararın, algoritmik karar modelinin değerlendirmesi ve/veya ilgili kişinin itirazları da gözetilerek bir insan tarafından alınması sağlanabilecektir⁶³³. Her iki durumda da artık tamamen otomatik işlemeye dayalı karar almanın kriterleri oluşmayacağından, ilgili kişi yeni kararlar karşısında m.22/3 tahtındaki haklardan faydalanamayacaktır⁶³⁴. Bir diğer alternatif ise, girdi verisinin ve işlemenin bir insan tarafından incelenmesi ve yeni kararın tamamen bir algoritmik sistem tarafından verilmesidir⁶³⁵. Bu durumda ilgili kişi, m.22/3 tahtındaki haklarını kullanabilecektir⁶³⁶. Bu hakların ayrı ayrı kullanılabilmesi ve böylece ilgili kişinin insan müdahalesini talep etmeden veya kendi görüşünü beyan etmeksizin sadece karara itiraz hakkını kullanabileceğinin kabul edildiği senaryoda ise, yeni karar herhangi bir şekilde insan müdahalesi olmaksızın verilebilecektir⁶³⁷. Bu karar “tamamen otomatik işlemeye dayalı” kabul edileceğinden, ilgili kişi bu karara karşı da m.22/3 kapsamında itiraz hakkını kullanabilecektir⁶³⁸. Wachter ve diğerleri, en makul seçeneğin hakların ayrı ayrı kullanılması olduğunu ileri sürmüştür. Zira ilgili kişi, kendisi hakkındaki bir otomatik kararı yeterince anlayamadığı veya yanlış anladığı hallerde görüşlerini beyan etme veya insan müdahalesi talep etme haklarına başvurmak isteyebilecekse de bu haklarına başvurulması, özellikle itiraz süreci maliyetli olacaksa veya başarı olasılığının düşük olduğu öngörülüyorsa, karara itiraz ile sonuçlanmayabilecektir⁶³⁹.

Wachter ve Mittelstadt, çıkarımlara dayalı otomatik kararlara itiraz hakkının, karar alma faaliyetleri hakkında temel standartlar (*decision-making standards*) oluşturulmadan fiilen uygulama alanı bulup bulmayacağı sorusunu değerlendirmiştir⁶⁴⁰. Buna göre, burada bahsi geçen karar alma standartları, veri

⁶³² Wachter & Mittelstadt & Russell, s.873.

⁶³³ Wachter & Mittelstadt & Russell, s.873.

⁶³⁴ Wachter & Mittelstadt & Russell, s.873.

⁶³⁵ Wachter & Mittelstadt & Russell, s.873.

⁶³⁶ Wachter & Mittelstadt & Russell, s.873.

⁶³⁷ Wachter & Mittelstadt & Russell, s.873.

⁶³⁸ Wachter & Mittelstadt & Russell, s.873.

⁶³⁹ Wachter & Mittelstadt & Russell, s.873, Dipnot 169.

⁶⁴⁰ Wachter & Mittelstadt, s.78-81.

sorumlusunun karar alma sürecini tamamen açıklanmasını gerektirmez; bunun yerine ilgili kişiye söz konusu prosedürlerin takip edilip edilmediğini tayin edebilmesi için gerekli olan karar alma adımlarının detaylarını içeren kısıtlı bir açıklama talep edilebilmesine zemin sağlar⁶⁴¹. Bu bağlamda, örneğin, bir iş başvurusunda (veya kredi başvurusu) bulunan kişi, işe alım kararının (veya kredi kararının) etnik köken gibi korunan bir özelliğe dayandırılmaması gibi belirli standartların takip edilmesine ilişkin hak iddia edebilecektir; zira bunun yapılmaması ayrımcılık teşkil etmektedir⁶⁴². Her ne kadar karara itiraz hakkı ilgili kişiye profillemeye de dahil tamamen otomatik işlemeye dayalı karar alma faaliyetleri karşısında sağlanan korumayı güçlendiriyor gibi görünse de ilgili kişinin itirazının, kararın geçersiz kılınması veya değiştirilmesinin sağlanması suretiyle başarılı olabilmesi için, ilgili karar ile karar alma konusunda uygulamadaki bir hukuki veya etik standartın ihlal edilmiş olması ve itirazın ihlal edilen standart ekseninde gerçekleştirilmesi gerekir⁶⁴³. Bu tür standartlar oluşturulmadığı müddetçe, karara itiraz eden ilgili kişi ancak girdi verisinin hatalı veya eksik olması ya da kişisel verilerin işlenmesine hakim olan ilkelerin ihlal edilmesi halinde bir sonuç elde edebilecektir⁶⁴⁴. Kararın arkasındaki mantık veya kararın dayandığı parametrelere itiraz edilebilmesi için, karar alma süreçlerinin içeriği veya sonuçlarıyla ilgili standartlar öngörmeyen veri koruma kanununun dışında, otomatik karar alma faaliyetleri özelinde, örneğin ayrımcılığı önlemeyi amaçlayan standartlar gibi tamamlayıcı nitelikte standartların belirlenmiş olması önem arz etmektedir⁶⁴⁵. Bu bağlamda 22. madde tahtında düzenlenen itiraz hakkı, yanlış veya eksik girdi verilerinin analiz edilmesi suretiyle gerçekleştirilen çıkarımlara dayanan kararların veya profillerin düzeltebilmesi açısından sadece usuli bir hak teşkil eder⁶⁴⁶. İlgili sektör özelinde karar alma faaliyetine ilişkin standartlar veya veri koruma kanunundaki düzenlemeler ihlal edilmediği müddetçe, veri sorumlularının çıkarımlara dayanan otomatik kararları düzeltmekle yükümlü tutulmaları mümkün

⁶⁴¹ Wachter & Mittelstadt, s.11-12.

⁶⁴² Wachter & Mittelstadt, s.11-12.

⁶⁴³ Wachter & Mittelstadt, s.79.

⁶⁴⁴ Wachter & Mittelstadt, s.80.

⁶⁴⁵ Wachter & Mittelstadt, s.80.

⁶⁴⁶ Wachter & Mittelstadt, s.80.

görünmemektedir⁶⁴⁷. Bu çerçevede, veri sorumlusunun kararda esas alınan parametreleri ilgili kişiye karşı meşrulaştırmasına gerek bulunmayacak, dolayısıyla, itiraz hakkı tek başına ilgili kişiye yeterli bir koruma sağlamayacaktır⁶⁴⁸.

29. Madde Çalışma Grubu ilgili rehberinde, belirtilen tedbirler kapsamında, veri sorumlusunun ilgili otomatik kararda herhangi bir önyargı olup olmadığını kontrol edebilmesi için, işlemeye konu edilen veri setleri üzerinde periyodik değerlendirmeler yapılması ve veri setleri arasındaki korelasyonlara gereğinden fazla güvenilmesi hali de dahil olmak üzere her türlü önyargı unsurunun tespit edilmesine yönelik araçlar geliştirilmesi, algoritmaların denetlenmesini sağlayan sistemlerin kurulması ve profillemeye de dahil olmak üzere otomatik karar almanın doğruluğunun ve uygunluğunun gözden geçirilmesi gerektiğini vurgulamıştır⁶⁴⁹.

29. Madde Çalışma Grubu'nun ilgili rehberinde, veri sorumlularının m.22 tahtındaki profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetlerinde alınacak tedbirler kapsamında dikkate almaları için bazı iyi uygulama önerileri sunulmuştur⁶⁵⁰:

- İlgili kişilere adil davranıldığığının ve özel nitelikli kişisel verilerin işlenmesi bağlamında veya başka bir şekilde ayrımcılığa uğramadıklarının temin edilmesi için sistemlerin periyodik olarak kalite güvence kontrollerinin gerçekleştirilmesi,
- Yapay öğrenme sistemleri tarafından kullanılan ve geliştirilen algoritmaların gerçekten amacına uygun şekilde çalıştığığının ve ayrımcı, hatalı veya haksız sonuçlar üretmediğinin kanıtlanması için test edilmesi (algoritmik denetim),
- Profillemeye dayalı karar almanın bireyler üzerinde yüksek bir etkiye sahip olduğu hallerde, bağımsız bir “üçüncü taraf” denetimi için, denetçiye

⁶⁴⁷ Wachter & Mittelstadt, s.80-81.

⁶⁴⁸ Wachter & Mittelstadt, s.80-81.

⁶⁴⁹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

⁶⁵⁰ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.32.

algoritmanın veya yapay öğrenme sisteminin nasıl çalıştığı hakkında gerekli tüm bilgilerin sağlanması,

- Üçüncü kişi algoritmaları için denetim ve testlerin gerçekleştirildiğinin ve algoritmanın kararlaştırılan standartlarla uyumlu olduğunun sözleşme ile güvence altına alınması,
- Profiller ve profilleri oluştururken veya uygularken kullanılan kişisel veriler için saklama sürelerinin açık şekilde belirlenmesi amacıyla, veri minimizasyonu için özel önlemlerin alınması,
- Profillemeye bağlamında anonimleştirme veya takma ad kullanma tekniklerinin kullanılması,
- İlgili kişinin kendi bakış açısını ifade etmesine ve karara itiraz etmesine izin verme yollarının belirlenmesi,
- Belirli durumlarda, örneğin, otomatik kararın ilgili kişiye bildirildiği noktada bir temyiz incelemesine imkan sağlanması gibi, insan müdahalesi için bir mekanizma oluşturulması ve bu inceleme için mutabık kalınan süre ve ilgili kişinin sorularını yöneltebileceği bir iletişim noktasının belirlenmesi,
- İşleme faaliyetleri için belgelendirme mekanizmalarının kurulması,
- Yapay öğrenme içeren süreçlerin denetlenmesini sağlamak için davranış kurallarının geliştirilmesi,
- Profillemeye amacıyla kullanılan çeşitli uygulamaların, topluma potansiyel fayda ve zararlarının değerlendirilebilmesi için etik kurallarının oluşturulması.

3.1.1.7. Çocukların Profillenmesi

GVK Tüzüğü'nde, 16 yaşından küçük çocukların kişisel verilerinin işlenmesine ilişkin veri sorumlularına bazı ilave yükümlülükler getirilmek suretiyle çocukların kişisel verilerine özel bir koruma atfedilmiştir⁶⁵¹. Tüzüğün giriş bölümünün 38. paragrafında, çocukların kişisel verilerinin işlenmesinden doğabilecek riskler, sonuçlar ve güvenceler ile kişisel verilerinin işlenmesi nedeniyle sahip oldukları haklara ilişkin farkındalıklarının yetişkin bireylere kıyasla daha az olmasına bağlı olarak özel bir korumaya gereksinim duydukları belirtilmiştir. Bu bağlamda özellikle (i) çocuklara pazarlama yapılması veya çocuklara ilişkin kullanıcı profilleri oluşturulması ve (ii) çocuğun doğrudan kendisine sunulan hizmetlerden yararlandığı sırada kişisel verilerinin toplanması amaçlarıyla çocukların kişisel verilerinin kullanılması durumunda, çocuklara özel bir koruma sağlanması gerekmektedir⁶⁵².

Tüzüğün 22. maddesinde, çocuklara ilişkin bir düzenlemeye yer verilmemiştir. Bu durum, 22. maddenin yetişkinler ve çocuklar açısından aynı şekilde uygulanacağını ve geçerli olduğunu göstermektedir. Tüzüğün 22. maddesi, otomatik kararın çocuklar üzerinde hukuki veya benzer şekilde önemli bir etkisinin bulunmaması halinde, veri sorumlularının profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetleri kapsamında çocuklara ait kişisel verileri işlemelerinin önünde bir engel teşkil etmemekle birlikte, çocuklar ile ilgili otomatik karar alma faaliyetleri, çocuğun seçimlerini ve davranışlarını etkileyebilme potansiyeline sahip olduğundan, bu seçim ve davranışların doğasına bağlı olarak çocuklar üzerinde hukuki veya benzer şekilde önemli etki doğurduğu kabul edilebilecektir⁶⁵³.

29. Madde Çalışma Grubu'nun ilgili görüşünde, çocukların özellikle çevrimiçi ortamda yetişkin bireylere göre toplumun daha savunmasız bir grubunu

⁶⁵¹ Bkz. GVK Tüzüğü, m.8.

⁶⁵² Bkz. GVK Tüzüğü, Giriş Bölümü, 38.Paragraf.

⁶⁵³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.29.

temsil ediyor oldukları ve çevrimiçi davranışsal reklamcılıktan daha kolay etkilenebildikleri göz önüne alınarak profillemeye faaliyetlerine konu edilmemeleri gerektiği belirtilmiştir⁶⁵⁴. Günümüzde çocukların yoğun ilgi gösterdiği çevrimiçi oyunlarda çocukların profillemesi suretiyle, algoritmanın oyuna para harcama olasılığının daha yüksek olduğu çıkarımında bulunduğu oyuncular hedeflenerek daha kişiselleştirilmiş reklamlar gösterilmektedir. Ancak çocukların yetişkinlere kıyasla bu tür pazarlama faaliyetlerinin hangi amaçla gerçekleştirildiğini ve davranışsal reklamcılığın seçim ve davranışları üzerindeki etkilerini ve sonuçlarını kavrama kapasitelerinin sınırlı olması, çocukların kişisel verilerinin Tüzük m.22 işlenmesi açısından önemli bir risk oluşturmaktadır⁶⁵⁵. Bu bağlamda, çevrimiçi davranışsal reklamcılık faaliyetleri kapsamında gerçekleştirilen tamamen otomatik işlemeye dayalı karar almanın, çocuk açısından hukuki etkiye benzer şekilde önemli bir etki doğurup doğurmadığına ilişkin yapılacak değerlendirmede, ilgili reklamların gösterilmesi ile çocuğun hangi seçim ve davranışlarının etkilenmesinin hedeflendiği, bunların çocuğu nasıl etkileyebileceği ve çocuğun davranışsal reklamcılık faaliyetleri karşısında yetişkin bir bireye göre daha savunmasız olduğu göz önüne alınmalıdır⁶⁵⁶. 29. Madde Çalışma Grubu, Tüzük m.40/2(g)'nin çocuklar için önlemlere ilişkin davranış kurallarının düzenlenebileceğine açıkça atıfta bulunulduğundan bahisle, mevcut davranış kurallarının bu kapsamda geliştirilebileceğini ifade etmiştir⁶⁵⁷. Avrupa Doğrudan Pazarlama Federasyonu (*Federation of European Direct Marketing- FEDMA*) tarafından yayınlanan E-ticaret ve İnteraktif Pazarlamaya ilişkin davranış kurallarında, (i) çocukları hedefleyen pazarlama faaliyetlerinin, çocukların savunmasızlığını ve deneyimsizliğini istismar etmemesi, (ii) çocukların herhangi bir internet sitesine erişimlerinin kişisel verilerinin işlenmesi şartına bağlanmaması, (iii) çocukları kişisel verilerini paylaşmaya ikna etmek amacıyla ödül, oyun gibi teşviklerin

⁶⁵⁴ Article 29 Working Party, Opinion 02/2013 on Apps on Smart Devices, 00461/13/EN WP202, 27 Şubat 2013, s.26, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

⁶⁵⁵ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.29.

⁶⁵⁶ Information Commissioner's Office, Guide to Data Protection- Key Data Protection Themes- Children, <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/>.

⁶⁵⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.29.

kullanılmasından kaçınılması gerektiği belirtilmiştir⁶⁵⁸. Öte yandan, Tüzüğün “kişisel verilerin doğrudan pazarlama amacıyla işlendiği hallerde ilgili kişinin itiraz hakkı” nı düzenleyen 21/2 maddesi yetişkinlerle aynı şekilde çocuklar için de geçerlidir. Bu kapsamda, kişisel verileri doğrudan pazarlama amaçlı olarak işlenen çocuklar, doğrudan pazarlama ile ilişkili olduğu sürece profillemeye de dahil olmak üzere doğrudan pazarlama amacıyla kişisel verilerinin işlenmesine herhangi bir zamanda itiraz hakkına sahiptir⁶⁵⁹.

Tüzüğün 22. maddesinde çocuklar ve yetişkinler açısından bir ayrım yapılmamış olmakla birlikte, bu maddenin gerekçesini teşkil eden giriş bölümünün 71. paragrafında, hukuki ya da benzer şekilde önemli etki doğuran profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetlerinin çocuklar uygulanmaması gerektiği belirtilmektedir⁶⁶⁰. 29. Madde Çalışma Grubu, bu hususun Tüzüğün bağlayıcı nitelikteki 22. maddesi yerine bağlayıcı olmayan gerekçe bölümünde belirtilmiş olmasını, çocukların kişisel verilerinin profillemeye de dahil olmak üzere otomatik karar alma faaliyetleri kapsamında işlenmesine yönelik mutlak bir yasak bulunmadığı şeklinde yorumlamıştır⁶⁶¹. Öte yandan, Çalışma Grubu kural olarak, veri sorumlularının Tüzük m.22/2’deki istisna hallerinden birine dayanarak çocuklara ait kişisel verilerin otomatik karar faaliyetleri kapsamında işlenmesinden kaçınılmasını tavsiye etmektedir⁶⁶². Bu bağlamda, 71. paragraftaki bu ifadenin çocukların bu tür bir veri işlemeye konu edilemeyeceğine ilişkin kesin bir yasak anlamına gelmediği, ancak buna dayanılarak çocukların kişisel verilerinin bu kapsamda işlenmesinin bir kural haline de getirilemeyeceği söylenebilecektir.

29. Madde Çalışma Grubu, veri sorumlularının, çocukların refahının korunması amacıyla, hukuki veya benzer şekilde önemli etkileri olabilecek

⁶⁵⁸ Federation of European Direct Marketing (FEDMA), FEDMA Code on E-Commerce & Interactive Marketing, 06.09.2000, <https://www.oecd.org/sti/ieconomy/2091875.pdf>.

⁶⁵⁹ Bkz. GVK Tüzüğü, m.21/2.

⁶⁶⁰ Bkz. GVK Tüzüğü, Giriş Bölümü, 71.Paragraf.

⁶⁶¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

⁶⁶² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

profilleme de dahil olmak üzere münhasıran otomatik karar alma faaliyetleri kapsamında çocukların kişisel verilerini işlemelerinin gerekli olabileceği durumların söz konusu olabileceğini belirtmiştir. Buna göre, bu gibi hallerde, veri sorumlusu m.22’de tanımlanan istisnalardan birine dayanılması halinde, m.22/2(b) ve m.22/3 kapsamında düzenlenen çocuğun haklarını, özgürlüklerini, meşru menfaatlerini korumak için uygun tedbirlerin alınması şartıyla çocuklara ait kişisel veriler işleyebilecektir⁶⁶³. Veri sorumlusu, bu tedbirlerin verileri işlenen çocukların haklarının, özgürlüklerinin ve menfaatlerinin korunmasında etkili olmasını temin etmekle yükümlüdür⁶⁶⁴.

Birleşik Krallık Bilgi Komisyonu Ofisi, çocukların kişisel verilerinin işlendiği hallerde aşağıdaki iyi uygulama kurallarının benimsenmesini tavsiye etmektedir⁶⁶⁵:

- Çocuklara yönelik risklerin değerlendirilmesi ve azaltılması amacıyla veri koruma etki değerlendirmesi yapılmalıdır. Özellikle işleme faaliyetinin çocukların hak ve özgürlükleri üzerinde yüksek risk oluşturma potansiyeli söz konusuysa, mutlaka veri koruma etki değerlendirmesi yapılmalıdır.
- Çocuğun rızasına dayanılması halinde, çocuğun neye rıza gösterdiğini anladığından emin olunmalıdır. Veri sorumlusu ile çocuk arasında söz konusu olabilecek güç dengesizliği suiistimal edilmemelidir.
- Sözleşmenin ifası için gerekli olma uygunluk sebebine dayanılması halinde, çocuğun bir sözleşmeye taraf olma ehliyetinin varlığı dikkate alınmalıdır.
- Meşru menfaat hukuka uygunluk sebebine dayanılması halinde, veri sorumlusu işlemenin risk ve sonuçlarını belirleme sorumluluğunun farkında olmalı ve çocuğun yaşına uygun güvenlik önlemleri almalıdır.

⁶⁶³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

⁶⁶⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.28.

⁶⁶⁵ Bkz. <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/>.

- Gizlilik bildirimleri açık, sade ve çocuğun yaşına uygun bir dilde olmalıdır. Şemalar, karikatürler, grafikler ve videolar, panolar, katmanlı ve tam zamanında bildirimler, simgeler ve semboller kullanılmalıdır.
- Çocukların ve ebeveynlerinin, kişisel verilerini paylaşmanın olası sonuçlarını anlamaları için işlemenin doğasında bulunan riskleri ve çocukların bunlara karşı nasıl korunmasının amaçlandığı çocukların anlayabileceği bir şekilde açıklanmalıdır.
- Çocuklara hangi kişisel verilerine neden ihtiyaç duyulduğu, kişisel verilerinin hangi amaçla kullanılacağı, kişisel verileri üzerinde hangi haklara sahip oldukları anlayabilecekleri bir dilde anlatılmalıdır.

3.1.1.8. Güncel Mahkeme Kararları

Amsterdam Bölge Mahkemesi 2021 yılında özel taksi sürücülerini yolcularla buluşturmak üzere tasarlanmış çevrimiçi uygulamalar olan Uber ve Ola hakkında, GVK Tüzüğü'nün 22. maddesinin uygulamasına ilişkin olmaları sebebiyle önem arz eden kararlar vermiştir. Çalışmanın bu bölümünde Mahkemenin Uber hakkındaki kararları⁶⁶⁶ ile Ola hakkındaki kararı⁶⁶⁷ karşılaştırılarak incelenecektir.

Birleşik Krallık ve Fransa dahil olmak üzere birçok ülkede, sürücüler ile Uber arasında bir işçi-işveren ilişkisi olup olmadığının tespiti amacıyla davalar

⁶⁶⁶Amsterdam Bölge Mahkemesi'nin 11 Mart 2021 tarihli C/13/687315 / HA RK 20-207 numaralı kararının Flemenkçe aslı için bkz. <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020>. Kararın resmi olmayan İngilizce tercümesi için bkz. <https://ekker.legal/en/2021/03/13/dutch-court-rules-on-data-transparency-for-uber-and-ola-drivers/>. (Karar, kısaca “Uber Şeffaflık Kararı” olarak anılacaktır). Amsterdam Bölge Mahkemesi'nin 11 Mart 2011 tarihli C / 13/692003 / HA RK 20-302 numaralı kararının Flemenkçe aslı ile resmi olmayan İngilizce tercümesi için bkz. <https://ekker.legal/en/2021/03/13/dutch-court-rules-on-data-transparency-for-uber-and-ola-drivers/>. (Karar, kısaca “Uber Deaktivasyon Kararı” olarak anılacaktır).

⁶⁶⁷Amsterdam Bölge Mahkemesi'nin 11 Mart 2011 tarihli C / 13/689705 / HA RK 20-258 numaralı kararının Flemenkçe aslı ile resmi olmayan İngilizce tercümesi için bkz. <https://ekker.legal/en/2021/03/13/dutch-court-rules-on-data-transparency-for-uber-and-ola-drivers/>(Karar, kısaca “Ola Şeffaflık Kararı” olarak anılacaktır).

açılmıştır⁶⁶⁸. Ancak Uber uygulamasının arkasındaki teknolojinin sahibi Uber'in Londra iştiraki değil, Hollanda'da bulunan ana şirket Uber B.V.'dir. Dolayısıyla sürücülerden bazıları, iş ilişkisinin ispatlanabilmesi için Uber B.V.'ye e-posta yoluyla veya Uygulama ve/veya Sürücü Uygulaması (*Drivers App*) aracılığıyla farklı zamanlarda başvurarak, Uber'in hangi kişisel verilerini hangi amaçla işlediği ve ne ölçüde profillemeye ve otomatik karar verme faaliyeti gerçekleştirildiği ile ilgili bilgilere erişmek istemiştir⁶⁶⁹. Talep ettikleri bilgilere erişemeyen başvuruçular, erişim talebi sonucunda otomatik karar verme ve/veya profil oluşturma varlığına ilişkin herhangi bir bilgi alamadıklarından bahisle konuyu Hollanda'da mahkemeye taşımışlardır. Uyuşmazlığa konu olan sistem Uber'in sürücü ile yolcu eşleştirmek suretiyle uygulama üzerinden talep edilen yolculukların sürücülere atanmasını sağlayan eşleştirme algoritmasıdır. Başvuruçulara göre, Uber'in gizlilik bildiriminde otomatik karar vermeyle ilgili ve web sitesinde sağladığı bilgiler eksik ve kısmen de yanlışır⁶⁷⁰.

Başvuruçuların iddiasına göre;

- Sürücü Uygulaması, sürüş davranışı, yolculuk sırasında telefonun kullanımı ve kabul edilen yolculukların yüzdesi hakkında bir çıkarımda bulunmaktadır. Bu çıkarım, profesyonel performans, güvenilirlik, davranış, konum ve seyahat bilgilerinin analizinin sonucudur ve profillemeye olarak sınıflandırılmalıdır;
- Uber'in sahip olduğu Sürücü Profili, GVK Tüzüğü'nün 4. Maddesi anlamında bir profildir, çünkü Uber bunu başvuruçuların 'uygunsuz davranış' gibi çok olumsuz niteliklere yol açabilecek kişisel yönlerini değerlendirmek için kullanır;

⁶⁶⁸2021 yılında Birleşik Krallık Yüksek Mahkemesi, Uber sürücüsü olan çalışan kişiler ile Uber'in Londra iştiraki olan Uber London Ltd arasında bir işçi-işveren ilişkisi bulunduğu hükmetmiştir. Birleşik Krallık Yüksek Mahkemesi'nin 19 Şubat 2021 tarihli UKSC 2019/0029 kararı için bkz. <https://www.supremecourt.uk/cases/uksc-2019-0029.html>.

⁶⁶⁹ Bkz. Uber Şeffaflık Kararı, 2.7-2.8 No'lu Paragraflar.

⁶⁷⁰ Bkz. Uber Şeffaflık Kararı, 4.65 No'lu Paragraf.

- Çeşitli kaynaklardan, Uber'in sürücüleri yolcularla ilişkilendirirken, gizlilik bildiriminde belirtilenler dışında, sürücünün iptal geçmişi ve yüz tanıma gibi kişisel veri kategorileri kullandığı anlaşılmaktadır⁶⁷¹.

Başvurucuların iddialarına karşılık olarak Uber ise,

- GVK Tüzüğü m.22 anlamında otomatik karar verme faaliyeti gerçekleştirmediğini ve her halükarda bunun bir yasak teşkil etmediğini,
- Toplu eşleştirme sistemi (*batched matching system*) aracılığıyla mevcut yolculukları tahsis etmek için otomatik veri işleme yöntemlerine başvurulduğunu,
- Bu sistemin, en yakın sürücüleri ve yolcuları toplu olarak gruplandırarak bir sürücü ile bir yolcu arasındaki o grup içindeki en uygun eşleşmeyi (bağlantıyı) belirlediğini,
- Konum, seyahat rotası, trafik hacmi, coğrafi faktörler, yolcunun alınma noktasına tahmini varış süresi bilgilerinin ve sürücüler tarafından Sürücü Uygulaması aracılığıyla belirtilen kişisel tercihlerin kullanıldığını,
- Herhangi bir yolcunun sürücüye geçmişte mevcut beş yıldızdan biri ile puan vermiş olması halinde, sistemin artık o yolcuyu aynı sürücü ile eşleştirmedeğini,
- Mevcut yolculukların otomatik olarak tahsis edilmesinin ilgili kişi açısından hukuki veya benzer şekilde önemli bir etkisinin bulunmadığını, bu nedenle de m.22 kapsamında bir otomatik karar verme gerçekleşmediğini,
- Sürücülerin Tüzük m.4 kapsamında bir profilinin çıkarılmadığını,
- Sürücü profilinin müşteri hizmetleri sisteminde kullanılan bir isimden ibaret olduğunu,

⁶⁷¹ Bkz. Uber Şeffaflık Kararı, 4.65 No'lu Paragraf.

- Dolandırıcılıkla mücadele kapsamında gerçekleştirilen veri işleme faaliyetlerinin, süreçte insan müdahalesi bulunması nedeniyle otomatik karar verme teşkil etmediğini savunmuştur⁶⁷².

Bu bağlamda, yolcu ile sürücünün eşleştirilmesi suretiyle gerçekleştirilen otomatik karar verme faaliyetinin sürücüler açısından hukuki veya benzer şekilde önemli derecede bir etkisinin olup olmadığının tespit edilmesi gerekmiştir. Mahkemece belirtilen algoritmik karar verme faaliyetinin GVK Tüzüğü m.22 kapsamında olup olmadığı incelenmiştir. Yolcu ve sürücülerin algoritmalar aracılığı ile eşleştirildiği sistemi inceleyen Mahkeme, sürücülerin Uber'in gerçekleştirdiği otomatik karar faaliyetlerine ilişkin erişim hakkını kullanarak bilgi alma talebini reddetmiştir. Mahkeme, kararında, başvuruçuların Uber'in kendileri ile ilgili kararları ne ölçüde m.22 anlamında otomatik karar vermeye dayalı olarak aldığını yeterince açıklayamadıklarına kanaat getirmiştir. Mahkemeye göre, toplu eşleştirme sistemi (*batched matching system*) ile peşin fiyatlandırma sisteminin (*upfront pricing system*) sürücü ile Uber arasındaki sözleşmenin uygulanmasına belli bir mertebede etkisinin bulunacağı kabul edilebilecekse de hukuki veya benzer şekilde önemli etkiye ilişkin herhangi bir kanıt bulunmamaktadır⁶⁷³. Mahkeme, bu bağlamda, ilgili kişinin Tüzük m.15 tahtında erişim hakkının, m.22 uyarınca veri sorumlusunun kendisi hakkında, münferiden otomatik işlemeye dayalı olarak, hukuki sonuçlar doğuran veya benzer şekilde önemli ölçüde etkileyen bir karar alması durumunda geçerli olduğundan bahisle bu uyuşmazlıkta erişim hakkının uygulanabilir olmadığına hükmetmiştir⁶⁷⁴.

Amsterdam Bölge Mahkemesinin bu kararı, gerek GVK Tüzüğü'nün 22.maddesi anlamında bir otomatik karar vermenin bulunup bulunmadığının incelenmiş olması, gerekse de Tüzüğü'n 15.maddesi tahtında erişim hakkının sınırlarına ilişkin bir hüküm oluşturulması sebebiyle oldukça önemlidir. Kararı

⁶⁷² Bkz. Uber Şeffaflık Kararı, 4.66 No'lu Paragraf.

⁶⁷³ Bkz. Uber Şeffaflık Kararı, 4.67 No'lu Paragraf.

⁶⁷⁴ Bkz. Uber Şeffaflık Kararı, 4.67 No'lu Paragraf.

önemli kılan bir diğer husus ise, Avrupa Birliği Adalet Divanı'nın Nowak kararının aksine, öznel düşünce ve değerlendirmelerin kişisel veri olmadığına hükmedilmiş olmasıdır. Kararda, Uber çalışanlarının sürücülerin davranışları hakkındaki değerlendirmelerin, çalışanların görüşlerini yansıtması ve doğruluğunun teyit edilebilir olmaması sebebiyle kişisel veri olmadığı, bu nedenle de görüşlerle ilgili olarak doğrulama, düzeltme, silme hakları kullanılamayacağı gibi, erişim hakkının da geçerli olmadığı belirtilmiştir. Öte yandan Mahkeme, Uber'insöz konusu değerlendirmelerin dayanağını oluşturan, yolcuların sürücüler hakkındaki geri bildirimlerinin (*feedbacks*) kişisel veri olduğundan bahisle söz konusu geribildirimlere erişim hakkı tanımakla yükümlü olduğuna karar vermiştir⁶⁷⁵. Ancak, müşterilerin sürücüler hakkındaki geri bildirimlerinin de müşterilerin nesnel görüşlerini yansıttığı göz önüne alındığında, bu geri bildirimlerin kişisel veri olarak kabul edilirken Uber çalışanlarının sürücüler hakkındaki değerlendirmelerinin kişisel veri olarak kabul edilmemesi karardaki tutarsızlığı yansıtmaktadır⁶⁷⁶.

Amsterdam Bölge Mahkemesi'nde görülen Uber hakkındaki diğer bir dava ise, sürücülerin lisans iptaline ilişkin otomatik kararlara itirazları hakkındadır. Söz konusu uyuşmazlık, Uber'in, birkaç sürücüsüne, haklarında dolandırıcılık şüphesi bulunduğunu ve bu nedenle sözleşme şartlarını ihlal ettikleri gerekçesiyle sürücü hesaplarının devre dışı bırakıldığını bildirmesi ile ortaya çıkmıştır. Sürücüler, bu kararın anlamlı bir insan müdahalesi olmaksızın tamamen otomatik olarak alındığını, böylelikle sözleşmenin derhal feshedilmesine ve gelir kaybına neden olduğunu ileri sürerek, Tüzük m.15/1(h) uyarınca otomatik kararın mantığı hakkında anlamlı bilgilere erişim talep etmiştir. Bir önceki Uber davasından farklı olarak, bu davada esas tartışma otomatik kararın Tüzük m.22 anlamında tamamen otomatik işlemeye dayalı bir karar olup olmadığı noktasında yoğunlaşmıştır. Davada Uber, lisans iptaline ilişkin nihai kararın, uygulamanın algoritmasının

⁶⁷⁵ Bkz. Uber Şeffaflık Kararı, 4.45 ve 4.52 No'lu Paragraflar.

⁶⁷⁶ Milica BASTA, Dutch Court Clarifies the Limits to the Right of Access, 7 Nisan 2021, <https://bdkadvokati.com/dutch-court-clarifies-the-limits-to-the-right-of-access/>.

ürettiği potansiyel dolandırıcılık sinyali ekseninde şirketin operasyonel risk ekibi tarafından verildiğini iddia etmiş, sürücüler ise bu iddiaya karşı herhangi bir itiraz ileri sürmemişlerdir⁶⁷⁷. Mahkeme, Hollanda Medeni Usul hukuku uyarınca taraflardan birinin iddiasına diğer tarafça itiraz edilmemesi halinde iddianın kanıtlanmış kabul edilmesi gerektiğinden, somut olayda otomatik münferit karar verme olmadığı sonucunda vararak sürücülerin Tüzük m.15 tahtında kararın mantığı hakkında anlamlı bilgilere erişim talebini reddetmiştir.

Ola davası da ilgili Uber davası ile benzer şekilde, sürücülerin Ola ile aralarında bir işçi-işveren ilişkisi bulunduğunu ispatlayabilmek için Tüzük m.15 tahtında bilgilere erişim talep etmeleri sonucunda doğmuştur⁶⁷⁸. Amsterdam Bölge Mahkemesi, Ola davasında, sürücülerin kazanç profilleri, usulsüzlüklerin tespitinde kullanılan sistemler ile şoförle müşteriye eşleştiren sisteme ilişkin algoritma ve otomatik karar verme süreçlerini incelemiştir. Mahkemeye göre, söz konusu sistemler şoförlerin davranışı üzerinde bir etkiye sahip olmakla birlikte, davacı tarafı teşkil eden şoförler bu sistemlerin hukuki veya benzer şekilde önemli bir etkiye sahip olduğunu ispatlayamamışlardır⁶⁷⁹. Öte yandan, Ola'nın sürücülere uygulanacak ceza ve kesintilerin belirlenmesinde kullandığı bilgisayar sistemi, belirli bir yolculuğun geçersiz sayılması halinde sürücüye para cezası uygulamaktadır⁶⁸⁰. Mahkeme, bu cezanın, sürücülerin Ola ile akdettikleri sözleşmeden doğan haklarını etkilediğinden bahisle, "hukuki etkiye benzer şekilde önemli derecede" etkilediğine karar vermiştir. Mahkeme kararda "anlamlı bilgi" kavramını, 29. Madde Çalışma Grubu'nun profileme ve otomatik karar vermeye ilişkin rehberini esas alarak irdelemiştir⁶⁸¹. Bu bağlamda değerlendirmede rol oynayan en önemli kriterlerin neler olduğu ve bunların fonksiyonu hakkında ilgili kişi bilgilendirilmelidir. Bu bilgiler ilgili kişinin kararın hangi kriterlere dayandığını anlayabilmesini ve işleme faaliyetinin hukuka uygunluğunu ve

⁶⁷⁷ Bkz. Uber Deaktivasyon Kararı, 2.24 No'lu Paragraf.

⁶⁷⁸ Bkz. Ola Şeffaflık Kararı, 2.5 No'lu Paragraf.

⁶⁷⁹ Bkz. Ola Şeffaflık Kararı, 4.47-4.50 No'lu Paragraflar.

⁶⁸⁰ Bkz. Ola Şeffaflık Kararı, 4.51 No'lu Paragraf.

⁶⁸¹ Bkz. Ola Şeffaflık Kararı, 4.41 No'lu Paragraf.

doğruluğunu onaylayabilmesini sağlamalıdır⁶⁸². Mahkeme Ola'nın Tüzük m.15 tahtında ilgili kişilere kararın mantığı hakkında anlamlı bilgiler sağlamakla, bu çerçevede Ola'nın ana değerlendirme kriterlerini ve bunların otomatik karardaki fonksiyonunu ilgili kişilere iletmekle yükümlü olduğuna hükmetmiştir⁶⁸³. Karara göre Ola, sürücülerin, performanslarına ilişkin derecelendirmelere (anonimleştirilerek), “dolandırıcılık olasılık puanlarının” (*fraud probability score*) hesaplanmasında kullanılan kişisel verilere ve sürücülere atanan iş dağılımını etkileyen “kazanç profillerinin” (*earning profiles*) çıkarılması için kullanılan verilere erişim imkanı sağlamalıdır⁶⁸⁴. Amsterdam Mahkemesi'nin Ola kararı, bir veri sorumlusunun tamamen otomatik işlemeye dayalı olarak alınan bir kararın mantığını açıklamakla yükümlü tutulduğu ilk karar olması bakımından önemlidir. Zira bu karar, GVK Tüzüğü'nün otomatik karar alma ve açıklama hakkına ilişkin çok tartışılan hükümlerinin pratikte de mahkemelerce uygulanabileceğini göstermiştir⁶⁸⁵. Bu bağlamda karar, kurum ve kuruluşların, tamamen otomatik işlemeye dayalı karar almaya ilişkin Tüzük hükümlerinin gerekliliklerini yerine getirmeleri ve otomatik karar sistemlerinin işleyiş mantığını açıklayabilir durumda olmaları için bir gerekçe teşkil etmektedir⁶⁸⁶.

⁶⁸² Bkz. Ola Şeffaflık Kararı, 4.41 No'lu Paragraf.

⁶⁸³ Bkz. Ola Şeffaflık Kararı, 4.52 No'lu Paragraf.

⁶⁸⁴ Bkz. Ola Şeffaflık Kararı, 4.36, 4.45, 4.47 No'lu Paragraflar.

⁶⁸⁵ Raphaël GELLERT & Marvin VAN BEKKUM & Frederik ZUIDERVEEN BORGESIOUS, The Ola & Uber Judgments: For the First Time a Court Recognises a GDPR Right to an Explanation for Algorithmic Decision-Making, 28 Nisan 2021, <http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html>.

⁶⁸⁶ Bkz. <http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html>.

3.2. HUKUKA UYGUNLUK NEDENLERİ

Kişisel verilerin işlenmesi hukukuna hakim olan en temel ilke, kural olarak kişisel verilerin işlenmesinin yasak olmasıdır⁶⁸⁷. Kişisel verilerin korunmasına ilişkin tüm düzenlemelerde genel nitelikli kişisel veriler ve özel nitelikli kişisel veriler açısından herhangi bir ayırım yapılmaksızın, kişisel verilerin işlenebilmesi için ilgili kişinin açık rızasının bulunması şart koşulmuştur. Avrupa Birliği mevzuatında ve ulusal mevzuatımızda hüküm altına alındığı üzere, herhangi bir veri işleme faaliyetinin hukuka uygun ve meşru olduğunun kabul edilebilmesi için işleme faaliyetinin ilgili kişinin açık rızasına veya ilgili kişinin açık rızasının bulunmadığı hallerde ise ilgili mevzuatta kişisel verilerin işlenmesi için öngörülen hallerden birine dayanması gerekmektedir⁶⁸⁸.

KVK Kanunu'ndaki kişisel verilerin işlenme şartları⁶⁸⁹ aynı zamanda hukuka uygunluk sebebi teşkil etmektedir⁶⁹⁰. Nitekim GVK Tüzüğü'nün ilgili 6.maddesinin başlığında “işlemenin hukuka uygunluğu” (*“lawfulness of processing”*) ifadesi tercih edilmiştir. GVK Tüzüğü'nde düzenlenen hukuka uygunluk sebepleri ile KVK Kanunu'nda düzenlenen kişisel verilerin işlenme şartları büyük ölçüde paralel şekilde düzenlenmiş olup, bazı noktalarda farklılık göstermektedir.

Belirtilmelidir ki, hukuka uygunluk sebepleri arasında bir hiyerarşi söz konusu değildir. Diğer bir ifadeyle, işleme faaliyetine dayanak teşkil eden sebeplerden biri diğerinden üstün veya daha iyi değildir⁶⁹¹. Ancak her halükarda, bu dayanaklardan her biri ilgili kişiye farklı haklar sağladığından, işleme faaliyetinin hangi hukuka uygunluk sebebine dayandırılacağına karar verilirken

⁶⁸⁷ Çekin, s.42.

⁶⁸⁸ Çekin, s.42-43.

⁶⁸⁹ Bkz. KVK Kanunu, m.5; KVK Kanunu, m.6.

⁶⁹⁰ Taştan, s.53. Hukuka aykırılık ve hukuka uygunluk sebepleri ile ilgili detaylı açıklama için bkz. Taştan, s. 154-156.

⁶⁹¹ Gonzalez & De Hert, s.599.

özenli hareket edilmelidir⁶⁹². Öte yandan, veri sorumlusunun sonradan farklı bir hukuka uygunluk sebebine dayanması zor olabileceğinden ve hatta başlangıçtaki hukuka uygunluk sebebinden farklı bir sebebe dayanılması kişisel verilerin korunması düzenlemelerine aykırılık oluşturabileceğinden, hukuka uygunluk sebebinin işleme faaliyetine başlanmadan önce belirlenmesi ve kayıt altına alınması önem teşkil etmektedir⁶⁹³. Zira ilgili kişinin işleme faaliyetine itiraz etmesi ve açık rıza dışındaki hukuka uygunluk sebeplerinden birine dayanılmış olması halinde “gereklilik” değerlendirmesinin geçilemediğinin, meşru menfaate dayanılmış olması halinde dengeleme testinin adil bir şekilde yapılmadığının veya kullanıcıların bilgilendirmeye dayalı, özgür ve açık bir rızasının bulunmadığının tespit edilmesi halinde, veri sorumlusu ciddi yaptırımlar ile karşı karşıya kalabilecektir⁶⁹⁴.

GVK Tüzüğü m.22’nin uygulama alanı dışında kalan profillemeye ve otomatik karar faaliyetleri, hukuka uygunluk sebeplerinden herhangi birine dayanılarak gerçekleştirilebilir. Bu bölümde, GVK Tüzüğü m. 22/1’de tanımlanan profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetleri olarak kabul edilmeyen profillemeye ve otomatik karar faaliyetleri için geçerli olan hukuka uygunluk sebepleri, GVK Tüzüğü m. 6/1 esas alınarak, KVK Kanunu ile karşılaştırmalı şekilde incelenmiştir.

3.2.1. İlgili Kişinin Rızası

Avrupa Birliği düzenlemelerinin hepsinde yer verilen ve iç hukukumuza da dahil edilen rıza kavramının, ilgili kişiye kendisiyle ilgili veriler üzerinde kontrol ve denetim imkanı sağlaması sebebiyle kişisel verilerin korunması düşüncesinin temelinde yer alan bireyin kişisel verilerinin geleceğini belirleme hakkının (*informational self determination*) doğal bir sonucu olduğu kabul edilmektedir⁶⁹⁵.

⁶⁹² Gonzalez & De Hert, s.599.

⁶⁹³ Gonzalez & De Hert, s.599.

⁶⁹⁴ Gonzalez & De Hert, s.615.

⁶⁹⁵ Küzeci, s.231.

Rıza, doğru şekilde alınırsa, ilgili kişiye kişisel verileri üzerinde kontrol imkanı sağlayan bir araç niteliği kazanacaktır⁶⁹⁶. Öte yandan, rızanın yanlış bir şekilde kullanılması, rızanın ilgili kişinin kişisel verileri üzerinde kontrol sahibi olduğu illüzyonu yaratılmasına ve ilgili veri işleme faaliyeti için doğru ve uygun olmayan bir işleme sebebi teşkil etmesine neden olacaktır⁶⁹⁷. Belirtilmelidir ki, ilgili kişinin rızasının varlığı ile diğer hukuka uygunluk sebepleri eşdeğer kriterler olup birinin diğerinden önce veya sonra gelmesi gibi bir durum bulunmamaktadır⁶⁹⁸. İlgili kişinin rızası, hukuka uygunluk sebepleri arasında önemli bir yere sahip olmakla birlikte, işleme faaliyetinin özelliklerine bağlı olarak, ilgili kişi veya veri sorumlusu açısından, diğer sebeplerinin birinin ilgili kişinin rızası yerine daha uygun bir hukuka uygunluk sebebi olarak kabul edilmesi her zaman ihtimal dahilindedir⁶⁹⁹. Ancak, bir işleme faaliyetinde açık rıza ile diğer hukuka uygunluk sebeplerinin birlikte bulunamayacağı unutulmamalıdır⁷⁰⁰. Nitekim ilgili mevzuatta öngörülen herhangi bir hukuka uygunluk sebebi mevcut ise, bu tür bir işleme faaliyeti için ilgili kişinin açık rızasının talep edilmesine gerek yoktur⁷⁰¹. Bu bağlamda, veri sorumlusu veri işleme faaliyetini gerçekleştirmek için öncelikle rıza haricindeki işleme şartlarından birinin veya birkaçının bulunup bulunmadığına bakmalı, bunlardan herhangi birinin bulunmaması halinde ilgili kişinin açık rızasının alma yolunu tercih etmelidir⁷⁰².

Gerek GVK Tüzüğü'nde gerek KVK Kanunu'nda rızanın ne zaman beyan edilmesi gerektiği ile ilgili açık bir düzenlemeye yer verilmemiştir. Kişisel verilerin korunması hukukunun hizmet ettiği hukuki yarar ve kişisel verilerin işlenmesine hakim olan ilkeler ışığında kural olarak, ilgili kişinin işleme faaliyeti başlamadan

⁶⁹⁶ Küzeci, s. 231.

⁶⁹⁷ Article 29 Working Party, Legitimate Interest, s.16.

⁶⁹⁸ Dülger, s.215.

⁶⁹⁹ Article 29 Working Party, Legitimate Interest, s.16.

⁷⁰⁰ Çekin, s.64.

⁷⁰¹ Çekin, s. 64.

⁷⁰² Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin İşlenmesi Şartları, s.6. Diğer yandan, açık rıza haricindeki koşulların geniş yorumlanmaya elverişli olması, işleme faaliyeti için açık rızanın zorunlu olduğu durumların kısıtlı kalmasına sebebiyet vermektedir. Küzeci, s.231.

evvel rıza beyanında bulunması gerektiği anlaşılmaktadır⁷⁰³. GVK Tüzüğü m.7/3'te ilgili kişinin işlemeye yönelik rıza beyanını her zaman geri alabileceği açıkça düzenlenmiş olmasına karşın, KVK Kanunu'nda bu hususta herhangi bir düzenlemeye yer verilmemiştir. Öte yandan KVK Kanunu'nun 11/e. maddesinde ilgili kişinin kişisel verilerinin silinmesini ve yok edilmesini talep etme hakkı hüküm altına alınmıştır. Bu bağlamda her ne kadar açık bir düzenlemeye yer verilmemiş olsa da, Kanun'un sistematüğinden ve ikincil düzenlemelerden⁷⁰⁴ rızanın her zaman geri alınabileceği sonucuna varılmaktadır. Geçerli bir rızanın varlığından bahsedilebilmesi için, rıza beyanının açık rızanın unsurlarını taşıması yeterli kabul edilmektedir. Diğer yandan, GVK Tüzüğü'nde ilgili kişinin işleme faaliyetine rızasının bulunduğunu ispat yükünü veri sorumlusuna yüklenmiş⁷⁰⁵; ve ayrıca rıza beyanının kanıtlanabilir nitelikte olması gerektiği de açıkça düzenlenmiştir⁷⁰⁶. Dolayısıyla, ilgilinin kişi çağrı merkezi, telefon, elektronik posta gibi araçlar vasıtasıyla yazılı veya sözlü olarak rıza beyanında bulunabileceği kabul edilmekle birlikte, veri sorumlusunun aydınlatma ve rıza alma sorumluluklarını yerine getirirken kullanacağı yöntemin ispat kuvvetini de gözetmekle yükümlü olduğu unutulmamalıdır⁷⁰⁷. Bu bağlamda ispat açısından rızanın yazılı olarak alınmasının daha uygun olacağını belirtmek gerekir⁷⁰⁸. Elektronik ortamda beyan edilen rızanın da yazılılık koşulunu yerine getirdiği ve yazılı olarak verilen rızayla eşdeğer hukuki niteliğe sahip olduğu kabul edilmektedir⁷⁰⁹.

⁷⁰³Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 17/EN WP259 rev.01, 28 Kasım 2017, s.9, <https://ec.europa.eu/newsroom/article29/items/623051> (Kısaltılmışı "Guidelines on Consent").

⁷⁰⁴ Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in 7/3 maddesi uyarınca, ilgili kişi her zaman vermiş olduğu rızayı geri alabilir. Aynı şekilde, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 8/5 ve 11/2 maddelerinde; ilgili kişinin trafik ve konum verilerinin işlenmesine yönelik olarak vermiş oldukları rızayı her zaman geri alabilecekleri düzenlenmiştir.

⁷⁰⁵ Bkz. GVK Tüzüğü, m.7/1; GVK Tüzüğü, Giriş Bölümü, 42.Paragraf.

⁷⁰⁶ Bkz. GVK Tüzüğü, m.7/1.

⁷⁰⁷ Çiğdem AYÖZGER ÖNGÜN, Kişisel Verilerin Korunması Hukuku (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil), Beta, Genişletilmiş 2.Baskı, 2019, İstanbul, s.137.

⁷⁰⁸ Ayözger Öngün, s.137.

⁷⁰⁹ Hayrunnisa ÖZDEMİR, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin, 1.Baskı, 2009, Ankara, s.170.

3.2.1.1. Açık Rıza

GVK Tüzüğü'nde kişisel verilerin hukuka uygun bir şekilde işlenebilmesi için öngörülen hukuka uygunluk sebeplerinden biri ilgili kişinin rızası alınması olup⁷¹⁰; kişisel verilerin korunması açısından ciddi ölçüde risk barındıran ve bu bağlamda ilgili kişiye kişisel verileri üzerinde daha yüksek bir seviyede kontrol imkanı tanınması gerektiren işleme faaliyetlerinde ise “açık rıza” şart koşulmuştur⁷¹¹. GVK Tüzüğü'nün 9/2(a) maddesi uyarınca özel nitelikli kişisel verilerin işlenmesinde, 49/1(a) maddesi uyarınca yeterli seviyede korumanın bulunmadığı üçüncü ülkelere veya uluslararası kuruluşlara yapılacak veri transferlerinde ve 22/2(c) maddesi uyarınca ilgili kişinin kendisi ile ilgili hukuki sonuçlar doğuran veya kendisini benzer biçimde önemli şekilde etkileyen profillemeye de dâhil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetlerinde, ilgili kişinin açık rızasının bulunması kişisel verilerin işlenmesinde hukuka uygunluk sebebi olarak kabul edilmiştir⁷¹². Belirtmek gerekir ki rızanın “açık” olması, rızanın ilgili kişi tarafından beyan edilme şeklini nitelendirmektedir. Bu bağlamda, ilgili kişinin açık rızasının varlığından bahsedebilmek için ilgili kişinin verilerinin işlenmesine rızanın bulunduğu işaret eden açık bir beyanın bulunması aranır⁷¹³. Rızanın açık olduğunu ortaya koymanın en etkili yollarından biri, rızanın yazılı bir beyan ile verilmesidir. Mümkün olduğu takdirde, veri sorumlusunun bu rıza beyanını imzalı olarak alması ise, ileride ortaya çıkabilecek muhtemel şüpheleri ve delil eksikliğine bağlı iddiaları ortadan kaldıracaktır⁷¹⁴.

GVK Tüzüğü m.4/11 tahtında “rıza” kavramı, “ilgili kişinin bir beyan yoluyla veya açık bir onaylayıcı eylemle kişisel verilerinin işlenmesine onay verdiğini gösteren, bilgilendirmeye dayanan (*informed*), özgür iradeyle verilmiş (*freely given*), belirli (*specific*) ve tereddüte yer vermeyecek şekilde açık

⁷¹⁰ Bkz. GVK Tüzüğü, m.6/1.

⁷¹¹ Article 29 Working Party, Guidelines on Consent, s.18.

⁷¹² Bkz. GVK Tüzüğü, m.9/2(a), 49/1(a), 22/2(c).

⁷¹³ Article 29 Working Party, Guidelines on Consent, s.18.

⁷¹⁴ Article 29 Working Party, Guidelines on Consent, s.18.

(*unambiguous*) işaret” şeklinde tanımlanmıştır⁷¹⁵. Rızanın bilgilendirmeye dayanması, veri sorumlusunun ilgili kişiyi kişisel verilerinin hangi amaçla işlendiği hususunda aydınlatma yükümlülüğünün bir görünümüdür. Aydınlatma yükümlülüğü uyarınca, veri sorumlusu ilgili kişiye, işlenen verinin niteliği, işlemenin amaçları, muhtemel veri aktarımlarının alıcıları, ilgili kişinin hakları, rızanın alınmamasının sonuçları gibi kanunda belirtilen tüm hususlar ve ilgili kişinin haklarıyla ilgili olarak net ve anlaşılır bir şekilde, doğru ve tam bilgi vermekle yükümlüdür⁷¹⁶. 29. Madde Çalışma Grubu, veri sorumlusunun ilgili kişiyi geçerli bir şekilde bilgilendirdiğinin kabul edilebilmesi için iki koşulun karşılanmış olmasını aramaktadır⁷¹⁷. Bunlardan ilki, bilgilendirme kalitesidir. Bu bağlamda bilgilendirmenin, ortalama zekaya sahip kişilerin anlayabileceği şekilde sade ve basit bir dille ve jargon kullanılmadan yapılması gerekir. İkincisi ise, bilgilendirmenin erişilebilir ve görünür olmasıdır. Bilgilendirmenin erişilebilir görünür olması şartı uyarınca bilgilendirmenin herhangi bir platformda erişilebilir olması yeterli olmayıp; bilgilendirmenin ilgili kişi tarafından rahatlıkla okunabilmesi⁷¹⁸ ve direkt olarak ilgili kişiye yapılması gerekir⁷¹⁹.

Veri sorumlusu aydınlatma yükümlülüğünü ilgili kişiye doğrudan bir aydınlatma metni sunmak suretiyle yazılı olarak yerine getirebileceği gibi çağrı merkezi gibi elektronik bir ortam vasıtasıyla sözlü olarak da gerçekleştirebilir⁷²⁰.

⁷¹⁵ Bkz. GVK Tüzüğü, m.4/11. KVK Kanunu’nda açık rıza, “ilgili kişinin belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızası” olarak tanımlanmıştır. Bkz. KVK Kanunu, m.3/a. Kanunun gerekçesinde bu tanımın 95/46 Sayılı Direktif’e dayandığı ifade edilmiştir. Bkz. Kişisel Verilerin Korunması Kanunu Tasarısı, s.7, <https://www2.tbmm.gov.tr/d23/1/1-0576.pdf>; 95/46 Sayılı Direktif, m.2/h. Kanun’un gerekçesinde ayrıca, açık rızanın tereddüte yer bırakmayacak açıklıkta olması gerektiği belirtilmiştir.

⁷¹⁶ Article 29 Working Party, Opinion on the Definition of Consent, s.19.

⁷¹⁷ Article 29 Working Party, Guidelines on Consent, s. 20.

⁷¹⁸ Bilgilendirmenin geçerlilik şartları, şüphesiz, genel işlem şartları kapsamındaki açık rızanın geçerliliğine ilişkin sorunları da beraberinde getirmektedir. Bu çerçevede 6502 sayılı TKHK m. 4/1’de belirtilen, (i) en az on iki punto büyüklüğünde olma (ii) anlaşılabilir bir dilde yazılmış olma (iii) açık, sade ve okunabilir bir şekilde düzenlenme şartlarının dikkate alınabileceği değerlendirilmektedir. Çekin, s.61.

⁷¹⁹ Article 29 Working Party, Guidelines on Consent, s. 20.

⁷²⁰ Bkz. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ, m. 5.

Diğer yandan, “katmanlı bilgilendirme” (*layered notice*)⁷²¹ olarak ifade edilen bilgilendirme yöntemine de başvurulması mümkündür. Rızanın bilgilendirmeye dayanması, ilgili kişinin bir tercihte bulunabilmesi için kritik öneme sahip bazı konularda bilgi sahibi olmasını gerektirir. 29. Madde Çalışma Grubu, rızanın bilgilendirmeye dayalı olduğunun kabul edilebilmesi için ilgili kişiye en azından,

- i. Veri sorumlusunun kimliği, rıza alınan her bir işleme faaliyetinin amacı,
- ii. Toplanacak ve kullanılacak veri türleri, ilgili kişinin rızasını geri alma hakkına sahip olduğu,
- iii. Kişisel verilerin GVK Tüzüğü m.22/2(c) tahtında tanımlanan şekilde bir otomatik karar alma faaliyeti için kullanıldığı,
- iv. GVK Tüzüğü m.46’da düzenlendiği şekilde uygun güvenlik tedbirlerinin bulunmadığı hallerde gerçekleştirilecek veri transferlerinin muhtemel riskleri hakkında bilgi verilmesi gerektiğini belirtmektedir⁷²².

Rızanın belirli bir konuya ilişkin olması şartı uyarınca, rızanın somut bir işleme amacına yönelik verilmiş olması gerekir⁷²³.İlgili kişinin kişisel verilerinin hangi bağlamda işlenmesine muvafakat ettiği açıkça belli olmayan, “battaniye rıza” veya “torba rıza” olarak da adlandırılan genel kapsamlı rıza beyanları geçerli değildir⁷²⁴. İlgili kişinin rıza beyanının tereddüte yer bırakmayacak açıklıkta olması rızanın elektronik ya da fiziki ortamda yazılı veya sözlü bir beyan şeklinde onaylayıcı bir davranış (*affirmative act*) ile açıklanmış olmasını ifade eder. Diğer bir ifadeyle, ilgili kişi açıkça onaylayıcı bir davranışla rızasını açıklamamış ve ilgili kişinin rıza gösterip göstermediğine dair makul bir şüphe söz konusu ise, tereddüte

⁷²¹ Katmanlı bilgilendirme, kişisel verilerin elde edilmesi sırasında ilgili kişiye kişisel verilerinin elde edildiği konusunda kısa bir bilgilendirme yapılarak bu bilgilendirmeden sonra daha detaylı bir şekilde bilgilendirileceği bir mecraaya yönlendirilmesini ifade etmektedir. Tanım için bkz. Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, s. 90. Katmanlı bilgilendirme hakkında detaylı bilgi için bkz. Information Commissioner’s Office, What is a layered approach?, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>.

⁷²² Article 29 Working Party, Guidelines on Consent, s.13.

⁷²³ Ayözger Öngün, s. 136.

⁷²⁴ Taştan, s.158.

yer vermeyecek açıklıkta bir rızadan bahsedilemeyecektir⁷²⁵. Rızanın özgür iradeyle açıklanmış olması ile kast edilen ilgili kişinin kişisel verilerinin işlenmesine rıza gösterip göstermeme hususunda tercih imkanına sahip olmasıdır. Diğer bir ifadeyle, ilgili kişinin kişisel verilerinin işlenmesini kabul etmemesi halinde bu sebeple doğacak muhtemel sonuçlar ilgili kişi açısından bir yaptırım niteliğindeyse, rızanın özgür iradeyle açıklandığından bahsedilemeyecektir⁷²⁶.

3.2.1.2. Profillemeye ve Otomatik Karar Faaliyetlerinde Rıza Şartlarının Uygulanabilirliği

GVK Tüzüğü, ilgili kişinin açık rızasına dayanması halinde, m. 22 tahtında düzenlenen profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma ve m. 22'nin uygulama alanının dışında kalan genel profillemeye ve otomatik karar faaliyetlerine izin vermektedir. İlgili kişinin rızasının, kişisel verilerin korunmasına ilişkin düzenlemelerde geçerli bir açık rıza için öngörülen şartları karşılayıp karşılamadığı tüm veri işleme faaliyetleri için tartışma konusu olabilmekle birlikte, yapay zeka ve büyük veri uygulamalarının kendine has özellikleri nedeniyle, ilgili kişinin profillemeye ve otomatik karar alma faaliyetlerine gösterdiği rızanın geçerliliğine ilişkin bazı belirgin sorunlar ortaya çıkmaktadır. Özellikle m. 22 kapsamındaki profil çıkarmaya dayalı tamamen otomatik işlemeye dayalı kararlarla ilgili olarak, ilgili kişinin rızasını çevrimiçi olarak vermesi gerektiği durumlarda, çevrimiçi olarak alınan rızanın “açık rıza” niteliğinde olup olmadığı belirsizlik yaratabilmektedir. Avrupa Komisyonu, Birleşik Krallık Bilgi Komisyoneri Ofisi, Avrupa Parlamentosu Bilim ve Teknolojinin Heyeti gibi kişisel

⁷²⁵ Voigt & Von Dem Bussche, s.183. Kişinin internet ortamında halihazırda işaretlenmemiş olan rıza beyan kutucuğunu işaretlemesi (*opt-in*) onaylayıcı bir davranışa örnek olarak gösterilebilir. Dolayısıyla, halihazırda işaretlenmiş rıza beyan kutucukları vasıtasıyla (*opt-out*) rıza gösterilmesi halinde, esasen kişiye reddetme hakkı tanınmış olmakla birlikte kişiye onaylayıcı bir eylem ile gösterebileceği tercih hakkı tanınmadığından ilgili kişinin rıza beyanı geçerli kabul edilmeyecektir. Bkz. GVK Tüzüğü, Giriş Bölümü, 32.Paragraf. Opt-out yönetimi hareketsizliğe bir sonuç bağlamakta olup, açık rıza veri toplama ve işleme öncesinde ilgili kişinin aktif bir harekette bulunmasını gerekli kıldığından, Article 29 Working Party tarafından bu tip yöntemlerle alınan rızanın geçerli olmadığı değerlendirilmektedir. Article 29 Working Party, Online Behavioural Advertising, s.15.

⁷²⁶ Taştan, s.160; Article 29 Working Party, Guidelines on Consent, s.12.

verilerin korunması alanında önemli çalışmalar yapan birçok kurum çeşitli raporlar aracılığı ile büyük veri ve yapay zeka uygulamalarında açık rıza şartlarının uygulanabilirliğine ilişkin sorunları gündeme getirmiştir. Aşağıda bu sorunlar, profillemeye ve otomatik karar uygulamaları bakımından sırayla incelenecektir.

Profillemeye ve otomatik karar alma faaliyetleri, genellikle, doğrudan ilgili kişi tarafından sağlanan veriler yerine, diğer verilerden türetilen veya çıkarılan verilere dayanır. Bu nedenle, profillemeye ve otomatik karar alma faaliyetleri şeffaf bir süreçte gerçekleşmeyebilir. Öte yandan, profillemeye faaliyetine hukuka uygunluk sebebi teşkil etmesi için ilgili kişinin rızasına dayanmak isteyen veri sorumlusunun, ilgili kişinin tam olarak neye rıza gösterdiğini anladığını gösterebilmesi ve rızanın her zaman veri işleme için uygun bir temel olmadığını göz önünde bulundurması gerekecektir. Her durumda, ilgili kişinin, işleme faaliyetine vermiş olduğu rızanın bilinçli bir seçimi temsil etmesi için, ilgili kişi kişisel verilerin öngörülen kullanım şekli ve işlemenin sonuçları hakkında yeterli şekilde bilgilendirilmelidir⁷²⁷. Ancak büyük veri ve yapay zeka uygulamaları ile gerçekleştirilen veri işleme faaliyeti, kişisel verileri işlenen kişilerin anlamlandıramayacağı derecede karmaşık bir şekilde gerçekleşmektedir. İlgili kişilerin, çoğunlukla algoritmaların çalışma şeklini kavrayabilmelerini sağlayacak donanım ve yeteneklere sahip olmadıkları göz önüne alındığında, profillemeye ve otomatik karar uygulamalarının barındırdığı riskleri anlayabilmeleri neredeyse imkansızdır⁷²⁸. İlgili kişi çoğunlukla kendisi hakkındaki profillemeye faaliyetinin farkında dahi değildir. Dolayısıyla ilgili kişi profillemeye açık rıza vermemişse, bu profil çıkarmaya dayalı olarak alınan bir otomatik karara da rıza göstermediği kabul edilir⁷²⁹. Örneğin, ilgili kişinin çerez (*cookies*) kullanımına yönelik açık rızasının bulunması, her zaman bu tür bir profillemeye dayalı otomatik karar faaliyetine de açık rızasının bulunduğu anlamına gelmemektedir⁷³⁰.

⁷²⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.20.

⁷²⁸ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.41.

⁷²⁹ Brkan, s.12.

⁷³⁰ Brkan, s.12.

Gizlilik bildirimleri genellikle ortalama bir internet kullanıcısının anlayamayacağı hukuki terminolojinin kullanıldığı oldukça karmaşık ve uzun metinler şeklinde düzenlenmektedir. Kullanıcıların/tüketicilerin, gerekli donanım ve yeteneklere sahip olsalar dahi, oldukça uzun ve karmaşık şekilde kaleme alınan gizlilik bildirimlerini baştan sona okumalarını beklemek de makul görünmemektedir⁷³¹. Nitekim birçok çalışma ile tüketicilerin çoğunlukla gizlilik politikalarının tamamını okumadıkları ve tamamını okuyup anlamadan kabul ettikleri somut şekilde ortaya koyulmuştur⁷³². Bu bağlamda, belirsiz ve karmaşık gizlilik bildirimlerinin pratikte gizlilik bildirimi yapılmamış olmasından farklı bir sonuç doğurmadığı söylenebilecektir. Gonzalez ve De Hert, ilgili kişiye yalın ve kolay anlaşılır bilgi sağlanması gerektiğini belirtmekle birlikte, büyük veri uygulamaları açısından bunun da önünde birtakım engeller bulunduğu değinmiştir⁷³³. Buna göre, basit bir dil kullanılarak ilgili kişiyi kapsamlı bir şekilde bilgilendirmek için gereken yeterli detay sağlanamayabilecektir. Nesnelerin interneti cihazlarının küçük ekranları, yapay öğrenme algoritmalarının kara kutu özelliği ve büyük veri analitiği ile ulaşılan sonuçların öngörülemez olması nedeniyle kişisel verilerin ikincil kullanımları hakkında yeterli bir şeffaflığın bulunmaması gizlilik bildirimlerin amacına hizmet etmesinin önünde engel teşkil eden sorunlardan birkaçıdır⁷³⁴. Bu sorunlara çözüm olarak, anlık bildirim, resim, simge veya ses gibi farklı araç ve yaklaşımların rol oynadığı şeffaflık üzerine kurulu bir bilgilendirme modelinin benimsenmesi tavsiye edilmiştir⁷³⁵. Nitekim Tüzüğün, kişisel verilerin hukuka uygun, adil ve şeffaf bir şekilde işlenmesi ilkesi uyarınca, ilgili kişinin işleme faaliyetinin varlığı ve amacı hakkında bilgilendirilmesi

⁷³¹ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.42.

⁷³² İlgili çalışmalar için bkz. Georgina KON, Does Anyone Read Privacy Notices? The Facts, <https://www.linklaters.com/en/insights/blogs/digilinks/does-anyone-read-privacy-notices-the-facts>; Brooke AUXIER & Lee RAINIE & Monica ANDERSON & Andrew PERRIN & Madha KUMAR & Erica TURNER, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, Pew Research Center, 15 Kasım 2019, <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>.

⁷³³ Gonzalez & De Hert, s. 601-602.

⁷³⁴ Gonzalez & De Hert, s. 601.

⁷³⁵ Gonzalez & De Hert, s. 602.

gerekliliğine değinen giriş bölümünün 60. paragrafında da bu bilgilendirmenin kolayca okunabilir ve anlaşılabilir kılınması için standart simgelerden yararlanılabileceği belirtilmektedir⁷³⁶.

GVK Tüzüğü'nde, ilgili kişi ile veri sorumlusu arasında “bariz bir güç dengesizliği” bulunan hallerde, ilgili kişiden rıza alınmış olmasının işleme faaliyeti için yeterli bir hukuka uygunluk sebebi teşkil etmemesi gerektiği, ilgili kişinin gerçek anlamda özgür bir şekilde tercih hakkının bulunmadığı durumlarda rızanın “özgür irade ile verilmiş” olduğunun kabul edilemeyeceği düzenlenmiştir⁷³⁷. İlgili kişinin herhangi bir zarara uğramaksızın rıza vermeyi reddetme ya da rızasını geri alma imkanına sahip olmadığı durumlarda, ilgili kişinin rıza göstermemesi halinde herhangi bir “aldatma, sindirme, zorlama veya önemli bir sonuç doğurma” riskinin olmadığı gösterilemediği sürece⁷³⁸, özgür iradeyle açıklanmış bir rızanın varlığından bahsedilemeyecektir⁷³⁹. Bunların yanında, ilgili kişilerin işleme faaliyetine rıza göstermeyi reddetmeleri, çoğunlukla, onlar için önemli veya gerekli hizmetlere erişimlerinin engellenmesi veya kısıtlanmasına neden olmaktadır. Günümüzde mobil uygulamaların birçoğu, kullanıcı bilgilerini davranışsal reklamcılık faaliyetleri için kullanmak üzere ilgili kişilerden açık rıza talep etmektedir. Örneğin, kullanıcıların fotoğraflarını yükleyerek üzerinde düzeltme yapabilmelerini sağlayan mobil uygulamaların, uygulamanın kullanılabilmesi için kullanıcıların konum bilgilerini ve davranışsal reklamcılık faaliyetlerinde kullanılmak üzere diğer verilerinin işlenmesine rıza gösterilmesini talep etmesi durumunda, ilgili kişi rıza göstermediği takdirde uygulamayı kullanamayacağından rızanın özgür irade ile verildiğinden bahsedilemeyecektir⁷⁴⁰. Diğer bir ifadeyle, profillemeye gerektirmeyen bir hizmetin ilgili kişinin profillemeye faaliyetine rıza göstermesi şartına dayandırılması halinde rızanın özgür iradeyle açıklandığından bahsedilemeyecektir. Bu bağlamda, profillemeye ve otomatik karar uygulamaları

⁷³⁶ Bkz. GVK Tüzüğü, Giriş Bölümü, 60.Paragraf.

⁷³⁷ Bkz. GVK Tüzüğü, Giriş Bölümü, 43.Paragraf.

⁷³⁸ Article 29 Working Party, Guidelines on Consent, s.7.

⁷³⁹ Bkz. GVK Tüzüğü, Giriş Bölümü, 42.Paragraf.

⁷⁴⁰ Article 29 Working Party, Guidelines on Consent, s. 6.

kapsamında ilgili kişilerden rıza alınsa dahi, rızanın, gerçekten bilinçli bir şekilde gösterilip gösterilmediği ve ilgili kişinin rıza gösterip göstermeme konusunda bir seçim imkanı tanınıp tanınmadığı belirsizlik yaratmaktadır.

Tüzüğün 22. maddesi kapsamındaki otomatik karar alma faaliyetleri için açık rıza alınması açısından sorun teşkil eden bir diğer husus ise “rıza yorgunluğu”dur. Rıza yorgunluğu, internet kullanıcılarının çevrimiçi ortamda kişisel verilerinin işlendiği her bir işlemde aktif bir davranışta bulunmak zorunda kalmalarının sonucunda veri işleme faaliyetinin içeriği ve amacını gözetmeksizin olumlu veya olumsuz yönde bir reaksiyon geliştirmelerini ifade eder⁷⁴¹. Tüzüğün 22. maddesi kapsamında veri işleme faaliyetlerinde, veri sorumlusunun, m. 22/2 kapsamında belirtilenlerin dışında kalan, veri sorumlusunun meşru menfaati de dahil olmak üzere diğer hukuka uygunluk sebeplerine dayanması mümkün değildir. Bu durum, ilgili kişinin rızasının alınması yoluna gidilmesi yönündeki eğilimde bir artışı da beraberinde getirmektedir. Bunun sonucunda ilgili kişide “rıza yorgunluğu” (*consent fatigue*) olarak adlandırılan durum ortaya çıkar⁷⁴². Tüzük m. 22 kapsamına girmeyen birçok işleme faaliyeti için çevrimiçi olarak rızası istenen kullanıcılar, halihazırda herhangi bir işleme faaliyetine düşünmeden rıza gösterir hale geldiklerinden, tamamen otomatik işlemeye dayalı karar alınması gibi gerçekten hassas işleme faaliyetlerine gereken özeni gösterememektedir⁷⁴³.

Yapay zeka ve büyük veri uygulamalarında kişisel verilerin işleme amacının verilerin ilk elde edilme anında belli olmaması ve sıklıkla toplanma amacından farklı bir amaç için işleniyor olması, rızanın “belirlilik” kriteri açısından sorun teşkil etmektedir. Çevrimiçi faaliyet gösteren ve büyük veri analitiği yöntemlerini kullanan hizmet verenler sıklıkla, ilerde ortaya çıkması muhtemel veri işleme amaçları da göz önüne alınarak ilgili kişilerden olabildiğince geniş kapsamlı işleme için rıza talep etme eğilimi göstermektedir. Bu durum amaçla sınırlılık

⁷⁴¹ Taştan, s.166.

⁷⁴² Andreas Nicolas HÄUSELMANN, Profiling and the GDPR: Harmonised Confusion, in: Jusletter 12 février 2018, s.12.

⁷⁴³ Häuselmann, s.12.

ilkesine aykırılık teşkil etmekle birlikte, ilgili kişiden alınacak rızanın “belirli bir konuya ilişkin olma” şartının da karşılanamamasına neden olmaktadır.

Öte yandan rızanın belirli bir işleme amacı için alınması halinde ise, kişisel verilerin toplanma anında bilinmeyen ve ilerde ortaya çıkması muhtemel işleme amaçları için, sosyal açıdan faydalı bir amaç olsa dahi, kullanılamaması söz konusu olabilmektedir⁷⁴⁴. Rızanın “belirli” olma şartı, tıbbi araştırma amacıyla sağlık kayıtlarının incelenmesi, bulaşıcı hastalık salgınının önceden tahmin edilmesi amacıyla milyarlarca internet aramasının analiz edilmesi, kara para aklama faaliyetlerinin tespiti ve bunların önlenmesi amacıyla finansal kayıtların araştırılması ve altyapı planlaması için, araç trafiğinin ve yayaların izlenmesi gibi birçok veri işleme faaliyetinde gelecekte ortaya çıkması muhtemel sosyal faydanın ve toplum için faydalı keşiflere ket vurulması riski barındırmaktadır⁷⁴⁵.

Öte yandan rızanın “belirli” olma şartının kapsamı, GVK Tüzüğü ile daraltılmıştır. Tüzüğün giriş bölümünün 33. paragrafında, kişisel verilerin toplanma anında bilimsel araştırma amacıyla işleneceğinin belirlenmesinin çoğu zaman mümkün olmadığından bahisle, ilgili kişilerin, bilimsel araştırma için kabul görmüş etik standartlara uygun gerçekleştirilmesi şartıyla, kişisel verilerinin belirli araştırma projeleri veya bilimsel araştırma konuları kapsamında işlenmesine izin verebilecekleri belirtilmektedir⁷⁴⁶. GVK Tüzüğü, sonraki işleme amacının bir hukuka uygunluk sebebinedayanması ve toplanma amacıyla uyumlu olması şartıyla, ilgili kişisadece belirli bir amaç için işlemeye izin vermiş olduğu hallerde dahi, verilerin daha sonra başka bir meşru amaç için işlenmesine izin vermektedir⁷⁴⁷.

Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı, rızanın kişisel verilerin korunmasının temel ve vazgeçilemez unsurlarından biri olduğu göz önüne alınarak

⁷⁴⁴ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.42.

⁷⁴⁵ EPRS, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, s.42.

⁷⁴⁶ Bkz. GVK Tüzüğü, Giriş Bölümü, 33.Paragraf.

⁷⁴⁷ Bkz. GVK Tüzüğü, Giriş Bölümü, 50.Paragraf.

büyük veri uygulamalarının özelliklerine uygun rıza yaklaşımlarının geliştirilmesi gerektiğini belirtilmiştir⁷⁴⁸. Zira büyük veri uygulamalarında halihazırda işlenmiş kişisel verilerin farklı amaçlar için sürekli yeniden kullanılması, veri koruma hukukunda genel kabul gören “bilgilendirme ve rıza alma” şeklindeki geleneksel rıza modelini, büyük veri ve yapay zeka uygulamaları açısından işlevsiz hale getirmiştir. Buna göre, ilgili kişilerin internet ortamında faaliyet gösteren bir hizmet sağlayıcı ile olan ilişkileri boyunca verilerinin farklı kullanımlarına izin verip vermeme hususunda tercih hakkına sahip oldukları kademeli bir onay süreci uygulanabilecektir⁷⁴⁹. Örneğin, mobil uygulama hizmet sağlayıcıları, kullanıcılardan başlangıçta geniş ve genel kapsamlı bir onay almak yerine, kullanıcıların konum verilerini analitik faaliyetlerinde kullanmak istediklerinde, kullanıcıdan buna yönelik anlık bildirim (*push notification*) ile onay vermesini talep edebilecektir⁷⁵⁰. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı, rızanın ilgili kişiden alınmasında ve ilgili kişinin rızasını geri alması süreçlerinde otomasyona başvurulmasını tavsiye etmiştir. Buna göre, kullanıcı adına onay veren yazılım araçları (*software agents*) ve büyük veri uygulamalarında başvuru sensör ve akıllı cihazlar aracılığı ile ilgili kişinin rızasını gösterir nitelikteki jest, hareket ve davranışların incelenmesi gibi yöntemler kullanılabilir⁷⁵¹.

Avrupa Veri Koruma Kurulu, sosyal medya kullanıcılarının hedeflenmesine ilişkin 2020 yılında yayınladığı rehberde, sosyal medya kullanıcılarının kendileri tarafından sağlanan veriler, kendileri hakkında gözlemlenen veriler ve çıkarılan verilere dayanılarak hedeflenmelerini çeşitli örnekler üzerinden incelemiştir. Çıkarılan verilere dayanan çevrimiçi davranışsal reklamcılık uygulamaları, bazı durumlarda sadece profillemeye bazı durumlarda ise GVK Tüzüğü m. 22 kapsamında düzenlenen ilgili kişi hakkında hukuki veya benzer derecede önemli etkiler doğuran

⁷⁴⁸ ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics, s.46.

⁷⁴⁹ ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In the Era of Big Data Analytics, s.46.

⁷⁵⁰ ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In the Era of Big Data Analytics, s.46.

⁷⁵¹ ENISA, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In the Era of Big Data Analytics, s.46.

profilleme de dahil olmak üzere otomatik karar alma içermektedir. Örneğin, Kısa filmlerle ilgili paylaşım yapan bir sosyal medya hesabının gönderilerini beğenen kişinin, bir kısa film festivali organizasyonunun “kısa filmlere ilgililik”, “cinsiyet”, “yaş” ve “ikamet yeri” gibi kriterler üzerinden hedeflediği kullanıcılara kendilerine ait sosyal medya hesaplarında yaklaşımakta olan festival ile ilgili reklamlar göstermesi halinde, Avrupa Birliği E-Gizlilik Direktifi⁷⁵² hükümleri de uygulama alanı bulacağından, ilgili kişinin önceden açık rızasının alınması gerektirir⁷⁵³.

Kurul’un başka bir örneğinde ise, sosyal medya hesabında sporla ilgilendiğini belirten bir kişi aynı zamanda ilgilendiği spor dallarının müsabaka sonuçlarını takip etmek için telefonuna bir uygulama indirmiş, müsabaka sonuçlarının yayınlandığı bir internet sayfasını dizüstü bilgisayarında tarayıcısının ana sayfası olarak ayarlamış ve mesai saatleri içinde işyerindeki masaüstü bilgisayarını son müsabaka sonuçlarını aratmak için kullanmıştır⁷⁵⁴. Bu kişi aynı zamanda birkaç çevrimiçi kumar sitesini de ziyaret etmektedir. Sosyal medya sağlayıcısı, kullanıcının çevrimiçi hareketlerini kullandığı farklı cihazlar üzerinden izlenmesiyle ve kullanıcının kendisi tarafından sağlanan bilgilerden kullanıcının çevrimiçi bahis oyunları ile ilgilenebileceği çıkarımında bulunur. Öte yandan, ilgili sosyal medya platformu, şirketlerin daha düşük gelirli ve dürtüsel davranmaya meyilli kişilerin hedefleyebilmelerini sağlayan bir hedefleme kriteri geliştirmiştir. Bahis yapmakla ilgilenen ve sıkı bir şekilde bahis oynamaya meyilli kişileri hedeflemek isteyen çevrimiçi bahis siteleri, reklamlarının gösterilmesi gereken kitleyi, sosyal medya sağlayıcısı tarafından sunulan bu hedefleme kriteri üzerinden hedefler. Kurul’a göre, bu örnekteki gibi çevrimiçi platformlarda bahis

⁷⁵² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>.

⁷⁵³ European Data Protection Board (EDPB), Guidelines 8/2020 on the Targeting of Social Media Users, Version 2.0, 13 Nisan 2021, s.25, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf (Kısaltılmışı “Guidelines 8/2020 on the Targeting of Social Media Users”).

⁷⁵⁴ European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, s.24-25,

reklamalarının gösterilmesi şeklinde gerçekleşen çevrimiçi davranışsal reklamcılık faaliyetleri, kişinin finansal durumunu önemli ölçüde ve olumsuz şekilde etkileme potansiyeline sahip çevrimiçi bahis oyunları ile ilgilenen finansal açıdan savunmasız kişileri hedeflediğinden, GVK Tüzüğü m.22 kapsamında değerlendirilebilecektir. Dolayısıyla ilgili kişinin açık rızasının alınması gerekmektedir. Nitekim izleme (*tracking*) tekniklerinin kullanılması nedeniyle E-Gizlilik Direktifi de uygulanacağından ilgili kişiden önceden izin alınması gerekecektir⁷⁵⁵.

3.2.2. Bir Sözleşmenin Kurulması veya İfası İçin Gerekli Olma

GVK Tüzüğü m.6/1(c) ile KVK Kanunu m.5/2(c) tahtında düzenlenen bu ilkeyle, bir hukuki işlem olan sözleşmenin, sözleşme ile amaçlanan sonucu doğurabilmesi için sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenebileceği hüküm altına alınmıştır⁷⁵⁶. Sözleşmenin kurulması veya ifası için gerekli olma, Tüzük m.22/2(a) uyarınca profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetleri açısından da hukuka uygunluk sebebi olarak hüküm altına alınmıştır⁷⁵⁷. Veri sorumlusunun gerçekleştireceği veri işleme faaliyetinin hukuka uygunluk sebebi kapsamında kabul edilebilmesi için, sözleşmenin kurulması ya da ifası için söz konusu kişisel verilerin işlenmesi “gerekli” olmalı, diğer bir ifadeyle veri sorumlusunun işleme faaliyetine alternatif olarak kabul edilebilecek başka bir imkanı bulunmamalıdır⁷⁵⁸.

Maddedeki “gereklilik” kistasının ölçüsünün ne olacağına ilişkin Tüzük’te bir açıklamaya yer verilmemiştir. 29. Madde Çalışma Grubu, gereklik kistasının dar bir şekilde yorumlanması gerektiğini, bir sözleşmenin ifası için gerçekten

⁷⁵⁵ European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, s.26.

⁷⁵⁶ Tüzüğün gerekçesinde, bir sözleşmenin kurulması niyetiyle ya da sözleşmenin ifası için kişisel veri işlenmesinin gerekli olması halinde, işleme faaliyetinin hukuka uygun olduğu belirtilmiştir. Bkz. GVK Tüzüğü, Giriş Bölümü, 44.Paragraf.

⁷⁵⁷ Bkz. GVK Tüzüğü, m.22/(a).

⁷⁵⁸ Çekin, s.68-69.

gerekli olmayan ancak veri sorumlusu tarafından ilgili kişiye tek taraflı olarak dayatılan veri işleme faaliyetlerine uygulanamayacağını, sözleşmenin bazı işleme faaliyetlerini kapsamaması veya işleme faaliyetinin sözleşmede belirtilmiş olmasının sözleşmenin ifası için gerekli olduğu anlamına gelmeyeceğini belirtmiştir⁷⁵⁹. Avrupa Veri Koruma Kurulu ise, Tüzüğün 6/1(b) maddesinin uygulanabilir olup olmadığının değerlendirilmesi için aşağıdaki soruların yol gösterici olabileceğine işaret etmiştir⁷⁶⁰:

- İlgili kişiye sağlanan hizmetin niteliği nedir? Hizmetin ayırt edici özellikleri nelerdir?
- Sözleşmenin temel amacı nedir?
- Sözleşmenin temel unsurları nelerdir?
- Sözleşmenin taraflarının sözleşme konusu hizmete ilişkin karşılıklı bakış açıları ve beklentileri nelerdir?
- Sözleşme konusu hizmet ilgili kişiye nasıl tanıtılır veya reklamı nasıl yapılır?
- Sözleşme konusu hizmetin herhangi bir kullanıcısı, hizmetin doğası gereği, taraf olduğu sözleşmenin kurulması veya ifa edilmesi için kişisel verilerinin öngörülen şekilde işlenmesini makul bir şekilde öngörebilir mi?

29. Madde Çalışma Grubu, gereklilik değerlendirmesinin nasıl yapılacağı ile kişisel verilerin amaçla sınırlılık ilkesine uygun işlenmesi arasında açık bir bağlantı olduğunu belirtmiştir⁷⁶¹. Zira büyük veri uygulamalarında gereklilik kriterinin belirlenmesindeki sorun, büyük veri analitiği yöntemlerinin doğası gereği, bir ürünün satılması veya bir hizmetin sunulması için gerekli olandan fazla verinin işleniyor olmasıdır⁷⁶². Diğer bir ifadeyle, ilgili kişiden çoğunlukla bir sözleşmenin kurulması veya ifası için gereken minimum veri alınsa da büyük veri

⁷⁵⁹ Article 29 Working Party, Legitimate Interest, s.16-17.

⁷⁶⁰ European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, 9 Nisan 2019, s.9, https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf (Kısaltılmışı “Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR”).

⁷⁶¹ Article 29 Working Party, Legitimate Interest, s.17.

⁷⁶² ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.35.

analitiği yöntemleri ile bu verilerden yeni veriler oluşturulabilmekte, veriler toplandıkları amaçlardan farklı bir amaç için işlenebilmektedir. 29. Madde Çalışma Grubu'nun örneği üzerinden somutlaştırılacak olursa, örneğin, herhangi bir üyelik talep etmeyen e-ticaret sitelerinde gerçekleştirilen alışverişlerde ödemenin ve teslimatın gerçekleştirilebilmesi için, kullanıcının kredi kartı ve adres bilgileri gerekir⁷⁶³. Bu bilgilerin işlenmesi, sözleşmenin ifası için gerekli olarak kabul edilmektedir. Ancak, kişinin ilgili alışveriş sitesine gerçekleştirdiği ziyaretlerinden toplanan verileri aracılığıyla beğenileri ve tercihlerine ilişkin bir profilinin çıkarılması, satım sözleşmesinin kurulması için gerekli değildir. Bu bağlamda profillemenin, sözleşme içeriğinde özellikle belirtilmiş olması, bu faaliyetin tek başına “gerekli” olmasını sağlamayacaktır⁷⁶⁴.

Avrupa Birliği Veri Koruma Kurulu, dolandırıcılığın önlenmesi amacıyla gerçekleştirilen izleme ve profilleme faaliyetlerinin sözleşmenin kurulması veya ifası için gerekli olma şartına dayanılarak gerçekleştirilemeyeceğini, ancak veri sorumlusunun meşru menfaati veya hukuki yükümlülüğünü yerine getirebilmesi sebeplerinden birine dayanılabileceğini belirtmiştir⁷⁶⁵. Kurul, çevrimiçi davranışsal reklamcılık faaliyetleri kapsamında gerçekleştirilen izleme ve profilleme faaliyetlerinin de sözleşmenin kurulması veya ifası için gerekli olma kriterlerini karşılamadığını ifade etmiştir. Kurul bu görüşünü çevrimiçi davranışsal reklamcılık faaliyetlerinin çevrimiçi hizmetlerin zorunlu bir unsuru olmadığına ve ilgili hizmetin dolaylı olarak reklamcılık gelirleri ile finanse edilmesinin de yeterli bir gerekçe olmadığına dayandırmıştır⁷⁶⁶. Kurul, içerik kişiselleştirme (*content personalization*) faaliyetlerinin, bazı durumlarda sözleşmenin kurulması veya ifası için gerekli olarak kabul edilebileceğini değerlendirmiştir. İçerik kişiselleştirmenin çevrimiçi bir hizmetin kendine özgü bir yönü olup olmadığı, her bir hizmetin özellikleri gözetilerek, ortalama bir kullanıcının hizmet şartlarının yanı sıra

⁷⁶³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.13.

⁷⁶⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.13.

⁷⁶⁵ European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR, s.12.

⁷⁶⁶ European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR, s.12-13.

hizmetin kullnıcılara tanıtılma şekli tahtında hizmetten beklentileri ve ilgili hizmetin kişiselleştirme olmaksızın sağlanıp sağlanamayacağına göre değerlendirilecektir. Bu bağlamda, örneğin, içerik kişiselleştirmenin sözleşmenin amacı için gerekli olmadığı ancak kullanıcıların sözleşme konusu hizmetle olan etkileşimlerinin artırılması için gerçekleştirildiği hallerde, veri sorumlularının işleme faaliyetine uygulanabilir olan diğer hukuka uygunluk sebeplerine başvurusu gerekir. Bir çevrimiçi haber sitesinin, kullanıcının beğenilerine göre farklı kaynaklardan uyarlanan haberleri tek bir arayüz üzerinden sunabilmek için kullanıcıdan ilgi alanlarına ilişkin bir profil oluşturmasını talep etmesi durumunda, hizmetin ifası ile içeriğin kişiselleştirilmesi doğrudan ilişkili olduğundan, veri sorumlusunun 6/1(b) maddesine dayanabileceği kabul edilebilecektir. Çevrimiçi otel rezervasyonu hizmeti sağlayan bir internet sitesinin, geçmiş rezervasyonlara ilişkin bilgileri kullanarak kullanıcıların harcama profillerini çıkardığı bir senaryoda ise, söz konusu profillemeye faaliyeti çevrimiçi rezervasyon hizmetinin sunulması için gerekli olmadığından veri sorumlusunun farklı bir hukuka uygunluk sebebine dayanması gerekecektir. Benzer şekilde, çevrimiçi alışveriş sitesinin, potansiyel alıcılara daha önce görüntüledikleri ürünlere göre kişiselleştirilmiş ürün önerilerinde bulunması halinde, kişiselleştirme faaliyeti alışveriş hizmeti sunmak için gerekli olmadığından veri sorumlusu hukuka uygunluk sebebi olarak 6/1(b) maddesine dayanamayacaktır⁷⁶⁷.

GVK Tüzüğü'nün 22. maddesinde ilgili kişinin “kendisi ile ilgili hukuki sonuçlar doğuran veya kendisini benzer şekilde önemli sderecede etkileyen profillemeye de dâhil olmak üzere tamamen otomatik işlemeye dayalı bir karara konu olmama hakkı”nın istisnalarından biri de ilgili veri işleme faaliyetinin sözleşmenin kurulması veya ifası için “gerekli” olmasıdır⁷⁶⁸. Veri sorumluları, sözleşmenin kurulması veya ifası amacıyla, GVK Tüzüğü m.22/1 kapsamında “profillemeye de dâhil olmak üzere tamamen otomatik işlemeye dayalı karar alma” uygulamalarını tercih edebilmektedir. Zira büyük verinin kullanıldığı ve işlendiği sistemler, rutin

⁷⁶⁷ European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR, s.12-13.

⁷⁶⁸ Bkz. GVK Tüzüğü, m.22/2(a).

olarak sürece insan katılımını elverişsiz veya imkansız hale getirmekte, hedefe ulaşılabilmesi için veri işleme sürecinin tamamen otomatik şekilde yürütülmesini gerektirebilmektedir⁷⁶⁹. Her ne kadar veri sorumluları, çeşitli avantajları sebebiyle profillemeye ve otomatik karar alma faaliyeti gerçekleştirmeyi tercih etseler de, bunların hiçbiri tek başına işleme faaliyetinin sözleşmenin ifası için gerekli olduğuna ilişkin yeterli bir sebep teşkil etmemektedir⁷⁷⁰. Bu bağlamda profillemeye ve otomatik karar alma sistemleri kapsamında kişisel verilerin işlenmesinin bir sözleşmenin kurulması yahut ifası için gerekli olduğunun tespiti ve ispatının çoğunlukla kolay olmadığı belirtilmektedir⁷⁷¹. 29. Madde Çalışma Grubu konuyla ilgili rehberde, bu durumda, veri sorumlusunun bireyin temel haklarına daha az müdahale eden veya hiç müdahale etmeyen bir veri işleme yönteminin kullanılıp kullanılamayacağını da göz önüne alarak, bu şekilde bir veri işlemenin gerekli olduğunu gösterebilmek zorunda olduğunu belirtmiştir. Kişinin temel hak ve özgürlüklerine daha hafif bir müdahale ile veya hiç müdahale edilmeden de aynı sonuca ulaşılmasını mümkün kılan etkili bir yöntem mevcut ise, bu durumda işleme faaliyetinin “gerekli olmadığı” sonucuna varılacaktır⁷⁷².

Brkan, maddenin dar yorumlanması halinde, sözleşmenin ifası için gerekli olduğu gerekçesiyle otomatik kararların hukuka uygun kabul edilmesinin neredeyse imkansız hale geleceği görüşündedir⁷⁷³. Brkan’a göre, bir sigorta veya kredi sözleşmesinin akdedilmesinin bir risk değerlendirmesi yapılmasını gerektirdiği ileri sürülebilecekse de bu riskin mutlaka kişisel verilerin otomatik araçlarla işlenmesi suretiyle değerlendirilmesi gerektiğini savunmak aynı derecede kolay değildir⁷⁷⁴. Benzer şekilde, uçuş fiyatları genellikle potansiyel alıcının profili dikkate alınarak "dinamik fiyatlandırma" yoluyla belirlense de bu tür bir otomatik fiyat belirleme faaliyetinin bu satın alma sözleşmesinin ifası için gerçekten gerekli olduğunu savunmak da pek kolay değildir. Brkan, açıklanan nedenlerle, maddedeki

⁷⁶⁹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.23.

⁷⁷⁰ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.13

⁷⁷¹ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.35.

⁷⁷² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.23.

⁷⁷³ Brkan, s.11.

⁷⁷⁴ Brkan, s.11.

“gereklilik” şartının bir sözleşmenin akdedilmesini “mümkün kılan” bir kıstas olarak dikkate alınması gerektiğini ileri sürmüştür. Buna göre, örneğin kredi riskinin otomatik olarak değerlendirilmesi, ilgili kişinin bankadan kredi kartı almasını sağlayan bir sözleşmenin akdedilmesini mümkün kılıyorsa, söz konusu otomatik değerlendirmenin bu sözleşmenin akdedilmesini mümkün kıldığı dolayısıyla da sözleşmenin ifası için gerekli olduğu kabul edilebilecektir⁷⁷⁵.

Belirtilmelidir ki, GVK Tüzüğü m.22/1 tahtında düzenlenen tamamen otomatik işlemeye dayalı karar alma faaliyetinin bir sözleşmenin kurulması veya ifası için mutlaka gerekli olduğu durumlar oldukça istisnaidir⁷⁷⁶. Bu istisnai durumlara, iş başvurularının otomatik olarak değerlendirildiği sistemler örnek olarak gösterilebilir. Onbinlerce başvurunun geldiği bir iş ilanında, ilgili kişiyle bir iş sözleşmesinin kurulabilmesi amacıyla, en azından ilandaki ilgili aday kriterlerine uymayan başvuruların ilk etapta elenerek, uygun adayların bir kısa listesinin çıkartılması için otomatik karar mekanizmasının kullanılmasının “gerekli” olduğu kabul edilebilir⁷⁷⁷. Benzer şekilde, bankaların, kredi talebinde bulunan kişilerin başvurularını anlık olarak otomatik şekilde sonuçlandırmak üzere kullandıkları yazılımların da gereklik kıstasını karşıladığı savunulabilecektir. Zira banka ve finansal kuruluşların, kredi başvurusunda bulunan kişinin talebini değerlendirebilmeleri için, kredinin geri ödenmeme riskini belirleyebilmek için kredinin geri ödenme ve ödenmeme ihtimallerine ilişkin bazı öngörüler edinmeleri gerekir. Bu kapsamda, başvuruda bulunan kişi hakkında farklı kurumlardan ve kaynaklardan veri toplanarak ilgili kişinin kredi notunun algoritmalar aracılığı ile hesaplandığı ve başvurusunun buna göre sonuçlandırıldığı otomatik karar sistemlerinin kullanılması kredi sözleşmesinin kurulması için gerekli olarak değerlendirilebilecektir.

⁷⁷⁵ Brkan, s.11

⁷⁷⁶ Information Commissioner’s Office, Big Data, Artificial Intelligence, Machine Learning and Data Protection, 73.Paragraf.

⁷⁷⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.23.

3.2.3. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Veri İşlemenin Zorunlu Olması

GVK Tüzüğü m.6/1(c) ve KVK Kanunu m.5/2(ç) uyarınca, veri sorumlusunun kanunlarla kendisine yüklenmiş olan bir sorumluluğu yerine getirmesi kişisel verilerin işlenmesini gerektiriyorsa, ilgili kişiden açık rıza alınmaksızın veri işleme faaliyeti gerçekleştirilebilir. Kamu tüzel kişileri de özel hukuk tüzel kişileri de bu hukuka uygunluk sebebinden yararlanabilir. Veri sorumlusunun vergi, sosyal güvenlik, kara paranın aklanması ve dolandırıcılığın önlenmesi ile ilgili hukuki düzenlemelerden doğan yükümlülükleri ile adli makamlar tarafından talep edilen belgelerin ibrazı bu kapsamdadır⁷⁷⁸. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için profillemeye ve otomatik karar alma mekanizmalarının kullanılması suretiyle veri işlemenin gerekli olduğu durumlar da söz konusu olabilir. 29. Madde Çalışma Grubu dolandırıcılığın ve kara para aklamanın önlenmesi amacıyla gerçekleştirilecek, m.22'nin uygulama alanı dışında kalan profillemeye ve otomatik karar alma faaliyetlerinin bu kapsamda kabul edilebileceğini belirtmiştir⁷⁷⁹.

Tüzük m.22/2 (b) uyarınca, “veri sorumlusunun tabi olduğu ve ilgili kişinin hak ve özgürlükleri ile meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de hüküm altına alındığı Avrupa Birliği veya üye devlet mevzuatında otomatik karar alma faaliyetine izin verilmesi” halinde, Tüzüğün 22. maddesinin ilk fıkrası uygulanmamaktadır. Dolayısıyla Avrupa Birliği veya üye devlet hukukunda izin verilmesi halinde, veri sorumlusu tamamen otomatik işlemeye dayalı karar alma faaliyeti kapsamında kişisel veri işleyebilecektir. Tüzüğün giriş bölümünün 71.paragrafında, Birlik kurumlarının veya ulusal gözetim organlarının düzenlemeleri, standartları ve tavsiyelerine uygun olarak yürütülen dolandırıcılığın ve vergi kaçakçılığının izlenmesi ve önlenmesi veya veri sorumlusu tarafından bir hizmetin güvenliğini ve güvenilirliği sağlamak amacıyla

⁷⁷⁸ Article 29 Working Party, Legitimate Interest, s.19.

⁷⁷⁹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.13.

gerçekleştirilenler de dahil olmak üzere, veri sorumlusunun tabi olduğu Birlik veya üye devlet mevzuatında açıkça izin verilen hallerde, profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetlerine izin verileceği belirtilmiştir⁷⁸⁰. Finansal kuruluşlar kara paranın aklanmasıyla mücadele (*anti money laundering*) ve müşterini tanı (*know your customer*) ilkesi gereği müşterileri hakkında geçmiş sorgulaması (*background screening*) yapmakla yükümlüdür. Bu kapsamda müşteri tanıma ve kimlik tespiti amacıyla, müşterinin risk profili çıkarılmakta ve bu profile dayanılarak bir karar alınmaktadır. Belirtilmelidir ki, her ne kadar karapara aklamayla mücadele ve müşterini tanı ilkesi kapsamında gerçekleştirilen müşteri sorgulamaları veri sorumlusunun hukuki sorumluluğunu yerine getirmesi için bir gereklilikse de, bu kapsamda gerçekleştirilen profillemeye ve otomatik karar alma faaliyetinin m.22 kapsamına girmesi halinde, m.22'nin hukuka uygunluk sebepleri arasında "hukuki yükümlülüğün yerine getirilmesi" bulunmadığından, 22. maddede belirtilen istina hallerinden birine dayanılması gerekecektir⁷⁸¹. Veri sorumlusunca işlemenin m.22'nin uygulama alanına girdiği değerlendiriliyorsa, hukuka uygunluk sebebi olarak m.22/2(b)'ye dayanılabilecektir⁷⁸².

PNR Direktifi⁷⁸³, otomatik karar alma faaliyetine izin veren ve uygun tedbirlerin alındığı Birlik mevzuatına örnek olarak gösterilmektedir⁷⁸⁴. Direktif kural olarak "bir kişi üzerinde olumsuz bir hukuki etki yaratan veya bir kişiyi önemli ölçüde etkileyen" tamamen otomatik işlemeye dayalı karar alma faaliyetlerine izin vermemekle birlikte, terörizm faaliyetlerine katılım ihtimalleri bağlamında yetkili makamlar tarafından gözetim altında tutulması gereken kişilerin otomatik olarak eşleştirilmesine veya kimliklerinin tespit edilmesine, bu işlemlerin

⁷⁸⁰ Bkz. GVK Tüzüğü, Giriş Bölümü, 71.Paragraf.

⁷⁸¹ Häuselmann, s.12.

⁷⁸² Häuselmann, s.18.

⁷⁸³ Directive (EU) 2016/681 of the European Parliament and of the Council Of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (Kısaltılmışı "PNR Direktifi") için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681&from=EN>.

⁷⁸⁴ Brkan, s.11.

otomatik olmayan yollarla gözden geçirilmesi şartıya, izin vermektedir⁷⁸⁵. Otomatik karar almaya izin veren Üye Devlet mevzuatlarından biri ise, sigortacılık faaliyetleri kapsamında tamamen otomatik işlemeye dayalı karar alınabilmesine açıkça izin veren ve GVK Tüzüğü'nü uygulayan Alman yasasıdır⁷⁸⁶.

3.2.4. Veri Sahibinin veya Üçüncü Bir Gerçek Kişinin Hayati Menfaatlerinin Korunması İçin İşleme Faaliyetinin Gerekli Olması

GVK Tüzüğü m. 6/1(d) tahtında düzenlenen bu hukuka uygunluk sebebi, veri işleme faaliyetinin veri sahibinin veya üçüncü bir gerçek kişinin hayati menfaatlerinin korunması için gerekli olduğu halleri kapsar. Bu sebebe dayanılabilmesi için, veri sorumlusunun dayanabileceği başka bir hukuka uygunluk sebebinin bulunmaması gerekir⁷⁸⁷. Bu tür veri işleme faaliyetlerinin bazıları, ilgili kişinin hayati menfaatlerinin korunmasının yanında kamu yararının gözetilmesi açısından da önem teşkil eder⁷⁸⁸. Hayati tehlikeye neden olan salgın hastalıkların yayılımının tahmin edilerek aşılarda dağıtım, okulların kapatılıp kapatılmayacağı veya seyahat kısıtlamaları konusunda kararlar alınabilmesi için geliştirilen modellerde insani amaçlar için gerçekleştirilen profillemeye ve otomatik karar alma faaliyeti buna örnek olarak gösterilebilir⁷⁸⁹. Bu hallerde, işleme faaliyetinin hem kamu yararına hem de ilgili kişinin hayati çıkarlarına hizmet ettiği kabul edilebilecektir⁷⁹⁰.

Benzer şekilde, aynı aileye mensup kişilerin, bazı hastalıklara yatkınlıklarının tespit edilerek bu hastalıklara yakalanmalarını önleme amaçlı

⁷⁸⁵ Bkz. PNR Direktifi, m.7/6, m.6/5.Brkan, s.11.

⁷⁸⁶ Detaylı bilgi için bkz. Brkan, s.12.

⁷⁸⁷ Bkz. GVK Tüzüğü, Giriş Bölümü, 46. Paragraf.

⁷⁸⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.14.

⁷⁸⁹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.14. 2017 yılında İngiltere’de “BBC Pandemic” isimli bir uygulamanın kullanılması ile toplanan veriler aracılığıyla ölümcül bir grip salgını yaşanması ihtimaline yönelik bir deney çalışması gerçekleştirilmiştir. Bkz. BBC, BBC Pandemic Join a Potentially Life-Saving Citizen Science Experiment, <https://www.bbc.co.uk/programmes/articles/315gcc2VLF8PC9nFdDM30hm/bbc-pandemic-join-a-potentially-life-saving-citizen-science-experiment>.

⁷⁹⁰ Bkz. GVK Tüzüğü, Giriş Bölümü, 46.Paragraf.

tedavi görmelerini sağlamaya yönelik olarak genetik profillerinin çıkarılmasında da hayati menfaatlerin korunmasına dayanılabilecektir. Ancak bu ve benzeri durumların oldukça nadir olduğunu belirtmek gerekir⁷⁹¹. Diğer yandan veri işlemenin özel nitelikli kişisel veri içermesi halinde, işleme faaliyetinin GVK Tüzüğü m.9/2(c) kapsamında düzenlenen şartlarını da karşılaması gerekmektedir. Buna göre, özel nitelikli kişisel verilerin işlenmesini gerektiren bir veri işleme faaliyetinin ilgili kişi ya da üçüncü bir gerçek kişinin hayati menfaatlerinin korunması açısından gerekli olduğu iddiasına dayanılabilmesi için, ilgili kişinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması aranacaktır⁷⁹².

3.2.5. Kamu Yararı İçin Gerçekleştirilen Bir Görevin Yerine Getirilmesi veya Veri Sorumlusunun Resmi Yetkisini Kullanması İçin Veri İşlemenin Gerekli Olması

Tüzüğün 6/1(e) maddesi uyarınca kişisel veriler, “kamu yararına gerçekleştirilen bir görevin yerine getirilmesi ya da veri sorumlusuna verilen resmi bir yetkinin kullanılması hususunda işleme faaliyetinin gerekli olması” durumunda işlenebilecektir. KVK Kanunu’nda bu düzenlemeye karşılık gelen bir maddeye yer verilmemiştir⁷⁹³. Kamu tarafından büyük veri analitiği yöntemlerinin kullanıldığı veri işleme faaliyetlerinde, veri sorumlularınca ilgili kişinin rızasına veya meşru menfaat hukuka uygunluk sebebine dayanılamamaktadır. Kamu tarafından gerçekleştirilen profillemeye ve otomatik kararfaaliyetlerinde bu uygunluk sebebine dayanabilmesi için, kişisel veri işlenmesini gerektiren görev veya resmi yetkinin

⁷⁹¹ Council of Europe, The Protection of Individuals with regard to Automatic Processing of Personal Data in the Context of Profiling, Recommendation CM/Rec (2010)13 and Explanatory Memorandum, s.46, <https://rm.coe.int/16807096c3>.

⁷⁹² Bkz. GVK Tüzüğü, m.9/2 (c).

⁷⁹³ KVK Kanunu’nun “kanunlarda açıkça öngörülme” başlıklı 5/2(a) maddesi uyarınca kişisel veriler KVK Kanunu dışındaki kanunlarda işleme faaliyetine ilişkin açık düzenleme olması halinde işlenebilir. Küzeci, Kanun’daki bu istisnayı, ilgili hükümde hukuka uygunluk sebeplerinin sınırlı sayıda belirlenmesi olanağını ortadan kaldırdığı, hangi hallerde diğer kanunlarla bu alanda düzenleme yapılabileceğine ilişkin bir sınırlamaya Anayasada da yer verilmediği gerekçesiyle eleştirmiştir. Bu bağlamda, GVK Tüzüğü’nde “kanunda açıkça öngörülmüş olma” halinin bir hukuka uygunluk hali olarak düzenlenmediği ancak “işlemenin kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusunun resmi yetkisini kullanması için veri işlemenin gerekli olması” halinde hukuka uygun şekilde veri işlemenin mümkün olduğu belirtilerek, KVK Kanunu’nun 5/2-a maddesindeki işleme şartının da benzer şekilde düzenlenmesinin meşru veri işleme hallerinin öngörülebilirliği açısından faydalı olacağı ifade edilmiştir. Bkz. Küzeci, s.342-343.

açık bir hukuki dayanağı bulunmalıdır⁷⁹⁴. Profillemeye ve otomatik karar faaliyeti, “gereklilik” şartı uyarınca, kamu yararı için gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusunun resmi yetkisini kullanması ile doğrudan ilgili ve bunun için gerekli olmalıdır. Veri sorumlusu görevin yerine getirilmesi veya yetkinin kullanılmasında, ilgili kişinin temel haklarına daha az ya da hiç müdahale etmeyen alternatif bir yöntemle başvurma imkanına sahipse, veri işleme faaliyetinin gerekliliğinden bahsedilemeyecektir⁷⁹⁵. Kanundaki ilgili düzenlemeler gereği, şüpheli işlemleri mali suçların araştırılması ve kara paranın aklanmasını önlemekle görevli kamu otoritelerine bildirmekle yükümlü olan bankaların, bu yükümlülüklerini yerine getirmek için müşterilerinin profilini çıkarması bu kapsamda değerlendirilebilecektir⁷⁹⁶.

3.2.6. Kişisel Verilerin İşlenmesinin Veri Sorumlusunun veya Üçüncü Bir Kişinin Meşru Menfaati için Gerekli Olması

GVK Tüzüğü m.6/1(f) uyarınca, ilgili kişinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hak ve özgürlüklerinin, veri sorumlusu veya üçüncü bir kişinin meşru menfaatlerine ağır bastığı haller dışında, veri sorumlusunun meşru mefaati için veri işlenmesinin gerekli olması hukuka uygunluk hallerinden biri olarak kabul edilmiştir. Benzer şekilde KVK Kanunu m.5/2(f)’de ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatinin kişisel veri işlenmesini zorunlu kılması halinde, ilgili kişinin açık rızası olmasa dahi işleme faaliyetinin hukuka uygun olduğu düzenlenmiştir. Veri sorumlusunun meşru menfaati, diğer hukuka uygunluk sebeplerinin uygulanamadığı durumlarda, başvurulacak son çare olmadığı gibi, her türlü veri işleme faaliyetini hukuka uygun hale getirecek bir dayanak olarak da değerlendirilmemelidir⁷⁹⁷. Zira veri sorumlusunun meşru menfaat hukuka

⁷⁹⁴ ICO, Guide to the General Data Protection Regulation, s.77.

⁷⁹⁵ ICO, Guide to the General Data Protection Regulation, s.76.

⁷⁹⁶ Council of Europe, The Protection of Individuals with regard to Automatic Processing of Personal Data in the Context of Profiling, s.45.

⁷⁹⁷ Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin İşlenme Şartları, s.17, <https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari>.

uygunluk sebebine dayanılabilmesi, sadece kişisel veri işleme faaliyetinin söz konusu meşru menfaatin gerçekleşmesi için “gerekli” olması halinde mümkündür. Diğer bir ifadeyle, kişisel veri işlenmeden de söz konusu menfaatin gerçekleştirilmesi mümkünse, söz konusu veri işleme faaliyetinin gerekli olduğundan bahsedilemeyecektir. Bu bağlamda, kişisel veri işleme faaliyetinin meşru menfaatin gerçekleştirilmesi için zorunlu veya gerekli olduğunun kabul edilebilmesi için, veri işleme faaliyeti ile meşru menfaat arasında sıkı bir ilişki olması⁷⁹⁸ ve veri işleme faaliyetinin meşru menfaatin gerçekleştirilmesi için alternatifi olmayan bir yöntem olması gerekir⁷⁹⁹.

Meşru menfaat hukuka uygunluk sebebi, ilgili kişinin açık rızasına dayanmanın elverişli olmadığı hallerde veri sorumluları açısından kişisel verilerin hukuka uygun şekilde işlenmesi için bir alternatif teşkil etmektedir. İlgili kişinin açık rızasına dayanılması halinde, veri sorumlusu işleme faaliyetini kişisel verilerin korunmasına hakim olan ilkelere uygun şekilde yerine getirmekle yükümlü iken, ilgili kişi ise rıza göstermemesi halinde gerçekleşmeyecek bir veri işleme faaliyetine onay verip vermemekten sorumludur⁸⁰⁰. İlgili kişiden açık rıza alınmasından farklı olarak, meşru menfaat hukuka uygunluk sebebinde, sorumluluk veri sorumlusuna yüklenmiştir⁸⁰¹.

Veri sorumlusunun meşru menfaatinin hukuka uygunluk sebebi olarak kabul edilip edilmeyeceğinin tespitinde, üç kademeli bir meşru menfaat değerlendirmesi (*legitimate interest assesment*) yapılmalıdır⁸⁰². Bu değerlendirme ile veri sorumlusunun menfaatleri ile ilgili kişinin temel hak ve özgürlüklerinin kısıtlanması arasında bir denge kurulması sağlanır. İlk olarak, veri sorumlusunun

⁷⁹⁸ Çekin, s.72.

⁷⁹⁹ Çekin, s.69.

⁸⁰⁰ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.34.

⁸⁰¹ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.34.

⁸⁰² ICO, Guide to the General Data Protection Regulation, s.81-86; Article 29 Working Party, Legitimate Interests, s.24-25; Kişisel Verilerin İşlenme Şartları Rehberinde ise iki kademeli bir değerlendirmeden bahsedilmektedir. Buna göre, ilk olarak veri sorumlusunun meşru menfaatinin varlığı, ikinci olarak ise, bu menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar vermediği tespit edilmelidir. Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları, s.16.

meşru menfaatinin varlığı değerlendirilmelidir. Bu değerlendirmede, kişisel verileri işleme amacı ile veri sorumlusunun meşru menfaatinin birbirine karıştırılmaması önemlidir. Zira kişisel verileri işleme amacı, kişisel verilerin özel olarak ne sebeple işlendiği ile ilgili bir kavramken, veri sorumlusunun meşru menfaati, veri sorumlusunun veya toplumun işleme faaliyetinden elde edebileceği faydayı ifade eder⁸⁰³. Değerlendirme sonucunda, veri sorumlusunun kişisel veri işlemeyi zorunlu kılan (i) hukuka uygun, (ii) ilgili kişinin temel hak ve özgürlüklerine zarar vermediği yeterince açık bir şekilde belli olan, (iii) gerçek ve halihazırda mevcut bir meşru menfaatinin bulunduğu sonucuna varılması gerekir⁸⁰⁴. İkinci olarak, işleme faaliyetinin bu amaç için “gerekli” olduğu tespit edilmelidir. Son olarak ise, veri sorumlusunun bu kriterleri karşılayan meşru menfaatinin ilgili kişinin temel hak ve özgürlüklerine zarar vermediği belirlenmelidir⁸⁰⁵.

Profilleme ve otomatik karar alma faaliyetlerini meşru menfaate dayanarak gerçekleştirecek veri sorumlularının, veri analitiği uygulamalarının ilgili kişinin mahremiyetine etkisini değerlendirmeleri gerekir⁸⁰⁶. Belirtilmelidir ki, burada izin verilen profilleme ve otomatik karar alma faaliyeti, GVK Tüzüğü’nün 22/1 maddesinde belirtilen, “ilgili kişinin kendisi ile ilgili hukuki sonuçlar doğuran veya kendisini benzer derecede önemli şekilde etkileyen profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma” dışında kalan profilleme ve otomatik karar alma faaliyetleridir. Zira GVK Tüzüğü m.22/1 tahtında tanımlanan profilleme ve otomatik karar almanın izin verildiği haller, GVK Tüzüğü m. 22/2 altında sınırlı sayıda sayılmış olup, meşru menfaat hukuka uygunluk sebebi bunlardan biri değildir. Meşru menfaat değerlendirmesinde, ilgili kişiye ait profilin ne derecede detay içerdiği (ilgili kişinin, “ayda en az bir kere online yemek siparişi verenler” şeklinde geniş bir topluluk içinde mi profillendiği yoksa daha detaylı bir segmentasyona tabi tutularak hedefleme faaliyetine mi konu edildiği),

⁸⁰³Article 29 Working Party, Legitimate Interests, s. 24; KVKK, Kişisel Verilerin İşlenme Şartları, s.16.

⁸⁰⁴Article 29 Working Party, Legitimate Interests, s.25.

⁸⁰⁵ ICO, Guide to the General Data Protection Regulation, s.81-86; Article 29 Working Party, Legitimate Interests, s.24-25.

⁸⁰⁶ ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, s.34.

profillemenin kapsamı (ilgili kiři hakkında oluşturulan profilin kiři hakkında dar mı yoksa kapsamlı bir resim mi oluşturduđu), profillemenin ilgili kiři üzerindeki etki ve sonuçlarının ne olacađı, profillerin ilerde kullanılıp kullanılmayacacađı ve profillemeye faaliyetinde eşitliđin sađlanması, ayrımcılık ihtimalinin ortadan kaldırılması ve edinilen sonucun dođruluđunu teminen alınan önlemler önem teşkil etmektedir⁸⁰⁷. Verilerin ilgili kiřiden toplandıđı anda, verilerin bu amaçla işlenebilme ihtimalinin ilgili kiři tarafından makul bir şekilde öngörülebilir olup olmadığı, işlemenin veri sorumlusunun meşru menfaati için gerekli olup olmadığına ilişkin yapılacak deđerlendirmede önem teşkil etmektedir⁸⁰⁸. İlgili kiřinin makul bir şekilde kişisel verilerinin işlenmesini beklemeyeceđi hallerde, ilgili kiřinin temel hak ve özgürlüklerinin veri sorumlusunun menfaatine üstün gelecek ve dolayısıyla da veri sorumlusunun meşru menfaatinin varlıđından bahsedilemeyecektir⁸⁰⁹.

GVK Tüzüğü'nün ilgili başlangıç hükmünde doğrudan pazarlama faaliyetleri kapsamındaki kişisel veri işlemlerinde veri sorumlusunun meşru menfaati hukuka uygunluk sebebine dayanılabileceđi belirtilmiş olmakla birlikte, yukarıda açıklandıđı üzere, her bir doğrudan pazarlama faaliyeti özelinde meşru menfaat deđerlendirmesi yapılmak suretiyle meşru menfaat hukuka uygunluk sebebine dayanılmasının uygun olup olmadığı tespit edilmelidir. Pazarlama amaçlı gerçekleştirilen profillemeye faaliyetlerinde ise, öncelikle pazarlama amacının meşru olup olmadığı deđerlendirilmelidir. Pazarlama amacı meşru ise, ikinci olarak, bu amaç için profillemeye faaliyetinin meşru olup olmadığına bakılması gerekecektir⁸¹⁰. Öte yandan 29. Madde Veri Çalışma Grubu'nun, veri sorumlusunun meşru menfaatine ilişkin görüşünde, veri sorumlularının, pazarlama ve reklam amacıyla, kişilerin birden fazla internet sitesi, lokasyon, cihaz, hizmet veya veri brokeri

⁸⁰⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.14-15.

⁸⁰⁸ Data Protection Commission Ireland, Guidance Note: Legal Bases for Processing Personal Data, Aralık 2019, s.21-23, <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>.

⁸⁰⁹ Data Protection Commission Ireland, s.21-23.

⁸¹⁰ Council of Europe, The Protection of Individuals with regard to Automatic Processing of Personal Data in the Context of Profiling, s.46.

üzerinden izlenmesini gerektiren çevrimiçi davranışsal reklamcılık ve çevrimiçi doğrudan pazarlama kapsamında gerçekleştirilen profillemeye ve izleme faaliyetlerinde, meşru menfaat hukuka uygunluk sebebine dayanılamayacağı, bunun yerine ilgili kişinin rızasının alınmasının doğru hukuka uygunluk sebebi olacağı belirtilmiştir⁸¹¹.

29. Madde Çalışma Grubu'nun, meşru menfaat ile ilgili rehberinde yer verdiği örnek üzerinden konu somutlaştırılabilecektir. Çevrimiçi eczane hizmeti veren bir sitenin, pazarlama faaliyetleri kapsamında müşterilerinin sağlık ve zindelik durumlarına ilişkin profillerini oluşturmak için, müşterilerin yaş ve cinsiyet gibi bilgilerini, müşterilerin demografik bilgileriyle ve satın aldıkları ürünler ile internet sitesindeki gezinme geçmişini gösteren tıklama akışı verileri ile birleştirerek analiz etmektedir. Kullanıcılar hakkında oluşturulan profiller belirli bir kullanıcının hamile olduğunu, kronik hastalığa sahip olduğunu veya yılın belirli dönemlerinde cilt bakım ürünleri veya güneş kremi almakla ilgilenebileceğini gösteren bilgi ve tahminler içerir. Bu bilgi ve tahminler, belirli kişilere reçetesiz ilaçlar, vitamin takviyeleri ve diğer ürünlerin e-posta yoluyla pazarlanması amacıyla kullanılmaktadır. Çalışma Grubu, bu örnekte veri sorumlusunun, profillemeye faaliyetinin özel nitelikli kişisel verilerin işlenmesini gerektirmesi ve birçok kişinin gizli kalacağını bekleyeceği bilgilerin ortaya çıkmasına neden olması, profillemenin kapsamı ve şeklinin (tıklama akışı verilerinin (*click-stream data*) ve tahmine dayalı algoritmaların kullanımının) bireyin mahremiyetine müdahaleci bir nitelikte olması nedeniyle, gerek pazarlama için müşteri profillerini oluştururken gerek bu profilleri kullanırken meşru menfaate dayanamayacağını, ilgili kişiden rıza alınmasının bir alternatif olarak değerlendirilebileceğini belirtmiştir⁸¹².

Çalışma Grubunun ikinci örneğinde ise, kar amacı gütmeyen bir kuruluşun bağış toplama faaliyetlerini gerçekleştirmek üzere başvurduğu profillemeye

⁸¹¹ Article 29 Working Party, Legitimate Interest, s.18, s.47.

⁸¹² Article 29 Working Party, Legitimate Interest, s.59.

uygulamalarında meşru menfaat hukuka uygunluk sebebinin uygulanabilirliği incelenmiştir. Kuruluş, üyelerinden bağış toplama amacıyla, kuruluşun sayfasını beğenen, kuruluşun sosyal medya hesabında yayınlanan mesajları beğenen veya paylaşan, belirli içerikleri belirli aralıklarla görüntüleyen, kuruluşun twitter hesabından attığı tweetleri “retweet” eden kişileri hedefleyen yazılımlar aracılığıyla sosyal ağ siteleri üzerinden kişisel veri toplamaktadır. Üyelere bu verilerin analiz edilmesiyle çıkarılan profillerine göre mesaj ve haber bültenleri gönderilmektedir. Hayvan barınakları ile ilgili makaleleri beğenen ve köpek sahibi olan kişilerle, küçük çocuk sahibi kişiler ve farklı etnik kökene sahip kişiler birbirlerinden farklı mesajlar almaktadır. Çalışma Grubu bu örnekte verilerin kullanılma şeklinin bireylerin makul beklentilerini aşması, toplanan veri miktarı, verilerin toplama anında yeterli şeffaflığın olmaması, verilerin edinilme amacından farklı bir amaç için kullanılması nedeniyle veri sorumlusunun meşru menfaatine dayanılamayacağını, bu şekilde bir veri işleme faaliyetinin ancak ilgili kişinin rızası veya farklı bir hukuka uygunluk sebebine dayanılarak gerçekleştirilebileceğini belirtmiştir⁸¹³.

Tüzüğün giriş bölümünün 47-49. paragrafları arasında meşru menfaat hukuka uygunluk sebebinin uygulanabileceği örneklere yer verilmiştir. Ancak belirtilmelidir ki, bu hallerden birinin gerçekleşmesi dahi meşru menfaatin her koşulda uygulanabilir olduğu anlamına gelmemektedir⁸¹⁴. Her halükarda veri sorumlusunun her bir işleme faaliyeti özelinde meşru menfaat değerlendirmesi yapması gerekecektir⁸¹⁵. GVK Tüzüğü’nün 47. paragrafında, kamu otoritelerinin görevlerinin icrası kapsamında gerçekleştirdikleri veri işleme faaliyetlerinde, meşru menfaat iddiasına dayanamayacakları açıkça belirtilmiştir⁸¹⁶. Yine aynı paragraftaki açık düzenleme uyarınca, ilgili kişi ile veri sorumlusu arasında, müşteri ve hizmet veren veya çalışan ve işveren ilişkisi olduğu takdirde meşru menfaatin

⁸¹³ Article 29 Working Party, Legitimate Interest, s.60.

⁸¹⁴ Gonzalez & De Hert, s.604.

⁸¹⁵ Gonzalez & De Hert, s.604.

⁸¹⁶ Bkz. GVK Tüzüğü, Giriş Bölümü, 47.Paragraf.

varlığından söz edilebilecektir⁸¹⁷. Dolandırıcılığın önlenmesi kesin surette kişisel veri işlenmesini gerekli kılıyorsa, veri sorumlusunun meşru menfaatinin bulunduğu kabul edilir⁸¹⁸. Örneğin, sigorta dolandırıcılığının önlenmesi amacıyla sigorta şirketlerince gerçekleştirilen profillemeye faaliyetlerinde sigorta şirketinin meşru menfaatinin bulunduğu kabul edilebilecektir⁸¹⁹.

Avrupa Veri Koruma Kurulu'nun sosyal medya kullanıcılarının hedeflenmesine ilişkin rehberinde verdiği örneklerden birinde, bir banka müşterisi, hesap açılış işlemleri sırasında bankaya e-posta adresini verir⁸²⁰. Banka ilgili müşterisini, e-posta adresinin halihazırda kullanmakta olduğu banka hizmetleriyle bağlantılı tekliflerin reklamının yapılması amacıyla kullanılabileceği ve buna her zaman itiraz edebileceği konusunda bilgilendirir. Banka müşterisine ait e-posta adresini müşteri veritabanına ekler ve bu e-posta veritabanını sunduğu tüm finansal hizmetlere ilişkin teklifler ile müşterilerini sosyal medya platformunda hedeflemek için kullanır. Avrupa Veri Koruma Kurulu, bu örnekte veri sorumlusunun, (i) müşterinin e-posta adresinin kullanmakta olduğu hizmetlerle ilgili sosyal medya aracılığıyla reklam yapılması amacıyla kullanılabileceği hususuna bilgilendirilmiş olması, (ii) gösterilen reklamların halihazırda müşterinin yararlandığı hizmetlere benzer hizmetlerle ilgili olması ve (iii) işleme faaliyetinden önce işlemeye itiraz hakkı tanınmış olması göz önüne alınarak meşru menfaate dayanabileceğini belirtmiştir⁸²¹. Belirtmek gerekir ki, e-posta adreslerinin doğrudan pazarlama amacıyla kullanıldığı durumlarda, veri sorumluları GVK Tüzüğü'nün yanı sıra E-Gizlilik Direktifi'nin 13.maddesine uymakla yükümlüdür. Kurul, reklamın sosyal medya platformunda gösterilmeyeceği, ancak doğrudan ilgili kişiye anlık bildirim (*push notification*) veya direkt mesaj yoluyla gönderileceği durumlarda, E-Gizlilik Direktifi'nin 13. maddesinin geçerli olacağını belirtmiştir.

⁸¹⁷ Bkz. GVK Tüzüğü, Giriş Bölümü, 47.Paragraf.

⁸¹⁸ Bkz. GVK Tüzüğü, Giriş Bölümü, 47.Paragraf.

⁸¹⁹ Council of Europe, The Protection of Individuals With Regard to Automatic Processing of Personal Data in the Context of Profiling, s.45.

⁸²⁰ European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, Version 1.0, 2 Eylül 2020, s.17.

⁸²¹ European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, s.17.

Öte yandan, Direktif'in 13.maddesinin ikinci fıkrasında, bir işletmenin mevcut bir müşterinin elektronik iletişim bilgilerini "müşteriye kolay ve ücretsiz bir şekilde itiraz etme imkanı tanınması şartıyla kendi benzer ürün veya hizmetlerinin doğrudan pazarlanması" için kullanılabileceği belirtilmektedir⁸²². Dolayısıyla, Kurul bu örnekte, ilgili kişinin rızasının aranmayacağı değerlendirilmiştir⁸²³.

Avrupa Veri Koruma Kurulu'nu ilgili rehberindeki ikinci örneğinde, satın almayı planladığı bir evin finansmanı için uygun kredi imkanlarını görüşmek üzere bankadan e-posta ile randevu alan bir kişi görüşme sonunda ilgili bankadan kredi kullanmamaya karar verir. Banka ilgili kişinin e-posta adresini müşteri veri tabanına kaydeder ve ardından bir sosyal medya sağlayıcısının, bankanın e-posta adresleri listesini sosyal medya platformu tarafından tutulan adreslerle eşleştirmesine izin vererek sosyal medya platformunda finansal hizmetlerle ilgili olarak kullanıcıları hedefler. Kurul bu örnekte, ilgili kişinin banka ile kredi imkanlarını değerlendirmek amacıyla iletişime geçtiği ve akabinde de teklif edilen hizmetleri kullanmak istemediğini banka ile paylaştığından bahisle, kişisel verilerin veri sorumlusu ile paylaşılma şekli göz önüne alındığında, veri sorumlusunun meşru menfaate dayanamayacağını belirtmiştir. Ayrıca ilgili kişinin kişisel verilerinin hedefleme amacıyla kullanılacağına dair makul bir beklenti içinde olamayacağı ve GVK Tüzüğü m.6/4 kapsamında uyumluluk testinin yapılması ile söz konusu işleme faaliyetinin kişisel verilerin başlangıçta toplanma amacı ile uyumlu olmadığı sonucunun doğacağı ifade edilmiştir⁸²⁴.

⁸²² Bkz. E-Gizlilik Direktifi, m.13/2.

⁸²³ European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, s.17, Dipnot 59.

⁸²⁴ European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, s.18.

3.3. İLGİLİ KİŞİNİN HAKLARI

GVK Tüzüğü'nde ve KVK Kanunu'nda, ilgili kişiye, kişisel verilerinin işlenmesi sürecine çeşitli aşamalarda müdahale etme imkanı tanıyan bazı haklar tanınmıştır⁸²⁵. Bu haklar, kişisel verilerin korunması hukukunun temelini oluşturan bireyin kişisel verilerinin geleceğini belirleme hakkının kullanılması ve şeffaflık ilkesinin gerçekleşebilmesi açısından son derece önemlidir. Şeffaflık ilkesi uyarınca, veri sorumluları ilgili kişileri kişiler verilerinin işlendiği hususunda bilgilendirmekle yükümlüdür. Öte yandan şeffaflık ilkesinin amacı sadece bireyleri kişisel verileri üzerinde gerçekleşen işleme faaliyetlerinden haberdar etmek değil, aynı zamanda verilerinin nasıl işlendiğine ilişkin etkili bir şekilde kontrol imkanı tanımaktır⁸²⁶. Kişisel verilerinin işlendiğinden haberdar olup işleme faaliyetinin detayları ve bu faaliyete ilişkin sahip olduğu haklar ile ilgili bilgilendirilen ilgili kişi, işleme faaliyetinin tabi olduğu mevzuatta kendisine tanınan hakları kullanabilecektir. Profillemeye bağlamında bu haklar, ilgili kişinin profilini çıkaran ve ilgili kişi hakkında insan müdahalesi ile veya insan müdahalesi olmadan gerçekleşen otomatik işleme yoluyla bir karar veren veri sorumlusuna karşı kullanılabilir⁸²⁷.

Çalışmanın bu bölümünde, ilgili kişi nezdinde farkındalık yaratılmasını ve bu suretle ilgili kişinin kişisel verileri üzerinde denetim sahibi olmasını sağlamayı amaçlayan, ilgili kişinin bilgilendirilme hakkı, erişim hakkı, otomatik kararların açıklanmasını talep etme hakkı, veri taşınabilirliği hakkı incelendikten sonra bu hakların doğal bir sonucu olarak ortaya çıkan, ilgili kişinin kişisel verilerinin düzeltilmesini talep etme, silinmesini talep etme, işleme faaliyetini kısıtlama ve işleme faaliyetine itiraz etme hakları incelenecektir.

⁸²⁵ Küzeci, s.217.

⁸²⁶ Edwards & Veale, Slave to the Algorithm? Why a 'Right to an Explanation' is Probably not the Remedy You Are Looking for, s.41.

⁸²⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.16.

3.3.1. İlgili Kişinin Bilgilendirilme Hakkı

GVK Tüzüğü'nün 13 ve 14. maddelerinde “ilgili kişinin bilgilendirilme hakkı” (“*right to be informed*”) düzenlenmiştir. Bilgilendirilme hakkı, şeffaflık ilkesinin ilgili kişiye tanınan haklar bağlamında bir görünümüdür. Belirtmek gerekir ki, her ne kadar “hak” ifadesi kullanılmış ise de Tüzük'te ilgili kişiye tanınan diğer haklarından farklı olarak bilgilendirilme hakkı ilgili kişinin fiili bir davranışını gerektirmemektedir. Zira bu düzelemeler esasen veri sorumlusunun “bilgilendirme yükümlülüğü” ne ilişkindir. Tüzüğün 13. maddesinde kişisel verilerin doğrudan ilgili kişiden toplandığı hallerde, 14. maddesinde ise kişisel verilerin ilgili kişiden edinilmediği hallerde veri sorumlusunun ilgili kişiyi bilgilendirme yükümlülüğü düzenlenmiştir. Kişisel verilerin ilgili kişi tarafından veya üçüncü bir kişi tarafından sağlandığı hallerde yapılacak bilgilendirmenin kapsamının düzenlendiği bu iki maddenin de ilk fıkrasında ilgili kişiye hangi hususlarda bilgi vereceği, ikinci fıkrada ise bu bilgilere ilaveten kişisel verilerin elde edildiği anda adil ve şeffaf bir şekilde işlenmesinin sağlanması için ilgili kişiyle hangi bilgilerin paylaşılacağı düzenlenmiştir⁸²⁸. GVK Tüzüğü'nde ilgili kişinin hakları başlığı altında düzenlenen ilgili kişinin bilgilendirilmesi, KVK Kanunu'nun, “Veri Sorumlusunun Aydınlatma Yükümlülüğü” başlıklı 10. maddesinde veri sorumlusuna yüklenen “aydınlatma yükümlülüğü” olarak karşılık bulmuştur⁸²⁹.

GVK Tüzüğü'nün giriş bölümünün 60. paragrafında, veri sorumlusunun ilgili kişiyi profillemeye faaliyeti ile ilgili bilgilendirmesinin şeffaflık

⁸²⁸ Bkz. GVK Tüzüğü, m.13, m.14.

⁸²⁹ KVK Kanunu'nun 10.maddesi uyarınca veri sorumlusu, ilgili kişilere, veri sorumlusunun ve varsa temsilcisinin kimliği, verilerin hangi amaçla işleneceği, kimlere ve ne amaçla aktarılabileceği, verilerin toplanma yöntemi ve hukuki sebebi ve Kanun'un 11.maddesinde düzenlenen diğer hakları ile ilgili bilgi vermekle yükümlüdür.Kurum'un Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi'nde, aydınlatma yükümlülüğünün yazılı olarak yerine getirilmesi, aydınlatma metninin muğlak ifadeler içermeyecek şekilde açık ve sade bir dilde olması, bilgilendirme amacı taşıması, çok fazla hukuki ve teknik kelimeler içermemesi, ilgili kişi için kolayca erişilebilir formda olması gerektiği belirtilmektedir. Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s.15.

yükümlülüğünün bir uzantısı olduğu ifade edilmektedir⁸³⁰. Profillemeye ve otomatik karar alma faaliyetleri gerçekleştiren veri sorumluları, profillemeye ve otomatik karar alma sürecinin nasıl işlediği hususunda ilgili kişileri olabildiğince açık ve anlaşılır bir şekilde bilgilendirmekle yükümlüdür⁸³¹. Diğer yandan, veri işleminin profillemeye dayanan bir karar alma ile sonuçlandığı hallerde, karar sürecinde insan müdahalesi bulunup bulunmadığından bağımsız olarak, ilgili kişinin, kişisel verilerinin “profilinin çıkarılması ve bu profile dayanılarak kendisi hakkında bir karar alınması” amacıyla işlendiği hususunda bilgilendirilmesi gerekecektir⁸³². Böylelikle, profillemeye ve otomatik karar alma faaliyetinin varlığı hakkında bilgilendirilen ilgili kişi, profillemeye hakkında bilgilendirildikten sonra, profillemeye dayalı bir karar verilmiş olsa da olmasa da profillemeye itirazda bulunma hakkına sahip olacaktır⁸³³.

Şeffaflık ilkesinin icra edilmesine hizmet eden ilgili kişinin bilgilendirilme hakkı, bireylerin kişisel verilerinin işlenmesi suretiyle kendileri hakkında ne gibi çıkarımlarda bulunulduğunu veya doğrudan kendileri tarafından sağlanmayan hangi verilerin işlendiğini öğrenmelerine imkan sağlar. Bu hususlarda bilgi sahibi olan ilgili kişi, kişisel verilerin korunmasına ilişkin diğer haklarını da kullanabilecektir. Ancak Tüzüğün bu maddeleri muğlak ifadeler içerdiği ve dolayısıyla da uygulamaya yönelik belirsizlikleri beraberinde getirdiği sebebiyle eleştirilere konu edilmiştir. Öte yandan, profillemeye ve otomatik karar alma uygulamalarında kullanılan karmaşık analitik yöntemleri sebebiyle, veri sorumlusu “yürütülen mantığa ilişkin anlamlı bilgi” ve “öngörülen sonuçları” hakkında bilgilendirme yükümlülüğünü yerine getirmekte zorluklarla karşılaşabilecektir.

Tüzüğün 13. maddesinde, doğrudan ilgili kişiden edinilen veriler açısından veri sorumlusunun bilgilendirme yükümlülüğünün gereklilikleri hüküm altına alınmıştır. Bu madde uyarınca veri sorumlusu kişisel verilerin toplanma anında,

⁸³⁰ Bkz. GVK Tüzüğü, Başlangıç, 60. Paragraf.

⁸³¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.16.

⁸³² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.16.

⁸³³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.17.

ilgili kişiyi verilerinin işlenme amacı, verilerinin paylaşılacağı muhtemel üçüncü taraf alıcılar gibi hususlar hakkında bilgilendirmelidir. 13. maddenin lafzından da anlaşılacağı üzere, bu madde sadece gözlemlenen veriler de dahil olmak üzere ilgili kişiden edinilen veriler açısından uygulama alanına sahiptir⁸³⁴. Bu bağlamda, profillemeye faaliyeti kapsamında ilgili kişi hakkında bir çıkarımda bulunulmadan önce, veri sorumlusunun ilgili kişiyi profillemeye faaliyetinin varlığı hakkında bilgilendirmesi 13. maddeye tabi olacaktır⁸³⁵. Zira profillemeye faaliyeti sonucunda ilgili kişi hakkında yapılan çıkarımların bir kısmı ilgili kişi tarafından sağlanan verilere dayanmaktadır⁸³⁶. Ancak belirtilmelidir ki, profillemeye ve otomatik karar alma faaliyetleri kapsamında kişisel verilerin işlenmesi sonucu ilgili kişi hakkında oluşturulan çıkarılan veya türetilen veriler, veri sorumlusunun ilgili kişiyi bilgilendirme anında henüz çıkarılmamış veya türetilmemiş olduğundan, 13. maddenin uygulama alanına girmeyecektir⁸³⁷. Öte yandan, Tüzüğün 14. maddesi uyarınca, veri sorumlusu kişisel verilerin üçüncü bir kişiden edinildiği hallerde, ilgili kişiyi, kişisel verilerin işlenme amacı, bu verilerin hangi kategoriye dahil olduğu, ilgili kişinin sahip olduğu haklar, verilerin edinildiği kaynaklar, kişisel verilerin paylaşıldığı üçüncü kişi alıcılar, veri sorumlusunun veya üçüncü kişilerin işleme faaliyetini dayandırdıkları meşru menfaatler, kişisel verilerin hangi kaynaklardan edinildiği ve uygun olan hallerde kişisel verilerin kamunun erişimine açık kaynaklardan edinilip edinilmediği hakkında bilgilendirmekle yükümlüdür⁸³⁸. Bu bağlamda, çıkarılan verileri (kredi puanı gibi) üçüncü bir kişiden edinen veri sorumlusu, veriyi elde ettiği anda 14. madde tahtında belirtilen tüm bilgileri ilgili kişiye sağlamakla yükümlüdür⁸³⁹.

Wachter ve Mittelstadt, GVK Tüzüğü'nün bu iki maddesinin önemli boşluklar içerdiği görüşündedir⁸⁴⁰. Buna göre, 14. maddenin geçerli olduğu

⁸³⁴ Wachter & Mittelstadt, s.52.

⁸³⁵ Wachter & Mittelstadt, s.52.

⁸³⁶ Wachter & Mittelstadt, s.52.

⁸³⁷ Wachter & Mittelstadt, s.52.

⁸³⁸ Bkz. GVK Tüzüğü, m.14/2(g).

⁸³⁹ Wachter & Mittelstadt, s.53.

⁸⁴⁰ Wachter & Mittelstadt, s.51-53.

durumlarda, veri sorumlusu ilgili kişileri ilgili veri kategorileri hakkında bilgilendirmekle yükümlü olmakla birlikte, GVK Tüzüğü'nde "kişisel veri kategorileri" tanımlanmamıştır. Dolayısıyla, veri sorumlularının edindikleri kişisel verilerin ayrıntılarını açıklamalarına gerek olmadığı şeklinde bir yanılgıya düşmeleri, bunun sonucunda ise ilgili kişilerin hangi verilerinin işlendiğinin farkında olmamaları riski söz konusu olabilecektir⁸⁴¹. Öte yandan, Tüzük m.14/5(a) uyarınca, birden çok veri sorumlusunun rol aldığı bir işleme faaliyetinde, eğer verileri aktaran veri sorumlusu, ilgili kişiye yapmakla yükümlü olduğu bildirimde, verileri paylaşılabileceği potansiyel üçüncü kişi alıcılara yer veriyse, alıcı veri sorumlusu söz konusu veri transferine ilişkin olarak ilgili kişiye ilave bir bilgilendirme yapmakla yükümlü olmayacaktır⁸⁴². Yine Tüzük m.14/2(b) uyarınca, kamu yararına arşivleme, bilimsel ve tarihsel araştırma veya istatistiksel amaçlar için gerçekleştirilecek veri işleme faaliyetlerinde, söz konusu bilgilerin sağlanmasının imkansız olması veya "orantısız bir çaba" gerektirmesi halinde, veri sorumlusu ilgili kişiye bilgilendirme yapmakla yükümlü olmayacaktır⁸⁴³. Özellikle "orantısız çaba" kavramının, Tüzük'te bu kavrama ilişkin olarak "bilgilendirilmesi gereken ilgili kişilerin sayısı" ile ilgili olabileceğinin ötesinde bir açıklama getirilmediği gerekçesiyle, sorunlu olduğu belirtilmektedir⁸⁴⁴. Wachter ve Mittelstadt'a göre bu boşluklar, veri sorumlusunun her koşulda ilgili kişiyi kendisi hakkında üçüncü kişilerden edinilen, çıkarılan veya türetilen verilerin türü ve zamanı hakkında bilgilendirmekle yükümlü olmayacağını gösterir⁸⁴⁵. Maddenin yarattığı önemli boşuklardan biri de çıkarılan veya türetilen verilerin üçüncü bir kişiden edinilmediği, bunun yerine veri sorumlusunun kendisi tarafından ilgili işleme faaliyeti sonunda oluşturulduğu hallerde, veri sorumlusunun bilgilendirme yükümlülüğünün tetiklenmeyecek olmasıdır⁸⁴⁶. Zira bu halde ilgili işleme faaliyeti, verinin ne ilgili kişinin kendisinden ne de üçüncü kişiden edinilmemiş olması

⁸⁴¹ Wachter & Mittelstadt, s.53.

⁸⁴² Bkz GVK Tüzüğü, m. 14/5(a). Wachter & Mittelstadt, s.53.

⁸⁴³ Bkz. GVK Tüzüğü, m.14/5(b). Wachter & Mittelstadt, s.53.

⁸⁴⁴ Wachter & Mittelstadt, s.53.

⁸⁴⁵ Wachter & Mittelstadt, s.53-54.

⁸⁴⁶ Wachter & Mittelstadt, s.54.

sebebiyle, Tüzüğün 13. ve 14.maddelerinin uygulama alanı dışında kalacaktır⁸⁴⁷. Bu durum, veri sorumlusunun çıkarımları kendisi oluşturarak bilgilendirme yükümlüğünü yerine getirmekten kaçınabilmesine yol açabilecektir⁸⁴⁸.

Tüzüğün 13/2(f) ve 14/2(g) maddeleri ile, veri sorumlusu, hukuki veya benzer şekilde önemli etkiler yaratan, profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetleri kapsamında, ilgili kişiyi, “profillemeye de dahil olmak üzere, 22/1 ve 22/4 maddelerinde atıfta bulunulan otomatik karar almanın varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilginin yanı sıra işleme faaliyetinin ilgili kişi açısından önemi ve öngörülen sonuçları”⁸⁴⁹ hakkında belirli ve kolay erişilebilir bir şekilde bilgilendirmekle yükümlü kılınmıştır. Bu bağlamda, veri sorumlusu, GVK Tüzüğü m.22/1 kapsamına giren bir otomatik karar alma faaliyeti gerçekleştiriyor ise, (i) ilgili kişiyi bu faaliyetten haberdar etmek, (ii) otomatik karar alma sürecinin işleyiş mantığı hakkında anlamlı bilgiler vermek ve (iii) işleme faaliyetinin önemini ve öngörülen sonuçlarını açıklamakla yükümlü olacaktır. Ancak belirtilen düzenlemelerde sadece 22. maddenin 1. ve 4. fıkralarına atıf yapılmış, veri sorumlusunun almakla yükümlü olduğu tedbirlerin (ilgili kişiye insan müdahalesi talep etme hakkı, kendi görüşünü beyan etme hakkı ve karara itiraz etme hakkı tanınması) düzenlendiği 3. fıkraya ise yer verilmemiştir. Dolayısıyla, veri sorumlu ilgili kişiyi, m.22 tahtında düzenlenen profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı bir kararın konusu olmama hakkına ve m.22/3 tahtında düzenlenen insan müdahalesi talep etme, kendi görüşünü beyan etme ve karara itiraz etme haklarının bulunduğu ilişkin bilgilendirmekle yükümlü değildir⁸⁵⁰. Wachter ve diğerleri, bu bağlamda, Tüzüğün ilgili kişinin bilgilendirilmesine ilişkin belirtilen maddelerinin, m.22/4’te veri sorumlusunun almakla yükümlü olduğu

⁸⁴⁷ Wachter & Mittelstadt, s.54

⁸⁴⁸ Wachter & Mittelstadt, s.54; Gonzalez & De Hert, s.612.

⁸⁴⁹ Bkz. GVK Tüzüğü, m.13/2(f), 14/2(g).

⁸⁵⁰ Wachter & Mittelstadt & Russell, s.875.

tedbirler kapsamında ilgili kişiye sağlayacağı haklardan biri olan “karara itiraz hakkı”nın kullanılmasına yeterince yardımcı olmadığı görüşündedir⁸⁵¹.

Belirtmek gerekir ki veri sorumlusunun ilgili kişinin haklarına ilişkin bilgilendirme yükümlülüğünün, şeffaflık ilkesinin bir görünümü olarak amacı, ilgili kişinin Tüzük tahtındaki hakları ile ilgili bilgi sahibi olmasını sağlamak ve bu hakların kullanılmasını kolaylaştırmaktır⁸⁵². Bu bağlamda, veri sorumlusunun ilgili kişinin haklarını kullanmasına yardım etmek için farklı bir bilgi veya hukuki danışmanlık vermekle yükümlü olmadığını belirtmek gerekir⁸⁵³. İlgili kişinin hangi haklara sahip olduğuna ilişkin bilgilendirilmesi ve haklarını kullanmasını zorlaştıracak engellerin ortadan kaldırılması, sorulara makul bir sürede cevap verileceğinin garanti edilmesi ve kararı değiştirme yetkisine sahip birisi ile temasa geçebilmesine imkan tanınması da dahil olmak üzere, haklarını kullanabilmesi için gerekli zeminin sağlanmasının yeterli olduğu kabul edilmektedir⁸⁵⁴.

22. maddenin uygulama alanının dışındaki profillemeye ve otomatik karar alma faaliyetleri açısından da veri sorumlusunun, işlemenin dayandığı hukuka uygunluk sebebinden bağımsız olarak ilgili kişiyi bilgilendirmekle yükümlü olduğunu belirtmek gerekir. Ancak veri sorumlusunun 22. madde kapsamındaki profillemeye ve otomatik karar alma faaliyetlerinden farklı olarak, ilgili kişiyi otomatik kararın varlığı, karar sürecinin işleyiş mantığı ve öngörülen sonuçları hakkında bilgilendirmekle yükümlü olmayacaktır. Öte yandan, ilgili kişi de 22. madde tahtındaki insan müdahalesi talep etme, kendi görüşlerini ifade etme ve karara itiraz etme haklarından faydalanamayacaktır.

Tüzük’te, “yürütülen mantığa ilişkin anlamlı bilgi”nin kapsamının ne olacağına ilişkin açık bir düzenlemeye yer verilmemiştir. Selbst ve Powles, GVK Tüzüğü’nün 13, 14 ve 15. maddelerinin⁸⁵⁵ ilgili kişinin hakları ile ilgili olduğundan

⁸⁵¹ Wachter & Mittelstadt & Russell, s.875-876.

⁸⁵² Wachter & Mittelstadt & Russell, s.876.

⁸⁵³ Wachter & Mittelstadt & Russell, s.876.

⁸⁵⁴ Wachter & Mittelstadt & Russell, s.876.

⁸⁵⁵ Bkz. GVK Tüzüğü, m.13/2(f), 14/2(g), 15/1(h).

bahisle, veri sorumlularının bu maddeler tahtında ilgili kişilere sağlayacağı bilgilerin de ilgili kişilerin GVK Tüzüğü düzenlemeleri ile garanti edilen haklarını kullanmalarına yardımcı olacak kapsamda olması gerektiğini ifade etmiştir⁸⁵⁶. Buna göre, ilgili kişiye kendisi hakkında bir otomatik karara ilişkin açıklama yapılması halinde, ilgili kişinin bir ayrımcılık iddiasında bulunabilip bulunamayacağını belirleyebilmek için kararı yeterince iyi anlaması gerekmektedir⁸⁵⁷. Bu bağlamda, ilgili kişiye bu kapsamda sağlanacak bilgiler, ilgili kişinin kendisi hakkında verilen kararın nedenlerini anlayabilmesini sağlayacak kapsamda ve nitelikte olmalıdır⁸⁵⁸. İlgili kişiye bu kapsam ve nitelikte bir bilgi sağlanması, veri sorumlusunca GVK Tüzüğü'nün 22/3. maddesi ve 71. paragrafında atıfta bulunulan uygun tedbirlerin alınmasını da destekleyecektir⁸⁵⁹.

Tüzük m.12/7'de açıkça, ilgili kişinin bilgilendirilme hakkını düzenleyen 13. ve 14.maddelerin amacının “kolayca görülebilir, anlaşılabilir ve okunaklı bir şekilde, planlanan işleme faaliyetine yönelik anlamlı bir genel bakış” sağlamak olduğu belirtilmektedir⁸⁶⁰. Wachter ve diğerleri, neyin “anlamlı bir genel bakış” teşkil edeceği konusunda açıklamanın sağlanacağı aracın belirleyici olduğunu ileri sürmüştür⁸⁶¹. Bilgilendirme yükümlülüğünün, halihazırdaki gizlilik bildirimlerine yapılacak bir güncelleme ile veya kişisel verilerin ilgili kişiden değil üçüncü bir kişiden toplandığı hallerde ilgili kişiye gizlilik bildirimini ile bağlantı kuran bir e-posta gönderilmesi ile gerçekleştirilebileceği yönünde görüşler bulunmaktadır⁸⁶². Nitekim m.13 ve m.14'ün kapsam ve amacına ışık tutan m.12/7'de, bilgilendirmenin standart simgelerle sağlanabileceği belirtilmek suretiyle detaylı bir açıklamaya gerek bulunmadığına işaret edilmiştir⁸⁶³. Wachter ve diğerlerine göre, açıklanan nedenlerle, Tüzük m.13 ve m.14, belirli bir karar hakkında bilgi

⁸⁵⁶ Andrew D. SELBST & Julia POWLES, Meaningful Information and the Right to Explanation, International Data Privacy Law, Vol.7(4), 233-242, 2017, s.7-8, <https://ssrn.com/abstract=3039125>.

⁸⁵⁷ Selbst & Powles, s.8.

⁸⁵⁸ Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.25.

⁸⁵⁹ Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.25.

⁸⁶⁰ Bkz. GVK Tüzüğü, n.12/7.

⁸⁶¹ Wachter & Mittelstadt & Russell, s.865.

⁸⁶² Wachter & Mittelstadt & Russell, s.865.

⁸⁶³ Wachter & Mittelstadt & Russell, s.865.

değil, işleme faaliyetine ilişkin tüm ilgili kişiler için (örneğin tüm Facebook kullanıcıları için) anlam ifade eden bir şekilde genel bir bakış sağlamayı amaçlar⁸⁶⁴. Bu bağlamda, ilgili kişinin kredi puanının düşük olmasının ödeme seçeneklerine etkisinin ne olacağı, planlanan veri işleme faaliyetinin nasıl ilgili kişinin kredi veya iş başvurusunun reddedilmesine neden olabileceği, trafikteki davranışlarının ve araba kullanma alışkanlıklarının sigorta primlerini nasıl etkileyeceği hakkında bilgilendirilmesi bilgilendirilme hakkının Tüzük ile öngörülen kapsamı açısından uygun ve yeterlidir⁸⁶⁵.

Wachter ve diğerlerine göre, GVK Tüzüğü'nde ilgili kişinin otomatik kararları anlayabilmesini destekleyecek birçok düzenleme bulunmakla birlikte, veri sorumlusunun ilgili kişiye sağlamakla yükümlü olduğu bilgiler daha çok ilgili kişinin otomatik karar sistemleri hakkındaki genel anlayışını artırmaya yöneliktir⁸⁶⁶. Bu bağlamda, GVK Tüzüğü düzenlemeleri otomatik karar sistemlerinin iç işleyiş mantığının açıklanması için algoritmaların kara kutu olarak nitelendirilen mekanizmasının açığa çıkarılmasını ("kara kutunun açılmasını") gerektirmez⁸⁶⁷. Otomatik kararların açıklanmasına ilişkin açık bir ifadeye yer verilen tek düzenleme olan 71.paragraf da "kara kutunun açılmasını" gerektirecek bir hüküm içermemektedir⁸⁶⁸.

Birleşik Krallık Bilgi Komisyoneri Ofisi de "otomatik karar faaliyetinin işleyiş mantığına ilişkin anlamlı bilgi" nin, yapay öğrenme algoritmasının nasıl çalıştığı hakkında detaylı bir teknik açıklamadan ziyade, (i) profili oluşturmakta kullanılan veri kategorileri, (ii) verinin kaynağı ve (iii) verinin neden ilgili

⁸⁶⁴ Wachter & Mittelstadt & Russell, s.865.

⁸⁶⁵ Wachter & Mittelstadt & Russell, s. 866.

⁸⁶⁶ Wachter & Mittelstadt & Russell, s.864.

⁸⁶⁷ Wachter & Mittelstadt & Russell, s.863.

⁸⁶⁸ Article 29 Working Party, Automated Decision Making and Profiling, s.27.

görüldüğü hakkında açıklayıcı bir bilgi sağlanması gerekliliğine işaret ettiğini ifade etmiştir⁸⁶⁹.

Bu konuda daha detaylı açıklamalara çalışmanın “İlgili Kişinin Otomatik Kararların Açıklanmasını Talep Hakkı” başlığı altında yer verilmiştir.

3.3.2. İlgili Kişinin Erişim Hakkı

GVK Tüzüğü’nün erişim hakkını düzenleyen 15. maddesi ile KVK Kanunu’nun 11. maddesinde ilgili kişinin, veri sorumlusuna başvurarak “kendisi ile ilgili kişisel verileri işleyip işlemediğini öğrenme ve eğer işlenmişse buna ilişkin bilgi talep etme hakkı” tanınmıştır. Böylece hangi verilerinin kullanıldığını inceleme imkanına sahip olan ilgili kişi, kişisel verilerinin silinmesini veya düzeltilmesini de talep etme imkanına sahip olacaktır. İlgili kişinin bilgilendirilme hakkına ilişkin 13. ve 14. maddelerden farklı olarak, erişim hakkını düzenleyen 15. maddesinde kişisel verilerin ilgili kişiden veya üçüncü bir kişiden edinilmiş olması bakımından bir ayrıma gidilmemiştir. Dolayısıyla, kişisel verilerin ilgili kişiden veya üçüncü bir kişiden edinilmiş olması fark etmeksizin, ilgili kişi, veri sorumlusunun profillemeye ve otomatik karar alma faaliyeti kapsamında kendisi hakkında çıkarımlarda bulunduğunu ya da bulunacağını veya üçüncü bir kişiden edineceği çıkarımlar üzerinde yeni bir işleme faaliyeti gerçekleştirmek suretiyle kendisi hakkında bir karar vereceğini düşündüğü hallerde veri sorumlusuna başvurarak ilgili bilgilere erişim talep etme hakkına sahip olacaktır⁸⁷⁰. Bu bağlamda erişim hakkı, ilgili kişi hakkında çıkarılan veriler ile bu verilerden oluşturulan profiller açısından uygulama alanına sahiptir⁸⁷¹.

⁸⁶⁹ Information Commissioner’s Office, Feedback Request – Profiling and Automated Decision Making, 2017, s.15, <https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>.

⁸⁷⁰ Wachter&Mittelstadt, s.54.

⁸⁷¹ Article 29 Working Party, Data Portability, s.10; Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.17.

GVK Tüzüğü'nün 15.maddesi uyarınca ilgili kişi, işlemeye konu edilen verilerine ve aşağıdaki bilgilere erişme hakkına (“*right of access*”) sahiptir:

- İşleme amaçları;
- İşlenen kişisel veri kategorileri;
- Özellikle diğer ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin açıklandığı ya da açıklanacağı alıcılar veya alıcı kategorileri;
- Mümkün olan hallerde, kişisel verilerin saklanması için öngörülen süre; mümkün olmadığı hallerde ise bu sürenin belirlenmesinde esas alınan kriterlerin neler olduğu;
- Kişisel verilerinin düzeltilmesini veya silinmesini, söz konusu kişisel verilerinin işlenmesinin kısıtlanmasını talep etme veya işleme faaliyetine itiraz etme hakkının varlığı;
- Denetleyici kuruluşa şikayette bulunma hakkı;
- Kişisel verilerin doğrudan ilgili kişiden edinilmediği durumlarda, verinin kaynağına ilişkin mevcut bilgiler;
- GVK Tüzüğü'nün 22/1 ve 22/4 maddelerinde atıf yapılan şekilde profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar almanın söz konusu olması halinde, karar sürecinin arkasındaki mantığa ilişkin anlamlı bilgi ile birlikte işemenin ilgili kişi açısından önemi ve öngörülen sonuçları⁸⁷².

Belirtmek gerekir ki ilgili kişinin erişim hakkını kullanabilmesi veri sorumlusuna başvurmasını, bu da veri sorumlusunun kimliğini bilmesini gerektirmektedir⁸⁷³. Bu durum, hakkın kullanımının önünde bir zorluk teşkil etmekle birlikte, ilgili kişi bu hakkını kullansa dahi, m.15/1 kapsamında sadece işlenen veri kategorileri hakkında bilgiye erişmekle kalabilecektir⁸⁷⁴. Ancak, ilgili kişi m.15/3 uyarınca, “işleme sürecinden geçen tüm verilerinin kopyasını” talep

⁸⁷² Bkz. GVK Tüzüğü, m.15/1.

⁸⁷³ Wachter&Mittelstadt, s.54.

⁸⁷⁴ Wachter&Mittelstadt, s.54.

etmek suretiyle, daha fazla detay hakkında bilgi sahibi olabilecektir⁸⁷⁵. GVK Tüzüğü'nün 15/3 maddesi uyarınca, veri sorumlusu, işleme faaliyeti ile ilgili genel bilgilerin yanı sıra, profillemeye faaliyeti kapsamında girdi olarak kullanılan verilerle birlikte profile ilişkin bilgileri ve ilgili kişinin kategorize edildiği segmente ilişkin detayları da ilgili kişiye sağlamakla yükümlüdür⁸⁷⁶. Bu bağlamda erişim hakkı, veri sorumlusunun çıkarılan profilin kendisi yerine sadece ilgili kişi tarafından sağlanan veya veri sorumlusunca gözlemlenen verileri iletmekle yükümlü olduğu veri taşınabilirliği hakkından ayrılmaktadır⁸⁷⁷. Gözetim uygulamalarından kaynaklanan tehditlere karşı temel hak ve özgürlüklerin korunması amacıyla bir grup avukat tarafından kurulan Panoptikon Vakfı (*Panoptikon Foundation*) temsilcisinin Polonya Veri Koruma Kurumu'na gerçekleştirdiği şikayet sonucunda, Kurum 2021 yılında verdiği kararda, çevrimiçi platform sahibinin, şikayetçi platform kullanıcılarını, çerezler aracılığı ile toplanan verilerinin analiz edilmesi suretiyle oluşturulan profili ve hangi verilerinin çerezler ile toplanan verilerle birleştirildiği hakkında bilgilendirmesi gerektiğine hükmetmiştir⁸⁷⁸.

Profillemeye ve otomatik karar alma sistemlerinde, yapay öğrenme algoritmalarının çalışma prensibi ve veri işleme sürecine ilişkin açıklamalar, özellikle teknoloji ve yazılım şirketleri açısından, sektördeki diğer şirketlere karşı rekabet aracı teşkil ettiği gerekçesiyle ticari sır (*trade secret*) olarak kabul edilebilmektedir. GVK Tüzüğü'nde ticari sırlara ilişkin münferit bir düzenlemeye yer verilmemiştir. Öte yandan GVK Tüzüğü'nün başlangıç bölümünün 4. paragrafında “iş yapma özgürlüğü” (“*freedom to conduct a business*”) ifadesine yer verilmiştir⁸⁷⁹. Tüzüğün giriş bölümünün 63. paragrafında ise, otomatik karar mekanizmaları ile ilgili olarak “ilgili kişinin mekanizmanın çalışma mantığına

⁸⁷⁵ Wachter&Mittelstadt, s.54-55.

⁸⁷⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.17.

⁸⁷⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.17.

⁸⁷⁸ Ewa KACPEREK & Weronika Olszewska, Polish DPA says data subjects have the right to be informed about their behavioral profile, 10 Aralık 2021, <https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9VapCDEpUUyfpDsXgHJMKLFEppVpbbVX%2B3OXcP3PYxlq7sZUjdbSm5FIetvAtgfleVU8%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFct8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true>.

⁸⁷⁹ Bkz. GVK Tüzüğü, Giriş Bölümü, 4.Paragraf.

ilişkin bilgi alma hakkı” sınırlandırılmıştır. İlgili paragrafta, bu hakkın, ticari sırlar veya fikri mülkiyet dahil olmak üzere, başkalarının haklarını veya özgürlüklerini ve özellikle yazılımı koruyan telif haklarını olumsuz yönde etkilememesi gerektiği belirtilmektedir⁸⁸⁰.

Alman doktrini ve içtihatında, 95/46 Sayılı Direktif’in yürürlükte olduğu süre zarfında, Direktif’in 12.maddesi tahtında düzenlenen ilgili kişinin erişim hakkını kullanarak talep edebileceği bilgilerin sistem işlevselliğine ilişkin bilgi ile sınırlı olduğu kabul edilmiştir⁸⁸¹. Yazılımın “ticari sır” teşkil etmesi sebebiyle, veri sorumlusunun kullanılan yazılımı açıklamakla yükümlü olmadığını, otomatik karara etki eden özelliklerin açıklanmasının yeterli olduğundan bahisle ticari sır oluşturan algoritmaların açıklanmasına gerek bulunmadığını savunan görüşler mevcuttur⁸⁸². Bu görüşe göre, veri sorumlusu sadece “karar ağacının” mantığını açıklamakla yükümlü olup, yazılımın nasıl çalıştığına ilişkin veya yazılımın kodu ile ilgili detayları paylaşmakla yükümlü değildir⁸⁸³. Erişim hakkının ticari sırları ihlal etmemesi gerektiği Alman içtihatında 2014 yılında verilen SCHUFA kararlarında da belirtilmiştir. SCHUFA, Almanya’da kişiler ve şirketler için kredi puanı oluşturan özel bir kredi bürosudur. İchtihattaki SCHUFA kararlarının, temeldeki hesaplama formülü ticari sır olduğundan, ilgili kişinin kredi puanlama sistemleri de dahil olmak üzere otomatik veri işleme sistemlerinin doğruluğunu tam olarak sorgulama hakkına sahip olmadığını gösterdiği yönünde görüşler mevcuttur⁸⁸⁴. SCHUFA kararlarında mahkeme otomatik işlemenin sadece delillerin hazırlanmasına kullanıldığı ve esas kararın bir insan tarafından verildiği gerekçesiyle SCHUFA tarafından gerçekleştirilen kredi puanlama faaliyetinin otomatik karar alma faaliyeti içermediğine karar vermiştir⁸⁸⁵. Wachter ve diğerleri, kararların otomatik karar almaya ilişkin olmasa dahi, ilgili kişinin erişim hakkı

⁸⁸⁰ Bkz. GVK Tüzüğü, Giriş Bölümü, 63.Paragraf.

⁸⁸¹ Wachter&Mittelstadt&Floridi, s.24.

⁸⁸² Wachter&Mittelstadt&Floridi, s.24.

⁸⁸³ Wachter&Mittelstadt&Floridi, s.24.

⁸⁸⁴ Wachter&Mittelstadt&Floridi, s.24.

⁸⁸⁵ Wachter&Mittelstadt&Floridi, s.24.

karşısında ticari sırları korumaya yönelik güçlü bir eğilimi temsil ettikleri gerekçesiyle aydınlatıcı olduğunu belirtmiştir⁸⁸⁶.

95/46 Sayılı Direktif döneminde yürürlükte olan Fransız Veri Koruma Kanunu'nda, ilgili kişilerin, telif hakkı düzenlemelerine aykırı olmadığı sürece karar sürecinin mantığına ilişkin bilgi talep edebileceği düzenlenmiştir⁸⁸⁷. İlgili kişilerin kararlara itiraz etme haklarını kullanmalarına izin vermek için, belirli özelliklerin ağırlığına (diğer bir ifadeyle otomatik karar yazılımının koduna veya algoritmasına) ilişkin değil, genel mantık ve karara etki eden veriler hakkında bilgi verilmelidir⁸⁸⁸. Benzer şekilde, Birleşik Krallık'ın 1998 tarihli Veri Koruma Yasası'nda⁸⁸⁹ da ticari sırların korunmasını sağlamak için erişim hakkının kapsamı sınırlandırılmıştır. İlgili Yasa ile, ticari sır teşkil eden bilgilerin karar sürecinin mantığına ilişkin yapılacak açıklamanın kapsamında olmadığı hüküm altına alınmıştır. Veri sorumlusu, ilgili kişileri kararın temelini oluşturan değerlendirmede dikkate aldıkları faktörler hakkında bilgilendirmekle yükümlü olmakla birlikte, bu faktörlerin her birinin karara etkisinin ağırlığına ilişkin açıklama yapmak zorunda değildir⁸⁹⁰.

GVK Tüzüğü'nün giriş bölümünün 63. paragrafında, erişim hakkının ticari sırlar veya fikri mülkiyet dahil olmak üzere üçüncü kişilerin haklarını veya özgürlüklerini ve özellikle de telif hakkını olumsuz etkilememesi gerektiği, ancak veri sorumlusunun bunları gözeterek ilgili kişiye bilgi sağlanmasını tamamen de reddedemeyeceği vurgulanmıştır⁸⁹¹. Ayrıca veri sorumlusu, mümkün olan hallerde,

⁸⁸⁶ Wachter&Mittelstadt&Floridi, s.25.

⁸⁸⁷ Douwe KORFF, New Challenges to Data Protection Study-Working Paper No.2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, European Commission DG Justice, Freedom and Security, 2010, s.86.

⁸⁸⁸ Douwe KORFF, New Challenges to Data Protection Study-Country Report: France, European Commission DG Justice, Freedom and Security, 2010, s.27.

⁸⁸⁹ UK Data Protection Act 1998 için bkz. <https://www.legislation.gov.uk/ukpga/1998/29/contents>. Yasa, 2018'de yürürlüğe giren yeni veri koruma yasası (UK Data Protection Act 2018) ile ilga edilmiştir.

⁸⁹⁰ Douwe KORFF, New Challenges to Data Protection Study-Country Report: United Kingdom, European Commission DG Justice, Freedom and Security, 2010, s.48, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638938.

⁸⁹¹ Bkz. GVK Tüzüğü, Giriş Bölümü, 63.Paragraf.

ilgili kişiye kişisel verilerine doğrudan erişebilme imkanı tanıyacak güvenli bir sisteme uzaktan erişim sağlayabilmelidir⁸⁹². Bu bağlamda, gerek GVK Tüzüğü gerekse üye devlet mevzuatı ve içtihatı ile, profillemeye ve otomatik karar faaliyetleri gerçekleştiren ve ilgili kişinin erişim hakkını kullanmasıyla ticari sırlarının veya fikri mülkiyet teşkil eden bilgilerinin ifşa edilmesinden endişe duyan veri sorumlusu için belirli bir ölçüde koruma sağlanmışsa da, veri sorumlusu ticari sırlarının veya fikri mülkiyet haklarının korunması gerekçesine dayanarak ilgili kişinin erişim talebini tamamen reddedemeyecek, sadece kısıtlayabilecektir⁸⁹³. Bu hda, kişisel verilerin korunmasına ilişkin hak ve yükümlülüklerin sadece “gerekli” ve “ölçülü” olması halinde kısıtlanabileceğini belirten Tüzüğün giriş bölümünün 23. paragrafı ile de uyumludur⁸⁹⁴.

Wachter ve diğerleri, ilgili kişinin erişim hakkının veri sorumlusunun ticari sır ve fikri mülkiyet haklarıyla sınırlandırılmasının karşısında bireyin haklarının korunmasını sağlayacak bir tedbir olarak, otomatik karar faaliyetleri için bir dış denetim mekanizması geliştirilmesini veya veri sorumluları için iç denetim şartları oluşturulmasını tavsiye etmiştir⁸⁹⁵. İlgili kişi hakkında bir kararın gerekçesi ve karara etki eden koşullar da dahil olmak üzere, otomatik karar sisteminin bağımsız bir üçüncü tarafça denetlenmesine imkan tanınması, veri sorumlularının ticari sırlarının ifşa edilmesi riskini azaltırken, karara ilişkin açıklamalarından birinin anlayamayacağı kadar karmaşık olduğu durumlarda da ilgili kişi için bir gözetim mekanizması teşkil edecektir⁸⁹⁶. Bunun için denetim otoritelerinin yetkilerinin genişletilebileceği, alternatif olarak ise algoritmaların denetlenmesi için Avrupa Birliği’nde faaliyet gösterecek bir düzenleyici kuruluş oluşturulabileceği belirtilmiştir⁸⁹⁷.

⁸⁹² Bkz. GVK Tüzüğü, Giriş Bölümü, 63.Paragraf.

⁸⁹³ Article 29 Working Party, Automated Individual Decision-Making and Profiling, s.17; Malgieri & Comandé, s.34.

⁸⁹⁴ Malgieri & Comandé, s.34.

⁸⁹⁵ Wachter & Mittelstadt & Floridi, s.46.

⁸⁹⁶ Wachter & Mittelstadt & Floridi, s.46.

⁸⁹⁷ Wachter & Mittelstadt & Floridi, s.46.

3.3.3. İlgili Kişinin Otomatik Kararların Açıklanmasını Talep Hakkı

İlgili kişinin bilgilendirilme ve erişim hakkı, GVK Tüzüğü'nün geneline sirayet eden, kişisel verilerin şeffaf bir şekilde işlenmesi ilkesinin uygulamada hayat bulmasını sağlayan önemli araçlardır. Şeffaflık ilkesi, ilgili kişiye sağlanan bilgilerin “özlü, kolay erişilebilir ve anlaşılması kolay” olmasının yanı sıra, kişisel verileri "toplanan, kullanılan veya başka bir şekilde işlenen" ilgili kişinin “veri işleme faaliyetinin varlığı ve amaçları” hakkında da bilgilendirilmesini gerektirir⁸⁹⁸. GVK Tüzüğü'nün ilgili kişinin bilgilendirilmesine ilişkin 13. ve 14. maddeleri, erişim hakkına ilişkin 15. maddesi ve profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı kararlara konu edilmeme hakkına ilişkin 22. maddesi birlikte değerlendirildiğinde, ilgili kişiye m. 22 kapsamındaki otomatik kararlara ilişkin olarak, m. 22/3 tahtında düzenlenen insan müdahalesi talep etme hakkı, kendi görüşünü beyan etme hakkı ve karara itiraz etme hakkına ilaveten, “otomatik kararın açıklanmasını talep etme hakkı”⁸⁹⁹ (“*right to explanation*”) tanıyıp tanımadığı sorusu ortaya çıkmaktadır.

GVK Tüzüğü düzenlemelerindeki boşluklar ve belirsizlikler sebebiyle, profillemeye ve otomatik karar faaliyetleri bağlamında ilgili kişiye hangi kapsamda bilgi sağlanacağı, veri sorumlusunun ilgili kişiye verilerinin işlenmesinde yürütülen mantığına ilişkin anlamlı bilgi sağlama yükümlülüğünün ilgili kişiye kararın açıklanmasını talep hakkı tanıyıp tanımadığı, ilgili kişiye böyle bir hak tanınıyorsa açıklaması gereken bilginin kapsamının ne olacağı konularında doktrinde tartışmalar mevcuttur. Tüzüğün bu maddelerinin ilgili kişi açısından bir açıklama talep etme hakkı teşkil ettiğini savunan görüşlerin⁹⁰⁰ yanı sıra karşıt görüşler⁹⁰¹ de

⁸⁹⁸ Bkz. GVK Tüzüğü, Giriş Bölümü, 39.Paragraf, 58.Paragraf, 60.Paragraf.

⁸⁹⁹ Çalışmanın devamında kısaca “açıklama hakkı” olarak ifade edilmiştir.

⁹⁰⁰ Andrew D. SELBST & Julia POWLES, Meaningful Information and the Right to Explanation, International Data Privacy Law, Vol.7(4), 233-242, 2017; Bryce GOODMAN & Seth FLAXMAN, European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”, AI Magazine, Vol.38(3), 2017, <https://arxiv.org/abs/1606.08813>.

⁹⁰¹ Lilian EDWARDS & Michael VEALE, Slave to the algorithm? Why a ‘right to an explanation’ is probably not the remedy you are looking for, 16 Duke Law & Technology Review 18, 2017; Sandra WACHTER & Brent MITTELSTADT & Luciano FLORIDI, Why a Right to Explanation of

bulunmaktadır. Özellikle açıklamanın kapsamının ne olacağı konusunda bir görüş birliği bulunmamaktadır.

Wachter, Mittelstadt ve Floridi, otomatik kararlara ilişkin talep edilebilecek açıklamaları, açıklamanın içeriği ve açıklamanın zamanı bağlamında kategorilendirmiştir⁹⁰². Buna göre, bir otomatik karar, sistem gereksinim özellikleri (“*system’s requirements specifications*”), karar ağaçları (“*decision trees*”), önceden tanımlanmış modeller (“*pre-defined models*”), sınıflandırma yapıları (“*classification structures*”) gibi otomatik karar sisteminin genel anlamda işlevselliği, mantığı, önemi, öngörülen sonuçlarını ifade eden “sistem işlevselliği” (“*system functionality*”) bağlamında açıklanabileceği gibi, söz konusu açıklama özelliklerin ağırlıklandırılması, makine tanımlı vakaya özel karar kuralları (“*machine-defined case-specific decision rules*”), referans veya profil grupları hakkında bilgiler gibi belirli bir otomatik kararın gerekçesi, nedenleri ve karara etki eden bireysel koşullara ilişkin olarak “belirli bir kararın” (“*specific decision*”) açıklanması şeklinde de gerçekleşebilir⁹⁰³. Otomatik kararların açıklanması, açıklamanın karardan önce mi yoksa sonra mı gerçekleştirildiğine göre de ayrılmaktadır⁹⁰⁴. İlgili kişi hakkında bir karar alınmadan önce (*ex ante*), sistem işlevselliğine ilişkin açıklama yapılması; ilgili kişi hakkında bir karar alındıktan sonra (*ex post*) ise hem sistem işlevselliğine ilişkin hem de belirli bir karara ilişkin açıklama yapılması mümkündür⁹⁰⁵. Bu ayrım, otomatik kredi puanlama sistemi örneği üzerinden somutlaştırılmıştır⁹⁰⁶. Kredi puanı, ilgili kişinin kredi başvurusunda, başvurunun kabul edilip edilmeyeceğini, edilmesi halinde kredi faizi, vade gibi koşullarının belirleyen bir referans değerdir. Kredi puanına dayanılarak herhangi bir insan müdahalesi olmaksızın tamamen otomatik işlemeye dayalı olarak ilgili kişiye kredi verilip verilmemesine ilişkin bir karar alındığında

Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 2017.

⁹⁰² Wachter & Mittelstadt & Floridi, s.6.

⁹⁰³ Wachter & Mittelstadt & Floridi, s.6-7.

⁹⁰⁴ Wachter & Mittelstadt & Floridi, s.6.

⁹⁰⁵ Wachter & Mittelstadt & Floridi, s.6.

⁹⁰⁶ Wachter & Mittelstadt & Floridi, s.6.

m.22 tahtında bir otomatik karardan söz edilebilecektir. Bu karar alınmadan önce (*ex ante*), veri sorumlusu ilgili kişiyi sistemin işlevselliği hakkında, sistemin genel işleyiş mantığı, sistemin kullanım amacı, öngörülen sonuçlarına ilişkin bilgilendirebilecektir⁹⁰⁷. Karar verildikten sonra (*ex post*) ise, sistem işlevselliğine ilişkin bir açıklamanın yanı sıra, ilgili kişinin kredi puanına ilişkin, bu puanın oluşturulmasında izlenen mantık, dikkate alınan veriler ve karar modelinde bunların ağırlığının ne olduğu gibi karar özelinde açıklamalar yapılabilecektir⁹⁰⁸.

Kaltheuner ve Bietti, ilgili kişiye otomatik karardan önce (*ex ante*) yapılacak açıklamanın, profillemeye faaliyetinin ne gibi sonuçları olabileceğini muhakeme edebilmeleri ve buna göre otomatik karar alma faaliyetine rıza gösterip göstermemeye karar verebilmeleri açısından önemli olduğunu vurgulamışlardır⁹⁰⁹. Bu aşamada yapılacak açıklama ile ilgili kişi, otomatik kararın ne ölçüde profillemeye faaliyeti sonucunda ulaşılan çıkarım veya tahminlere dayanacağına ilişkin de bilgilendirilmelidir⁹¹⁰. İlgili kişiye otomatik karara rıza göstermeden önce yapılacak açıklamanın GVK Tüzüğü m.13/2(f), 14/2(g) ve 15/1(h) tahtında “anamlı bilgi” teşkil edebilmesi için,

- Otomatik karar sisteminde kullanılacak girdi verilerinin neler olduğu,
- Veri sorumlularının bu sistemin kullanılması suretiyle ne tür bilgilerin çıkarılmasını veya tahmin edilmesini amaçladıkları,
- Girdi verisinin hangi sıklıkla güncellendiği,
- Üçüncü kişilerin eylemlerinin ilgili kişi hakkındaki profillemeye faaliyetine bir etkisinin bulunup bulunmadığı,
- Sistemin algoritmalara dayandığı,

⁹⁰⁷ Wachter & Mittelstadt & Floridi, s.6-7.

⁹⁰⁸ Wachter & Mittelstadt & Floridi, s.6-7.

⁹⁰⁹ Kaltheuner & Bietti, s.15.

⁹¹⁰ Kaltheuner & Bietti, s.15.

- Veri sorumlusunun otomatik karar sisteminin neden olabileceği önyargılı, ayrımcı ve hatalı kararların önlenmesi için ne gibi tedbirler alacağına ilişkin bilgi içermesi gerekir⁹¹¹.

Kaltheuner ve Bietti, karardan sonra ise, ilgili kişinin, otomatik kararın hukuka aykırı veya haksız olup olmadığını, diğer bir ifadeyle, neden bu sonucu aldığı, bu sonucu almasına nelerin etki ettiği ve farklı bir sonuç alması için kişisel durumu, davranışları veya sistemin tasarımı ile ilgili neyin farklı olması gerektiğini, otomatik kararın hukuka aykırı veya haksız olup olmadığını değerlendirebilecek durumda olması gerektiği görüşündedir⁹¹². Buna göre, ilgili kişinin bu değerlendirmeyi yapabilmesi için, kendisine ilgili otomatik karar özelinde (*ex post*) bir açıklama yapılmalıdır⁹¹³. Kaltheuner ve Bietti, karardan sonra yapılacak “yürütülen mantığa ilişkin” açıklamanın, verilerin otomatik işleme şekline ilişkin bilginin yanı sıra ilgili kişilere kararın dayandırıldığı verilere erişim sağlanmasını gerektirdiğini, ayrıca veri koruma otorilerinin de kararlardaki muhtemel önyargı ve ayrımcılıkların ortaya çıkarılabilmesi için kararları denetleyebilmeleri gerektiğini ifade etmiştir⁹¹⁴.

Gerek Tüzüğün profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar almaya ilişkin 22. maddesinde, gerek veri sorumlusunun bilgilendirme yükümlülüğünü düzenleyen 13. ve 14. maddelerinde ilgili kişinin “açıklama hakkı”na ilişkin açık bir ifadeye yer verilmemiştir. Açıklama talep etme hakkına ilişkin açık bir düzenlemeye sadece m. 22’nin gerekçesini teşkil eden Tüzüğün giriş bölümünün (*recitals*) 71. paragrafında yer verilmiştir. Tüzüğün 71. paragrafında, Tüzük m. 22/3 tahtında otomatik karar alma faaliyetlerinde alınacak uygun tedbirlerin yanısıra açık bir şekilde, ilgili kişiye, kendisi hakkında verilen bir otomatik karara ilişkin açıklama talep etme hakkı tanınması gerektiği belirtilmektedir⁹¹⁵. GVK Tüzüğü, giriş bölümündeki gerekçeler (*recitals*) ve

⁹¹¹ Kaltheuner & Bietti, s.15-16.

⁹¹² Kaltheuner & Bietti, s.16.

⁹¹³ Kaltheuner & Bietti, s.15.

⁹¹⁴ Kaltheuner & Bietti, s.16.

⁹¹⁵ Bkz. GVK Tüzüğü, Giriş Bölümü, 71.Paragraf.

maddeler (*articles*) olmak üzere iki bölümden oluşur. Belirtmek gerekir ki, Avrupa Birliği hukukunda gerekçe düzenlemelerinin, üye devletlerin ilgili mevzuat hükümlerini yorumlamalarına rehberlik eden ve destek olan ancak bağlayıcı hak ve yükümlülükler tesis etmeyen düzenlemeler olduğu kabul edilmektedir. Bununla birlikte GVK Tüzüğünde, ana metinde üzerinde anlaşmaya varılamayacak kadar tartışmalı olan birçok konunun, bu husus görmezden gelinerek gerekçeler bölümünde düzenlenmiş olması, bu düzenlemelerin bağlayıcılığına ilişkin tartışmaların doğmasına neden olmuştur⁹¹⁶.

Benzer şekilde, Tüzük m.22’de açık bir hükme yer verilmeksizin gerekçelerin (giriş bölümü) 71.paragrafında açık bir şekilde açıklama talep etme hakkından bahsedilmiş olmasına dayanılarak, 22. maddenin ilgili kişiye bir açıklama talep etme hakkı tanıdığı sonucunun çıkarılıp çıkarılamayacağı konusunda farklı görüşler oluşmuştur. Wachter, Mittelstadt ve Floridi, gerekçelerin üye devletlerin ilgili mevzuatın amacını anlamalarına yardımcı olmak üzere tasarlanmış düzenlemeler olduğu ve tek başına bağlayıcılığa sahip olmadıkları gerekçesiyle, 71. paragrafın veri sorumluları açısından bağlayıcı bir yükümlülük tesis etmediğini ileri sürmüştür⁹¹⁷. Buna göre, Tüzüğün 71. paragrafındaki gibi bir açıklama talep etmek hakkı tesis edilmesi amaçlanıyorsa, Tüzüğün bağlayıcı nitelikteki esas maddelerinden birinde açık bir düzenleme yapılmalıdır⁹¹⁸. Buna alternatif olarak, üye devletlerin GVK Tüzüğü’nün yanı sıra kararın açıklanmasını talep hakkını açıkça düzenleyen ayrı bir kanunu yürürlüğe koymaya teşvik edilebilecekleri belirtilmiştir⁹¹⁹. Edwards ve Veale de bu görüşe paralel şekilde, giriş bölümünün 71. paragrafının açıklama talep etme hakkına sağlam bir temel teşkil etmeyeceği görüşündedir⁹²⁰. Buna karşın Brkan, Tüzüğün gerekçe düzenlemelerinin bağlayıcı olmadığı gerekçesiyle Tüzüğün ilgili kişiye açıklama

⁹¹⁶ Edwards & Veale, *Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for*, s.50.

⁹¹⁷ Wachter & Mittelstadt & Floridi, s.8-10.

⁹¹⁸ Wachter & Mittelstadt & Floridi, s.44.

⁹¹⁹ Wachter & Mittelstadt & Floridi, s.44.

⁹²⁰ Edwards & Veale, *Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for*, s.50.

talep etme hakkı tanıma olasılığının reddedilmesinin “şekilci” bir yaklaşımı temsil ettiğini ileri sürmüştür⁹²¹. Zira her ne kadar açıklama talep etme hakkı 22.maddede açıkça düzenlenmemiş olsa da maddenin gerekçesinde bu hakkın açıkça belirtilmiş olması, Tüzüğün taslak aşamasında bu hakka yer verilip verilmeyeceği konusunda ortaya çıkan uyuşmazlığa uzlaştırmacı bir çözüm olarak, kanun koyucunun bu hakkı tamamen Tüzüğün dışında bırakmama yönündeki niyetine işaret etmektedir⁹²². Tüzüğün bu şekilde kaleme alınmış olması, aynı zamanda kanun koyucunun ilgili kişiye böyle bir hak tesis edilip edilmeyeceği ile ilgili son kararı Avrupa Birliği Adalet Divanı’na bıraktığını göstermektedir⁹²³. Öte yandan, Adalet Divanı içtihatından, gerekçelerin ilgili Avrupa Birliği mevzuatı hükümlerinin hukuka aykırı bir şekilde yorumlanması için kullanılamayacağı sonucu ortaya çıkmaktadır⁹²⁴. Brkan, bu duruma işaret etmekle birlikte, GVK Tüzüğü’nün farklı düzenlemelerin birlikte ve 71.paragrafı açıklama talep etme hakkının varlığını destekleyen şekilde yorumlayan yaklaşıma dayanılmasının hukuka aykırı bir yoruma neden olmayacağını, aksine, ilgili GVK Tüzüğü hükümlerinin birlikte okunmasından kaynaklanan belirsizliği çözmek için bir araç olarak hizmet edeceğini belirtmiştir⁹²⁵. Brkan, ayrıca, Avrupa Birliği Adalet Divanı’nın kişisel verilerin en üst seviyede korunmasını sağlamaya yönelik çabaları ve duruşu göz önüne alındığında, Mahkeme’nin Tüzük düzenlemelerini ilgili kişi lehine bir açıklama talep etme hakkı tesis edilecek şekilde yorumlamayı tercih etmesini muhtemel görmektedir⁹²⁶.

Goodman ve Flaxman, Tüzüğün veri sorumlusunun ilgili kişiye karar sürecinin işleyiş mantığı hakkında bilgilendirme yükümlülüğünü düzenleyen 13/2(f) ve 14/2(g) maddeleri ile otomatik karar faaliyetlerinde veri sorumlusunun alması gereken tedbirleri düzenleyen 22/3 maddesinin birlikte değerlendirildiğinde, ilgili kişiye kendisi hakkında bir otomatik karara ilişkin olarak, karar verildikten

⁹²¹ Brkan, s.16.

⁹²² Brkan, s.16.

⁹²³ Brkan, s.16.

⁹²⁴ Brkan, s.16.

⁹²⁵ Brkan, s.16-17.

⁹²⁶ Brkan, s.17.

sonra (*ex post*) “açıklama talep etme hakkı” tanındığını ileri sürmüştür⁹²⁷. Bu görüşe göre, ilgili kişiye kendisi hakkında verilen bir otomatik karar ile ilgili yapılacak bir açıklamanın, ilgili kişiyi en azından karar sürecine etki eden girdi verilerinin kendisi hakkındaki tahminlerle ne şekilde ilişkili olduğuna dair yeterli şekilde aydınlatması gerekir⁹²⁸. İlgili kişiye bu bağlamda yapılacak açıklama, “Başvuru sahibinin azınlık grubundan olması halinde skorlama modelinin kredi önerme olasılığı azalır mı yoksa artar mı?” ve “Hangi özellikler tahminde en büyük rolü oynuyor?” gibi sorulara cevap sağlayan nitelikte olmalıdır⁹²⁹.

Wachter, Mittelstadt ve Floridi, bu görüşün iki açıdan hatalı olduğu görüşündedir⁹³⁰. İlk olarak, 13/2(f) ve 14/2(g) maddelerinin lafzından, veri sorumlusuna sadece, karar alınmadan önce (*ex ante*) sistem işlevselliğine ilişkin açıklama yapma yükümlülüğü yüklendiği sonucu çıkmaktadır. Zira ilgili kişinin bilgilendirilmesi verilerin toplandığı anda, yani karardan önce gerçekleştirilmektedir. Bu maddeler uyarınca, ilgili kendisi hakkında bir otomatik karar alınmadan önce, genel olarak otomatik karar sisteminin nasıl çalıştığı, hangi amaçlar için kullanıldığı ve öngörülen etkisinin ne olduğu hususlarına ilişkin olarak bilgilendirilmelidir. Maddelerin lafzından, ilgili kişiye kendisi hakkında bir karar alındıktan sonra (*ex post*), kararın nasıl alındığı veya bu sonuca nasıl ulaşıldığına ilişkin bir bilgi verilmesi yerine, otomatik karar sisteminin nasıl çalıştığı, diğer bir ifadeyle sistemin işlevselliğine ilişkin bir açıklama yapılmasının mümkün olduğu sonucu çıkmaktadır⁹³¹. İkinci olarak ise, Goodman ve Flaxman’ın Tüzüğün belirtilen maddelerinin ilgili kişi için bir açıklama hakkı tesis ettiğine ilişkin iddiasında, m.13/2(f) ve m.14/2(g) ile m.22/3 ilişkilendirilmiş olmakla birlikte, esasen Tüzük’te bu maddeler arasında kurulmaya çalışılan şekilde bir ilişki bulunmamaktadır. Zira m.13/2(f) ve m.14/2(g) sadece m.22/1 ve m.22/4’e uygulanabilmektedir⁹³². Bu bağlamda, ilgili kişinin otomatik karar sürecinde

⁹²⁷ Goodman & Flaxman, s.6.

⁹²⁸ Goodman & Flaxman, s.6.

⁹²⁹ Goodman & Flaxman, s.6.

⁹³⁰ Wachter & Mittelstadt & Floridi, s.15.

⁹³¹ Wachter & Mittelstadt & Floridi, s.15.

⁹³² Bkz. m.13/2(f), m.14/2(g).

yürütülen mantık, kararın önemi ve öngörülen sonuçları hakkında bilgilendirilme hakkına ilişkin 13/2(f) ve 14/2(g) maddeleri ile ilgili kişiye karar verildikten sonra (*ex post*) açıklama hakkı tanındığı iddia edilen m.22/3'ün ilişkilendirilmesinin hatalı ve mesnetsiz olduğu belirtilmiştir⁹³³. Wachter ve diğerlerine göre, ilgili kişinin bilgilendirilme hakkına ilişkin maddelerin, karar alındıktan sonra (*ex post*) açıklama hakkı tanındığının iddia edilmesi, (i) karar alınmadan önce (*ex ante*) otomatik karar sisteminin mantığı, önemi ve öngörülen sonuçları hakkında ilgili kişinin bilgilendirilmesine ilişkin hukuki olarak bağlayıcı bir yükümlülük teşkil eden 13/2(f) ve 14/2(g) maddeleri ile (ii) ilgili kişiye belirli bir kararın, karar alındıktan sonra (*ex post*) açıklanmasına ilişkin bağlayıcı olmayan bir hak tanıyan giriş bölümünün 71.paragrafı arasındaki farklılıkların kavranamadığını göstermektedir⁹³⁴.

Wachter ve diğerleri, Tüzüğün 13/2(f), 14/2(g) ve 15/1(h) maddelerinin lafzının birebir aynı olduğundan bahisle, ilgili kişinin m.22 tahtındaki otomatik karar alma kapsamında erişim hakkını düzenleyen m. 15/1(h)'nin otomatik bir karara ilişkin açıklama sağlayamayacağı, sadece algoritmanın “sistem işlevselliğine”, yani “otomatik bir karar sisteminin mantığı, önemi, öngörülen sonuçları ve genel işlevselliğine” ilişkin açıklama sağlayacağı görüşündedir⁹³⁵. Buna göre, her üç maddede de “öngörülen sonuçlar” (“*envisaged consequences*”) ve “otomatik kararın varlığı” (“*the existence of automated decision making*”) ifadelerine yer verilmiş olması, ilgili kişilere sağlanacak bilgilerin içeriğinin de m.13/2(f) ve m.14/2(g) ile düzenlenen bilgilendirme yükümlülüğü ile aynı olmasının amaçlandığına işaret etmektedir⁹³⁶. Ayrıca, veri sorumluları kullandıkları otomatik karar sistemlerinin muhtemel sonuçlarını öngörmekle yükümlü olmakla birlikte, Tüzüğün belirtilen maddelerindeki “öngörülen” (“*envisaged*”) ifadesi ile veri sorumlularının otomatik karar sistemlerinin kullanılmasının muhtemel sonuçlarına ilişkin tahminleri, sistemin işlevselliği ile ilgili yapılacak açıklamalar

⁹³³ Wachter & Mittelstadt & Floridi, s.15.

⁹³⁴ Wachter & Mittelstadt & Floridi, s.15-16.

⁹³⁵ Wachter & Mittelstadt & Floridi, s.16.

⁹³⁶ Wachter & Mittelstadt & Floridi, s.17.

ile sınırlandırılmıştır⁹³⁷. Öte yandan, veri sorumlusunun ilgili kişiye “otomatik kararın varlığı” (“*existence of an automated decision*”) hakkında da bilgilendirmesi gerekmektedir. “Otomatik kararın varlığı” ifadesinin, veri sorumlusunun ilgili kişiyi sadece kişisel verilerinin işlenmesinde otomatik karar alma yöntemlerinin kullanıldığı konusunda bilgilendirmesi gerektiğine işaret ettiği, karara nasıl ulaşıldığı konusunda bir açıklama yapılmasını öngörmediği belirtilmiştir⁹³⁸. Bu bağlamda, Tüzüğün, Direktif’ten farklı şekilde, karar almanın zamanlamasına ilişkin olarak gelecek zamana atıfta bulunan “öngörülen sonuçlar” ifadesini içermesi ve erişim hakkına ilişkin 15.madde ile veri sorumlusunun bildirim yükümlülüğünü düzenleyen 13. ve 14. maddelerin lafzının aynı olması, otomatik karar alma açısından erişim hakkının da sadece sistem işlevselliği ile ilgili yapılacak açıklamalarla sınırlandırıldığını göstermektedir⁹³⁹. 29. Madde Çalışma Grubu, profillemeye ve otomatik karar almaya ilişkin rehberinin ilk versiyonunda⁹⁴⁰, bu görüşle paralel şekilde, ilgili kişinin erişim hakkına ilişkin 15.maddenin, belirli bir karara ilişkin açıklama talep etme hakkından ziyade otomatik kararlara ilişkin genel bir gözetim sağlamak üzere hüküm altına alındığını, ancak her halükarda ilgili kişinin bu hakkı kullanarak profillemeye içerenler de dahil olmak üzere tamamen otomatik işlemeye dayalı kararlar hakkında farkındalık kazanacağını belirtmiştir⁹⁴¹. Edwards ve Veale, Çalışma Grubu’nun bu yaklaşımını, otomatik karar verildikten sonra kararın açıklanmasına ilişkin bir açıklama hakkının tesis edilmesi ihtimali açısından zarar verici olarak nitelendirmiştir⁹⁴².

Wachter ve diğerlerinin aksine, Malgieri ve Comandé, m.15/1(h)’nin lafzı itibarıyla ilgili kişinin sadece otomatik karar alınmadan önce (*ex ante*) bilgi talep edebileceği bir erişim hakkından ibaret olmadığı görüşündedir. Bu görüşe göre,

⁹³⁷ Wachter & Mittelstadt & Floridi, s.17.

⁹³⁸ Wachter & Mittelstadt & Floridi, s.18.

⁹³⁹ Wachter & Mittelstadt & Floridi, s.28.

⁹⁴⁰ İlgili rehberin 2018’de revize edilen versiyonunda bu ifadeye yer verilmemiştir.

⁹⁴¹ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), 3 Ekim 2017, s.24, <https://perma.cc/3X54-2DGC>.

⁹⁴² Veale & Edwards, Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, s.400.

13/2(f), 14/2(g) ve 15/1(h) maddelerinin lafzı aynı olsa da işlevleri farklıdır. Zira m.13/2(f) ve m.14/2(g) ile veri sorumlularına, ilgili kişileri otomatik işleme faaliyetine ilişkin detayları hakkında verilerin işlenmesinden önce bilgilendirme konusunda proaktif bir yükümlülük getirilirirken, m.15/1(h) ile ilgili kişiye kendisi hakkındaki bir otomatik işleme faaliyetine ilişkin bilgi talep edebilmesi için, karardan önce veya sonra herhangi bir zamanda kullanabileceği erişim hakkı tesis edilmiştir⁹⁴³. Öte yandan, ilgili maddelerdeki “öngörülen sonuçlar” ifadesi, ilgili kişiye karar alınmadan önce (*ex ante*) verilebilecek bilgiye atıf yapıyor ise de “yürütülen mantığa ilişkin” anlamlı bilgi verilmesi de ancak karar alındıktan sonra (*ex post*) yapılabilecek bir açıklamaya işaret etmektedir⁹⁴⁴.

Malgieri ve Comandé ile benzer görüşte olan Edwards ve Veale, ilgili kişinin yapay öğrenme algoritmaları ile çalışan sistemlerin işleyişinin şeffaf bir şekilde açıklanması talebinin, Tüzüğün otomatik karar almaya ilişkin 22. maddesi yerine, doğrudan otomatik karar almaya ilişkin olmayan ve ilgili kişinin erişim hakkını düzenleyen 15.maddeye dayandırılabilirliğini ileri sürmüşleridir⁹⁴⁵. Bu bağlamda, ilgili kişi Tüzük m.15 tahtında erişim hakkını kullandığında, kendisine belirli bir otomatik karara ilişkin olarak, karar verildikten sonra (*ex post*), kararın mantığı ve karara etki eden koşullara ilişkin detayları içeren bir açıklama sağlanabilecektir⁹⁴⁶. Edwards ve Veale, Tüzüğün ilgili kişi lehine bir açıklama talep etme hakkı tesis ettiğinin kabul edilebileceğini belirtmekle birlikte, yapay öğrenme algoritmalarının işleyişi bakımından bu hakkın pratikte kullanılmasına ilişkin bazı engeller söz konusu olduğunu da belirtmiştir⁹⁴⁷.

Tüzüğün ilgili düzenlemelerini ayrı ayrı ele alan Wachter ve diğerlerinin aksine Brkan, açıklama talep etme hakkına ilişkin yapılacak incelemede, Tüzüğün

⁹⁴³ Malgieri & Comandé, s.20.

⁹⁴⁴ Malgieri & Comandé, s.21.

⁹⁴⁵ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.51.

⁹⁴⁶ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.52; Malgieri & Comandé, s.20.

⁹⁴⁷ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.44-54.

ilgili maddelerinin birlikte değerlendirilmesi gerektiği görüşündedir⁹⁴⁸. Buna göre, giriş bölümünün 71. paragrafı ışığında, m.22 ile m.13/2(f), m.14/2(g) ve m.15/1(h) birlikte ele alınarak, ilgili kişiye kendisi hakkında bir otomatik karar karar verildikten sonra (*ex post*) kararın açıklanmasını talep etme hakkı verecek şekilde yorumlanmalıdır⁹⁴⁹. Brkan, Avrupa Adalet Birliği Adalet Divanı'nın Google kararında⁹⁵⁰, mahkemenin “unutulma hakkı”nın (*right to be forgotten*) tesisi için 95/46 sayılı Direktif'in erişim hakkı ve itiraz hakkı ile ilgili düzenlemelerini birlikte ele aldığından bahisle, ilgili kişi lehine belirli bir hakkın tesis edilmesi amacıyla farklı veri koruma düzenlemelerinin metodolojik olarak gruplandırılmasının, Adalet Divanı içtihatında olağandışı bir durum olmadığını belirtmiştir⁹⁵¹. Açıklanan nedenle, Avrupa Birliği Adalet Divanı, ilgili kişi için bir açıklama talep etme hakkı tesis etmek istiyorsa, ilgili maddeleri birlikte ele almalı ve yorumlamalıdır⁹⁵². Öte yandan Tüzük kapsamında ilgili kişiye tanınan haklardan biri olan otomatik karara itiraz hakkı, kararın esasına ilişkin bir hak olduğundan, ilgili kişiye kendisi hakkındaki bir karara ilişkin herhangi bir açıklama yapılmaması halinde, otomatik kararlara itiraz etme hakkı da tamamen etkisiz hale gelecektir⁹⁵³. İlgili kişinin kendisi ile ilgili bir otomatik karara itiraz edebilmesi için, kararın oluşturulmasına etki eden girdi verilerinin neler olduğuna ve kararın gerekçesine ilişkin makul bir açıklama yapılması gerekir⁹⁵⁴. Brkan'ın, Tüzük'te açıklama talep etme hakkının bulunduğu yönelik değerlendirmesinde sunduğu gerekçelerden bir diğeri de m.22/3'ün dikkatli bir şekilde ele alınması halinde belirtilen tedbirlerin sınırlı sayıda olmadığı sonucunun ortaya çıkmasıdır⁹⁵⁵. Zira maddede veri sorumlusunun, “en azından” ilgili kişiye belirtilen hakları sağlayarak uygun tedbirleri alması gerektiği ifade edilmiştir⁹⁵⁶. Dolayısıyla, hukuki yorum ile bu

⁹⁴⁸ Brkan, s.15.

⁹⁴⁹ Brkan, s.15.

⁹⁵⁰ Google Spain SL, Google Inc v. Agencia Española de Protección de Datos kararı için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN>.

⁹⁵¹ Brkan, s. 15.

⁹⁵² Brkan, s. 15-16.

⁹⁵³ Brkan, s.16.

⁹⁵⁴ Brkan, s.16.

⁹⁵⁵ Brkan, s.17.

⁹⁵⁶ Brkan, s.17.

haklara yeni bir hak eklenmesi, m. 22/3'ü ihlal eden veya hükmün lafzına aykırı bir yorum teşkil etmeyecektir⁹⁵⁷. Son olarak Brkan, Tüzük'te genel anlamda bir açıklama hakkının varlığı tanınmasa dahi, bu hakkın özel nitelikli kişisel verilerin işlenmesine dayanan otomatik karar faaliyetleri açısından kabul edilmesi gerektiğini savunmuştur⁹⁵⁸. İlgili kişinin açık rızasının bulunması veya kayda değer ölçüde kamu yararı için işleme faaliyetinin gerekli olması halleri dışında, otomatik karar faaliyetlerinde özel nitelikli kişisel verilerin işlenmesi yasaktır⁹⁵⁹. Tüzük, özel nitelikli kişisel verilerin işlendiği otomatik karar faaliyetlerinde veri sorumlusunun ilgili kişiye karar sürecinin mantığı hakkında anlamlı bilgi vermekle yükümlü tutmaktadır⁹⁶⁰. Tüzük'te, genel olarak özel nitelikli kişisel verilerin işlenmesine daha fazla koruma öngörülmüş olmakla birlikte, özel nitelikli kişisel verilerin işlenmesi sonucu verilen bir otomatik kararın ilgili kişi üzerinde hukuki ya da benzer şekilde önemli bir etkiye neden olması durumunda, ilgili kişiye kararın arkasındaki sebepleri kavrayabilmesini sağlayacak bir bilgilendirme yapılmadan sadece sistemin genel işleyişi hakkında bilgi verilmesi, ilgili kişinin Tüzük'te öngörülen korumadan faydalanamamasına neden olacaktır⁹⁶¹.

Wachter, Mittelstadt ve Russell'a göre, ilgili kişinin yapay öğrenme algoritmalarının "kara kutu" (*black box*) olarak nitelendirilen çalışma mekanizmasına ilişkin bilgilendirilmesi amacıyla bir açıklama hakkının tesis edilmesi girişiminin önünde dört önemli hukuki ve teknik engel bulunmaktadır⁹⁶². İlk olarak GVK Tüzüğü, ilgili kişiye hukuki olarak bağlayıcı bir açıklama hakkı tesis etmemektedir. İkincisi, hukuki olarak bağlayıcı bir açıklama hakkı tesis ettiği kabul edilse dahi, bu hak sadece belirli sınırlı durumlarda (m.22'nin kapsamına giren profillemeye ve otomatik karar alma faaliyetleri açısından) uygulama alanı bulacaktır. Üçüncüsü, otomatik karar sistemlerinin karmaşık algoritmik yapısının ve işleyişinin ve belirli kararların arkasındaki mantığın açıklanması teknik açıdan

⁹⁵⁷ Brkan, s.17.

⁹⁵⁸ Brkan, s.17.

⁹⁵⁹ Bkz. GVK Tüzüğü, m.9/2(a), 9/2(g).

⁹⁶⁰ Bkz. GVK Tüzüğü, m.13/2(f), 14/2(g), 15/1(h).

⁹⁶¹ Brkan, s.17.

⁹⁶² Wachter & Mittelstadt & Russell, s. 842.

da oldukça zordur. Son olarak, veri sorumluları, “ticari sır” olduğundan bahisle, otomatik karar sisteminin algoritmasının detaylarını açıklamaktan, üçüncü kişilerin hak ve özgürlüklerini ihlal etmekten ve ilgili kişilerin karar sistemini manipüle etmesine izin vermekten kaçınma eğilimi gösterebilmektedir⁹⁶³. Öte yandan, Tüzüğün giriş bölümünün 71. paragrafında da 22. madde kapsamına giren otomatik kararlara itiraz edilebileceği veya otomatik kararların “kara kutu” olarak tabir edilen işleyişinin sorgulanmasına ilişkin bir ifadeye yer verilmemiştir. Nitekim 29. Madde Çalışma Grubu da ilgili rehberinde, veri sorumlusunun ilgili kişiyi, kullanılan algoritmaların karmaşık bir açıklamasının yapılması veya algoritmanın tamamının ifşa edilmesi yoluna başvurulmaksızın, otomatik kararın gerekçeleri ve dayandığı kriterler hakkında basit ve anlaşılır şekilde bilgilendirmesi gerektiğini belirtmiştir⁹⁶⁴.

Wachter ve diğerlerine göre, otomatik kararlara ilişkin yapılacak açıklamalar üç amaca hizmet eder. Buna göre, otomatik kararlara ilişkin yapılacak açıklamalar, (i) ilgili kişiyi bilgilendirmek ve neden ilgili kararın verildiğini anlamasına yardımcı olmayı, (ii) ilgili kişinin kendisi hakkında olumsuz bir karara itirazını dayandırabileceği gerekçeleri ve (iii) mevcut karar modeline dayanılarak ileride istenen bir sonucu elde edebilmek için neyi değiştirmesi gerektiğini anlamasını sağlamayı amaçlar⁹⁶⁵. Ancak GVK Tüzüğü bu amaçların gerçekleştirilmesi için yeterli bir hukuki çerçeve sunmamaktadır⁹⁶⁶. Wachter ve diğerleri, algoritmik karar alma uygulamalarına karşı toplum nezdinde yeterli güven tesis edildiği ölçüde bu uygulamaların kabul göreceğinden bahisle, veri sorumluları ile ilgili kişiler arasında güven ortamı yaratılmasının önünde engel teşkil eden şeffaflık ve hesap verebilirlik ile ilgili sorunların çözülmesi gerektiği görüşündedir. Bunu sağlamak amacıyla, GVK Tüzüğü ile getirilen düzenlemelerin dışına çıkılarak, temeli analitik felsefeye dayanan “karşı olgusal açıklamaların” (“*counterfactual explanations*”) otomatik bireysel kararların yapay öğrenme

⁹⁶³ Wachter & Mittelstadt & Russell, s.843.

⁹⁶⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.25.

⁹⁶⁵ Wachter & Mittelstadt & Russell, s.843.

⁹⁶⁶ Wachter & Mittelstadt & Russell, s.843.

alanında uzman ve uzman olmayan kişilere açıklanmasında etkili bir araç olarak kullanılabileceğini ileri sürmüştür⁹⁶⁷.

Karşı olgusal açıklamalar kredi örneği üzerinden somutlaştırılabilecektir⁹⁶⁸: “Yıllık gelirin (X) tutarında olduğu için kredi talebiniz reddedilmiştir. Gelirin (Y) tutarında olsaydı, talebiniz reddedilmeyecek ve size bir kredi teklif edilebilecekti.” Otomatik kararların açıklanmasına yönelik yeni bir yöntem olarak sunulan karşı olgusal açıklamaların, algoritmik kararların yorumlanabilmesi ve veri sorumlularının algoritmik karar alma faaliyetleri açısından hesap verebilirliğine ilişkin birçok sorunun üstesinden gelebileceği, bu bağlamda GVK Tüzüğü’nde bağlayıcı bir açıklama hakkının tesis edilmesinin önünde engel teşkil eden ilgili kişi ile veri sorumlusunun çıkarları arasındaki boşluğu doldurabileceği belirtilmektedir⁹⁶⁹. Karşı olgusal açıklamalar, algoritmaların kara kutu olarak tabir edilen mekanizmasının işleyiş mantığı hakkında bilgi sağlanması yerine, arzu edilen bir karar için hangi dış etkenlerin değiştirilebileceğine odaklanır⁹⁷⁰. Açıklama kararın verildiği anda otomatik olarak oluşturulabileceği gibi, modelin kayıt altına alınan bir kopyası esas alınarak daha sonra da oluşturulabilecek; kararın verildiği anda veya ilgili kişinin ya da üçüncü kişi denetçinin talebi üzerine iletilebilecektir⁹⁷¹. Gerek olumlu gerekse olumsuz otomatik kararlar için, kararların tamamen (çoğunlukla olanın aksine) otomatik işlemeye dayalı olup olmadığına veya hukuki veya benzer şekilde önemli etkiler doğurup doğurmadığına bakılmaksızın, koşulsuz olarak karşı olgusal açıklamalar sağlanması gerektiği belirtilmiştir⁹⁷². Zira karşı olgusal açıklamalar ile GVK Tüzüğü’ndeki “otomatik bireysel karar alma” tanımının yol açtığı sınırlı uygulama alanının ötesine geçilerek, (i) ilgili kişinin kendisi hakkındaki bir otomatik kararı anlamasına yardımcı olacak anlamlı bir açıklama, (ii) ilgili kişinin karara itiraz etmek istemesi halinde itirazını dayandırabileceği gerekçeler ve (iii) ilgili kişinin

⁹⁶⁷ Wachter & Mittelstadt & Rusell, s.843-846.

⁹⁶⁸ Wachter & Mittelstadt & Rusell, s.844.

⁹⁶⁹ Wachter & Mittelstadt & Rusell, s.843.

⁹⁷⁰ Wachter & Mittelstadt & Rusell, s.880.

⁹⁷¹ Wachter & Mittelstadt & Rusell, s.881.

⁹⁷² Wachter & Mittelstadt & Rusell, s.844, s.881.

memnun olacağı şekilde bir sonuç elde etmek için (kredi başvurusunun onaylanması gibi) davranışlarını veya koşullarını nasıl değiştirebileceğine ilişkin öneriler sağlanabilmektedir⁹⁷³.

Karşı olgusal açıklamalar, otomatik kararların GVK Tüzüğü'nün "açıklama hakkı" ekseninde nasıl açıklanabileceğine ilişkin yapay öğrenme ve hukuk alanında ileri sürülen önerilerle kıyaslandığında çeşitli avantajlar sunar⁹⁷⁴. Öncelikle, karşı olgusal açıklamalar yapay öğrenme sistemlerinin karmaşık iç işleyişinin açıklanmasına gerek bulunmadığı anlayışına dayanmaktadır. Bu bağlamda, karşı olgusal açıklamalar algoritmaların uzman kişilerce dahi anlaşılmasını zorlaştıran ve "kara kutu" olarak tabir edilen iç işleyişinin açıklanmasının önündeki zorlukları ortadan kaldırır. Böylece karşı olgusal açıklamalar ile ilgili kişiye kolaylıkla anlayabileceği bir şekilde, otomatik kararın altında yatan gerekçeleri anlamasını, karara itiraz edebilmesini ve ileride daha memnun olacağı bir sonuç elde etmek için davranışlarını ne şekilde değiştirmesi gerektiğini anlamasına yardımcı olacak faydalı bilgiler sağlanabilir⁹⁷⁵. Öte yandan, otomatik kararların iç işleyiş mantığı hakkında insan zihninin kavrayabileceği şekilde anlamlı bir bilginin var olup olmadığı net olmamakla birlikte, bu tür bir bilgilendirmenin yapay öğrenme konusunda uzman olmayan kişilere nasıl yapılacağı da ayrı bir sorun teşkil etmektedir. Kaldı ki, sistemin iç işleyiş mantığına ilişkin bilgilerin açıklanması ticari sırların veya eğitim veri setinde bulunan üçüncü kişilere ait verilerin açıklanmasına neden olarak üçüncü kişilerin haklarının ihlal edilmesine yol açabilecektir⁹⁷⁶. Buna karşın, karşı olgusal açıklamalar, otomatik karar sürecinin iç işleyiş mantığı ile ilgili bilgi verilmeksizin ve üçüncü kişilerin hak ve özgürlüklerinin ihlal edilmesine neden olmaksızın basit bir şekilde oluşturulabilir ve ilgili kişiye aktarılabilirler⁹⁷⁷. Karşı olgusal açıklamalar ile "kara kutunun açılmasına" gerek olmaksızın, ilgili karara etki eden dış faktörler ile temel

⁹⁷³ Wachter & Mittelstadt & Rusell, s.844.

⁹⁷⁴ Wachter & Mittelstadt & Rusell, s.860.

⁹⁷⁵ Wachter & Mittelstadt & Rusell, s.860.

⁹⁷⁶ Wachter & Mittelstadt & Rusell, s.882-883.

⁹⁷⁷ Wachter & Mittelstadt & Rusell, s.861, s.883.

değişkenler hakkında bilgi sağlamak suretiyle ilgili kişilerin m.22 tahtında düzenlenen otomatik karara itiraz etme hakkını kullanmalarına uygun bir zemin hazırlanabilecek ve GVK Tüzüğü'nden daha iyi bir koruma sağlanacaktır⁹⁷⁸.

3.3.4. İlgili Kişinin Düzeltme Hakkı

GVK Tüzüğü'nün 16. maddesi uyarınca, ilgili kişi veri sorumlusundan “kendisi ile ilgili doğru olmayan kişisel verilerin düzeltilmesini ve tamamlanmasını talep etme hakkına” (“*right to rectification*”) sahiptir⁹⁷⁹. Benzer şekilde, KVK Kanunu'nun 11/d maddesinde, ilgili kişinin “kişisel verilerin eksik veya yanlış işlenmiş olması halinde, bunların düzeltilmesini talep edebileceği” düzenlenmiştir. İlgili kişi aynı zamanda, kişisel verilerinin veri sorumlusunca düzeltilmesi halinde, veri sorumlusundan “kişisel verilerinin aktarıldığı üçüncü kişilere bu hususunun bildirilmesini talep etme” hakkına sahiptir⁹⁸⁰.

Profilleme faaliyeti sonucunda yapılan çıkarımların bir tahmin sonucunu yansıtması, bu çıkarımların yanlış olma riskini artırmaktadır⁹⁸¹. Girdi olarak kullanılan veriler yanlış veya konuyla ilgisiz olabileceği gibi, veri setleri arasındaki korelasyonları tespit eden algoritma da hatalı olabilir⁹⁸². İlgili kişi, profillemeye ve otomatik karar alma faaliyetleri kapsamında kendisi hakkında yapılan çıkarımların doğru olmadığı ve düzeltilmesi gerektiği iddiasında bulunmak istediğinde, kişisel verilerinin düzeltilmesini talep etmek suretiyle bunu gerçekleştirebilecektir⁹⁸³. Ancak bu hakkın otomatik kararlar için kullanılması pratikte önemli bir sorunla karşı karşıyadır. İlgili kişiye karara etki eden girdi verilerinin hatalı veya eksik olması halinde bunların düzeltilmesini talep hakkı tanınmış olmakla birlikte, veri sorumluları ilgili kişileri kararın hangi verilere dayandığı hususunda bilgilendirmekle yükümlü değildir. Bu durum karardan memnun olmayan ve karara

⁹⁷⁸ Wachter & Mittelstadt & Russell, s.878.

⁹⁷⁹ Bkz. GVK Tüzüğü, m.16.

⁹⁸⁰ Bkz. KVK Kanunu, m.11/f.

⁹⁸¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.17.

⁹⁸² Article 29 Working Party, Automated Individual Decision Making and Profiling, s.17.

⁹⁸³ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.17.

hangi verisinin ne ölçüde etki ettiği konusunda bilgi sahibi olmayan ilgili kişinin, veri yığınlarını incelemek zorunda kalmasına ve böylece ilgili kişinin üzerindeki yükün artmasına neden olmaktadır⁹⁸⁴.

Öte yandan, ilgili kişinin, veri sorumlusunun kendisi hakkındaki yanlış çıkarımları düzeltmesini sağlayabilmesi için öncelikle çıkarımların yanlış olduğunu ispat edebilmesi gerekmektedir. Zira bir kaydın hatalı veya eksik olduğu kanıtlanabildiği ölçüde düzeltilmesi talep edilebilecektir⁹⁸⁵. Kullanılan veriler doğrulanabilir nitelikte olduğunda (örneğin isim, doğum tarihi, medeni durum, gelir gibi) düzeltme hakkının uygulanması kolaydır⁹⁸⁶. Ancak, kişisel verilerin yapay öğrenme algoritmaları ile analiz edilmesi suretiyle “olasılıklara dayalı varsayımlar” dan oluşan çıkarımların üretildiği profillemeye ve otomatik karar alma uygulamaları açısından durum böyle değildir⁹⁸⁷. Bazı çıkarımların ilgili kişi tarafından teyit edilmesi suretiyle doğrulanabilmesi mümkündür. Örneğin, ilgili kişinin çevrimiçi alışveriş alışkanlıklarının izlenmesiyle tahmin edilen eğitim seviyesinin doğru olup olmadığı kendisine sorularak teyit edilebilecektir⁹⁸⁸. Öte yandan bazı çıkarımlar ise doğası itibarıyla sübjektif niteliktedir veya tahmine dayalıdır. Buna bağlı olarak da doğrulanmaları objektif veriler gibi kolay değildir⁹⁸⁹. Kişinin suça eğilimliliğine veya kredi borcunu ödemediği temerrüde düşme ihtimaline ilişkin tahminler bu kapsamdadır⁹⁹⁰.

Çıkarımların doğrulanabilir olup olmamasına ilişkin bu ayrım, kişisel veri tanımı ve kapsamının ne şekilde belirleneceği ile de ilgilidir⁹⁹¹. Nitekim kişisel verilerin kapsamına sadece doğrulanabilir (objektif) verilerin girdiği ve dolayısıyla da düzeltme hakkının sadece doğrulanabilir kişisel veriler (ve çıkarımlar) açısından uygulanabilir olduğunu savunan görüşler olduğu gibi, verinin doğrulanabilir olup

⁹⁸⁴ Wachter & Mittelstadt & Russell, s.878.

⁹⁸⁵ Wachter & Mittelstadt, s.57.

⁹⁸⁶ Wachter & Mittelstadt, s.57.

⁹⁸⁷ Wachter & Mittelstadt, s.57.

⁹⁸⁸ Wachter & Mittelstadt, s.57.

⁹⁸⁹ Wachter & Mittelstadt, s.57.

⁹⁹⁰ Wachter & Mittelstadt, s.57.

⁹⁹¹ Çalışmanın “1.3.3.2. Profillemeye ve Otomatik Karar Alma Uygulamaları İle Edinilen Çıkarımların Hukuki Niteliği” başlıklı bölümü için bkz. s.37.

olmamasının ilgili kişi açısından etkisini belirlemede bir etkiye sahip olmadığından bahisle düzeltme hakkının doğrulanabilir olmayan (sübjektif) veriler (ve çıkarımlar) açısından da uygulanabilir olması gerektiğini savunan görüşler de bulunmaktadır⁹⁹².

3.3.5. İlgili Kişinin Kişisel Verilerinin Silinmesini Talep Etme Hakkı

“Unutulma hakkı” (“*right to be forgotten*”) olarak da ifade edilen, ilgili kişinin “kişisel verilerinin silinmesini talep etme hakkı” (“*right to erasure*”) uyarınca, ilgili kişi, GVK Tüzüğü m.17 tahtında veri sorumlusundan kendisi ile ilgili kişisel verilerin gecikmeksizin silinmesini talep edebilir⁹⁹³. Kişisel verilerin silinmesini talep etme hakkı, KVK Kanunu’nun 7. ve 11. maddelerinde düzenlenmiştir. KVK Kanunu’na tabi işleme faaliyetlerinde, ilgili kişi, kişisel verilerinin işlenmesini gerektiren sebepler ortadan kalktığında, veri sorumlusundan kişisel verilerinin “silinmesini talep etme”; silme gerçekleşikten sonra ise veri sorumlusundan “kişisel verilerinin aktarıldığı üçüncü kişilere bu hususun bildirilmesini isteme” haklarına sahiptir⁹⁹⁴.

Kişisel verilerin silinmesini talep etme hakkı sınırsız nitelikte bir hak değildir. GVK Tüzüğü m.17 tahtında ilgili kişi, kişisel verilerin toplanma veya işlenme amacı için artık gerekli olmaması, ilgili kişinin kişisel verilerinin işlenmesi için verdiği izni geri alması, kişisel verilerin hukuka aykırı şekilde işlenmiş olması, Avrupa Birliği veya üye devlet mevzuatı gereği verilerin silinmesinin zorunlu olması, ilgili kişinin GVK Tüzüğü’nün 21. maddesinin birinci veya ikinci fıkrası uyarınca işleme faaliyetine itirazda bulunması ve veri sorumlusunun kişisel verilerin işlenmesi için ağır basan bir hukuka uygunluk sebebinin bulunmaması hallerinden biri gerçekleştiği takdirde kişisel verilerinin silinmesini talep

⁹⁹² Wachter & Mittelstadt, s.57-58.

⁹⁹³ Bkz. GVK Tüzüğü, m.17/1.

⁹⁹⁴ Bkz. KVK Kanunu, m.11/e, m.11/f. Silmenin nasıl gerçekleşeceğine ilişkin usul ve esaslar, 1 Ocak 2018 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik’te düzenlenmiştir. İlgili Yönetmelik için bkz. <https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm>.

edebilmektedir⁹⁹⁵. Bu hallerden birinin gerçekleştiği durumlarda, veri sorumlusu ilgili kişinin talep etmesi halinde kişisel verilerini gecikmeksizin silmekle yükümlüdür.

29. Madde Veri Çalışma Grubu'nun ilgili rehberinde, ilgili kişinin gerek GVK Tüzüğü'nün 16. maddesinde düzenlenen kişisel verilerinin düzeltilmesini talep etme hakkının, gerekse Tüzüğün 17. maddesinde düzenlenen kişisel verilerin silinmesi hakkının, hem profillemeye faaliyetlerindeki girdi olarak işlenen veriler hem de profillemeye sonucunda ulaşılan çıkarımlar açısından uygulanabilir olduğu belirtilmektedir⁹⁹⁶. Buna göre, ilgili kişi profilinin çıkarılmasında kullanılan ve bizzat kendisi tarafından sağlanan kişisel verilerinin yanı sıra, profillemeye faaliyeti kapsamında kendisi hakkında yapılan gözlemler sonucunda ulaşılan varsayım ve tahmine dayalı çıkarımların da düzeltilmesini ve/veya silinmesini talep edebilecektir⁹⁹⁷. Bu bağlamda silme hakkının, ilgili kişi açısından kabul edilmeyen, doğru bulunmayan, memnun olunmayan çıkarımlar açısından bir “hukuki çare” işlevine sahip olduğu söylenebilecektir⁹⁹⁸.

Edwards ve Veale, yapay öğrenme algoritmaları ile gerçekleştirilen işleme faaliyetleri bakımından, ilgili kişinin kişisel verilerinin silinmesini talep edebileceği en az 3 temel durum olduğunu belirtmiştir. Buna göre, ilgili kişi, (i) kişisel verilerinin artık veri sorumlusunda bulunmasını istemediği için veri sorumlusundan verilerini silmesini, (ii) bir yapay öğrenme modeli aracılığı ile kendisi hakkında yapılan çıkarımlardan memnun olmadığı için verilerinin bu modelden silinmesini, (iii) yapay öğrenme modelinin tamamının veya belli yönlerinin silinmesini talep edebilir⁹⁹⁹. Edwards ve Veale, ilgili kişinin kişisel verilerinin artık veri sorumlusunda bulunmasını istemediği için silinmesini talep etme hakkının çıkarılan veriler veya çıkarımlar için de uygulanabilir olup olmadığını da incelemiştir. Buna

⁹⁹⁵ Bkz. GVK Tüzüğü, m.17/1.

⁹⁹⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.18.

⁹⁹⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.18.

⁹⁹⁸ Wachter & Mittelstadt, s.59.

⁹⁹⁹ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.68-71.

göre, 29.Madde Çalışma Grubu’nun veri taşınabilirliği hakkına ilişkin rehberinde benimsenen çıkarımların ilgili kişiye değil çıkarımı oluşturan sisteme ait olduğu yaklaşımı, kişisel verilerin silinmesini talep hakkı açısından da benimsenebilecektir¹⁰⁰⁰. Edvards ve Veale, Tüzük m.17 tahtında düzenlenen kişisel verilerin silinmesini talep hakkı ile Tüzük m.20 tahtında düzenlenen veri taşınabilirliği hakkının bu bağlamda birbirini tamamlayan düzenlemeler olduğundan bahisle iki hak arasında bir ilişki kurarak, silme hakkının, tıpkı veri taşınabilirliği hakkı gibi çıkarımlar açısından uygulanabilir olmadığını ileri sürmüştür¹⁰⁰¹. Wachter ve Mittelstadt ise, Tüzüğün 20. maddesinde açıkça, veri taşınabilirliği hakkının kullanılmasının, silme hakkının kullanılmasına bir etkisinin olmayacağı hüküm altına alındığından bahisle, iki hak arasında iddia edildiği şekilde bir “tamamlayıcı ilişki” nin varlığının şüpheli olduğu görüşündedir¹⁰⁰².

Öte yandan, veri sorumlusunun çıkarılan verilerin üretilmesi aşamasında yaptığı masraflar sebebiyle sahip olduğu menfaatin ilgili kişinin kişisel verilerinin silinmesini talep hakkına üstün gelebileceğini savunan görüşler mevcuttur¹⁰⁰³. Benzer şekilde, kişisel verilerin veri sorumlusunun iş geliştirme veya ticari kazancı için gerekli olması halinde meşru menfaat iddiasına dayanılarak silme talebinin reddedilebileceğini savunan görüşler de bulunmaktadır¹⁰⁰⁴. Wachter ve Mittelstadt ise, bu görüşlere atıfta bulunarak, ilgili kişinin kişisel verilerin silinmesi talebinin ticari menfaat ve finansal maliyet gerekçeleriyle reddedilmesinin, işleme faaliyetlerin çoğunda bu gerekçelere dayanılmasına yol açarak hakkı işlevsiz hale getireceğini vurgulamıştır¹⁰⁰⁵. Zira Edvards ve Veale’nin silme hakkının çıkarımlar açısından uygulanabilir olmadığını ileri süren görüşü ile birlikte ele alındığında, ilgili kişinin sadece kendisinin sağladığı kişisel verilerin, veri sorumlusunun ticari çıkarları ile çatışmaması şartıyla, silinmesini talep edebileceği sonucu ortaya

¹⁰⁰⁰ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.69.

¹⁰⁰¹ Edvards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.69.

¹⁰⁰² Wachter & Mittelstadt, s.63.

¹⁰⁰³ Wachter & Mittelstadt, s.63.

¹⁰⁰⁴ Wachter & Mittelstadt, s.62.

¹⁰⁰⁵ Wachter & Mittelstadt, s.63.

çıkılmaktadır¹⁰⁰⁶. Öte yandan, profillemeye ve otomatik karar alma faaliyetleri açısından değerlendirilecek olursa, bu görüşün benimsenmesi, veri analitiği faaliyetlerinin maliyeti göz önüne alındığında, ilgili kişi tarafından sağlanan verilerin silinmesine kıyasla çıkarılan verilerin (çıkarımların) silinmesini sağlamayı daha da zor bir hale getirecektir¹⁰⁰⁷.

Wachter ve Mittelstadt, ilgili kişinin kendisi hakkındaki çıkarılan verilerin silinmesini talep etmesi halinde, bu verilerin üçüncü kişiler ile paylaşılmış olması halinde ne yapılacağı sorununa değinmiştir¹⁰⁰⁸. Buna göre, çıkarılan veriler silinse dahi, bunlar daha önceden üçüncü kişilerle paylaşılmış olabilir. Veri sorumluları, verilerin paylaşıldığı üçüncü kişileri silme işlemi ile ilgili bilgilendirme konusunda sınırlı yükümlülüklerle sahiptir. GVK Tüzüğü'nün 19. maddesi uyarınca veri sorumlusu, imkânsız olmaması veya aşırı bir çaba gerektirmemesi halinde silme işlemini kişisel verilerin açıklandığı her bir üçüncü kişiye bildirmekle yükümlüdür¹⁰⁰⁹. Yine, GVK Tüzüğü'nün 17. maddesinin ikinci fıkrasında, veri sorumlusunun, kişisel verileri kamuya açık hale getirdiği ve kişisel verileri silmek zorunda olduğu hallerde, ilgili kişinin silinmesini talep ettiği kişisel verileri işleyen veri sorumlularını bu verilerin silinmesi hususunda bilgilendirmek üzere teknik tedbirler de dahil olmak üzere makul adımları atmakla yükümlü olduğu belirtilmektedir¹⁰¹⁰. Profiller ve çıkarımlar rutin olarak kamuya açıklanmadığından, GVK Tüzüğü'nün 17/2 maddesinin çıkarımlara uygulanması olası değildir¹⁰¹¹. Öte yandan her iki düzenleme kapsamında da çıkarımlar bir veri sorumlusu tarafından silinse dahi, çıkarımların paylaşıldığı üçüncü kişilerce kullanılmaya devam edebileceğinden, bu üçüncü kişilerin tespit edilerek bunlara karşı silme talebinde bulunulması ilgili kişinin yükümlülüğünde olacaktır¹⁰¹². Ancak ilgili kişinin bilgilendirilmesi ve erişim hakkının düzenlendiği GVK Tüzüğü'nün 13., 14. ve 15.

¹⁰⁰⁶ Wachter & Mittelstadt, s.63.

¹⁰⁰⁷ Wachter & Mittelstadt, s.63-64.

¹⁰⁰⁸ Wachter & Mittelstadt, s.64.

¹⁰⁰⁹ Bkz. GVK Tüzüğü, m.19.

¹⁰¹⁰ Bkz. GVK Tüzüğü, m.17/2.

¹⁰¹¹ Wachter & Mittelstadt, s.64.

¹⁰¹² Wachter & Mittelstadt, s.64.

maddelerinin, veri sorumlusuna, sadece kişisel verilerinin paylaşıldığı veya paylaşılacağı alıcı kategorilerini açıklama yükümlülüğü getirdiği göz önüne alındığında, ilgili kişinin kişisel verilerinin açıklandığı üçüncü kişileri tespit edebilmesi kolay olmayabilecektir¹⁰¹³.

Kaltheuner ve Bietti, silme ve düzeltme talep etme haklarının uygulama kapsamının belirlenmesine rehberlik edecek daha fazla bilgiye ihtiyaç bulunduğu görüşündedir¹⁰¹⁴. Diğer bir ifadeyle, bu maddelerin, ihlallerin şeffaf olmadığı ve tespit edilmesinin zor olduğu yapay öğrenme algoritmaları ile gerçekleşen otomatik karar alma faaliyetlerine nasıl uygulanacağı hususunda daha fazla açıklamaya ihtiyaç vardır¹⁰¹⁵. Özellikle de ilgili kişinin bilgilendirilme ve açıklama talep etme haklarının nasıl güçlendirileceği ve ilgili kişinin kişisel verilerinin silinmesini ve düzeltilmesini talep etme hakları ile nasıl ilişkilendirileceği konusunda açık bir rehber ihtiyacı bulunmaktadır¹⁰¹⁶.

3.3.6. İlgili Kişinin İşlemeyi Kısıtlama Hakkı

GVK Tüzüğü'nün 18. maddesinde ilgili kişinin “işlemeyi kısıtlama hakkı” (*“right to restriction of processing”*) düzenlenmiştir¹⁰¹⁷. Tüzüğün “Tanımlar” bölümünde, işlemenin kısıtlanması, “saklanan kişisel verilerin gelecekte işlenmesini sınırlamak amacıyla işaretlenmesi” olarak tanımlanmıştır¹⁰¹⁸. Bu madde uyarınca ilgili kişi, “ (a) kişisel verilerinin doğruluğuna itiraz etmesi halinde, veri sorumlusunun kişisel verilerin doğruluğunu ispat etmesine imkan tanıyacak bir süre boyunca; (b) işleme faaliyetinin hukuka aykırı olması ve ilgili kişinin kişisel verilerin silinmesine karşı gelmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi halinde; (c) veri sorumlusunun işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak ilgili

¹⁰¹³ Wachter & Mittelstadt, s.64.

¹⁰¹⁴ Kaltheuner & Bietti, s.16.

¹⁰¹⁵ Kaltheuner & Bietti, s.16.

¹⁰¹⁶ Kaltheuner & Bietti, s.16.

¹⁰¹⁷ Bkz. GVK Tüzüğü, m.18.

¹⁰¹⁸ Bkz. GVK Tüzüğü, m.4/(3).

kişinin hukuki iddialarda bulunması, bu iddiaların uygulanması veya savunulması amacıyla bu verilere ihtiyaç duyması halinde; (d) ilgili kişinin GVK Tüzüğü'nün 21/1 maddesi uyarınca işleme faaliyetine itiraz etmesi halinde veri sorumlusunun hukuka uygunluk sebeplerinin ilgili kişinin hukuka uygunluk sebeplerine üstün gelip gelmediği doğrulanana kadar", veri sorumlusundan işleme faaliyetinin kısıtlanmasını talep edebilecektir.

İlgili kişinin veri işleme faaliyetini kısıtlama hakkı, bir tarafta ilgili kişinin kişisel verilerinin düzeltilmesi veya silinmesindeki menfaati ile diğer tarafta veri sorumlusunun söz konusu kişisel verileri işlemeye devam etmekteki menfaatinin çatıştığı noktada, silme veya düzeltme gerekçelerinin bulunup bulunmadığının doğrulanmasının gerektiği veya veri sorumlusu ile ilgili kişi arasında ihtilafa neden olduğu durumlarda, bu çatışan menfaatlerin dengelenmesini sağlamaktadır¹⁰¹⁹. Bu hak, ilgili kişiye, veri sorumlusunun kişisel verilerini kullanma şekline kısıtlama getirebilme yetkisi veren, kişisel verilerin silinmesini talep etme hakkına alternatif bir hak olarak kabul edilmektedir. İlgili kişi, veri sorumlusunun tuttuğu kişisel verilerinin içeriği veya verilerinin nasıl işlendiği ile ilgili sebeplere dayanarak ve çoğunlukla da sadece belirli bir süre için işleme faaliyetinin kısıtlanmasını talep edebilecektir¹⁰²⁰.

29. Madde Veri Çalışma Grubu'nun ilgili rehberinde, profillemeye sürecinin her aşamasında ilgili kişinin kişisel verilerinin işlenmesinin kısıtlanmasını talep etme hakkına sahip olduğu belirtilmektedir¹⁰²¹. Bu bağlamda, profillemeye faaliyetinin herhangi bir aşamasında, yukarıda sayılan hallerden birinin geçerli olduğu durumda ilgili kişi veri sorumlusundan işleme faaliyetinin kısıtlanmasını talep edebilecektir.

¹⁰¹⁹ Voigt & Von Dem Bussche, s.424.

¹⁰²⁰ Information Commissioner's Office, Right to the General Data Protection Regulation, s.128.

¹⁰²¹ Article 29 Working Party, Automated Decision Making and Profiling, s.18.

3.3.7. İlgili Kişinin Veri Taşınabilirliği Hakkı

“Veri taşınabilirliği hakkı” (*“right to data portability”*), kişisel verilerin korunması hukukunda ilk kez GVK Tüzüğü’nün 20. maddesinde düzenlenerek açıkça bir hak olarak kabul edilmiştir¹⁰²². Bu düzenleme uyarınca ilgili kişi, veri sorumlusundan kişisel verilerinin yapılandırılmış ve makinalar tarafından okunabilir bir biçimde kendisine verilmesini veya üçüncü bir veri sorumlusuna taşınmasını talep etme hakkına sahiptir.

Edwards ve Veale, veri taşınabilirliği hakkının, GVK Tüzüğü’nün 17. maddesinde düzenlenen ilgili kişinin kişisel verilerinin silinmesini talep etme hakkına, kavramsal anlamda, “kardeş hak” olduğunu belirtmiştir. Buna göre, ilgili kişi teorik olarak, kişisel verilerinin bir internet sitesinden silinmesini talep ederken aynı zamanda verilerinin kendisine ait bir yazılım sistemine taşınmasını talep edebilecektir¹⁰²³.

Bu hakkın Avrupa Birliği içinde serbest veri akışını destekleyeceği, rekabeti teşvik edeceği ileri sürülmektedir¹⁰²⁴. Diğer yandan, bu düzenleme ile ilgili kişiye kişisel verileri üzerinde kontrol imkanı sağlayarak ilgili kişinin veri sorumlusu karşısındaki konumunun güçlendirilmesini amaçladığı belirtilmektedir¹⁰²⁵. Zira ilgili kişi, veri sorumlusundan kişisel verilerini alabildiği takdirde, kendisiyle ilgili çıkarımlardan da haberdar olacak ve bunların doğruluğunu kontrol edebilecektir¹⁰²⁶.

¹⁰²² Bkz. GVK Tüzüğü, m.20.

¹⁰²³ Edwards & Veale, *Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for*, s.72.

¹⁰²⁴ Article 29 Working Party, *Data Portability*, s.3; European Data Protection Supervisor, *Opinion 7/2015, Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, 19 Kasım 2015, https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf, s.13.

¹⁰²⁵ Küzeci, s. 223; Article 29 Working Party, *Data Portability*, s.4.

¹⁰²⁶ Edwards & Veale, *Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for*, s.74.

Belirtilmelidir ki, GVK Tüzüğü'nün 20/1 maddesi uyarınca ilgili kişi, sadece kendi rızasıyla sağladığı kişisel veriler bakımından veri taşınabilirliği hakkından faydalanabilecektir¹⁰²⁷. Dolayısıyla, meşru menfaat veya başkaca bir hukuka uygunluk sebebine dayanılarak gerçekleştirilen profillemeye veya işleme faaliyeti açısından bu hak uygulanabilir değildir¹⁰²⁸. Ayrıca, bu hak sadece otomatik araçlarla gerçekleştirilen veri işleme faaliyetleri bakımından uygulanabilmektedir¹⁰²⁹. Bu bağlamda, veri taşınabilirliği hakkının Tüzük m.22 tahtında düzenlenen profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetlerinden ziyade, bu maddenin dışında kalan otomatik karar alma faaliyetleri açısından daha uygulanabilir bir hak olduğu söylenebilecektir¹⁰³⁰.

Çıkarılan verilerin GVK Tüzüğü'nün 20. maddesi kapsamında olup olmadığı hususunda bir fikir birliği bulunmamaktadır¹⁰³¹. 29. Madde Çalışma Grubu, veri taşınabilirliğine ilişkin rehberinde, “ilgili kişi tarafından sağlanan verileri” iki kategori altında gruplandırmıştır¹⁰³². Bu gruplandırmaya göre, ilgili kişinin bizzat veri sorumlusuna sağladığı telefon numarası, adres bilgisi, kimlik bilgileri gibi kişisel verileri ile ilgili kişinin bir hizmet ya da cihazı kullanmak suretiyle veri sorumlusuna sağladığı kendisi hakkındaki “gözlemlenen veriler” ilgili kişi tarafından sağlanan veriler olarak kabul edilir. Gözlemlenen veriler, kişinin internetteki arama geçmişi, konum bilgisi, internet trafik verisini içermektedir. Çıkarılan veri ise, kişinin kendisi tarafından sağlanan verilerin aksine, kişinin kendisi tarafından sağlanan verilerin analizi ile ulaşılan yeni verileri ifade etmektedir¹⁰³³. Bu bağlamda, kişi hakkında oluşturulan kredi puanı veya kara

¹⁰²⁷ Bkz. GVK Tüzüğü, m.20/1.

¹⁰²⁸ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.74.

¹⁰²⁹ Bkz. GVK Tüzüğü, m.20/1 (b).

¹⁰³⁰ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.74.

¹⁰³¹ Edwards & Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably not the Remedy You Are Looking for, s.73.

¹⁰³² Article 29 Working Party, Data Portability, s.10.

¹⁰³³ Article 29 Working Party, Data Portability, s.10.

paranın aklanması mevzuatına uyum sağlanması amacıyla, kişinin finansal verilerinin analiz edilmesi suretiyle oluşturulan profili, kişinin kendisi tarafından sağlanan bir kişisel veri olarak kabul edilmeyecektir¹⁰³⁴. Her ne kadar kişinin profili de kişinin kendisi tarafından sağlanan verilerin analiz edilmesiyle gerçekleştirilen bir çıkarımdan ibaret olsa da çıkarılan veriler, tipik şekilde kişinin kendisi tarafından sağlanan veriler kategorisinde kabul edilemeyeceğinden, veri taşınabilirliği hakkının da uygulama alanına dahil olmayacaktır¹⁰³⁵.

3.3.8. İlgili Kişinin İtiraz Hakkı

GVK Tüzüğü'nün 21. maddesinde, ilgili kişinin veri işleme faaliyetine “itiraz etme hakkı” (“*right to object*”) düzenlenmiştir¹⁰³⁶. Maddenin birinci fıkrası uyarınca ilgili kişi, kendi özel durumuna ilişkin gerekçeleri ileri sürerek, kişisel verilerinin işlenmesine (profillemeye de dahil olmak üzere) itiraz edebilme hakkına sahiptir¹⁰³⁷. Belirtilmelidir ki, bu düzenleme ilgili kişiye koşulsuz bir itiraz hakkı tanımamaktadır. İlgili kişinin itirazının kabul edilebilmesi için, ilgili kişinin “özel durumuna ilişkin gerekçelerinin” bulunması şart koşulmuştur. 29. Madde Çalışma Grubu ilgili rehberinde, veri sorumlusunun işleme faaliyetindeki menfaatleri ile ilgili kişinin itiraz gerekçeleri arasında her zaman dengeleyici bir uygulama olması gerektiği belirtilmiştir¹⁰³⁸. Buna göre, ilgili kişinin itiraz hakkının doğru olmadığı, ilgili kişinin “özel durumuna ilişkin gerekçeleri” ile veri sorumlusunun kişisel verilerin işlenmesine ilişkin meşru hakları ve menfaatleri arasında bir denge testi (*balance test*) yapılarak, hangi tarafın menfaatlerinin ağır bastığına göre tespit edilmelidir¹⁰³⁹.

GVK Tüzüğü'nün 21.maddesinin lafzından, ilgili kişinin itirazının reddedilmesi için veri sorumlusunun varlığını ispatlaması gereken meşru menfaat

¹⁰³⁴ Article 29 Working Party, Data Portability, s.10.

¹⁰³⁵ Article 29 Working Party, Data Portability, s.10.

¹⁰³⁶ Bkz. GVK Tüzüğü, m.21. KVK Kanunu'nda, GVK Tüzüğü'nde yer verilen kapsamda bir itiraz hakkı düzenlenmemiştir.

¹⁰³⁷ Bkz. GVK Tüzüğü, m. 21/1, GVK Tüzüğü, Giriş Bölümü, 69. Paragraf.

¹⁰³⁸ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.19.

¹⁰³⁹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.19.

kriteri olarak, GVK Tüzüğü'nün 6/1(f) maddesinde veri sorumlusunun kişisel verilerin işlenmesinde hukuka uygunluk sebebi olarak aranan meşru menfaatine göre daha yüksek bir eşiğin öngörüldüğü anlaşılmaktadır¹⁰⁴⁰. İlgili kişi, kişisel verilerinin işlenmesine itiraz etmesi halinde, veri sorumlusu ancak ilgili kişinin menfaatleri, hakları ve özgürlüklerine üstün gelen “zorlayıcı meşru gerekçelere” (“*compelling legal grounds*”) sahip olduğunu ispat edebilirse, ilgili kişinin itirazını dikkate almayarak işleme faaliyetine devam edebilecektir¹⁰⁴¹. GVK Tüzüğü ile 95/46 Sayılı Direktif'ten farklı olarak, zorlayıcı meşru gerekçeleri ispat yükümlülüğü ilgili kişiye değil, veri sorumlusuna yüklenmiştir¹⁰⁴². Öte yandan, GVK Tüzüğü'nde hangi hallerin “zorlayıcı meşru gerekçe” olarak kabul edileceğine ilişkin bir açıklamaya yer verilmemiştir. Bu nedenle hangi hallerin “zorlayıcı meşru gerekçe” teşkil edeceği belirsizdir¹⁰⁴³. 29. Madde Çalışma Grubu, zorlayıcı meşru gerekçeye örnek olarak, profillemeye veri sorumlusunun ticari çıkarlarından ziyade bulaşıcı hastalıkların yayılımını tahmin etmek gibi toplum için faydalı hallerde başvurulduğu durumları göstermiştir¹⁰⁴⁴. Bu konuda bir belirsizlik bulunmakla birlikte, ilgili kişinin işleme faaliyetinin durdurulmasına yönelik üstün bir menfaatinin bulunması veya rızasını usulüne uygun şekilde geri almış olması halinde, GVK Tüzüğü'nün 17. maddesi uyarınca kişisel verilerinin silinmesini talep edebileceği kabul edilmektedir¹⁰⁴⁵.

29. Madde Çalışma Grubu'nun ilgili rehberinde, ilgili kişinin bu hakkını kullanmayı talep ettiğinde, veri sorumlusunun, profillemenin işleme faaliyetinin amacı açısından önemini ve profillemenin ilgili kişinin menfaatleri, hakları ve özgürlükleri üzerindeki etkisini (bu amaca ulaşmak için gerekli olan minimum ile sınırlı olacak şekilde) göz önünde bulundurarak bir dengeleme testi yapması gerektiği belirtilmektedir¹⁰⁴⁶. Veri sorumlusu, ilgili kişinin menfaatleri, hakları ve

¹⁰⁴⁰ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.19.

¹⁰⁴¹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.19.

¹⁰⁴² Bkz. GVK Tüzüğü, m.21/1; GVK Tüzüğü, Giriş Bölümü, 69.Paragraf.

¹⁰⁴³ Wachter & Mittelstadt, s.62.

¹⁰⁴⁴ Working Party, Automated Individual Decision Making and Profiling, s.18.

¹⁰⁴⁴ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.19.

¹⁰⁴⁵ Wachter & Mittelstadt, s.62.

¹⁰⁴⁶ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.18.

özgürlüklerine üstün gelen zorlayıcı meşru gerekçeler sunamadığı takdirde, profillemeye sürecini durdurmalı veya başlatmaktan kaçınmalıdır¹⁰⁴⁷.

GVK Tüzüğü'nün 21.maddesinin ikinci fıkrasında ilgili kişiye, kişisel verilerinin profillemeye de içeren doğrudan pazarlama amacıyla işlenmesine itiraz hakkı tanınmıştır¹⁰⁴⁸. Maddenin ilk fıkrasında düzenlenen itiraz hakkının aksine, doğrudan pazarlamaya itiraz hakkı herhangi bir şarta tabi değildir. Diğer bir ifadeyle, ilgili kişi kişisel verilerinin işlenmesine itiraz ettiği takdirde, menfaatlerin dengelenmesine gerek olmaksızın, veri sorumlusu itirazın gerekçelerini sorgulamadan ilgili kişinin talebini yerine getirmekle yükümlüdür¹⁰⁴⁹. Nitekim Tüzüğün giriş bölümünün 70. paragrafında bu hakkın her zaman ve bedelsiz olarak kullanılabileceği ifade edilmiştir¹⁰⁵⁰.

3.4. KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDA İLGİLİ DÜZENLEMELER

GVK Tüzüğü'nün ilgili düzenlemeleri, uygulamaya yönelik çeşitli problemler barındırsa da bu düzenlemeler “ilgili kişiyi hukuki veya benzer şekilde önemli derecede etkileyen profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma” faaliyetleri hukuki çerçeveye kavuşturulmuştur. Tüzüğün 22. maddesi ile bu şekilde bir veri işleme faaliyetine izin verilen istisnai haller belirlenmiş ve ilgili kişinin bu kararlara karşı sahip olduğu haklar hüküm altına alınmıştır. KVK Kanunu'nun 11. maddesinin (g) bendindeki düzenleme ile GVK Tüzüğü'nün 22. maddesindeki ilgili kişinin tamamen otomatik işlemeye dayalı kararların konusu olmama hakkı kısmen iç hukukumuzda dahil edilmiştir. İlgili maddeyle ilgili kişiye, “işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhine bir sonucun ortaya çıkmasına itiraz

¹⁰⁴⁷ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.18.

¹⁰⁴⁸ Bkz. GVK Tüzüğü, m.21/2.

¹⁰⁴⁹ Article 29 Working Party, Automated Individual Decision Making and Profiling, s.18.

¹⁰⁵⁰ Bkz. GVK Tüzüğü, Giriş Bölümü, 70.Paragraf.

etme” hakkı tanınmıştır¹⁰⁵¹. KVK Kanunu ile GVK Tüzüğü’ndeki ilgili düzenlemeler arasındaki farklar aşağıda sırayla incelenmiştir.

İlk olarak, GVK Tüzüğü’nün 22. maddesindeki “profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma” ifadesinden farklı olarak KVK Kanunu’nun 11/g maddesinde profillemeye bir atıfta bulunulmamıştır. Öte yandan, KVK Kanunu’ndaki düzenlemede, otomatik karara itirazda bulunabilmek için “hukuki veya benzer şekilde önemli bir etki” aranmamış, “kişinin aleyhine bir sonuç” ortaya çıkması yeterli kabul edilmiştir. Ayrıca, GVK Tüzüğü’nden farklı olarak maddede herhangi bir istisnai duruma da yer verilmemiştir. Yine, Tüzük’ten farklı olarak, ilgili kişiye sürece insan müdahalesi talep etme, kendi görüşünü beyan etme gibi haklar sağlanacağına ilişkin bir hükme yer verilmemiştir. İlgili kişinin Kanun’un 11/g maddesi tahtında itiraz hakkını kullanılmasının hüküm ve sonuçlarının ne olacağı belirsizdir. Bu bağlamda Kanun’un 11/g maddesi ilgili kişiye profilleme ve otomatik karar alma uygulamaları karşısında yeterli bir koruma sağlamaktan oldukça uzak görünmektedir.

İki düzenleme arasındaki önemli farklardan biri de GVK Tüzüğü’nün, 13., 14. ve 15. maddelerindeki gibi otomatik karar alma faaliyetlerine ilişkin bilgilendirilme ve erişim haklarına KVK Kanunu’nda açıkça yer verilmemesidir. GVK Tüzüğü’ndeki gibi açık bir düzenlemeyle ilgili kişinin bilgilendirilme ve erişim haklarının hukuki çerçeveye kavuşturularak hüküm altına alınması, ilgili kişinin bu haklarının garanti edilmesini sağlayacaktır. Öte yandan, bu hakların açıkça düzenlenmemiş olması ilgili kişinin bu haklardan tamamen yoksun olduğu sonucunu doğurmamalıdır¹⁰⁵². Zira KVK Kanunu’nun 10. maddesinde, veri sorumlusuna kişisel verilerin hangi amaçla işleneceği, kimlere hangi amaçla aktarılabileceği, veri toplama metodu ve hukuki nedenini ilgili kişiye açıklama yükümlülüğü bulunduğu hüküm altına alınmıştır¹⁰⁵³. Kanun’un bu maddesinde

¹⁰⁵¹ Bkz. KVK Kanunu, m.11/g.

¹⁰⁵² Aşıkoglu, s.50.

¹⁰⁵³ Aşıkoglu, s.50.

profilleme ve otomatik işlemeye dayalı karar alma ile ilgili açık bir bilgilendirme yükümlülüğüne yer verilmemişse de, ilgili kişinin “profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma” faaliyeti gerçekleştirilmeden önce, “profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar almanın varlığı” ve “kişisel verilerinin bu kapsamda işlenmesinin muhtemel etki ve sonuçları” hakkında bilgilendirilmesi, veri sorumlusunun aydınlatma yükümlülüğünü dürüstlük kuralına uygun şekilde yerine getirebilmesi açısından önemlidir¹⁰⁵⁴.

GVK Tüzüğü’nün 14. maddesinin ikinci fıkrasında, veri sorumlusunun adil ve şeffaf bir veri işleme için, maddenin birinci fıkrasında sayılan bilgilere ek olarak ilgili kişiye sağlamakla yükümlü olduğu bilgiler sıralanmıştır¹⁰⁵⁵. Tüzük m. 14/2 (f) uyarınca veri sorumlusu, ilgili kişinin verilerinin elde edildiği kaynağı ve kamuya açık kaynaklardan edinilip edinilmediğini ilgili kişiye açıklamakla yükümlüdür¹⁰⁵⁶. Öte yandan, Tüzüğün giriş bölümünün 61. paragrafında, verilerin elde edildiği kaynakların çok çeşitli olduğu ve doğrudan belirtilemediği hallerde genel bilgilerin sağlanması gerektiği belirtilmiştir¹⁰⁵⁷. KVK Kanunu’nda ise veri sorumlusunun aydınlatma yükümlülüğüne, verilerin elde edildiği kaynakların da dahil olduğuna ilişkin açık bir düzenlemeye yer verilmemiştir¹⁰⁵⁸. Özellikle profilleme ve otomatik karar alma faaliyetleri kapsamında kullanılan büyük veri uygulamalarındaki veri kaynaklarının çeşitliliği göz önüne alındığında, ilgili kişinin kişisel verilerinin hangi kaynaklardan edinildiğini bilmesi, veri işleme faaliyetinin şeffaf ve kontrol edilebilir olması açısından son derece önemlidir¹⁰⁵⁹. Bu bağlamda, KVK Kanunu’nda bu hususta özel bir düzenleme bulunmamakla birlikte, veri sorumluları

¹⁰⁵⁴ Aşıkoğlu, s.49.

¹⁰⁵⁵ Bkz. GVK Tüzüğü, m.14/2.

¹⁰⁵⁶ Bkz. GVK Tüzüğü, m.14/2 (f).

¹⁰⁵⁷ Bkz. GVK Tüzüğü, Giriş Bölümü, 61.Paragraf.

¹⁰⁵⁸ Aşıkoğlu, s.51.

¹⁰⁵⁹ Irmak ERDOĞAN, “Otomatik Karar Çağında Hukuk: Avrupa Birliği ve Türkiye’de Karşılaştırmalı Profilleme Düzenlemeleri”, Gelişen Teknolojiler ve Hukuk II : Yapay Zeka, On İki Levha Yayıncılık A.Ş., 1. Baskı, İstanbul, Nisan 2021, s.384.

ilgili kişiyi aydınlatma yükümlülükleri uyarınca işledikleri kişisel verilerin kaynaklarını tespit edebilmeli ve ilgili kişiyi bilgilendirmelidir¹⁰⁶⁰.

Kanaatimizce, gerek KVK Kanunu’nun Tüzük ile uyumlaştırılma ihtiyacı gereği, gerek KVK Kanunu’nun uygulama alanına giren profillemeye ve otomatik karar alma faaliyetleri kapsamında ilgili kişinin hak ve menfaatlerinin güvence altına alınabilmesi için, Kanun’un yeterli bir koruma öngörmeyen 11/g maddesi yerine daha detaylı ve açık bir hükme yer verilmelidir. Bu bağlamda, Kanun’un “Tanımlar” başlıklı maddesinde “Profillemeye” tanımı yapılması, otomatik karar almaya ilişkin olarak Tüzük m.22 ile paralel bir hüküm eklenmesi ve aydınlatma yükümlülüğünün kapsamının profillemeye ve otomatik karar alma faaliyetleri açısından genişletilmesi yerinde olacaktır. Kanun’un aydınlatma yükümlülüğüne ilişkin mevcut düzenlemeleri kapsamında veri sorumlusunun ilgili kişiyi profillemeye ve otomatik karar alma faaliyetlerine ilişkin olarak aydınlatması gerektiği açıktır. Ancak fiili durumda aydınlatma metinlerinde sadece işleme amacı kapsamında “profillemeye” ye atıf yapılmakta ve ilgili kişinin m.11/g kapsamında “İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme” hakkına sahip olduğu belirtilmektedir. Bu durum, ilgili kişiden profillemeye ve otomatik karar alma faaliyetleri açısından alınan rızanın “bilgilendirmeye dayanan” bir “açık rıza” olup olmadığı konusunda soru işaretlerine neden olmaktadır. Dolayısıyla, aydınlatma yükümlülüğünün bu hususta açık bir düzenlemeyle “otomatik işlemeye dayalı karar almanın varlığı ve söz konusu işleme faaliyetinin ilgili kişi açısından önemi ve öngörülen sonuçları”nı içerek şekilde genişletilmesi, aydınlatma metinlerinin mevcut durumdaki sınırlı kapsamının dışına çıkılarak hukuki amacına hizmet etmesi açısından faydalı olacaktır.

¹⁰⁶⁰ Erdoğan, s.384.

Belirtilen kapsamda,

- Kanun'un "Tanımlar" başlıklı 3.maddesine (ğ) bendi olarak "Profilleme" tanımı eklenmelidir:

"ğ) Profilleme: kimliği belirli veya belirlenebilir bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere ilgili kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel veriler üzerinde gerçekleştirilen her türlü otomatik işleme faaliyetini,"

- Kanun'un 11/g maddesi çıkartılarak "Otomatik İşlemeye Dayalı Karar Alma" başlığı altında yeni bir madde eklenmelidir¹⁰⁶¹:

"Otomatik İşlemeye Dayalı Karar Alma"

(1) Kişisel veriler, ilgili kişiyi önemli şekilde etkileyen, profilleme içerenler de dahil olmak üzere, anlamlı bir insan müdahalesi bulunmayan ve otomatik işlemeye dayalı olarak gerçekleştirilen karar alma faaliyetleri kapsamında işlenemez.

(2) Otomatik işlemeye dayalı karar alma faaliyetinin, ilgili kişinin açık rızasına dayanması veya kanunlarda açıkça öngörülmesi veya veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması halinde 1.paragraf uygulanmaz.

¹⁰⁶¹ Madde kaleme alınırken, Paul De Hert ve Guillermo Lazcoz tarafından Tüzüğün 22. maddesinin sorunlu yönleri gözetilerek önerilen değişiklik teklifi dikkate alınmıştır. İlgili değişiklik teklifi için bkz. Paul DE HERT & Guillermo LAZCOZ, Radical rewriting of Article 22 GDPR on machine decisions in the AI era, 13 Ekim 2021, European Law Blog.

(3) Veri sorumlusu, ilgili kişiye, karara itiraz etme, kendi görüşünü beyan etme, kararın gerekçesine ilişkin bilgi talep etme, nihai kararın algoritma yerine bir kişi tarafından verilmesini talep etme haklarına sahiptir.

(4) 2. fıkra kapsamındaki otomatik kararlar, Kanun'un 6. maddesinin 3. fıkrasının uygulanabilir olduğu ve Kurul tarafından belirlenen yeterli önlemlerin alındığı haller dışında, özel nitelikli kişisel verilerin işlenmesine dayanamaz.”

- Kanunun “Veri sorumlusunun aydınlatma yükümlülüğü” başlıklı 10. maddesine, (e) bendi olarak aşağıdaki ifade eklenmelidir:

“e) Otomatik işlemeye dayalı karar almanın varlığı ve söz konusu işleme faaliyetinin ilgili kişi açısından önemi ve öngörülen sonuçları”

- Aydınlatma metinlerinde profillemeye ve otomatik karar alma faaliyetlerine ilişkin detaylı açıklamalara yer verilmelidir. Aşağıda örnek olarak banka ve finans kuruluşlarının aydınlatma metinlerinin profillemeye ve otomatik karar alma faaliyetlerine ilişkin asgari olarak içermesi gereken ifadelere yer verilmiştir:

“Size sunabileceğimiz ürün ve hizmetlerle ilgili bazı riskleri belirlemek veya belirli sonuçların ortaya çıkma ihtimalini tahmin edebilmek için kişisel verilerinizi tahmine dayalı veri analiz yöntemleri kullanarak otomatik olarak değerlendirmemiz gerekebilecektir.

Bu kapsamda kişisel bilgileriniz kullanılarak profiliniz çıkarılabilecek, size ürün ve hizmet sağlamaya ilişkin bazı kararlar bu profile dayanılarak otomatik olarak verilebilecektir.

Profillemeye, kişisel verileri kullanarak müşterilerimizi ve onların özel ihtiyaçlarını daha ayrıntılı olarak anlamamıza ve pazarlama süreçlerimizi ve ürün teklifimizi bu çerçevede uyarlamamıza imkan tanıyan bir araçtır.

Bu tür veri işleme örnekleri arasında;

- Kredi/kredi kartı limitlerinin otomatik olarak hesaplanması;
- Kredi taleplerinin kabul veya reddine ilişkin kararların otomatik olarak verilmesi;
- Belirli ürünler için kredi referans kontrollerinin sağlanması;
- Dolandırıcılık ve kara para aklama da dahil olmak üzere mali suçların tespit edilmesi ve önlenmesi veya kredi kartınızın üçüncü bir kişi tarafından kullanılıp kullanılmadığının belirlenmesi amacıyla, müşteri veya hesap etkinliğiyle ilgili risk düzeyinin belirlenmesi yer almaktadır.

Bu kararları nasıl verdiğimiz hakkında belirli hususlarda bilgilendirilme ve nihai kararın yetkili biri tarafından verilmesini talep etme haklarına sahipsiniz. Daha fazla ayrıntıya haklarınızın belirtildiği bölümde ulaşabilirsiniz.”

KVK Kanunu’nun 28. maddesinde, Kanun’un uygulama alanı dışında kalan istisnai haller düzenlenmiştir. İlgili maddenin (ç) bendinde, “kişisel verilerin milli savunma, milli güvenlik, kamu düzeni veya ekonomik güvenlik tesis etmeye yönelik olarak koruyucu ve istihbari faaliyet kapsamında işlenmesi”; (d) bendinde ise, “soruşturma, kovuşturma, yargılama veya infaz işlemlerinin gerçekleştirilmesi amacıyla yargı veya infaz mercileri tarafından işlenmesi” Kanun’un koruma kapsamı dışında bırakılmıştır¹⁰⁶². Belirtilen kapsamda işlenen veriler, KVK Kanunu’nun koruma kapsamı dışında bırakılmış olsa da kamu kurumları, yargı ve infaz mercileri tarafından, 28. maddede belirtilen kapsamda veri işlenmesi, profillemeye ve otomatik karar alma gerçekleştirilmesi halinde, Anayasanın 20. Maddesi ve Avrupa İnsan Hakları Sözleşmesi’nde temel bir hak olarak düzenlenen kişisel verilerin korunmasının gözetilmesi gerekeceği tabiidir¹⁰⁶³. Bu bağlamda, kanunun ilgili maddelerinde belirtilen kapsamda profillemeye ve otomatik karar alma

¹⁰⁶² Bkz. KVK Kanunu, m.28.

¹⁰⁶³ Erdoğan, s.385.

faaliyetleri koruma kapsamı dışında bırakılmış olmakla birlikte, kamu otoritelerinin yetkisinin de sınırsız olmadığı unutulmamalıdır¹⁰⁶⁴. Öte yandan, kişisel verilerin belirtilen kamu kurumlarınca işlenmesine ilişkin münferit bir düzenleme de bulunmamaktadır. Bu alanda profillemeye ve otomatik karar alma faaliyetlerini de içeren detaylı münferit bir düzenleme yapılması, kişisel verilerin korunması hakkı ile kamu düzeni arasındaki dengenin tesis edilmesine önemli katkılar sağlayacaktır¹⁰⁶⁵. Kanaatimizce Kanun'da otomatik karar almaya ilişkin açık bir hüküm eklenmesi halinde, bu hükmün kamu kurumlarına tanınan muafiyetin kapsamını profillemeye ve otomatik karar alma faaliyetleri açısından daraltacak şekilde kaleme alınması değerlendirilebilecektir.

¹⁰⁶⁴ Erdoğan, s.385.

¹⁰⁶⁵ Erdoğan, s.384-485.

SONUÇ

Dijital verilerde ve büyük veri kümelerine erişimi olan işletme sayısındaki artış ile yapay öğrenme algoritmalarındaki gelişmeler, bireysel ve toplumsal hayatı etkileyen konularda algoritmik karar alma faaliyetlerine ivme kazandırmıştır. Algoritmalar, karar almada giderek daha fazla sorumlu hale gelmektedir. Profilleme ve otomatik karar faaliyetlerinde kişisel verilerin opak algoritmalar kullanılarak işlenmesi, ilgili kişiler ile veri sorumluları arasındaki bilgi asimetrisini artırmaktadır. Bu durum bireylerin veri sorumluları konumundaki özel şirketler veya kamu kuruluşları karşısında çaresiz ve güçsüz hissetmelerine neden olmaktadır. Öte yandan, her ne kadar bu sistemler ile alınan kararların isabetliliğinde önemli gelişmeler kat edilmişse de yapay zeka teknikleri kusursuz değildir. Algoritmaların barındırdığı kara kutu problemi, bu sistemler ile ulaşılan çıkarımların neye dayandığının uzmanlar tarafından dahi anlaşılmasını zorlaştırmaktadır. Karar almanın algoritmik sistemler ile gerçekleştirilmesinden beklenen faydalara karşılık, bu uygulamalarının, bireyler açısından ayrımcı ve haksız uygulamalara, bireysel özerklik, bilgilerin geleceğini belirleme hakkının ve seçme hakkının zarar görmesine, toplumun manipüle edilmesine, demokratik toplum temellerinin sarsılmasına neden olduğunu gösteren kayda değer sayıda vaka ortaya çıkmıştır. Bu durum, büyük verinin kamu hizmetleri, özel sektör ve genel olarak toplum için teşkil ettiği potansiyel faydanın, ancak mahremiyet ve kişisel verilerin korumasına ilişkin mekanizmaların benimsenmesi ve etkili bir şekilde uygulanması halinde ortaya çıkacağına yönelik bir farkındalık oluşturmuştur. Algoritmik karar alma sistemlerinin olumsuz etkilerine karşı geliştirilen farkındalık, dünyanın farklı ülkelerinde bu sistemlerin toplum üzerindeki etkilerini izlemeyi, kararların mantığını anlamaya çalışarak kara kutu probleminin etkilerini hafifletmeyi amaçlayan kar amacı gütmeyen inisiyatiflerin oluşmasıyla sonuçlanmıştır. Gerek bu girişimlerin gerekse de denetleyici kamu otoriteleri tarafından hazırlanan, algoritmik sistemlerin etik ve açıklanabilirlik bağlamında sorunlarını ele alan tavsiye niteliğindeki rehber, rapor ve benzeri metinler,

profilleme ve otomatik karar alma faaliyetlerinin şeffaflığı ve hesap verebilirliğinin sağlanmasına yönelik önemli kazanımlar sağlamıştır.

GVK Tüzüğü'nde, algoritmaların doğasından kaynaklanan özelliklerin bireyin mahremiyeti ve diğer hak ve özgürlükleri açısından teşkil ettiği riskler dikkate alınarak, hak temelli bir yaklaşım benimsenmiş, bireylere verileri üzerinde daha fazla kontrol sağlanmasına, veri sorumlularının hesap verebilirliği ve tamamen otomatik işlemeye dayalı karar alma faaliyetlerinin sınırlandırılmasına yönelik düzenlemeler getirilmiştir. Belirtilmelidir ki, kişisel verilerin korunması, büyük veri analitiği açısından sadece hukuki bir gereklilik değildir. Kişisel verilerin korunmasına ilişkin düzenlemeler, büyük veri analitiğinde gerek kamu gerekse özel sektör için kritik bir önem teşkil eden “veri kalitesi” nin sağlanması için de önemli bir araçtır. Ancak gerek kişisel verilerin korunmasına ilişkin genel düzenlemelerin gerekse de profilleme ve otomatik karar vermeye ilişkin özel düzenlemeler hakkında uygulamaya yönelik çeşitli sorunlar söz konusudur.

Kişisel verilerin korunmasına hakim olan ilkelerin, yapay zeka teknikleri kullanılan profilleme ve otomatik karar faaliyetlerine, diğer bir ifadeyle kişisel verilerin büyük veri bağlamında işlenmesine uygulanması birçok açıdan daha zordur. Verinin hacmi, birçok farklı kaynaktan edinilmesi, verinin üretilme şekilleri, verinin edinilme amacından farklı yeni amaçlar için kullanılma ve veri depolama imkanlarındaki gelişmelere bağlı olarak verilerin gerektiğinden uzun süreler saklanması eğilimi, veri sorumlularının işleme sürecinin karmaşıklığı ve opaklığı, algoritmaların hesaplama metodunun olasılıklara dayalı olması ve buna bağlı olarak bireyler açısından beklenmedik sonuçlar üretmesi, kişisel verilerin işlenmesinde gözetilmesi gereken amaçla sınırlılık, veri minimizasyonu, işleme amacı için gerekli olan süre kadar muhafaza edilme, doğru ve gerektiğinde güncel tutulma ilkelerinin uygulanabilirliği ile ilgili sorunları beraberinde getirmiştir. Kişisel verilerin korunmasına hakim olan ilkelerin büyük veri analitiği bakımından uygulanmasındaki sorunların temel nedenleri, şeffaflık ve hesap verebilirlik ilkelerinin kişisel verilerin korunması hukukundaki önemini artırmıştır.

GVK Tüzüğü'ndeki yüksek şeffaflık arayışı, Tüzüğün genel yapılanmasına sirayet etmiştir. Kara kutu problemi gibi teknik engellerin yanı sıra, şirketlerin algoritmaların “ticari sır” olduğu iddiasına dayanabilmeleri de algoritmik şeffaflığın önündeki önemli engellerdir. Ancak bu engellere karşın, mümkün olan en üst seviyede algoritmik şeffaflığa ulaşılması, ilgili kişinin kişisel verilerinin hangi amaçla işlendiği ve kararın dayanağı hakkında bir fikir sahibi olmasını sağlayacaktır. Bu bağlamda algoritmik şeffaflık, kişisel verilerin korunmasının temelindeki bireyin bilgilerinin geleceğini belirleme hakkı ile doğrudan ilişkilidir. Öte yandan, algoritmik şeffaflık, profillemeye ve otomatik karar sistemlerinin belirgin risklerinden biri olan, bireylerin hayatında ayrımcı uygulamalara yol açan önyargıların ortadan kaldırılması açısından etkili bir yaklaşımdır. Önyargıyı tanımak ve belirleyebilmek, onu ortadan kaldırmak ve somut kararı daha adil hale getirmek için önemli bir adımdır. İlgili kişilerin kendileri hakkında algoritmalar ile gerçekleştirilen çıkarımları çürütebilecekleri somut yollar belirlenmesi de şeffaflık arayışına uyumlu bir yaklaşımdır. Yapay öğrenme algoritmalarının önyargılı veya taraflı bir sonuç üretme potansiyelinin bulunup bulunmadığı, çalışma şeklinin amaca uygun, makul ve kabul edilebilir olup olmadığı, son kullanıcılar için yeterince şeffaf olup olmadığının tespit edilmesi gerekliliği algoritmaların denetlenmesine olan ihtiyacı artırmıştır. Bu bağlamda algoritmaların denetimine ilişkin standartlar oluşturulmalı, denetim mekanizmaları ve araçları geliştirilmeli, denetim sürecinde rol alacak kişilerin görev tanımları yapılmalıdır. Başarılı bir algoritma denetimi veri ve bilgisayar bilimlerinin yanı sıra, hukuk, psikoloji, sosyal bilimler, davranışsal ekonomi, insan merkezli tasarım ve etik gibi birçok farklı alanda disiplinler arası bir iş birliğini ve bütüncül bir bakış açısı gerektirmektedir.

Algoritmik şeffaflıkla yakından bağlantılı olan bir diğer ilke ise hesap verebilirliktir. Hesap verebilirlik, işleme faaliyetlerinin veri koruma yasasına ve ilgili yükümlülüklerine uygunluğundan sorumlu olan veri sorumlularının ve veri işleyenlerin, işleme faaliyetlerinin kamuya ve denetleyici otoritelere veri koruma hükümlerine uygunluğunu gösterebilmeleri ve işleme faaliyetlerinde veri

korumasının sağlanması için, proaktif önlemlerin ve yaklaşımların geliştirilmesini ve uygulanmasını gerektirir. Bu çerçevede, profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetleri kapsamında veri sorumlusunun hesap verebilirliği için işleme faaliyetlerinin talep edilmesi halinde denetleyici otoritelere sunulmak üzere kayıt altına alınması, belirli durumlarda, kişisel verilerin korunmasıyla ilgili tüm konulara dahil olan bir veri koruma görevlisi atanması, gerçek kişilerin hak ve özgürlükleri için yüksek risk oluşturması muhtemel işleme türleri için veri koruma etki değerlendirmelerinin yapılması, kişisel verilerin tasarımdan itibaren ve varsayılan olarak korunmasının sağlanması, ilgili kişilerin haklarını etkin şekilde kullanabilmelerini sağlamaya yönelik usul ve prosedürlerin uygulanması, onaylanmış standartlara veya sertifikasyon mekanizmalarına bağlı kalınması gibi yaklaşımların benimsenmesi önemlidir.

GVK Tüzüğü, büyük veri analitiğinin kişisel verilerin korunması açısından barındırdığı sorunları ele alarak bireyin mahremiyet haklarını güçlendirmek amacıyla 95/46 Sayılı Direktif'ten farklı olarak, profillemeye ve otomatik karar faaliyetlerinin sınırlandırılmasına ilişkin özel düzenlemelerin yanı sıra, tasarımdan itibaren ve varsayılan olarak veri koruma ile veri koruma etki değerlendirmesi gibi veri sorumlusuna yeni yükümlülükler getirmiştir. Özellikle tasarımdan itibaren veri koruma ilkesi, profillemeye ve otomatik karar faaliyetlerinin “açıklanabilir”, “şeffaf” ve “adil” olmasını sağlamak adına oldukça önemlidir. Profillemeye ve otomatik karar faaliyetleri bakımından kişisel verilerin tasarımdan itibaren korunması, algoritmaların tasarım aşamasından itibaren veri minimizasyonu, şeffaflık, amaçla sınırlılık, hesap verebilirlik gibi veri koruma ilkelerinin etkili bir şekilde uygulanmasını ve Tüzüğün gerekliliklerinin yerine getirilmesi için gerekli güvencelerin tesis edilmesi amacı ile uygun tedbirlerin alınarak ilgili kişilerin haklarının korunmasını amaçlar. Bu önlemler, girdi verilerinin amaçlanan sonuca ulaşmak için yeterliliğini ve uyumluluğunun kontrol edilmesini, çıkarımların ve bu süreçte uygulanan metotların makul olup olmadığının değerlendirilmesini, haksız ve ayrımcı sonuçlar üretilmediğinden emin olunmasını gerektirir. Bu bağlamda, kişisel verilerin tasarımdan itibaren korunmasının sağlanması için, yapay zeka ve

veri analitiği alanında ciddi bir teknik uzmanlığa ihtiyaç ortaya çıkmaktadır. Bu seviyede bir uzmanlığın tüm sistem geliştiriciler ve tasarımcılardan beklenemeyeceği göz önüne alındığında, tasarımdan itibaren veri koruma ilkesinin yapay zeka alanında hayata geçirilmesi için sistem geliştirici ve tasarımcılarına yönelik rehber ve yönergelerin hazırlanması önem kazanmaktadır. Veri koruma görevlisi de ilk kez Tüzük ile hukuki çerçeveye kavuşturulan yeniliklerden biridir. Profilleme ve otomatik karar faaliyetlerinde bireylerin davranışsal verilerinin toplandığı ve karmaşık modeller kullanılarak analiz edilerek bazı çıkarımlara ulaşıldığı göz önüne alındığında, sürecin uzman ve bağımsız bir üçüncü kişi tarafından incelenmesinin yarattığı fayda önem arz etmektedir. Öte yandan GVK Tüzüğü'nde yapay zeka ve büyük veri analitiğindeki gelişmeler gözetilerek buna yönelik düzenlemeler getirilmişse de, ilgili madde hükümlerinin boşluklar içermeleri ve farklı şekillerde yorumlanabilmelerine yol açan şekilde kaleme alınmış olmaları sebebiyle, veri sorumluları için rehber ve yönergeler hazırlanmasına ihtiyaç olduğu yönünde görüşler beyan edilmektedir.

Tüzüğün ilgili kişinin bilgilendirilme hakkına ilişkin 13. ve 14.maddeleri ile erişim hakkına ilişkin 15.maddesi, şeffaflık ilkesinin ilgili kişinin hakları bağlamında bir görünümünü teşkil eden düzenlemelerdir. Özellikle ilgili kişinin “Tüzüğün 22.maddesi kapsamında profilleme de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetinin varlığı, yürütülen mantığa ilişki anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin ilgili kişi açısından önemli ve öngörülen sonuçları” hakkında bilgilendirilme hakkı ve bunlara erişim hakkı, algoritmik şeffaflığa ve açıklanabilirliğe atfedilen önemi göstermektedir. Otomatik karar alma sistemleri, açıklanabilir olduğu ölçüde güvenilirlik kazanacaklardır. Ancak bu düzenlemelerin ilgili kişiye bir “açıklama talep etme hakkı” (*right to an explanation*) sağlayıp sağlamadığı konusunda farklı görüşler bulunmaktadır. Açıklama hakkı, özellikle yapay öğrenme algoritmaların kullanıldığı tamamen otomatik işlemeye dayalı ve kişinin hayatında hukuki veya benzer şekilde önemli bir etkiye sahip kararların gerekçesinin açıklanmasını talep etme hakkını ifade eder. Tüzüğün tamamen otomatik işlemeye dayalı karar almaya

ilişkin 22.maddesinde açık bir şekilde açıklama hakkına ilişkin bir ifadeye yer verilmemiştir. Tüzüğün taslağında bu hususta bir atıf bulunmakla birlikte yasalaşma sürecinde çıkarıldığı bilinmektedir. Tüzüğün 22. maddesinin gerekçesini teşkil eden 71.paragrafta açıklama hakkına atıf yapılmış ise de böyle bir düzenlemeye Tüzüğün bağlayıcı nitelikteki 22.maddesinde yer verilmesi tercih edilmemişken bağlayıcı olmayan gerekçelere eklenmesi, kanun koyucunun iradesinin ilgili kişiye bağlayıcı bir açıklama hakkı sağlamak olmadığı yönünde eleştirilere neden olmuştur. Öte yandan, belirtilen düzenlemelerin ilgili kişiye açıklama hakkı sağladığı kabul edilse dahi, hakkın kapsamı ciddi şekilde sınırlı olacaktır. Zira sadece, “hukuki veya benzer şekilde önemli etkiye sahip” ve “tamamen otomatik işlemeye dayalı” kararlar açısından uygulama alanı bulacaktır. Tüzüğün 13/2(f),14/2(g) ve 15/1(h) maddelerinin ilgili kişiye açıklama hakkı sağlayıp sağlamadığına ilişkin tartışmalar, ilgili maddelerinin lafzı itibariyle, açıklamanın ne zaman yapılacağı noktasında yoğunlaşmıştır. Bir kısım görüşe göre, ilgili kişinin profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetinin varlığı, karar sürecinin mantığı ve öngörülen sonuçları hakkında bilgilendirilme hakkına ilişkin 13/2(f) ve 14/2(g) maddeleri sadece karar verilmeden önce (*ex ante*) karar sisteminin genel anlamda işlevselliği, mantığı, öngörülen sonuçlarına ilişkin bir açıklama yapılması imkanı tanımaktadır. Karşıt görüşe göre ise, bu maddeler ilgili kişiye karar verildikten sonra (*ex post*) ilgili kararın gerekçesi, nedenleri ve karara etki eden bireysel koşullara ilişkin bir açıklama hakkı sağlamaktadır. Öte yandan, bilgilendirme hakkını düzenleyen 13. ve 14. maddeleri yerine, erişim hakkına ilişkin 15.maddesinin, ilgili kişiye karar verildikten sonra açıklama hakkı sağladığının kabul edilebileceğini savunan görüşler bulunmaktadır. Karşıt görüşe göre ise, 15.maddenin lafzı 13.ve 14.maddeler ile birebir aynı olduğundan, erişim hakkının sağladığı açıklama hakkının kapsamı da bilgilendirilme hakkının sağladığı açıklama hakkının kapsamından farklı olmayacaktır. Çalışmanın ilgili bölümünde incelendiği üzere 2021 yılında Amsterdam Bölge Mahkemesi tarafından ilk kez açıklama hakkına atıf yapan bir karar verilmiştir. Bununla birlikte, önüne gelen uyuşmazlıklarda GVK Tüzüğü’nün ilgili hükümlerini yorumlarken Tüzüğün ilgili kişiye bir açıklama

hakkı tanıyıp tanımadığı konusunda nihai değerlendirmeyi AB Adalet Divanı yapacaktır.

Tüzüğün ilgili kişinin profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar almanın konusu olmama hakkının düzenlendiği 22.maddesinin lafzı itibariyle veri sorumlusuna yüklenen bir yasak olarak mı yoksa ilgili kişinin bir hakkı olarak mı yorumlanması gerektiği konusunda farklı görüşler oluşmuştur. 22.madde ile ilgili kişiye tanınan hakkın, veri sorumlularının uymak zorunda olduğu tamamen otomatik işlemeye dayalı karar verme yasağı olarak yorumlanması ve uygulanması halinde ilgili kişinin hak ve çıkarlarının daha fazla korunacağı açıktır. Maddenin uygulama alanı bulabilmesi için otomatik kararın hiçbir suretle insan müdahalesi içermeksizin münferiden otomatik işlemeye dayalı olarak verilmesi gerekir. Öte yandan, işleme faaliyetini 22.maddenin kapsamı dışına çıkarmak amacıyla insan müdahalesi varmış gibi bir izlenim yaratılmasının önüne geçilmesi amacıyla bu müdahalenin, şekli bir incelemeden ziyade “anlamlı” bir inceleme ve değerlendirme olmasının gerekmektedir. Bu bağlamda, kararın incelenmesi ve değerlendirilmesi, karara etki eden tüm verileri inceleyerek karara müdahale etmek suretiyle kararı değiştirebilme yetki ve becerisine sahip biri tarafından gerçekleştirilmelidir. İlgili kişinin, Tüzüğün tamamen otomatik işlemeye dayalı karar almaya ilişkin 22. madde ile kendisine tanınan korumadan faydalanabilmesi için, söz konusu kararın hukuki ya da benzer şekilde önemli bir etki doğurması gerekmektedir. Hukuki etki doğuran kararların neler olabileceği açıkça tespit edilebilmekteyken, hukuki etkiye benzer şekilde önemli etki doğuran kararların neler olduğunu kesin şekilde belirlemek zordur. Kredi veya iş başvurusuna ilişkin kararlar, sağlık ve eğitim hizmetlerine erişimi etkileyen kararlar gibi kişinin meşru menfaatinin bulunduğu kabul edilebileceği hallerin “hukuki etkiye benzer şekilde önemli” etki doğurduğu kabul edilmektedir. Tüzüğün 22. maddesinin bu açıdan açıklığa kavuşturulması, en azından “önemli etki” nin ilgili kişinin öznel bakış açısından mı yoksa bazı objektif standartlara göre mi belirleneceğinin tanımlanması yararlı olacaktır. Zira bu hususun açıklığa kavuşturulmaması, hukuki etkiye benzer şekilde önemli bir etki doğurduğu bariz

bir şekilde açık olmayan otomatik karar alma faaliyetlerinin Tüzük m.22'nin kapsamı dışında kalmasına neden olabilecektir. Nitekim tamamen otomatik işlemeye dayalı karar alma içeren çevrimiçi davranışsal reklamcılık faaliyetleri karşısında ilgili kişinin Tüzük m.22 ile tanınan korumadan faydalanıp faydalanamayacağı konusunda farklı görüşler bulunmaktadır. Davranışsal reklamların “hukuki etkiye benzer şekilde önemli” etki doğurduğundan bahisle 22.maddenin uygulama kapsamında olduğunu ileri süren görüşler bulunduğu gibi, davranışsal reklamcılık faaliyetlerinin hangi hallerde ilgili kişi üzerinde önemli etkiler doğurduğunun belirlenmesinin neredeyse imkansız olduğu yönünde görüşler de mevcuttur.

95/46 Sayılı Direktif'in tamamen otomatik işlemeye dayalı karar almaya ilişkin 15. maddesinden farklı olarak, GVK Tüzüğü m.22 ile veri sorumlusuna, ilgili kişiye, otomatik karar sürecine insan müdahalesi talep etme, karara ilişkin kendi görüş ve bakış açısını beyan etme ve ilgili karara itiraz etme hakkı tanıma yükümlülüğü getirilmiştir. Bu güvenceler, tamamen otomatik işlemeye dayalı karar alma faaliyetlerinin olumsuz etkileri karşısında bireyin hak ve menfaatlerinin korunması ve şeffaflık ilkesinin tesis edilmesi açısından önemli olmakla birlikte uygulamaya yönelik belirsizlikleri de beraberinde getirmiştir. Karar sürecine insan müdahalesinin, kararı değiştirebilme yetkinliğinde bir kişi tarafından gerçekleştirilmesi ve bu kişi tarafından ilgili kişinin sağladığı tüm ek bilgiler de dahil olmak üzere otomatik karar verme faaliyetine esas alınan tüm verilerin kapsamlı şekilde değerlendirilmesi gerekir. İlgili kişinin kendi görüşünü beyan etmesinin hukuki sonuçlarının ne olacağına ilişkin bir düzenlemeye yer verilmemiştir. Tüzük'te bu konuda bir boşluk söz konusudur. İtiraz hakkının nasıl kullanılacağı ise, güvencelerin düzenlendiği maddenin (m.22/3) nasıl yorumlandığına göre farklılık arz edecektir. Zira Tüzüğün 22.maddesi, ilgili maddede belirtilen güvencelerin hepsine birlikte başvurulması gerektiği şeklinde yorumlanabileceği gibi, bunlara ayrı ayrı başvurulmasına izin verecek şekilde de yorumlanabilmektedir.

İlgili kiři ve veri sorumlusu arasında bir sözleşmenin kurulması veya ifası için gerekli olması Tüzük m.22 kapsamındaki tamamen otomatik işlemeye dayalı karar alma açısından hukuka uygunluk sebebi olarak kabul edilmiştir. “Gereklilik” kıstasının ölçüsünün ne olacağı ile ilgili farklı görüşler bulunmakla birlikte, genel olarak, kişinin temel hak ve özgürlüklerine daha hafif bir müdahale ile veya hiç müdahale edilmeden de aynı sonuca ulaşılmasını mümkün kılan etkili bir yöntem mevcut ise, bu durumda işleme faaliyetinin “gerekli olmadığı” sonucuna varılabilecektir. Bu bağlamda, özellikle tamamen otomatik işlemeye dayalı karar alma faaliyetinin bir sözleşmenin kurulması veya ifası için mutlaka gerekli olduğunun tespiti ve ispatının çoğunlukla kolay olmadığı, bu durumların oldukça istisnai olduğu kabul edilmektedir. Öte yandan ilgili kişinin açık rızasına dayanılması halinde ilgili kiři hakkında profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar almaya izin verilmektedir. Ancak usulüne uygun bir açık rıza alınmasının önünde bazı engeller mevcuttur. Profillemeye ve otomatik karar faaliyetlerinde kullanılan algoritmaların çalışma şeklinin şeffaf olmaması ve verilerin hangi amaçla işleneceğinin ilk edinilme anında belirsiz olması sebebiyle verilerin toplanma anında ilgili kişinin açık ve net bir şekilde bilgilendirilmesi tam anlamıyla mümkün olmamaktadır. Veri sorumlularının bilgilendirme yükümlülüklerini yerine getirmek için başvurdukları gizlilik bildirimleri ise amacına hizmet etmemektedir. Bu bildirimlerin kullanıcılar tarafından çoğunlukla okunmadığı, okunsa dahi teknik ve karmaşık içeriğı sebebiyle uzman olmayan kişilerce anlaşılmasının zor olduğu bilinmektedir. Açık rıza alınması ile ilgili bir diğer sorun ise, çevrimiçi platformlarda sürekli rızasına başvurulanan kullanıcılarda “rıza yorgunluğu” olarak adlandırılan durumun ortaya çıkmasıdır. Bu durum gerek genel profillemeye ve otomatik karar faaliyetleri gerekse Tüzüğün 22.maddesinde düzenlenen profillemeye de dahil olmak üzere tamamen otomatik işlemeye dayalı karar alma faaliyetleri açısından açık rızanın bilgilendirmeye dayanma, özgür iradeyle verilmiş olma, belirli ve tereddüde yer vermeyecek şekilde açık olma gerekliliklerinin karşılanamamasına neden olmaktadır. Diğer bir ifadeyle, içinde bulunduğumuz büyük veri çağında, artık geleneksel bildirim ve rıza mekanizmaları şeffaflığın sağlanması ve ilgili kişinin verileri üzerinde kontrol sahibi olması için

yeterli işleve sahip değildir. Açıklanan sebeplere bağlı olarak, profillemeye ve otomatik karar verme faaliyetlerinin hukuka ve dürüstlük kurallarına uygun şekilde gerçekleştirilebilmesine ilişkin belirsizlikler söz konusudur.

KVK Kanunu’nun 11/g maddesi ile ilgili kişiye, “kişisel verilerin tamamen otomatik sistemler ile analiz edilmesi suretiyle kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme” hakkı tanınarak, Tüzüğün 22. maddesi oldukça sınırlı bir şekilde iç hukuka dahil edilmiştir. Ancak ilgili kişinin bu hakkını kullanmak istemesi halinde itirazın hüküm ve sonuçlarının ne olacağı belli değildir. Öte yandan gerek bu maddenin sınırlı kapsamı gerekse de Tüzük’teki gibi tamamen otomatik işlemeye dayalı karar alma faaliyetlerine ilişkin ilgili kişiye bilgilendirilme ve erişim haklarının tanınmamış olması sebebiyle, KVK Kanunu ilgili kişilere münhasıran otomatik işlemeye dayalı karar alma faaliyetleri karşısında yeterli bir koruma sağlamaktan uzaktır. Veri sorumlusu aydınlatma yükümlülüğü gereği, ilgili kişiyi profillemeye ve otomatik karar alma amacı ve Kanun’un 11/g maddesi kapsamında böyle bir karara itiraz hakkı bulunduğu ile ilgili bilgilendirmekle yükümlü ise de kanaatimizce bu kapsamda bir bilgilendirme şeffaflık ve hesap verebilirlik ilkesinin gerekliliklerini karşılamakta yetersiz kalmaktadır. Tamamen otomatik işlemeye dayalı karar alma faaliyetlerinin gerektirdiği üstün koruma göz önüne alınarak, veri sorumlusunun dayanabileceği hukuka uygunluk sebeplerinin de sınırlandırılması ve bu sebeplerden birine dayanılsa dahi veri sorumlusunun ilgili kişiye, sürece insan müdahalesi talep etme, kendi görüşünü beyan etme gibi haklar sağlamakla yükümlü tutulması faydalı olacaktır.

6098 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girdikten kısa bir süre sonra Genel Veri Koruma Tüzüğü Avrupa Birliği Parlamentosu’nda kabul edilmiştir. KVK Kanunu’nun lafzında ve düzenlemelerinde, GVK Tüzüğü’nden önce yürürlükte olan 95/46 Sayılı Direktif esas alındığından, her ne kadar KVK Kanunu ile GVK Tüzüğü arasında oldukça fazla benzerlik olsa da bu aşamada tam anlamıyla bir uyumluluktan bahsedilebilmesi mümkün değildir. Özellikle büyük veri uygulamaları bakımından uygulama alanına sahip olan profillemeye ve tamamen

otomatik işlemeye dayalı karar vermeye ilişkin özel hükümlerin yanı sıra, hesap verebilirlik, veri koruma etki analizi, veri koruma görevlisi, tasarımdan itibaren ve varsayılan ayarlarla veri koruma ilkelerine ilişkin düzenlemeler, GVK Tüzüğü'nün KVK Kanunu'ndan ayrıldığı önemli noktaları teşkil etmektedir. Belirtmek gerekir ki, 95/46 Sayılı Direktif'e dayanılarak oluşturulan KVK Kanunu ile kişisel verilerin korunması alanında yüksek standartların benimsendiği bir ülke olunması için önemli bir adım atılmış ve Kanun'un yürürlüğe girdiği günden bu zamana oldukça değerli kazanımlar edinilmiştir. Öte yandan kişisel verilerin korunmasına ilişkin küresel ölçekte bir hukuki çerçeve oluşturan GVK Tüzüğü ile kıyaslandığında, Kanun'un birçok yönden sınırlı olduğu bilinmektedir. Türkiye ile Avrupa Birliği'nin siyasi ve ticari ilişkilerinin yanı sıra, Türkiye Büyük Millet Meclisi tarafından 18.07.2019 tarihinde onaylanan 2019-2023 yıllarına ilişkin 11. Kalkınma Planı'nın hedefleri arasında "6698 sayılı Kişisel Verilerin Korunması Kanunu'nun AB'nin Genel Veri Koruma Tüzüğü dikkate alınarak güncellenmesi" nin de yer aldığı göz önüne alındığında, sistematik bir şekilde hedefler konularak Kanun'un Tüzüğe tam uyumlu hale getirilmesi gerektiği sonucu doğmaktadır. Kanun'un Tüzük ile uyumlu hale getirilmesi, Türkiye'nin de Avrupa Birliği ile ticari ilişki içindeki diğer ülkeler gibi "yeterli koruma düzeyine sahip ülke" olarak tanınması için kaçınılmazdır. Bugüne kadar özellikle ticari faaliyetlerle ilgili hukuki düzenlemelerde Avrupa Birliği Hukuku ile uyumun yakalanmasına gayret edilmiştir. Kişisel verilerin korunması bağlamında da iç hukukun Avrupa Birliği standartları ile uyumlu hale getirilmesi, her geçen gün daha da dijitalleşen bir dünyada, Avrupa Birliği ile ekonomik ilişkilerin ve Türkiye'nin küresel ekonomik düzende arzu edilen seviyeye ulaşması açısından göz ardı edilemeyecek öneme sahiptir. Kanun'un profillemeye ve otomatik karar alma faaliyetleri bağlamında Tüzüğe nasıl uyumlaştırılacağı konusunda ise, Tüzüğün ilgili düzenlemeleri ile ilgili süregelen tartışmaların ve çözüm önerilerinin yanı sıra ilgili kurum ve kuruluşların rehber ve raporlarının dikkate alınması gerekecektir. Bu bağlamda çalışmamızda, kişisel verilerin korunmasına hakim olan ilkeler, ilgili kişinin hakları, hukuka uygunluk sebepleri, GVK Tüzüğü'ndeki profillemeye ve otomatik karar vermeye ilişkin özel düzenlemeler, profillemeye ve otomatik karar verme

uygulamaları açısından ilgili düzenlemelerin uygulanabilirliğine ilişkin sorunlar ve tartışmalar da ele alınarak incelenmiş, profillemeye ve otomatik karar alma faaliyetleri açısından KVK Kanunu'nun eksikliklerine ve Tüzük düzenlemelerinin uygulanabilirliğine ilişkin sorunlara ışık tutulması amaçlanmıştır.

Kişisel Verilerin Korunması Kanunu'nda, çalışmamızda önerdiğimiz gibi profillemeye ve otomatik karar alma faaliyetlerine ilişkin açık düzenlemeler yapılması halinde, otomatik karar alma faaliyetlerine ilişkin bireyin hakları ve veri sorumlularının yükümlülükleri hukuki bir çerçeveye oturtulacaktır. Böylece profillemeye ve otomatik karar alma faaliyetlerine karşı toplumsal bilincin ve farkındalığın yaratılması açısından önemli bir adım atılmış olacaktır. Zira Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesini takiben, Kanun'un uygulamasına ilişkin tartışmaların gündeme gelmesi, şirket ve kamu kurum ve kuruluşlarının uyum çalışmaları yürütmesi, konuya ilişkin akademik çalışmaların yapılması, Kurum rehberlerinin yayınlanması ve farkındalık eğitimleri verilmesi, veri koruma kültürünün ve veri koruma bilincinin oluşturulması adına önemli katkılar sağlamıştır. Kanun'un Genel Veri Koruma Tüzüğü ile profillemeye ve otomatik karar alma uygulamaları bağlamında uyumlaştırılmasının da en önemli faydalarından biri, toplumda uyandıracak farkındalık olacaktır. Uyumlaştırma ile birlikte, algoritmik karar sistemlerinin olumsuz etkilerine ilişkin kamusal, bireysel ve kurumsal ölçekte farkındalık eğitimleri verilmesi, özellikle de çocuklarda ve gençlerde bu farkındalığın yaratılmaya başlanması önem teşkil etmektedir. Toplumsal bilincin artırılmasında, otomatik karar alma sistemlerinin olumsuz etkilerini izlemek, araştırmak, analiz etmek ve kişisel verilerin korunmasını savunma amacıyla kurulmuş farklı disiplinlerden uzmanların yer aldığı bağımsız inisiyatiflerin, sivil toplum örgütlerinin ve araştırma enstitülerinin etkisi göz ardı edilmemelidir. Avrupa ve Birleşik Krallık'ta gerek bu tür girişim ve inisiyatiflerin yanı sıra denetleyici kamu otoriteleri tarafından hazırlanan, algoritmik sistemlerinin kişisel verilerin korunması bağlamında olumsuz etkilerini ve çözüm önerilerini ele alan tavsiye niteliğindeki rehber, rapor ve benzeri çalışmalar ile önemli kazanımlar sağlanmıştır. Ülkemizde de bu şekilde oluşumların teşvik edilmesi, Kurum'un da

profilleme ve otomatik karar alma faaliyetleri alanındaki çalışmalarını genişletmesi gerekmektedir.

Hızla dijitalleşen dünyamızda hukuki düzenlemelerin tek başına yeterli olmadığı unutulmamalı, yetişmiş insan gücünün önemi göz ardı edilmemelidir. Nitekim, kişisel verilerin korunması hukuk ve uyum departmanlarının yanı sıra veri analitiği, bilgisayar bilimleri, veri bilimi, pazarlama, müşteri ilişkileri yönetimi gibi farklı alanlarda çalışan kişilerin de görev alanına girmektedir. İlgili alanlardaki çalışanların profilleme ve otomatik karar alma uygulamalarının kişisel verilerin korunması açısından barındırdığı risk faktörlerine ilişkin yüksek bir farkındalığa sahip olmaları gerekir. Bunun yanı sıra bu kişilerin, anonimleştirme, veri koruma etki değerlendirmesi, tasarımdan itibaren gizlilik gibi tedbir ve yaklaşımları etkili şekilde uygulayabilecek yeterlilikte donanıma sahip olmaları gerekir. Bu bağlamda, kişisel verilerin korunmasına ilişkin kapsamlı bir ders kataloğunun ilgili yüksek öğretim bölümlerinde müfredata dahil edilmesi önemli bir adım olacaktır.

KAYNAKÇA

ACQUISTI, A., & GROSS, R. (2006, June), *Imagined Communities: Awareness, Information Sharing, and Privacy on The Facebook*. In International Workshop on Privacy Enhancing Technologies (p.36-58). Berlin, Springer.

AGRAWAL, S., & AGRAWAL, J. (2015), Survey on Anomaly Detection Using Data Mining Techniques. *Procedia Computer Science*, 60, 708-713.

AKSOY-RETORNAZ, E., & GÜÇLÜTÜRK, O.G. (2021), *Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi*. Gelişen Teknolojiler ve Hukuk II: Yapay Zeka (Editörler: E. Eylem Aksoy Retornaz/Osman Gazi Güçlütürk), İstanbul, On İki Levha.

ALLEN, M. (2018), Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates. <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>.

ALMEIDA, F. L. (2017), Benefits, Challenges and Tools of Big Data Management. *Journal of Systems Integration*, 8(4), 12.

ALPAYDIN, E. (2020), *Introduction To Machine Learning*. MIT press. Massaschusetts, Cambridge.

ALPAYDIN, E. (2020), *Yapay Öğrenme: Yeni Yapay Zekâ*. (Çeviri: Aylin Ağar), 1.Baskı, İstanbul, Tellekt Yayınları.

ANGWIN, J., LARSON, J., MATTU, S., & KIRCHNER, L. (2016), *Machine Bias*. In *Ethics of Data and Analytics* (p.254-264). Auerbach Publications. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

BAŞALP, N. (2015), Avrupa Birliği veri koruması genel regülasyonu'nun temel yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21(1), 77-106.

BAYAMLIOĞLU, E. (2018), Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097653.

BERBER, L. K., ATABEY, A., & EREN, E. (2020), *E-Privacy Report: Lessons learned from the European Experience & Reflections for e-Privacy Laws in Turkey*. Istanbul Bilgi University IT Law Institute, Istanbul.

BIEGA, A. J., & FINCK, M. (2021), Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. *Technology and Regulation*, 44-61.

BINDRA, C. (2021), *Building A Privacy-First Future For Web Advertising*. Ads & Commerce Blog. <https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/>.

BIRNBAUM, E. (2020), *The DOJ Sues Google for Monopoly Practices- and Says There's More to Come*. <https://www.protocol.com/google-justice-department-lawsuit-antitrust>.

BRKAN, M. (2019), Do Algorithms Rule The World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond. *International Journal of Law and Information Technology*, 27(2), 91-121.

BROWNLEE, J. (2021), *What is Semi-Supervised Learning*. <https://machinelearningmastery.com/what-is-semi-supervised-learning/>.

BURRELL, J. (2016), How The Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms. *Big Data & Society*, 3(1), 1-2.

BÜYÜKÖZKAN-FEYZİOĞLU, G. (2021), *Dijitalleşen Dünyada Yapay Zeka”, Gelişen Teknolojiler ve Hukuk II: Yapay Zeka*. (Editörler: Eylem Aksoy Retornaz, Osman Gazi Güçlütürk), 1. Baskı, İstanbul, On İki Levha.

CAIN-MILLER, C (2015), *Algorithms and Bias: Q. and A.* With Cynthia Dwork, NY Times <https://www.nytimes.com/201508/11/upshot/algorithms-and-bias-q-and-a-with-cynthia-dwork.html>.

CANPOLAT, Y.K. (2019), *Privacy by Design- Şirketlerin Rekabet Avantajı Yaratması İçin Yeni Formül.* <https://medium.com/canpolat-legal/privacy-by-design-%C5%9Firketlerin-rekabet-avantaj%C4%B1-yaratmas%C4%B1-i%C3%A7in-yeni-form%C3%BCI-99cfe0133aa1>.

CAPLAN, R., & DONOVAN, J., & HANSON, L., & MATTHEWS, J. (2018), Algorithmic Accountability: A Primer, *Data & Society*, https://datasociety.net/wp-content/uploads/2019/09/DandS_Algorithmic_Accountability.pdf.

CASADO, R., & YOUNAS, M. (2015), Emerging Trends and Technologies in Big Data Processing. *Concurrency and Computation: Practice and Experience*, 27(8), 2078-2091.

CAVOUKIAN, A., & JONAS, J. (2012), *Privacy by Design in the Age of Big Data.* <https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf>.

CAVOUKIAN, A. (2009), *Privacy by Design: The 7 foundational principles.* <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

CELIS, L.E., MEHROTRA, A., & VISHNOI, N. K. (2019), Toward Controlling Discrimination in Online Ad Auctions. *ICML*.

COFFMAN, E., GALAMBOS, J., MARTELLO, S., & VIGO, D. (2018), *Guide Software Development with Data Protection by Design and by Default.* <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true>.

COLONNA, L. (2016), *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices*. Faculty of Law, Stockholm University Research Paper No. 5.

CUSTERS, B. (2001), *Data Mining and Group Profiling on the Internet*. In: Vedder A (red.) *Ethics and the Internet*. Antwerpen, Intersentia, 87-104.

CUSTERS, B. (2018), *Profiling as Inferred Data. Amplifier Effects and Positive Feedback Loops*. Being Profiled: Cogitas Ergo Sum 10 Years of Profiling the European Citizen (Eds: Emre Bayramlioğlu, Irina Baraluic, Liisa Janssens, Mireille Hildebrandt), Amsterdam University Press.

CUSTERS, B. H., & SCHERMER, B. W. (2014), *Responsibly Innovating Data Mining and Profiling Tools: A New Approach to Discrimination Sensitive and Privacy Sensitive Attributes*. In Responsible Innovation 1 (Eds: J. Van den Hoven & Others), Springer, Dordrecht.

CUSTERS, B., & VRABEC, H.U. (2016), Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection. *International Data Privacy Law*, 6(1), 4-15.

ÇEKİN, M.S. (2008), *6698 Sayılı Kişisel Verilerin Korunması Kanunu*. Yayıncılık, 1.Baskı, İstanbul, On İki Levha.

DANKS, D., & LONDON, A. J. (2017), Algorithmic Bias in Autonomous Systems. Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17), 4691-4697.

DATTA, A., TSCHANTZ, M. C., & DATTA, A. (2015), *Automated Experiments On Ad Privacy Settings A Tale of Opacity, Choice, and Discrimination*. <https://arxiv.org/abs/1408.6491>.

DE HERT, P.& LAZCOZ G. (2021). Radical rewriting of Article 22 GDPR on machine decisions in the AI era. *European Law Blog*. <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/>.

DELACROIX, S., & VEALE, M. (2020), *Smart Technologies and Our Sense of Self: Going Beyond Epistemic Counter-Profiling*. In *Life And The Law In The Era of Data-Driven Agency*. (Eds: Mireille Hildebrandt & Kieron O'Hara), Edward Elgar Publishing.

DIAKOPOULOS, N., FRIEDLER, S., ARENAS, M., BAROCAS, S., HAY, M., HOWE, B., & ZEVENBERGEN, B. (2016), Principles for Accountable Algorithms and a Social Impact Statement for Algorithms. *FAT/ML*. <https://www.fatml.org/resources/principles-for-accountable-algorithms>.

DOMINGOS, P. (2019), *Master Algoritma- Yapay Öğrenme Hayatımızı Nasıl Değiştirecek?* İstanbul, Paloma Yayınları.

DÜLGER, M.V. (2019), *Kişisel Verilerin Korunması Hukuku*. 1. Baskı, İstanbul, Hukuk Akademisi.

EDWARDS, L., & VEALE, M. (2017), Slave to the Algorithm: Why a Right to an Explanation is Probably not the Remedy you are Looking for. *Duke Law & Technology Review*, Vol.16.

ERDOĞAN, I. (2021), *Otomatik Karar Çağında Hukuk: Avrupa Birliği ve Türkiye’de Karşılaştırmalı Profilleme Düzenlemeleri*. Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ, 1. Baskı, İstanbul, On İki Levha Yayıncılık.

FERRARIS, V., BOSCO, F., CAFIERO, G., D'ANGELO, E., & SULOYEVA, Y. (2013), *Defining profiling*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366564.

FLORIDI, L. (2016), On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, 29(4), 307-312.

FORGÓ, N., HÄNOLD, S., & SCHÜTZE, B. (2017), *The Principle of Purpose Limitation and Big Data*. In *New Technology, Big Data and The Law* (pp. 68). Singapore: Springer.

GANDOMI, A., & HAIDER, M. (2015), Beyond The Hype: Big Data Concepts, Methods, and Analytics. *International Journal of Information Management*, 35(2), 137-144.

GELLERT, R., VAN BEKKUM, M., & ZUIDERVEEN-BORGESIOUS, F. (2021), *The Ola & Uber Judgments: For the First Time a Court Recognises a GDPR Right to an Explanation for Algorithmic Decision-Making*. <http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html>.

GIANGIACOMO, O. (2020), The Market's View: Interview with Andrea d'Agostino on How Digital Advertising Players are Creating a New Era in the TV Market. <https://www.dentons.com/en/insights/articles/2020/may/4/how-digital-advertising-players-are-creating-a-new-era-in-the-tv-market>.

GIL GONZÁLEZ, E., & DE HERT, P. (2019, April), Understanding The Legal Provisions That Allow Processing and Profiling of Personal Data—An Analysis of GDPR Provisions and Principles. *In Era Forum*, 19(4), 597-621.

GOEL, V. (2022), Get To Know The New Topic API For Privacy Sandbox, 25 Ocak 2022, <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/>.

GOGGIN, B. (2019), *Inside Facebook's suicide algorithm: Here's how the company uses artificial intelligence to predict your mental state from your posts*. Business Insider. <https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12>.

GOODMAN, B., & FLAXMAN, S. (2017), European Union Regulations on Algorithmic Decision-Making and A “Right to Explanation”. *AI Magazine*, 38(3), 50-57.

GRASSEGGER, H., & KROGERUS, M. (2017), *The data that turned the world upside down*. Vice Motherboard. <https://www.vice.com/en/article/mg9vvv/how-our-likes-helped-trump-win>.

GREEN, B. (2022), The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, Volume 45.

GÜÇLÜTÜRK O.G. & KADIOĞLU, Y.M. (2021), “Yapay Zekâ ve Regülasyon”, *Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ* (Editörler: Eylem Aksoy Retornaz & Osman Gazi Güçlütürk), 1.Baskı, İstanbul, On İki Levha Yayıncılık.

HALLINAN, D., & ZUIDERVEEN-BORGESIOUS, F. (2020), Opinions Can Be Incorrect (In Our Opinion)! On Data Protection Law’s Accuracy Principle. *International Data Privacy Law*, 10(1), 1-10.

HAMILTON, I. A. (2018), Why It’s Totally Unsurprising That Amazon’s Recruitment AI Was Biased Against Women. *Business Insider*, <https://www.businessinsider.com/amazon-ai-biased-against-women-no-surprise-sandra-wachter-2018-10>.

HARDESTY, L. (2018), Study Finds Gender and Skin-Type Bias in Commercial Artificial-İntelligence Systems. <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>.

HARIRI, R. H., FREDERICKS, E. M., & BOWERS, K. M. (2019), Uncertainty in Big Data Analytics: Survey, Opportunities, and Challenges. *Journal of Big Data*, 6(1), 1-16.

HÄUSELMANN, A. N. (2018), *Profiling and the GDPR: Harmonised Confusion*.12 février 2018.

https://jusletter.weblaw.ch/fr/dam/publicationsystem/articles/jusletter/2018/924/profiling-in-the-gdp_3b8e8a124f/Jusletter_profiling-in-the-gdp_3b8e8a124f_fr.pdf.

HILDEBRANDT, M. (2006), Profiling: From Data to Knowledge. *Datenschutz und Datensicherheit-DuD*, 30(9), 548-552.

HILDEBRANDT, M. (2008), *Defining Profiling: A New Type of Knowledge*. Profiling The European Citizen. (Eds: Mireille Hildebrandt & Serge Gutwirth), Dordrecht, Springer.

HILDEBRANDT, M. (2019), 10. ‘Legal by Design’ or ‘Legal Protection by Design’?, *Law for Computer Scientists*, <https://lawforcomputerscientists.pubpub.org/pub/gfzd6k0g/release/12>.

HILDEBRANT, M. (2018), Primitives of Legal Protection In The Era of Data-Driven Platforms. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3140594.

KALTHEUNER, F., & BIETTI, E. (2018), Data is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in The GDPR. *Journal of Information Rights, Policy and Practice*, 2(2).

KAMA-IŞIK, S. (2018), *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış*, 1. Baskı, İstanbul, On İki Levha Yayıncılık.

KAYA, M. B. (2020), Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi. *İstanbul Hukuk Mecmuası*, 78(4), 1859-1897.

KAYA, M.B. (2020), *Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge, Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, (Editörler: Leyla Keser Berber & Ali Cem Bilgili), 1.Baskı, İstanbul, Oniki Levha Yayıncılık.

KELLEHER, J.D., & TIERNEY, B. (2020), *Veri Bilimi*. (Çeviri: Onur Öztürk), 1. Baskı, İstanbul, Tellekt.

KESER-BERBER, L. (2014), *Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması*. İstanbul, On İki Levha Yayıncılık.

KIM, L. (2021), Ridiculously Powerful Facebook Ad Targeting Strategies. Retrieved from Word Stream. <https://www.wordstream.com/blog/ws/2015/01/28/facebook-ad-targeting>.

KITCHENS, B., JOHNSON, S. L., & GRAY, P. (2020), Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption. *MIS Quarterly*, 44(4). 1619-1649.

KOÇ, O., & KASAP, M. (2018), *Daha İyi Bir Dünya İçin Yapay Zekâ*. İstanbul, Doğan Kitap Yayıncılık.

KON, G. Does anyone read privacy notices? Linklaters. <https://www.linklaters.com/en/insights/blogs/digilinks/does-anyone-read-privacy-notices-the-facts>.

KORFF, D. (2010), New Challenges to Data Protection Study-Country Report: France. *European Commission DG Justice, Freedom and Security Report*.

KORFF, D. (2010), New Challenges to Data Protection Study-Country Report: United Kingdom. *European Commission DG Justice, Freedom and Security Report*.

KORFF, D. (2010), New Challenges to Data Protection Study-Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments. *European Commission DG Justice, Freedom and Security Report*.

KÜZECİ, E. (2019), *Kişisel Verilerin Korunması*. Ankara, Turhan Kitabevi.

LAMMERANT, H., & DE HERT, P. (2016), Predictive profiling and its legal limits: Effectiveness gone forever. *Exploring The Boundaries of Big Data* (Eds. Van

der Sloom, D. Broeders, & E. Schriivers), Vol.32, 145-173, Amsterdam University Press/WRR.

LEE, N. T., RESNICK, P., & BARTON, G. (2019), *Algorithmic Bias Detection and Mitigation: Best Practices and Policies To Reduce Consumer Harms*. Brookings. <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>.

LOVELACE, A., & DATAKIND, U. K. (2020), *Examining The Black Box: Tools For Assessing Algorithmic Systems*. Technical Report, AdaLovelace Institute, 8-14, <https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/>.

LUBARSKY, B. (2017), Re-identification of “anonymized” data. Georgetown Law Technology Review. *Georgia Law Technology Review*, 211. <https://perma.cc/86RR-JUFT>.

MALGIERI, G., & COMANDÉ, G. (2017), Why a Right to Legibility of Automated Decision-Making Exists in The General Data Protection Regulation. *International Data Privacy Law*, 7(4), 243-265.

MARR, B. (2017), *What is the Difference Between Data Mining and Machine Learning?*, <https://www.discoverdatascience.org/articles/data-mining-vs-machine-learning/>.

MARR, B. (2019), *Büyük Veri İşbaşında 45 Yıldız Şirket Büyük Veriyi Nasıl Kullandı?* (Çeviren: Başak Gündüz), İstanbul, MediaCat Kitapları.

MATZ, S. C., KOSINSKI, M., NAVE, G., & STILLWELL, D. J. (2017), Psychological Targeting as an Effective Approach to Digital Mass Persuasion. *Proceedings of The National Academy of Sciences*, 114(48), 12714-12719.

MAYER-SCHÖNBERGER, V., & CUKIER, K. (2013), *Büyük Veri: Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim*. İstanbul, Paloma Yayınevi.

MAYER-SCHÖNBERGER, V., & PADOVA, Y. (2015), Regime Change: Enabling Big Data Through Europe's New Data Protection Regulation. *Columbia Science & Technology Law Review*, 17, 315-335.

MCMAHAN, B., & RAMAGE, D. (2017), *Google AI blog: Federated learning: Collaborative Machine Learning Without Centralized Training Data*. <https://ai.googleblog.com/2017/04/federated-learning-collaborative.html>.

MCMAHAN, B., MOORE, E., RAMAGE, D., HAMPSON, S., & Y ARCAS, B. A. (2017), Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS) 2017. JMLR, W&CP Vol.54*.

MCMAHAN, H. B., KAIROUZ, P., AVENT, B., BELLET, A., BENNIS, M., BHAGOJİ, A. N., & ZHAO, S. (2021), Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*. 14(1-2), 1-210.

MENDOZA, I., & BYGRAVE, L. A. (2017), *The Right Not to Be Subject to Automated Decisions Based on Profiling*. EU Internet Law (pp. 77-98). Springer, Cham. University of Oslo Faculty of Law Research Paper.

MITTELSTADT, B. D., & FLORIDI, L. (2016), The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *The Ethics of Biomedical Big Data*, 445-480.

MITTELSTADT, B. D., ALLO, P., TADDEO, M., WACHTER, S., & FLORIDI, L. (2017), The Ethics of Algorithms: Mapping The Debate. *Big Data & Society*, 3(2).

MUNNE', R. (2016), *Big Data in the Public Sector, New Horizons for a Data Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*, (Eds: José María Cavanillas, Edward Curry, Wolfgang Wahlster), Saarbrücken, Springer Open.

NAJAFABADI, M. M., VILLANUSTRE, F., KHOSHGOFTAAR, T. M., SELIYA, N., WALD, R., & MUHAREMAGIC, E. (2015), Deep Learning Applications and Challenges in Big Data Analytics. *Journal of Big Data*, 2(1).

NIELD, D. (2021), *What's Google FLoC? And How Does It Affect Your Privacy?*. <https://www.wired.com/story/google-floc-privacy-ad-tracking-explainer/>.

NISSENBAUM, H. (1996), Accountability in A Computerized Society. *Science And Engineering Ethics*, 2(1), 25-42.

OHM, P. (2009), Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57.

OLIVIER, D., & CHIFFELLE, J. (2008), *Reply: Direct and Indirect Profiling in the Light of Virtual Persons*", *Profiling the European Citizen-Cross Disciplinary Perspectives*. (Eds: Mireille Hildebrandt & Serge Gurwith), Dordrecht, Springer.

ÖZBAYOĞLU, M. (2017), *Derin Öğrenme ile Büyük ve Açık Veri Analizi*", *Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar*, (Editörler: Şeref Sağıroğlu & Orhan Koç), 1. Baskı, Ankara, Grafiker Yayınları.

ÖZDEMİR, H. (2009), *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*. Ankara, Seçkin Yayınevi.

ÖZPARLAK, B.O. (2020), *İşe Alımda Ayrımcılık ve Yapay Zeka Sistemleri*. *Gelişen Teknolojiler ve Hukuk II: Yapay Zeka*. (Editörler: Eylem Aksoy Retornaz & Osman Gazi Güçlütürk), 1.Baskı, İstanbul, On İki Levha Yayıncılık.

PADHY, N., MISHRA, D., & PANIGRAHI, R. (2012), The Survey of Data Mining Applications and Feature Scope. *International Journal of Computer Science, Engineering and Information Technology (IJCEIT)*, 2(3), 44.

PALMER, A. (2018), *Facebook may be Developing a System to Automatically Detect How Rich or Poor You are: Patent Reveals How the Site Could Track Your Socioeconomic Status.* <https://www.dailymail.co.uk/sciencetech/article-5346733/Facebook-patent-uses-track-socioeconomic-status.html>.

PERRY, W. L., MCINNIS, B., PRICE, C.C., SMITH, S.C., & HOLLYWOOD, J.S. (2013), *Predictive Policing: The Role of Crime Forecasting In Law Enforcement Operations*. Rand Corporation. Washington, Rand Offices.

PORTER, J. (2020), UK ditches exam results generated by biased algorithm after student protests. *The Verge*.

PRAISER, E. (2011), Beware Online ‘Filter Bubbles’, TED Talk. <https://ed.ted.com/lessons/beware-online-filter-bubbles-eli-pariser>.

PURTOVA, N. (2018), The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*, 10(1), 40-81.

ROOSENDAAL, A. (2013), Digital Personae and Profiles in Law: Protecting Individuals' Rights in Online Contexts. *Wolf Legal Publishers (WLP)*.

RUSSELL, M.& ZAMFIR, I. (2018), Digital Technology in Elections: Efficiency Versus Credibility?, *European Parliamentary Research Service (EPRS) Briefing*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI\(2018\)625178_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf).

SCHERER, M. U. (2016), Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2).

SCHIFF, A. (2021), Google Will Not Run FLoC Origin Tests in Europe Due To GDPR Concerns (At Least For Now).

<https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/>.

SCHIFFER, Z. (2019), Owned Social Networks, *The Verge*. <https://www.theverge.com/interface/2019/11/12/20959479/eli-pariser-civic-signals-filter-bubble-q-a>.

SELBST, A. D., & BAROCAS, S. (2018), The Intuitive Appeal of Explainable Machines. *Fordham Law Review*, 87(3), 1091-1092.

SELBST, A., & POWLES, J. (2018), “Meaningful Information” and The Right To Explanation. *International Data Privacy Law*, 7(4), 233-242.

SHARMA, S. (2020), *Data Mining vs. Data Analytics: Difference between Data Mining & Data Analytics*. <https://www.upgrad.com/blog/data-mining-vs-data-analytics/>.

SICULAR, S. (2013), *Gartner’s Big Data Definition Consists of Three Parts, Not to Be Confused with Three “V”s*. <https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/?sh=2c470e9b42f6>.

STEWART, M. (2020), *Data Privacy in the Age of Big Data*. <https://towardsdatascience.com/data-privacy-in-the-age-of-big-data-c28405e15508>.

STONE, P., BROOKS, R., BRYNJOLFSSON, E., CALO, R., ETZIONI, O., HAGER, G., & TELLER, A. (2016). *Artificial Intelligence and Life in 2030: The one Hundred Year Study on Artificial Intelligence*. https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.

STREET, F. (2012), How Filter Bubbles Distort Reality: Everything You Need To Know, <https://fs.blog/filter-bubbles/>.

SUNSTEIN, C. R. (1999), The Law of Group Polarization. *The Journal of Political Philosophy* 10(12), 175-195.

SWEENEY, L. (2013), Discrimination in Online Ad Delivery: Google Ads, Black Names and White Names, Racial Discrimination, and Click Advertising. *Queue*, 11(3), 10-29.

TAGER, M. (2003), Cass Sunstein's Republic.com. *Journal of the Association for History and Computing* 6(1).

TAŞTAN, F.G. (2017), *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. 2. Baskı, İstanbul, On İki Levha Yayıncılık.

TENE, O., & POLONETSKY, J. (2013), Big Data For All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property*, 11(5).

VAN DE WAERDT, P. J. (2020), Information Asymmetries: Recognizing The Limits of the GDPR on the Data-Driven Market. *Computer Law & Security Review*, 38, 105436.

VEALE, M., & EDWARDS, L. (2018), Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling. *Computer Law & Security Review*, 34(2), 398-404.

VEDDER, A. (1999), KDD: The Challenge To Individualism. *Ethics and Information Technology*, 1(4), 275-281.

VERBERT, K., PARRA, D., & BRUSILOVSKY, P. (2014, January), *The Effect of Different Set-Based Visualizations on User Exploration of Recommendations*. In CEUR Workshop Proceedings (Vol. 1253, Pp. 37-44). University of Pittsburgh.

VINCENT, J. (2018), Amazon Reportedly Scraps Internal AI Recruiting Tool That Was Biased Against Women. *The Verge*, 10. <https://www.theverge.com/2018/10/10/17958784/ai-recruiting-tool-bias-amazon-report>.

VOIGT, P., & VON DEM BUSSCHE, A. (2017), The EU General Data Protection Regulation (Gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10(3152676), 10-5555.

WACHTER, S. (2018), Normative Challenges of Identification in The Internet of Things: Privacy, Profiling, Discrimination, and The GDPR. *Computer Law & Security Review*, 34(3), 436-449.

WACHTER, S. (2018), The GDPR and The Internet of Things: A Three-Step Transparency Model. *Law, Innovation and Technology*, 10(2), 266-294.

WACHTER, S. (2020), Affinity Profiling and Discrimination By Association in Online Behavioural Advertising. *Berkeley Technology Law Journal*, 35(2).

WACHTER, S., & MITTELSTADT, B. (2019), A Right To Reasonable Inferences: Re-Thinking Data Protection Law in The Age Of Big Data And AI. *Columbia Business Law Review*.

WACHTER, S., MITTELSTADT, B., & FLORIDI, L. (2017), Why A Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76-99.

WACHTER, S., MITTELSTADT, B., & RUSSELL, C. (2017), Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, 31(2), 842-887.

YANISKY-RAVID, S. (2017), Generating Rembrandt: Artificial Intelligence, Copyright, And Accountability In The 3A Era-The Human-Like Authors Are Already Here-A New Model, *Michigan State Law Review*, *Award Winning: The 2017 Visionary Article in Intellectual Property Law, Forthcoming*.

YOUYOU, W., KOSINSKI, M., & STILLWELL, D. (2015), Computer-Based Personality Judgments are More Accurate Than Those Made By Humans. *Proceedings of the National Academy of Sciences*, 112(4), 1036-1040.

ZARSKY, I. (2017), The GDPR in the Age of Big Data. *Seton Hall Law Review*, 47(2), 1007-1008.

ZARSKY, T. Z. (2002), Mine Your Own Business: Making The Case for the Implications of The Data Mining of Personal Information in the Forum of Public Opinion. *Yale Journal of Law & Technology*, 5(1).

ZEDNIK, C. (2021), *Solving The Black Box Problem: A Normative Framework for Explainable Artificial Intelligence*. <https://arxiv.org/pdf/1903.04361.pdf>.

ZIMMERMANN, C. (2015), A Categorization of Transparency-Enhancing Technologies. *Amsterdam Privacy Conference 2015*. <https://arxiv.org/abs/1507.04914v2>.

İNTERNET KAYNAKLARI

Accenture (2021), *Artificial Intelligence Unleashed-How Agencies Can Use AI to Automate & Augment Operations to Improve Performance*.
https://www.accenture.com/_acnmedia/pdf-86/accenture-essential-insights-pov.pdf.

Amnesty International (2020), *We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands*.
<https://www.amnesty.org/en/documents/eur35/2971/2020/en/>.

Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*.
<https://ec.europa.eu/newsroom/article29/items/612053>.

Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*.
https://ec.europa.eu/newsroom/article29/items/612048/en_

Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679*.
<https://ec.europa.eu/newsroom/article29/items/623051>.

Article 29 Working Party, *Advice Paper on Special Categories of Data ("Sensitive Data")*.
https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.

Article 29 Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*.
<https://ec.europa.eu/newsroom/article29/items/622227/en>.

Article 29 Working Party, *Opinion 3/2010 on the Principle of Accountability (WP 173)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is “likely to result in a high risk” for the Purpose of Regulation* 2016/679. <https://ec.europa.eu/newsroom/article29/items/611236/en>.

Article 29 Working Party, *Guidelines on the Right to Data Portability*. <https://ec.europa.eu/newsroom/article29/items/611233>.

BBC, *BBC Pandemic Join a Potentially Life-Saving Citizen Science Experiment*. <https://www.bbc.co.uk/programmes/articles/315gcc2VLF8PC9nFdDM30hm/bbc-pandemic-join-a-potentially-life-saving-citizen-science-experiment>.

Centre For Information Policy Leadership, *Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party’s “Guidelines on Automated Individual Decision – Making and Profiling” adopted on 3 October 2017*. <https://www.informationpolicycentre.com/>.

Competition and Markets Authority, *Investigation into Google’s ‘Privacy Sandbox’ Browser Changes*. <https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes>.

Council of Europe, *Ad Hoc Committee on Artificial Intelligence (CAHAI) Feasibility Study CAHAI (2020) 23*. <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da>.

Council of Europe, *Handbook on European Data Protection Law, 2018 Edition*. https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf.

Council of Europe, *The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling*. Recommendation CM/Rec (2010)13 and Explanatory Memorandum. <https://rm.coe.int/16807096c3>.

Council of Europe, The Committee of Experts on Internet Intermediaries (MSI-NET), *Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) and Possible Regulatory Implications*. <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

Council of Europe, *Protection of individuals with regard to automatic processing of personal data in the context of profiling*. Recommendation CM/REC (2021)8, <https://www.coe.int/en/web/human-rights-rule-of-law/-/data-protection-committee-of-ministers-updates-recommendation-on-profiling>.

Data Protection Commission Ireland, *Guidance Note: Legal Bases for Processing Personal Data*. <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>.

Data Secure (2021), *Google's FLoC & It's Impact on Privacy*. <https://www.datasecure.ind.in/googles-floc-its-impact-on-privacy/>.

European Commission, (2018), *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>.

European Parliament, *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L0681>.

European Data Protection Board (EDPB), *Guidelines 8/2020 on the Targeting of Social Media Users*. Version 2.0. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

European Digital Rights (EDRi), *An Introduction to Data Protection. The EDRi Papers*, Issue 06, http://www.edri.org/files/paper06_datap.pdf.

European Commission, High Level Expert Group On Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

European Commission, *What does data protection ‘by design’ and ‘by default’ mean?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

European Data Protection Board (2020), *Letter Out Ref. 2020-004*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf.

European Parliament, Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA), *A Governance Framework for Algorithmic Accountability and Transparency*. [https://www.europarl.europa.eu/stoa/en/document/EPRS_STU\(2019\)624262](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)624262).

European Parliament, Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA), *Understanding Algorithmic Decision-Making: Opportunities and Challenges*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU\(2019\)624261_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf).

European Parliament, Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA), *The Ethics of Artificial Intelligence Issues and Initiatives*,

Panel for the Future of Science and Technology.
[https://www.europarl.europa.eu/stoa/en/document/EPRS_STU\(2020\)634452](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)634452).

European Parliament, Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA), *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence.*
[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU\(2019\)0122_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)0122_EN.pdf).

Federation of European Direct Marketing (FEDMA) (2000), *FEDMA Code on E-Commerce & Interactive Marketing.*
<https://www.oecd.org/sti/ieconomy/2091875.pdf>.

Information Commissioner's Office (2016), *Big Data, Artificial Intelligence, Machine Learning and Data Protection.* <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

Information Commissioner's Office (2018), *What is Automated Individual Decision Making and Profiling?*. <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling-1-1.pdf>.

Information Commissioner's Office (2018), *Guide to the General Data Protection Regulation (GDPR).* <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>.

Information Commissioner's Office (2017), *Feedback Request – Profiling and Automated Decision Making.* <https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>.

Information Commissioner's Office, *What is a layered approach?*, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>.

Information Commissioner's Office, *Guide to Data Protection-What is Special Category Data?*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>.

Information Commissioner's Office (2017), *Feedback Request-Profiling and Automated Decision Making*. <https://ico.org.uk/media/about-the-ico/consultations/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>.

Information Commissioner's Office, *Guide to Data Protection-Key Data Protection Themes- Children*, <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/>.

Information Commissioner's Office & The Alan Turing Institute (2020), *Explaining Decisions Made with AI*. https://iapp.org/media/pdf/resource_center/ico_explaining_decisions_with_ai.pdf.

Intellectual Property Office, *Artificial Intelligence, A worldwide overview of AI patents and patenting by the UK AI sector*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf.

Kişisel Verileri Koruma Kurumu, *Kişisel Veri Saklama ve İmha Politikası*. <https://kvkk.gov.tr/Icerik/5383/Diger-Dokumanlar>.

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*. <https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler>.

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*. <https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari>.

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*. <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular>.

Kişisel Verileri Koruma Kurumu, *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*. <https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi>.

Kişisel Verileri Koruma Kurumu, *100 Soruda Kişisel Verilerin Korunması Kanunu*. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf>.

Kişisel Verileri Koruma Kurumu, *Covid-19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler, Kamuoyu Duyurusu*. <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler->.

National Public Research (2019), *Market Profiling and Segmentation*. <https://nationalpublicresearch.com/survey-types/market-profiling-segmentation/>.

The Civil Liberties Union for Europe (Liberties), *Algorithmic Bias: Why And How Do Computers Make Unfair Decisions?* <https://www.liberties.eu/en/stories/algorithmic-bias-17052021/43528>.

The European Union Agency for Cybersecurity (ENISA) (2014), *Privacy and Data Protection by Design-From Policy to Engineering*. <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

The Royal Society (2017), *Machine Learning: The Power and Promise of Computers that Learn by Example*. <https://royalsociety.org/~media/policy/projects/machine-learning/publications/machine-learning-report.pdf>.

Theviewpoint, *Why You Should Look Into Addressable TV Advertising*.
<https://theviewpoint.com/insights/blog/why-you-should-look-into-addressable-tv-advertising/>.

