

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
YÜKSEK LİSANS TEZİ

**ŞEFFAFLIK VE HESAP VERİLEBİLİRLİK
AÇISINDAN KİŞİSEL VERİLERİN KORUNMASI
VE YAPAY ZEKÂ**

Mehmet Oğuz KARTÖZ

2501161219

TEZ DANIŞMANI

Prof. Dr. H. Burak GEMALMAZ

İSTANBUL – 2020



T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



YÜKSEK LİSANS
TEZ ONAYI

ÖĞRENCİNİN;

Adı ve Soyadı : MEHMET OĞUZ KARTÖZ Numarası : 2501161219
Anabilim Dalı / Anasat Dalı / Programı : KAMU HUKUKU Danışmanı : DOÇ.DR. HAYDAR BURAK GEMALMAZ
Tez Savunma Tarihi : 03.02.2020 Saati : 15.00
Tez Başlığı : ŞEFFAFLIK VE HESAP VERİLEBİLİRLİK AÇISINDAN KİŞİSEL VERİLERİN KORUNMASI VE YAPAY ZEKA

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin 36. Maddesi uyarınca yapılmış, Sorulan sorulara alınan cevaplar sonunda adayın tezinin KABULÜNE OYBİRLİĞİ / OYÇOKLUĞUYLA karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1-PROF.DR. MELİKŞAH YASİN	M. Nari	KABUL
2-DOÇ.DR. HAYDAR BURAK GEMALMAZ	De	Kabul
3-DOÇ.DR. ABDURRAHMAN SAVAŞ	Adu	Kabul
4-DR.ÖĞR.ÜYESİ ELİF KÜZECİ EROL	Erol	Kabul
5-DR.ÖĞR.ÜYESİ MEHMET BEDİİ KAYA	em	Düzeltilme

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1-DOÇ.DR. MURAT VOLKAN DÜLGER		
2-DR.ÖĞR.ÜYESİ CAHİT GÜNEL		

ÖZ

ŞEFFAFLIK VE HESAP VERİLEBİLİRLİK AÇISINDAN KİŞİSEL VERİLERİN KORUNMASI VE YAPAY ZEKÂ MEHMET OĞUZ KARTÖZ

Yapay zeka sistemleri günümüzde bireyleri ve toplumları etkileyen kararların alınmasında yaygın olarak kullanılmaktadır. Yapay zeka sistemlerinin veri setlerine dayalı olarak öğreniyor olması, çıktılarının insani önyargı ve ayrımcılıklarından uzak olacağını garanti etmiyor. Yapay zekanın her yeni kullanım şeklinde; eşitsizliğe, ayrımcılığa ve kişisel verilerin korunması hakkının ihlaline neden olma riski artmaktadır.

Algoritmik karar alma sistemlerinin kişisel verilerin korunması hukukuna uyumlu kişisel veri işleme faaliyetinde nasıl bulunacağı hakkında seçeneklerin araştırılması gerekmektedir. Bu çalışmada şeffaflık ve hesap verilebilirlik açısından kişisel verilerin korunması ve yapay zekâlı sistemler araştırılmıştır. Araştırma metodu olarak, mevcut bir durumun tespiti yapılacağı için nitel araştırma yöntemlerinden biri olan kaynak derleme metodu kullanılmıştır.

Çalışmada; yapay zeka sistemlerinin türlerine ve kullanım alanlarına, GDPR kapsamında profillemeye ve otomatik karar alma mekanizmalarına ilişkin düzenlemelere yer verilmiştir. Ayrıca, kara kutu ve opaklık sorunlarının, algoritmik önyargının ve algoritmik ayrımcılığın şeffaflık ve hesap verilebilirlik ile ilişkisi incelenmiştir. Son olarak ise veri koruma etki değerlendirmeleri, tasarımdan itibaren kişisel verilerin korunması kavramı, veri koruma görevlisi ve algoritmik denetim mekanizmaları ele alınmıştır.

Anahtar Kelimeler: GDPR, Genel Veri Koruma Düzenlemesi, Hesap Verilebilirlik, Kişisel Verilerin Korunması, KVKK, Profillemeye, Otomatik Karar Alma Mekanizmaları, Şeffaflık, Yapay Zekâ.

ABSTRACT

PERSONAL DATA PROTECTION AND ARTIFICIAL INTELLIGENCE IN TERMS OF TRANSPARENCY AND ACCOUNTABILITY MEHMET OĞUZ KARTÖZ

Artificial intelligence systems are widely employed nowadays when making decisions that have impacts on individuals and society. The fact that AI systems learn from data sets does not guarantee that their outputs will be free of human bias or discrimination. With each new use case of AI, the risk of it causing inequality, discrimination and breaching data protection rights increases.

It was necessary to investigate options about how algorithmic decision-making systems would engage in personal data processing that comply with data protection law. In this study, personal data protection and artificial intelligence systems in terms of transparency and accountability were investigated. As a research method, literature review method, which is one of the qualitative research methods, has been used since an existing situation will be identified.

In this study, the types and usage areas of artificial intelligence systems, articles regarding profiling and automatic decision making mechanisms within the scope of GDPR have been included. Furthermore, the black box and opacity issues, the concepts of algorithmic bias and algorithmic discrimination and their relations with transparency and accountability have been evaluated. Finally, the Data protection impact assessments, the concept of data protection by design, data protection officer and emerging algorithmic audit mechanisms have been covered.

Keywords: GDPR, General Data Protection Regulation, Accountability, Personal Data Protection, The Turkish Personal Data Protection Law, Profiling, Automated Decision-Making Mechanisms, Transparency, Artificial Intelligence.

ÖNSÖZ

Sevdiğin işi yaparsan, bir gün bile çalışmamış olursun derlermiş. Kişisel verilerin korunması hukuku alanındaki okuduğum her makale veya içinde bulunduğum her uyum projesi bu sözü daha iyi anlamamı sağladı. Kişisel verilerin korunması alanı, yaşadığımız dönem ile gelecekteki insanların ve toplumların hava gibi su gibi temel olan bir ihtiyacını karşılayacağını iddia etmektedir; Hürriyet. İnsan haklarının korunduğu bir dünyada barış ve huzurun olacağına inanmam sebebiyle bu gaye doğrultusunda çalışma yapmaya karar verdim. Yapay zekâ sistemlerinin, şeffaflık ve hesap verilebilirlik ilkeleri perspektifinden kişisel verilerin korunmasına uyumlu olabilmesi için Türk Hukukundaki ve Avrupa Birliği Hukukundaki düzenlemeleri güncel konseptler ve örnekler üzerinden incelemeye çalıştım.

Başta İstanbul Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Başkanı Prof. Dr. Adem Sözüer'e çok teşekkür ederim.

Tez çalışmam süresince rotamı çizen, sorunlarımı çözen ve her daim ufkumu daha da genişleten tez danışmanım Prof. Dr. H. Burak Gemalmaz'a çok teşekkür ederim.

Tezimin eksiklerini kıymetli yorumlarıyla tamamlayan jürimde olmasından şeref duyduğum Prof. Dr. Melikşah Yasin, Doç. Dr. Abdurrahman Savaş, Dr. Elif Küzeci, Dr. Mehmet Bedii Kaya, Doç. Dr. Murat Volkan Dülger ve Dr. Cahit Günel'e, her zaman sıcaklığıyla ve ilgisiyle akademiye ve öğrenmeye şevkimi artıran Doç. Dr. Sercan Gürler'e, Yüksek Lisans'da derslerini alarak akademik çalışmanın ve hukukçuluğun inceliklerini öğreten Doç. Dr. Saadet Yüksel'e ve Dr. Gülay Arslan Öncü'ye çok teşekkür ederim.

Tezi başarıyla tamamlayabilmemdeki tartışmasız en büyük pay sahibi olan annem Av. Jale Kartöz'e, her zaman bana olan inancını eksik etmeyen babam Av. Mehmet Kartöz'e ve hayattaki ilk arkadaşım kız kardeşim Av. Zehra Kartöz'e teşekkür ederim.

MEHMET OĞUZ KARTÖZ

İSTANBUL, 2020

İÇİNDEKİLER

	Sayfa
ÖZ	iii
ABSTRACT	iv
ÖNSÖZ.....	v
İÇİNDEKİLER	vi
ŞEKİLLER LİSTESİ	ix
KISALTMALAR LİSTESİ.....	x

GİRİŞ.....	1
------------	---

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GELİŞİMİ, TEMEL KAVRAMLAR VE YAPAY ZEKÂ

1.1. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GELİŞİMİ	7
1.2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BAZI TEMEL KAVRAMLAR, İLKELER VE KONSEPTLER	17
1.2.1. Kişisel Veri	17
1.2.2. Özel Nitelikli Kişisel Veri	18
1.2.3. Veri Sorumlusu ve Veri İşleyen.....	20
1.2.4. Kişisel Verinin Hukuki Niteliği.....	23
1.2.4.1. Genel	23
1.2.4.2. Mülkiyet Hakkı Görüşü.....	24
1.2.4.3. Kişilik Hakkı Görüşü.....	29
1.3. YAPAY ZEKÂLI SİSTEMLER	31
1.3.1. Tanımı.....	32
1.3.2. Türleri.....	34
1.3.2.1. Makine Öğrenimi.....	34
1.3.2.2. Gözetimli ve Gözetimsiz Öğrenme	35
1.3.2.3. Derin Öğrenme	37
1.3.3. Kullanım Alanları.....	37

İKİNCİ BÖLÜM

YAPAY ZEKÂ SİSTEMLERİNDE KİŞİSEL VERİLERİN İŞLENMESİ

2.1. YAPAY ZEKÂ SİSTEMLERİ BAKIMINDAN KİŞİSEL VERİLERİN İŞLENMESİNDEKİ TEMEL İLKELER	46
2.1.1. Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi	47
2.1.2. Doğru ve Gerektiğinde Güncel Olma İlkesi	49
2.1.3. Belirli, Açık ve Meşru Amaçlar için İşlenme İlkesi	50
2.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma	52
2.2. KİŞİSEL VERİLERLE İLGİLİ DİĞER İLKELER.....	54
2.2.1. Şeffaflık ve İlgili Kişileri Bilgilendirme İlkesi.....	54
2.2.2. Hesap Verilebilirlik İlkesi	61
2.2.3. Veri Güvenliği İlkesi	64
2.3. YAPAY ZEKÂ SİSTEMLERİNDE KİŞİSEL VERİLERİN İŞLENMESİ	65
2.3.1. Profilleme	66
2.3.2. Otomatik Karar Alma Mekanizmaları	71
2.4. ALGORİTMALAR.....	73
2.4.1. Genel Olarak.....	73
2.4.1.1. Arama Algoritmaları	74
2.4.1.2. Sıralama Algoritmaları	75
2.4.1.3. Şifreleme Algoritmaları	76
2.4.2. Algoritmik Sistemlerin Kişisel Verilerin Korunması Bakımından Değerlendirilmesi	77
2.4.2.1. Kara Kutu ve Opaklık.....	77
2.4.2.2. Algoritmik Önyargı	82
2.4.2.3. Algoritmik Ayrımcılık	87
2.4.2.4. Algoritmik Şeffaflık.....	94
2.4.2.5. Algoritmik Hesap Verilebilirlik	100

ÜÇÜNCÜ BÖLÜM

YAPAY ZEKÂ SİSTEMLERİ BAKIMINDAN KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HAKLAR VE ALINMASI GEREKEN TEDBİRLER

3.1. İLGİLİ KİŞİNİN HAKLARI.....	105
3.1.1. Bilgi Edinme, Düzeltme, Sildirme Hakkı.....	105
3.1.2. İtiraz Etme ve Zararların Giderilmesini İsteme Hakkı.....	109
3.1.3. Profilleme de Dahil Olmak Üzere Otomatik Karar Vermenin Varlığı ve Gerçekleştirilen İşleme Faaliyetinin Kişi Açısından Önemi ve Öngörülen	

Sonuçları da Dahil Olmak Üzere Çalışma Mantığına İlişkin Anlamlı Bilgilerin Sunulması Hakkı	110
3.1.4. Profilleme, İnsan Müdahalesi Talep Etme ve Açıklama Talep Etme Hakkı	111
3.2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINABİLECEK TEKNİK VEYA İDARİ TEDBİRLER.....	120
3.2.1. Teknik Tedbirler	120
3.2.1.1. Eğitim Verisinin Minimizasyonuna İhtiyaç Duyularak Alınacak Tedbirler	120
3.2.1.2. Eğitim Verisinin Minimizasyonuna Gerek Duyulmadan Alınabilecek Tedbirler	122
3.2.1.3. Algoritmik Sistemleri Açıklama Yöntemleri	125
3.2.2. İdari Tedbirler.....	129
3.2.2.1. Veri Koruma Etki Değerlendirmesi.....	129
3.2.2.2. Veri İhlali Riskinin Yüksek Olması Hâlinde Bu Riskin Kişisel Verileri Koruma Kurumuna ve İlgili Kişiye Bildirimde Bulunma Zorunluluğu.....	135
3.2.2.3. Tasarımdan İtibaren Kişisel Verilerin Korunması.....	137
3.2.2.4. Veri Koruma Görevlisi.....	140
3.2.2.5. Algoritmik Denetim.....	143
SONUÇ VE ÖNERİLER	145
KAYNAKÇA.....	156

ŞEKİLLER LİSTESİ

Sayfa

Şekil 2.1: Modern Şifreleme Algoritmaları 77



KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABAD	: AB Adalet Divanı (<i>CJEU - Court of Justice of the European Union</i>)
ABD	: Amerika Birleşik Devletleri
AİHK	: Avrupa İnsan Hakları Komisyonu (<i>European Commission of Human Rights</i>)
AİHM	: Avrupa İnsan Hakları Mahkemesi (<i>ECHR - European Court on Human Rights</i>)
AİHS	: Avrupa İnsan Hakları Sözleşmesi (<i>The European Convention on Human Rights</i>)
AİHHŞ	: Afrika İnsan ve Halkların Hakları Şartı (<i>ACHPR - African Charter on Human and Peoples Rights</i>)
Ame.İHS	: Amerikan İnsan Hakları Sözleşmesi (<i>ACHR - American Convention on Human Rights</i>)
Bkz./bkz.	: Bakınız
CHRC	: <i>Canadian Human Rights Commission</i> (Kanada İnsan Hakları Komisyonu)
CCTV	: <i>Close Circuit TeleVision</i> (Kapalı Devre Televizyon)
CMK	: Ceza Muhakemesi Kanunu
EC	: <i>European Commission</i> (Avrupa Komisyonu)
EDPB	: <i>European Data Protection Board</i> (Avrupa Veri Koruma Kurulu)
EİHB	: Evrensel İnsan Hakları Beyannamesi (<i>UDHR - Universal Declaration of Human Rights</i>)
GANs	: Generative Adversarial Networks
GDPR	: <i>General Data Protection Regulation</i> (Genel Veri Koruma Düzenlemesi)
GPS	: <i>Global Positioning System</i> (Küresel Konumlama Sistemi)
IAPP	: <i>International Association of Privacy Professionals</i>
ICO	: <i>Information Commissioner's Office</i>
ISO	: <i>International Organization for Standardization</i> (Uluslararası Standartları Teşkilatı)
IWG	: <i>International Working Group</i>
KVK	: Kişisel Verilerin Korunması
KVKH	: Kişisel Verilerin Korunması Hakkı

KVKK	: Kişisel Verilerin Korunması Kanunu
LFR	: <i>Live Facial Recognition</i> (Canlı Yüz Tanıma)
m.	: Madde
MSIT-PE	: <i>Master of Science in Information Technology – Privacy Engineering</i>
NHS	: <i>National Health Service</i> (İngiltere Ulusal Sağlık Servisi)
NIST	: <i>National Institute of Standards and Technology</i> (Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü)
OECD	: <i>Organization for Economic Cooperation and Development</i> (Ekonomik İşbirliği ve Kalkınma Örgütü)
OHCHR	: The Office of the High Commissioner for Human Rights (UN Human Rights)
PET	: <i>Privacy Enhanced Technologies</i> (Veri Korumayı İyileştirme Teknolojileri)
RAID	: <i>Redundant Array of Independent Disks</i> (Bağımsız Disklerin Yedekli Dizisi)
TBMM	: Türkiye Büyük Millet Meclisi
UİHH	: Ulusalüstü İnsan Hakları Hukuku (<i>Supra-national Human Rights Law</i>)
VERBİS	: Veri Sorumluları Sicil Bilgi Sistemi
VKED	: Veri Koruma Etki Değerlendirmesi (<i>DPIA - Data Protection Impact Assessment</i>)
YSA	: Yapay Sinir Ağları (<i>ANN - Artificial Neural Networks</i>)
YZ	: Yapay Zekâ

GİRİŞ

Bu bölümde araştırmada ele alınan konunun önemi, araştırmada kullanılan metot, çalışmanın amacı, sınırları, planı ve kaynakları ele alınacaktır.

Konunun Önemi

Özel hayata ve aile yaşamına saygı hakkının ihlaline sebep olan devletler veya kurumlar tarafından gerçekleştirilen kişisel veri işleme ve anlamlı sonuçlar üretme faaliyetleri gerekli değerlendirmeler yapılmadan gerçekleştirilirse, dolaylı yoldan kişilerin düşünce, vicdan ve inanç özgürlüğünün, ifade özgürlüğünün, ayrımcılık yasağının, mülkiyet hakkının, eğitim hakkının, serbest seçim hakkının, çalışma hakkının ölçüsüz bir biçimde sınırlandırılmasına neden olmaktadır. Diğer bir yönüyle kişilerin özgürlüklerinin korunması hedeflenirken, devletlerin kamu güvenliğini ve düzenini sağlama adına alacağı, kurum ve kuruluşların ticari sırlarını, kar elde etme gibi var olma amaçlarını muhafaza edebilme adına aldığı tedbirlerin etkisiz hale gelmesi riski ile karşı karşıya kalınmaktadır. Ayrıca internet kullanan kullanıcı sayısının ve kullanım sıklığının artması, kullanılan dijital platformların ve ortamların gitgide daha fazla ve çeşitli veri türünü toplaması, bunların daha kompleks ve çeşitli şekilde çalışan yapay zekâ (YZ) sistemleri tarafından işlenip ve anlamlandırılması sonucunda bireylerin hayatlarının neredeyse her katmanında etkili olmaktadır.

Kişisel Verilerin Korunması (KVK) hukukunda yer alan temel ilkeler, işleme şartları, kanun kapsamındaki kurum veya kuruluşların sorumlulukları veya ilgili kişilerin haklarına ilişkin tezler, makaleler veya kitaplar telif edilmiştir ve edilmeye devam edilmektedir. KVK düzenlemelerine uyum sağlama adına atılan adımların hukuki doküman düzenleme veya mevcut olanların gözden geçirilmesinin ötesine nadiren geçildiği dönemde bulunmaktayız. KVK alanında kişilerin temel hak ve hürriyetlerinin en ağır ve ölçüsüz bir şekilde ihlal edildiği, politik düşüncelerinin veya ticari alışkanlıklarının şekillendirildiği, profiller oluşturmak suretiyle eşit şartlarda çalışma hakkından veya rekabet edebilme hakkından mahrum bırakıldığı, sağlık alanından adli konulara kadar birçok alanda kullanılan yapay zekâ sistemlerinin

sebebi olduđu KVK ve özel hayatın gizliliđi hakkının ihlali durumlarının incelenmesi gerekmektedir.

Arařtırma Metodu

Bu alıřmada arařtırma metodu olarak, mevcut bir durumun tespiti yapılacađı için nitel arařtırma yöntemlerinden biri olan kaynak derleme metodu kullanılmıřtır.

alıřmanın Amacı

alıřmanın amacı; bireylerin bařta politik grř, ırk ve uyrukları, dini inan, felsefi grř, sađlık durumları ve cinsel ynelimleri gibi zel nitelikli kiřisel verileri olmak zere genel itibariyle kiřisel verilerinin iřlenmesi sonucunda retilen profillerinin yapay zekâlı sistemlerin altyapısını oluřturduđu otomatik veya yarı otomatik karar alma mekanizmalarında kullanılması sebebiyle kiřilerin uđradıđı haksızlıđı ve ayrımcılıđı engelleme amacıyla, temel hak ve hrriyetleri koruma amacıyla inřa edilmiř bařta řeffaflık ve hesap verilebilirlik olmak zere KVK hukukundaki temel ilkelere uyumlu veri iřleme faaliyetine bulunabilme adına mevcut bulunan teorileri, pratik hayattan rnekleri, zm nerilerini, teknik ve idari tedbirleri arařtırmaktır.

Arařtırmada ayrıca; temel insan haklarının ve toplumsal deđerlerin realize edilmesinin nasıl mmkn olduđu; insanların yerine otomatize karar alma mekanizmalarının karar almasının, demokratik deđerlerin ve temel insan hak ve zgrlklerin korunmasına ne gibi etkilerinin olduđu; toplumsal deđerler ve temel zgrlklerin, algoritmaların tasarımı yapılırken nasıl yorumlanabileceđi ve entegre edilebileceđi; demokratik deđerlerin, hukukun stnlđnn ve temel hakların korunması adına ne gibi teknik ve idari tedbirler alınması gerektiđi sorularına da yanıt aranmıřtır. Bunun yanı sıra arařtırmada; hukuk đrencilerinin, akademisyenlerin, avukatların ve konuya ilgi duyan diđer tm paydařların; kiřisel verilerin temel hak ve hrriyetleri dođrudan nasıl etkilediđine iliřkin bilgi sahibi olması, yapay zekânın genel erevesi hakkında fikri olması ve bu konularda kendini geliřtirmek isteyenlere hem bir bařlangı hem de atıf yapılan kaynaklarla yardımcı olması hedeflenmektedir.

Çalışmanın Sınırları

Çalışma; şeffaflık ve hesap verilebilirlik özelinde kişisel verilerin korunması ve yapay zekâlı sistemler ile sınırlıdır.

7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nu hayatımıza girmesiyle birlikte yeni birçok hukuki sorunu da gündeme getirmiştir. Düzenlemenin pratikte nasıl uygulanacağından içeriğindeki düzenlemelerin nasıl yorumlanması gerektiğine kadar üzerinde çalışma yapılması gereken yönü bulunmaktadır. Çalışmamızı sınırlandırarak daha farklı açılarından ele alabilmek için kendimize alan yaratmaya çalıştık.

Çalışmamızın konusunu kişisel veri işleyen yapay zekâlı sistemler olma sebebi en geniş çapta ve önemli açıdan kişinin hayatını etkileyen sonuçların bu mekanizmaların içinde bulunduğu süreçlerde ortaya çıkmasıdır. Ayrıca her türlü kimlik grubundan toplumda azınlık olarak bulunan veya kaynaklara ulaşım açısından eşit imkanlarda bulunmayan toplulukların daha fazla haksızlığa ve ayrımcılığa uğramasına da yine bu sistemlerin neden olduğu görülmektedir. Temel insan hakları ihlal edilen kişi veya toplulukların uzun yıllardır verdikleri mücadelede elde ettikleri kazanımlar yapay zekâların devreye girmesiyle ellerinden kayabilir hatta daha da geriye gitme riski ile karşılaşılabilir. Ayrıca daha önce karşılaşılmamış yeni profilde kişilerin veya topluluklarında öngörülemeyen şekilde haklarının ihlale uğraması yüksek bir ihtimal olarak bulunmaktadır.

Çalışma konumuzu sadece hukuki açıdan değil düzenlemede de geçtiği şekliyle idari ve teknik açılardan incelemeye çalıştık. Hususiyle teknik konular artık hukukun her alanında kendine yer bulmaktadır. Bu sebeple teknik yönüyle atılacak adımların hukuken hangi sonuçların doğuracağıının anlaşılmasının önemli olduğuna kanaat getirmekteyiz. Özellikle ele almayı çalıştığımız teknolojik kavramlar veya konseptler daha detaylı bilgi almak isteyen meraklılara bir başlangıç olması için çalışmada yer almaktadır. Yabancı literatür üzerinden araştırmamızı yaptığımız için

toplu bir şekilde bir dokümanda ilgili konuların yer almasının daha faydalı olacağını düşündük.

Kişisel verilerin korunmasının hukukun çok farklı alanda sorunlar üretmesi sebebiyle o yönüyle de bir sınırlamaya gidilmesi gerekti. Kişisel verilerin korunması alanındaki rol alan gruplar 3 başlık altında; bireyler, kurumlar ve devletler şeklinde sayılabilir. Çalışmamızda temel olarak insan hakları perspektifinden değerlendirmeler yapılacaktır.

Birey ile özel teşebbüsler arasındaki ilişkinin nasıl insan hakları zaviyesinden ele alınacağına sorusunu çalışma süresince sıkça almaktaydık. Kişisel Verilerin Korunması Kanunu, anayasanın 20. maddesinde düzenlenen İnsan hakları hukuku devletlerin, bireylerin haklarını ihlal etmemesini sağlama amacıyla negatif yükümlülükler getirmektedir. Aynı zamanda bireylerin haklarının devlet veya kurum veya kuruluşlar tarafından ihlal edilmesini önlemek amacıyla devletlerin gerekli düzenlemeleri yapması ve tedbirleri alması gibi pozitif yükümlülükler de getirmektedir.

Yapay zekâ, nesnelerin interneti, otonom araçlar gibi teknolojilerin sosyal veya hukuki etkilerinin düzenlenebilmesi için etik değerlerin tasarımlara uygulanması ve bu değerler bağlamında incelemelerin yapılmasına ilişkin birçok çalışma da bulunmaktadır. Ancak insan hakları etik değerlendirmelerden ayrı olarak hukuken uygulanabilir olma özelliği taşıdığı için denetim ve yaptırım gibi araçların gerçekleşmesi için zorlayıcı unsurları barındırmaktadır.

Kanun kapsamında kişinin özerk alanına yönelik müdahalelerin gerçek hayattan örneklerle çerçevesinin çizilmesi, mevcut hukuki düzenlemelerdeki ilke ve mekanizmaların değerlendirilmesi ve çözüm yollarının araştırılmasının gerekli olduğunu düşünerek devlet ve özel veya kamu kurum ve kuruluşlarının bireylerle olan ilişkisinde ölçünün nasıl sağlanacağı dengenin nasıl tekrar yerine konacağı ele alınmaya çalışılmaktadır.

Çalışmanın Planı

Bu çalışma üç ana bölümden oluşmaktadır. Çalışmanın birinci bölümünde; kişisel verilerin korunması hukukunun gelişimi, temel kavramlar ve yapay zekâ konuları ele alınacaktır. Bu başlık altında kişisel verilerin korunmasının bugüne gelmesinde hukuksal düzenlemelerinin ortaya çıkışı ve gelişimi değerlendirilmiştir. Kişisel verilerin korunmasındaki bulunan kavramlardan konumuzla yakından ilişkili olduğunu düşündüklerimizin açıklaması yapılmıştır. Yapay zekânın genel tanımı, türleri ve uygulama alanları son olarak ele alınan konulardır.

İkinci bölümde; Yapay Zekâ Sistemlerinde Kişisel Verilerin İşlenmesi konusu incelenecektir. Kişisel verilerin korunmasında temel ilkelerin anlaşılması kanuna uygun veri işleme faaliyette bulunabilmesi için oldukça önemlidir. Yapay zekâ sistemlerinin ve ortaya çıkardığı sorunların doğrudan ilişkili olduğunu düşündüğümüz temel ilkeler ele alınmıştır. Ayrıca kanunumuzun lafzında geçmese de hem Kişisel Verileri Koruma Kurumunun kararlarında, rehberlerinde hem de diğer akademik çalışmalarda yer verilmesi ve bizim de önemli olduğunu düşünmemiz sebebiyle diğer bazı ilkeler açıklanmıştır. İkinci bölümün son kısmında, kişisel verilerin korunması kapsamında da tanımlanmış bazı ilkelerin algoritmik sistemlerin anlaşılması ve uyumluluğu açısından kullanılması yönüyle değerlendirmelerde bulunulmuştur. Algoritmik sistemlerin kişisel verilerin korunmasındaki ilkelere uyumluluğu engelleyen hangi yönlerinin bulunduğu ve hangi sonuçlara sebep olduğu da incelenmiştir.

Üçüncü bölümde ise yapay zekâ sistemleri bakımında kişisel verilerin korunmasına ilişkin haklar ve alınması gereken tedbirler işlenecektir. İlgili kişinin haklarının yapay zekâlı sistemlerin düzenlemelere uyumluluğu açısından nasıl kullanılabileceği ele alınacaktır. Kişisel verilerin korunması hakkının ihlal edilmemesi adına devletlerin, kurumların ve kuruluşların kullandıkları algoritmik sistemlerin teknik ve idari yönleriyle alabileceği tedbirler ifade edilecektir.

Çalışmanın Kaynakları

Alan yazında Türkçe olarak yapılmış çalışmalar ekseriyetle, kanunun içeriği üzerine yoğunlaşmış, kavramların ve ilkelerin açıklanması, hak ve sorumlulukların izah edilmesi üzerine devam etmiştir. Ancak ele alınan hukuki sorunların çözümü için ulusal ve uluslararası alandaki hukuki düzenlemelerin ilgili bölümlerine bakılmalıdır. Çalışmamızda Kişisel Verilerin Korunması Kanunu, GDPR, ilgili mevzuat, mahkeme kararları ve içtihatlar temel alınacak hukuki kaynaklar olacaktır.

Amazon, Google ve Facebook gibi şirketlerin uygulamaya aldığı yeni teknolojilerin medya yoluyla duyulması ve ardından kişisel veri koruma otoritelerinin veya kamu kurumlarının inceleme başlatmak şeklinde harekete geçmesiyle beraber akademisyenlerin yayımlanmış çalışmaları, araştırma konusunun yaşadığımız zaman itibarıyla önemli bir ihtiyaç olduğuna işaret etmektedir. Araştırmamızda felsefe, sosyoloji, hukuk, psikoloji, mühendislik, yazılım gibi farklı disiplinlerde kaleme alınmış uluslararası dergilerde yayımlanan makalelere ağırlık verilmiştir. Konunun yeni olması sebebiyle halen sorunun tespiti adına en isabetli yolların araştırıldığı, çözüm yolları açısından fikir birliğine varılamadığı bir dönemde yeterli görülen tüm imkanlardan faydalanılmaya çalışılmaktadır.

Avrupa Birliği (AB), İngiliz ve Fransız kişisel veri koruma otoritelerinin yayımları bu çalışmada faydalanılan kaynaklar arasındadır. Ayrıca, çeşitli ulusal ve uluslararası kuruluşların, hükümetlerin ve sivil toplum örgütlerinin sorunun çeşitli boyutlarını inceleyen raporları, önerileri, değerlendirmeleri de bu araştırmanın temel kaynakları arasında yer almaktadır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GELİŞİMİ, TEMEL KAVRAMLAR VE YAPAY ZEKÂ

Bu bölümde KVK hukukunun gelişimi, KVK'ya ilişkin bazı temel kavramlar, ilkeler ve konseptler ile yapay zekâlı sistemler incelenecektir.

1.1. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GELİŞİMİ

Bu araştırmanın konusu belirli kimlik (siyasi görüş, ırk, dini veya felsefi inanç, cinsel yönelim, sendika bilgisi, vb.) özelliklerine göre ayrımcılığa veya haksızlığa tabi tutulma üzerinden temellendiği için, öncelikli olarak KVK hukukunun tarihçesinin kısaca ele alınmasında fayda bulunmaktadır.

Kişinin hukuken korunmasından neyin anlaşıldığı zaman içerisinde değişmiştir. İlk başta fiziksel müdahalelere karşı kişinin ve mülkiyetin korunmasından başlayan, insanın ruh, duygu ve zekâ açısından yeni bir katmanının kabulü ile devam eden korunmaya değer bulunan süreç, kişinin yalnız başına kalabilme ve maddi veya manevi her türlü formdaki malın mülkiyet kapsamına girebileceği dolayısıyla yeni haklar elde etmesiyle daha farklı bir koruma anlayışına doğru evrilmiştir. Kişinin ve ailesinin itibarının ve şerefının zarar görmesinin neden olacağı psikolojik zararların ve üzüntülerin, fiziksel zararlardan daha öteye gidebileceği Özel Hayatın Gizliliği Hakkı'nın (*Right to Privacy*) ilk defa dile getirildiği 15 Aralık 1890 tarihinde ileride Yüksek Mahkeme (*Supreme Court*) yargıcı olacak Louis Brandeis ile Amerikalı avukat Samuel Warren tarafından kaleme alınan Harvard Hukuk Dergisi'nde yayımlanan makalede kişinin kendine has aleminin korunmaya değer olduğunu ifade ederek modern çağda insanlığı ve hukuku en çok meşgul edecek alanlardan birisinin temellerini atmıştır.¹ KVK'ya yönelik ihtiyaç, Yirminci Yüzyılda bilişim teknolojilerinin gelişimiyle beraber bir zorunluluk haline

¹ Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy", **Harvard Law Review**, Vol.4, No.5, December 15, 1890, pp.193-220 (Çevrimiçi) <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> 8 December 2019.

gelmiştir. 1960'lı yıllarla birlikte ekseriyetle verilerin otomatik bir şekilde işlenmesini sağlayan teknolojiler hız kazanmıştır. Böylece devlet kurumları, bireylere ait kişisel verileri içinde barındıran oldukça geniş veri havuzları oluşturmaya başlamıştır. Fakat bu gelişmelerle birlikte özel hayatın gizliliğinin korunmasına ve devlet tarafından bireylere ait bu tür kişisel verilerin toplanmasıyla sağlanan bu bilgi hâkimiyetinin sınırlandırılmasına ilişkin talepler de artmıştır.²

KVK ve bunun bir hak olarak kabul edilmesinin altında yatan temel neden esasen bu tür verilerin ayrımcılığa veya çeşitli haksızlıklara yol açmasıdır. KVK'nın ortaya çıkma sürecinde 1946 yılında bilgisayarın geliştirilmesinin ve 20. Yy'ın ikinci yarısında bilişim teknolojilerinin gelişimi aracılığıyla kayıtların ve verilerin toplanma, yayılma ve kullanılmasıdaki değişikliklerin ve bilgisayarın kullanımının artmasının etkili olduğu kabul edilebilir³. Özellikle kamu ve özel şirketlerin merkezi veri bankalarında kişilerin bilgilerinin toplanması ve eğitim, etnik köken, finansal ve suça karışmaya ilişkin profillerinin oluşturulması bu gelişimi desteklemiştir. Fiziksel ortamdaki dijital ortama dönüşüm sebebiyle kişisel verilerin daha hızlı ve geniş kapsamda işlenmesi mümkün olmuştur. Toplanan verilerin fiziksel arşivlerde saklanmasından daha rahat bir şekilde dijital ortamlarda saklanması ve yer değiştirmesi sağlanabilmiştir.

KVK'nın bugünlere nasıl geldiğinin anlaşılması adına; 1970'li yıllardaki finansal alanda ve 1980'li yıllarda haberleşme ve iletişimin gizliliği alanındaki gelişmeler önemlidir⁴. 1990'lı yıllarda internetin gelişimi ve eposta kullanımının artmasıyla birlikte KVKK üzerine daha fazla çalışma yapılmaya başlanmıştır. İnternet üzerinden iletişimin artması, internette her hareketin veri üretmesine yol açmıştır. Metinlerden ses, görüntü ve görsel şekillerde bilginin paylaşımına geçiş ve veri aktarım hızının artması anlık ve yoğun bir etkileşime neden olmaktadır. Cep telefonu ve bilgisayar gibi cihazlar aracılığıyla elektronik ortamlar üzerinden

² Mesut Serdar Çekin, "Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu", **On İki Levha Yayıncılık**, İstanbul, 2018, s.5.

³ Daniel J. Solove, "A brief history information privacy law", GWU Law School Public Law Research Paper No. 215, **Proskauer on Privacy, PLI**, 2016, p.25, (Çevrimiçi) https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications 8 January 2020.

⁴ Solove, **Ibid.** pp.28-34.

platformlar ve uygulamalar ile günlerce beklenen mektup veya birçok aracıyı zorunlu kılan telgrafın ötesinde saniyeler içerisinde bilgi aktarılması sağlanmıştır.

Bunun, doğrudan kullanıcıların sağladığı bilgiler ve internette gezinirken kullanıcının bilgisi ve onayı olmaksızın toplanan bilgiler olmak üzere iki farklı türü bulunmaktadır. Doğrudan kullanıcıların sağladığı bilgiler, kişinin bir siteye üye olurken, kitap satın aldığı anda, yemek siparişi verdiğinde, tweet attığında veya instagramda paylaşım yaptığı anda verdiği bilgilerdir. İnternette gezinirken kullanıcının bilgisi ve onayı olmaksızın bilgi toplanmasında ise kişinin IP adresinin izlenmesi ve çerezler (cookies) gibi yöntemler kullanılmaktadır. Çerezler⁵, kişinin hangi sitelerde gezindiğini tespit etmektedir ki bu da kişisel ilgi ve eğilimleri ortaya çıkarıp profillemeye imkân sağlamaktadır. Arama motorlarında yapılan aramalar da kişilerin eğilimlerine ilişkin fikir vermektedir⁶. Arama motoruna yazılan kelimelerin bir hastalığı ya da boşanma avukatını araştıran kişinin durumu hakkında bilgi vermesi gibi sonuçlar buna örnek gösterilebilir⁷.

11 Eylül 2001 tarihindeki terörist saldırısının ardından ABD'nin sınır güvenliği başta olmak üzere, eposta aktarımının ve IP adreslerinin takibi, daha sonradan Edward Snowden'ın paylaşımları ile daha detaylı öğrenilecek olan Ulusal Güvenlik Ajansı'nın (National Security Agency "NSA") mahkeme kararı olmadan, kesintisiz ve toplu halde yaptığı gözetimler konunun önemini gözler önüne sermiştir. Kişisel verilerin korunmasına ilişkin dönüm noktası ise gözetim (surveillance) sağlayan yeni teknolojilerin gelişimidir ki bu tür teknolojiler KVK Hukuku'na duyulan ihtiyacı artırmıştır. "Kapalı Devre Televizyon" anlamına gelen "*Close Circuit TeleVision*"

⁵ Çerezler, ziyaret edilen bir websitesi tarafından kullanıcının cihazından depolanan bilgilerdir. Çerezlerin, internetin gelişiminde ve kişisel verilerin korunması alanındaki kritik önemine ilişkin bkz. John Schwartz. "Giving the Web a Memory Cost Its Users Privacy", September 4, 2001. (Çevrimiçi) [https://pdfs.semanticscholar.org/77c3/88be3f57c80889e5291dc103f8f375718f56 .pdf](https://pdfs.semanticscholar.org/77c3/88be3f57c80889e5291dc103f8f375718f56.pdf) 31 December 2019.

⁶ Bu çalışmanın temelindeki profiller/davranış eğilimleri aslında bizim fiziksel veya dijital ortamlardaki hareketlerimiz ve arama motorlarında yaptığımız aramalarımız ile platformlara temin ettiğimiz bilgilerin veri madenciliği yapıp ilişkilendirilmesiyle oluşturulmaktadır (bkz. Elif Küzeci, "Kişisel Verilerin Korunması", **Turhan Kitabevi**, Ankara, 2019, s.38).

⁷ İnternet trafiğinin yüzde 12'si Google, yüzde 11,5'i Netflix, yüzde 7,8'i Facebook, yüzde 5,1'i Microsoft, yüzde 4'ü Apple ve yüzde 3'ü Amazon tarafından olmak üzere %43 oranında sayılan şirketler üzerinden sağlanmaktadır. Daha detaylı bilgi için bkz. Sandvine, "The Global Internet Phenomena Report", September 2019 (Online) https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/Internet%20Phenomena/Internet%20Phenomena%20Report%20Q32019%2020190910.pdf 31 December 2019.

(CCTV) kameraları, parmak izi tanıma (*fingerprint identification*), avuç içi tanıma (*palmpoint identification*) ve yüz tanıma (*facial recognition*) gibi biyometrik doğrulama sistemleri, “Küresel Konumlama Sistemi” (*GPS - Global Positioning System*) gibi lokasyon takip sistemleri bu tür teknolojilere örnek olarak gösterilebilir.

Özellikle son yıllarda gözetim sağlayan yeni teknolojilere yönelik gizlilik ve veri güvenliği konularında yaşanan olumsuzluklar (veri sızıntıları) dünya genelinde KVK'ya yönelik kaygı yaratmaktadır. Buna en yakın iki örnek olarak 2019 yılında Çin ve İngiltere’de yaşanan olaylar gösterilebilir. 2019 yılı Şubat ayında, güvenlik uzmanları tarafından yapılan bir kontrolde Çin'in Silikon Vadisi olarak tanınan Shenzhen şehrindeki bir yüz tanıma ve güvenlik yazılımı şirketi olan SenseNets'in korunmasız bir veritabanından yaklaşık 2,6 milyon kişinin 6,7 milyon civarındaki kişisel verilerini (kimlik kartı numarası, yayın ve bitiş tarihi, cinsiyet, uyruk, adres, doğum günü, pasif resim, işveren ve son 24 saat içinde bulunulan konumlar gibi) içeren ciddi bir veri sızıntısı olduğu tespit edilmiştir⁸. 2019 yılı Ağustos ayında, yüz tanıma bilgisi ve parmak izi gibi biyometrik bilgiler de dahil olmak üzere 1 milyondan fazla kişinin kişisel verileri, İngiliz polisi, savunma sanayi şirketleri ve bankalar tarafından kullanılan kamuya açık bir veri tabanında bulunmuştur⁹. Özellikle biyometrik bilgilerin neredeyse değişmediği ve veri sızıntısının sonuçlarının şiddetli ve uzun yıllar boyunca etkili olabileceği göz önüne alındığında, bu ve benzeri kişisel veri ihlallerinin mağdurlara çok büyük zararlar verme ihtimali bulunmaktadır.

KVK Hukuku'nun gerçek anlamda gelişimi 1970'li yıllar itibariyle olmuştur. Özellikle İkinci Dünya Savaşı ve öncesi dönemin Almanyasında kişilerin fişlenmesi ve soykırıma uğramasında bu kişilerin verilerinin devlet tarafından toplanması, ayrıca Doğu Almanya'daki takip faaliyetleri ve sisteme muhalif kişilerin tespitinde

⁸ Victor Gevers, “There is this company in China named SenseNets. They make artificial intelligence-based security software systems for face recognition, crowd analysis, and personal verification. And their business IP and millions of records of people tracking data is fully accessible to anyone.” and “This database contains over 2.565.724 records of people with personal information like ID card number (issue & expire date, sex, nation, address, birthday, passphoto, employer and which locations with trackers they have passed in the last 24 hours which is about 6.680.348 records.”, **Twitter**, 13 February 2012 (Çevrimiçi) <https://twitter.com/OxDUDE/status/1095702540463820800/photo/1> 20 November 2019.

⁹ Josh Taylor, “Major breach found in biometrics system used by banks, UK police and defence firms.” **The Guardian**, 14 August 2019, (Çevrimiçi) <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms> 20 November 2019.

verilerin kullanılması, dolayısıyla o dönem Almanya’da kişisel verilerin yanlış kullanımının getirdiği korku, bu alanın Almanya’da doğmasına sebep olmuştur. Nitekim, kişisel verilerin korunması hakkındaki ilk hukuki düzenlemeye de daha önce Almanya’da kişisel verilerin yanlış kullanımının yarattığı olumsuz sonuçların korkusundan dolayı Almanya’da rastlanmaktadır¹⁰. 7 Ekim 1970’de Almanya’nın Hessen Eyaleti’nde kabul edilen Kişisel Verilerin Korunması Kanunu’nda elektronik olarak tapu kayıtlarına erişilebilmesi karşısında elektronik ortamdaki verilerinin toplanması, bunların yetkisiz üçüncü kişilere karşı korunması gerektiği, veri işleme faaliyetinde bulunan kişilerin, veri içeriği hususunda sır saklama yükümlülükleri ve ilgili kişilerin haklarındaki yanlış verileri düzeltme taleplerine yönelik çeşitli düzenlemeler getirilmiştir¹¹.

Kişisel verilerin korunmasına ilişkin İlk ulusal düzenleme ise 1973 yılında İsveç’te çıkarılan Veri Koruma Kanunu’dur¹². Avrupa Parlamentosu tarafından Avrupa Komisyonu’na (*EC - European Commission*) daha önce kabul edilen yasaları kişisel verilerin korunmasına ilişkin düzenlemelere uyumlu hale getirecek bir yönerge önerisi çağrısında bulunulmuş; 1990’a kadar Norveç, Avusturya, Almanya, İsveç, Fransa ve Birleşik Krallık en az bir ülkeye veri akışını engellemiş ya da yasaklamıştır¹³. Yönerge 24 Ekim 1995 tarihinde resmen kabul edilmiş ve üye devletin yerel yasaları uyumlu hale getirmesini gerektiren bir yönerge olarak üç yıl içinde devletler tarafından uygulanmıştır. 2000 yılının Ocak ayında Avrupa Komisyonu, bu yönergenin gerektiği gibi ulusal yasalarına dahil etmeyen üye devletlere (Fransa, Lüksemburg, Hollanda, Almanya ve İrlanda) karşı yasal işlem başlatmıştır. Yönergenin önemli bir yönü, her üye devlette yönergenin şartlarını

¹⁰ Francoise Gilbert, Lisa J. Sotto, Thomas J. Smedinghoff, “Twentieth Annual Institute on Privacy and Data Security Law”, **Practising Law Institute (PLI)**, New York, 2019, s.804.

¹¹ Kişisel Verileri Koruma Kurumu (KVKK), “Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi”, **KVKK Yayınları**, Ankara, 2018, s.11; Fatih Dinkci, “Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği”, Yüksek Lisans Tezi, **Ondokuz Mayıs Üniversitesi**, Samsun, 2014, s.15; Küzeci, **A.g.e.**, s.103.

¹² Berrak Yılmaz, “Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması”, Doktora Tezi, **Hacettepe Üniversitesi**, Ankara, 2019, s.121.

¹³ Joel R. Reidenberg, “Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?”, **Fed. Comm. L. J.**, No.44, 1992, pp.195-243. (Çevrimiçi) <https://pdfs.semanticscholar.org/5f5f/2fd2ff989226bd4a7a0e05c614fd7ad09a18.pdf> 18 November 2019, p.199.

yerine getirmek için bir “kamu otoritesi” veya “ajans” oluşturma zorunluluğu olmuştur.¹⁴

1973 yılında İsveç'te çıkarılan Veri Koruma Kanunu'nu takiben 1970'li yıllarda KVK Hukuku'na yönelik diğer gelişmeler sırasıyla Amerika Birleşik Devletleri (ABD), Kanada, Fransa, Danimarka, Norveç, Avusturya ve Lüksemburg'da gerçekleşmiştir. 1974'te ABD'deki “*Privacy Act*” (Özel Hayatın Gizliliği Yasası) ile kişisel özel alanda korumaya yönelik düzenlemeler yapılmıştır¹⁵. Bunu takiben 1977'de Kanada'da kabul edilen “*Canadian Human Rights Act*” (Kanada İnsan Hakları Kanunu) ile ayrımcılığa dayanan bazı uygulamaların mağduriyet yaratabileceği kişilere eşitlik hakkının sağlanabilmesine yönelik hukuki adımlar atılmıştır¹⁶. Kanada'yı takiben 6 Ocak 1978 tarihinde Fransa'da elektronik ortamda veri işleme, veri dosyaları ve bireysel özgürlüklere ilişkin 78-17 No'lu Kanun kabul edilmiştir¹⁷. Aynı yıl içinde Danimarka (Haziran 1978), Norveç (Haziran 1978) ve Avusturya'da (Ekim 1978) ve sonraki yıl Lüksemburg'da (Mart 1979) da kişisel verileri korumaya yönelik bir takım hukuki düzenlemeler gerçekleştirilmiştir¹⁸.

7 Ekim 1970'de Almanya'nın Hessen Eyaleti'nde kabul edilen Kişisel Verilerin Korunması Kanunu'nu takiben KVK'ya yönelik ilk geniş çaplı ve uluslararası düzenlemeler, esasen 1950'li yıllar itibarıyla konunun önemini gören devletlerin yer aldığı uluslararası organizasyonlar öncülüğünde yapılmıştır. Devletler otoriter rejimlerin veya çok güçlenebilecek şirketlerin demokrasiye ve hukukun üstünlüğüne verebilecekleri zararları göz önünde tutularak dünyanın tümünde benzer bir

¹⁴ Gilbert / Sotto / Smedinghoff, **Ibid.**, p.805.

¹⁵ Nil Melek Gültekin, “Kişisel Verilerin Ceza Hukuku Yönünden Korunması”, Yüksek Lisans Tezi, **Galatasaray Üniversitesi**, İstanbul, 2012, p.xiii.

¹⁶ Kanada İnsan Hakları Komisyonu (CHRC - Canadian Human Rights Commission), “Human Rights in Canada”. (Çevrimiçi) <https://www.chrc-ccdp.gc.ca/eng/content/human-rights-in-canada> 28 September 2019

¹⁷ Avrupa Komisyonu: “Draft Law for a digital Republic Impact assessment”, **Avrupa Birliği**. 2015, November 24. p.1. (Çevrimiçi) <http://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2015&num=627&iLang=EN> 19 November 2019

¹⁸ Colin J. Bennett, “Regulating Privacy: Data Protection and Public Policy in Europe and the United States”, Cornell University Press, Ithaca and London, 1992, p.59 (Çevrimiçi) https://books.google.com.tr/books?id=z6FhDwAAQBAJ&pg=PA59&lpg=PA59&dq=denmark+data+protection+1970%27s&source=bl&ots=scJlhhMOV_&sig=ACfU3U0Ymd_MSaLzMfgMbGedGbBSkCSdww&hl=tr&sa=X&ved=2ahUKEwjZvf3X5YDmAhWtIsKHW2VAE8Q6AEwAnoECAkQAQ#v=onepage&q=denmark%20data%20protection%201970's&f=false 3 November 2019.

istikamet yürütülmesi için ilkeler üzerinden gidilmiştir. Bu ilkeler büyük oranda benzer bir doğrultuda olmuştur. Şeffaflık ve Hesap Verilebilirlik ilkesinin bulunduğu sözleşmeler buna örnek olarak gösterilebilir. Bu bağlamda, Ekonomik İşbirliği ve Kalkınma Örgütü (OECD - Organization for Economic Cooperation and Development)¹⁹ tarafından ilki 1980 yılında yayınlanan ve 2019 yılına dek sadece bir kez (2013 yılında) güncellenen Özel Hayatın Gizliliğinin ve Sınır Ötesi Veri Akışının Korunmasına İlişkin Rehber İlkeler (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)²⁰, kişisel verilerin korunması konusundaki çalışmalarının temel taşı olarak kabul edilmektedir. Ancak KVK Hukuku'nun 4 Kasım 1950'de Roma'da imzaya açılmış olup 3 Eylül 1953'te yürürlüğe girmiş olan Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) (The European Convention on Human Rights)²¹ "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesine dayandığı söylenebilir. Bu konudaki diğer uluslararası düzenlemeler; 28 Ocak 1981'de imzaya açılmış olup Avrupa Konseyi'nin tüm üyeleri tarafından kabul edilen 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, No.108)²² ve 14 Aralık 1990 tarih ve 45/95 sayılı

¹⁹ Yayınlanan ilkelere daha sonradan birçok metin ve düzenlemede atıfta bulunulmasına rağmen hukuken bağlayıcılığı bulunmayan bir rehber mahiyetinde yer almıştır.

²⁰ Ekonomik İşbirliği ve Kalkınma Örgütü (OECD - Organization for Economic Cooperation and Development), "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" OECD (Çevrimiçi) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofprivacyandtransborderflowsofpersonaldata.htm> (1980 version) <http://www.oecd.org/sti/ieconomy/privacy.htm> (2013 version) 20 November 2019.

²¹ Asıl adı İnsan Haklarının ve Temel Özgürlüklerin Korunması Sözleşmesi (The Convention for the Protection of Human Rights and Fundamental Freedoms) olup sözleşmenin İngilizce ve Türkçe versiyonları için bkz. Avrupa İnsan Hakları Mahkemesi (AİHM) (ECHR - European Court on Human Rights), "Avrupa İnsan Hakları Sözleşmesi (AİH) (The European Convention on Human Rights)", 3 September 1953 (Çevrimiçi) https://www.echr.coe.int/Documents/Convention_TUR.pdf (Türkçe tercümesi), https://www.echr.coe.int/Documents/Convention_ENG.pdf (Orijinal versiyonu, İngilizce) 21 Kasım/November 2019.

²² 2001 yılında sözleşmeye eklenen 181 nolu protokol de kabul edilmiştir. Türkiye 108 sayılı Sözleşme'yi 2016 yılında usulüne göre yürürlüğe koymuş ve tarafı olmuştur. Dolayısıyla Anayasanın 90. maddesi 5. fıkrası uyarınca sözleşme kanun hükmündedir. 108+ isimli yenilenen protokol 18 Mayıs 2018 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilmiştir. Ancak bu protokol henüz Türkiye tarafından onaylamamıştır. Avrupa konseyi üyesi olmayan devletler de 108 sayılı Sözleşmeye taraf olabilmektedir. Ayrıca Kişisel verilerin korunması açısından hukuken bağlayıcılığı bulunan ilk metin olma özelliğini taşımaktadır. İlgili sözleşme metni için bkz. Avrupa Komisyonu (EC - European Commission), "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması

Birleşmiş Milletler Genel Kurulu kararı ile kabul edilmiş olan "Guidelines for the Regulation of Computerized Personal Data Files" (Bilgisayarlı Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Yönergeler)²³ olarak sıralanabilir.

KVK'ya yönelik AB tarafından yapılan düzenlemeler; 24 Ekim 1995 tarih ve 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi (*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*)²⁴ ve 7 Aralık 2000 tarih ve 2000/C 364/01 sayılı Avrupa Birliği Temel Haklar Bildirgesi (*The Charter of Fundamental Rights of the European Union*)²⁵ şeklindedir.

KVK Hukuku'na yönelik Türkiye'deki gelişmelere bakıldığında, konuya ilişkin ilk düzenlemelerin 26 Eylül 2004 tarihinde kabul edilerek 12 Ekim 2004 tarihinde Resmî Gazetede yayınlanan ve sonraki yıllarda üzerinde bazı değişiklikler yapılan

Karşısında Bireyin Korunması Sözleşmesi)", **Avrupa Birliği**. 28 January 1981, (Çevrimiçi) <https://rm.coe.int/1680078b37> 19 November 2019.

²³ Birleşmiş Milletler Genel Kurulu (United Nations General Assembly) (45th sess.: 1990-1991): "Guidelines for the Regulation of Computerized Personal Data Files" (Bilgisayarlı Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Yönergeler), 14 Aralık 1990 (Çevrimiçi) <https://www.refworld.org/pdfid/3ddcafaac.pdf> 21 November 2019.

²⁴ 32016R0679 no'lu Yönetmelik ile yürürlükten kaldırılmış olan 24 Ekim 1995 tarihli bu Yönerge'nin son geçerlilik tarihi 24 Mayıs 2018'dir. Yönerge'nin 20/11/2003 tarihli en son konsolide versiyonu için bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), "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 (95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi)", **Avrupa Birliği**. 24 October 1995 (Çevrimiçi) <http://data.europa.eu/eli/dir/1995/46/oj> 23 November 2019. Ayrıca, 27 Nisan 2016 tarihinde kabul edilen ve 25 Mayıs 2018 tarihinde yürürlüğe giren 32016R0679 no'lu Yönetmelik'in yürürlükte olan 4 Mayıs 2016 tarihli en son versiyonu için bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data (GDPR - General Data Protection Regulation) (EU 2016/679 Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Gerçek Kişilerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Düzenlemesi (Genel Veri Koruma Düzenlemesi)), **Avrupa Birliği**. 27 April 2016 (Çevrimiçi) <http://data.europa.eu/eli/reg/2016/679/oj> 23 November 2019.

²⁵ Avrupa Parlamentosu (European Parliament): "The Charter of Fundamental Rights of the European Union (7 Aralık 2000 tarih ve 2000/C 364/01 sayılı Avrupa Birliği Temel Haklar Bildirgesi)", **Avrupa Birliği**, 7 December 2000 (Çevrimiçi) https://www.europarl.europa.eu/chart er/pdf/text_en.pdf 23 November 2019.

Türk Ceza Kanunu'nun (TCK) 135-140. maddelerinde²⁶ yapıldığı görülmektedir. İlgili maddelerde; hukuka uygun olmayacak şekilde; kişisel verilerin kaydını yapan, kişisel verileri başka birine sunan, yayımını sağlayan ya da elde eden, kaydedilmiş kişisel verileri kanunlarda belirtilen süreler içinde yok etme görevi olmasına karşın bunu yerine getirmeyen kişilere verilecek hapis cezasına ilişkin düzenlemeler yapılmıştır. Ayrıca TCK'nın 243-246. maddelerinde bilişim alanındaki suçlara ilişkin KVK'ya ilgilendiren hükümlere de yer verildiği görülmektedir. ilgili maddelerde bahsi geçen suçların gerçekleştirilmesi yoluyla kendisi için haksız çıkar elde eden tüzel kişilere ilişkin onlara özgü güvenlik tedbirlerinin uygulanacağı (Madde 140/I ve Madde 246/I) düzenlenmiştir.

KVK Hukuku'na ilişkin Türkiye'deki bir diğer gelişme, 1982 tarihli Türkiye Cumhuriyeti Anayasası'nın 20. maddesine 12 Eylül 2010 tarihinde eklenen fıkra²⁷ ile gerçekleşmiştir. Bu ek fıkra ile Anayasaya; öncelikli olarak her bireyin kendiyile ilgili olan kişisel verilerin korunmasını isteme hakkının bulunduğu; bu hakkın kapsamının bireyin kendiyile ilgili kişisel verilere ilişkin bilgilendirilmesini, bireyin kişisel verilerine erişebilmesini, bireyin bu kişisel verilere yönelik düzeltme ya da bunların silinmesi taleplerinde bulunabilmesini, bireyin kendiyile ilgili toplanan bu kişisel verilerin kullanımının amaçlarına uygun olup olmadığını öğrenebilmesini içine aldığı, kişisel verilerin işlenebilmesinin yalnızca yasalarda belirtilen durumlarda ya da bireyin açıkça rıza göstermesi halinde mümkün olduğu ve son olarak da KVK'yla ilgili usul ve esasların kanun ile düzenlendiği hükümleri eklenmiştir.

KVK Hukuku'na ilişkin Türkiye'deki son gelişme ise 24 Mart 2016 tarihinde kabul edilerek 7 Nisan 2016 tarihinde Resmî Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)'dur. 6698 sayılı KVKK'nın temel amacı, kişisel veriler işlenirken öncelikli olarak bireylerin özel hayatlarının gizliliğinin korunması başta olmak üzere temel hak ve özgürlüklerinin korunması, kişisel

²⁶ Türk Ceza Kanunu (TCK), Kanun Numarası: 5237, Kabul Tarihi: 26/9/2004, Resmî Gazetede Yayımlandığı Tarih: 12/10/2004 ve Sayı: 25611. 26 Eylül 2004 (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMeti/n/1.5.5237.pdf> 23 Kasım 2019.

²⁷ Türkiye Büyük Millet Meclisi (TBMM): "Türkiye Cumhuriyeti Anayasası", Kanun Numarası: 2709, Kabul Tarihi: 18/10/1982, Resmî Gazetede Yayımlandığı Tarih: 9/11/1982 ve Sayı: 17863. 21/1/2017 tarihli ve 6771 sayılı Kanun ile yapılan Anayasa değişikliklerinin kabul edildiği tarih: 16/4/2017, bu değişikliklerin Resmî Gazetede Yayımlandığı Tarih: 27/4/2017 ve Sayı: 30050 Mükerrer Sayı. 27 Nisan 2017 (Çevrimiçi) <https://www.anayasa.gov.tr/tr/mevzuat/anayasa/> 24 Kasım 2019.

verilerin işlenmesini gerçekleştiren gerçek ve tüzel kişilere yönelik yükümlülükler ve uymaları gereken usul ve esasların düzenlenmesidir²⁸. Bu kanun, KVK'nın düzenlenmesinin yanı sıra aynı zamanda kişisel verilerle ilgilenen kişi veya kurumların uyması gereken birçok yeni zorunluluğu getirmesi yönüyle türünün ilk örneğidir. Bu kanunun kabul edildiği 2016 yılına dek KVK, düzenlenmiş belirli sektörler haricinde Türkiye Cumhuriyeti Anayasasında tek bir hüküm ve TCK'da birkaç hüküm ile düzenlenmişti. Bu hükümlerin hiçbiri giderek daha karmaşık hale gelen teknolojilerin ihtiyaçlarına ve her gün işlenen ve aktarılan kişisel veri miktarlarına yanıt vermede yeterli değildi. Kendisinden önce yürürlükte bulunan mevzuata kıyasla 6698 sayılı KVKK, toplanan ve işlenen sürekli artan kişisel veri hacminin gereksinimlerine cevap vermeyi amaçlayan modern bir kanundur. Bu kanun, Türk mevzuatını AB mevzuatı ile uyumlu hale getirme yönünde önemli bir adımdır ve veri koruma konusunda 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Yönerge'ye dayanarak hazırlanmıştır. 6698 sayılı KVKK, 95/46/EC sayılı Yönerge'ye çok benzemekle birlikte tam bir kopyası değildir. Bu Kanunun 95/46/EC sayılı Yönerge'den farklı olan hükümlerinin bir kısmı, "iyileştirmeler"den ziyade "eksiklikler" şeklinde değerlendirilmektedir²⁹. Nitekim, daha önce de bahsedildiği üzere 95/46/EC sayılı Yönerge, 27 Nisan 2016 tarihinde kabul edilip 25 Mayıs 2018 tarihinde yürürlüğe giren GDPR'nin yürürlükte olan 4 Mayıs 2016 tarihli en son versiyonu ile 24 Mayıs 2018 tarihinde yürürlükten kalkmıştır. Yasa koyucular GDPR ile "kopernik tipi bir devrim" yaparak dokümanlara odaklı ve bürokratik zorunluluk anlayıştan uzaklaşıp pratikte uyum sağlanması ve bireyin güçlenmesine yönüne doğru ulaşmayı hedeflemektedir³⁰. Dolayısıyla 6698 sayılı KVKK'nın GDPR ile getirilen yeni hükümler çerçevesinde güncellenmesi gerekmektedir³¹. Ayrıca, daha önce Türkiye'de bu konuda Anayasa'da tek bir hüküm, TCK'da birkaç hüküm ve TMK'da

²⁸ Kişisel Verilerin Korunması Kanunu (KVKK), Kanun Numarası: 6698, Kabul Tarihi: 24/3/2016, Resmî Gazetede Yayımlandığı Tarih: 7/4/2016 ve Sayı: 29677. 26 Eylül 2004 (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf> 23 Kasım 2019.

²⁹ Ozan Karaduman, "The New Personal Data Protection Law 2019 in Turkey", **Gün + Partners**, 14 February 2019 (Çevrimiçi) <https://gun.av.tr/tr/the-new-personal-data-protection-law-2019-in-turkey/> 24 November 2019

³⁰ Christopher Kuner, "The European Commission's proposed data protection regulation: A copernican revolution in European data protection law", **Bloomberg BNA Privacy and Security Law Report**, February 6, 2012, pp.1-15 (Çevrimiçi) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2162781_code1213479.pdf?abstractid=2162781.&mirid=1 31 December 2019.

³¹ Çalışmanın esas konusu olan GDPR kapsamındaki ilkeler, konseptler, hak ve yükümlülükler bu güncellemenin ne kadar gerekli ve acil olduğunu gözler önüne sermektedir.

kişilik hakları çerçevesindeki hükümler dışında bir düzenleme olmadığı için KVKK'nın toplumun tüm kesimlerini alıştırarak ve veri koruma kültürü oluşturarak üst seviyeye çıkarılması uygun olacaktır. Diğer yandan KVK'ya yönelik yalnızca düzenleme yapılması yeterli değildir. Güvenli bir ülke olabilmek için kanunun eksiksiz bir şekilde uygulanması gerekmektedir.

1.2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BAZI TEMEL KAVRAMLAR, İLKELER VE KONSEPTLER

Bu bölümde KVK'ya ilişkin kişisel veri, özel nitelikli kişisel veri, veri sorumlusu ve veri işleyen, kişisel verilerin hukuki niteliği ve kişisel veri koruma hukukunun sükeleri gibi bazı temel kavramlar, ilkeler ve konseptler ele alınacaktır.

1.2.1. Kişisel Veri

Avrupa Konseyi'nin 108 No'lu Sözleşmesi'nin 2. maddesinin (a) fıkrasında kişisel verinin tanımı; tanımlanmış veya tanımlanabilir bir bireye ilişkin herhangi bir bilgi şeklinde yapılmıştır³². 6698 sayılı KVKK'nın 3. maddesinin 1. fıkrasının (d) bendinde ise kişisel veri; kimliği belli ya da belirlenebilir olan gerçek kişilere yönelik her tür bilgi olarak tanımlanmıştır³³. Örneğin, isim, adres, doğum tarihi, pasaport numarası, ayakkabı numarası, DNA örneği, kredi kartı numarası, favori restoran, cinsel tercihler, uçak yolculuğunun varış yeri, plakalar, sosyal sigorta numarası, görüntü veya ses kaydı, e-posta adresi, hobiler, ortaklıklar gibi bilgiler kişisel verilere örnek gösterilebilir. Açıkça görüldüğü üzere, yaşayan bir bireyi ilgilendiren her türlü bilgi bu tanımın kapsamında olabilir. Bu nedenle kişisel verilerin listesi kolayca genişletilebilir ve çeşitlendirilebilir.³⁴ AB yasalarına göre bir bilgi/veri, belirli bir kişiyi tanımlıyorsa veya verilen bilgilerden/verilerden yola çıkıldığında o kişinin kimliğinin

³² Avrupa Komisyonu (European Commission), **Ibid.**, Article 2/a.

³³ Kişisel Verilerin Korunması Kanunu (KVKK), m.3/I-d.

³⁴ İlke Gürsel, "Protection of Personal Data in International Law and the General Aspects of The Turkish Law", **D.E.Ü. Hukuk Fakültesi Dergisi**, Vol.18, No.1, 2016, pp.33-61, (Çevrimiçi) <http://hukuk.deu.edu.tr/wp-content/uploads/2016/10/İLKE-GÜRSEL.pdf> 10 October 2019.

belirlenmesi önemli düzeyde kolaylaşıyorsa, o bilginin/verinin kişisel bilgi/veri içerdiği, dolayısıyla kişisel veri olarak değerlendirilmesi gerektiği kabul edilir³⁵.

Daha önce veri türlerinin 2'ye ayrıldığına ilişkin giriş yapmıştık. Bunu biraz daha açıp *Information Accountability Foundation*'ın yapmış olduğu 4'lü taksonomiye değineceğiz. Bunlar³⁶:

- Kişi tarafından paylaşılmış veriler (*provided data*), bilinçli bir şekilde paylaşılan veriler, formdaki kutucukların doldurulması gibi,
- Gözlemlemeyle elde edilen veriler (*observed data*), otomatik olarak kaydedilen veriler, online çerezler (*cookies*) veya sensörler veya CCTV bağlanmış yüz tanıma sistemleri aracılığıyla toplananlar gibi,
- Türetilen veriler (*derived data*), kişinin diğer verilerinden daha basit ve düz bir yöntemle üretilen veriler, müşterinin mağazayı ziyaret sayısı ve aldığı ürünlere ilişkin sayılardan müşteri karlılık oranının hesaplanması gibi
- Çıkarım yapılarak üretilen veriler (*inferred data*), daha kompleks analitik yöntemler kullanılarak veri setleri arasında ilişkinin bulunması ve bu kategorilerle de kişileri profilleyerek üretilen veri türüdür, kredi skorlarının hesaplanması veya sağlığının geleceğinin tahmin edilmesi gibi. Bu veri türleri ihtimallere dayandırılmakta ve türetilen verilere nazaran daha az kesinlik arz etmektedir.

1.2.2. Özel Nitelikli Kişisel Veri

Bireyler bir takım kişisel özellikleri ve bu özelliklere ilişkin bilgilere kolay erişilebilmesi nedeniyle toplumun çeşitli kesimlerinde ayrımcılığa maruz kalabilirler. Bu ayrımcılıklar iki grupta toplanabilir. Bunlardan ilki ırk, doğum yeri, inanç gibi kişinin statik yani değişmez ya da değişmesi zor olan bilgileri nedeniyle uğradığı

³⁵ Council of Europe, "Handbook on European Data Protection Law - 2014 Edition", p. 39, (Çevrimiçi) https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf 11 October 2019.

³⁶ Martin Abrams, "The Origins of Personal Data and its Implications for Governance", **The Information Accountability Foundation**, 2014, (Çevrimiçi) <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf> 31 December 2019.

ayrımcılıklardır. İkinci grup ayrımcılıklar ise yeme alışkanlığı, uyuma, dışarıya çıkma, konum verileri, arama motoru kullanımı, çerezler aracılığıyla tespiti gezinti yapılan web siteleri, sosyal medya hesaplarında takip edilenler, arkadaşlar ve iletişim kurulan kişiler gibi kişinin dinamik yani değişken ya da değişmesi kolay olan verileri sebebiyle uğradığı ayrımcılıklardır.³⁷

İşte bu noktada da özel nitelikli KVK önem kazanmaktadır. Özel nitelikli kişisel veri, öğrenildiğinde söz konusu bireye ilişkin ayrımcılığa ya da mağduriyete yol açabilecek özellikteki bilgiler olduğundan bu tür verilerin diğer kişisel verilerle kıyaslandığında daha iyi korunması gerekmektedir³⁸. Nitekim gerek GDPR’de gerekse 6698 sayılı KVKK’da özel nitelikli kişisel veriler hassas bilgiler olarak kabul edilmiş ve bunlara özel bir önem verilerek ayrı bir düzenlemeye gidilmiştir.

GDPR’nin 9. maddesinde ırksal veya etnik kökene işaret eden kişisel veriler, siyasal görüşleri ortaya koyan kişisel veriler, dini veya felsefi inançları açığa çıkaran kişisel veriler, sendika üyeliğini ortaya koyan kişisel veriler, genetik veriler, biyometrik veriler (tanımlama amacıyla kullanıldığı yerlerde), sağlıkla ilgili veriler, bir kişinin cinsel yaşamına ilişkin veriler ve bir kişinin cinsel yönelimi ile ilgili veriler özel nitelikli veriler olarak kabul edilmiştir³⁹. Benzer şekilde 6698 sayılı KVKK’da özel nitelikli kişisel verilere ayrı bir önem verilerek bunlar kıyas yoluyla genişletilemeyecek şekilde dar ve sınırlı bir kapsamda tanımlanmış ve bu verilerin tanımı ve işleme şartlarına ilişkin 6. maddede ayrı bir düzenleme getirilmiştir.

³⁷ Genel nitelikteki verilerden, özel nitelikli kişisel veri mahiyetinde çıkarımlar ve türetmeler yapılabilir. Yeme alışkanlığından obezite veya uyuma ve konum verilerinden spor yapmasına bakılarak sağlığına ilişkin yorumlama, aradığı kelimelerden gezdiği sitelerden de yine siyasi görüşü, dini inancı, satın aldığı ürünlerden hastalığı olduğu google tarafından etiketlenebilir. Polonya merkezli dijital haklar üzerine çalışan sivil toplum kuruluşu Panoptikon Vakfı’nın Polonya Veri Koruma Otoritesine yaptığı çevrimiçi reklam açık arttırma sistemine ilişkin (ad auction) şikâyetinde Google’ın hukuka aykırı bir şekilde internet kullanıcıları dini inançları, etnik kökenleri, hastalıkları, engelleri ve cinsel yönelimleri açısından nasıl profilelediğini gözler önüne sermektedir. Daha da ötesinde; ensest veya istismar mağduru, yeme bozukluğu, sol görüşlü, scientology dinine mensup gibi şirketin kendi ürettiği kategorilerde kişilerin profilelediği ortaya konmuştur (bkz. Johnny Ryan, “Update on GDPR complaint (RTB ad auctions)”, **Brave Insights**, Jan 28, 2019, (Çevrimiçi) <https://brave.com/update-rtb-ad-auction-gdpr/> 31 December 2019).

³⁸ Kişisel Verileri Koruma Kurumu, “Özel Nitelikli Kişisel Verilerin İşleme Şartları”, 2018, s.1, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari> 12 Ekim 2019.

³⁹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 9**, pp.38-39.

6698 sayılı KVKK'nın 6.maddesinin I. fıkrasında; ırk, etnik köken, siyasi görüşler, dini ve felsefi inançlar, mezhep ya da diğer inançlar, giyim tarzı, bir derneğe, vakıfa veya sendikaya üyelik durumu, sağlık, cinsel hayat, herhangi bir cezadan mahkûmiyet yaşıyıp yaşamadığı ve güvenlik tedbirleri ile ilgili verilerin yanı sıra genetik ve biyometrik veriler, özel nitelikli kişisel veriler arasında sıralanmıştır. İlgili maddenin II. fıkrasında göre özel nitelikli kişisel verilerin kişiden açık rıza alınmadan işlenebilmesi kanunen yasak sayılmakla birlikte III. fıkarda bu tür verilerin kanunlarda belirtilen sınırlı hallerde açık rıza olmaksızın işlenebileceği de eklenmiştir. Buna göre; I. fıkarda belirtilen cinsel hayata ve sağlığa ilişkin olanlar haricindeki kişisel veriler, kanunlarda belirtilen sınırlı hallerde açık rıza olmaksızın işlenebilmektedir. Yine III. fıkarda geçen hükümlere göre cinsel hayat ve sağlıkla ilgili kişisel veriler de yalnızca kamu sağlığını koruma, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım gibi sağlık hizmetlerinin yürütülmesinde, sağlık hizmetlerinin ve sağlık finansmanının planlanmasında ve yönetiminde, sır saklama yükümlülüğüne sahip kişiler ya da yetkili kurumlar/kuruluşlarca kişiden açık rıza alınmadan işlenebilecektir. 6. maddenin IV. ve son fıkrasında ise özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kişisel Verileri Koruma Kurulu'nca belirlenmiş/belirlenecek olan yeterli tedbirlerin alınması şart koşulmuştur.⁴⁰

Anlaşılabacağı üzere diğer temel hak ve özgürlüklerin korunmasında mevcut bulunan sınırlı durumlar, özel nitelikli kişisel veriler için de geçerlidir. Diğer yandan bu verilere ilişkin sınırlamalarda Türkiye Cumhuriyeti Anayasası'nın 13. maddesindeki esasların dikkate alınması gereklidir. Bu maddeye göre temel hak ve özgürlüklere ilişkin sınırlamaların Anayasanın çeşitli maddelerinde geçen sebeplere bağlı olarak ve kanunla gerçekleştirilebileceği⁴¹ belirtilmiştir. Diğer yandan pek çok temel hak ve özgürlüğün kullanılmasında, özel nitelikli kişisel verilerin işlenmesi zorunlu olmaktadır. Bundan dolayı da bu tür verilerin işlenmesinde mutlak yasaklığın geçerli olması söz konusu değildir.⁴²

1.2.3. Veri Sorumlusu ve Veri İşleyen

⁴⁰ KVKK, m.6.

⁴¹ TBMM, **a.g.e.**, m.13, s.3.

⁴² Kişisel Verileri Koruma Kurumu, "Özel Nitelikli Kişisel Verilerin İşlenme Şartları", 2018, s.2.

6698 sayılı KVKK'nın 3. maddesinin 1. fıkrasının (ı) bendinde “veri sorumlusu”, (ğ) bendinde ise “veri işleyen”in tanımları yapılmıştır. Bu maddelere göre veri sorumlusu; kişisel verileri işlemede amaç ve araçları belirleyen, verilerin kayıt sistemini kurma ve yönetmeden sorumlu gerçek ya da tüzel kişi olarak tanımlanmaktadır. Veri işleyenin tanımı ise; veri sorumlusu tarafından verilen yetki dahilinde ve veri sorumlusu adına kişisel verilerin işlenmesi fiilini gerçekleştiren gerçek ya da tüzel kişi⁴³ şeklinde yapılmıştır. Veri sorumlusu ve veri işleyene ilişkin yukarıda geçen tanımların, GDPR'nin 4. maddesinin 7 ve 8. fıkralarında geçen tanımlarla⁴⁴ aynı olduğu görülmektedir.

İster kamu hukuku ister özel hukuk çerçevesinde olsun bir farklılık gözetilmeksizin tüzel kişiler, kişisel verilerin işlenmesine ilişkin faaliyetlerinde doğrudan veri sorumluları olarak kabul edilirler⁴⁵. Diğer yandan veri sorumlusu ve veri işleyen görevleri aynı gerçek ya da tüzel kişide toplanabilir. Buna örnek olarak bir muhasebe şirketinin kendi personeline yönelik kaydettiği veriler kapsamında “veri sorumlusu”, müşterilerine yönelik kaydettiği veriler kapsamındaysa “veri işleyen” sayılması gösterilebilir. Ancak bir şirkette verilerin işlenmesine ilişkin faaliyetler çerçevesinde belgelerin teslim alınması ve kaydedilmesi işlemlerini yapan kişi “veri sorumlusu” sayılmaz, burada veri sorumlusu sıfatı şirketin kendisine ait olur.⁴⁶

Kişisel verileri işlemede amaç ve araçları belirleyen kişi olan veri sorumlusu⁴⁷, verilerin işlenmesi fiilinin nasıl ve niçin yapılacağına yönelik soruların yanıtını verebilecek kişidir.⁴⁸ Diğer yandan veri sorumlusu tarafından kendi yetkisinde olan bu konulardaki karar alma yetkisinin ayrı bir sözleşmeyle veri işleyene bırakması da mümkündür⁴⁹.

⁴³ KVKK, m.3.

⁴⁴ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 4**, p.33.

⁴⁵ Kişisel Verileri Koruma Kurumu, “Veri Sorumlusu Kimdir”, 2017, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir> 14 Ekim 2019.

⁴⁶ Kişisel Verileri Koruma Kurumu, “Veri Sorumlusu ve Veri İşleyen”, 2018, ss.1-4, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf> 14 Ekim 2019.

⁴⁷ Küzeci, **a.g.e.**, s.15.

⁴⁸ Kişisel Verileri Koruma Kurumu, “Veri Sorumlusu Kimdir”.

⁴⁹ Kişisel Verileri Koruma Kurumu, “Veri Sorumlusu ve Veri İşleyen”, 2018, s.3.

Veri sorumlusunun hakkında veri topladığı kişileri aydınlatma, verilerin güvenliğini sağlama, Veri Sorumluları Sicili'ne (VERBİS) kaydolma ve veri işleme faaliyetlerine ilişkin beyanlar verme, hakkında veri toplanan kişilerin taleplerine yanıt verme ve Kişisel Verileri Koruma Kurulu'nun şikâyet ya da ihlal iddiası sonucu verdiği hukuka aykırılıkların giderilmesine yönelik kararlarını uygulama gibi yükümlülükleri bulunmaktadır.⁵⁰

Veri sorumlusunun aydınlatma yükümlülüğü, temel olarak 6698 sayılı KVKK'nın 10. maddesinde düzenlenmiş olup veri sorumlusunun ya da yetkilendirdiği kişinin, hakkında veri toplanan kişilere sorumlusunun ya da yetkilendirdiği kişinin kimliği, verilerin toplanma ve işleme amacı, verilerin kimlere ve ne gerekçelerle verilebileceği, verilerin toplanmasında kullanılan yöntem ve bunların hukuki dayanakları ve son olarak da yine 6698 sayılı KVKK'nın 11. maddesinde geçen hakkında bilgi toplanan kişinin ne gibi hakları olduğuna yönelik bilgi verme yükümlülüğü bulunmaktadır. İlgili kişinin bu hakları 11. maddede; kişisel veri işlenip işlenmediği, işleniyor ise bunlara yönelik bilgi verilmesi, bu verilerin hangi amaçla işlendiğini ve işlenmesinin amaca uygun olup olmadığını öğrenme, varsa bu bilgilerin aktarıldığı yerli ve yabancı kişileri öğrenme, bu verilerin yanlış işlenmesi durumunda düzeltilmelerini isteme, aynı kanunun 7. maddesinde belirtilen şartlar doğrultusunda bu verilerin silinmesini ya da yok edilmesini talep etme, düzeltme, silme ve yok etme işlemlerinin ilgili üçüncü şahıslara da iletilmesini sağlama, verilerin işlenmesi sırasında özellikle otomatik sistemlerle analizinde ortaya çıkabilecek ilgili kişinin aleyhine olacak sonuçlara itirazda bulunma, bu verilerin kanuna uygun olmayan yol ve yöntemlerle işlenmesinden kaynaklı zararların giderilmesini isteme şeklinde sıralanmıştır.⁵¹ Veri sorumlusunun aydınlatma yükümlülüğü, Kişisel Verileri Koruma Kurumu tarafından hazırlanarak 10.03.2018 tarihinde Resmi Gazetede yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği'nde yer alan 8 madde⁵² ile de ayrıca düzenlenmiştir.

⁵⁰ Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu Kimdir".

⁵¹ Kişisel Verilerin Korunması Kanunu (KVKK), m.10-11.

⁵² Kişisel Verileri Koruma Kurumu: "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği", 2018, Resmi Gazetede Yayımlandığı Tarih: 10.03.2018 ve Sayı:30356, (Çevrimiçi)
https://www.resmigazete.gov.tr/eskiler/2018/03/2018031_0-5.htm (16 Ekim 2019).

1.2.4. Kişisel Verinin Hukuki Niteliği

Bu bölümde kişisel verinin hukuki niteliği öncelikle genel anlamda, ardından mülkiyet hakkı ve kişilik hakkı görüşleri çerçevesinde ele alınacaktır.

1.2.4.1. Genel

KVKH, klasik anlamda Roma hukuku zamanından ortaya çıkan ve kara Avrupası sisteminde takip edilen özel ve kamu hukuku sisteminden ayrı olarak üçüncü bir ayırım olarak ortaya çıkan karma hukuk sistemi içerisinde yer almaktadır. Dolayısıyla bazı yönleriyle özel hukuktan, bazı yönleriyle ise kamu hukukundan özellikler taşımaktadır.⁵³

Kişisel Verilerin Korunması Hakkı (KVKH), tarihsel süreçte yer alan birçok temel hak ve özgürlükle yakından ilişkilidir. Bunlar arasından başta gelenler özel hayatın gizliliği ve insan onurudur. Bunlara ek olarak ifade özgürlüğü, bilgi edinme hakkı ve haberleşme özgürlüğü gibi bazı temel hak ve özgürlüklerin de zaman zaman KVKH'yı destekledikleri zaman zaman da bu hakka ters düştüğü görülmektedir.⁵⁴ Dolayısıyla tarihsel süreçte bu hakkın hangi temel hak ve özgürlükler kapsamında değerlendirilmesi gerektiği konusunda farklı görüşler oluşmuştur. Ancak yaygın olan görüş, temel insan haklarından biri olarak kabul edilen özel hayatın gizliliği kapsamında değerlendirilmesi gerektiği yönündedir. Diğer yandan bu hakkın günümüzde daha değerli hale gelmesi nedeniyle ekseriyetle ABD başta olmak üzere birçok ülkede KVKH'nın mülkiyet hakkı kapsamında değerlendirilmesi gerektiğine yönelik görüşlere de rastlanmaktadır.⁵⁵

Bu bağlamda, KVKH, aşağıda, mülkiyet hakkı ve kişilik hakkı görüşleri çerçevesinde incelenecektir.

⁵³ Furkan Güven Taştan, "Türk Sözleşme Hukukunda Kişisel Verilerin Korunması", Onikilevha Yayınları, İstanbul, 2017, s.8.

⁵⁴ Küzeci, **a.g.e.**, s.58.

⁵⁵ Sinem Göçmen-Uyarer, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması", Seçkin Yayınları, Ankara, 2019, s.23.

1.2.4.2. Mülkiyet Hakkı Görüşü

Kişisel verilerin hukuki niteliğine ilişkin tartışmalar içinde sıkça eleştiriye maruz kalan görüşlerin başında KVKH'nın mülkiyet hakkı⁵⁶ çerçevesinde değerlendirilmesi gerektiğine ve bireylerce serbestçe üzerinde tasarruf edilebilecek, alınıp satılabilecek, kiralanabilecek bir hak olarak görülmesi gerektiğine yönelik görüşlerdir⁵⁷. KVKH'nın mülkiyet hakkı çerçevesinde kabul görmesi gerektiği görüşüne sahip olan yazarlar tarafından bu konu farklı açılardan savunulmaktadır. Bu bağlamda, birtakım yazarlarca KVKH'nın mülkiyet hakkı çerçevesinde kabul görmesinin, kişisel verilerine ilişkin ellerinden alınan hakları bireylere tekrar verebileceği veya bireylerin verileriyle olan doğal bağlarını onaylamayı sağlayacağı savunulmaktadır. Ayrıca ABD hukuk sistemi ve siyasi sisteminin doğal kısıtlamalarının ve sınırlandırmalarının üstesinden gelinebilmesinde yegâne çözümün bireylerin kişisel verileri üzerindeki mülkiyet haklarının verilmesiyle sağlanabileceği⁵⁸ yönündedir. Tüm bu görüşler arasında en fazla tartışma konusu olan, KVKH'nın mülkiyet hakkı çerçevesinde kabul görmesi yaklaşımının hukuktaki ekonomik analize dayandığı görüşüdür⁵⁹. Esas olarak bu husustaki ekonomik analiz, kişisel verilerin yeni bir değer ve güç odağına dönüşmesiyle yakından ilişkilidir.

⁵⁶ Mülkiyet hakkının gerek modern anayasalar gerekse Ulusalüstü İnsan Hakları Hukuku'nda (UIHH) (*Supra-national Human Rights Law*) birçok belge içinde temel insan haklarından biri olarak yer bulduğu görülmektedir. Anayasalar dışında bakıldığında, EİHB'nin 17. maddesi, Amerikan İnsan Hakları Sözleşmesi'nin (Ame.İHS) (*ACHR - American Convention on Human Rights*) 21. maddesi ve Afrika İnsan ve Halkların Hakları Şartı'nın (AİHHŞ) (*ACHPR - African Charter on Human and Peoples Rights*) 14. maddesi mülkiyet hakkının yer aldığı insan hakları belgelerindendir (Adı geçen belgeler için bkz. Haydar Burak Gemalmaz, "Avrupa İnsan Hakları Sözleşmesinde Mülkiyet Hakkı", Beta Yayınları, İstanbul, 2009, ss.3-6). Ayrıca, Türkiye'nin de taraf olduğu AİHS'nin 1 No'lu Protokolü'nde mülkiyet hakkına ilişkin düzenlemeler bulunmaktadır (Haydar Burak Gemalmaz, "Avrupa İnsan Hakları Sözleşmesi Açısından Mülkiyet Hakkının Sınırlanmasında "Adil Denge" İlkesi", İÜHFM, Cilt.19, Sayı.1-2, 2011, ss.649-674).

⁵⁷ İbrahim Korkmaz, "Kişisel Verilerin Ceza Hukuku Kapsamında Korunması", Seçkin Yayıncılık, Ankara, 2017, s.78.

⁵⁸ ABD'nin yaklaşımı, KVKH'nın mülkiyet hakkı kapsamında korunması gerektiği görüşünü desteklemektedir. Ancak son zamanlardaki California'daki düzenleme ve beklenen federal düzenleme ile bu görüşte bazı değişikliklere gidilmesi muhtemel görünmektedir.

⁵⁹ Nadezhda Purtova, "Property Rights in Personal Data: Learning from the American Discourse" *Computer Law & Security Review*, Vol.25, No.6, 2009, s.507 (Çevrimiçi) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1554341_code1337775.pdf?abstractid=1554341&mirid=1 (27 November 2019).

Bunun da ötesinde kişisel veriler, çağımızın en değerli varlıklarından biri olarak görülmektedir⁶⁰.

Çağımızda ekseriyetle dev işletmelerin başı çektiği sayısız kamu ve özel kurumu/kuruluşunun gerek sermaye gerekse güç açısından en değerli varlıkları arasında bu işletmelerce müşterilerden veya kullanıcılardan toplanan veriler gelmektedir. Bu öyle bir noktaya ulaşmıştır ki bazı işletmeler veri toplamada ve işletmede üstesinden gelemedikleri maliyetleri minimize edebilmek adına, bu tür verilere kendi veri bankalarında sahip olan işletmelerden satın alma yoluna gitmektedirler.⁶¹ Bir diğer deyişle, kendi veri bankasında bu tür bilgilere sahip olan işletmeler kendi ticari faaliyetlerinden elde ettikleri kârlara ek olarak bu verilerden de kazanç sağlamaktadırlar.

KVKH'nın bir mülkiyet hakkı olarak kabul edilmesi görüşüne göre, bu tür verilerin 2000'lerle birlikte önemini daha da artırdığı, yeni bir ekonomik/maddi değer⁶² gibi kabul edildiği ve ekseriyetle ABD gibi ülkelerin bu değer artışından kazanç sağlamaya çalıştığı görülmektedir⁶³. ABD ve AB ülkeleri arasında KVK'ya yönelik önemli farklılıklar bulunmaktadır⁶⁴. ABD'de yasaların KVK konusunda yetersiz kaldığı ve verilerin güvenliğine ilişkin sık ihlaller yaşandığı, AB Adalet Divanı'nca (ABAD) (*CJEU - Court of Justice of the European Union*) da kabul edilmektedir⁶⁵. Nitekim KVKH, ABD'de anayasal haklardan olmayıp⁶⁶, temel haklar

⁶⁰ Kişisel verilerin çağımızın en değerli varlıklarından biri olan petrol olarak değerlendirildiği haber için bkz. The Economist, "Regulating the internet giants - The world's most valuable resource is no longer oil, but data", 6 May 2017, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (25 November 2019).

⁶¹ Purtova, *Ibid.*, p.509.

⁶² Kişisel verilerin çağımızın bir para birimi olarak değer görmesi gerektiğine yönelik haber için bkz. Irene Ng, "Personal Data as Currency", 28 July 2018, (Çevrimiçi) <https://medium.com/hub-of-all-things/personal-data-as-currency-ab1590163ad6> (25 November 2019).

⁶³ Paul M. Schwartz, "Property, Privacy and Personal Data", **Harvard Law Review**, Vol.117, 2004, p.2056 (Çevrimiçi) <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3150&context=facpubs> (12 November 2019). Schwartz'a göre ABD'de kişisel verileri metalaştırmaya yönelik sağlam bir görüş ortaya çıkmış ve bu sürece ABD vatandaşları da katılmaya başlamıştır.

⁶⁴ Elif Mendos-Kuşkonmaz, "Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması", Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul, 2013, s.19.

⁶⁵ AB'nin KVK'ya yönelik yaptığı birçok düzenlemede, veri güvenliği yeterli olmayan ülkelere AB ülkelerinden veri transfer edilmesi yasaklanmaktadır ki ABD'de bu yasaklı ülkeler arasında yer almaktadır. Nitekim dünyanın hemen hemen her ülkesinde ABD'yle ticaretin

ve özgürlükler arasında korunmamakta, kişisel verilerin korunmasının sağlanabilmesinde sektörel yaklaşımlara⁶⁷ başvurulmaktadır. Buna örnek olarak ABD’de ekseriyetle finansa ve sağlığa ilişkin sektörlerde işlenen kişisel verilerin miktarca yüksek olması nedeniyle her iki sektöre yönelik kanun maddeleri arasında kişisel verilerin korunmasıyla ilgili hükümlere de yer verildiği görülmektedir⁶⁸. Şüphesiz bu hükümlerin, kişisel verilerin korunmasındaki genel sistematik yaklaşıma uygun ve yeterli kapsamda oldukları söylenemez. AB ülkeleri ve Kıta Avrupa Hukukunun uygulandığı ülkelere bakıldığında KVK’nın temel hak ve özgürlükler arasında korunduğu ve bu bağlamda kişisel verilerin doğuştan kazanılan bir insan hakkı olduğunun, ticaretinin yapılamayacağını ve devredilemeyeceğinin kabul edildiği görülmektedir⁶⁹ ki bu görüş bir sonraki bölümde ele alınacaktır.

Öte yandan KVK’nın bir mülkiyet hakkı olması gerektiği görüşünü benimseyen yazarlarsa, AB ülkelerinde ve AB’nin düzenlediği sözleşmelerde bile KVKH’nın bir temel hak ve özgürlüklerden sayılmadığını, AİHM kararlarında KVKH’nın AİHS’nin “Özel ve aile hayatına saygı hakkı (*Right to respect for private and family life*)” başlıklı 8. maddesi⁷⁰ çerçevesinde korunduğunu öne sürmektedirler.⁷¹ Gemalmaz’a göre AİHS kapsamında KVKH, mülkiyet hakkı çerçevesinde temel mülk türlerinden Gayri Maddi Nesne’ye (*Res incorporales*) dayanmaktadır. Gayri maddi, yani maddi olmayan nesneler, fiziksel olarak bir karşılığa sahip değildir; yani bu nesneler birer hak objesidirler. Bu bakımdan bu değerler, kural gereği devredilmeye ve/veya mirasla intikal edilmeye elverişlidirler.

sahip olduğu yüksek önem ve elektronik ticarete en büyük işletmelerin ABD menşeli olmasından dolayı, ABD’yle veri transferi yapılabilmesine yönelik imzalanmış olan Safe Harbour sözleşmesi ABAD tarafından verilen bir kararla geçersizleştirilmiştir (Göçmen-Uyarer, **a.g.e.**, s.29).

⁶⁶ Viktor Mayer-Schonberger, "Beyond Privacy, Beyond Rights- Toward a Systems Theory of Information Governance", *California Law Review*, Vol.98, 2010, p.1857, (Çevrimiçi) <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1058&context=californialawreview> 27 November 2019.

⁶⁷ Atul Singh, "Protecting Personal Data as a Property Right ", *ILI Law Review*, Winter Issue, 2016, p.126, (Çevrimiçi) http://ili.ac.in/pdf/p9_atul.pdf 4 November 2019; Samuelson, Pamela, "Privacy as Intellectual Property", *Stanford Law Review*, Vol.52, 1999, p.1126, (Çevrimiçi) <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3137&context=facpubs> 4 November 2019.

⁶⁸ Atul, **Ibid.**, p.126.

⁶⁹ Göçmen-Uyarer, **a.g.e.**, s.26.

⁷⁰ AİHM (ECHR), **a.g.e.**, m.8.

⁷¹ Purtova, **Ibid.**, pp.520-521; Küzeci, **a.g.e.**, ss.64-98; Göçmen-Uyarer, **a.g.e.**, s.29.

Bu mülk türünün alt kategorilerinden fikri mülkiyet hakkı,⁷² teknolojinin gelişiminin yarattığı yeni fikri mülkiyet sorunları çerçevesinde yeni yaklaşımlar gösterilmesini gerektirmekte olup 1990'lar itibarıyla uluslararası niteliğini güçlendirmiştir. Nitekim fikri mülkiyetin AİHS'nin 1 No'lu Protokolü kapsamında değerlendirilebileceğine yönelik ilk kararın, Avrupa İnsan Hakları Komisyonu'nca (AİHK) (*European Commission of Human Rights*) 1994'te alınan A.D.v. Netherlands'a ilişkin karardır⁷³.

Gemalmaz'a göre bazı kişisel verilerin, fikri mülkiyetin alt kategorilerinden "siber mülkiyet" ve "sanal mülkiyet" kapsamında, bazılarının ise AİHS'nin 8. maddesi kapsamında korunması mümkündür. Şöyle ki; hak ve özgürlüklerin yarışması teorisine göre, veri tabanı ve e-posta gibi bir kısım sanal mülkiyet türlerinde sözleşme doğrultusunda mülkiyet hakkı yerine özel hayatın gizliliğinin korunması hakkı, daha işlevsel olabilir. Örneğin, e-posta ya da kişisel verilerin depolandığı bazı veri tabanlarında yetkisi olmayan üçüncü kişiler tarafından okuma fiilinin işlenmesi halinde, KVK bağlamında mülkiyet hakkı çerçevesinde konuya uygunluk ve nitelik bakımından AİHS'nin 8. maddesinde geçen özel ve aile hayatına saygı hakkının işlevselliği daha öne çıkacak; yani, e-posta ya da kişisel verilerin depolandığı bazı veri tabanlarındaki KVK'da AİHS'nin 8. maddesinin uygulanabilirliği öncelikli olacaktır⁷⁴. Diğer yandan Gemalmaz, kişi ve/veya kurumlara ait web sitelerine yönelik gerçekleştirilen hack saldırılarında ise AİHS'nin 1 No'lu Protokolü'ndeki mülkiyet hakkının gayet işlevsel olabileceğini düşünmektedir⁷⁵.

Purtova'ya göre, KVKH'nın diğerlerinden bağımsız olarak kendi başına temel hak ve özgürlüklerden biri olduğuna yönelik AİHM'nin gerek kamu gerekse özel

⁷² "Fikri mülkiyet" veyahut Türk eşya hukukunda geçtiği haliyle "fikri haklar", ekonomik bir değere sahip olmaları nedeniyle anayasal mülkiyet hakkı kapsamına girmektedir. AİHM'nin içtihatlarındaki fikri mülkiyetin AİHS'nin 1 No'lu Protokolü kapsamında korunması, uzun bir geçmişe sahiptir (Haydar Burak Gemalmaz, "Mülkiyet Hakkı: Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 6", **Avrupa Konseyi**, Ankara, 2018, s.36).

⁷³ Bkz. A.D.v. Netherlands, App. No.21962/93, Admissibility Decision of 11 January 1994, DR Vol.76-A, March 1994, pp.157-163 (Haydar Burak Gemalmaz, "Avrupa İnsan Hakları Sözleşmesinde Mülkiyet Hakkı", Doktora Tezi, **İstanbul Üniversitesi**, İstanbul, 2008).

⁷⁴ bkz. Van der Velden v. Netherlands, App. No.29514/05, Admissibility Decision of 7 December 2006, para.2 (The Law); ayrıca bkz. S. and Michael Marker v. the United Kingdom, App. Nos.30562/04-30566/04, Admissibility Decision of 16 January 2007; ayrıca bkz. Nos.30562/04-30566/04, Admissibility Decision of 16 January 2007; Genel olarak bkz. Andrew Roberts & Nick Taylor, "Privacy and the DNA Database", EHRLR, 2005, No.4, pp.373-392 (Gemalmaz, **a.g.e.**, 2008, s.260).

⁷⁵ AİHS'de mülkiyet hakkına ilişkin daha fazla bilgi için bkz. Gemalmaz, **a.g.e.**, 2008.

sektörü içine alan bir ifadesi bulunmamakta; bunda AİHS'nin yalnızca imzalayan devletleri yükümlü kılan bir sözleşme olma özelliğinin etkisi bulunmaktadır⁷⁶. Bununla ilgili Samuelson, Aksoy ve Prins gibi yazarlarca⁷⁷, bireylere KVKH'dan feragat edebilmelerini sağlayacak bir sözleşme serbestisi verilmesi gerektiği savunulmaktadır. Bu görüşe göre, özel sektörde zaten kişisel verilerin işlenmesi söz konusu olduğundan, kişisel verilerine ilişkin bireylerin mülkiyet hakkının olması gerektiği, ayrıca bireylerce kişisel verilerinin değerlerinin belirlenmesiyle satılabileceği, bu sayede bireyler için de bu verilerinden kazanç sağlanabileceği, işleme amaçlı parayla kişisel veri satın alan işletmelerinse doğal olarak bu hususa daha fazla dikkat gösterecekleri belirtilmektedir.⁷⁸

Özetlemek gerekirse, kişisel verilerin mülkiyet olarak kabul edilmesi halinde alınıp satılabilmesi ve ardından verinin ilk başta öngörülme amaçla başka birine devri veya bunun korunmasını takip etme yükünün malikine verilmesi söz konusudur. Bahsi geçen tüm bu görüşleri bir arada değerlendirdiğimizde, KVK'nın mülkiyet hakkı çerçevesinde değerlendirilmesinin isabetli olmayacağı, öyle yapılması halinde ise yalnızca kamu ve özel sektör sermayelerine fayda sağlayacağı anlaşılmaktadır. Tabi ki çağımızda ekseriyetle elektronik ticarete satışları arttırmak amacıyla müşteri alışkanlıklarının belirlenmeye çalışılması veya sosyal medyada kullanıcıların siyasi eğilimlerine ilişkin fikir edinilmeye ve bu eğilimlerin yönlendirilmeye çalışılması sayesinde bu veriler önemli bir ekonomik değere kavuşmuştur⁷⁹. Bu verilerin ekseriyetle internetin bireylerin hayatında yer almaya

⁷⁶ Purtova, **Ibid.**, pp.520-521; AİHM'nin aksi yöndeki bir kararı için bkz. *Arzte für das Leben v. Austria* kararı, No.10126/82, 17.11.1985. Bu karara göre bireylerin, özel kişilerin gerçekleştirebilecekleri müdahalelere karşı AİHS'nin 8. maddesinde belirtilen haklarının korunması devletin sorumluluğundadır. Buna göre AİHS, sözleşmeyi imzalayan devletler için bağlayıcı olsa da AİHM, bireylerin özel kişilere veya kuruluşlara karşı korunmasında devletlere yüklediği birçok yükümlülük bulunmaktadır (A. Şeref Gözübüyük, & Feyyaz Gölcüklü, "Avrupa İnsan Hakları Sözleşmesi ve Uygulaması", Turhan Kitabevi, Ankara, 2009, s.333).

⁷⁷ Samuelson, **Ibid.**, p.1131. Ayrıca bkz. Hüseyin Can Aksoy, "Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması", Çakmak Yayınevi, Ankara, 2010, ss.58-59. Ayrıca bkz. Corien Prins, "Property and Privacy: European Perspectives and the Commodification of Our Identity", Information Law Series, Vol.16, 2006. p.232.

⁷⁸ Göçmen-Uyarer, **a.g.e.**, s.26.

⁷⁹ ABD'deki yakın tarihli seçimler, KVK'nın ne derecede önemli olduğunu bir kez daha gözler önüne sermiştir. 2018'de politik ve stratejik danışmanlık şirketi Cambridge Analytica'ya yönelik olarak, Facebook kullanıcıları tarafından yüklenen bir uygulama yoluyla kullanıcıların ve arkadaş listesindekilerin profil bilgileri ve kullanıcı geçmişi bilgilerine ulaşıldığı, bu yolla şirketin yaklaşık 87 milyon Facebook kullanıcısının kişisel bilgilerine ulaştığı, bu bilgileri de işletmenin 2016'daki ABD Başkanlık seçiminde Donald Trump'ın lehine etki edecek şekilde

başladığı 1990'lı yıllar itibariyle değerini artırdığı hatta çağın petrolü olarak adlandırıldığı göz önünde bulundurulduğunda, toplumun fertlerinin gerek kamu gerekse özel sektör kurum ve kuruluşlara karşı geçmişte olduğundan daha çok korunmaya muhtaç olduğu görülmektedir. Hiç şüphesiz bireyler, kendilerine ait bilgilerin kaderini belirleme hakkına sahip olmalıdırlar⁸⁰. Diğer yandan devletin de bireylerin bu hakkını korumak amacıyla düzenlemeler yapması zorunludur. Yoksa bireylerin bu yöndeki özgür iradesi kısıtlanmış ve bu irade devlet ve sermaye tarafından kullanılmış ve/veya yönlendirilmiş olacaktır⁸¹.

1.2.4.3. Kişilik Hakkı Görüşü

Haklara ve borçlara sahip olabilen varlıklara kişi denilmektedir⁸². Kişilik hakkı, fiziksel, duygusal ve sosyal kişilik değerlerinin üzerinde sahip olunan hak olduğu şeklinde ifade edilmektedir. Kişilik hakkı, kişinin insan olması nedeniyle doğuştan kazandığı, mirasla intikal etmeyen, devredilemeyen veya haczedilemeyen, kişinin manevi çıkarlarını gözetken bir hak⁸³, olarak tanımlanmaktadır. Kişisel verilerin korunması hakkını Kıta Avrupası ve Türk hukuku temel hak ve hürriyetler çerçevesinde ele alıp bir insan hakları hukuku çerçevesinde değerlendirmiştir. Bu açıdan KVK, insan onurunun sağlanması için korunan kişiliğin serbestçe geliştirilmesi hakkına dayanmaktadır.

Anayasa'nın 5. maddesi de insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamayı devletin temel amaç ve görevleri arasında saymıştır. Devlet sadece bireylerin haklarını ihlal etmemesini gerektiren negatif yükümlülüğü açısından değil aynı zamanda bireylerin haklarını korumak için gerekli tedbirleri alması gerektiğini düzenleyen pozitif yükümlülük açısından da sorumludur. Devlet, kişisel verilerin korunmasının hakkının korunabilmesi amacıyla yasal, idari, mali,

kullandığı iddiaları, gerek Facebook gerekse anılan işletme hakkında bir soruşturma başlatılmasına neden olmuştur (Göçmen-Uyarer, **a.g.e.**, s.29; detaylı bilgi için bkz. James Sanders & Dan Patterson, "Facebook data privacy scandal: A cheat sheet", 24 July 2019, (Çevrimiçi) <https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/> 20 November 2019.

⁸⁰ Schwarz, **Ibid.**, p.2087.

⁸¹ Mendes-Kuşkonmaz, **a.g.e.**, s.21; Ayrıca bkz. Küzeci, **a.g.e.**, s.65.

⁸² Jale Akipek, Turgut Akıntürk, Derya Ateş, "Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku", **Beta Yayınları**, İstanbul, 2018. s. 237.

⁸³ Öykü Özyürek, "Kişilik Haklarına Saldırı Nedeniyle Manevi Tazminat", **İstanbul Bilgi Üniversitesi**, İstanbul, 2019, s.11.

yargısal ve diğer önlemleri almak zorundadır⁸⁴. Bu nedenle Anayasa ve AİHS kapsamında, kişisel verilerin korunmasının gereği olarak devlet pozitif yükümlülükleri gereği koruma tedbirlerini almalıdır.

Diğer bireylerden veya kurumlardan gelebilecek saldırıları engelleme adına gerekli önlemleri almak zorundadır. Özellikle kurumların kişisel verileri işlerken veya korurken yaptıkları çalışmaları yakından takip edip, denetleyerek ve düzenleyerek insan hakları yönüyle belirli güvenceler getirmelidir. Kişisel verilerin korunması alanındaki özel düzenlemelerden kaynaklı bireylerin de farklı hakları bulunmaktadır. Ancak teknolojinin gelişimiyle birlikte daha da karmaşık hale gelmesi, bireylerin hakları aktif bir şekilde kullanmasını ve anlamasını beklemek çok güçleştirmiştir.

KVKH, AB ülkeleri ve Kıta Avrupa Hukukunun uygulandığı ülkeler tarafından uzun yıllardır bir insan hakkı olarak görüldüğünden, kişilik hakkı görüşünü desteklemektedir. KVKH, AİHS’de bulunan özel hayatın ve aile yaşamının gizliliğine yönelik 8. madde, BM Evrensel İnsan Hakları Beyannamesi’nin (EİHB) (*UDHR - Universal Declaration of Human Rights*) 17. maddesi, BM Bireysel ve Siyasal Haklar Şartı’nın 12. maddesi doğrultusunda, özel hayatın gizliliği çerçevesinde, bunların yanı sıra Avrupa Birliği Temel Haklar Şartı ve bazı AB ülkelerinin Anayasa metinleri gibi birçok yeni metinde KVKH’nın özel hayatın gizliliği hakkında bağımsız olarak da ayrı bir şekilde temel haklardan kabul edilerek korunmaktadır. Bu yönde Avrupa İnsan Hakları Mahkemesi’nce (AİHM) verilmiş birçok karar bulunmaktadır. Özel hayatın gizliliğinin yanı sıra KVKH, ifade özgürlüğü, unutulma hakkı, insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı, bilgi edinme hakkı, özel haberleşmenin gizliliği, bilim özgürlüğü gibi birçok insan hak ve özgürlüğüyle yakından ilişkilidir.⁸⁵ Kişisel verilerin korunması hakkının ilk olarak Federal Almanya Anayasa Mahkemesi’nin 1983 senesindeki kararında insan onuru ile kişiliğin serbestçe geliştirilmesi hakkı ile ilişkilendirildiği görülmektedir⁸⁶. Mahkeme, hakları

⁸⁴ Bernadette Rainey, Elizabeth Wicks, Clare Ovey, “Jacobs, White and Ovey: the European Convention on Human Rights”, **Oxford University Press**, Oxford, 2017. p.102.

⁸⁵ Küzeci, **a.g.e.**, ss.64-98; Göçmen-Uyarer, **a.g.e.**, s.29.

⁸⁶ Küzeci, Elif: “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, **İnsan Hakları Yıllığı**, Cilt.32, 2014, ss.53-54, (Çevrimiçi) https://www.academia.edu/37176330/%C4%B0statistik%C3%AE_Birimler_ve_Bilgilerin_Gelece%C4%9Fini_Belirleme_Hakk%C4%B1_Statistical_Units_and_Right_to_Informational_Self-Determination 31 Aralık 2019.

beraber değerlendirip “bilgilerin geleceğini belirleme hakkı”⁸⁷ tanımlamıştır. Bireyin kendisi hakkındaki hangi bilgilerin elde edildiği ve bu bilgilere kimlerin sahip olduğunu bilememesi halinde özgür ve bilinçli bir şekilde karar alabilmesi çok mümkün değildir. Özellikle çalışmamızda ileride işleyeceğimiz otomatik karar alma sistemleri kapsamında profiller üzerinden okuyacağı haberin, arkadaş olacağı kişilerin, vatandaşlık puanına bağlı olarak kamu veya özeldeki işe layık olup olmadığının belirlenmesi yukarıda sayılan haklara tehdit oluşturmaktadır.

KVKH’nın bir diğer hakla olan ilişkisi de algoritmik sistemler aracılığıyla devlet kaynaklarının toplumun ve yaşanan coğrafyaların gelir seviyesi analiz edilerek dağıtılmasıyla sosyal güvenlik hakkı açısından çeşitli sorunlara neden olmasıdır. Seçme ve seçilme hakkına müdahale edildiğine ilişkin kanıtlar, demokrasinin de kişisel verilerin korunmasıyla ilişkisini ortaya koymaktadır.⁸⁸

1.3. YAPAY ZEKÂLİ SİSTEMLER

Bu bölümde zekâ, yapay zekâ ve yapay zekâli sistemlerin tanımı, yapay zekâli sistemlerin türleri ve kullanım alanları ele alınacaktır.

⁸⁷ Doktrinde “bilginin kendi kaderini tayin hakkı” olarak da geçen bu terim, Almandaca “*Informationelles Selbstbestimmungsrecht*”, İngilizcede “*Self-Determinasyon*” olarak geçmektedir.

⁸⁸ 2010 ABD seçimlerinde 61 milyon facebook kullanıcısına, her bir profil grubuna göre özelleştirilen mesajların iletilmesi özgürce bilgi edinme hakkını, oy verme hakkını ve seçimlerin eşit şartlarda yürümesi ilkelerini ihlal etmiştir. Ayrıca mesajlar sadece alan kişileri değil onların arkadaşlarını ve arkadaşlarının arkadaşlarını da etkilemiştir. Bu durum, seçim dönemindeki yakın arkadaşlarla ilişkiler ve aralarındaki sosyal ilişkiler sebebiyle mesajların etkisinin ötesinde sonuçlar doğurmuştur (bkz. Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle, James H. Fowler, “A 61-million-person experiment in social influence and political mobilization”, *Nature*, Vol.489, No.7415, 2012, pp.295–298). Google, Netflix, Youtube gibi öneri (*recommendation*) sistemiyle çalışan platformlarda kişinin karşısına hep aynı doğrultuda içeriklerin çıkması bir dayatma olarak görülebilir. Bireylerin düşünce ve fikir hürriyetine baskı yapılması filtre baloncukları veya yankı odaları olarak ifade edilen konseptlerin toplumda polarizasyona, ırkçı fikirlerin gelişmesine ve güçlenmesine katkı sağlaması yönüyle üzerinde dikkatle durulması gereken diğer bir husustur.

1.3.1. Tanımı

Yapay zekâ ve yapay zekâlı sistemlerin bir tanımını yapabilmek için öncelikle bu tanımla ilişkili olan insan zekâsı ya da daha basit bir ifadeyle zekânın tanımlanmasında fayda bulunmaktadır.

Ebbinghaus'a göre zekâ, fikirlerin düzenlenmesi ve temsil ettikleri nesnel gerçeklerin doğal ilişkileri nedeniyle üniter bir gruba girmesi gereken tüm bu fikirlerin birbirine bağlanmasıdır. O'na göre zekânın temeli ne yalnızca "hafıza" ne de yalnızca "dikkat"e dayanır; zekâ, hafıza ve dikkatin bir araya getirilmesiyle meydana gelir.⁸⁹ Zekâ, gerçeğin keşfedilmesine hizmet eder ve bireyin çevresine en iyi şekilde adapte olmasıyla kendini gösterir⁹⁰. Zekâ, ilişkileri görme ve problem çözme yeteneğini kullanma becerisidir⁹¹. Stanovich'e göre zekâ, akılcı bir şekilde düşünmeyi ve davranmayı, kişinin amaçları ve inançları doğrultusunda elindeki imkanlara uygun eylemlerde bulunmayı gerektirir. Bu nedenle zekâ, pratik ilişkiler alanındaki en uygun davranış olup bireyin hedeflerine en optimum düzeyde ulaşmasına yardımcı olur.⁹²

Yapay zekâ⁹³'nin Oxford Advanced Learner's Dictionary ve Oxford Advanced American Dictionary'deki aynı olan İngilizce tanımının Türkçe karşılığı "bilgisayarların zeki insan davranışlarını taklit etmesini sağlamakla ilgilenen bir çalışma alanı"⁹⁴ şeklindedir. Winston'a göre yapay zekâ; algılamayı, akıl yürütmeyi

⁸⁹ Hermann Ebbinghaus, "Psychology: An Elementary Text-book", M.F. Meyer (Ed.). **Heath**, Boston, 1908.

⁹⁰ Alfred Binet & Théodore Simon, "The development of intelligence in children (the Binet-Simon scale)", In H.H. Goodard (Ed.), **Williams & Wilkins**, Baltimore, 1916.

⁹¹ David Fontana, "Psychology for Teachers", **Macmillan**, London, 1988.

⁹² Keith E. Stanovich, "Assessing Cognitive Abilities: Intelligence and More", Journal of Intelligence, Vol.2, No.1, 2014, pp.8–11, (Çevrimiçi) http://www.keithstanovich.com/Site/Research_on_Reasoning_files/Stanovich_JOI.pdf 27 November 2019.

⁹³ Yapay zekâ ifadesini tarihte ilk defa 1956 yılında Dartmouth konferansında John McCarthy kullanmıştır (Rockwell Anyoha, "Can Machines Think?", **Harvard University**, (Çevrimiçi) <http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/> 31 Aralık 2019).

⁹⁴ Oxford Advanced Learner's Dictionary & Oxford Advanced American Dictionary, "artificial intelligence", (Çevrimiçi) <https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence?q=artificial+intelligence> 13 November 2019.

ve harekete geçmeyi mümkün kılan bir hesaplama çalışmasıdır⁹⁵. Fogel ise yapay zekâyı bir sistemin davranışlarını hedeflerine ulaşmayı sağlayacak şekilde çeşitli ortamlara uyarlama yeteneği şeklinde tanımlamıştır⁹⁶. Zekanın özü, yetersiz bilgi ve kaynaklarla çalışırken çevreye uyum sağlama ilkesidir. Buna göre, akıllı bir sistem sonlu işlem kapasitesine güvenmeli, gerçek zamanlı olarak çalışmalı, beklenmeyen işlere açık olmalı ve deneyimlerden ders almalıdır.⁹⁷ Bu çalışma tanımına göre zekânın, göreceli bir rasyonellik şekli olarak yorumlandığı görülmektedir.

Yapay zekâ sistemleri, genel olarak karmaşık bir amaç verilen ve verilen bu hedefe ulaşmak için çevrelerini veri toplama yoluyla algılayarak, toplanmış yapılandırılmış veya yapılandırılmamış verileri yorumlayarak, bu verilerden elde edilen bilgiyi düşünerek ve en iyi önlemleri almaya karar vererek fiziksel veya dijital ortamda hareket eden yazılım (ve muhtemelen donanım) sistemleridir. Ortamın önceki eylemlerinden nasıl etkilendiğini analiz ederek davranışlarını uyarlamayı öğrenmek amaçlı da tasarlanabilen YZ sistemleri; bilimsel bir disiplin olarak, makine öğrenmesi (derin öğrenme ve güçlendirme öğrenimi), makine mantığı/sorgulaması (planlama, zamanlama, bilgi sunumu ve muhakeme, arama ve optimizasyon dahil), robotik (kontrol, algı, sensörler ve aktüatörlerin yanı sıra diğer tüm tekniklerin siber-fiziksel sistemlere entegrasyonu dahil) gibi yaklaşım ve teknikleri kapsamaktadır.⁹⁸ Dolayısıyla gerek yapay zekâyı gerekse YZ sistemlerine yönelik bu tanımlar, bu sistemlerinin temel çalışma prensibine ilişkin genel yapıyı ortaya koymaktadır.

⁹⁵ Patrick Henry Winston, "Artificial Intelligence", Addison-Wesley Publishing Company, 1992, (Çevrimiçi) <https://courses.csail.mit.edu/6.034f/ai3/rest.pdf> 27 November 2019.

⁹⁶ David B. Fogel, "Defining Artificial Intelligence. In Evolutionary Computation: Toward a New Philosophy of Machine Intelligence", The Institute of Electrical and Electronics Engineers, Inc., **IEEE Press**, 2006.

⁹⁷ Pei Wang, "What Do You Mean by 'AI'?", In P. Wang, B. Goertzel, and S. Franklin (Eds.), Artificial General Intelligence 2008, Proceedings of the First AGI Conference, Frontiers in Artificial Intelligence and Applications, No.171, pp.362–373. IOS Press Amsterdam, **The Netherlands**, 2008, (Çevrimiçi) https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf 27 November 2019.

⁹⁸ Francesca Rossi, "A Definition of AI: Main Capabilities and Scientific Disciplines", **High-Level Expert Group on Artificial Intelligence**, 22 March 2019, (Çevrimiçi) http://www.pcci.gr/evpeimages/0101_F483.pdf 30 November 2019.

Birleşik Krallık Bilgi Komiserliği Ofisi (ICO - Information Commissioners Office), yapay zekâlı sistemlerin KVKK'yı ilgilendiren yönlerini şu şekilde sıralamıştır⁹⁹:

1. Algoritma kullanması,
2. Veri işlemenin opaklığı,
3. Bütün veriyi toplamaya olan eğilimi,
4. Başlangıçtaki veri işleme amacının sonradan değiştirilmesi,
5. Yeni veri türlerinin kullanılması

1.3.2. Türleri

Yapay zekâlı sistemlerin başlıca türleri üç grupta toplanabilir. Bunlar:

- Makine Öğrenimi (Machine Learning)
- Gözetimli ve Gözetimsiz Öğrenme (Supervised and Unsupervised Learning)
- Derin Öğrenme (Deep Learning)

1.3.2.1. Makine Öğrenimi

Verileri işleyip yeni model (*pattern*) ve bilgi (*knowledge*) elde eden, veri ile ilgili etkili tahmin yapılmasında kullanmak için modeller üreten herhangi bir metodoloji veya tekniğe makine öğrenimi denilmektedir¹⁰⁰.

Makine öğreniminin tarihsel gelişimine baktığımızda 5 temel yolun izlendiği görülmektedir. Bunlar; “*symbolists*”, “*connectionists*”, “*evolutionaries*”, “*bayesians*” ve “*analogizers*”. Tarihsel açıdan ilk başta daha çok tercih edilen yöntem olan sembolist yöntemi; “*knowledge*” kavramı ile anılmakta, sisteme eldeki tüm verinin ve

⁹⁹ Birleşik Krallık Bilgi Komiserliği Ofisi (ICO - Information Commissioner's Office), “Big Data, Artificial Intelligence, Machine Learning and Data Protection”, September 4, 2017, (Çevrimiçi) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> 31 December 2019.

¹⁰⁰ Van Otterlo, Martijn: “A Machine learning view on profiling”, In M. Hildebrandt, and K. de Vries (Eds.), Privacy, Due Process and the Computational Turn - The Philosophy of Law Meets the Philosophy of Technology, pp. 41–64, 2013, (Çevrimiçi) https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf 27 November 2019.

çıkarılan sonuçların girilmesiyle geriye dönük olarak çıkarım yapılması ve boşlukların doldurulmasına denilmektedir. “*connectionists*”, öğrenme kavramı ile anılmakta, insan beyninin çalışma stilini ve prensiplerinden yararlanarak sistemi tasarlayan, derin öğrenme yöntemi ile tanınmış olan yoldur. Özellikle görüntü tanıma ve çeviri yapma alanında çok kullanılmaktadır. Diğer yollar çok tercih edilmemesi nedeniyle üzerinde durulmayacaktır.¹⁰¹

Makine öğrenimi karar almaya ilişkin kuralların otonom bir şekilde tanımlanması ve değiştirilmesi kapasitesine sahip olma şeklinde de ifade edilmektedir. Algoritmalar sınıflandırma yapısına veya modele yeni girdiler sağlayabilmektedir. Örneğin; Görüntü tanıma sistemleri (*image recognition systems*) görüntüdeki objenin hangi türden olduğuna karar verebilmektedir.

Algoritmalar yeni girdilerin (*inputs*) nasıl sınıflandırılacağına belirlenmesine ilişkin kuralların tanımlanmasıyla öğrenebilme faaliyetini gerçekleştirirler. Algoritmaların karar almayı öğrenebilmesi için iki farklı yöntem bulunmaktadır.

1.3.2.2. Gözetimli ve Gözetimsiz Öğrenme

Daha önceden etiketlenmiş (labeled) veri setleri aracılığıyla yapılan öğrenim şekline gözetimli öğrenim (Supervised Learning) denilmektedir. Makine öğreniminin iki aşaması bulunmaktadır; eğitim aşaması ve uygulama aşaması. Eğitim aşamasında; eldeki etiketlenmiş veri setiyle algoritma besleniyor ve bir model elde ediliyor. Kedi fotoğraflarının, algoritmanın beslenmesi sonucunda kedilerin görüntülerine ilişkin piksel örüntüleri (pattern) tespit edip bir model çıkarmasıdır. İkinci aşama olan uygulama aşamasında; yeni bir veri setini modele yüklediğinizde istediğiniz çıktıyı almanızı sağlayacaktır. Eğer yüklediğiniz görseller kuş fotoğrafıysa bunun kedi fotoğrafı olmadığını söyleyecektir.

Yüz tanıma, kanser teşhisi ve otonom araçlar gibi görüntü tanımaya ilişkin alanlarda, Siri Alexa gibi sanal asistanlar veya chatbotlarda kullanılan konuşmanın tanınması yöntemlerinde, Google araması yaparken veya bir siteye girildiğinde yapılan otomatik tamamlama tahminlerinde, Google aramalarında ve Facebook

¹⁰¹ Pedro Domingos, “The Master Algorithm: How The Quest For The Ultimate Learning Machine Will Remake Our World”, **Basic Books**, New York, 2015.

veya Instagram'ın ana sayfasında kullanılan sıralama sisteminde, Netflix, Spotify, Youtube ve Amazon'daki tüm öneri sistemlerinde bu yöntem kullanılmaktadır. İnsanların görme, duyma, yazma ve gerekçelendirme kabiliyetlerinin yukarıda sayılan sistemlerde taklit edildiğini görebilmekteyiz.

Gözetimli öğrenim ile eğitilmiş algoritmaların yaptığı genellemelerin ve tahminlerin daha isabetli olabilmesi sistemin daha fazla veri ile beslenmesiyle mümkün olmaktadır. Bu durum da kişisel verilerin korunması hukukunu yakından ilgilendirmektedir.

Daha önceden etiketlenmemiş veri setindeki en uygun modeli (pattern) veya karakteristik özellikleri (feature) önceden girilen kural setlerine göre tespit eden öğrenim şekline de gözetimsiz öğrenim (Unsupervised Learning) olarak ifade edilmektedir¹⁰².

Az bir miktarda etiketlenmiş veri setiyle etiketlenmemiş veri setinin desteklenmesiyle yapılan öğrenim şekline yarı gözetimli öğrenim (Semi-supervised Learning) denilmektedir. Yapay zekâyı ajan (agent) olarak adlandırıp deneme yanılma yöntemi ile en isabetli kararı verdiğinde geri dönüş yapılarak algoritmayı ödüllendirme sistemiyle eğiten yonteme de pekiştirmeli öğrenim (Reinforcement Learning) denilmektedir.¹⁰³

Çalışmamızda incelenecek hususlar açısından önemli olan noktalardan birisi, sistemi kullanan insanın algoritmalar tarafından alınan kararların arkasında yatan mantığı anlamasına gerek bulunup bulunmamasıdır¹⁰⁴.

¹⁰² Bart W. Schermer, "The limits of privacy in automated profiling and data mining", **Computer Law & Security Review**, Vol.27, No.1, 2011, pp. 45–52, (Çevrimiçi) <https://www.infona.pl/resource/bwmata1.element.elsevier-a860e641-825f-3a79-9385-b2b5af42c740> 31 December 2019.

¹⁰³ Isha Salian, "Supervize Me: What's the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning", August 2, 2018, (Çevrimiçi) <https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/> 31 December 2019.

¹⁰⁴ Matthias, Andreas: "The responsibility gap: Ascribing responsibility for the actions of learning automata", **Ethics and Information Technology**, Vol.6, No.3, 2011, pp.175–183 (Çevrimiçi) <https://link.springer.com/article/10.1007/s10676-004-3422-1> 31 December 2019.

Algoritmaların öğrenme kapasitesinin kendilerine belirli bir seviyede otonomi kazandırdığı söylenebilir. Sonuç olarak algoritmaların gerçekleştirecekleri görevlerin önceden tahmin edilebilmek (yeni girdiyi nasıl değerlendireceği) veya sonradan açıklayabilmek (belirli bir kararı nasıl verdiği) güç olmaktadır. Söz konusu belirsizlik nedeniyle algoritmaların tasarlanması ve uygulamaya alınması konusunda etik, hukuki ve sosyal endişeler ve güçlükler daha fazla ele alınır hale gelmiştir.¹⁰⁵

1.3.2.3. Derin Öğrenme

Derin öğrenme, halihazırda kullanılan en gelişmiş makine öğrenimi yöntemi olarak kabul edilmektedir. Derin öğrenme, çok yüksek hacimde veri ile beslenen insan beynindeki nöronların yapısından ilham alınarak oluşturulan yapay sinir ağları ile tasarlanmış birden çok gizli katmanı bulunan insanın bilgiyi öğrenme ve işleme şeklinin taklit edildiği bir yöntemdir.¹⁰⁶

1.3.3. Kullanım Alanları

Geçmişte filmlerde, bilim kurgu romanlarında ve diğer medya yayınlarında gösterilen tüm yaşam alanlarının dijitalleşmesi temsili, çağımızda tek tek gerçeğe dönmeye başlamıştır. Bireylerin hemen hemen her gün faydalandıkları birçok teknolojik cihaz, bilgisayarlar, akıllı cep telefonları, internete bağlı diğer cihazlar, sanal gerçeklik, artırılmış gerçeklik, sesli asistanlar (Siri, Alexa, Echo vb.), yüz tanıma (facial recognition) sistemleri, bilgisayar kontrollü makineler, otonom araçlar, robot makineler, robot insanımsılar, ev otomasyon sistemleri, tavsiye sistemleri, özellikle İnternet üzerinden insan kullanıcılarla konuşmayı simüle etmek için tasarlanmış bilgisayar programları (chatbots) gibi teknolojiler gün geçtikçe insan davranışlarını daha fazla kopyalayarak ve insan hatalarını minimize ederek daha fazla bilgiyi daha hızlı analiz etmeye, internete bağlı diğer şeylerle daha fazla bilgi alış verişinde bulunmaya başlamıştır.

¹⁰⁵ Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, & Luciano Floridi, "The ethics of algorithms: Mapping the debate", **Big Data & Society**, Vol.3, No.2, 2016, pp.1-21.

¹⁰⁶ Martín Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, Li Zhang, "Deep learning with differential privacy", Conference Paper, **2016 ACM SIGSAC Conference on Computer and Communications Security**, Vienna, Austria, October 24-28, 2016, (Çevrimiçi) <https://dl.acm.org/citation.cfm?id=2978318> 31 December 2019.

İşlenen ve işlenebilecek bilginin fazlalığı Büyük Veri¹⁰⁷ (Big Data) ve veri madenciliği¹⁰⁸ gibi alan ve mesleklerin doğmasına vesile olmuş, bilginin değeri artmış, buna karşılık gerek özel gerekse devlet kuruluşlarınca üzerlerinden birtakım çıkarlar elde edilebileceği fark edilen bu büyük veriler korunmaya daha açık hale gelmiş ve bu da hem genel olarak verilerin hem de kişisel verilerin korunması sorununu ortaya çıkarmıştır. Devlet bireyleri daha fazla ve daha kolay kontrol altında tutabilmek ve toplum düzenini sağlamak adına özellikle yapay zekâlı sistemlerin kullanıldığı parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, retina tarama, DNA tanıma gibi güvenlik sistemleri başta olmak üzere bireylerden daha fazla kişisel bilgi toplamaya başlamıştır. Özel sektör kuruluşları ise gerek bilgisayar yazılımları ve bireylere ilgili ve ihtiyaç duydukları alanlarda belirli bir hizmet sunan web sayfaları gerekse cep telefonlarındaki çeşitli uygulamaları kullanma karşılığında kamera ve ses erişimi, bilgisayar ve cep telefonlarında bireyin fiziksel konum bilgisi, sosyal ağlarda bağlantılar, arkadaş ve ilişkilere yönelik kişisel verileri toplamaya devam etmektedir. Sunulan hizmetleri kullanmak isteyen bireyler adeta kullanım karşılığı bedel olarak kişisel verilerini sunmak zorunda kalmaktadırlar.¹⁰⁹

Tüm bu baş döndüren teknoloji içinde özellikle yüz tanıma sistemleri, yapay zekâlı sistemlerin kullanımında ırkçı ayrımcı pratiklerin ortaya çıktığı bir alan olarak dikkati çekmektedir. Özellikle KVKH'nın en çok göz ardı edildiği ülkelerden biri olan

¹⁰⁷ Yapay zekâ ile Büyük Veri de sıklıkla birbirinin yerine kullanılmaktadır. Büyük Veri Gartner tarafından; “gelişmiş bilgi, karar alma ve süreç otomasyonu sağlayan düşük maliyet, inovatif bilgi işleme yöntemleriyle elde edilen çok hacimli, çok hızlı ve çok çeşitli bilgi kaynakları” şeklinde tanımlanmıştır (bkz. Gartner, “Information Technology, Gartner Glossary, Big Data”, (Çevrimiçi) <http://www.gartner.com/it-glossary/big-data> 31 December 2019).

¹⁰⁸ Veri madenciliği, toplanan verilerden anlamlı bilgiler elde etmek, veri setlerinde bulunan örüntüleri ve eğilimleri belirleyip ve çeşitli değişkenler arasındaki bağlantıları tespit etmek ve profiller ve davranışsal yönelimler çıkarmak ve bu şekilde kişilerin veya toplumların gelecekteki davranma biçimlerini tahmin ederek kurum veya kuruluşlar tarafından alınacak kararlara destek sağlamak amacıyla uygulanan yöntemlere denilmektedir (Bkz. Chris Rygielskia, Jyun-Cheng Wang, David C. Yen, “Data mining techniques for customer relationship management”, **Technology in Society**, Vol.24, No.4, 2002, pp. 483–502 (Çevrimiçi) <https://www.sciencedirect.com/science/article/pii/S0160791X02000386?via%3Dihub> 31 December 2019).

¹⁰⁹ Facebook, Google gibi şirketlerin teknoloji şirketi olarak adlandırılmasının sorunlu olduğu, bilgi brokerları veya hükümetin gözetim sağlamada kullandığı ajanlar olarak adlandırılarak toplumsal kabul görmesinin yaptıklarının sonuçları ve hesap verilebilirliği açısından daha uygun olacağı ifade edilmiştir (Bkz. Anil Dash, “There is no “technology industry””, August 19, 2016, (Çevrimiçi) https://anildash.com/2016/08/19/there_is_no_technology_industry/ 31 December 2019).

ABD'deki sivil toplum kuruluşları hem devlete hem de büyük sosyal medya şirketlerine karşı bu konuda hukuki girişimlerde bulunmuş ve bulunmaya devam etmektedirler. KVKH'yı bir anda tüm dünyanın gündemine açıkça oturtması nedeniyle buna en önemli örnek olarak, daha önce de bahsi geçen Cambridge Analytica davası gösterilebilir. 2018'de ABD'de politik ve stratejik danışmanlık şirketi Cambridge Analytica'ya yönelik olarak, Facebook kullanıcıları tarafından yüklenen bir uygulama yoluyla kullanıcıların ve arkadaş listesindekilerin profil bilgileri ve kullanıcı geçmişi bilgilerine ulaşıldığı, bu yolla şirketin yaklaşık 87 milyon Facebook kullanıcısının kişisel bilgilerine ulaştığı, bu bilgileri de işletmenin 2016'daki ABD Başkanlık seçiminde Donald Trump'ın lehine etki edecek şekilde kullandığı iddiaları üzerine gerek Facebook gerekse anılan işletme hakkında bir soruşturma başlatılmıştır.¹¹⁰ Yine daha önce bahsedildiği üzere 2019 yılında Çin ve İngiltere'de yaşanan olaylar, son yıllarda gözetim sağlayan yeni teknolojilere yönelik gizlilik ve veri güvenliği konularında yaşanan olumsuzluklar (veri sızıntıları) olarak ortaya çıkmış ve dünya genelinde KVK'ya yönelik kaygı yaratmıştır. 2019 yılı Şubat ayında, güvenlik uzmanları tarafından yapılan bir kontrolde Çin'in Silikon Vadisi olarak tanınan Shenzhen şehrindeki bir yüz tanıma ve güvenlik yazılımı şirketi olan SenseNets'in korunmasız bir veritabanından yaklaşık 2,6 milyon kişinin 6,7 milyon civarındaki kişisel verilerini (kimlik kartı numarası, yayın ve bitiş tarihi, cinsiyet, uyruk, adres, doğum günü, pasif resim, işveren ve son 24 saat içinde bulunulan konumlar gibi) içeren ciddi bir veri sızıntısı olduğu tespit edilmiştir¹¹¹. 2019 yılı Ağustos ayında, yüz tanıma bilgisi ve parmak izi gibi biyometrik bilgiler de dahil olmak üzere 1 milyondan fazla kişinin kişisel verileri, İngiliz polisi, savunma sanayi şirketleri ve bankalar tarafından kullanılan kamuya açık bir veri tabanında bulunmuştur¹¹². Özellikle biyometrik bilgilerin neredeyse değişmediği ve veri sızıntısının sonuçlarının şiddetli ve uzun yıllar boyunca etkili olabileceği göz önüne alındığında, bu ve benzeri¹¹³ kişisel veri ihlallerinin mağdurlara çok büyük zararlar verme ihtimali bulunmaktadır.

¹¹⁰ Göçmen-Uyarer, **a.g.e.**, s.29; detaylı bilgi için bkz. Sanders & Patterson, **Ibid.**

¹¹¹ Gevers, **Ibid.**

¹¹² Taylor, **Ibid.**

¹¹³ Çin'deki yüz tanıma sistemleri, vatandaş skorlama sistemi, ABD'de polis teşkilatlarının kullandığı yüz tanıma sistemi gibi.

Kişisel veri toplamada yapay zekâlı sistemlerin kullanımında yaşanan olumsuzluklar sonucunda bireylerin özel hayatlarına yönelik hak ihlalleri, yukarıdaki bu örneklerle sınırlı değildir. Örneğin; İngiltere Mahkemesi'nin polis tarafından canlı yüz tanıma (LFR: Live Facial Recognition) teknolojisinin kullanımı hakkında verdiği bir kararda veri toplanması ve işlenmesinin yasal olduğuna hükmetmiştir. Dava, bazı İngiliz polislerin, bilinmeyen şüphelilerin görüntülerini geçmişteki suçlarla eşleştirme ve uluslararası rugby maçları gibi büyük olayları izlemede yüz tanıma teknolojisini kullanmasının KVKK'yı ihlali ettiği gerekçesiyle açılmıştır. İngiliz polisince insanların yüzleri canlı Kapalı Devre Kamera sistemi ("Closed Circuit Television" veya "CCTV") yayınlarından alınmış ve gerçek zamanlı olarak aranan kişilerin biyometrik bilgileriyle karşılaştırılan biyometrik yüz bilgilerini elde etme amaçlı işlenmiştir. Davacı, uygulamanın hedefsiz ve spekülatif olduğunu ve polisin uygun bir veri koruma etkisi değerlendirmesi yapamadığını savunmuştur. Mahkeme, izleme listelerinin sadece iyi bir nedenle bulunması gereken insanlara yönelik olarak hazırlanmış olduğuna ve işlemlerin veri sorumlusunun meşru çıkarları için gerekli olduğuna karar vermiştir. Mahkeme'ye ayrıca, her maddi zamanda işlemin ilgili bir değerlendirme tarafından desteklendiğini gösteren "Gizlilik Etki Değerlendirmesi (Sürüm 4)" adlı bir belge gösterilmiştir. Bu nedenle işlemin yasal kabul edilmiştir. Ancak ICO, bu teknolojinin kullanımının polise olan güveni baltalama potansiyeli olduğunu vurgulayarak karar hakkında bir açıklama yayınlamıştır.¹¹⁴ İlgili açıklamada ICO sözcüsü; kararı dikkatlice inceleyeceklerini; mahkemenin, polisin LFR sistemlerini 2018 Veri Koruma Yasasına uyulmasını gerektiren, halkın hassas kişisel verilerinin işlenmesine uygun olarak kullanması gerektiğine karar vermesini beklediklerini; bu yeni ve müdahaleci teknolojinin doğru gizlilik önlemleri olmadan kullanılmasının polise olan güveni arttırmak yerine zayıflatacağını; bu teknolojinin polis tarafından pilot kullanımına ilişkin yakın zamanda tamamladıkları araştırma sonucunda, polis kuvvetlerine gelecekteki herhangi bir LFR sisteminin nasıl planlanacağı, yetkilendirileceği ve uygulanacağı konusundaki önerileri sonuçlandırmada mahkemenin bulgularını değerlendireceklerini; bu arada bu sistemleri kullanan tüm polis güçleri veya özel kuruluşların mevcut veri koruma

¹¹⁴ Gerrish Legal, "The UK Court has issued a judgment on the use of live facial recognition technology by the police", 16 September 2019, (Çevrimiçi) <https://www.facebook.com/LegalBusinessPartner/posts/the-uk-court-has-issued-a-judgment-on-the-use-of-live-facial-recognition-technol/2682787115086668/> 10 October 2019.

kanunu ve talimatlarının hala geçerli olduğunun farkında olmaları gerektiğini belirtmiştir.¹¹⁵

Kişisel veri toplamada yapay zekâlı sistemlerin kullanımında yaşanan bir diğer olumsuzluk da sistemi oluşturan/yazılımını yapan kişilerin ırk ayrımcılığı yapan algoritmalar eklemesi halinde yol açacakları KVK hukukuna aykırılıktır. Buna örnek olarak ABD'ye yapılmış bir araştırmada azınlık çalışanların bir iş başvurusunun kabul edilebilmesi için beyaz çalışanlara kıyasla yüzde 60 daha fazla özgeçmiş göndermesi gerektiği sonucunun bulunmuş olmasıdır. Karar mekanizmasının YZ sistemleri değil de bir insan olması halinde bile bu önyargı işe alınma değerlendirmesini yapacak yöneticilerin bazılarının bilinçaltında var olduğu tarihsel bir olgudur. Kişinin ad ve soyadının Afrikalı, Hintli veya Batılı olmayan birini çağrıştırmaları halinde de sadece işe alımlarda ya da daha net ifadeyle potansiyel mesleki fırsatlarını kaçırmada değil bazı hizmet alımlarında da bu ayrımcılığa maruz kalma söz konusu olabilir. Örneğin; 2018 yılında *The Sun*'da geçen bir raporda, arabasının yıllık sigortasını yaptırmak üzere sigorta şirketlerine başvuruda bulunan *Mohammed* adlı müşterilere, adları *John* olan müşterilere kıyasla ortalama birkaç yüz pound daha yüksek fiyat verildiği tespit edilmiştir. Raporda, *Mohammed* adlı müşterilere beş farklı sigorta şirketi tarafından 205 ila 919 Sterlin arasında değişen fiyatlar verildiği belirtilmiştir.¹¹⁶ Bu konuda bir başka örnek de Goldman Sachs tarafından yönetilen Applecard'ı kullanan bir erkeğe, kendisiyle aynı vergi beyannamesi veren eşine oranla 20 kat daha yüksek kredi limiti verilmesidir ki bu gelecekteki muhtemel cinsiyet ayrımcılıklarının bir göstergesi olarak kabul edilmektedir¹¹⁷. Algoritmik önyargı (Bölüm 2.4.2.2) ve ayrımcılık (Bölüm 2.4.2.3) konularına ilerleyen bölümlerde girileceğinden burada bu örnekten bahisle yetinilecektir. Ancak kısaca şunu belirtmekte fayda bulunmaktadır: Bu ve benzer

¹¹⁵ Birleşik Krallık Bilgi Komiserliği Ofisi (ICO - Information Commissioner's Office), "Statement on the High Court judgement on the use of live facial recognition technology by South Wales Police", 4 September 2019 (Çevrimiçi) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/09/statement-high-court-judgement-frt-south-wales-police/> 10 October 2019.

¹¹⁶ Natalie Morris, "What is unconscious name bias and why is it so damaging?", **Metro News**, 17 September 2019, (Çevrimiçi) <https://metro.co.uk/2019/09/17/unconscious-name-bias-damaging-10757825/?ito=cbshare> 30 November 2019.

¹¹⁷ Karen Hao, "There's an easy way to make lending fairer for woman. Trouble is, its illegal", **MIT Technology Review**, Nov 15, 2019. (Çevrimiçi) <https://www.technologyreview.com/s/614721/theres-an-easy-way-to-make-lending-fairer-for-women-trouble-is-its-illegal/> 31 December 2019.

durumlarda bir algoritmanın kişisel verilerin korunması hukukuna aykırı bir şekilde önyargılı ve ayrımcı bir zihniyet taşımasının sebebinin sadece o algoritmayı yazan insanın düşüncelerinden kaynaklandığını da söylemek çok kolay olmamaktadır. Hatta o algoritmayı yazan kişi bu tür önyargı ve ayrımcı düşüncelere sahip olmasa ve bunu algoritmada yazmasa bile, dışardan bağımsız/serbestçe bilgi olarak kendi değerlendirme kriterlerini oluşturan bir YZ sistemi bile gerek sosyal medya gerekse diğer web sayfalarında yer alan bu tür fikirlerden etkilenerek olumsuz kararlar verebilir. Dolayısıyla bir insanı önyargı ve ayrımcı değerlendirmeler yapmasına yol açabilen bilgi akışı, insan zekâsını örnek alan bir YZ sistemi tarafından da benimsenebilir. Bu gibi durumlara maruz kalan bir YZ algoritmasının hem psikolojik hem de sosyolojik testlere tabi tutulması, temel değer ve ahlaki kriterler konusunda da kodlanması gerekecektir ki bu konuyu inceleyen sayısız literatür¹¹⁸ bulunmaktadır.

Bu konudaki bir diğer örnek, yine Çin'deki gözetim sağlayan yapay zekâlı yüz tanıma sistemlerine ilişkindir. Yakın zamanda Çin'deki Fudan Üniversitesi'ndeki bilim adamları tarafından, Çin Bilimler Akademisi'nden Changchun Optik Enstitüsü ile birlikte, on binlerce insandan oluşan bir stadyum kalabalığı içinden tek bir kişiyi tanımlayabilen 500 megapiksel çözünürlükte görüntü alabilen ultra güçlü bir kamera geliştirmiştir. Kamera, kalabalığın arasından kişileri seçebilmek için gerçek zamanlı izleme ile birlikte yüz tanıma teknolojisini kullanmaktadır ki bu da Çin'in geniş kapsamlı gözetim ağı için kullanışlı bir araç olarak görülmektedir. Şu anda Çin'de faaliyet gösteren yaklaşık 170 milyon CCTV kamerası bulunmaktadır ki bu da ülkedeki her 12 kişiye 1 kamera düştüğü anlamına gelmektedir. Bu gibi teknolojik konularda başı çeken Çin, ayrıca ülkede yaşayanları takip etmek için dünyanın en gelişmiş gözetim yazılımı ve donanımını da piyasaya sürmüştür. 2018 yılında ülke, yalnızca 50 metre uzaklığa kadar insanları yürüyüşlerinden tanıyan bir yapay zekâ kullanan yürüyüş tanıma teknolojisini kullanmaya başlamıştır.¹¹⁹ Son yıllarda

¹¹⁸ Yapay zekâ ve ahlak konusunda 2004-2014 Kasım tarihleri arasında yapılmış çalışmaların geniş bir listesi için bkz.: Kathy Baxter, "Ethics in AI research papers and articles", 19 November 2019, (Çevrimiçi) <https://blog.einstein.ai/ethics-in-ai-research-papers-and-articles/> 30 November 2019.

¹¹⁹ 500 megapiksel kameranın görüntü netliğini anlayabilmeyi kolaylaştırmak adına, 2018 yılında Şili'deki bir gözlemevinde kullanılmaya başlanan ve amacı uzak galaksileri gözlemlemek olan 570 megapiksel kameraya oldukça yakın olması kıyasen verilebilir. Işıkyılı mesafelerdeki galaksileri gözlemlemeye yetecek netlikte görüntü sağlayan Çin'deki bu kamera, ülkenin gözetim sistemlerine oldukça önem verdiğini göstermektedir.

gözetim sistemleri oldukça gelişmiş olan Çin'de bu konudaki bir başka girişim de gökyüzünden gelen kalabalığı izlemek amacıyla kullanımına başlanan güvercin benzeri uçaklardır. "Casus kuş" adı verilen bu program, yeryüzündeki insanları da gizlice gözlemek için yüksek çözünürlüklü kameralarla donatılmış robotik kuş sürülerini kullanmaktadır. Çin'in bu tür YZ sistemlerinden oluşan yaygın gözetim ağı, ülkenin vatandaşlarına, davranışlarına göre bir sıralama sağlayan sosyal kredi sistemindeki puanlamalara temel veri sağlamaktadır ki puanları düşük olanların devlet işlerine girmekten çocuklarını istedikleri okullara yerleştirmeye kadar her konuda engellerle karşılaşmaları muhtemel görünmektedir. Bir kısım insan hakları savunucuları sistemi "ürpertici" olarak tanımlarken İnsan Hakları İzleme Örgütü araştırmacısı Maya Wang, program hakkındaki bir blog yazısında "Hükümetin, vatandaşları, alışveriş alışkanlıklarından çevrimiçi konuşmaya kadar çeşitli davranışlarını değerlendirerek sorunsuz bir toplum üretme niyetinde" olduğunu belirtmiştir.¹²⁰ Ancak bu durum görüldüğü kadar masum değildir. Nitekim bireylerin yüksek duvarlarla çevrili ancak üzeri açık olan bahçelerinde, kendi evlerinin balkon ve teraslarında da gözetlenme ihtimali söz konusudur ki bu özel hayatın gizliliğini ihlal etmektedir. Ancak sadece Çin değil hemen hemen her devlet buna benzer gözetim sistemlerinin yasal açıdan uygunluğunu sağlamak adına oluşturdukları kanun maddelerinde toplumun ve devletin güvenliğini sağlamayı gerektiren durumlarda kişisel verilerin işlenebileceğine yönelik düzenlemelerde bulunmaktadır.

Kompleks yapay zekâlı sistemler, doktorların çok isabetli kararlar alabilmesine ve teşhis yapabilmesine imkân sağlayacaktır. Stanford, Chicago, California üniversitelerinden ve Google'dan araştırmacıların bulunduğu bir ekip, hastalara ilişkin anonim yüz binlerce veri ile Google'ın çok güçlü bir cihazında makine öğrenimi algoritmasını eğitmiştir¹²¹. Algoritmalar çok yüksek isabet oranı ile hastalıkları teşhis etmekten, ölme ihtimali ve hastanede kalma süresine ilişkin

¹²⁰ Anthony Cuthbertson, "China Invents Super Surveillance Camera That Can Spot Someone From Crowd of Thousands - Device's Resolution is Five-Times More Detailed Than Human Eye", **The Independent**, 2 October 2019, (Çevrimiçi) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/china-surveillance-camera-facial-recognition-privacy-a9131871.html> 30 November 2019.

¹²¹ Alvin Rajkoma, Eyal Oren, Kai Chen, Andrew M. Dai, Nissan Hajaj, Michaela Hardt, Jeffrey Dean, "Scalable and accurate deep learning with electronic health records", **NPJ Digital Medicine**, Vol.1, No.1, 2018. (Çevrimiçi) <https://www.nature.com/articles/s41746-018-0029-1#citeas> 31 December 2019.

öngörüde bulunmaya kadar çeşitli kararlar almayı başarmıştır. Örneğin hastaneye yatmış bir kişinin 24 saat içinde kişinin ölme ihtimalini %90 isabetle öngördüğü ifade edilmektedir. Ancak bu algoritmaların nasıl karar aldığını ekip açıklayamamaktadır. Hastaların verilerinin hangi verilerinin toplandığı ve nasıl işlendiğine ilişkin bilgi sahibi olması gerekmektedir.¹²²

Yapay zekâlı sistemler tarafından kişisel veri kullanım ihlallerine bir diğer örnek de dünya genelinde 100 milyondan fazla cihazda kullanılan, Alexa ses komutuyla çalışan sesli asistanlar gösterilebilir. Bu tür ihlallerle ilgili kullanıcı bildirimleri oldukça fazladır. Örneğin; 2017 yılında Londra'da yaşayan Martin Josephson akşam işten eve döndüğünde Amazon'un ses asistanı Echo Dot'ın "Alexa" ses aktive komutunu almadan kendiliğinden işlemler yaptığına şahit olmuştur. Bu işlemler, Josephson'ın daha önceki kişisel verilerini (beğenilerine) dayanarak daha önce almış olduğu yolculuklar için tren bileti rezervasyonu yapma ve daha önce izlediği TV şovlarını kaydetme gibi önceki işlemleri tekrarlayan işlemlerdir. Tüm çabalarına karşın ses Echo Dot'ı durdurmayı başaramamıştır. Bir diğer örnek olarak, 2018 yılında Almanya'daki bir Amazon müşterisine yanlışlıkla başka birinin Echo Dot sesli asistanından yaklaşık 1.700 ses dosyasının gönderilmesi gösterilebilir. Amazon bu talihsiz durumu insan hatasına bağlamıştır. Yine bir başka örnek olarak San Francisco'da yaşayan Shawn Kinnear'ın, Echo'nun kendi kendine çalışmaya başladığını ve neşeli bir şekilde "Gözlerimi her kapattığımda, tüm gördüğüm insanlar ölüyor." dediğini bildirmesi gösterilebilir. Son ve açıklanması oldukça güç olan bir diğer ihlalde ise Oregon Portland'da bir kadın, ses asistanı Echo'nun özel konuşmaların kayıtlarını kocasının çalışanlarından birine göndermeyi üstlendiğini fark etmiştir. Bu durum karşısında Echo'nun üreticisi Amazon, yaptığı açıklamada, Echo'nun yanlışlıkla uyanma komutunu duymuş olabileceğini, yanlışlıkla bir mesaj gönderme talebi aldığını sanmış olabileceğini, telefon rehberindeki bir adı dinledikten sonra da parke zeminler hakkında bir konuşma sırasında mesajı göndermek için bir onay gönderdiğini söylemiştir.¹²³

¹²² Andrew Burt, Samuel Volchenboum, "How Health Care Changes When Algorithms Start Making Diagnoses", **Harvard Business Review**, May 8, 2018, (Çevrimiçi) <https://hbr.org/2018/05/how-health-care-changes-when-algorithms-start-making-diagnoses> 31 December 2019.

¹²³ Dorian Lynskey, "Alexa, are you invading my privacy?' – the dark side of our voice assistants", **The Guardian**, 9 October 2019, (Çevrimiçi) <https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants> 30 November 2019.

Elbette ki çok fazla bilgiyi çok kısa sürelerde işleyebilen bu tür yapay zekâlı algoritmaların, yüz milyonlarca belki milyarlarca kez kullanıldığında istenilmeden olarak bazı ihlallere yol açması muhtemeldir. Kaldı ki insanlar da istemeden de olsa benzer ihlaller yapabilmektedir. Ancak bir insanın iyi ile kötüyü ayırt etme veya bir isteğin bir bireyin kişisel verilerini koruma hakkını ihlal edip etmediğini anlayabilmesi yukarda geçen örneklerde sesli asistan yerine bir insanın olması halinde oldukça kolaydır. Burada sorun bir YZ algoritmasının bir insanın yapabileceğinden çok daha fazlasını çok kısa bir sürede yapabilme gücünden kaynaklanmaktadır. Bir diğer deyişle bir YZ algoritması bir işi bir insandan daha hızlı ve daha kapsamlı yapabilme özelliği ile daha fazla güce sahipken bir insanın yapabileceği küçük hatalar ise YZ algoritmasında devasa hatalar şeklinde kendini gösterebilmektedir. Dolayısıyla YZ algoritmalarının daha önce ifade edildiği üzere etik ve psikolojik testlere tabi tutulma zorunluluğunun yanı sıra kişisel verilerin korunması hakkına ilişkin kanun metinleri ile de eğitilmeleri/kodlanmaları da önemli bir zorunluluk olarak karşımıza çıkmaktadır. Unutulmamalıdır ki bir YZ sistemi, kendine öğretilmeyen veya öğrenmesi gerekli görülmeyen bir şeyi dikkate alamaz. Sonuç olarak bu sistemlerin yazılımcılarının KVK konusunda da gerekli eğitimleri alıp sistemin tasarımında ve uygulanması gerekli tedbirleri almaları veya yazılımlarının bizzat bu konuda devlet tarafından yetkilendirilecek KVK hukuku konusunda bilgili yazılımcılar tarafından incelenip onaylandıktan sonra piyasaya sürülmelerine müsaade edilmesi değerlendirilebilecek çözüm önerileri arasındadır.

İKİNCİ BÖLÜM

YAPAY ZEKÂ SİSTEMLERİNDE KİŞİSEL VERİLERİN İŞLENMESİ

Bu bölümde; yapay zekâ sistemleri bakımından kişisel verilerin işlenmesindeki temel ilkeler, kişisel verilerle ilgili diğer ilkeler, yapay zekâ sistemlerinde kişisel verilerin işlenmesi ve son olarak da algoritmalar konusu işlenecektir.

2.1. YAPAY ZEKÂ SİSTEMLERİ BAKIMINDAN KİŞİSEL VERİLERİN İŞLENMESİNDEKİ TEMEL İLKELER

Kişisel verilerin işlenmesindeki temel ilkeler, 6698 sayılı KVKK'nın "Kişisel Verilerin İşlenmesi" başlıklı İkinci Bölümünün "Genel İlkeler" alt başlığı altında yer alan 4. maddesinin 2. fıkrasında düzenlenmiştir. İlgili maddeye göre kişisel verilerin işlenmesi sırasında uyulması zorunlu olan bazı ilkeler bulunmaktadır. Bunlar¹²⁴:

- a) Hukuka ve dürüstlük kurallarına uygun olma.
- b) Doğru ve gerektiğinde güncel olma.
- c) Belirli, açık ve meşru amaçlar için işlenme.
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme".

Bu doğrultuda bu bölümde, yapay zekâ sistemleri bakımından kişisel verilerin işlenmesindeki temel ilkeler; hukuka ve dürüstlük kuralına uygun işlenmesi, doğru ve gerektiğinde güncel olma ilkesi, belirli, açık ve meşru amaçlar için işlenme ilkesi ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma başlıkları altında ele alınacaktır.

¹²⁴ KVKK, m.4(2).

2.1.1. Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi

GDPR'nin 5. maddesinin 1. fıkrasının (a) bendinde kişisel verilerin işlenmesinin hukuka uygun, adil¹²⁵ ve şeffaf (*lawfulness, fairness and transparency*) olması gerektiği¹²⁶ geçmektedir. Türkiye'de ise buna karşılık gelen hükümler, 6698 sayılı KVKK m.4/2(a)'da geçen "hukuka ve dürüstlük kurallarına uygun olma"¹²⁷ ilkesidir. Diğer yandan çalışmamızda şeffaflık ilkesine odaklanmamız nedeniyle "şeffaflık" ilkesine uygunluğu ayrı bir başlık altında (Bölüm 2.2.1'de) inceleyeceğimizden burada sadece hukuka uygunluk ve dürüstlük kuralına uygunluk konularını ve kısaca şeffaflık ilkesiyle ilişkisini ele alacağız.

Hukuka ve dürüstlük kurallarına uygunluk ilkesi, diğer ilkelerin de temelini oluşturmasının yanı sıra bu ilkeler arasında en önemlisidir¹²⁸. Bu doğrultuda, bu ilkenin "hukuka uygunluk" ve "dürüstlük kuralına uygunluk" olarak iki kısımda incelenmesi daha isabetli olacaktır.

Kişisel verilerin hukuka uygun olarak işlenmesi; mevcut yasalara, hukuki düzenlemelere, ilke ve yükümlülöklere uygun olarak işlenmesi anlamına gelmektedir. Hukuka uygun olma ilkesinin gerek KVK hukukuna yönelik mevzuata gerekse genel anlamda hukuk kuralları ve evrensel hukuk normlarının tamamına uygun olma şeklinde yorumlanması gerekmektedir¹²⁹. Bu bakımdan diğer ilkelere uygunluk da açıkça hukuka uygun olma ilkesinin doğal bileşenleri olarak kabul edilmelidir¹³⁰.

Kişisel verilerin dürüstlük kuralına uygun olarak işlenmesi ise verileri işlenen kişiye karşı şeffaf olunmasını yani şeffaflık ilkesini ifade etmektedir. 6698 sayılı

¹²⁵ Yapay zekâli sistemlerin yaptığı veri işleme faaliyetlerinin adillik ilkesine uyumluluğu incelenmelidir. Adillik ilkesi birçok unsuru içerisinde barındırmaktadır. Şeffaflık ilkesi bunların başında gelmektedir. Ancak veri işleme faaliyetinin bireye olan etkisi ve bireyin verinin nasıl işleneceğine ilişkin beklentisi de adillik değeriendirilmesindeki iki önemli husustur.

¹²⁶ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 5/1(a)**, p.35.

¹²⁷ KVKK, **m.4/2(a)**.

¹²⁸ Göçmen-Uyarer, **a.g.e.**, s.120.

¹²⁹ Murat Volkan Dölger, "Kişisel Verilerin Korunması Hukuku", **Hukuk Akademisi**, İstanbul, 2018, s. 109.

¹³⁰ Küzeci, **a.g.e.**, s.201.

KVKK m.4/2(a)'da belirtilen bu ilke için 4721 Sayılı Türk Medenî Kanunu'nun¹³¹ "Başlangıç" başlıklı bölümündeki "B. Hukukî ilişkilerin kapsamı" başlığı altındaki "İ. Dürüst davranma" alt başlığında yer alan 2. maddeye bakılması gerekecektir. İlgili maddede; her bireyin hukukun kendilerine tanıdığı hakları kullanmaları ve borçları yerine getirmeleri sırasında dürüstlük kuralına uygun hareket etmeleri gerektiği, hukuk düzeninin dürüstlük kuralının açık bir şekilde kötüye kullanılmasına hiçbir şekilde izin vermeyeceği bildirilmiştir.

Buna göre; kişisel verilerin işlenmesinde, veri sorumlularının ve veri işleyenlerin bu verileri dürüstlük kuralına uygun hareket ederek işleme yükümlülükleri bulunacaktır. Bunun yanı sıra kişisel verileri dürüstlük kuralına uygun işleme ilkesinin yorumlanmasında; veri sorumluları veya veri işleyenler tarafından, kişisel verileri işlemede kendilerine hukuka uygun olarak rıza gösteren bireylerin öngörebileceği biçimde hareket etmeleri veya bunların işlenmesinde amacına uygunluk ve sadece amacın gerektirdiği miktarlarda olması ilkelerine de uygun hareket etmeleri gerekeceği¹³² söylenebilir. Dürüstlük kuralına uygun olma ilkesi ayrıca veri işlemenin verileri işlenen bireye yönelik şeffaflık içermesini de kapsamaktadır ki buna göre verileri işlenen bireyler verileri işleyenlerce bilgilendirilmeli ve gerektiğinde uyarılmalıdırlar¹³³. Sonuç olarak kişisel verilerin yasal normlara uygun olarak işlenmesinin tek başına yeterli olmadığı, veri işlemede dürüstlük kuralına uyulmadığı takdirde bu işlemin hukuka aykırı olduğu söylenebilecektir¹³⁴.

¹³¹ 4721 Sayılı Türk Medenî Kanunu (TMK), Kanun Numarası: 4721, Kabul Tarihi: 22/11/2001, Resmî Gazetede Yayımlandığı Tarih: 8/12/2001 ve Sayı: 24697. (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf> 1 Aralık 2019.

¹³² Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenmesine ilişkin Temel ilkeler", 2018, ss.1-12, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler> 2 Aralık 2019, s.3.

¹³³ Küzeci, **a.g.e.**, s.207.

¹³⁴ Nitekim, konuya ilişkin olarak Kişisel Verileri Koruma Kurumu'nun verdiği bir örnekte kişisel verileri hukuka uygun işlemede, bu verilere erişimde belirli sayıda kişiye yetki verilmesi gerekmekteyken, amacı aşan sayıda kişiye yetki verilmiş olmasının dürüstlük kuralına aykırılık yaratacağı bildirilmiştir (Bkz. Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenmesine...", s.4). Ayrıca Kişisel Verileri Koruma Kurumu'nun, Facebook'a yönelik verdiği 11/04/2019 Tarih ve 2019/104 Sayılı kararda bu konuya değinilerek, kullanıcı fotoğraflarına erişimde kullanılan yazılımdaki bir hata sonucunda kullanıcıların izne açmadığı fotoğraflara da 12 gün süresince erişilebildiği ve bunun gerek hukuka uygun olma gerekse dürüstlük kuralına uygun olma ilkelerini çiğnediği belirtilmiştir (İlgili karar için bkz.: Kişisel Verileri Koruma Kurulu, "Facebook Hakkında Kişisel Verileri Koruma Kurulunun

2.1.2. Doğru ve Gerekliğinde Güncel Olma İlkesi

GDPR'nin 5. maddesinin 1. fıkrasının (d) bendinde kişisel verilerin işlenmesinin doğru ve gerektiğinde güncel olması, işlenme amaçları dikkate alınarak, yanlış olan kişisel verilerin gecikmeden silinmesini veya düzeltilmesini sağlamak için her makul adımın atılması gerektiği (*accuracy*)¹³⁵ geçmektedir. Türkiye'de ise buna karşılık gelen hükümler, 6698 sayılı KVKK m.4/2(b)'de geçen "doğru ve gerektiğinde güncel olma"¹³⁶ ilkesidir.

Kişisel verilerin doğru işlenmesi ve gerektiği veya talep edildiği durumlarda güncel olması/güncellenmesiyle ilgili olan bu ilke, kişisel verilerin işlenmesine yönelik uluslararası düzenlemelerde verileri işlenen kişilere tanınmış olan kendi verilerine erişebilme hakkı ve düzeltilmesini isteme hakkı ile uyumlu olmasının yanı sıra 6698 sayılı KVKK m.11/1(d)'de düzenlenmiş olan "*Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme*"¹³⁷ hakkıyla da paraleldir. GDPR m.13/2(b)'de de verileri toplanan kişinin kendi kişisel verilerine erişme, düzeltilmesini veya silinmesini ya da kendisiyle ilgili işlemlerin kısıtlanmasını isteme, verilerinin işlenmesine itiraz etme ve verilerinin taşınmasını isteme gibi haklarının olduğunun, veri sorumlusu tarafından verileri toplanan kişiye bildirilmesi gerektiği¹³⁸ geçmektedir. Görüleceği gibi GDPR çerçevesinde de verileri işlenen kişilerin gerektiği durumlarda verilerinin düzeltilmesini isteme hakkı AB tarafından da düzenlenmiştir.

11.04.2019 tarih ve 2019/104 sayılı Karar Özeti", Karar Tarihi: 11/04/2019, Karar No: 2019/104, 10 Mayıs 2019 (Çevrimiçi) <https://www.kvkk.gov.tr/lcerik/5450/2019-104> 2 Aralık 2019).

¹³⁵ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 5/1(d)**, p.35.

¹³⁶ KVKK, **m.4/2(b)**.

¹³⁷ KVKK, **m.11/1(d)**.

¹³⁸ İlgili madde GDPR'de; "2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:... (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability" şeklinde geçmektedir (bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 13/2(b)**, p.41).

Kişisel verileri işlenen kişilerin bu verilerin doğru olarak işlenmesi, güncel değilse güncellenmesini isteme hakkı gerek ilgili kişiler gerekse bu verilerin işlenmesinden sorumlu kişiler açısından büyük önem taşımaktadır. Ekseriyetle işlenen kişisel verinin konusunun kişinin sağlığına yönelik veriler olduğu durumlarda, ortaya çıkması muhtemel maddi-manevi zararların ciddiyeti nedeniyle bu önem daha da artmaktadır. Ayrıca, ilgili kişinin kişisel verisinin işlenmesi, ilgili kişiyi olumsuz etkileyecek bir sonuç doğuruyorsa (Örneğin bir finans kuruluşundan kredi alma işlemi sırasında eksik veya yanlış veri nedeniyle kredi alamama gibi) veri sorumlusu verilerin doğru ve güncel olması konusunda aktif özen göstermekle yükümlü tutulmaktadır.¹³⁹

Makine öğrenimi uygulamalarının çok fazla kaynaktan veri toplaması sebebiyle toplanan verinin kişiye ait olmaması veya kişinin daha sonraki geçirdiği süreçler sebebiyle güncelliğini yitirmesi mümkündür. Veri sorumlusunun topladığı ve işlediği kişisel verilerin doğruluğunu ve güncelliğini sağlayabilme adına YZ sistemlerin veri işleme süreçlerine özel tedbirler alması gerekmektedir.

2.1.3. Belirli, Açık ve Meşru Amaçlar için İşlenme İlkesi

GDPR'nin 5. maddesinin 1. fıkrasının (b) bendinde kişisel verilerin işlenmesinin belirli (*specified*), açık (*explicit*) ve meşru (*legitimate*) amaçlar için toplanmış ve bu amaçlara aykırı şekilde işlenmemiş olması gerektiği; ayrıca yine GDPR'nin 89. maddesinin 1. fıkrası uyarınca kamu yararına, bilimsel veya tarihi araştırma amaçlarına veya istatistiksel amaçlara yönelik arşivleme amacıyla başka işlem yapılmasının da başlangıç amaçlarına aykırı olduğu anlamına gelmeyeceği (amaç sınırlandırma - *purpose limitation*)¹⁴⁰ geçmektedir. Türkiye'de ise buna karşılık gelen hükümler, 6698 sayılı KVKK m.4/2(c)'de geçen "belirli, açık ve meşru amaçlar için işlenme"¹⁴¹ ilkesidir. Burada özellikle dikkat edilmesi gereken nokta, bu ilkenin "amacın sınırlandırılması" ile ilgili olduğudur ki literatürde sıklıkla "verilerin minimizasyonu" ilkesi ile karıştırıldığı görülmektedir. Burada, yani kişisel verilerin belirli, açık ve meşru amaçlar için işlenme ilkesinde; verilerin işlenme amaçlarının

¹³⁹ Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenmesine...", s.6.

¹⁴⁰ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 5/1(b)**, p.35 and **Article 89/1**, pp.85-86.

¹⁴¹ KVKK, **m.4/2(c)**.

açıkça ve kesin olarak tanımlanmış (belirli) olması, verilerin işleme amaçlarının karışıklık veya şüpheyi yer bırakmayacak şekilde ayrıntılı ve net ifade edilmiş (açık) olması ve son olarak da verilerin işleme amaçlarının yasalara veya kurallara uygun (meşru) olması kastedilmektedir.

Bu ilkeye göre kişisel verilerin işlenmesi ancak bu verilerin kişilerin açık rızalarının alınması ile veya yasalarda geçen haller çerçevesinde açık rızaya gerek kalmaksızın mümkün olabilecektir. Açık rıza gerektiren durumlarda kişinin açık rızasının yasalara uygun şekilde alınmış olabilmesi için verilerin işleme amaçlarına yönelik olarak kişilerin doğru ve eksiksiz olarak bilgilendirilmiş olması gerekecektir. Bunun için de kişisel verilerin işleme amaçları, kapsamı, sınırları ve işleme süresinin bireylere açıkça belirtilmiş olması, verileri işlenecek kişiler bilgilendirilirken kullanılan aydınlatma/bilgilendirme/açık rıza gibi metinlerde ilgili kişiler tarafından kolaylıkla anlaşılabilir terminolojik bir dilin kullanılması zorunlu olacaktır.¹⁴² Aksi halde, yani amaçların yeterince açık ve/veya belirli olmaması, veri sorumluları tarafından bu kişisel verilerin işlenmesi hususundaki sınırları belirsizleştireceğinden, bu ilkenin kişisel verilerin işlenmesindeki öneminin oldukça yüksek olduğu düşünülmektedir.

Dolayısıyla, veri sorumlularının kişisel verileri işlemeleri, ilgili kişilere bildirdikleri amaçlarla sınırlıdır. Veri sorumlularının, bu amaçlar haricinde hangi sebeple olursa olsun kişisel verileri işlemeleri bu ilkeye ters düşeceğinden hukuken uygun değildir. Bir diğer deyişle belirli amaçlar dahilinde ilgili kişiden izni alınmış olan veri işleme faaliyetinin amaçları daha sonra genişletilir ise ve kişiden yeniden rıza alınmamış ise bu durum hukuka aykırı sayılacaktır. Öte taraftan, kişisel verilerin ilgili kişilerden açık rıza alınmaksızın işlenmesi durumunda da amacın meşru, yani yasalara ve kurallara uygun olması gerekecektir.¹⁴³

¹⁴² Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin İşlenmesine...”, s.8.

¹⁴³ Göçmen-Uyarer, **a.g.e.**, s.123. Nitekim, 6698 sayılı KVKK’da özel nitelikli kişisel verilere ayrı bir önem verilerek bunlar kıyas yoluyla genişletilemeyecek şekilde dar ve sınırlı bir kapsamda tanımlanmış ve bu verilerin tanımı ve işleme şartlarına ilişkin 6. maddede ayrı bir düzenleme getirilmiştir. İlgili maddenin I. fıkrasında; ırk, etnik köken, siyasi görüşler, dini ve felsefi inançlar, mezhep ya da diğer inançlar, giyim tarzı, bir derneğe, vakıfa veya sendikaya üyelik durumu, sağlık, cinsel hayat, herhangi bir cezadan mahkûmiyet yaşayıp yaşamadığı ve güvenlik tedbirleri ile ilgili verilerin yanı sıra genetik ve biyometrik veriler, özel nitelikli kişisel veriler arasında sıralanmıştır. İlgili maddenin II. fıkrasında göre özel nitelikli kişisel

2.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

GDPR'nin 5. maddesinin 1. fıkrasının (c) bendinde kişisel verilerin işlenmesinin işlendikleri amaçla ilgili (*relevant*)¹⁴⁴ olması, yeterli/ölçülü (*adequate*) ve sınırlı (*limited*) olması gerektiği (veri minimizasyonu - *data minimisation*)¹⁴⁵ geçmektedir. Türkiye'de ise buna karşılık gelen hükümler, 6698 sayılı KVKK m.4/2(ç)'de geçen "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"¹⁴⁶ ilkesidir. Burada özellikle dikkat edilmesi gereken nokta, bu ilkenin "amacın sınırlandırılması" ile ilgili değil "verilerin minimizasyonu" ile ilgili olduğudur. Bir diğer deyişle burada "verilerin sınırlandırılması" söz konusudur.

Bu doğrultuda öncelikle kişisel veri niteliği ve işlenme amacının birbiri ile bağlantılı/uyumlu olması gerekmektedir. Bu ilke, amacın gerektirmediği kişisel verilerin işlenmemesini gerektirmektedir. Kişisel Verileri Koruma Kurumu, verilerin işlenmesine yönelik konuda daha sonra belirebilecek olası gereksinimlere dayalı olarak kişisel verilerin işlenmesinin uygun olmadığını bildirmiştir¹⁴⁷. Bunun yanı sıra ilgili kurumun bir marketler zincirinin sadakat kart uygulamasına yönelik verdiği 25/03/2019 tarihli ve 2019/82 sayılı bir başka kararda, işletmenin müşterilerini aydınlatma/bilgilendirme metninde, müşterilerinin kişisel verilerini de işleyebileceğine yönelik koymuş olduğu ifadeleri, işletmenin kişisel veri işlemeye

verilerin kişiden açık rıza alınmadan işlenebilmesi kanunen yasak sayılmakla birlikte III. fıkarda bu tür verilerin kanunlarda belirtilen sınırlı hallerde açık rıza olmaksızın işlenebileceği de eklenmiştir. Buna göre; I. fıkarda belirtilen cinsel hayata ve sağlığa ilişkin olanlar haricindeki kişisel veriler, kanunlarda belirtilen sınırlı hallerde açık rıza olmaksızın işlenebilmektedir. Yine III. fıkarda geçen hükümlere göre cinsel hayat ve sağlıkla ilgili kişisel veriler de yalnızca kamu sağlığını koruma, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım gibi sağlık hizmetlerinin yürütülmesinde, sağlık hizmetlerinin ve sağlık finansmanının planlanmasında ve yönetiminde, sır saklama yükümlülüğüne sahip kişiler ya da yetkili kurumlar/kuruluşlarca kişiden açık rıza alınmadan işlenebilecektir. 6. maddenin IV. ve son fıkrasında ise özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kişisel Verileri Koruma Kurulu'na belirlenmiş/belirlenecek olan yeterli tedbirlerin alınması şart koşulmuştur (KVKK, m.6).

¹⁴⁴ Amaca uygun, ele alınan konu ile ilgili/alakalı olması.

¹⁴⁵ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 5/1(c)**, p.35.

¹⁴⁶ KVKK, **m.4/2(ç)**.

¹⁴⁷ Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenmesine...", s.9; Küzeci, **a.g.e.**, s.198.

yönelik bir faaliyette olmaması nedeniyle ilgili metninden çıkarması gerektiğine karar verilmiştir¹⁴⁸.

Kişisel verilerin işlenmesinin yeterli/ölçülü olması ilkesi GDPR'nin 5. maddesinin 1. fıkrasının (c) bendinde “adequate” sözcüğüyle ifade edilmiştir. Bu ifadenin Türkçe karşılığı esasen “yeterli” sözcüğüdür ki sözlük anlamı bakımından “kalite veya miktar olarak kabul edilebilir veya tatmin edici” anlamındadır. Bu sözcüğün karşılığı olarak KVKK m.4/2(ç)'de “ölçülü” sözcüğü kullanılmıştır ki bu kullanımın yerinde olduğunu düşünmekteyiz. Çünkü bu sözcük, “yeterli” sözcüğü ile ifade edildiğinde alt sınırı olmakla birlikte yeterli düzeyden fazla olması halinde ilkeye ters düşmeyecekti, yani üst sınırı olmayacaktı. Halbuki “ölçülü” şeklinde kullanıldığında hem alt sınır hem de üst sınır konulmuş oluyor. Çünkü bir şeyin ölçülü olması hem yeterli düzeyde olmasını hem de gerektiğinden fazla olmamasını ifade etmektedir. Dolayısıyla kanun koyucunun bu ilkenin Türk hukukuna kazandırılmasında dikkatli ve isabetli bir ifade kullandığı düşünülmektedir. Bu ilkeye örnek olarak kişisel veri işleme amacı “pazarlama” eksenli olan bir tekstil işletmesinin, müşterilerinin özel nitelikteki kişisel verilerini işlemesi “ölçülü” olma ilkesine ters düşmesi gösterilebilir¹⁴⁹.

Son olarak kişisel verilerin işleme amaçlarıyla sınırlı olması da bu ilke çerçevesindeki en önemli konulardan birisidir. Buna göre veri sorumlusu, kişisel veri toplamadaki amaçlarını sınırlandırmalıdır. Doktrindeki bir görüş, yeni ihtiyaçlar ortaya çıktığında yeni amaçların oluşacağı, bu durumun veri işleme açısından yeni bir faaliyet olacağı, bu nedenle de yeni amaçların gerektirdiği yeni veri işleme faaliyetlerinin de verisi işlenen bireylerin yeniden onayına sunulması ve onların yeniden açık rızalarının alınmasını gerektirdiği yönündedir¹⁵⁰ ki biz de bu görüşe katılmaktayız. Bireyden, kişisel verilerinin işlenmesine yönelik daha önce alınmış olunan açık rıza, belirtilmiş belirli amaçlar için verilerin toplanmasına yönelik

¹⁴⁸ Kişisel Verileri Koruma Kurulu, “Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/82 sayılı Karar Özeti”, Karar Tarihi: 25/03/2019, Karar No: 2019/82, 2019 (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/5463/-Bir-market-zincirinin-sadakat-kart-uygulamasina-iliskin-ihbar-ve-sikayetler-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-25-03-2019-tarihli-ve-2019-82-sayili-Karari> 4 Aralık 2019.

¹⁴⁹ Göçmen-Uyarer, **a.g.e.**, s.124.

¹⁵⁰ Çiğdem Ayözger, “Kişisel Verilerin Korunması – Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil”, **Beta Yayınları**, İstanbul, 2016, s.128.

olacaktır ki bu da yeni amaçlar için veri toplanmasının tekrar kişinin onayına sunulmasını zorunlu kılacaktır.

Yapay zekâ sistemlerinde kişisel verilerin işlenmesi bakımından ise bu ilke, yazılım geliştiricilerin Yapay Zekâ (YZ) algoritmalarını geliştirirken bu algoritmaları, ihtiyaç duyacakları kişisel verilerin amaçla ilgili, sınırlı ve ne gereğinden fazla ne gereğinden az olacak şekilde modellemelerini, ona göre tasarımlarını ve bu ilkeye uygun veri işlemeyi YZ'lere öğretmelerini zorunlu kılmaktadır.

2.2. KİŞİSEL VERİLERLE İLGİLİ DİĞER İLKELER

Bu bölümde kişisel verilerle ilgili önceki bölümde incelenen ilkelere ek olarak şeffaflık ve ilgili kişileri bilgilendirme, hesap verebilirlik ve veri güvenliği ilkeleri ele alınacaktır.

2.2.1. Şeffaflık ve İlgili Kişileri Bilgilendirme İlkesi

Hükümetler kullandıkları gücün kaynağını vatandaşlardan almaktadır. Aslında vatandaşın veya toplumun sahip olduğu gücün geçici olarak devri söz konusudur. Bu nedenle şeffaflık, demokrasinin sağlıklı bir biçimde çalışabilmesi için gereken temel bileşenlerden birisidir.¹⁵¹

Şeffaflık ilkesi tamamen iyidir ve her şeyin çözümüdür de denilemez. Çünkü şeffaflık arttıkça diğer bazı değerler veya korunan haklarla bir takas ve dengelemenin yapılması kaçınılmaz olmaktadır.¹⁵² Etkili olma (effectiveness), güven (trust), adillik (fairness) ve hesap verilebilirlik gibi değerlere şeffaflığın artması katkı

¹⁵¹ James R. Hollyer, B. Peter Rosendorff, James Raymond Vreeland, "Democracy and Transparency", **The Journal of Politics**, Vol.73, No.4, 2011, pp.1191–1205 (Çevrimiçi) www.jstor.org/stable/10.1017/s0022381611000880 31 December 2019.

¹⁵² Ting Li, Till Unger, "Willing to pay for quality personalization? Trade-off between quality and privacy", **European Journal of Information Systems**, Vol.21, No.6, 2012, pp.621-642 (Çevrimiçi) <https://orsociety.tandfonline.com/doi/abs/10.1057/ejis.2012.13>. 31 December 2019; Sabrina Karwatzki, Olga Dytnko, Manuel Trenz, Daniel Veit, "Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization", **Journal of Management Information Systems**, Vol.34, No.2, 2017, pp.369-400 (Çevrimiçi) <https://www.tandfonline.com/doi/abs/10.1080/07421222.2017.1334467> 31 December 2019.

sağlarken diğer bir yandan verimlilik, gizlilik ve kalite açısından olumsuz etkiye neden olduğu ifade edilmektedir¹⁵³.

Kime karşı ve hangi süreçte şeffaflığın sağlanacak olduğunun belirlenmesi, açıklandığında riskli olduğu ortaya çıkacak ve dolayısıyla çekinilecek kararların alınmamasının yaratacağı zararları önleme adına önemlidir. Örneğin, çok riskli kalp ameliyatlarına giren cerrahların, ameliyatları neden yapmayı tercih ettiklerine ilişkin gereğinden fazla şeffaf olmaları beklenirse, bu türden ameliyatlara girecek doktor bulmakta zorlanılacaktır.

Şeffaflık ilkesinin hukuki düzenlemelerde hangi araçlarla sağlanacağına ilişkin siyaset bilimi açısından bilgi edinme hakkı (Freedom of information)¹⁵⁴ veya idare hukuku açısından yapılan idari işlemlerde gerekçelendirme yükümlülüğü¹⁵⁵ veya mahkeme kararlarındaki gerekçe ilkesi incelenebilir¹⁵⁶.

Şeffaflık ilkesinin teoride beklenen katkıları göz önünde tutularak hukuki düzenlemelerde yer verilmesine rağmen pratikte beklenen faydaları gösterememesinin örneğini bilgi edinme düzenlemelerinde görmekteyiz. Çünkü; bilgi edinme hakkını kullananların başvurularına; telefonla veya yüzyüze geri dönüş yaparak çözüm bulmaya çalışmaları ve eposta veya herhangi bir şekilde yazılı cevaptan imtina etmek suretiyle sonradan izlenebilir, takip edilebilir veya denetlenebilir olmaktan kaçınmışlardır.

¹⁵³ John F. Morrall III, "Regulatory Impact Analysis: Efficiency, Accountability, and Transparency", **Conference of the APEC-OECD Co-operative Initiative on Regulatory Reform**, Singapore, 2001. (Çevrimiçi) <http://www.oecd.org/governance/regulatory-policy/1901526.doc> 31 December 2019.

¹⁵⁴ Stephan Grimmelikhuijsen, Peter John, Albert Meijer, Ben Worthy, "Do Freedom of Information Laws increase transparency of government? A replication of a field experiment", **Journal of Behavioral Public Administration**, Vol.2, No.1, 2018, pp.1-10. (Çevrimiçi) <https://www.journal-bpa.org/index.php/jbpa/article/view/34> 31 December 2019.

¹⁵⁵ Sinan Seçkin, Gül Üstün. "İdari İşlemlerde Takdir Yetkisi ve Gerekçe İlkesi", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.21, Sayı.2, 2015, ss.509-534. (Çevrimiçi) http://dspace.marmara.edu.tr/bitstream/handle/11424/5910/_DAR_%20LEMLERDE%20TAKD_R%20YETK_S_%20VE%20GEREK_E%20_LKES_%5b%23289900%5d-273387.pdf?sequence=1&isAllowed=y 31 Aralık 2019; Elizabeth Fisher, "Transparency and Administrative Law: A Critical Evaluation", **Current Legal Problems**, Vol.63, No.1, 2010, pp.272-314. (Çevrimiçi) <https://doi.org/10.1093/clp/63.1.272> 31 December 2019.

¹⁵⁶ Kürşat Göktürk, "Gerekçeli Karar Hakkı." **Ankara Barosu Dergisi**, Sayı.3, 2014, ss.1-224. (Çevrimiçi) <https://dergipark.org.tr/tr/download/article-file/398187> 31 December 2019.

Şeffaflık ilkesinin gerekliliklerinin yerine getirilmesi hakkında karşılaşılan zorluklardan birisi de alınması gereken tedbirlerin masraflı olmasıdır. Bu yüzden şeffaflığa ilişkin tedbirler pratikte etkisiz olmakta ve hedeflenenin aksi yönünde sonuçlar doğurabilmektedir. Onora O'Neill 2002 yılındaki derslerinde şeffaflık ilizyonundan (transparency illusion) bahsetmiş; şeffaflığın, güveni tekrardan tesis etmesi ve kurumların güvenilirliğini artırması beklenirken, kamu görevlilerine ve kurumlara güveni azalttığına görüldüğünü belirtmiştir. Şeffaflığa ilişkin tedbirlerin sembolik bir şeffaflığın oluşumuna neden olduğunu söylemektedir.¹⁵⁷

Şeffaflığın sağlanması için salt bir hukuki yaklaşımdan ziyade pratikte ilgili kişilere fayda sağlayacak yönlerden bakılmalıdır. Ayrıca sınırsız bir şeffaflığın arzu edilmediği, sınırlarının bulunması gerektiğine ilişkin bilincin artırılmasına ihtiyaç duyulmaktadır. Ölçüsüz bir şeffaflığın yerine getirilmesi imkânsız yükümlülükler neden olacağı ve manipölasyon yapılmasına zemin hazırlayacağı da dikkate alınmalıdır.

Şeffaflığa ilişkin tedbirlerin kişisel verilerin korunması hukukunda özellikle açık rıza alınması ve bilgilendirme yapılması sürecinde önemli bir yönü ifade eden kutucuk işaretleme (box ticking) gibi göstermelik ve etkisiz işlemler haline dönüşmesinin engellenememesi halinde uygulayıcıların düş kırıklığına uğramasına ve soğumalarına neden olacaktır.

Şeffaflık, rüşvet veya yolsuzluk yapılması, görevin ve yetkinin suiistimal edilmesi halinde kişilerin yakalanabilecek olduklarından korkmalarına sebep olması yönüyle caydırıcı olumlu bir etkide bulunmaktadır. Ayrıca Kolluk kuvvetlerinin işkenceye, delilleri karartmaya giden birçok örnekle çoğaltılabilecek genellikle insan hakları ihlallerinin yoğun olarak görüldüğü yetkinin istismar edildiği alanlarda da şeffaflığın sağlanması temel hak ve hürriyetleri korumak açısından önemli bir araç olacaktır. Caydırıcı yönünün yanında katkı sağladığı yönler de vardır. Kişilerin aldıkları kararın sonradan kamuya veya kişilere açıklanacak olduğunu veya kamu tarafından denetlenebilecek olduğunu bilmeleri alınan kararların dayanaklarının araştırılması, kaynakların daha verimli kullanılması, kararın sonucunun ayrımcılıkta

¹⁵⁷ Onora O'Neill, "Reith Lectures 2002: A Question of Trust Lecture 4: Trust and Transparency", 27 April, 2002. (Çevrimiçi) http://downloads.bbc.co.uk/rmhttp/radio4/transcripts/20020427_reith.pdf 31 December 2019.

veya haksızlıkta bulunmayacak şekilde olması için karar alıcıların azami özen göstermesini sağlayacaktır.

Şeffaflığı sağlama adına kullanılacak yöntemlerden olan gerekçelendirerek veya açıklayarak karar almanın olumsuz sonuçlarından üçü şunlardır:

1. Masraflı olan süreçlere neden olması,
2. Hak arama amacından ziyade başka amaçları güden davaların açılmasına sebep olması,
3. Halihazırda yürüyen ve başarılı kararlar alınan süreçleri bozabilme ihtimalidir.

Şeffaflık ilkesi kamunun vatandaştan aldığı yetkiyi yolsuzluk aracı yapmaması ve gücünün istismarını önlemek amacıyla öne çıkmıştır. Şirketler yapıları gereğince kamu kadar şeffaf olmak zorunda değildi. Ancak Kişisel verilerin korunması hukuku kapsamında getirilen ilkeler özel veya kamu ayrımı yapmadan herkese uygulandığı için artık hukuki statülerinin de eskiden anlaşıldığı şekliyle değerlendirilmemesi gerekmektedir.

İlgili kişilerin beklentilerinin ne olduğunun belirlenmesi şeffaflık ilkesinin nasıl gerçekleştirildiğiyle bağlantılıdır. Bilgilendirmenin nasıl yapıldığı ve daha sonradan çıkan veri işleme faaliyetinin sınırlı amaçla işleme ilkesi kapsamında yapılacak değerlendirme ile başlangıçtaki amaçla ne kadar uyumlu olduğu kişinin beklentisini anlama adına atılacak adımlardır.¹⁵⁸

Şeffaflık ilkesi, GDPR'nin "*İlgili kişinin hakları*" (Rights of the data subject¹⁵⁹) başlıklı Üçüncü Bölümünün "*Şeffaflık ve modaliteler*" (Transparency and modalities) başlıklı Birinci Ayrımında, "*İlgili kişinin haklarını kullanmasında şeffaf bilgi, iletişim ve modaliteler*" (Transparent information, communication and modalities for the

¹⁵⁸ ICO, *Ibid.*, p.22.

¹⁵⁹ GDPR'de "*data subject*" olarak geçen ve doktrinde "*ilgili kişi*", "*verisi işlenen kişi*", "*veriye konu olan kişi*", "*veri sahibi*" şeklinde de kullanılan gibi tanımlamalar yerine, çalışmamızın genelinde KVKK'da geçtiği şekliyle "*ilgili kişi*" teriminin kullanılması tercih edilmiştir.

exercise of the rights of the data subject) başlıklı 12. maddesi altındaki toplam 8 fıkra¹⁶⁰ düzenlenmiştir.

GDPR'ye göre veri sorumlusunun ilgili kişiyi bilgilendirmede kısa, açık, sade, şeffaf, kolay ve anlaşılır bir dil kullanması gerekmektedir. Bilgilendirme, elektronik yollarla da dahil olmak üzere yazılı veya ilgili kişinin kimliğinin kanıtlanması şartıyla sözlü olarak yapılabilmektedir (GDPR m.12/1). Ancak ilgili kişinin elektronik yolla bilgi talep etmesi halinde yine ilgili kişi tarafından aksi talep edilmedikçe

¹⁶⁰ İlgili maddenin 1. fıkrasına göre; veri sorumlusu, 13. ve 14. maddelerde belirtilen herhangi bir bilgiyi ve özellikle çocuklara yönelik herhangi bir bilgide açık ve sade bir dil kullanarak, özlü, şeffaf, anlaşılır ve kolay erişilebilir bir biçimde ilgili kişiye verilerinin işlenmesine yönelik bilgiyi sağlamada, 15. ve 22. ve 34. maddelerdeki herhangi bir iletişimi sağlamada uygun tedbirleri almakla yükümlüdür. İlgili fıkra göre; bilgilendirme yazılı olarak veya uygun ise elektronik yollarla da dahil olmak üzere diğer yollarla da sağlanabileceği gibi verileri işlenen kişi tarafından talep edilmesi halinde, kimliğinin başka yollarla kanıtlanması şartıyla sözlü olarak da sağlanabilir. İlgili maddenin 2. fıkrasına göre veri sorumlusu, 15 ila 22 arasındaki maddeler uyarınca ilgili kişinin haklarını kullanmasını kolaylaştırmakla yükümlüdür. Ayrıca, Madde 11(2)'de belirtilen durumlarda veri sorumlusu, 15 ila 22 arasındaki maddeler uyarınca ilgili kişinin haklarını kullanma konusundaki talebi üzerine hareket etmeyi, ilgili kişiyi tanımlayacak bir konumda olmadığını göstermedikçe reddetmeyecektir. İlgili maddenin 3. fıkrasına göre veri sorumlusu, 15 ila 22 arasındaki maddeler uyarınca bir istek üzerine gerçekleştirilen işlem hakkında, ilgili kişiye gecikmeksizin ve konunun alınmasından sonraki bir ay içerisinde herhangi bir durumda yapılması gerekenlere ilişkin bilgi sağlamakla yükümlüdür. Bu süre, taleplerin karmaşıklığı ve sayısı dikkate alınarak gerektiğinde iki ay daha uzatılabilir. Veri sorumlusu, bu tür bir uzatma işlemine ilişkin ilgili kişiyi talebin alınmasından sonraki bir ay içinde ve gecikme nedenleriyle birlikte bilgilendirmelidir. İlgili kişinin elektronik yollarla talep ettiği durumlarda, ilgili kişi tarafından aksi talep edilmedikçe, bilgilendirmenin mümkün olduğunda elektronik yollarla sağlanması gerekmektedir. İlgili maddenin 4. fıkrasına göre; veri sorumlusunun, ilgili kişinin isteği üzerine işlem yapmaması halinde, ilgili kişiyi gecikmeksizin ve isteği aldıktan itibaren en geç bir ay içerisinde, işlem yapmama nedenleri, denetleme otoritesine şikâyetle bulunma ve yargı yoluna başvurma ihtimalleri hakkında bilgilendirme yükümlülüğü bulunmaktadır. İlgili maddenin 5. fıkrasına göre; 13 ve 14. maddelere göre sağlanan bilgiler ile 15 ila 22 arasındaki ve 34. maddelere göre yapılan her türlü iletişim ve herhangi bir işlem ücretsiz olarak sağlanacaktır. İlgili kişiden gelen taleplerin açıkça temelsiz veya aşırı olduğu durumlarda, özellikle tekrarlayan karakterleri nedeniyle, ilgili kişi (a) bilgi veya iletişimi sağlama veya talep edilen işlemi gerçekleştirmenin idari maliyetlerini dikkate alarak makul bir ücretlendirme yapma veya (b) istek üzerine işlem yapmayı reddetme hakkına sahiptir. Ancak isteğin açıkça temelsiz veya aşırı karakterini gösterme yükümlülüğü de veri sorumlusuna aittir. İlgili maddenin 6. fıkrasına göre; 15 ila 21 arasındaki maddelerde belirtilen talebi yapan gerçek kişinin kimliği ile ilgili makul şüpheleri olması durumunda veri sorumlusu, 11. maddeye hâle getirmeksizin, ilgili kişinin kimliğini doğrulamak için gerekli ek bilgilerin sağlanmasını talep edebilir. İlgili maddenin 6. fıkrasına göre; 13. ve 14. maddeler uyarınca ilgili kişiye sağlanacak bilgiler, amaçlanan işleme anlamlı bir genel bakış sağlamak adına kolayca görülebilir, anlaşılır ve net bir şekilde okunaklı olacak şekilde standart ikonlarla/simgelerle birlikte sağlanabilir. İkonların/Simgelerin elektronik olarak sunulduğu durumlarda makine tarafından okunabilir olması gerekmektedir. İlgili maddenin 8. ve son fıkrasına Avrupa Komisyonu, ikonlar/simgeler ile sunulacak bilgileri ve standartlaştırılmış ikonları/simgeleri sunma prosedürlerini belirlemek amacıyla, Madde 92'ye uygun kanun hükmünde kararnameler hazırlama yetkisine sahiptir (bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 12**, pp.39-40).

bilgilendirme elektronik yollarla sağlanmalıdır (GDPR m.12/3). Veri sorumlusu ilgili kişinin haklarını kullanmasını kolaylaştırmalıdır ve bu hakları kullanma konusunda ilgili kişiye yardımcı olmalıdır (GDPR m.12/2). İlgili kişinin 15-22. maddelere ilişkin işlem isteklerine yönelik veri sorumlusunun bilgi sağlama süresi maksimum 1 ay olmakla birlikte talep sayısı ve talebin karmaşıklığı söz konusu ise talepten sonraki 1 ay içinde bu gecikme ve nedenlerine yönelik bilgilendirme yapmış olmak kaydıyla 2 ay daha uzatılabilir (GDPR m.12/3). Diğer yandan veri sorumlusunun ilgili kişinin isteği üzerine işlem yapmama hakkı da bulunmaktadır. Ancak bu hakkın kullanımında veri sorumlusu tarafından gerekçelerin ilgili kişiye belirtilmesi gerekliliğinin yanı sıra bir denetleme otoritesine şikâyetle bulunma ve yargı yoluna başvurma hakkı olduğunun da ilgili kişiye talep alındıktan sonraki 1 ay içinde belirtilmesi gerekmektedir (GDPR m.12/4). GDPR 13-14. ve 15-22. maddelerinde belirtilen bilgilerin ve iletişimin sağlanması ücretsiz olarak yerine getirilmekle birlikte ilgili kişiden gelen taleplerin açıkça temelsiz veya aşırı olduğu durumlarda makul bir ücretlendirme yapılabilir (GDPR m.12/5). GDPR 15-21. maddelerinde belirtilen talebi yapan gerçek kişinin kimliği ile ilgili makul şüpheler bulunması halinde veri sorumlusu, 11. maddeye halel getirmeksizin, ilgili kişinin kimliğini doğrulamak için gerekli ek bilgilerin sağlanmasını talep edebilir (GDPR m.12/6). GDPR 13-14. maddeler uyarınca ilgili kişiye sağlanacak bilgilerin, makine tarafından okunabilir olması şartıyla, kolayca görülebilir, anlaşılır ve net bir şekilde okunaklı olacak şekilde standart ikonlarla/simgelerle birlikte sağlanabilmesi mümkündür (GDPR m.12/7) ve Avrupa Komisyonu'nun bu konuda kanun hükmünde kararnameler hazırlama yetkisi bulunmaktadır (GDPR m.12/8)¹⁶¹.

GDPR'nin 12. maddesinde geçen şeffaflık ve ilgili kişileri bilgilendirme ilkeleri, Türk hukukunda temel olarak 6698 sayılı KVKK'nın "Haklar ve Yükümlülükler" başlıklı Üçüncü Bölümde yer alan "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10. maddesinde geçen hükümlere karşılık gelmekle birlikte, aynı bölümde yer alan "İlgili kişinin hakları" başlıklı 11. maddedeki hükümleri, "Başvuru, Şikâyet ve Veri Sorumluları Sicili" başlıklı Dördüncü Bölümde yer alan "Veri sorumlusuna başvuru" başlıklı 13. maddedeki hükümleri ve aynı bölümde yer alan "Kurula şikâyet" başlıklı 14. maddedeki hükümleri¹⁶² de kapsamaktadır. Yine de

¹⁶¹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 12**, pp.39-40.

¹⁶² KVKK, **m.10-11, m.13-14**.

KVKK'nın bu maddelerinde geçen hükümlerin GDPR'nin 12. maddesinde geçen hükümlerin tamamını karşılayamadığı da görülmektedir.

6698 sayılı KVKK m.10/1'e¹⁶³ göre veri sorumlusunun veya yetki verdiği kişinin ilgili kişiyi aydınlatma yükümlülüğü bulunmaktadır. Bu yükümlülük; 10 maddede geçen veri sorumlusu ve mevcutsa temsilcisinin kimliğine, kişisel verilerin işleme amacına ve kimlere ne gibi gerekçelerle aktarılabilmesine yönelik ve ayrıca 11. maddede geçen ilgili kişinin sahip olduğu haklara yönelik bilgi verme yükümlülüklerini kapsamaktadır. İlgili kişinin sahip olduğu bu haklar ise 11. maddede; herkesin kendisine ilişkin herhangi bir kişisel verinin işlenip işlenmediğine yönelik bilgi isteme, kişisel veri işlenmiş ise buna yönelik bilgi isteme, bu verilerin hangi amaçla işlendiğini ve amaca uygun işleme yapılıp yapılmadığını öğrenme, yurtiçi ya da yurtdışında bu verilerin gönderildiği üçüncü şahısları öğrenme, varsa bu verilerdeki eksiklik ya da yanlışlıkların düzeltilmesini talep etme, aynı kanunun 7. maddesi uyarınca kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde bunların silinmesi ya da yok edilmesini talep etme; düzeltme, silme ve/veya yok edilme durumlarında bu verilerin yurtiçi ya da yurtdışında gönderildiği üçüncü şahısların da bu konuda bilgilendirilmesini talep etme, işlenen kişisel verilerin özellikle otomatik sistemler yoluyla analizi sonucu ilgili kişinin aleyhine sonuç doğurmasına itiraz etme ve son olarak ilgili kişinin kişisel verilerinin yasalara uygun olmayacak şekilde işlenmesi nedeniyle ilgili kişi için herhangi bir zarar doğurması halinde bu zararların tazminini isteme hakları şeklinde geçmektedir. KVKK'nın 13. maddesinde ise tıpkı GDPR m.12'de olduğu gibi veri sorumlusunun ilgili kişi tarafından talep edilen KVKK gereğince hakkı bulunan bilgileri en kısa sürede ve en geç 30 gün içinde ve ücretsiz olarak karşılama yükümlülüğü bulunmakta; yine GDPR m.12'de olduğu gibi istenen bilgilerin niteliğinin bir maliyet gerektirmesi halinde kurul tarafından belirlenen tarifiede geçen ücret karşılığında iletilmesini gerektirmektedir. Yine GDPR m.12'de olduğu KVKK m.13/2'ye göre de veri sorumlusunun talebi kabul etme ya da gerekçesini açıklayarak reddetme hakkı bulunmaktadır. Ancak yanıtın GDPR m.12'de geçen sözlü olarak iletilmesi KVKK'da geçmemekte, KVKK m.13/3'e göre yanıtın elektronik yol da dahil olmak üzere yazılı olarak verilmesi gerekmektedir. KVKK m.14/1-2'ye göre ilgili kişinin başvuru talebinin veri sorumlusu tarafından reddi, alınan yanıtın yetersizliği ya da 30 gün

¹⁶³ KVKK, m.10/1.

içinde yanıt alınamaması hallerinde ilgili kişinin yanıtı aldığı an ve/veya 30 günlük sürenin bitimi itibarıyla 60 gün içinde kurula şikâyet hakkı bulunmaktadır. İlgili kişinin kişilik haklarının ihlâli durumunda genel hükümler gereğince tazminat hakkının bulunduğu KVKK m.14/3'te düzenlenmiştir.¹⁶⁴

Bilgilendirme yükümlüğü, kişisel verilerinin korunması bakımından oldukça önemli bir ilkedir. Zira kendisi hakkında kişisel verilerinin işlendiğini veya bu konudaki haklarını bilmeyen bir kişinin kişisel verilerinin korunmasına yönelik kanunun kendisine tanıdığı hakları kullanabilmesi de söz konusu olamaz. Bu ilke aynı zamanda kişisel verilerin işlenmesinde dürüstlük ilkesine dolayısıyla şeffaflık ilkesine uyulmasının da bir gereğidir.

Artık bireylerin uzun bilgilendirme metinlerini okumaması, verilerin sensörlerle toplandığı anlarda bilgilendirme yapmanın zorluğu, YZ sistemlerinde kullanılan analiz yöntemlerinin ilgili kişilere açıklanma güçlüğü, veri sorumlularının önceden öngöremediği veri işleme faaliyetleri nedeniyle bilgilendirme metinlerinin adil ve şeffaf veri işleme faaliyetini gerçekleştirme hususunda yetersiz kaldığı ifade edilmektedir. Bu nedenle anlaşılması güç hukuki ifadeler içeren uzun bilgilendirme metinlerinin değiştirilmesi ve yeni yöntemlerin üretilmesi gerekmektedir.¹⁶⁵

Sade bir dil ile bilgilendirme metinlerinin yazılması, video aracılığıyla anlatım, bilgilendirme metinlerinde görsellerin kullanılması, logo ve simgelerin eklenmesi, katmanlı ve just-in-time bilgilendirme yöntemlerinin tercih edilmesi kişisel verilerin düzenlemelere uyumlu işlenebilmesine katkı sağlayacak önerilerden birkaçıdır.¹⁶⁶

2.2.2. Hesap Verilebilirlik İlkesi

Şeffaflık ilkesinin açıklandığı bölümde değinildiği üzere şeffaflığın sağlandığı hükümetler sahip oldukları iktidara dayalı olarak güçlerini nasıl kullandıklarına ilişkin hesap verebilir olması beklenir. Bireylerin nasıl yönetildiğini anlaması ve kendilerini ilgilendiren kararların gerekçelerini öğrenmesi hesap verilebilirlik ilkesinin

¹⁶⁴ KVKK, m.10-11, m.13-14.

¹⁶⁵ ICO, *Ibid.*, pp.65-67.

¹⁶⁶ ICO, *Ibid.*, p.110.

amaçlarındandır.¹⁶⁷ Hesap verilebilirlik; “ne yapıyorsak onu söylüyoruz, ne söylüyorsak onu yapıyoruz” şeklinde basitçe ifade edilebilir.

Hesap verebilirlik ilkesi, verileri işlenen kişinin veri sorumlusuna hesap sorabilme gerekliliğinin sonucu olarak ortaya çıkmıştır. Bu ilke, verilerin işlenmesi sırasında sağlamlık ve güvenin sağlanmasına yönelik olarak veri sorumlusuna yüklenen bir yükümlülüktür. Kişisel verilerin işlenmesi sırasında gereken tedbirleri almak ve talep edildiğinde en kısa süre içinde kişisel verilerin yasalarca daha önce belirlenmiş hükümlere uygun olarak işlendiğini kanıtlayan belge ve bilgilerin sunulması, bunun yanı sıra hesap verebilirlik ilkesi doğrultusunda, veri işlemenin kanunda belirtilmiş diğer ilkelere de uygun olarak yürütülmesi sorumlulukları veri sorumlusunun üzerindedir.¹⁶⁸

Hesap verebilirlik (*accountability*) ilkesi GDPR’nin 5. maddesinde düzenlenmiştir. İlgili maddenin 2. fıkrasına göre, hesap verebilirlik ilkesi gereğince, veri sorumlusunun kişisel veriler ve bunların işlenmesiyle ilgili GDPR m.5/1’de belirtilen uyulması gereken ilkelere ve yaptığı işlemlerin bu ilkelere uygun olduğunu ispat sorumluluğu bulunmaktadır. Veri sorumlusunun işlemlerinde hesap vermekle yükümlü olduğu bu ilkeler GDPR m.5/1’de; kişisel verilerin işlenmesinin hukuka uygun, adil ve şeffaf olması (GDPR m.5/1a), doğru ve gerektiğinde güncel olması, işleme amaçları dikkate alınarak, yanlış olan kişisel verilerin gecikmeden silinmesini veya düzeltilmesini sağlamak için her makul adımın atılması (GDPR m.5/1d), kişisel verilerin belirli, açık ve meşru amaçlar için toplanmış ve bu amaçlara aykırı şekilde işlenmemiş olması (GDPR m.5/1b), amaçla ilgili/bağılantılı olması, yeterli/ölçülü ve sınırlı olması (GDPR m.5/1c), kişisel verilerin işlendiği amaçlar çerçevesinde gerekenden daha uzun süre ilgili kişinin kimliğinin tanımlanmasına izin verecek biçimde tutulmaması; yalnızca kamu yararı için arşivleme, bilimsel veya tarihsel araştırma amaçlı veya istatistiksel amaçlarla uygun teknik ve kurumun uygulanmasına tabi olan m.89/1’e göre istatistiksel amaçlarla işleneceği için uzun süre saklanabilmesinin veri konusundaki hakların ve özgürlüklerin güvence altına

¹⁶⁷ Tom Willems, Wouter Van Dooren, "Coming to terms with accountability: Combining multiple forums and functions", **Public Management Review**, Vol.14, No.7, 2012, pp.1011-1036.

¹⁶⁸ Erkan Ağırılan, “Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi”, Yüksek Lisans Tezi, **T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü**, Ankara, 2015, s.12.

alınması için bu GDPR'nin gerektirdiği tedbirlere tabi olması (depolama sınırlaması - *storage limitation*) (GDPR m.5/1e) ve son olarak da kişisel verilerin, yetkisiz veya yasadışı işlemeye karşı ve uygun teknik veya örgütsel tedbirleri kullanarak kazara kayba, tahrip veya tahribata karşı koruma dahil olmak üzere uygun güvenliğinin sağlayacak şekilde işlenmiş olması (bütünlük ve gizlilik - *integrity and confidentiality*)¹⁶⁹ şeklinde sıralanmıştır. Buna göre veri sorumlusunun veri işlemeyle ilgili tüm işlemlerde KVK'na yönelik ilkelere uygun hareket etme ve talep edildiğinde bu yönde işlemler yaptığını belgeleme sorumluluğu bulunmaktadır.

Hesap Verilebilirliğin sağlanabilmesi için kurum ve kuruluşların; kişisel verileri işleme envanterleri hazırlaması, kişisel veri işlemeye ilişkin süreçleri ve işleme amaçlarını belirlemesi, işledikleri tüm kişisel verileri tespit etmesi ve haritalandırması gerekmektedir. YZ sistemleri, kişisel verileri iş süreçlerinin gereksinimlerine göre analiz edip farklı iş süreçlerinin ortaya çıkmasıyla veri setlerindeki ilişkileri tespit edip yeni veri işleme amaçları üretebilmektedir.¹⁷⁰

Daha önce 95/46 Yönergesinin ulusal düzenlemeye uyarlanması sürecinde Alman Federal Kişisel Verileri Koruma Kanununda detaylı olarak düzenlendiğini gördüğümüz Veri Koruma Görevlisi¹⁷¹ (Data Protection Officer bundan böyle "DPO" olarak adlandırılacaktır), hesap verilebilirliğin sağlanması adına GDPR kapsamında getirilen önemli yükümlülüklerdendir.

Yapay zekâ perspektifinden bakıldığında ise yakın zamana dek YZ sistemlerine yönelik düzenlemelerin çok kapsamlı olmadığı görülmektedir. Buna göre, insan kullanıcıların nihai kararı vermede sağduyularını kullanacağı varsayılmıştır. Ancak dünya genelinde birbiri peşi sıra gelen yakın zamanlı ve kapsamlı düzenlemelere rağmen insanların YZ sistemlerine çok fazla güvenmesin karşın sistemin önemli hata ve ihlallere yol açtığı birçok durumla karşılaşmıştır. YZ

¹⁶⁹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 5**, pp.35-36.

¹⁷⁰ Alexei Andreev, "The Death of the Hypothesis, or, Investing in Big Data Analytics and Deep Learning", **Harris and Harris Group**, September 23, 2014. (Çevrimiçi) <http://www.hhvc.com/blog/death-hypothesis-investing-big-data-analytics-deep-learning/> 31 December 2019

¹⁷¹ SKW Schwarz, "The New German Federal Data Protection Act", **SKW Schwarz IT-Ticker - Special Issue**, 7 January, 2017. (Çevrimiçi) https://www.skwschwarz.de/fileadmin/user_upload/Artikel_Dokumente/BDSG-neu_2017-06-07_EN.pdf 31 December 2019

sistemleri daha yaygın ve birbirini etkileyen alanlarda kullanıldığından, bunların yeterince düzenlenip düzenlenmediği ve ne ölçüde hesap verebilir olduğuna yönelik kaygılar artmaktadır. Kötü düzenlemelerin YZ sistemlerinin hesap verebilirliğini iyileştirmesi mümkün olmamakla birlikte aynı zamanda bu sistemlerin birçok faydalı uygulamalarını da engellemesi söz konusudur. Diğer yandan yeterince kapsamlı olmayan düzenlemelerin sadece kişisel verilerin korunması hakkının değil birçok hakkın ihlaline yol açması da muhtemeldir.¹⁷² Bu nedenle de kişisel verilere ilişkin hesap verebilirlik ilkesi aynı zamanda YZ sistemlerinin bir bütün olarak hesap verebilirliği ve bu sistemlerin gelişimi ile de yakından ilişkilidir.

YZ sistemlerinin kişisel verilerin korunmasını en çok ilgilendiren kullanımlarından ve bu konuda hesap verebilirliği en çok etkileyen hususlardan birisi, özel sektörden ziyade kamu kuruluşlarının kamu düzenini sağlamaya ve dijital teknolojilere dayalı akıllı yönetim anlayışını gerçekleştirmeye çalıştığı örneklerdir. Akıllı yönetim, kamu idarelerinin sadece şeffaf olmalarını değil aynı zamanda YZ algoritmaları kullanarak aldıkları kararlardan da sorumlu olmalarını gerektirir. Hesap verebilirlik, YZ algoritmaları temelinde alınan kararları açıklama ve gerekçelendirme yükümlülüğünü ifade eder. Hesap verebilirlik yoluyla kamu idareleri, karar vermede YZ algoritmalarını kullanımlarını haklı çıkarmakta ve nasıl çalıştıklarını, hangi verileri kullandıklarını, hangi sonuçların beklendiğini ve hangi sonuçların elde edildiğini açıklamaktadırlar.¹⁷³ Bu konuya Bölüm 2.4.2.5'te değinileceğinden burada sadece kısa bir bahisle geçilmiştir.

2.2.3. Veri Güvenliği İlkesi

Kişisel verilerin; doğal afet, siber saldırı, sistemsel arızalar, veri sisteminden sorumlu kişinin dalgın, dikkatsiz ve/veya tedbirsiz davranması veyahut yetkinin

¹⁷² Finale Doshi-Velez, Mason Kortz, Ryan Budish, Christopher Bavitz, Samuel J. Gershman, David O'Brien, Stuart Shieber, Jim Waldo, David Weinberger, Alexandra Wood, "Accountability of AI Under the Law: The Role of Explanation", Working Paper, **Berkman Klein Center Working Group on Explanation and the Law**, 2017. (Çevrimiçi) https://dash.harvard.edu/bitstream/handle/1/34372584/2017-11_aiexplainability-1.pdf?sequence=3 6 December 2019.

¹⁷³ Agustí Cerrillo i Martínez, "How can we open the black box of public administration? Transparency and accountability in the use of algorithms", *Revista Catalana de Dret Public*, No.58, 2019, pp. 13–28, (Çevrimiçi) <http://revistes.eapc.gencat.cat/index.php/rcdp/article/download/10.2436-rcdp.i58.2019.3277/n58-cerrillo-en.pdf> 7 December 2019.

kötüye kullanımı gibi nedenlerle tehdit altında kalması söz konusu olabilir¹⁷⁴. Bu gibi tehditlere yönelik olarak gereken tedbirlerin alınmasında veri güvenliği ilkesi büyük öneme sahiptir.

Veri güvenliği ilkesine yönelik yükümlülükler, 6698 sayılı KVKK'nın 12. maddesinde yer alan toplam 5 fıkarda düzenlenmiştir. Buna göre; kişisel verilere ilişkin hukuka uygun olmayacak şekilde işleme ve erişimin önlenmesi ile bu verilerin korunmasının sağlanması için gereken güvenliğin edinilmesine ilişkin tüm idari ve teknik tedbirlerin alınmasından veri sorumlusu sorumludur (KVKK, m.12/1). Ancak kişisel verilerin veri sorumlusu adına gerçek ya da tüzel diğer kişi ve/veya kişilerce işleniyor olması durumunda ise KVKK, m.12/1'de geçen tedbirlerin alınmasına ilişkin sorumluluk hem veri sorumlusu hem de veri sorumlusunun kendi adına verileri işlemesine izin verdiği kişi/kişilerde olacaktır (KVKK, m.12/2). Veri sorumlusunun KVKK'ya yönelik yasal hükümlerin uygulanmasının sağlanmasında, bulunduğu/çalıştığı kurumda/kuruluşta gereken denetimleri yapma ya da yaptırma yükümlülüğü bulunmaktadır (KVKK, m.12/3). Toplanan kişisel verilerin başkalarına açıklanmamasına ve işleme amaçları haricinde kullanılmamasına ilişkin yükümlülük, veri sorumluları ve veri işleyenler açısından ömür boyu devam eden bir yükümlülüktür (KVKK, m.12/4). Toplanan kişisel verilerin hukuka aykırı bir şekilde bir başkası tarafından ele geçirilmesi durumunda veri sorumlusunun bu ihlâli mümkün olan en kısa süre içinde ilgili kişiye ve Kurula bildirmesi gerekmektedir. Kurul da gerekli ise bunu kendi web sitesi veya uygun bulduğu bir diğer yöntem ile ilan edebilir (KVKK, m.12/5).

2.3. YAPAY ZEKÂ SİSTEMLERİNDE KİŞİSEL VERİLERİN İŞLENMESİ

Teknolojideki gelişmelere paralel olarak işletmeler ve devletler, kişisel verilerini toplayarak işledikleri kişilerin davranış ve tercihlerini tahmin edebilmek amacıyla, “profilleme” ve “otomatik karar alma mekanizmaları”na dayanan büyük

¹⁷⁴ Nur Halet Avcioğlu, “Türk Hukukunda Kişisel Verilerin Korunması Hakkı”, Yüksek Lisans Tezi, **KTO Karatay Üniversitesi**, Konya, 2018, s.30.

veri uygulamalarına her geçen gün daha da çok başvurumaktadırlar¹⁷⁵. Bankacılık, finans, sağlık, vergilendirme, sigorta, pazarlama ve reklamcılık, karar vermeye yardımcı olmada profillemeye ve otomatik karar alma mekanizmalarının daha düzenli olarak kullanıldığı alanlardan başlıcalarıdır¹⁷⁶.

Bu bölümde YZ sistemlerinde kişisel verilerin işlenmesinde profillemeye ve otomatik karar alma mekanizmaları ele alınacaktır.

2.3.1. Profillemeye

Veri setlerinin, veri madenciliği yöntemleri ile işlenmesiyle kişilerin davranış eğilimleri ve karakterleri tahmin edilmeye çalışılmaktadır. Bu durum literatürde profillemeye veya segmentasyon olarak karşımıza çıkmaktadır. Profillemeyi; belirli bir kategorideki kişilerin kişisel verilerinin işlenerek yine o gruptaki kişiler hakkında bir bilgi (knowledge) veya sonuç (inferences) üretilmesi ve bunların da kişilerin vasıfları ve davranış biçimleri hakkında varsayımlarda bulunmak için kullanılması olarak tanımlayan araştırmacılar bulunmaktadır.¹⁷⁷

Bireylerin ve grupların nasıl yönetileceği, yönlendirileceği ve şekilleneceği yapılan profillemelere bağlıdır. Çünkü üretilen davranış biçimleri sınıflandırma algoritmaları aracılığıyla çeşitli grup ve profillerle eşleştirilmektedir. Profillemeyi kullanan Amerikan perakende şirketi Target, müşterilerine hamileliğin hangi ayında bulunduklarına bağlı olarak ilgilerini çekebilecek kuponları gönderebilmek için 25 ürününün satın alma modellerini analiz ederek kişilerin “hamilelik tahmini” skorlarını

¹⁷⁵ Şehriban İpek Aşıkoğlu, “Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri”, Yüksek Lisans Tezi, **İstanbul Üniversitesi**, İstanbul, 2018, s.142.

¹⁷⁶ Article 29 Data Protection Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 17/EN, WP251rev.01, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 2018 (Çevrimiçi) https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826 7 December 2019, p.5.

¹⁷⁷ Mireille Hildebrandt, “Defining Profiling: A New Type of Knowledge?”, In M. Hildebrandt, and S. Gutwirth (Eds.), Profiling The European Citizen, **Springer**, 2008.

belirledi. Ancak ailesinden hamile olduğunu gizleyen henüz daha yetişkin olmamış kişilerde bu durum ciddi problemlere neden oldu.¹⁷⁸

Kullanıcıların kimliklerini şekillendirdiği de ileri sürülen öneri sistemleri (recommendation systems) ne zaman ve nasıl egzersiz yapacağı, neyin ilgisini çekebileceği ve satın alabileceği, hangi rotayı tercih etmesi gerektiği ve kiminle bağlantı kurup ağına dahil etmesi gerektiği gibi hususlarda kişileri yönlendirmektedir.¹⁷⁹

YZ ve makine öğrenmesi alanındaki gelişmeler, kişilerin hak ve özgürlükleri üzerinde büyük etkileri bulunan profillemeye ve otomatik karar alma mekanizmalarına yönelik kullanımlarda kolaylık ve yaygınlık sağlamaktadır.¹⁸⁰ Teknolojideki gelişmelere paralel olarak yaygınlığı artan bu faaliyetler, 24 Ekim 1995 tarihinde yayımlanan ve 25 Mayıs 2018 tarihinde yürürlüğe giren GDPR ile yürürlükten kalkan 95/46/EC Sayılı Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi'nde kapsamlı bir biçimde düzenlenmemiştir. Bu Yönergenin devamı ancak sayısız eksikliğin giderilerek günümüz şartlarına daya uygun hale getirildiği GDPR'de gerek profillemeye ve otomatik karar alma mekanizmalarına yönelik sonuçlar gerekse profillemeye amaçlı kişisel veri toplanması ve oluşturulan bu profillerin kişilere yönelik ne tür uygulamalarda ve ne şekilde kullanılabileceğine yönelik gibi düzenlemelere de yer verilmiştir. Ancak KVKK'da profillemeye veya otomatik karar alma mekanizmalarına ilişkin bir tanım bulunmamaktadır.

AB'nin GDPR'sinin "*Definitions*" (Tanımlar) başlıklı 4. maddesinin 4. fıkrasında "profillemeye"nin (*profiling*) tanımı şu şekilde yapılmıştır: "Profillemeye veya profil oluşturma; bir gerçek kişiyle ilgili belirli kişisel yönleri değerlendirmek için kişisel verilerin kullanılmasından oluşan, özellikle o kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranış biçimi, konumu veya hareketlerine ilişkin yönleri analiz etmek veya tahmin etmek için

¹⁷⁸ Luciano Floridi, "Big Data and Their Epistemological Challenge", **Philosophy & Technology**, Vol.25, No.4, pp.435–437, (Çevrimiçi) <https://link.springer.com/content/pdf/10.1007%2Fs13347-012-0093-4.pdf> 31 December 2019.

¹⁷⁹ Katya Vries, "Identity, profiling algorithms and a world of ambient intelligence", **Ethics and Information Technology**, Vol.12, No.1, 2010, pp.71–85.

¹⁸⁰ Article 29 Data Protection Working Party, "**Guidelines on Automated...**", p.5.

kullanılan, kişisel verilerin otomatik olarak işlenmesi anlamına gelir”¹⁸¹ (GDPR m.4/4). Bu tanıma göre profillemeye; (1) kişisel veri kullanan/işleyen¹⁸², (2) verileri otomatik işleyen¹⁸³, (3) bir gerçek kişi ile ilgili belirli kişisel yönleri değerlendirmek için kullanılan bir faaliyettir.

Dolayısıyla profillemeye faaliyeti, tanımının ihtiva ettiği otomatik işlemenin kısmen veya tamamen otomatik olmasına göre ve ayrıca toplanan kişisel verilerin bir karar mekanizması yoluyla işlenip işlenmediği durumuna göre kendi içinde kısımlara ayrılmaktadır. Örneğin kısmi veya tamamen otomatik yolla profillemeye amaçlı toplanan bilgi henüz bir karar mekanizması ile değerlendirilmemişse bu “genel profillemeye” sayılmaktadır. Bu veri bir karar mekanizmasından yararlanılarak ancak insan yoluyla değerlendirilmişse “otomatik karar mekanizmalarından faydalanılan profillemeye” sayılmaktadır. Bu veri insan değerlendirmesi olmadan tamamen bir algoritmanın aldığı kararlar yoluyla otomatik karar verme mekanizmalarına dayanıyorsa da o zaman “tamamen otomatik karar mekanizmalarına dayanan profillemeye” sayılacaktır.¹⁸⁴

¹⁸¹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 4/4**, p.33.

¹⁸² Bir faaliyetin, kişisel veri işleme faaliyeti sayılabilmesi için 6698 sayılı KVKK m.2’ye göre; kişisel verileri (1) tamamiyle ya da kısmi olarak otomatik yolla veya (2) otomatik olmayan yolla ilk kez edinerek başlatılan veri işleme süreci ve takip eden diğer veri işleme faaliyetleri; KVKK m.3’deki tanıma göre ise “*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*” kişisel verilerin işlenmesi’ olarak değerlendirilir. Dolayısıyla insan eliyle otomatik olmayan yolla toplanan kişisel veriler de toplandıkları/elde edikleri anda ‘kişisel verilerin işlenmesi’ faaliyeti sayılacaktır.

¹⁸³ 6698 sayılı KVKK m.2’ye göre kişisel verinin otomatik, kısmen otomatik veya otomatik olmayan yollarla işlenebildiğinden bahsetmiştik. GDPR’ye göre ise bir faaliyetin profillemeye faaliyeti sayılabilmesi için kişisel verileri otomatik olarak işlemesi gerektiğini belirtmiştik. Bu tanımlara göre otomatik olmayan yolla, örneğin tamamen insan yoluyla gerçekleştirilen gerçek kişileri değerlendirme amaçlı bir faaliyetin/işlemin profillemeye olarak sayılmaması, ancak bir veri işleme faaliyeti olarak kabul edilmesi gerekmektedir. Ancak kısmen de olsa otomatik yolla toplanan ve insan yoluyla da işlenen gerçek kişilere ait kişisel verilerin bu kişileri değerlendirme amaçlı kullanılması, işin içinde insan eli olsun ya da olmasın kısmen otomatik işlemlere dayandığı için “profillemeye”nin tanımına girecektir.

¹⁸⁴ Örneğin GDPR’nin 71. paragrafında çevrimiçi bir kredi başvurusunun otomatik olarak reddedilmesi veya herhangi bir insan müdahalesi olmadan e-işe alım gibi uygulamaların tamamen otomatik işlemeye dayanan ve ilgili kişi üzerinde yasal etkiler yaratan veya önemli etkiler yaratma ihtimali olan, kişiyle ilgili kişisel yönleri değerlendiren profillemeye gibi karar mekanizmalarını da içine alan faaliyetlere örnek olarak gösterilmiş ve ilgili kişinin kendisiyle

GDPR'ye göre, kişisel veri, ilgili kişiden elde edilmiş olsun (GDPR m.13/2f)¹⁸⁵ ya da olmasın (GDPR m.14/2g)¹⁸⁶, veri sorumlusunun GDPR m.22/1 ve m.22/4'te belirtilen profillemeye dahil olmak üzere otomatik karar vermenin varlığına ilişkin ve varlığı halinde değerlendirmede kullanılan mantığa (yapılan değerlendirmenin çalışma mantığına) yönelik makul ve anlamlı bilgilerin yanı sıra, bu tür işlemlerin ilgili kişi açısından önemi ve öngörülen sonuçlarına ilişkin anlamlı bilgileri ilgili kişiye sunma ve işlemlerin ilgili kişiye ilişkin adil ve şeffaf olduğunu temin etme yükümlülüğü bulunmaktadır. Aynı zamanda GDPR m.15/1(h)'ye göre ilgili kişinin veri sorumlusundan kendisiyle ilgili kişisel verilerin işlenip işlenmediğine dair bilgi alma hakkının yanı sıra eğer kendisiyle ilgili kişisel bilgi işleniyorsa/işlenmişse bu bilgilere erişim hakkı ve yine GDPR m.22/1 ve m.22/4'te belirtilen profillemeye dahil olmak üzere otomatik karar vermenin varlığına ilişkin ve varlığı halinde değerlendirmede kullanılan mantığa (yapılan değerlendirmenin çalışma mantığına) yönelik makul ve anlamlı bilgilerin yanı sıra, bu tür işlemlerin ilgili kişi açısından önemi ve öngörülen sonuçlarına ilişkin anlamlı bilgileri isteme hakkı¹⁸⁷ bulunmaktadır. Dolayısıyla bu durumun, GDPR'de kişisel verinin doğrudan ilgili kişiden veya başka yollardan toplanmış olduğu her iki durumda da veri sorumlusu açısından bilgi verme/aydınlatma yükümlülüğü ve ilgili kişi açısından da bir bilgi isteme/alma hakkı olarak ayrı ayrı düzenlendiği görülmektedir. GDPR m.22'de ise profillemeye/profil oluşturma da dahil olmak üzere otomatik bireysel karar verme konusu "*Automated individual decision-making, including profiling*" başlığı altında ele alınmıştır. Yani GDPR m.22'de otomatik karar alma mekanizmaları ile profillemeye birlikte ele alınmıştır. GDPR m.22/1'e göre ilgili kişi, kendisi ile ilgili yasal etkiler veya benzeri önemli etkiler yaratan, profil oluşturma dahil olmak üzere yalnızca otomatik işlemeye dayalı alınan bir karara tabi olmama, reddetme/itiraz etme hakkına sahiptir. Ancak GDPR m.22/2'ye göre; (a) kararın ilgili kişi ile veri sorumlusu arasında bir sözleşmeye girilmesi veya uygulanması için gerekli olması; (b) kararın veri sorumlusunun tabi olduğu Birlik veya Üye Devlet yasaları tarafından yetkilendirilmesi

ilgili alınan bu tür otomatik kararlara tabi olmama, reddetme/itiraz etme hakkına sahip olması gerektiğinden bahsetmektedir (bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, par.71**).

¹⁸⁵ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 13/2f**, p.41.

¹⁸⁶ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 14/2g**, p.42.

¹⁸⁷ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 15/1h**, p.43.

ve veri konusunun hak ve özgürlüklerini ve meşru çıkarlarını korumak için uygun tedbirler getirmesi ve (c) kararın ilgili kişinin açık onayına dayanması hallerinde, m.22/1 geçerli olmayacaktır. GDPR m.22/3'e göre ise GDPR m.22'nin 2. fıkrasının (a) ve (c) bentlerinde belirtilen durumlarda, veri sorumlusu, ilgili kişinin hak ve özgürlüklerini ve meşru menfaatlerini, en azından bu konuda insan müdahalesi alma hakkını korumak için, ilgili kişinin bakış açısını ifade ve karara itiraz etmek için uygun tedbirler almalıdır. GDPR m.22/4'e göre ise GDPR m.22/2'de atıfta bulunulan kararlar, m.9/2 'nin (a) veya (g) noktalarının uygulanmadığı ve ilgili kişinin hak ve özgürlükleri ile meşru çıkarlarının korunması için uygun tedbirler söz konusu olmadığı sürece, m.9/1'de belirtilen özel kişisel veri kategorilerine¹⁸⁸ dayandırılmayacaktır.¹⁸⁹

Özet olarak, 22. madde şunları sağlamaktadır¹⁹⁰:

- i. Kural olarak, yasal veya benzer şekilde önemli bir etkiye sahip olan profillemeye dahil olmak üzere, tamamen otomatikleştirilmiş bireysel karar verme mekanizmaları genel olarak yasaktır.
- ii. Bu kuralın istisnaları vardır.
- iii. Bu istisnalardan birinin geçerli olduğu durumlarda, ilgili kişinin hak ve özgürlüklerini ve meşru çıkarlarını korumak için tedbirler alınıyor olması söz konusu olmalıdır.

Diğer yandan, otomatikleştirilmiş bireysel karar verme mekanizmalarına insan müdahalesi eklenmesi, kararın tamamen bir algoritma tarafından belirli

¹⁸⁸ GDPR'nin 9. maddesinde ırksal veya etnik kökene işaret eden kişisel veriler, siyasi görüşleri ortaya koyan kişisel veriler, dini veya felsefi inançları açığa çıkaran kişisel veriler, sendika üyeliğini ortaya koyan kişisel veriler, genetik veriler, biyometrik veriler (tanımlama amacıyla kullanıldığı yerlerde), sağlıkla ilgili veriler, bir kişinin cinsel yaşamına ilişkin veriler ve bir kişinin cinsel yönelimi ile ilgili veriler özel nitelikli veriler olarak kabul edilmiştir (bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, Article 9, pp.38-39). 6698 sayılı KVKK'nın 6.maddesinin 1. fıkrasında ise ırk, etnik köken, siyasi görüşler, dini ve felsefi inançlar, mezhep ya da diğer inançlar, giyim tarzı, bir derneğe, vakıfa veya sendikaya üyelik durumu, sağlık, cinsel hayat, herhangi bir cezadan mahkûmiyet yaşayıp yaşamadığı ve güvenlik tedbirleri ile ilgili verilerin yanı sıra genetik ve biyometrik veriler, özel nitelikli kişisel veriler arasında sıralanmıştır (bkz. KVKK, m.6).

¹⁸⁹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 22**, p.46.

¹⁹⁰ Article 29 Data Protection Working Party, "**Guidelines on Automated...**", p.19.

kriterlere dayalı olarak alınması ve/veya bir insan etkisinin algoritmanın değerlendirdiği kriterler dışında başka kriterleri de değerlendirmeden algoritma kararını onaylaması ve/veya insan etkisinin işlevsel ve/veya anlamlı düzeyde olmaması halinde kararın tamamen otomatik karar alma mekanizmalarıyla alınmış olduğu gerçeğini değiştirmeyecektir ki bu da veri sorumlusunun bu konudaki yükümlülüklerini ve/veya ilgili kişinin bu konudaki haklarını ortadan kaldırmayacaktır¹⁹¹. İlgili kişilerle ilgili profillemeleri kişisel verilerin korunması açısından incelediğimizde;

1. Verilerin profil üretmek amacıyla nasıl toplandığı,
2. Bireylerin kendileriyle ilgili işlenen verilere nasıl erişim sağlayacağı,
3. Üretilen profillerin kullanımı ve aktarılmasını nasıl kontrol edebileceği

şeklinde soruları sıralayabiliriz¹⁹².

Profillemeyele ilgili incelenen diğer bir husus da özel nitelikli olmayan kişisel verilerden olan, örneğin satın almaya veya web sitelerindeki gezintiye ilişkin verilerin sağlık gibi hassas verilere algoritmalar aracılığıyla dönüştürülmesinde bu verilerin KVK'ya uygun nasıl işlenebileceği ve korunabileceğidir. Sosyal medyadaki verilerimizin politik görüşümüze dair bilgiye dönüştürüldüğü, konum bilginimizin sağlığımıza dair çıkarımlar yapmayı sağladığı bir zamanda daha fazla soru sorarak üzerinde dikkatle düşünülmesi gerekecektir.¹⁹³

2.3.2. Otomatik Karar Alma Mekanizmaları

Günümüz koşullarında çoğunlukla kredi veren kuruluşlar, sigorta firmaları, işçi bulma kuruluşları, işe alım ve reklam verme konularında işletmeler, profillemeye ilişkin faaliyetlerde bulunmakta, elde ettikleri verileri otomatik karar alma mekanizmaları yardımıyla değerlendirmektedirler. Kişilere verilecek kredi miktarını ve kişinin krediyi ödemedeki risk seviyesini mevcut kredi geçmişi, krediye başvurma

¹⁹¹ Aşkoğlu, **a.g.e.**, s.144; Article 29 Data Protection Working Party, “**Guidelines on Automated...**”, p.20.

¹⁹² 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**, Vol.18, May 24, 2017, pp.18-84. (Çevrimiçi) <https://ssrn.com/abstract=2972855> 31 December 2019.

¹⁹³ Edwards / Veale, **Ibid.**

sıklığı, bir yerde sigortalı çalışıp çalışmadığı, aldığı maaş, diğer kredi ödemeleri, ödemelerinin toplam kredilerine oranı vb. kredi alışkanlıklarından yola çıkarak “kredi risk notu” şeklinde hesaplayan sistemlerde veya binleri, on binleri aşkın çalışana sahip büyük şirketlerde yoğun olan işe giriş/çıkış sirkülasyonu ile baş edebilmek, bu konuda insan çalışan sayısını asgari düzeyde tutmak, etik kurallara uygun olarak adil bir ön değerlendirme yapmak için profillemeye verilerini kullanan otomatik karar mekanizmalarından yararlanmaktadırlar. Pazarlamadaysa reklam veren işletmeler tarafından etkin bütçe yönetimi amacıyla tüketicilere yönelik bilgiler içeren profillere dayalı olarak hedef kitleye özel reklam gösteren uygulamalar tercih edilmektedir.¹⁹⁴

Otomatik karar mekanizmalarını profilemeden ayıran husus “bir insanın müdahalesi” faktörüdür. Otomatik karar alma mekanizmalarındaki algoritmalarda insan müdahalesinin kullanılmadığı, tamamen algoritmanın kendisine yüklenen kriterler doğrultusunda tek başına verdiği bir karar ile elde edilen bir değerlendirme sonucu söz konusudur. Kişinin kredi geçmişi ve alışkanlıklarına dayalı olarak otomatik olarak verilen kredi risk notları buna en iyi örnektir. Otomatik karar mekanizmalarında yapılan değerlendirmeler sonucu herhangi bir kişisel profilin oluşturulup oluşturulmaması önemli değildir. Genelde profilemede sıklıkla otomatik karar alma mekanizmaları kullanılmakla beraber bu mekanizmalardan yararlanmaksızın yapılan profilemeler de mümkün olabilmektedir. Örneğin, otoyollardaki trafik kameralarının yoldan geçen araçların ortalama hızlarını otomatik bir şekilde hesaplamak suretiyle trafik cezası yazma işlemi, profilemeye yönelik bir işleme dayanmayan bir otomatik karar alma mekanizması işlemidir. Diğer yandan, bir kişinin zaman içindeki araç sürme alışkanlıklarını izleyerek kişilere özel sürüş profilleri oluşturma işlemi sayesinde profileme işlemine dayalı bir karar alınması söz konusu olacaktır.¹⁹⁵

Daha önce de bahsedildiği ancak otomatik karar alma mekanizmalarını ilgilendirmesi nedeniyle yeniden bahsedilmesinde fayda görüldüğü üzere, AB’nin GDPR’sinin 71. paragrafında, ilgili kişinin, tamamen otomatik işlemeye dayanan ve ilgili kişi üzerinde yasal etkiler yaratan veya önemli etkiler yaratma ihtimali olan,

¹⁹⁴ Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, “EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies”, **Computer Law & Security Reviews**, Cilt.34, Sayı.1, 2018, pp.134-153, p.141.

¹⁹⁵ Aşıkoğlu, **a.g.e.**, s.142.

kişiyile ilgili kişisel yönleri değerdendiren profillemeye dahil olmak üzere otomatik karar alma mekanizmalarının aldığı bu tür otomatik kararlara tabi olmama, reddetme/itiraz etme hakkına sahip olduğu belirtilmiştir.¹⁹⁶ Benzer şekilde otomatik karar alma mekanizmaları ile profillemenin birlikte ele alındığı GDPR m.22'nin 1. fıkrasında da ilgili kişinin, kendisi ile ilgili yasal etkiler veya benzeri önemli etkiler yaratan, profil oluşturma dahil olmak üzere yalnızca otomatik işlemeye dayalı alınan bir karara tabi olmama, reddetme/itiraz etme hakkına sahip olduğu ancak bunun bazı istisnaları olduğu da açıkça belirtilmiştir. GDPR m.22/2'de bu istisnalar; (a) kararın ilgili kişi ile veri sorumlusu arasında bir sözleşmeye girilmesi veya uygulanması için gerekli olması; (b) kararın veri sorumlusunun tabi olduğu Birlik veya Üye Devlet yasaları tarafından yetkilendirilmesi ve veri konusunun hak ve özgürlüklerini ve meşru çıkarlarını korumak için uygun tedbirler getirmesi ve (c) kararın ilgili kişinin açık onayına dayanması hallerinde m.22/1'in hükümlerinin geçerli olmayacağı yönündedir¹⁹⁷. Yazında GDPR'nin otomatik karar alma mekanizmalarıyla ilgili bu düzenlemelerinin dar yorumlanma ve/veya sıkı bir biçimde uygulanma ihtimali nedeniyle büyük veri uygulamalarının beklenen yararlarının engellenebileceği konusunda endişe bildiren görüşler¹⁹⁸ de bulunmaktadır.

2.4. ALGORİTMALAR

Bu bölümde genel olarak algoritmalar ele alındıktan sonra algoritmik sistemlerin kişisel verilerin korunması bakımından değerlendirilmesi yapılacaktır.

2.4.1. Genel Olarak

Algoritmaların tanımı konusunda teknik anlam ve popüler anlam diyebileceğimiz iki çeşit yaklaşım bulunmaktadır. Teknik tanım olarak Hill; *“Verilen talimatlar uyarınca istenilen amacı gerçekleştiren sonlu, soyut, etkili, birleşik kontrol yapısı bulunan matematiksel yapılar”* şeklinde ifade etmiştir. Ancak talimatlar ve

¹⁹⁶ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, par.71**.

¹⁹⁷ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 22**, p.46.

¹⁹⁸ Tal Z. Zarsky, “Incompatible: The GDPR in the Age of Big Data”, **Seton Hall Law Review**, Vol.47, No.4, 2017, pp.995-1020, pp.1002, 1017.

amaç söz konusu olduğu için algoritmaların uygulanması (implementation) ve faaliyete alınması (executed) etki doğurabilmesi ve aksiyon alınabilmesi için gerekmektedir. Popüler tanım bu noktada öne çıkmaktadır. Halk arasında algoritmalar denildiğinde bu matematiksel yapıların teknolojilere uygulanması ve yapılandırılmış teknolojilerin belirli bir amaç doğrultusunda kullanılması anlaşılmaktadır.¹⁹⁹ Çalışmamda daha ziyade halk arasında anlaşıldığı şekliyle algoritmalarından kastedilen anlam kullanılacaktır.

Farklı hesaplama ve değerlendirmelerde kullanılan algoritmalar birçok insan aktivitesinde önemli bir rol oynamaktadır. Arama algoritmaları çevrimiçi bilgi arayışını yapılandırırken; işletme yönetimi sistemlerinde kullanılan algoritmalar çalışanların en iyi şekilde farklı görevlere ve vardiyalara nasıl tahsis edilmesi gerektiğine yardımcı olmaktadır. Birebir ticari iletişim platformlarında kullanılan algoritmalar, işgücü, beceri, bilgi ve maddi mallarda yeni tür geçici işlemlere izin verirken; trafik yönetimi gibi izleme sistemlerinde kullanılan algoritmalar olayların tahmin edilmesine ve müdahale gerektirebilecek muhtemel durumların belirlenmesine yardımcı olmayı hedeflemektedirler.²⁰⁰

Sayırsız algoritma türü bulunmaktadır. Ancak bu bölümde kişisel verilerin işlenmesini ilgilendiren arama, sıralama ve şifreleme algoritmaları ele alınacaktır.

2.4.1.1. Arama Algoritmaları

Günümüzde arama algoritmaları denildiğinde ilk akla gelen internet üzerinden istenilen bilginin elde edilmesine yarayan arama motorlarında kullanılan çevrimiçi algoritmalar gelmektedir. Ancak bunlar dışında gerek kişisel gerekse şirket bilgisayarlarında çevrimdışı olarak da arama yapmaya yardımcı olan arama algoritmaları da bulunmaktadır. Arama algoritmalarının temeli istenilen bilgiye erişme, bilgiyi elde etme, bilginin geri getirilmesi (*Information Retrieval*) fikrine dayanır

¹⁹⁹ Robin K. Hill, "What an Algorithm Is", **Philosophy & Technology**, Vol.29, No.1, 2016, pp.35–59. (Çevrimiçi) <https://philpapers.org/rec/HILWAA> 31 December 2019.

²⁰⁰ Bennett Borden, Jessica Lee, Alexandra Ross, Yodi Hailemariam, "Minority Report: The Ethics & Impacts of Algorithms", **MCCa Global Tec Forum**, 4-5 April, 2019, San Francisco, CA, (Çevrimiçi) <https://www.mcca.com/wp-content/uploads/2019/04/Minority-Report-The-Ethics-and-Impacts-of-Algorithms.pdf> 8 December 2019.

ki bu da başlı başına bir bilim dalıdır.²⁰¹ Öncülüğünü Gerard Salton'ın yaptığı ve 1960'lı yıllardan 1990'ların başlarına kadar önemli katkılarda bulunduğu bu bilim dalını Salton; "bilgiyi yapılandırma, analiz etme, organize etme (düzenleme), depolama, arama ve geri getirme konularıyla ilgili bilim dalı" şeklinde tanımlamıştır²⁰². Çevrimdışı ortamlarda kullanılan arama algoritmalarına örnek olarak Boolean, vector space, olasılık (probabilistic), meta modelleri kullanan algoritmalar gösterilebilir. Daha fazla veri içermesi, dinamik, link (bağlantı) yapılı ve kendinden organize olma özellikleriyle geleneksel (çevrimdışı) olanlardan ayrılan çevrimiçi arama motorları ise istenilen bilgiyi en hızlı ve istenilen bilgiye en yakın olacak şekilde (kalite) getirmede birden fazla algoritmayı bünyesinde barındırabilmektedir²⁰³.

Arama motorları; indeksler (içerik indeksi, yapı indeksi, özel amaç indeksi), modüller (*Indexing* - İçerik modülü, *Query* - Sorgu modülü, *Ranking* - Sıralama modülü, *Crawler* - Tarama modülü), kullanıcı ara yüzü ve web sayfaları olmak üzere birçok bölümden oluşur²⁰⁴. Günümüzde web üzerinden internet erişimi olan herkese açık olarak kullanılan arama algoritmaları arasında en gelişmiş (en hızlı ve en kaliteli bilgiyi getiren) olanın Google arama motorunda kullanılan algoritma olduğu düşünülmektedir.

2.4.1.2. Sıralama Algoritmaları

Algoritmalar, sıralama (*ranking*) amacıyla da kullanılabilir. Pek çok hizmet, daha büyük bir öge kümesi içinden seçilen belirli sayıda bir kısa liste oluşturmayı sağlayan veya önceden belirlenmiş kriterlere göre bir dizi öğeyi sıralayan "filtreleme" veya "sıralama" algoritmaları içerir. Sıralama algoritmalarının uygulama alanları arasında; karşılaştırma web siteleri (seyahat, sigorta, finansal hizmetler,

²⁰¹ Muhittin Işık, "Arama Motorları Mimarisi, Web Sayfalarının İçerik Skoru ve Google Pagerank Formülünün İncelenmesi", Yüksek Lisans Tezi, **Kadir Has Üniversitesi**, İstanbul, 2013, s.1.

²⁰² W. Bruce Croft, Donald Metzler, Trevor Strohman, "Search Engines - Information Retrieval in Practice". Pearson, New Jersey, 2010, p.1. (Çevrimiçi) https://ciir.cs.umass.edu/downloads/SE_IRiP.pdf 8 December 2019.

²⁰³ Işık, **a.g.e.**, s.1.

²⁰⁴ Amy N. Langville, Carl D. Meyer, "Google's PageRank and Beyond: The Science of Search Engine Rankings", **Princeton University Press**, Princeton, New Jersey, 2006, (Çevrimiçi) <http://geza.kzoo.edu/~erdi/patent/langvillebook.pdf> 8 December 2019.

telekomünikasyon ve enerji gibi) ve ayrıca e-ticaret platformları, uygulama mağazaları ve arama motorları sayılabilir. Sıralama algoritmaları bazen “ilgi düzeyi algoritmaları” olarak da adlandırılır. Ayrıca, bu algoritmalar aynı zamanda ilgili kullanıcıya gösterilebilecek tüm yayınların bir sıralamasını gerektiren “haber akışı” işlevlerini içeren birçok sosyal medya hizmetinin de önemli bir ögesidir. Sıralama algoritmaları, sıralanan öğeleri bir kullanıcının ihtiyaçlarına veya tercihlerine göre ayarlayarak arama maliyetlerini düşürerek kişiye ekonomik yönden katkıda bulunabilir.²⁰⁵

Bu alandaki en güçlü algoritmaların başında yine Google’ın, kullanıcıların erişebildiği bilgileri ve sonrasında sahip olacakları bilgileri etkileyen/yönlendiren ve Google arama motorunda kullanılan sıralama algoritması gelmektedir.²⁰⁶

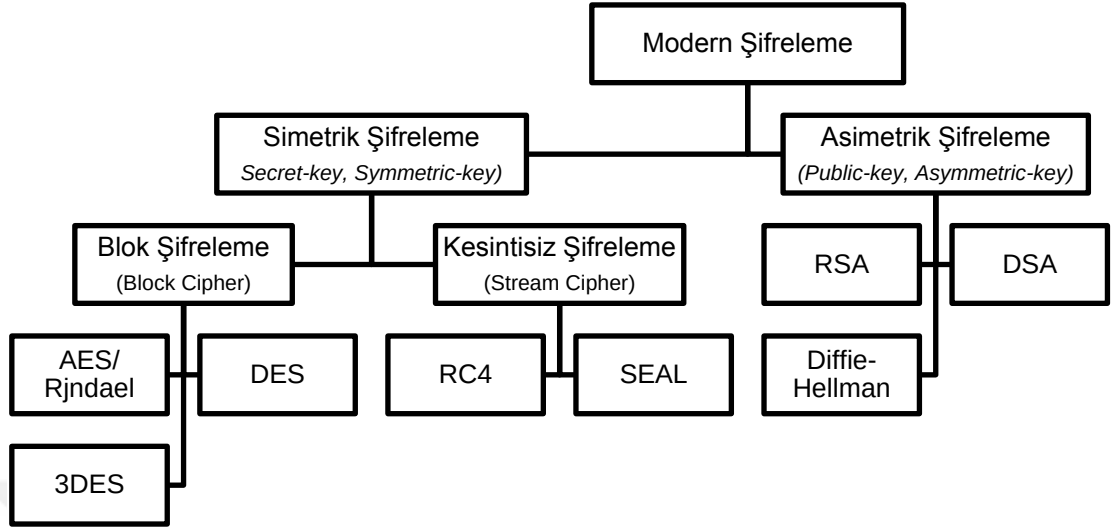
2.4.1.3. Şifreleme Algoritmaları

Şifreleme (*Encryption*), hassas bilgilerin güvenliğini garanti altına almanın temel yollarından biridir. Bilgi güvenliğinde kullanılan şifreleme algoritması, düz metin (şifreleme öncesi orijinal mesaj) üzerinde çeşitli şifreleme ve dönüşümler gerçekleştirir ve şifreli metne dönüştürür (şifreleme sonrası şifreli mesaj). Birçok şifreleme algoritmasına internet üzerinden kolaylıkla erişilebilir. Modern şifreleme algoritmaları temel olarak kullandıkları şifreleme yöntemine göre simetrik ve asimetrik şifreleme olarak iki gruba ayrılır. Simetrik şifreleme, *Symmetric-key* veya gizli şifreleme anlamına gelen *Secret-key* olarak da bilinir. Asimetrik şifreleme ise *Asymmetric-key* veya genel şifreleme anlamına gelen *Public-key* olarak da bilinir.²⁰⁷ Şekil 2.1’de algoritmalara da isimlerini veren, modern şifreleme yöntemlerine göre sınıflandırılmış şifreleme türleri gösterilmiştir.

²⁰⁵ Autorité de la Concurrence & Bundeskartellamt: “Algorithms and Competition”, November 2019, pp.6-7, Germany & France, (Çevrimiçi) <https://www.autoritedelaconcurrence.fr/sites/default/files/algorithms-and-competition-summary.pdf> 5 December 2019.

²⁰⁶ Caitlin Lustig, “Algorithmic Authority of the Bitcoin Blockchain”. Master’s Thesis, **University of California**, Irvine, 2018, p.12 (Çevrimiçi) <http://wtf.tw/ref/lustig.pdf> 6 December 2019.

²⁰⁷ Gurpreet Singh & Supriya Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, **International Journal of Computer Applications**, Vol.67, 2013, No.19, pp.33–38, p.33.



Şekil 2.1: Modern Şifreleme Algoritmaları²⁰⁸

Kişisel verilerin korunması bağlamında şifreleme algoritmaları; *pseudonymization* (takma adlandırma), yani bir veri kaydındaki kişisel olarak tanımlanabilir bilgi alanlarının bir veya daha fazla yapay tanımlayıcı veya takma ad ile değiştirilmesi ve verinin şifrelenerek korunması (*encryption*) açısından önemlidir.

2.4.2. Algoritmik Sistemlerin Kişisel Verilerin Korunması Bakımından Değerlendirilmesi

Bu bölümde; kara kutu ve opaklık, algoritmik önyargı, algoritmik ayrımcılık, algoritmik şeffaflık, algoritmik hesap verilebilirlik ve algoritmik denetim konuları, kişisel verilerin korunması bakımından değerlendirilecektir.

2.4.2.1. Kara Kutu ve Opaklık

İnsan bilmediği şeyden korkar. Buradaki korku insanı pasifleştirmektedir. Bilmesine rağmen yine korkmaya devam edebilir ancak bu sefer elinde, muhatap olduğu şey hakkında nasıl bir aksiyon almak istediğine karar verebilecek kadar yeterli veri bulunur.

²⁰⁸ Singh & Supriya, *Ibid.*, p.34.

Yapay zekâ sistemlerinin, insanlığın karşılaştığı ciddi sorunların çözümünden gündelik yaşamdaki tekrarlanan işlerin yapılmasına kadar birçok alanda daha yoğun olarak kullanılabilmesi için bu sistemlerin verileri nasıl topladığı, işlediği ve nasıl karar aldıklarını anlaşılabilmesi gerekmektedir. Bu sebeple algoritmik karar alma sistemlerinin kararları nasıl aldığının net bir şekilde açıklanamaması ilgili kişilere karşı şeffaf olunamamasının sebeplerindendir.²⁰⁹

Daha önce yapay zekânın türlerine ilişkin izahların yapıldığı Bölüm 1.3.2’de geçen özellikle büyük veri setlerine bağlı olarak eğitilen derin öğrenme teknikleri kullanılarak faaliyet gösteren otonom araçların veya web sitelerindeki ürün öneri sistemlerinin hangi gerekçeye dayalı olarak karar verdiğinin açıklanamaması sebebiyle çeşitli sorunlarla karşılaşmaktadır. Bunlardan birisi, gündelik ve basit işlerin yapılması sürecinden daha kompleks ve sofistike sorunların çözümüne geçişin yarattığı sancılardan olan kara kutu (Black Box) problemidir. Sadece kullanıcılar veya müşteriler açısından değil sistemi geliştiren veya tasarlayan kişiler tarafından da nasıl karar aldığı anlaşılamayan algoritmaların açıklanması da oldukça güç olmuştur.²¹⁰

YZ sistemlerin şeffaflığının ve hesap verilebilirliğinin önündeki diğer bir zorluk da opaklık sorunudur. Opaklığa ilişkin ilk olarak en etkili analizleri Paul Humphrey yapmıştır²¹¹. Carlos Zednik, opaklığı; sistemlerin içine bakılmasının güç olduğu bu sebeple de neden ve nasıl çalıştıklarının anlaşılmaması şeklinde ifade etmiştir²¹².

²⁰⁹ ICO, *Ibid.*, p.110.

²¹⁰ Davide Castelvecchi, “Can We Open the Black Box of AI?”, *Nature*, November 5, 2016. (Çevrimiçi) <https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731> 31 December 2019.

²¹¹ Humphrey sistemin opaklığını iki yönüyle açıklamıştır. İlki, bir sistemin kendisinin opak olmadığı, kullanıcıya bağlı olarak göreceli olduğunu ifade etmiştir. İkincisi, kullanıcının bilgisizliğinden kaynaklı opaklık durumunun oluştuğu belirtmiştir (Daha detaylı bilgi için bkz. Paul Humphrey, “The philosophical novelty of computer simulation methods”, *Synthese*, Vol.169, No.3, 2009, pp.615-626. (Çevrimiçi) https://pages.shanti.virginia.edu/Paul_Humphreys_Home_Page/files/2016/02/The-Philosophical-Novelty-of-Computer-Simulation-Methods.pdf 31 December 2019).

²¹² Carlos Zednik, “Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence”, March 3, 2019, (Çevrimiçi) arXiv preprint arXiv:1903.04361 31 December 2019.

Derek Doran ve diğerkleri, sistemin içindeki girdilerin çıktıya dönüşümünü haritalayan mekanizmaların kullanıcıya görünmez oluşu şeklinde tanımlamıştır²¹³.

Makinaların aldıkları kararın izah edilememesinin doğurduğu sorunlardan birisi de alınan kararın doğru bir karar olup olmadığının sağlarnasının yapılmasındaki güçlölüklerdir. Ayrıca algoritmik sistemlerdeki opaklık ilgili kişilerin kurum ve kuruluşlara karşı güvenlerinin azalmasına neden olacaktır ve dolayısıyla daha az etkileşime geçeceklerdir.²¹⁴

Algoritmaların opak olarak adlandırılması ve nasıl karar aldığına ilişkin insanlara tatmin edici seviyede açıklama yapılamamasının farkında olan sadece hakları ihlal edilen kişiler veya konuya ilgi duyan araştırmacılar değil, aynı zamanda yapay zekâ sistemlerini geliştirenler ve uygulamaya alanlardır. Ancak opaklığın azaltılması sonucunda isabetsiz ve yanlış kararların artması veya daha kompleks problemlerin çözülememesi gibi sorunlarla karşılaşılması sebebiyle atılacak adımlara ilişkin kararların atılması görünen daha girift bir haldedir.

Algoritmaların opak olmasının nedenlerini 3 başlık altında;

1. Şirket veya devlet sırlarının korunması gayesiyle kasten opak olunması,
2. Teknik anlamda çok az insanın programla dilleri ve makine öğrenimi sistemleri hakkında yeterli bilgiye sahip olması,
3. Makine öğrenimi algoritmaların tabiatından ve hedeflenen gayeyi gerçekleştirmesi için ulaşılması gereken komplekslik seviyesinden kaynaklanan opaklık, veya başka bir ifadeyle makine öğrenimi algoritmalarının Matematiksel yapıları ile insanlara özgü semantik yorumlamalar arasındaki uyumsuzlukların neden olduğu opaklık,

²¹³ Derek Doran, Sarah Schulz, Tarek R. Besold, "What does explainable AI really mean? A new conceptualization of perspectives", October 2, 2017. (Çevrimiçi) <https://arxiv.org/abs/1710.00794> 31 December 2019.

²¹⁴ ICO, *Ibid.*, p.28.

şeklinde inceleyen çalışmalar bulunmaktadır. Hangi tür opaklık formunun bulunduğu tespit edilmesi çözüm için kullanılacak olan aracın hukuki mi idari mi kodlamaya ilişkin mi yoksa teknik mi olacağını belirlemek adına önemlidir²¹⁵.

Algoritmik sistemlerin opaklığının sebepleri teknik (algoritmanın kendisinin kolayca açıklanamaması), ekonomik (şeffaflığı sağlamanın masraflı oluşu ve ticari sırlarının ifşa edilmesi riski) ve sosyal veya hukuk (sistemdeki girdinin açığa çıkarılmasının KVK ilişkin beklentileri ihlal edebileceği) kaynaklı olabileceği ifade edilmiştir.²¹⁶

Kişilerin yeniden suç işlemeye eğilimine ilişkin risk değerlendirmeleri ABD’de hüküm verilmesi öncesi süreçlerdeki soruşturma raporlarında sıkça yer almaktadır. Bu değerlendirmelerde kişinin geçmişine dikkate alınarak yeniden suç ihtimali incelenmektedir. Bu konudaki önemli davalardan birisi State vs Loomis davasıdır²¹⁷. Wisconsin Yüksek Mahkemesi yerel mahkemenin hüküm vermede kullandığı çalışma metodolojisinin mahkemeye veya sanığa açıklanmamasına rağmen algoritmik risk analizinin sanığın haklarını ihlal etmediğine karar verdi. Hüküm verilmesi öncesindeki soruşturma raporlarında COMPAS risk analizi de yer almaktaydı. COMPAS risk analizleri kişinin yeniden suç işleme eğilimini sorgu ve geçmişinden elde edilen bilgiler çerçevesinde yapılmaktadır²¹⁸. COMPAS’ın metodolojisi ticari sır olduğu için yeniden suç işlemeye ilişkin değerlendirme kriterleri sadece mahkemeye açıklanmıştır. Mahkeme de hüküm verirken COMPAS risk analizine atıf yaparak cezaya hükmetmiştir. Sanık, Loomis haklarının ihlal edildiği gerekçesiyle karara itiraz etmiştir. risk değerlendirmesinde cinsiyet gibi ayrımcılığa sebep olabilecek veri kategorilerinin kullanımına ilişkin başvurucunun taleplerini, şirket ticari sır savunmasına dayanarak sistemlerinin denetlenmesini ve gözden

²¹⁵ Jenna Burrell, “How the machine ‘thinks’: Understanding opacity in machine learning algorithms”, **Big Data&Society**, June 2016. (Çevrimiçi) <https://journals.sagepub.com/doi/full/10.1177/2053951715622512#articleCitationDownloadContainer> 31 December 2019.

²¹⁶ Association for Computing Machinery (ACM), “Statement on Algorithmic Transparency and Accountability”, **ACM U.S. Public Policy Council & ACM Europe Policy Committee**, May 25, 2017. (Çevrimiçi) https://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf 31 December 2019.

²¹⁷ State v Loomis, 2015AP157-CR (WI, 2016).

²¹⁸ Harvard Law Review, “State vs Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing.” **Harvard Law Review**, March 10, 2017. (Çevrimiçi) <https://harvardlawreview.org/2017/03/state-v-loomis/> 31 December 2019.

geçirilmesini engellemiştir²¹⁹. Bu açıdan ticari sırların saklanması ve korunması işletmeler ile şirketler açısından büyük önem taşımaktadır. Özellikle teknoloji şirketleri bakımından, kişisel verilerin işlenmesine ilişkin olarak algoritmalarının çalışma prensibi ve bir veriden nasıl yararlandıklarına ilişkin açıklamalar diğer paydaşlara karşı rekabet üstünlüğü yarattığı gerekçesi ile ticari sır olarak kabul edilebilecektir²²⁰.

Ancak Yüksek mahkeme ikna edici gerekçeler sunulmadığı sebebiyle sanığın cinsiyet temelli ayrımcılığa maruz kaldığı iddialarını reddetmiştir. Ayrıca COMPAS sistemi aleni ve sanık tarafından temin edilen verileri kullandığı için sanığın söz konusu rapordaki verileri inkâr ederek veya açıklayarak hükümde kullanılan verileri doğrulayabileceği edebileceği ifade edilmiştir. Sanık raporun kararda ana gerekçe olarak kullanılamayacağını iddia etmişse de COMPAS analizinin yeterli seviyede özenle değerlendirildiğini çünkü mahkemenin gerekli durumlarda analize katılmamak için takdir yetkisine ve yeterli bilgiye sahip olduğunu ortaya koymuştur. Yüksek mahkeme, risk analizini kullanan yargıçların hüküm de dikkate aldıkları hususları risk analizinden ayrı olarak açıklamasının gerekliliğini de vurgulamıştır. COMPAS gibi sistemler hakkında Yargıçların yetersiz bilgiye sahip oluşu ile analizi kullanmaya ilişkin iç ve dış baskılar mahkemelerin kararlarına karşı yeni bir tür şüphenin doğmasına sebep olacaktır. Ayrıca Loomis davasında kullanılan analiz sisteminin bağımsız kuruluşların denetlemesi sonucunda ulaşılmıştır ki siyahi olan faillerin beyaz faillere oranla daha yüksek risk puanı almaktadır²²¹. Bir başka daha büyük bir sorun ise yargıçların çoğunluğunun algoritmik risk değerlendirmelerinin nasıl çalıştığını anlamıyor oluşudur.

Şeffaflık ve hesap verilebilirlik sağlanamadığı için YZ sistemlerini geliştiren şirketlerin, sistemleri tasarlarken ve geliştirirken hangi özellikleri ön plana aldıkları,

²¹⁹ Bilgisayar programlarının fikri mülkiyet hukuku çerçevesinde korunmasına ilişkin detaylı bilgi için bkz. Mustafa Aksu, "Bilgisayar Programlarının Fikri Mülkiyet Hukukunda Korunması", **Beta Basım Yayım**, İstanbul, 2006, özellikle s.107 vd.

²²⁰ Gianclaudio Malgieri, "Trade Secrets v Personal Data: A possible solution for balancing rights", **International Data Privacy Law**, Vol.6, No.2, 2016, p.103.

²²¹ Sam Corbett-Davies, Emma Pierson, Avi Feller, Sharad Goel, "A Computer Program Used for Bail and Sentencing Decisions Was Labeled Biased Against Blacks. It's Actually Not That Clear", **Washington Post**, October 17, 2016. (Çevrimiçi) <https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas> 31 December 2019.

veri setlerini hangi kriterlere göre seçtikleri ve bu süreçte etik ve hukuki yönleri nasıl dikkat ettikleri bilinmemektedir²²².

AlgorithmWatch tarafından yapılan araştırmaya göre, Avrupadaki en az 10 polis teşkilatının yüz tanıma sistemini kullandığı, 5 tanesinin de yakın zamanda kullanmaya başlayacağı ortaya konulmuştur²²³. Belçika’da ve İspanya’da yerel polisin kişilerin yürüyüş şekillerinden veya kıyafetinden kişileri takip eden teknolojiyi kullandığı, aynı sistemin yüz tanımı da yapabildiği ancak resmi izinin henüz gelememesi sebebiyle beklemede olduğu belirtilmektedir. Yüz tanıma sistemlerinin hatalı doğrulama (*false positive*) yaptığı iddiasında bulunulması halinde sistemin, opaklığı sebebiyle denetlenebilmesi veya gözden geçirilmesi mümkün olmamakta, bu sebeple kötüye kullanıma izin verilmektedir. Çok yakın bir zaman sonra kolluk kuvvetlerin kullandığı yüz tanıma sistemlerinin mağdur ettiği kişi sayısında artış olacağını öngörmek hiç de zor değildir²²⁴.

Opaklığın önündeki engellerin kaldırılabilmesi ve çözülebilmesi için çeşitli adımlar atılmalıdır. Kamu kurumları, şirketlerin toplumsal ve etik değerleri dikkate alarak ve hukuki ilke ve düzenlemelere uyumlu olarak otomatik karar alma sistemleri geliştirmeleri yönünde baskı kurabilmek için pazardaki satın alma güçleri başta olmak üzere pazarlık masasında ellerinin güçlü olduğu kısımları tespit etmeli ve buna göre stratejiler geliştirmelidir.²²⁵

2.4.2.2. Algoritmik Önyargı

Makine öğrenimi yöntemleri ve veriden kaynaklı problemler istenilmeyen sonuçlara neden olabilmektedir. Algoritmaların neden olduğu istenilmeyen

²²² Elizabeth E. Joh, “The undue influence of surveillance technology companies on policing”, **NYU Law Review**, Vol.92, 2017, p.101.

²²³ Nicolas Kayser-Bril, “At least 10 police forces use face recognition in the EU”, **AlgorithmWatch reveals**, December 11, 2019. (Çevrimiçi) <https://algorithmwatch.org/en/story/face-recognition-police-europe/> 31 December 2019.

²²⁴ Clare Garvie, “Garbage In, Garbage Out. Face Recognition on Flawed Data”, **GeorgeTown Law Center on Privacy&Technology**, May 16, 2019, (çevrimiçi) <https://www.flawedfacedata.com> 31 December 2019.

²²⁵ Hugo van Haastert, “Government as a Platform: Public Values in the Age of Big Data”, **Oxford Internet Institute**, 2016. (Çevrimiçi) <http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/Government%2520as%2520a%2520Platform%2520-%2520Big%2520data%2520paper.pdf> 31 December 2019.

sonuçların sebeplerinden birisi de Önyargılı veri (biased data) setleridir²²⁶. Önyargı; ten rengi, ırk, cinsiyet veya din vb. dış etkenlere dayanarak birine karşı haksız peşin hükümde veya ayrımcılıkta bulunmaktır²²⁷. Çalışmamızda önyargı ifadesiyle ile istenilmeyen (unintended) sonuçlara neden olan veya zarar verme potansiyeli bulunan veri setleri kastedilecektir. Tarihsel açıdan olduğu gibi hatalı hesaplamalardan kaynaklanan önyargılarda istenilmeyen sonuçların sebeplerinden birisi olmaktadır²²⁸.

Algoritmik karar alma sistemlerinin haksız veya ayrımcı kararlar almasına neden olan önyargı içeren eğitim verileri (biased training data) tarihsel olarak yaşanan insan hakları ihlallerinin çözümünde veya daha da artmasında önemli bir eşik olacaktır. Eğer eğitim verisi önyargı veya tarihsel ayrımcılıkları içeriyorsa, algoritmik karar alma sistemi bu değerlendirme biçimini miras alacak ve gelecekte karar alırken kullanacaktır. Google'ın haberlerdeki makaleleri kullanarak eğittiği sistemi gündelik hayatta sıkça karşılaşılan cinsiyete dayalı genelleşici bir tutum sergilemektedir. Sistem kendisine sunulan hemşire, resepsiyonist, kütüphaneci, kuaför, stilist, temizlikçi, iç tasarımcı gibi meslek gruplarını kadınlara ilişkin, felsefeci, gemi kaptanı, mimar, finans uzmanı, savaşçı, büyücü, patron gibi kategorileri de erkeklere ilişkin meslekler veya eğilimler olarak görmektedir²²⁹.

Adil ve ayrımcılıkta bulunmayan makine öğrenimi sistemleri tasarlayabilmenin yollarından birisi olarak, kullanılan veri setlerindeki ırk veya cinsiyet gibi kolonların hariç tutulması düşünülmektedir. Ancak bu hariç tutulan veri kategorilerinin diğer değişkenlerle olan ilişkileri sonucunda üretilen ayrı veri kategorilerinin veri havuzuna dahil edilmesi sebebiyle, kalan değişkenleri değerlendirip çıkarılan değişkenin tahmin edilmesi mümkün olmaktadır ve istenilmeyen ayrımcılıktan kaçınılamamaktadır. Facebook'un hedefli reklam

²²⁶ Harini Suresh, John V. Guttag, "A Framework for Understanding Unintended Consequences of Machine Learning", arXiv preprint, January 28, 2019. (Çevrimiçi) <https://arxiv.org/abs/1901.10002> 31 December 2019.

²²⁷ Morris, **Ibid.**

²²⁸ Suresh / Guttag, **Ibid.**

²²⁹ Tolga Bolukbasi, Kai-Wei Chang, James Zou, Venkatesh Saligrama, Adam Kalai, "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings", **Advances in Neural Information Processing Systems**, July 21, 2016. (Çevrimiçi) <https://arxiv.org/abs/1607.06520> 31 December 2019.

hizmetinde ırk bilgisinin sorulmasının yasaklanmasına rağmen kişilerin davranışlarından etnik aidiyetinin tespit edildiğine ilişkin çalışmalar görülmektedir.²³⁰

Cinsiyet, ırk veya dini inanç gibi hassas veri türlerinin veri setinden çıkarılmasının da farklı bir soruna yol açtığını araştırmalarda görmekteyiz. Örnek (sample) veri setinde belirli bir grubun yeterince temsil edilememesi²³¹ ve algoritmanın riski azaltma amacına bağlı olarak karar vermeye tasarlandığı durumlarda ulaşılması hedeflenen amacın gerçekleşmesiyle ilgisi bulunmayan ırk gibi hassas veri kategorilerinin çıkarılması ‘belirsizlik önyargısı’na (uncertainty bias) sebep olmaktadır²³².

Makine öğreniminin kullanıldığı tek alan sınıflandırma algoritmaları olmasa da çalışmamızda odaklanılan konular açısından araştırmacıların en çok ele aldığı alanların başında gelmektedir. Bunun sebebi, tarihsel anlamda bozuk, sapkın ve mantıklı bir şekilde izah edilemeyecek ırksal sınıflandırmalardır. Algoritmaların daha objektif bir şekilde sınıflandırma yapacağına (ayrıca geçmişteki eksiklikleri ve sınıflandırmalardaki haksızlıkları gidereceği) ilişkin iddia, sistemi tasarlayan kişilerin düşünme biçimlerinin doğrudan veya dolaylı yoldan algoritmik sistemi şekillendireceğinden dolayı sağlam delillerle ispat edilmeye muhtaç görünmektedir²³³.

Açık pozisyonların reklamının yapılmasından, pozisyonlara adayın istihdam edilmesine kadar insanların hayatlarında önemli bir yeri olan profesyonel kariyerlerine ilişkin süreçlerde de otomatik karar alma mekanizmalarının kullanımında artış görülmektedir. Görevini layıkıyla yapabilmesi için adayın kabiliyetlerini, ilgi alanlarını ve potansiyelini algoritmik sistemlerin isabetli bir şekilde

²³⁰ Julia Angwin, Terry Parris Jr., “Facebook Lets Advertisers Exclude Users by Race”, **PROPUBLICA**, October 28, 2016. (Çevrimiçi) <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race> 31 December 2019; Julia Angwin, Ariana Tobin, Madeleine Varner, “Facebook (Still) Letting Housing Advertisers Exclude Users by Race”, **PROPUBLICA**, November 21, 2017. (Çevrimiçi) <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin> 31 December 2019.

²³¹ Yi Li, Nuno Vasconcelos, “REPAIR: Removing Representation Bias by Dataset Resampling”, Conference paper, **IEEE Conference on Computer Vision and Pattern Recognition**, April 16, 2019. (Çevrimiçi) <https://arxiv.org/pdf/1904.07911.pdf> 31 December 2019.

²³² Bryce Goodman, Seth Flaxman, “European Union regulation on algorithmic decision-making and a “right to explanation”, **AI Magazine**, Vol. 38, No.3, 2017, pp.50-57.

²³³ Burrell, **Ibid**.

değerlendirebilmesi gerekmektedir. LinkedIn’de iş ilanlarının içeriğinin unvan adlarıyla ilişkisini ve bunun da cinsiyetle olan bağlantısını inceleyen bir çalışmada, cerrah olarak unvanını işaretleyen kadınların oranının yüzde 14,6 olduğunu tespit eden araştırmacıların algoritmik sistemin tekrar cerrahları tahmin etmesini istediğinde bu oran kadınlarda yüzde 11,6’ya düşmüştür.²³⁴

Çevrimiçi reklam alanında da kullanılan YZ sistemlerinin önyargılı veri setleriyle çalışması halinde ilgili kişilerin verilerinin beklemedikleri ve bilgileri dahilinde olmayan şekilde işlenmesi gerçekleşecektir. Bir adım ötesinde rahatsız edici ve dijital ayrımcılığa uğradığı olaylarla karşılaşmaktadır. Dijital ortamda her bireye belirli şartlar gözetilerek farklı reklamlar gösterilmesi, bu kişilerin ırklarına bağlı olarak maruz kalacağı ayrımcılığı daha da artıracak şekilde profillendiğini göstermektedir²³⁵. Diğer bir araştırmada da ABD’de; internet aramalarında siyah ten renkli kişilerin daha yaygın kullandığı isimlerin yazılması halinde, beyaz ten renkli kişilerin yaygın olarak kullandığı isimlerle yapılan aramalara nazaran çok daha fazla tutuklama kayıtlarıyla ilişkili olabilecek reklamların gösterildiği de tespit edilmiştir²³⁶.

Eğer yaşadığımız dünyada, tarihimizde, insanlarda önyargı var ise neden Algoritmik önyargı önemli sorusu akla geliyor. Otomatik karar alma mekanizmaları verileri tüketen pasif bir oyuncu olmanın ötesinde, bugün yaptıkları tahminler ile geleceğimizi şekillendiriyor. Hangi haberi okuyacağımızdan ve hangi ürünleri satın alacağımızdan hangi iş ilanlarını göreceğimize kadar yaşamı nasıl tecrübe edeceğimizi belirliyor. Toplumumuzdaki mevcut önyargıyı koruyan hatta daha da fazla artıran analizler ve tahminler yaptığı da birçok çalışma tarafından ortaya

²³⁴ Maria De-Arteaga, Alexey Romanov, Hanna Wallach, Jennifer Chayes, Christian Borgs, Alexandra Chouldechova, Sahin Geyik, Krishnaram Kenthapadi, Adam Tauman Kalai, "Bias in bios: A case study of semantic representation bias in a high-stakes setting." Conference paper. **The Conference on Fairness, Accountability, and Transparency (ACM)**, January 27, 2019. (Çevrimiçi) <https://arxiv.org/abs/1901.09451> 31 December 2019.

²³⁵ Cecilia Esther Rabess, "Can big data be racist?", **The Bold Italic**, March 31, 2014, (Çevrimiçi) <http://www.thebolditalic.com/articles/4502-can-big-data-be-racist> 31 December 2019

²³⁶ Latanya Sweeney, "Discrimination in Online Ad Delivery", arXiv preprint, 2013, (Çevrimiçi) <https://arxiv.org/abs/1301.6822> 31 December 2019

konulduğu için alt kategorileri, neden olduğu zararların, nasıl azaltılabileceğine ilişkin çözümlerin dikkatle üzerinde durulması gerekmektedir.²³⁷

YZ sistemlerinin %100'e yakın isabetli olduğunu düşünen, bu teknolojilerin nasıl çalıştığını yeteri kadar bilmeyen toplumun her kesiminde insan bulunmaktadır. Büyük bir kesim algoritmik sistemlerin objektif ve hata yapmayan mekanizmalar olduğunu düşünmektedir.²³⁸ Bu sebeple aldıkları kararlara karşı itiraz edilmesi ihtiyacının olabileceğine ihtimal vermemektedirler. Algoritmik sistemlerin, insan kaynağıyla yapmaya nazaran daha ucuz oluşu da daha önce saydığımız sorunların göz ardı edilmesine destek olacaktır. YZ teknolojilerinin bir bıçak gibi olduğu iyi yönde de kötü yönde de kullanılabileceğine ilişkin savunmalar yapılarak çeşitli uygulamalardaki ayrımcılığın sebebinin makinelerden kaynaklanmadığı buna insanların sebep olduğu savunması yapılmaktadır. Ancak bunun gibi savunmalar da algoritmik sistemlerin neden olduğu hatta artırdığı²³⁹ ayrımcılıkların çözümüne engel olmaktadır.

Her veri setinde farklı bir standarda veya norma dayalı olarak bir önyargı bulunmaktadır. Araştırmacılar tarafından ele alınması gereken sorulardan bazıları şöyle sıralanabilir²⁴⁰:

1. Planlanan projenin yapılmasına gerçekten ihtiyaç duyuluyor mu?
2. Eğitim verisinin adil olduğunu ve her kesimi temsil ettiğini test ettik mi?
3. Verideki önyargının kaynağı hakkında çalışıldı ve anlaşıldı mı?
4. Veri veya kod denetlenebilmekte midir?
5. Farklı gruplar için sistemin adil kararlar vermesi ve hatalarına ilişkin oranı nedir?

²³⁷ Ziad Obermeyer, Brian Powers, Christine Vogeli, Sendhil Mullainathan, "Dissecting racial bias in an algorithm used to manage the health of populations", **Science**, Vol.366, October 25, 2019, pp.447-453. (Çevrimiçi) <https://science.sciencemag.org/content/366/6464/447> 31 December 2019.

²³⁸ Solon Barocas, Andrew D. Selbst, "Big data's disparate impact", **California Law Review**, Rev., Vol.104, 2016, pp.671-732.

²³⁹ Detaylı bilgi için bkz. David Casacuberta, "Bias in a Feedback loop: Fuelling Algorithmic Justice", **Cultural Research and Innovation Lab**, May 9, 2018. (Çevrimiçi) <http://lab.cccb.org/en/bias-in-a-feedback-loop-fuelling-algorithmic-injustice/> 31 December 2019.

²⁴⁰ Rachel Thomas, "16 Things You can Do to Make Tech More Ethical, part 1", April 22, 2019. (Çevrimiçi) <https://www.fast.ai/2019/04/22/ethics-action-1/#risks-sweep> 31 December 2019.

6. Hatalı sonuçlara veya itirazlara karşı hangi süreçler öngörülmektedir?
7. Projeyi yapan grup ne kadar farklı kimlikten veya görüşten olan kişilerden oluşmaktadır?

2.4.2.3. Algoritmik Ayrımcılık

AİHS'nin 14. maddesinde Ayrımcılık Hakkı; *“Bu Sözleşme’de tanınan hak ve özgürlüklerden yararlanma, cinsiyet, ırk, renk, dil, din, siyasal veya diğer kanaatler, ulusal veya toplumsal köken, ulusal bir azınlığa aidiyet, servet, doğum başta olmak üzere herhangi başka bir duruma dayalı hiçbir ayrımcılık gözetilmeksizin sağlanmalıdır.”* şeklinde tanımlanmıştır. Ancak ayrımcılığın ne olduğunu net bir şekilde ifade etmemektedir. Bir kişinin belirli bir gruba dahil olması sebebiyle adil olmayan muameleye tabi tutulması ayrımcılık olarak tanımlanmaktadır²⁴¹. İncelemede bulunduğunuz bir gruba veya kimliğe ilişkin davranışı diğer hangi grupla karşılaştırdığınıza bağlı olarak da ayrımcılık olup olmadığı değişecektir. Bu sebeple göreceli bir kavram olduğu söylenebilir.

Ayrımcılık arzu edilmeyen ve toplumdan temizlenmesi gereken bir şeydir. Bir zamanlar yaygın olarak makinaların tarafsız karar vericiler olacağı ve insanların sahip olduğu önyargıları sergilemeyeceği düşünülmekteydi.²⁴² Ancak ilerleyen süreçte birçok algorithmada insan önyargılarının bir sonucu olarak önyargılı yaklaşımların varlığı tespit edilmiş, dolayısıyla algoritmaların insanların önyargılı düşünce ve yaklaşımlarından yeterince arındırılmadığı görülmüştür.

95/46/EC sayılı Yönerge’nin hazırlandığı dönemde Avrupa Komisyonu 1992 yılında makinelerin “daha kompleks ve gelişmiş yazılımlarla çalışan sistemler tarafından üretilen sonuçlara insan karar vericilerin çok fazla önem vermesinin ve kendi sorumluluklarını artık yerine getirmemeye başlamasının arkasında yatan

²⁴¹ Andrew Altman, “Discrimination”, **The Stanford Encyclopedia of Philosophy**, **Stanford University**, August 30, 2015. (Çevrimiçi) <https://plato.stanford.edu/entries/discrimination/> 31 December 2019

²⁴² Christian Sandvig, “Seeing the Sort: The Aesthetic and Industrial Defence of “the Algorithm”, **Journal of the New Media Caucus**, 2015. (Çevrimiçi) <http://median.newmediacaucus.org/art-infrastructures-information/seeing-the-sort-the-aesthetic-and-industrial-defense-of-the-algorithm/> 31 December 2019.

sebebi bu sistemlerin inkâr edilemez kabiliyetleri”²⁴³ olduğunu belirterek yaklaşan tehlikeyi açık bir şekilde tanımlamıştır.

Kaynakların verimli kullanımı amacıyla yapılan Algoritmik profillemeye, belirli kriterlere dayalı olarak kategorilere ayrılmış kişiler hakkında daha önceden çerçevesi çizilmiş gruplardan hangisinde olduğuna bağlı olarak karar alınması sonucunda ayrımcılık ile karşılaşılabilir. Özellikle ABD’deki ırksal ayrımcılığa ilişkin kayda geçen olaylara bakıldığında otomatik karar alma sistemlerinin aldığı kararların sorgulanması başta olmak üzere sistemin tasarımının en baştan gözden geçirilmesi gerektiği konunun uzmanları ifade etmeye başlamıştı²⁴⁴. Gün geçtikçe karşılaşılan olaylar bu iddiaları doğrular niteliktedir. ABD sağlık sisteminde kullanılan ticari algoritmalarda ırksal önyargıya ilişkin bulgular tespit edilmiştir. Yapılan araştırmalarda beyaz hastalar ile hastalığı daha ileri seviyede olan siyahi hastaların aynı risk seviyesinde olduğuna sistemin karar verdiği görülmüştür. Bu sebeple de siyahi hastaların alacağı yardımların hak edilen ve ihtiyaç duyulandan daha az olmasına neden olduğu belirtilmiştir. Aynı seviyede hastalık derecesine sahip olan siyahi hastaların, beyaz hastalardan daha sağlıklı olduğuna algoritmanın kanaat getirdiği ifade edilmektedir²⁴⁵.

Yapay zekâ sistemleri tarafından Büyük Verinin işlenip anlamlandırılmasıyla açığa çıkacak olan büyük resmin mevcut toplumun yansıması olacağına ilişkin tespitler de bulunmaktadır²⁴⁶. Ancak geçmişten günümüze değin devletlerin, kurumların, kuruluşların veya ayrımcılıkta bulunabilecek herhangi bir öznenin elinde imkanlar sınırlıydı. Artık günümüzde kurum veya kuruluşların kişiler hakkında tahminin ötesinde anlık yaptıkları hakkında bilgi sahibi olmaları sebebiyle kişileri isabetli bir şekilde sınıflandırmaları ve hayatlarına dokunmaları mümkündür. Bu sebeple geçmişten gelen önyargıların, ayrımcılıkların ve toplumda var olan her tür hoşla gitmeyen etik, ahlaki ve hukuki olmayan pratiklerin dijital ortama yansımalarının üzerinde dikkatle durulmalıdır.

²⁴³ EU Commission, “Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM (92) 422 final”, October 18, 1992, (Online) <http://aei.pitt.edu/10375/1/10375.pdf> 31 December 2019.

²⁴⁴ Mittelstadt / Allo / Taddeo / Wachter / Floridi, **Ibid.**

²⁴⁵ Obermeyer / Powers / Vogeli / Mullainathan, **Ibid.**

²⁴⁶ Viktor Mayer-Schönberger, Kenneth Cukier, “Big Data: A Revolution That Will Transform How We Live, Work, And Think”, **Houghton Mifflin Harcourt**, 2013.

Yirmibirinci Yüzyıl'da Devlet veya şirketlerden ziyade algoritmik karar sistemleri ayrımcılığa neden olmaktadır. Algoritmik sistemlerin geçmişteki önyargıları içeren veri setleri ile eğitilmesi, geçmişte yaşanan istenilmeyen olayların yeniden yaşanmasına hatta ayrımcılığı daha fazla artırması riskini barındırmaktadır. Başka bir görüşe göre de algoritmik sistemlerin, her insanda olacağı gibi sistemi geliştirenlerde de bulunacak olan önyargıları içereceği ve dolaylı olarak, gayri ihtiyari ve farkında olunmayarak ayrımcılığa sebep olacağı ifade edilmektedir.²⁴⁷

Algoritmik önyargı makine öğrenimi ile doğal dil işleme teknikleriyle metinlerin analiz edilmesi sonucunda da gözlemlenebilir. Yazı ve ses oluşturulması, makine çevirisi, duygu analizi, cümle tamamlama, sayfaların sıralanması ve filtre baloncuklarıyla internet kullanıcılarına bilginin sunulması gibi uygulamalarda ayrımcılığa sebep olan birçok örnek ile karşılaşılabilir. Baba ile doktorun eşleştirildiği bir önermenin anne nedir sorusuna hemşire olarak yanıt vermesi, erkek kariyer odaklıdır önermesine karşı anne aile odaklıdır cevabı vermesi cinsiyet ayrımcılığına ilişkin durumlardır.²⁴⁸

Algoritmik karar alma sistemlerinin sadece temel hak ve hürriyetlere tehdit oluşturmakla kalmadığı daha da ötesinde uzun dönemde sosyal farklılıklar ürettiği ve bu yöndeki gidişatı güçlendirdiği ifade edilmektedir. Risk seviyelerini tanımlayıp hangi değerde olduğuna karar verdiği kişiler ve topluluklar hakkında kararlar alıp onları yönetmektedir. Sınıflandırmaların ve belirli kategorilerin üretilmesinin uzun vadede etkileri sosyal bir şekillendirme olarak görülebilir.²⁴⁹

YZ sistemlerin toplumu kontrol altında tutmak, şekillendirmek, muhalif görüşte bulunanları sindirmek gibi amaçlarla kullanılması sonucunda kişilerin hem özel hayatlarının gizliliği hakkı ihlal edilip kişisel verileri temel insan haklarına aykırı

²⁴⁷ Toon Calders, Indrė Žliobaitė, "Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures", *Discrimination and privacy in the information society*. Springer, 2013, pp.43-57.

²⁴⁸ Aylin Caliskan-Islam, Joanna J. Bryson, A.R. Vijaya Narayanan, "A Story of Discrimination and Unfairness Implicit Bias Embedded in Language Models", 2016. (Çevrimiçi) <https://www.semanticscholar.org/paper/A-Story-of-Discrimination-and-Unfairness-Implicit-Caliskan-Islam-Bryson/6a0850123cefa90dbff00d2e0903bf99a9ec1c49> 31 December 2019.

²⁴⁹ David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies", In D. Lyon (Ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, pp.13–30, Routledge, New York, 2003.

bir şekilde işlenmektedir. Daha önce de bahsettiğimiz gibi kişilerin ifade özgürlüğü, haber alma özgürlüğü, toplantı ve gösteri yürüyüşü hakkı gibi sağlıklı bir demokrasinin temellerini oluşturan haklarının da ihlal edilmesine kullanılamaz hale gelmesine neden olmaktadır.

George Orwell'in 1984 isimli romanında; iyi bir vatandaş ol ve ödüllendiril şeklinde ifade edilen distopik olarak tanımlanabilecek bir gelecek projeksiyonunun hiç o kadar da uzak olmadığını Çin'deki pratiklerden görebilmekteyiz²⁵⁰. Vatandaşların hukuki kurallara, ahlaki normlara, profesyonel ve etik standartlara uyumlu yaşamalarına bağlı olarak güvenilirliklerini ölçmeyi hedefleyen Çinin sosyal kredi sistemi 2014 yılında ulusal çapta kullanıma alınmıştır. Devlet ve özel sektörün beraber çalışması sonucunda hayata geçirilen projede bireyler hangi unsurların sosyal kredi skoruna katkı sağladığını, nasıl birleştirildiklerini, nasıl yorumlanıp kullanıldığını bilememektedir. Kişisel verilerin korunması hakkına yapılan ölçsüz müdahalenin ötesinde kişilerin kişisel verilere erişim dolayısıyla yaşam hakkı, düşünce ve fikir hürriyeti, din ve vicdan hürriyeti gibi temel haklarının ciddi tehdit altında bulunmasına neden olunmaktadır²⁵¹. Bilimsel araştırma amaçlı bulunan yöntemler kötü niyetli kurumların elinde ayrımcılık ve haksızlık sağlamaya neden olan bir araç haline de gelebilir. Sınır kontrolleri, gümrükteki geçişler, kamu güvenliği gibi hedeflerle geliştirilen uygulamaların kişisel verilerin korunması hakkına uyumlu olabilmesi için belki de en baştan üretilmeye izin verilmemesi de düşünülmelidir²⁵².

Klasik anlamda ayrımcılık şeklinde değerlendirilmese de algoritmik karar alma sistemlerinin karar alırken kullandıkları kriterlerinde haksızlığa sebep olup olmadığının incelenmesi de oldukça önemlidir. Örneğin bir çalışan adayının

²⁵⁰ Rachel Botsman, "Big data meets Big Brother as China moves to rate its citizens", **Wired UK**, October 21, 2017. (Online) <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion> 31 December 2019.

²⁵¹ Yongxi Chen, Anne S.Y. Cheung, "The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System", **The Journal of Comparative Law**, Vol.12, No.2, June 26, 2017, pp.356-378. (Çevrimiçi) <https://ssrn.com/abstract=2992537> 31 December 2019.

²⁵² Uygur, Tibetli, Koreli gibi Çin ile ilişkili ırklardaki kişilerin yüz tanıma sistemleriyle ırklarının tespit edilmesine ilişkin çalışmanın detaylı bilgisi için bkz. Cunrui Wang, Qingling Zhang, Wanquan Liu, Yu Liu, Lixin Miao, "Facial feature discovery for ethnicity recognition", **Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery**, Vol.9, No.1, 2019. (Çevrimiçi) <https://onlinelibrary.wiley.com/doi/full/10.1002/widm.1278> 31 December 2019.

başvurusu değerlendirilirken, yardımcı olduğu ispat edilse dahi kişinin web tarayıcısının da dikkate alınması adil bir hüküm vermeyi sağlayacak mıdır?²⁵³

YZ sistemlerinin kararlarının haksızlığa sebep olmasını iki yönüyle inceleyebiliriz; ilki kararın alınmasında kullanılan kişisel verilerin amaç ile bağlantısı, ölçülü olması ve kişinin bunu bekleyecek durumda ve pozisyonda bulunmasıdır. İkincisi alınan kararın nasıl alındığının açıklanmasıdır. Çünkü Algoritmik sistemler aracılığıyla alınan kararla etkilenen kişiler açısından düşünülürse kararın açıklanmaması da bir haksızlık olarak değerlendirilebilir.

Otomatik karar alma mekanizmalarında kullanılan profillemeye algoritmalarının kasıtlı olmadan marjinalleşmiş popülasyonlara karşı ayrımcılık yaptığı gibi²⁵⁴, Google'ın çevrimiçi reklam sisteminde de (*online advertisements*) kişilerin isimlerinden hangi etnik kökene ait olduğunu tahmin ederken çeşitli haksızlıklara sebep olmaktadır²⁵⁵.

Yukarıda ve önceki bölümlerde örnekleriyle değinilmiştir ki yargı, kolluk kuvvetleri, sağlık veya eğitim gibi hassas alanlarda insan karar alıcıların yerini alan veya destekleyen algoritmik karar alma sistemlerinin, ayrımcılıkla, haksızlıkla veya kişisel verilerin ihlal edilmesiyle sonuçlanacak kararlar almasının önüne geçmek için gerekli tedbirler alınmalıdır²⁵⁶.

Daha önce Bölüm 2.1.1'de Hukuka ve Dürüstlük Kuralına uygun İşlenmesi ilkesinin açıklandığı bölümde değinildiği üzere KVKK'da ve GDPR'de adillik ilkesine (fairness) uyumluluk kişisel verilerin toplanması ve işlenmesinin temelinde gözetilmesi gereken bir yükümlülük olarak belirlenmiştir.

²⁵³ E.H., "How might your choice of browser affect your job prospects?", **The Economist**, April 11, 2013. (Çevrimiçi) <https://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-browser-affects-job-prospects> 31 December 2019.

²⁵⁴ Solon Barocas, "Data mining and the discourse on discrimination", **Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining**, 2014. (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899 31 December 2019

²⁵⁵ Sweeney, **Ibid.**

²⁵⁶ European Parliamentary Research Service (EPRS), "Understanding Algorithmic Decision-Making: Opportunities and Challenges", **Scientific Foresight Unit (STOA)**, PE 624.261, March 2019, (Çevrimiçi) [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/1/EPRS_STU\(2019\)624261_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/1/EPRS_STU(2019)624261_EN.pdf) 31 December 2019

Ayrımcılığın önlenmesine ilişkin GDPR’de doğrudan bir düzenleme (par.71)²⁵⁷ de bulunmaktadır. Irk, etnik köken, siyasi görüş, dini inanç, felsefi görüş, sendika üyeliği, genetik veya sağlık durumu, cinsel yönelim gibi hassas nitelikteki kişisel verilerin kullanımıyla elde edilen profillemeye dayalı veri işleme faaliyetlerinin neden olduğu ayrımcılığı önleyici tedbirler alınması gerektiği ifade edilmektedir.

Kişisel verilerin adil bir şekilde işlenmesinin sağlanabilmesi için algoritmik karar alma sistemlerinin kişilere etkilerinin ve kişilerin bu sistemler aracılığıyla kişisel verilerinin nasıl işleneceğine ilişkin beklentilerinin titizlikle ele alınması gerekmektedir.²⁵⁸

ICO’nun Yapay zekâ ve makine öğrenimi kullanan mekanizmaları KVK açısından incelediği raporda; haksızlığa neden olan sonuçların gerekçelerinden birisinin, verilerin işleme amacı ile toplanma amacı arasındaki uyumsuzluklardan kaynaklandığını ifade etmektedir²⁵⁹. Tam da bu ve benzeri sorunların çözülüp kişisel verilerin korunmasının sağlanabilmesi için “kişinin beklentisi” (reasonable expectations) konseptinin ve şeffaflık (transparency) ilkesinin üzerinde dikkatle durulmalıdır. Çünkü kişisel verilerin işleneceği tüm amaçlara dair ilgili kişilerin bilgilendirilmesi gerekmektedir ve bunun sağlanabilmesi yukarıda sayılan kavramlarla yakından ilişkilidir. İleride Algoritmik şeffaflığın tartışıldığı Bölüm 2.4.2.4’te daha detaylı irdelenecektir.

Makine öğrenimi ve büyük verinin temel amacının eldeki mevcut verinin tekrar başka bir amaçla işlemek olması esas itibarıyla KVK’daki önceden belirlenmiş, spesifik ve sınırlı bir amaçla işleme ilkesiyle çelişmektedir. Ayrı bir ifadeyle; Bölüm 2.1.3’te değerlendirilen Belirli, Açık ve Meşru Amaçlar için İşlenme İlkesi kapsamında da bir ihlal gerçekleşmiş olacaktır. Söz konusu sistemlerde verilerin sınırsız sürelerle saklanması, her türlü veriyi toplamaya yönelik eğilimler ve hizmetin sunulması için gerekmeyen verilerin toplanması da veri minimizasyonu ilkesine ve sınırlı tutulma ilkesine aykırılık oluşturacaktır. Kişisel verilerin korunması

²⁵⁷ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, par.71.**

²⁵⁸ ICO, **Ibid.**, p.22.

²⁵⁹ ICO, **Ibid.**, p.23.

hukuku açısından algoritmik karar alma sistemlerinin neden olduğu sorunlardan bazıları yukarıda sayılmaya çalışılmıştır²⁶⁰.

Algoritmik karar alma sistemleri çoğunlukla elde bulunan veri setleri ile eğitilmiş makine öğrenimi algoritmaları üzerinde tasarlanmaktadır. Bu aşamada haksızlığın veya ayrımcılığın kaynağının tek bir sebebi bulunmamaktadır²⁶¹.

Yeterli şekilde açıklanamayan ve tahmin edilemeyen öğrenen algoritmalar tarafından alınan problemleri bir kararın bir “bug” nedeniyle mi sistematik bir hata nedeniyle mi yoksa önyargı (bias) sebebiyle mi olduğunu tespit etmenin çok zor olduğu ifade edilmektedir²⁶².

Algoritmik karar alma sistemlerinin haksız (unfair) veya ayrımcı (discriminatory) kararlar almasının sebepleri arasında Önyargı içeren eğitim verileri (biased training data) ve hatalı eşleştirmeler (Accuracy Disparity) sayılmaktadır. Ancak önyargılı eğitim verilerinin yerine nötr eğitim verilerinin kullanılmasıyla agnostik makine öğrenimi algoritmalarının kullanılmasının problemi tam anlamıyla çözmeyeceği düşünülmektedir²⁶³.

Ayrımcılığın nedenlerinden birisi de daha önceden toplumda bulunmayan ancak gelişmiş veri işleme ve anlamlandırma teknikleriyle üretilen yeni gruplardır. Geçmişteki veri işleme yöntemleri elindeki değişkenleri kullanan şimdikiye göre daha basit yöntemlerdi. Ancak veri madenciliği sadece değişkenleri kullanmakla kalmaz aynı zamanda yeni değişkenler de üretir. Veri setinden modelleri bularak

²⁶⁰ Avrupa Komisyonu (EC - European Commission), “Article 29 Working Party, Opinion 03/2013 On Purpose Limitation”, April 2, 2013, p.45 vd. (Online) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf 31 December 2019

²⁶¹ Barocas / Selbst, **Ibid.**

²⁶² Andrew Tutt, “An FDA for Algorithms”, **69 Administrative Law Review**, Vol.83, 2017. (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994 31 December 2019.

²⁶³ Mireille Hildebrandt, “Privacy as Protection of the Imcomputable Self: From Agnostic to Agnostic Machine Learning”, **Theoretical Inquiries in Law**, Vol.20, No.1, 2019, p.101.

yeni profiller üretir. Üretilen yeni profillerde yeni bireylerle ilişkilendirilir ve daha önce yapılmayan ayrımcılıklara sebep olabilmektedir.²⁶⁴

Dijital ayrımcılık (digital discrimination) olarak adlandırılan veri madenciliği kaynaklı ortaya çıkan önyargı ve ayrımcılığı tespit etmek ve çözebilmek için yöntemleri geliştirmeye çalışan makine öğrenimi alanındaki araştırmacıların sundukları öneriler ilerideki bölümlerde daha detaylı bir şekilde incelenmeye çalışılacaktır²⁶⁵.

2.4.2.4. Algoritmik Şeffaflık

İnsan haklarını koruyan ve topluma faydalı algoritmik sistemlerin geliştirilmesi ve tasarlanması için kullanılabilecek araçlardan birisi de şeffaflıktır. Bu araç kendi başına değil hedeflediği şeylere olan katkısı ölçüsünde değerlidir. Otomatik karar alma mekanizmalarında veya algoritmalarda şeffaflığın (algorithmic transparency) ne olduğu ve şeffaflığı elde etmek için neye ihtiyaç duyulduğuna ilişkin bir netlik bulunmamaktadır. Bir yönüyle şeffaflık, bir kurumun veya kuruluşun ne yaptığını bilmiyorsak onu hesaba çekemeyiz şeklinde ifade edilebilir. Ancak algoritmik sistemler için bu açıklamanın daha ötesine gitme ihtiyacı duyulmaktadır. Algoritmik sistemlerin şeffaf olmasının talep edilmesinin en önemli sebeplerinden birisi özel, ailevi veya profesyonel hayatımızın, ekonomimizin tam merkezinde yer almaya başlaması ve çoğunun modellerinin ve algoritmalarının insan zekasının anlayabileceği seviyenin üstünde kompleks olmasıdır²⁶⁶.

²⁶⁴ Bettina Berendt, "More than modelling and hiding: towards a comprehensive view of Web mining and privacy", **Data Mining and Knowledge Discovery**, Vol.24, No.3, May 2012, pp.697-737.

²⁶⁵ Dijital ayrımcılıkla ilgili kavramı hakkında daha detaylı bilgi için "Digital Discrimination" kavramının ilk defa kullanıldığı esere bkz. Lyon, **Ibid**.

²⁶⁶ European Parliamentary Research Service (EPRS), "A governance framework for algorithmic accountability and transparency", **Scientific Foresight Unit (STOA)**, PE 624.262, April 2019, (Çevrimiçi) [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU\(2019\)624262_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf) 31 December 2019, p.4.

Özellikle kamunun ve kamusal alanın yönetişiminin sağlanmasında otomatik karar alma mekanizmalarının kullanılması, algoritmik şeffaflığın ve hesap verilebilirliğin elde edilebilmesi için yapılan araştırmalara hız kazandırdı²⁶⁷.

Algoritmik şeffaflık ile hangi amaca ulaşmak istenildiği ve algoritmanın çalışma mantığına ilişkin nasıl bilgi verilmesine ihtiyaç duyulduğunun belirlenmesi önemli bir başlangıçtır. Çünkü algoritmik karar alma sisteminin türüne ve kullanımına bağlı olarak; kod, mantık, model, hedef, karardaki değişkenler(variables) arasından bir veya birden fazla husus kastedilebilmektedir. Algoritmik şeffaflık, herhangi bir girdiye(input) ilişkin sistemin davranışına ilişkin anlayışa sahip olmayı ifaden eden “global” olarak adlandırılabilen gibi, belirli bir girdinin spesifik bir çıktıyla ilişkisi hakkında bilgiye sahip olmak olarak adlandırılan “local” şeklindeki konsepti de kastedebilmektedir.²⁶⁸

Her makine öğrenimi algoritmasının ve uygulamasının birbirinden farklı şeffaflık ve hesap verilebilirlik yaklaşımıyla incelenmesini öneren çalışmalar bulunmaktadır. Tam otonom karar alan sistemler ile insanlara bilgi veya destek vererek yardımcı olan sistemlerin birbirinden farklı yaklaşımlarla ele alınması daha isabetli olacağı gibi okul servislerinin rotasının veya kamu kurumlarının çalışma saatlerinin optimize edilmesinde kullanılacak sistemlerin de farklı bir yaklaşımla incelenmesinin uygun olacağı belirtilmektedir. Çünkü her birinin uygulamaya alınması ve geliştirilmesi süreçlerinde aynı kategorideki paydaşlarla işbirliği yapmaması sebebiyle farklı tipte şeffaflık ve hesap verilebilirlik yöntemlerinin geliştirilmesi gerekmektedir.²⁶⁹

Avrupa Parlamentosunun hazırlamış olduğu raporda Makine öğrenimi sistemlerinin şeffaf olması istenilen yedi başlığı belirlenmiştir. Bunlar; veri, algoritmalar, amaçlar, çıktılar, uyum, etki ve kullanım şeklindedir. Veri ile kastedilen; verinin kaynağı, hazırlanması, önyargısız ve ölçülü seviyede temsili sağlayan metotlar, verinin güncellendiği veya yeniden eğitildiği süreçlerin hepsidir.

²⁶⁷ Jake Goldenfein, “Algorithmic Transparency and decision-making accountability: Thoughts for buying machine learning algorithms”, In Office of the Victorian Information Commissioner (Ed) **Closer to the Machine: Technical, Social, and Legal aspects of AI**, 2019. (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=344587331 December 2019.

²⁶⁸ EPRS, **Ibid.**, p.4.

²⁶⁹ Goldenfein, **Ibid.**

Algoritmalar başlığı altında; çıktılar ile girdilerin korelasyonlarının test edilmesi, 3. Kişiler tarafından kodun gözden geçirilmesi (third party code review), iç ve dıştan kaynaklı bug raporlarının kontrolü incelenmektedir. Otonom araçların trafik kazalarını azaltmayı, doğaya olan zararlı etkiyi düşürmeyi, ciddi yaralanmayı azaltmayı, ulaşım sürelerini kısaltmayı, yolculuk kalitesini artırmayı da amaçları arasında sayabiliriz. Otonom araçların kaç tane kazaya neden olduğu, ne kadar enerji harcadığı gibi bilgiler de çıktıları arasındadır. Şeffaflığa ilişkin hangi gereksinimleri yerine getirdikleri uyum açısından değerlendirilmelidir. Sistem eğer belirli bir hususu ön plana çıkarıyor ve bunu da ücret alarak veya başka menfaatlerde yapıyorsa bunun da açık olması etki edilmek istenilen şeyin belirlenmesi adına önemlidir. Otonom aracın yaptığı seyahatlere ilişkin detaylı bilgiler trafiğin, güvenliğin veya yakıt verimliliğinin optimizasyona ilişkin kullanılabilir ancak buna ilişkin hangi verileri işlendiğinin açıklanması da kullanım açısından önemlidir.²⁷⁰

Algoritmik karar alma sistemlerinin teknik anlamda yaptıkları işlemleri ve tercihleri değerlendirmenin ötesinde, insanların ve kurumların aldıkları kararlara olan etkileri yönüyle analizinin yapılmasının algoritmik şeffaflığın sağlanması adına daha isabetli olacağı düşünülen araştırmacılar bulunmaktadır.²⁷¹

Şeffaflık; yetkili kişi veya kurumların talepleri doğrultusunda erişim sağlanması, kamuya bilginin paylaşılması, iç süreçlerin teftiş edilmesi, sistemin isabetliliği ve adilliğine ilişkin üreticisinin testlerine ilişkin sonuçların paylaşılması, sistemdeki verinin yetkili kurumlar tarafından denetlenmesi, sonuçlara ilişkin düzenleyici kurumlara bildirimde bulunulması gibi kategorilerde farklı şekillerde anlaşılabilir.²⁷²

YZ sistemlerinin verilerinin ve algoritmalarının denetlenmesiyle; önyargının, sistemin adilliğinin, hatalarının kontrol edilmesi hedeflenmektedir. YZ sistemlerinin uyum durumlarının kamuya açıklanmasıyla kurumlar tarafından hesap sorulabilmesine imkân tanınması istenmektedir. Ayrıca toplum da kurumların

²⁷⁰ EPRS, *Ibid.*, p.4.

²⁷¹ 3. Bölümdeki Açıklama yöntemlerine ilişkin kara kutu (black box) yaklaşımındaki LIME yönteminin açıklandığı Bölüm 3.2.1.3'e bakılabilir.

²⁷² EPRS, *Ibid.*, p.6.

güvenilirliğini değerlendirip sistemin risklerini, faydalarını belirleyip buna bağlı olarak bilgilenmiş kararlar alabilecektir.²⁷³

Algoritmik şeffaflığın elde edilememesinin birçok nedeni bulunmaktadır. Bunlardan ilki YZ sistemlerindeki kara kutu ve opaklık sorunlarıdır. Makine öğrenimi algoritmalarının yapıları sebebiyle hangi veri noktalarının (data points) hesaplamada kullanıldığı ve sonuç üzerinde ne kadar ağırlığa ve etkiye sahip olduğunun belirlenmesi hususunda netlik bulunmamaktadır.²⁷⁴

Algoritmalarla risk değerlendirmesinin yapılmasının YZ sistemlerinin insan haklarına en fazla temasta bulunduğu alanların başında gelmektedir. Sosyal yardımlara ve eğitim olanaklarına erişimde, iltica başvurularına ilişkin kararlarda makine öğrenimi sürecin belirli safhalarında risk değerlendirilmesi yapılabilmesi amacıyla kullanılmaktadır. Yargılama sürecinde şartlı tahliye kararı verilebilmesi için kişinin sicili, eğitim ve iş geçmişi, finansal durumu, aile durumu, kalacak yer bilgisi, arkadaşları, alkol ve uyuşturucu kullanımı, karakteri ve davranış biçimi gibi kategoriler sisteme girilerek risk değerlendirmesi yapılmaktadır. Kefalet, şartlı tahliye veya cezanın takdiri gibi konularda YZ sistemler kararın alınmasına destek olmaktadır.²⁷⁵ Bu tip karar almaya ilişkin destek sistemleri halihazırda ABD'nin birçok yargı yerinde kullanılmaktadır.

Otomatik karar alma mekanizmalarının kolluk kuvvetleri tarafından kullanımının kamu güvenliği ve suçla mücadele kapsamında kullanılması özel hayatın gizliliği hakkının ve diğer temel hakların ihlal edilmesine sebep olacaktır. Gelecek polisliği "Predictive policing" süreçlerinde de algoritmik karar alma sistemlerinin²⁷⁶ yaygın olarak kullanıldığı görülmektedir²⁷⁷. Ne zaman veya nerede suçun suçun işlenme ihtimali olduğuna ve kimin fail olabileceğine ilişkin soruları

²⁷³ EPRS, **Ibid.**, p.7.

²⁷⁴ Goldenfein, **Ibid.**

²⁷⁵ Bernard H. Harcourt, "Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age", **University of Chicago Press**, 2007.

²⁷⁶ Amerikanın Echelon sistemi, Amerikadaki predictive policing uygulamaları, Çindeki Facial recognition kameraları üzerinden kişilerin takibi ve credit scoring yapılması gibi.

²⁷⁷ Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith, John S. Hollywood, "Predictive policing: The role of crime forecasting in law enforcement operations", **Rand Corporation**, 2013 (Çevrimiçi)
https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf 31 December 2019.

gelecek polisliđi yanıtlamaya çalışmaktadır. Bu alanın öne çıkan şirketlerinden Palantir New Orleans, Los Angeles ve Chicago’da cezaya ilişkin bilgileri içeren veri tabanlarından çektiđi balistik, çete faaliyetleri, şartlı tahliye, cezaevi telefon kayıtlarına ilişkin verileri işlediđi sistemler kurarak potansiyel olarak gelecekte suç işleyebilecek faillerin ve suçun mağdurlarının tespitini yapmaya çalışmaktadır.²⁷⁸ Avustralya’da “predictive policing” kullanımının sonuçlarında sistemin tespit ettiđi kişilerin %44’ünün “indigenous” yani yerli halktan olduđu görülmüştür²⁷⁹. Yine bu sistemlerinde şeffaflığının sağlanması da kişilerin haklarını savunabilmesi için mekanizmaların oluşturulabilmesi, hak arama hürriyetinin korunması ve savunma hakkını kullanabilmesi için oldukça gereklidir.

Otomatik karar alma mekanizmaları aracılığıyla yapılan risk değerlendirmelerinde algoritmik şeffaflığa ilişkin başlıca zorluklar şunlardır:

1. Risk değerlendirmesinde kullanılacak verilerin seçimi ve sonuca etkileri²⁸⁰,
2. Sosyal açıdan zararlı etkileri²⁸¹,
3. Kullanılan veri ile önemli olan verinin arasındaki uyumsuzluk²⁸².

Kamusal alanlarda algoritmik sistemlerin kullanılmasının verimlilik açısından faydalı olacağı tezi öne sürülmektedir. Ancak kara kutu ve opaklık sorunları karşısında bu argüman yeterli görülmemektedir. Kamu finansmanının daha verimli kullanılabilmesi için yapılan baskılar sonucunda şeffaflık ve hesap verilebilirlik

²⁷⁸ Ali Winston, “Palantir has secretly been using New Orleans to test its predictive policing technology”, **The Verge**, February 27, 2018. (Çevrimiçi) <https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd> 31 December 2019.

²⁷⁹ Vicki Sentas, Camilla Pandolfini, “Policing young people in NSW: A study of the suspect targeting management plan”, A Report of the Youth Justice Coalition, **NSW**, 2017, (Çevrimiçi) <https://www.piac.asn.au/wp-content/uploads/2017/10/17.10.25-YJC-STMP-Report.pdf> 31 December 2019.)

²⁸⁰ Julia Dressel, Hany Farid, “The accuracy, fairness, and limits of predicting recidivism”, **Science Advances**, Vol.4, No.1., 2018.

²⁸¹ Cathy O’Neil, “Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy”, **Broadway Books**, 2016; Virginia Eubanks, “Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor”, **St Martin’s Press**, 2018.

²⁸² David G. Robinson, “The challenges of prediction: Lessons from criminal justice”, **IS: A Journal of Law and Policy for the Information Society**, Vol.14, No.2, 2017, p.151.

ilkelerini feda etmeden algoritmik sistemlerin istihdam edilmesinin yollarının ve yöntemlerinin bulunması gerekmektedir.²⁸³

Algoritmik sistemlerin şeffaflığının sağlanabilmesi için nasıl çalıştığının anlaşılabilmesine ihtiyaç duyulmaktadır. Veri noktasının değiştirilmesinin sistemin tahminine olan etkisinin bilindiği oranda ilgili kişinin diğerlerinden hangi noktada ayrıldığı tespit edilebilecektir. Ayrıca örneğin tarihsel anlamda ayrımcılığa uğramış topluluklar gibi farklı gruplara karşı algoritmik modelin herhangi bir farklı yaklaşımda bulunduğu tespiti için de sistemin analiz edilebilmesi gerekmektedir.²⁸⁴

Algoritmik şeffaflığı artırabilmek alınan kararların gerekçelendirilmesi ve sonrasında yargısal denetime gidilmesi aracılığıyla da dolaylı yoldan sağlanabilecektir. Otomatik karar alma mekanizmalarında şeffaflığın esas alınması algoritmik yönetişimi (algorithmic governance) ve algoritmik hesap verilebilirliği (algorithmic accountability) sağlamada katkı sağlayacaktır.

Algoritmik şeffaflığın sağlanabilmesi için kullanılacak olan sistemin nasıl karar aldığı ve çalıştığı belirli bir seviyeye kadar açıklanması çözümü eğer riskler iyi hesaplanmadan gerçekleştirilse, aleyhe kullanıma, YZ sisteminin saldırıya uğramasına ve şirketlere karşı dava açılmasına veya kamu kurumlarının inceleme başlatmasına neden olabilecektir.²⁸⁵

Algoritmik sistemlerde şeffaflığın elde edilmesi amacıyla atılacak adımların risk değerlendirmeleri veya maddi yönden belirli karşılıkları olacaktır. Ayrıca veri güvenliği açısından YZ sistemlerinin tehditlere daha açık hale gelmesi de değerlendirme yapılırken dikkate alınmalıdır. Makine öğrenimi modellerinin eğitim verisine erişim sağlanmadan veya kaynak koduna erişime ihtiyaç duymadan sistemin davranış modellerinin manipüle edilebilmesi mümkündür. Klasik anlamda hackleme yollarına başvurmadan şeffaflığın sağlanması amacıyla takip edilen

²⁸³ Ben Wagner, "Efficiency vs. Accountability? – Algorithms, Big Data and Public Administration", December 2016. (Çevrimiçi) <https://cihr.eu/efficiency-vs-accountability-algorithms-big-data-and-public-administration/> 31 December 2019.

²⁸⁴ James Wexler, Mahima Pushkarna, Tolga Bolukbasi, Martin Wattenberg, Fernanda Viegas, Jimbo Wilson, "The What-If Tool: Interactive Probing of Machine Learning Models", **IEEE Transactions on Visualization and Computer Graphics**, Vol.26, No.1, 2019, pp.56-65. (Çevrimiçi) <https://arxiv.org/pdf/1907.04135.pdf> 31 December 2019.

²⁸⁵ Andrew Burt, "The AI Transparency Paradox", **Harvard Business Review**, 13 Aralık 2019, (Çevrimiçi) <https://hbr.org/2019/12/the-ai-transparency-paradox> 31 December 2019.

süreçlerin yansımaları analiz edilip sistemin istenilen yönde kullanılması ihtimali bulunmaktadır. Olumsuz muhtemel sonuçlar arasında ki; veri sızıntıları ve sistemin manipüle edilmesi, kurumların kişisel verilerin korunması açısından veri güvenliğini sağlayamadıkları sebebiyle yaptırımlara maruz kalmasına neden olacaktır.²⁸⁶

Kötü niyetli aktörler sistemin şeffaflığını sağlayan yöntemler aracılığıyla sistemin üreticilerinden daha iyi sistemi tanıyıp zarara uğramasına neden olabilir. Çözüm olarak eğitim verisine rastgele parazit (noise) eklenmesini sağlayan differential privacy yöntemi, farklı katmanlarda veriyi işlemeye yarayan federated learning metodu veya açıklanabilir algoritmalar Scalable Bayesian Rule Lists (SBRL)²⁸⁷ algoritması ele alınabilir.

2.4.2.5. Algoritmik Hesap Verilebilirlik

Yaşadığımız dönem itibariyle günlük yaşantılarımızın nasıl değiştiğini, teknolojinin hayatımızda ne kadar fazla yer aldığını daha önceki bölümlerde anlatmıştık. YZ sistemlerinin bize sağladığı faydaların yanı sıra, aldıkları kararlarla çoğu zaman öngörülemeyen haksızlıklara veya ayrımcılıklara sebep olabileceği de ifade edilmişti. Hukukun, teknolojiyi düzenleme hususunda geride kaldığı günümüzde, kurumların veya kuruluşların algoritmaların neden olduğu sorunları çözme hususunda önde gitmesi gerektiği yazılıp çizilmektedir. YZ sistemlerini kullanan kurumların uygulamaya aldığı algoritmalarının neden olabileceği sorunları öngörüp bunları azaltmaya ilişkin tedbirleri alması beklenmektedir.²⁸⁸

Algoritmik hesap verilebilirlik, algoritmaların karar alma süreçlerindeki rolüne ilişkin tartışmalarda öne çıkan bir kavram. Otomatik karar alma süreçleri için geliştirilen ve kullanılan algoritmaların ayrımcı, hatalı ve gayri meşru sonuçlara

²⁸⁶ Sophie Stalla-Bourdillon, Brenda Leong, Patrick Hall, Andrew Burt, "Warning Signs. The Future of Privacy and Security in an Age of Machine Learning", **Future of Privacy Forum**, September 2019. (Çevrimiçi) https://fpf.org/wp-content/uploads/2019/09/FPF_WarningSigns_Report.pdf 31 December 2019.

²⁸⁷ Hongyu Yang, Cynthia Rudin, Margō Seltzer, "Scalable Bayesian Rule Lists", **Proceedings of the 34th International Conference on Machine Learning**, Vol.70, 2017, (Çevrimiçi) <https://arxiv.org/abs/1602.08610> 31 December 2019.

²⁸⁸ Hemant Taneja, "The need for algorithmic accountability", September 8, 2016. (Çevrimiçi) <https://techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/> 31 December 2019.

neden olup olmadığının kontrol edilebilmesi algoritmaların hesaba çekilmesi anlamına gelmektedir.

Algoritmik sistemler hatalı veya istenmeyen sonuçlara yol açabilir. Bunlara başlıca örnek olarak şunlar verilebilir:

1. Yapısallaşmış ayrımcılığı artırması²⁸⁹,
2. Hatalı sonuçlar üreterek kişilerin hizmeti alamamasına neden olması²⁹⁰,
3. Seçim sonuçlarına ilişkin hatalı sonuçlar üretmesi²⁹¹.

YZ sistemlerinin neden olduğu zararların veya ihlallerin sorumluluğunun kimde olacağı aslında başka bir hukuk dalının konusu. Fakat toplumdaki YZ sistemlerin üretilmesine ilişkin bilgi eksikliği sebebiyle alınan kararların sorumluluğunun kimde olacağının kolaylıkla bilinemeyeceği bu sebeple de mağduriyetlerin telafisi amacıyla hangi yollara başvurulacağı ve kime yönelteceği konusunda da kafa karışıklığı görülmektedir. "Singularity"²⁹² seviyesine kadar YZ sistemlerine bir sorumluluk yüklenmesi hem bilimsel hem de mantıklı görünmemektedir. Algoritmalar ve eğitilmelerinde kullanılan veri setlerinin ne olacağına ilişkin kararları insanlar tarafından verilmektedir. Algoritmik sistemler tarafından veya desteğiyle alınan kararların sorumluluğu her halükârda bir gerçek kişiye veya tüzel kişiye ait olacaktır. YZ sistemlerinin hata yaptıklarında veya arzu edilmeyecek sonuçlara sebep olduklarında; algoritmalar yaptı açıklaması yeterli olmayacaktır. Çünkü bir görüşe göre; algoritmik hesap verilebilirlik ilkesi, otomatik karar alma sistemlerinin aldığı kararların meşru gerekçelendirmesinin bulunmasına

²⁸⁹ Lum Kristian, Isaac William, "To predict and serve?", **Significance**, Vol.13, No.5, 2016, pp.14-19. (Çevrimiçi) <https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x> 31 December 2019.

²⁹⁰ Meghan E. Irons, "Caught in a dragnet", July 17, 2011, (Çevrimiçi) http://archive.boston.com/news/local/massachusetts/articles/2011/07/17/man_sues_registry_after_license_mistakenly_revoked/ 31 December 2019.

²⁹¹ Michael Reilly, "Prediction Models Gone Wild: Why Election Forecasts and Polls Were So Wrong", **MIT Technology Review**, Nov 9, 2016. (Online) <https://www.technologyreview.com/s/602829/prediction-models-gone-wild-why-election-forecasts-and-polls-were-so-wrong/> 31 December 2019.

²⁹² Singularity; sıradan insanların yapay zekâlığı makineler veya bilişsel olarak geliştirilmiş biyolojik zekalar tarafından ele geçirilmesi olarak ifade edilmektedir. İnsan seviyesinde yapay zekâların bulunmasının kişilik, sorumluluk, haklar ve kimlik gibi konuların tartışılmasını gerektirecektir. Ancak tabi ki de ihtimal dahilinde olan bu günlerin gelmesinden önce konunun ele alınmasında fayda görüyoruz. Detaylı bilgi için bkz. Vernor Vinge, "The coming technological singularity: How to survive in the post-human era", **Science Fiction Criticism: An Anthology of Essential Writings**, 1993, pp.352-363.

ve sosyal anlamda etkilerini veya potansiyel zararlarını azaltabilecek önlemlerin alınmasına ilişkin yükümlülük getirmektedir²⁹³.

FAT/ML adında bir topluluk tarafından, aralarında saygın araştırmacıların ve iş profesyonellerinin bulunduğu, yapılan çalışma sonucunda ortaya konan prensipler algoritmik hesap verilebilirliğin değerlendirilmesi açısından bir başlangıç olabilir. Algoritmik sistemler tarafından desteklenen kararların sosyal etkileri çok ciddi sonuçlar doğurmaktadır. Algoritmik sistemlerin hesap verilebilir olmasıyla kastedilenin;

1. Bildirim yükümlülüğü,
2. Açıklama yükümlülüğü,
3. Algoritmik sistemin aldığı kararların meşru gerekçelerini ortaya koyma yükümlülüğü,
4. Negatif sosyal etkilerini ve potansiyel zararlarını telafi etme yükümlülüğü

olduğu ifade edilmiştir²⁹⁴.

FAT/ML algoritmik hesap verilebilirliğe ilişkin ilkelerini 5 temel başlık altında belirlemiş;

1. Sorumluluk (Responsibility); algoritmik karar alma sisteminin bireysel veya toplumsal etkilerini telafi edebilmek için kurumlara gelebilecek başvuru ve bilgi alma yollarının tasarlanması ve kurum içerisinde bu süreçten sorumlu bir kişi veya departmanın belirlenmesini gerektirmektedir. Herkes tarafından erişilebilir bir kişi olması, sistemi düzeltecek, geliştirecek kaynaklara sahip olması ve yeterli donanım ve bilgiye sahip olması beklenmektedir.
2. Açıklanabilirlik (Explainability); YZ sistemleriyle alınan tüm kararların son kullanıcıya ve diğer paydaşlara teknik olmayan terimlerle açıklanabilmesi.

²⁹³ Nicholas Diakopoulos, Sorelle Friedler, Marcelo Arenas, Solon Barocas, Michael Hay, Bill Howe, H.V. Jagadish, Kris Unsworth, Arnaud Sahuguet, Suresh Venkatasubramanian, Christo Wilson, Cong Yu, Bendert Zevenbergen, "Principles for Accountable Algorithms and a Social Impact Statement for Algorithms", **Fairness Accountability and Transparency in Machine Learning (FAT/ML)**, November 18, 2016 (Çevrimiçi) <https://www.fatml.org/resources/principles-for-accountable-algorithms> 31 December 2019.

²⁹⁴ Diakopoulos / Friedler / Arenas / Barocas / Hay / Howe / Jagadish / Unsworth / Sahuguet / Venkatasubramanian / Wilson / Yu / Zevenbergen, **Ibid.**

3. Doğruluk (Accuracy); algoritmalar ve veri toplanan kaynaklar ile ilgili belirsizliklerin ve hataların belirlenmesi, kaynakların kayıt altına alınıp işlemlerin loglanması, bu sayede risklerin ve olumsuz sonuçların azaltılmasına ilişkin süreçlerin daha iyi belirlenmesi ve planlanmasının sağlanması.
4. Denetlenebilirlik (Auditability); ilgili 3. Kişilerin ayrıntılı dokümantasyon ve teknik olarak uygun API'ler ile otomatik karar alma mekanizmalarını izlemesi ve kontrol edebilmesi, sistemin açıklanması yoluyla algoritmaların karar alma davranışlarının incelenmesi ve anlaşılabilmesi.
5. Adillik (Fairness); algoritmik sistemlerle alınan kararların, ırk, cinsiyet gibi kişisel verileri hesaba katarak ayrımcı ve haksızlığa neden olabilecek sonuçlar üretmediğinden emin olunması. Tarihsel ve sosyal anlamdaki veri setlerindeki mevcut önyargının YZ sistemleriyle devam ettirilmesinin ve hatta artmasının engellenmesi.

Algoritmik sistemlerin aldıkları kararların sorumluluğunun kime yöneltileceğinin de önceden belirlenmesine ihtiyaç duyulmaktadır. ABD yargı sisteminde kullanılan yargılama süreçlerine ve cezalandırmaya ilişkin karar destek sistemlerini besleyen risk değerlendirme skorları açısından algoritmik hesap verilebilirlik ilkesi önemlidir.²⁹⁵ Geçmişteki sanıklara ilişkin bilgilerin yer aldığı veri setleriyle eğitilen makine öğrenimi algoritmaları içeriğinde sanıkların yaşları, suç geçmişleri ve karakterine ilişkin diğer veri kategorilerinin de yer aldığı modellemeler ile tarihsel önyargı aktarılmış olmaktadır. Yapılan araştırmalarda risk değerlendirme araçlarının siyahileri yüksek riskli sanıklar olarak belirlemeye daha fazla eğilimli olduğu tespit edilmiştir.²⁹⁶

Algoritmik hesap verilebilirlik için önerilen karar verme döngüsünde insanın yer alması (human-in-the-loop) fikrinin mekanizmanın önyargısını giderebilme adına beklenen faydayı göstermeyeceği ifade edilmektedir. Sistemin hangi gerekçeyle karar aldığını anlayamayan ve dolayısıyla gerekli açıklamayı yapamayacak olan

²⁹⁵ EPIC, "Algorithms in the Criminal Justice System: Pre-Trial Risk Assessment Tools", June 24, 2016. (Çevrimiçi) <https://epic.org/algorithmic-transparency/crim-justice/> 31 December 2019.

²⁹⁶ Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner, "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks", **ProPublica**, May 23, 2016. (Çevrimiçi) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> 31 December 2019.

kişilerin kararlara müdahale etmesi ihtimali göz önünde bulundurulursa, toplumsal değerlerin teknolojik sistemlerin tasarlandığı ve geliştirildiği safhalarda sistemin özüne işlenmesinin en sonunda yapılacak gözden geçirmeler veya düzeltmelerden daha başarılı olacağı düşünülmektedir.²⁹⁷

Algoritmik sistemler üzerine çalışanların ayrımcılığı daha henüz gerçekleşmeden tespit edip önleyebilecek çözümler üretmesi beklenebilmektedir. Ancak ex-ante önlemlerin, süreçler uygulamaya alındıktan sonra da denetlemeye imkân sağlayan ex-post yaklaşımlarla da desteklenmesi gerekmektedir. Algoritmik hesap verilebilirliğin ikili sistemi içerisinde ilgili kişinin haklarının kapsamlı bir şekilde yerine getirilmesi ve çözüm odaklı yönetim yapısına sahip kurumlar bulunmaktadır. Çalışmamızın son bölümünde bu ikili sistem ele alınacaktır.

²⁹⁷ Goldenfein, **Ibid.**

ÜÇÜNCÜ BÖLÜM

YAPAY ZEKÂ SİSTEMLERİ BAKIMINDAN KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HAKLAR VE ALINMASI GEREKEN TEDBİRLER

Bu bölümde yapay zekâ sistemleri bakımından kişisel verilerin korunmasına ilişkin haklar ve alınması gereken tedbirler; ilgili kişinin hakları ile kişisel verilerin korunmasına ilişkin alınabilecek teknik veya idari tedbirler başlıkları altında incelenecektir.

3.1. İLGİLİ KİŞİNİN HAKLARI

Yapay zekâ sistemleri bakımından kişisel verilerin korunmasına ilişkin hakkında veri toplanan ilgili kişinin hakları dört kategoride toplanabilir. Bunlar; (1) bilgi edinme, düzeltme, sildirme hakkı, (2) itiraz etme hakkı, (3) profillemeye de dahil olmak üzere otomatik karar vermenin varlığı ve gerçekleştirilen işleme faaliyetinin kişi açısından önemi ve öngörülen sonuçları da dahil olmak üzere çalışma mantığına ilişkin anlamlı bilgilerin sunulması hakkı ve (4) profillemeye, insan müdahalesi talep etme ve açıklama talep etme hakkıdır. Bu bölümde bu haklar ele alınacaktır.

3.1.1. Bilgi Edinme, Düzeltme, Sildirme Hakkı

Bilgi edinme, düzeltme, sildirme hakkı; 6698 sayılı KVKK'nın "Haklar ve Yükümlülükler" başlıklı Üçüncü Bölümde yer alan "İlgili kişinin hakları" başlıklı 11. maddesinin 1. fıkrasının a-f bendlerinde düzenlenmiştir. İlgili kişinin bu hakları; kişisel veri işlenip işlenmediği (m.11a), işleniyor ise bunlara yönelik bilgi verilmesi (m.11b), bu verilerin hangi amaçla işlendiğini ve işlenmesinin amaca uygun olup olmadığını öğrenme (m.11c), varsa bu bilgilerin aktarıldığı yerli ve yabancı kişileri öğrenme (m.11ç), bu verilerin yanlış işlenmesi durumunda düzeltilmelerini isteme (m.11d), aynı kanunun 7. maddesinde belirtilen şartlar doğrultusunda bu verilerin silinmesini ya da yok edilmesini talep etme (m.11e), düzeltme, silme ve yok etme

işlemlerinin ilgili üçüncü şahıslara da iletilmesini sağlama (m.11f) şeklinde sıralanmıştır.²⁹⁸

GDPR’de ise hakkında bilgi toplanan ilgili kişinin bilgi edinme hakkı m.15’te (toplam 4 fıkra), bilgilerin düzeltilmesini isteme hakkı m.16’da (tek fıkra), bilgileri sildirme veya unutulma hakkı ise m.17’de (toplam 3 fıkra), düzenlenmiştir. GDPR’nin “*Right of access by the data subject*” (ilgili kişinin erişim hakkı) başlıklı 15. maddesinin 1. fıkrasına göre ilgili kişi, kendisi ile ilgili kişisel verilerin işlenip işlenmediği konusunda veri sorumlusundan teyit alma ve bu durumda kişisel verilerine ve aşağıdaki bilgilere erişim hakkına sahiptir²⁹⁹:

- (a) işleminin amaçları,
- (b) ilgili kişisel veri kategorileri,
- (c) kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri, özellikle üçüncü ülkelerdeki veya uluslararası kuruluşlardaki alıcılar,
- (d) mümkünse, kişisel verilerin saklanacağı öngörülen süre veya mümkün değilse, o dönemi belirlemek için kullanılan kriterler,
- (e) veri sorumlusundan kişisel verilerin düzeltilmesini veya silinmesini veya veri konusu ile ilgili kişisel verilerin işlenmesinin kısıtlanmasını talep etme veya bu işleme itiraz etme hakkının varlığı,
- (f) denetim makamına şikâyetle bulunma hakkı,
- (g) kişisel verilerin ilgili kişiden toplanmadığı durumlarda, kaynaklarına ilişkin mevcut bilgiler,
- (h) GDPR m.22/1 ve m.22/4’te belirtilen profileme dahil olmak üzere otomatik karar vermenin varlığına ilişkin ve varlığı halinde değerlendirmede kullanılan mantığa (yapılan değerlendirmenin çalışma

²⁹⁸ Kişisel Verilerin Korunması Kanunu (KVKK), m.11.

²⁹⁹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 15**, p.43.

mantığına) yönelik makul ve anlamlı bilgilerin yanı sıra, bu tür işlemlerin ilgili kişi açısından önemi ve öngörülen sonuçlarına ilişkin anlamlı bilgiler.

GDPR m.15/2'ye göre kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarıldığı durumlarda, ilgili kişinin, aktarımla ilgili 46. madde uyarınca uygun güvencelerden haberdar olma hakkı bulunmaktadır. GDPR m.15/3'e göre veri sorumlusu, ilgili kişiye işlenmekte olan kişisel verilerin bir kopyasını sağlayacaktır. Veri sorumlusu, ilgili kişi tarafından talep edilen diğer kopyalar için idari maliyetlere dayalı olarak makul bir ücret talep edebilir. İlgili kişinin talebi elektronik yollarla yapması ve ilgili kişi tarafından aksi istenmedikçe, bilgi yaygın olarak kullanılan bir elektronik yolla sağlanacaktır. GDPR m.15/4'e göre ise m.15/3'te atıfta bulunulan bir kopya elde etme hakkı, başkalarının hak ve özgürlüklerini olumsuz etkilememelidir.³⁰⁰

Bilgilerin düzeltilmesini isteme hakkı GDPR'nin "*Rectification and erasure*" (Düzeltilme ve silme) başlıklı 3. Bölüm'ünde yer alan "*Right to rectification*" (Düzeltilme hakkı) başlıklı 16. maddede, tek fıkrada düzenlenmiştir. Buna göre; ilgili kişi, kendisi ile ilgili hatalı kişisel verilerin gecikmeksizin düzeltilmesini veri sorumlusundan isteme hakkına sahiptir. İşlemin amaçları göz önünde bulundurularak, ilgili kişinin tamamlayıcı bir beyan da dahil olmak üzere eksik kişisel verilerini tamamlama hakkı bulunmaktadır.³⁰¹

Bilgileri sildirme veya unutulma hakkı, yine 3. Bölüm'de yer alan "*Right to erasure ('right to be forgotten')*" (Sildirme hakkı/unutulma hakkı) başlıklı 17. maddede, toplam 3 fıkrada düzenlenmiştir. GDPR m.17/1'e göre ilgili kişi, kendisiyle ilgili kişisel verilerin gereksiz gecikme olmaksızın silinmesini veri sorumlusundan edinme hakkı olacaktır ve veri sorumlusu aşağıdaki gerekçelerden birinin geçerli olduğu durumlarda, kişisel verileri gereksiz gecikme olmaksızın silme yükümlülüğü bulunmaktadır³⁰²:

³⁰⁰ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 15**, p.43.

³⁰¹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 16**, p.43.

³⁰² Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 17**, pp.43-44.

- (a) Kişisel verilerin, toplanma amaçları veya başka bir şekilde işleme amaçları ile ilgili olarak artık gerekli olmaması,
- (b) İlgili kişinin, işlemin m.6/1a veya m.9/2a'ya dayandığı ve işlem için başka yasal bir zeminin bulunmadığı durumlarda rızasını geri çekmesi,
- (c) İlgili kişinin, m.21/1 uyarınca verinin işlenmesine itiraz etmesi ve işleme için geçersiz bir meşru gerekçe olmaması veya ilgili kişinin m.21/2 uyarınca işleme tabi tutulması,
- (d) kişisel verilerin yasalara aykırı olarak işlenmesi,
- (e) kişisel verilerin, veri sorumlusunun tabi olduğu Birlik veya Üye Devlet hukukundaki yasal bir yükümlülüğe uygun olması için silinmesinin gerekmesi,
- (f) kişisel verilerin, m.8/1'de atıfta bulunulan bilgi toplumu hizmetlerinin sunulmasına ilişkin toplanmış olması.

GDPR m.17/2'ye göre veri sorumlusu; kişisel verileri kamuya açık hale getirdiği ve m.1 uyarınca kişisel verileri silmek zorunda olduğu durumlarda, mevcut teknolojiyi ve uygulama maliyetini göz önünde bulundurarak, ilgili kişinin silinmesini talep ettiği kişisel verileri işleyen veri sorumlularını, bu kişisel verilerle ilgili herhangi bir bağlantı veya kopya veya çoğaltma hakkında bilgilendirmek için teknik tedbirleri de içeren makul tedbirler alacaktır.³⁰³

GDPR m.17/3'e göre ise veri işlemenin gerekli olduğu aşağıdaki durumlarda m.17/1 ve 17/2 geçerli olmayacaktır³⁰⁴:

- (a) ifade ve bilgi özgürlüğü hakkını kullanmak için,
- (b) veri sorumlusunun tabi olduğu Birlik veya Üye Devlet yasalarının işlenmesini gerektiren yasal bir yükümlülüğe uyulması veya kamu yararına veya veri sorumlusuna verilen resmi otoritenin uygulanmasında yürütülen bir görevin yerine getirilmesi için,
- (c) m.9/2 (h) ve (i) bentleri ile m.9/3 uyarınca, halk sağlığı alanında kamu yararı nedenlerinden dolayı,

³⁰³ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 17/2**, p.44.

³⁰⁴ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 17/3**, p.44.

- (d) 89 (1) maddesi uyarınca kamu yararına, bilimsel veya tarihsel araştırma veya istatistiki amaçlarla arşivleme amacıyla 1. paragrafta atıfta bulunulan hakkın, bu işlemin amaçlarına ulaşılmasını imkânsız hale getirmesi veya ciddi şekilde bozmasının muhtemel olması,
- (e) yasal taleplerin tesis edilmesi, uygulanması veya savunulması için³⁰⁵

Görüleceği gibi bilgi edinme, düzeltme, sildirme hakkı; GDPR’de m.15-17’de kapsamlı ve bütünleyici istisnalarıyla birlikte düzenlenmişken, 6698 sayılı KVKK’da temel olarak m.11/1’in a-f bendlerinde istisnaları belirtilmeksizin ancak yalnızca 7. maddeye atıfta bulunularak düzenlenmiştir. Bu bakımdan sadece 6698 sayılı KVKK’nın doğrudan ve net olarak “İlgili kişinin hakları” başlıklı 11. maddesi hakların ilgili kişinin haklarını kullanabilmesi açısından yeterli olmamakta ve hatta ilk bakışta bu hakların ilgili kişi tarafından kolaylıkla alınabileceğini düşündürmektedir. Ancak ilgili kanunun diğer maddelerinde (m.5-9) yer alan istisnalar ve diğer koşullar da bu hakkın kullanılabilmesini etkilemekte, özellikle m.7’de kişisel verilerin silinmesine, yok edilmesine ya da anonimleştirilmesine yönelik diğer kanunlardaki hükümlerin saklı olduğu, bu konudaki usul ve esasların yönetmelik ile düzenlendiği belirtilerek bu hakların ilgili kişi tarafından kullanılabilmesine geniş istisnalar getirilmektedir.

3.1.2. İtiraz Etme ve Zararların Giderilmesini İsteme Hakkı

İtiraz etme ve zararların giderilmesini isteme hakkı, 6698 sayılı KVKK’nın “Haklar ve Yükümlülükler” başlıklı Üçüncü Bölümde yer alan “İlgili kişinin hakları” başlıklı 11. maddesinin 1. fıkrasının g ve ğ bendlerinde düzenlenmiştir. İlgili kişinin bu hakları; verilerin işlenmesi sırasında özellikle otomatik sistemlerle analizinde ortaya çıkabilecek ilgili kişinin aleyhine olacak sonuçlara itirazda bulunma (m.11g) ve bu verilerin kanuna uygun olmayan yol ve yöntemlerle işlenmesinden kaynaklı zararların giderilmesini isteme (m.11ğ) şeklinde sıralanmıştır.³⁰⁶

³⁰⁵ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 17/3**, p.44.

³⁰⁶ Kişisel Verilerin Korunması Kanunu (KVKK), m.11.

3.1.3. Profillemeye de Dahil Olmak Üzere Otomatik Karar Vermenin Varlığı ve Gerçekleştirilen İşleme Faaliyetinin Kişi Açısından Önemi ve Öngörülen Sonuçları da Dahil Olmak Üzere Çalışma Mantığına İlişkin Anlamlı Bilgilerin Sunulması Hakkı

Algoritmik sistemlerle karar verilmeden önce ilgili kişinin aydınlatılması, kararın doğru bir şekilde verilmesine etki etme ve yanlış veya hatalı verilmemesini sağlama adına önemlidir. GDPR'ye göre, kişisel veri, ilgili kişiden elde edilmiş olsun (GDPR m.13/2f)³⁰⁷ ya da olmasın (GDPR m.14/2g)³⁰⁸, veri sorumlusunun GDPR m.22/1 ve m.22/4'te belirtilen profillemeye dahil olmak üzere otomatik karar vermenin varlığına ilişkin ve varlığı halinde değerlendirmede kullanılan mantığa (yapılan değerlendirmenin çalışma mantığına) yönelik makul ve anlamlı bilgilerin yanı sıra, bu tür işlemlerin ilgili kişi açısından önemi ve öngörülen sonuçlarına ilişkin anlamlı bilgileri ilgili kişiye sunma ve işlemlerin ilgili kişiye ilişkin adil ve şeffaf olduğunu temin etme yükümlülüğü bulunmaktadır (GDPR m.13/2f ve m.14/2g). Dolayısıyla veri sorumlusunun bu yükümlülüğü, ilgili kişi açısından bir hak doğurmaktadır. Buna göre; verileri toplanan ilgili kişinin, kendisi hakkında profillemeye yapıp yapılmadığına, bu verilerin değerlendirilmesinde bir otomatik karar alma mekanizması kullanılıp kullanılmadığına, bu sistemin nasıl çalıştığına, kişisel verileri bu yollarla işlemenin kişi açısından önemine ve kişiye muhtemel etkilerine ilişkin veri sorumlusundan açıklama isteme hakkı bulunmaktadır. KVKK kapsamında sistemin yürüttüğü mantığa ilişkin izah getirilmesi amacıyla herhangi bir düzenleme bulunmamaktadır.

GDPR madde 13(2)(f), 14(2)(g) ve 22 ile par.60 kapsamında, veri sorumlusunun yapacağı bilgilendirmenin içeriğinde aşağıdaki temel unsurlar yer almalıdır:

1. Kişisel veri işleme sürecinde bir profillemenin yapıldığı,
2. Profillemenin amaçları,
3. Profillemenin neden olacağı sonuçlar,
4. Veri işleme faaliyetinin arkasında yatan mantık,
5. Tamamen otomatik karar alma mekanizmasıyla kararın alınıp alınmadığı,

³⁰⁷ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 13/2f**, p.41.

³⁰⁸ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 14/2g**, p.42.

ICO'nun rehberlerinde sade bir dil ile basit bir aydınlatmanın yapılabilmesi için katmanlı bilgilendirme, hareketli tablolar (dashboard), anında bilgilendirme (just-in-time) logolar (icons) ve her türlü inovatif çözümünün kullanılması gerektiği ısrarla ifade edilmektedir³⁰⁹. Avustralya veri koruma otoritesinin veri analitiği ve KVK ile ilgili ilkeler hakkında hazırladığı rehberde bilgilendirme metinlerinin olabildiğince basit, net ve etkili tasarlanması gerektiğini belirtmiştir. Dinamik, farklı katmanlardan oluşan ve kullanıcı dostu bir tasarımın veri sorumlusunun yeterli seviyede bilgilendirme yaptığını kanıtlaması adına etkili olacağı aktarılmıştır³¹⁰.

Sistemin çalışma mantığına ilişkin anlamlı bir bilgi ile neyin kastedildiği, gereksinimlerinin ne olduğu ve nasıl açıklanacağı hususunda düzenlemede bir netlik bulunmamaktadır³¹¹.

3.1.4. Profilleme, İnsan Müdahalesi Talep Etme ve Açıklama Talep Etme Hakkı

GDPR m.22'de otomatik karar alma mekanizmaları ile profilleme birlikte ele alınmıştır. GDPR m.22'de profilleme/profil oluşturma da dahil olmak üzere otomatik bireysel karar verme konusu "*Automated individual decision-making, including profiling*" başlığı altında düzenlenmiştir. GDPR m.22/1'e göre ilgili kişi, kendisi ile ilgili yasal etkiler veya 'benzeri önemli etkiler'³¹² yaratan, profil oluşturma dahil olmak

³⁰⁹ Birleşik Krallık Bilgi Komiserliği Ofisi (ICO - Information Commissioner's Office), "What methods can we use to provide privacy information", May 16, 2018. (Çevrimiçi) <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> 31 December 2019.

³¹⁰ Office of the Australian Information Commissioner, "Guide to Big Data and The Australian Privacy Principles", March 21, 2016. (Çevrimiçi) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/#s2-3-notification-app-5>, 1 Ocak 2020.

³¹¹ Goodman / Flaxman, **Ibid.**

³¹² Buradaki 'benzeri önemli etkiler' tabiri GDPR'nin 71. paragrafında "*where it produces legal effects concerning him or her*" tabirinin devamında "*or similarly significantly affects him or her*" şeklinde geçmektedir. İlk tabir "kişinin kendisi ile ilgili yasal etkiler yaratan" anlamına gelmektedir. Devamındaki tabir ise "veya benzer şekilde kişiyi önemli düzeyde etkileyen" anlamında kullanılmaktadır. Doktrinde "*similarly significantly affects*" tabirinin ne gibi benzer önemli etkiler olduğu tartışma konusudur. Ancak GDPR'nin 71. paragrafında bu tür etkilere yol açacak durumlara örnek olarak "*...such as automatic refusal of an online credit application or e-recruiting practices without any human intervention*" tabiri ile "çevrimiçi bir kredi başvurusunun otomatik olarak reddedilmesi veya herhangi bir insan müdahalesi olmadan e-işe alım gibi" uygulamalar gösterilmiştir. Bu örneklerden yola çıkıldığında "benzer önemli etkiler" yaratan uygulamaların kişinin ekonomik durumunu etkileyecek iki örnekle

üzere yalnızca otomatik işlemeye dayalı alınan bir karara tabi olmama, reddetme/itiraz etme hakkına sahiptir. Ancak GDPR m.22/2'ye göre; (a) kararın ilgili kişi ile veri sorumlusu arasında bir sözleşmeye girilmesi veya uygulanması için gerekli olması; (b) kararın veri sorumlusunun tabi olduğu Birlik veya Üye Devlet yasaları tarafından yetkilendirilmesi ve veri konusunun hak ve özgürlüklerini ve meşru çıkarlarını korumak için uygun tedbirler getirmesi ve (c) kararın ilgili kişinin açık rızasına dayanması hallerinde, m.22/1 geçerli olmayacaktır. GDPR m.22/3'e göre ise GDPR m.22'nin 2. fıkrasının (a) ve (c) bentlerinde belirtilen durumlarda, veri sorumlusu, ilgili kişinin hak ve özgürlüklerini ve meşru menfaatlerini, en azından bu konuda insan müdahalesi alma hakkını korumak için, ilgili kişinin bakış açısını ifade

(kredi alımı ve işe kabul gibi) sınırlı tutulduğu görülmektedir. Bu noktada ise GDPR'nin gerek 71. paragrafında gerekse "Definitions" (Tanımlar) başlıklı 4. maddesinin 4. fıkrasında geçen "profilleme"nin (profiling) tanımı yardımcı olacaktır: İlgili tanıma göre profilleme veya profil oluşturma; bir gerçek kişiyle ilgili belirli kişisel yönleri değerlendirmek için kişisel verilerin kullanılmasından oluşan, **özellikle o gerçek insanın işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirlik, davranış, konum veya hareketlerle ilgili yönleri analiz etmek veya tahmin etmek için kullanılan**, kişisel verilerin otomatik olarak işlenmesi anlamına gelmektedir. Dolayısıyla profillemeye kullanılan ve "benzer önemli etkiler" yaratan uygulamaların bir kısmının "özel nitelikli veriler"in tahmin edilmesinde kullanıldığı, yani profilleme işlemi ile amaçlanan şeyin aslında kişiyi önemli düzeyde etkileyebilecek "özel nitelikli verilerini" dolaylı yoldan toplama işlemi olduğu düşünülebilir. Bu bağlamda "benzer önemli etkiler" yaratan uygulamaların kişinin özel nitelikli verilerini ve GDPR'nin 71. paragrafında geçen diğer önemli verilerini tahmin etmeye yönelik uygulamalar olarak değerlendirilmesinin isabetli olacağı kanaatindeyiz. Çeşitli kuruluşları bu tür otomatik karar mekanizması uygulamalarını kullanmaya iten ana neden özel nitelikli kişisel veriler için açık rıza gerekmesi ve kişilerin böyle bir rızayı vermeye gönüllü olmayacaklarını düşünerek bu verileri başka yollarla (otomatik karar alan mekanizmalar sayesinde ÖNKV işlemeyen de ÖNKV verisi üretme) elde etmeye çalışmalarıdır. Örneğin kişinin Facebook beğenmelerinden (like'larından) cinsel yöneliminin, ırkının, dini görüşünün, psikolojik durumunun veya politik görüşünün tespit edilebilmesi gibi durumlar bu uygulamaların bir sonucudur. GDPR'nin 71. paragrafında geçen verilerin GDPR'nin 9. maddesinde geçen **ırksal veya etnik kökene işaret eden kişisel veriler, siyasal görüşleri ortaya koyan kişisel veriler, dini veya felsefi inançları açığa çıkaran kişisel veriler, sendika üyeliğini ortaya koyan kişisel veriler, genetik veriler, biyometrik veriler (tanımlama amacıyla kullanıldığı yerlerde), sağlıkla ilgili veriler, bir kişinin cinsel yaşamına ilişkin veriler ve bir kişinin cinsel yönelimi ile ilgili veriler gibi özel nitelikli veriler** (bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, Article 9) ve 6698 sayılı KVKK'nın 6.maddesinin 1. fıkrasında geçen; **ırk, etnik köken, siyasi görüşler, dini ve felsefi inançlar, mezhep ya da diğer inançlar, giyim tarzı, bir derneğe, vakıfa veya sendikaya üyelik durumu, sağlık, cinsel hayat, herhangi bir cezadan mahkûmiyet yaşayıp yaşamadığı ve güvenlik tedbirleri ile ilgili verilerin yanı sıra genetik ve biyometrik veriler** gibi özel nitelikli kişisel veriler (bkz. KVKK, m.6) doğrultusunda genişletilmesi gerektiğini düşünmekteyiz. Ayrıca kişiyi önemli düzeyde etkileyebilecek diğer konuların da dahil edilmesi gerekmektedir. Örneğin bir araç sigorta şirketi eğer müşterilerinin dikkatsiz araç kullanması halinde bir sonraki dönemde primlerini artıracaksa araçlarına yerleştirdiği bir takip cihazıyla bunu önceden bildirmelidir. Yine de doktrinde bu konuda yapılan tartışmaların son bulabilmesi için gerek GDPR'de gerekse 6698 sayılı KVKK'da bu "benzeri önemli etkiler"in (*similarly significantly affects*) kıyas yoluyla genişletilemeyecek şekilde tanımlanması gerekmektedir.

ve karara itiraz etmek için ‘uygun tedbirler’³¹³ almalıdır. GDPR m.22/4’e göre ise GDPR m.22/2’de atıfta bulunulan kararlar, m.9/2 ‘nin (a) veya (g) noktalarının uygulanmadığı ve ilgili kişinin hak ve özgürlükleri ile meşru çıkarlarının korunması için uygun tedbirler söz konusu olmadığı sürece, m.9/1’de belirtilen özel nitelikli kişisel verilere dayandırılmayacaktır.³¹⁴ GDPR’nin 9. maddesinde ırksal veya etnik kökene işaret eden kişisel veriler, siyasal görüşleri ortaya koyan kişisel veriler, dini veya felsefi inançları açığa çıkaran kişisel veriler, sendika üyeliğini ortaya koyan kişisel veriler, genetik veriler, biyometrik veriler (tanımlama amacıyla kullanıldığı yerlerde), sağlıkla ilgili veriler, bir kişinin cinsel yaşamına ilişkin veriler ve bir kişinin cinsel yönelimi ile ilgili veriler “özel nitelikli veriler” olarak kabul edilmiştir³¹⁵. 6698 sayılı KVKK’nın 6.maddesinin I. fıkrasında ise ırk, etnik köken, siyasi görüşler, dini ve felsefi inançlar, mezhep ya da diğer inançlar, giyim tarzı, bir derneğe, vakıfa veya sendikaya üyelik durumu, sağlık, cinsel hayat, herhangi bir cezadan mahkûmiyet yaşayıp yaşamadığı ve güvenlik tedbirleri ile ilgili verilerin yanı sıra genetik ve biyometrik veriler, “özel nitelikli kişisel veriler” arasında sıralanmıştır³¹⁶.

GDPR’nin 22. maddesine göre ilgili kişiler kendilerinin önemli gördüğü değil, kendileri ile ilgili hukuki sonuçlar doğuran veya benzer önemli etkiler üreten kararlar kararlara tabi olmama hakkına sahiptir. Bunun dayanağı yoksunluk ilkesidir (Deprivation principle). Kişi cezalandırıldığı veya bir haktan mahrum kaldığı durumlarda, kararın gerekçesini öğrenme hakkına sahiptir³¹⁷. Kişilerin kendi iradesi dışında hukuki düzenlemelerin mecbur bırakmasıyla maruz kaldığı ve etkilediği sonuçlarda gerekçesini öğrenme hakkı vardır³¹⁸. Hukukun üstünlüğü ilkesinin gereği olarak (rule of law) kamu yaptığı işlemlerin hukuka uygun olmasını sağlayabilmek için aldığı kararları gerekçe ilkesi kapsamında izah etmelidir. İşlemlere muhatap

³¹³ GDPR m.22/3’te “uygun tedbirler” tabiri “*suitable measures*” olarak geçmektedir. Bunlara örnek olarak Bölüm 3.2’de ele aldığımız idari tedbirler arasından kişisel veri etki analizi, tasarımdan itibaren kişisel verilerin korunması ve veri koruma görevlisi gösterilebilir.

³¹⁴ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 22**, p.46.

³¹⁵ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 9**, pp.38-39.

³¹⁶ KVKK, m.6.

³¹⁷ Göktürk, **A.g.e.**

³¹⁸ M. Nedim Bekri, “Gerekçeli Karar Hakkı”, **Ankara Barosu Dergileri**, Cilt.72, Sayı.3, 2014, ss.205-228. (Online) <http://www.ankarabarusu.org.tr/siteler/ankarabarusu/tekmakale/2014-3/6.pdf> 31 Aralık 2019.

olan, hukuken veya sosyal anlamda etkilenen kişilerin açıklama talep etmesi ve bilgi sahibi olması en doğal hakkıdır.

Article 22 (3)'de düzenlenen "human-in-the-loop" şeklinde ifade edilen hak; otomatik karar alma mekanizmalarıyla alınan kararlar hakkında insan müdahalesi talep ederek (human intervention) görüşlerinin alınması ve karara karşı itiraz edilmesi şeklinde anlaşılmaktadır. Algoritmik karar alma sisteminin bilgi temin etmek veya analizler yapmak suretiyle, insanın kendi başına alacağı kararlarda destek sağladığı sürece "human-in-the-loop" denilmektedir.³¹⁹

Özet olarak, GDPR'nin 22. maddesi; kural olarak, yasal veya benzer şekilde önemli bir etkiye sahip olan profillemeye dahil olmak üzere, tamamen otomatikleştirilmiş bireysel karar verme mekanizmalarının genel olarak yasak olduğunu; bu kuralın bazı istisnaları olduğunu; bu istisnalardan birinin geçerli olduğu durumlarda, ilgili kişinin hak ve özgürlüklerini ve meşru çıkarlarını korumak için tedbirler alınıyor olmasının söz konusu olması gerektiğini belirtmektedir³²⁰. Diğer yandan kararın tamamen otomatik karar alma mekanizmalarıyla alınmış olduğu gerçeğini değiştirmeyecek durumlar söz konusudur. Bunlar; otomatikleştirilmiş bireysel karar verme mekanizmalarına insan müdahalesi eklenmesi, kararın tamamen bir algoritma tarafından belirli kriterlere dayalı olarak alınması, algoritmanın değerlendirdiği kriterler dışında başka kriterleri de değerlendirmeden algoritma kararını bir insanın onaylaması, insan etkisinin işlevsel ve/veya anlamlı düzeyde olmaması gibi durumlardır. Bu durumlar veri sorumlusunun bu konudaki yükümlülüklerini ya da ilgili kişinin bu konudaki haklarını ortadan kaldırmayacaktır³²¹.

GDPR'nin 71. paragrafına göre çevrimiçi bir kredi başvurusunun otomatik olarak reddedilmesi veya herhangi bir insan müdahalesi olmadan e-işe alım gibi uygulamalar tamamen otomatik işlemeye dayanmaktadır. İlgili paragrafta bu uygulamalar, ilgili kişi üzerinde yasal etkiler yaratan veya önemli etkiler yaratma ihtimali olan, kişiyle ilgili kişisel yönleri değerlendiren profillemeye gibi karar mekanizmalarını da içine alan faaliyetlere örnek olarak gösterilmiştir.

³¹⁹ Goldenfein, *Ibid.*

³²⁰ Article 29 Data Protection Working Party, "Guidelines on Automated...", p.19.

³²¹ Aşıkoglu, *a.g.e.*, s.144; Article 29 Data Protection Working Party, "Guidelines on Automated...", p.20.

Ayrıca GDPR par.71’de ilgili kişinin kendisi hakkında alınan bu tür otomatik kararlara tabi olmama, reddetme/itiraz etme hakkına sahip olması gerektiğinden de bahsedilmektedir³²². İlgili paragrafın bir diğer önemli ifadesi de 4. cümlede geçmektedir. İlgili cümle; “her halükârda bu tür bir işlemin (profilleme de dahil otomatik karar alma mekanizmalarıyla yapılan veri işleminin), ilgili kişiye özgü bilgileri ve insan müdahalesi alma hakkını, görüşünü ifade etme, bu değerlendirmeden sonra alınan kararın bir açıklamasını elde etme ve karara itiraz etme hakkını içermesi gereken uygun tedbirlere tabi olması gerektiği”nden bahsetmektedir. Bu cümlede geçen ifade GDPR’nin 22. maddesinin 3. fıkrasındaki ifadeye oldukça benzerdir.

GDPR m.22/3’te; “aynı maddenin 2. fıkrasının (a) ve (c) bentlerinde belirtilen durumlarda, veri sorumlusunun, ilgili kişinin hak ve özgürlüklerini ve meşru menfaatlerini, en azından bu konuda insan müdahalesi alma hakkını korumak için, ilgili kişinin bakış açısını ifade ve karara itiraz etmek için uygun tedbirler alması gerektiği”nden bahsetmektedir.

GDPR par.71’in 6. cümlesinde ise kişisel verilerin işlendiği belirli koşullar ve bağlam dikkate alınarak, ilgili kişiye ilişkin adil ve şeffaf bir işlem yapılmasını sağlamak için, veri sorumlusunun profil oluşturma için uygun matematiksel veya istatistiksel prosedürleri kullanması, uygun teknik³²³ ve idari tedbirleri uygulaması gerektiği belirtilmiştir. İlgili cümlede bu tedbirlerin ayrıca özellikle kişisel verilerde yanlışlıklara neden olan faktörlerin düzeltilmesini ve hata riskinin en aza indirilmesini sağlamaya, kişisel verileri, ilgili kişinin menfaatleri ve hakları için potansiyel riskleri dikkate alacak şekilde güvence altına almaya yönelik olması gerektiği ve ırksal veya etnik köken, siyasi görüş, din veya inançlar, sendika üyeliği, genetik veya sağlık durumu veya cinsel yönelim gibi özel nitelikli kişisel verilerin temelinde gerçek kişiler üzerindeki ayrımcı etkileri önlemesi veya böyle bir etkiye sahip tedbirler olması gerektiği belirtilmiştir.

³²² Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, par.71.**

³²³ Hataları minimize etmek için gerekli teknik tedbirlere örnek olarak Bölüm 3.2.1.2’de ele alınan eğitim verisinin minimizasyonuna gerek duyulmadan alınabilecek tedbirler arasından “Differential Privacy” konseptiyle kişisel verilerin korunmasını sağlayan algoritmalara ve veri korumayı otomatize eden uygulamalara (*PET - Privacy Enhanced Technologies*), ayrımcılık etkilerini azaltacak tedbirlere örnek olarak ise Bölüm 2.4.2.3’e (Algoritmik Ayrımcılık) bakılabilir.

GDPR par.71'in doğrudan özel nitelikli kişisel verilerin işlenmesiyle elde edilen profillemelerden kaynaklı ayrımcılığı belirtmesi önemlidir. Ancak algoritmik modelden özel nitelikteki kişisel veri kategorilerinin silinmesinin ardından yapılan tahminlemelerde, veri setinden çıkarılan değişkenlerin de değerlendirmeye alınmadığından emin olunamamaktadır. Veri setinin başlangıcında özel nitelikli kişisel veriler bulunmasa dahi sonradan yapılan analizlerle artık özel nitelikli kişisel veriler farklı kategorideki genel nitelikteki kişisel verilerin eşleştirilmesiyle de elde edilmektedir. Hassas veri kategorisinde olmayan coğrafi bilgi ile kredi değerlendirmesi yapıldığında kişilerin ırklarına ilişkin tahminler yapıldığı görülmektedir³²⁴. Ayrıca IP adres, satın alma geçmişi özel nitelikli olmayan kişisel verilerden kişilerin sağlık durumlarına ilişkin sonuçlar çıkarılabilmektedir³²⁵.

GDPR par.71'de ifade edilen uygun teknik ve idari tedbirlerden bazıları; ilgili kişilerin hakkaniyetli ve ayrımcı olmayan şekilde muameleye tabi tutulduğundan emin olunması için düzenli kalite kontrolleri süreçleri, algoritmik denetim, bağımsız denetim, veri minimizasyonu, net saklama sürelerinin belirlenmesi, "takma adlandırma" (pseudonymisation), sertifikasyon mekanizmaları, etik değerlendirme kurullarıdır³²⁶.

GDPR'nin 71. paragrafında geçen kararın açıklamasını talep etme hakkının varlığına ilişkin doktrinde çeşitli görüş farklılıkları bulunmaktadır. Bryce Goodman ve Seth Flaxman tarafından kaleme alınan yazı³²⁷, GDPR'ın açıklama talep etme hakkını oluşturduğundan öte detaya girmeyen konuya ilişkin ilk makale olmuştur. İkinci olarak böyle bir hakkın bulunmadığına ilişkin Sandra Wachter, Brent Mittelstadt ve Luciano Floridi'den bir makale³²⁸ gelmiştir. Son olarak da Andrew D.

³²⁴ Matthias Leese, "The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union", **Security Dialogue**, Vol.45, No.5, 2014, pp.494-511.

³²⁵ David Robinson Harlan Yu Aaron Rieke, "Civil Rights, Big Data, and Our Algorithmic Future". **Social Justice and Technology**, September 2014. (Online) https://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf 31 December 2019.

³²⁶ Article 29 Data Protection Working Party, **Ibid.**, p.32.

³²⁷ Goodman / Flaxman, **Ibid.**

³²⁸ Sandra Wachter, Brent Mittelstadt, Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", **International Data Privacy Law**, Vol.7, No.2, 2017, pp.76-99.

Selbst ile Julia Powles tarafından kaleme alınan makale³²⁹ açıklama talep etme hakkının bulunduğunu desteklemiştir. Söz konusu bilginin ne anlam ifade ettiğine ilişkin, pratik hayatta sistemin geneli hakkında mı veya belirli bir bireysel karara ilişkin mi olacağı ve hangi derinlikte açıklamanın gerekli olacağına ilişkin tartışmalar sürmektedir³³⁰.

FAT/ML tarafından da hesap verebilir bir algoritmik sistemin açıklanabilir olması gerektiği belirtilmiştir. Açıklanabilir olma ilkesi;

1. Hangi tipte bir son kullanıcıya veya paydaşlara açıklamayı yapacağının belirlenmesini,
2. Algoritmanın veya sistemin ilişkin hangi seviyede ve detayda son kullanıcıya veya paydaşlara açıklanacağını belirlenmesini,
3. Veri kaynaklarının ne kadarının açıklanacağını belirlenmesini

gerektirmektedir. Eğer makine öğrenimi modelleri kullanılan bir YZ sistemi ise;

1. Doğrudan yorumlanabilir veya açıklanabilir model kullanılmasının değerlendirilmesi,
2. Eğitim verilerinin nasıl, ne zaman ve neden tercih edildiğine ilişkin gerekçelerinin hazırlanması

tavsiye edilmektedir³³¹.

Bir kararın alınması sürecinin tamamen otonom bir şekilde olup olmadığı tespit edilirken karşılaşılan bazı güçlükler dile getirilmektedir. Veriyi işleme sürecinin herhangi bir aşamasında insan karar vericinin bulunması kararın tamamen otonom

³²⁹ Andrew Selbst, Julia Powles, "Meaningful information and the right to explanation", **International Data Privacy Law**, Vol.7, No.4, November 2017, pp.233–242.

³³⁰ Gianclaudio Malgieri, Giovanni Comandé, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", **International Data Privacy Law**, Vol.7, No.3, 2017, pp.243-265, (Çevrimiçi) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3088976_code2392402.pdf?abstractid=3088976&mirid=1 8 January 2020.

³³¹ Diakopoulos / Friedler / Arenas / Barocas / Hay / Howe / Jagadish / Unsworth / Sahuguet / Venkatasubramanian / Wilson / Yu / Zevenbergen, **Ibid.**

bir şekilde alındığının kabulüne engel mi teşkil edecektir?³³² Karar alma sürecinin herhangi bir safhasında insanın bulunmasının hukuki açıdan tamamen otonom kabul edilmesinin kapsamından çıkarılması halinde, bu endişeye sebep olan bir sınırlama olarak görülecektir.

Bayamlıoğlu, GDPR madde 22 (1)'de geçen "yalnızca otomatik işleme süreçlerine dayalı alınmış kararlar"³³³ ifadesinin insanların katılım sağladığı veya parçası olduğu bazı kararları da kapsamı gerektiğini ifade etmektedir³³⁴. Ancak Alman Federal mahkemesinin 95/46 Yönergesi'nin dayalı olarak kredi skorlarına dair verdiği kararda; karar alma süreçlerine herhangi bir şekilde insan müdahalesi olması halinde düzenlemenin uygulanmayacağı hükmü geçmekteydi³³⁵. Hangi seviyeye kadar insan müdahalesinin kabul edilebilir olduğu belirsizliğini korumaktadır.

Diğer bir yönüyle de karardan etkilenen kişinin algoritmik karar alma sisteminin aldığı karara karşı nasıl bir itiraz öne sürmesinin beklendiği de henüz netlik kazanmamıştır³³⁶. Otomatik karar alma mekanizmalarının aldığı kararların hızının ve çapının artış hızı göz önüne alınırsa, belirli hallerde insan müdahalesiyle tekrardan değerlendirilmesinin ne kadar etkili bir yöntem olacağı da tartışılmaktadır.³³⁷

GDPR kapsamında müphem bir şekilde düzenlenmesi sebebiyle cevaplanma ihtiyacı bulunan sorular;

³³² Isak Mendoza, Lee A. Bygrave, "The Right Not to Be Subject to Automated Decisions Based on Profiling", EU Internet Law, **Springer, Cham**, May 8, 2017, pp.77-98 (Çevrimiçi) <https://ssrn.com/abstract=2964855> 31 December 2019.

³³³ GDPR madde 22 (1)'de "decision based solely on automated processing" şeklinde geçmektedir.

³³⁴ Emre Bayamlıoğlu, "Transparency of automated decisions in the GDPR: An attempt for systemisation", **SSRN**, January 7, 2018. (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097653 31 December 2019.

³³⁵ Alman Federal Adalet Mahkemesi'nin (Bundesgerichtshof) 2014 senesinde VI ZR 156/13 sayılı "SCHUFA" davası olarak adlandırılan otomatik kredi skorlama sistemleri hakkındaki kararı.

³³⁶ Emre Bayamlıoğlu, "Contesting Automated Decisions", European Data Protection Law Review, Vol.4, June 24, 2019, pp.433-446; Tilburg Law School Research Paper Forthcoming. **SSRN**, <https://ssrn.com/abstract=3305272> 31 December 2019.

³³⁷ Goldenfein, **Ibid**.

1. İnsan müdahalesinin otomatik karar alma sürecinin hiçbir aşamasında mı bulunmaması gerekiyor? İnsan müdahalesi hangi seviyeye kadar kabul edilebilir?
2. İlgili kişilerin kurumlara insan müdahalesi talep ederek başvururken nasıl bir gerekçe öne sürmeleri gerekiyor?
3. İnsan müdahalesi talep eden kişilere kurumlar açıklama hakkı kapsamında neleri açıklaması bekleniyor?

şeklinde sıralanabilir.

Algoritmik sistemi gözden geçirecek olan insanın aşağıdaki sayılanlar kapsamında yetkin olması gerekmektedir³³⁸.

1. YZ sisteminin nasıl çalıştığı ve limitleri,
2. Sistemin yanlış yönlendirdiğini öngörebilmek ve nedenlerini anlayabilmek,
3. Sistemin hangi sıklıkla hatalı olabileceğini göz önünde bulundurarak çıktılarına makul seviyede şüpheyile yaklaşabilmek,
4. Algoritmik sistemin çıktısını reddetmek veya kabul etmekle ilgili anlamlı açıklamalar yapabilmek,

Sistemin yorumlanabilir modelle tasarlanması, gözden geçirecek kişilerin eğitilmesi gibi tedbirlerin alınmasının ardından da sistemin aldığı kararların uzun süreli bir kontrol süreci altında tutulması, insan gözden geçiricilerin neden ve kaç defa sistemin aldığı kararları kabul ettiği veya reddettiğinin analiz edilmesi sistemin düzenleme kapsamında tamamen otomatik karar alma mekanizması olarak kabul edilip edilmeyeceğinin tespiti açısından önemli olacaktır³³⁹.

³³⁸ Reuben Binns, Valeria Gallo, "Automated Decision Making: The role of meaningful human reviews", **Information Commissioner's Office**, April 12, 2019. (Çevrimiçi) <https://ico.org.uk/about-the-ico/news-and-events/ai-blog-automated-decision-making-the-role-of-meaningful-human-reviews/> 31 December 2019.

³³⁹ Binns / Gallo, **Ibid**.

3.2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINABİLECEK TEKNİK VEYA İDARİ TEDBİRLER

6698 sayılı KVKK'nın 12. maddesinin 1. fıkrasına göre veri sorumlusunun kişisel verilere ilişkin hukuka uygun olmayacak şekilde işleme ve erişimin önlenmesi ile bu verilerin korunmasının sağlanması için gereken güvenliğin edinilmesine ilişkin tüm idari ve teknik tedbirlerin alınması yükümlülüğü bulunmaktadır.³⁴⁰

Bu bölümde, kişisel verilerin korunmasına ilişkin alınabilecek teknik veya idari tedbirler ele alınacaktır.

3.2.1. Teknik Tedbirler

Kişisel verilerin korunmasına ilişkin alınabilecek teknik tedbirler; eğitim verisinin minimizasyonuna ihtiyaç duyularak alınacak tedbirler, eğitim verisinin minimizasyonuna gerek duyulmadan alınabilecek tedbirler ve Algoritmik Sistemleri Açıklama Yöntemleri olmak üzere üç grupta incelenebilir.

3.2.1.1. Eğitim Verisinin Minimizasyonuna İhtiyaç Duyularak Alınacak Tedbirler

Veri minimizasyonu (*Data minimisation*), GDPR'nin 5/1c'de düzenlenmiştir. Bu maddeye göre kişisel verilerin işlenmesinin işlendikleri amaçla ilgili (*relevant*) olması, yeterli/ölçülü (*adequate*) ve sınırlı (*limited*) olması gerekmektedir³⁴¹. Türkiye'de ise buna karşılık gelen hükümler, 6698 sayılı KVKK m.4/2(ç)'de geçen "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"³⁴² ilkesidir. Bu ilke, ilgili kişinin

³⁴⁰ Ancak kişisel verilerin veri sorumlusu adına gerçek ya da tüzel diğer kişi ve/veya kişilerce işleniyor olması durumunda hem veri sorumlusu hem de veri sorumlusunun kendi adına verileri işlemesine izin verdiği kişi/kişiler KVKK, m.12/1'de geçen tedbirlerin alınmasından sorumlu olmaktadır (KVKK, m.12/2).

³⁴¹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 5/1(c)**, p.35.

³⁴² KVKK, **m.4/2(ç)**.

kişisel verilerinin korunması doğrultusunda asgari müdahalede bulunacak tekniğin kullanılmasını gerektirir³⁴³.

Buna göre, veri minimizasyonu ilkesi doğrultusunda YZ geliştiricileri, geliştirme sırasında kullanılan kişisel veri miktarını mümkün olduğunca en aza indirmeli ve bu tür verilerin, tanımlanan amaçlar için gerekli ve gerekli olan verilerle (örneğin eğitim verileriyle) sınırlı olmasını sağlamalıdır. Minimizasyon için anonimleştirilmiş verilerin kullanımı gibi tekniklere ek olarak, aşağıdakileri içeren, ancak bunlarla sınırlı olmayan çeşitli teknikler kullanılabilir:³⁴⁴

- a) Üretken Düşmanca Ağlar veya Çekişmeli Üretici Ağlar (GANs - *Generative Adversarial Networks*),
- b) Birleşik Makine Öğrenimi (*Federated Machine Learning*)
- c) Matris kapsülleri (*Matrix capsules*)

Türkçe literatürde Üretken Düşmanca Ağlar veya Çekişmeli Üretici Ağlar olarak anılan GAN'lar sentetik veri üretmede kullanılır. Bugün itibariyle, GAN'lar çoğunlukla görüntü üretimi için kullanılmaktadır. Bununla birlikte, diğer alanlarda çok sayıda yüksek kaliteli, sentetik eğitim verisi üretmede kullanılabilecek yöntemlere adaydır. Bu teknik sayesinde gerçek kişisel bilgiler içeren büyük miktarda veri

³⁴³ Oğuz Şimşek, "Anayasa Hukukunda Kişisel Verilerin Korunması", **Beta Basım Yayın**, İstanbul, 2008, s.99. Buna örnek olarak bir işletmede güvenlik amaçlı ve/veya çalışanların işletmeye giriş çıkışlarını kontrol amaçlı olarak parmak izleriyle girebildikleri bir sistemin kullanılması gösterilebilir. Burada bireylere verilecek basit bir giriş kartı uygulaması ile işletmeye giriş-çıkış yapabilmeleri sağlanabilecekken parmak izlerinin alınmasıyla gerçekleştirilen veri işleme faaliyeti amacını aşan ve bireylerin kişisel verilerinin korunmasına asgari düzeyin çok ötesinde müdahale eden, dolayısıyla veri minimizasyonu ilkesine ters düşen bir uygulama olacaktır. Bu tür bir uygulamanın ilgili kişinin rızası alınmış olması halinde hukuka uygun olduğu öne sürülürse de yeterlilik/ölçülülük ve sınırlılık ilkelerine aykırı olacağından hukuken uygun kabul edilmeyecektir (bkz. Hüseyin Murat Develioğlu, "6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku". **On İki Levha Yayıncılık**, İstanbul, 2017, s.47).

³⁴⁴ International Working Group (IWG), "Working Paper on Privacy and Artificial Intelligence", 29-30 November 2018, **International Working Group on Data Protection in Telecommunications**, 64th Meeting, Queenstown (New Zealand), (Çevrimiçi) <https://epic.org/IWG/WP-AI.pdf> 9 December 2019, p.15.

kullanmaya gerek kalmadan hem etiketlenmiş veri hem de büyük miktarda veri ihtiyacı karşılanabilir.³⁴⁵

Standart makine öğrenimi yaklaşımları, eğitim verilerinin bir makinede veya veri merkezinde merkezileştirilmesini gerektirir. Birleşik Makine Öğrenimi ise bu yaklaşımın bir adım ileriye taşındığı, bir tür dağıtılmış öğrenmedir. Birleşik öğrenme, merkezi bir modelin en son sürümünü bir müşteri birimine, örneğin bir cep telefonuna indirerek çalışır. Daha sonra model, yerel veriler temelinde müşteri biriminde yerel olarak geliştirilir. Modeldeki değişiklikler daha sonra sunucuya geri gönderilir ve burada diğer istemcilerdeki modellerden gelen değişiklik bilgileriyle birleştirilir. Daha sonra, merkezi modeli geliştirmede değiştirilen bilgilerin ortalaması kullanılır. Yeni, geliştirilmiş merkezi model artık tüm müşteriler tarafından indirilebilir. Bu, mevcut bir modeli, çok sayıda kullanıcı temelinde, kullanıcıların verilerini paylaşmak zorunda kalmadan geliştirme fırsatı sunar.³⁴⁶

Matris kapsülleri ise sinir ağlarının yeni bir varyantıdır ve öğrenme için mevcut derin öğrenme normundan daha az veri gerektirir. Çıktıları aynı varlığın farklı özelliklerini temsil eden bir grup nöron olan kapsüllerin kullanıldığı bu teknik, makine öğrenimi için çok daha az veri gerektirmesi bakımından büyük bir avantaj sunmaktadır.³⁴⁷

3.2.1.2. Eğitim Verisinin Minimizasyonuna Gerek Duyulmadan Alınabilecek Tedbirler

Eğitim verisinin minimizasyonuna gerek duyulmadan alınabilecek tedbirler, aşağıdaki teknikleri içeren ancak bunlarla sınırlı olmayan tedbirleri içerir:

³⁴⁵ Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio, “Generative Adversarial Nets”, Département d’informatique et de recherche opérationnelle **Université de Montréal**, France, 2014, (Çevrimiçi) <https://papers.nips.cc/paper/5423-generative-adversarial-nets.pdf> 10 December 2019, pp.1-3.

³⁴⁶ McMahan Brendan & Daniel Ramage, “Federated Learning: Collaborative Machine Learning without Centralized Training Data”, 2017, April 6, <https://ai.googleblog.com/2017/04/federated-learning-collaborative.html> 11 December 2019.

³⁴⁷ Geoffrey Hinton, Sara Sabour, Nicholas Frosst, “Matrix capsules with em routing”, Conference Paper, **ICLR 2018**, Toronto, Canada, 2018, (Çevrimiçi) <https://openreview.net/pdf?id=HJWLfGWRb> 12 December 2019, pp.1-2.

- a) Diferansiyel Gizlilik (*Differential Privacy*)
- b) Homomorfik Şifreleme (*Homomorphic Encryption*)
- c) Transfer Öğrenimi (*Transfer Learning*)
- d) Bağımsız Disklerin Yedekli Dizisi³⁴⁸ (*RAID - Redundant Array of Independent Disks*)

Diferansiyel Gizlilik, üçüncü şahısların belirlenmiş bir amaçla oluşturulmayan algoritma sonuçlarına erişerek verilere ilişkin bazı çıkarımlar yapmasına karşı titiz, istatistiksel garantiler sağlamayı amaçlayan bir araştırma alanıdır. Tanımı ilk olarak bir Microsoft Araştırmacısı olan Cynthia Dwork'un 2006 yılında yayımlanan ICALP belgesinde³⁴⁹ yapılmıştır. O zamandan beri bu terim hem teorik analiz hem de pratik örnekler açısından yapılan katkılarla giderek daha popüler bir araştırma alanı haline gelmiştir.³⁵⁰ 'Diferansiyel Gizlilik' bir tanımdır, bir algoritma değildir. Belirli bir hesapsal (*computational*) görev ve daha küçük olduğunda daha iyi kişisel veri koruması sağlayan bir parametre değeri için, hesapsal görevi diferansiyel olarak en küçük parametre değerine sahip olacak şekilde elde etmede birçok farklı özel algoritma kullanılabilir. Bu durumda da diferansiyel gizlilik için geliştirilen bazı algoritmalar diğerlerinden daha iyi doğruluğa sahip olacaktır.³⁵¹

Homomorfik şifreleme, şifre metin (şifreli düz metin) üzerinde hesaplamalar yapılabilen ve sonuçta ortaya çıkan şifre metninin şifresinin çözülmesiyle elde edilen sonucun düz metin üzerinde yapılan hesaplamaların sonucuna eşit olabildiği bir şifreleme düzenidir. Bu şifreleme düzenleri, homomorfik şifrelemenin şifrelenmiş bilgiler üzerinde işlemlerin uygulanmasına olanak tanınması nedeniyle bulut bilişim ortamlarında yaygın kullanımı konusunda gelecek vadetmektedir.³⁵² Homomorfik

³⁴⁸ Türkçe literatürde Bağımsız Disklerin Artık Dizisi, Yedekli Bağımsız Diskler Dizisi, Fazladan Bağımsız Disk Dizisi olarak da anılmaktadır.

³⁴⁹ Bkz. Cynthia Dwork, "Differential Privacy". ICALP 2006, Part II, **Springer-Verlag**, Berlin Heidelberg, 2006, pp.1–12.

³⁵⁰ Stephen Tu, "Lecture 20: Introduction to Differential Privacy", **Advanced Topics in Data Processing**, Fall 2013, (Çevrimiçi) <https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf> 15 December 2019.

³⁵¹ Cynthia Dwork, Aaron Roth, "The Algorithmic Foundations of Differential Privacy", **Foundations and Trends® in Theoretical Computer Science**, Vol.3-4, 2013. p.6. pp.1-277. (Çevrimiçi) <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf> 20 December 2019.

³⁵² Mete Akgün, A. Osman Bayrak, Buğra Özer, M. Şamil Sağıroğlu, "Privacy preserving processing of genomic data: A survey", **Journal of Biomedical Informatics**, 2015, Vol.56, p.110.

şifreleme, kişisel verilerin korunma düzeyini yükseltmektedir. Bu teknik ve herhangi bir ilgili kişinin kimliğinin ifşa olmasına yol açabilecek hassas verilere sadece süzgeçten geçirildikten sonra erişim sağlanabilmesi sayesinde kişisel verilerin korunması yeterli bir düzeye ulaşabilmektedir. Kısaca, bu teknik sayesinde yalnızca şifrelenmiş verilerle işlem yapılabilen; homomorfik işlemle elde edilen sonuçlar da veri setinin tamamı üzerinde yapılan işlemle elde edilen sonuçlarla aynı olmaktadır.³⁵³

'Transfer Öğrenimi'nde, her zaman modellerin sıfırdan geliştirilmesi gerekmez. Benzer görevleri çözen mevcut modeller kullanılabilir. Bu teknikte, çoğu zaman veri işlemenin bu mevcut modellere dayandırılarak daha az veriyle ve daha kısa sürede aynı sonucu vermesi mümkün olabilmektedir. Önceden eğitilmiş modeller içeren kütüphanelere internet üzerinden kolaylıkla erişilebilmektedir.³⁵⁴ Bu bakımdan Transfer Öğrenimi, kullanıcıların büyük veri kümeleriyle önceden örneklenmiş merkezi modellerden (öğretmen modellerinden) “öğrenerek” hızlı bir şekilde doğru derin öğrenme modelleri (öğrenci modelleri) oluşturmalarına olanak tanıyan güçlü bir yaklaşım olma özelliği taşımaktadır (Örn. Google'ın InceptionV3'ü gibi)³⁵⁵.

RAID ise verilerin tek bir mantıksal birimmiş gibi depolanabilmesi için birden çok sabit disk bağlayan veya birleştiren bir depolama teknolojisidir ve tek bir sürücü olarak işlevi görür. RAID tekniği, birlikte çalışan birden çok diskin tek bir pahalı diskten daha iyi güvenilirlik ve hız sunacağı ve aynı zamanda tek hata noktasını önleyeceği fikrinden yararlanır. Kullanım amacına bağlı olarak RAID, fiziksel sınırlamaları nedeniyle yüksek arıza oranı ve sınırlı hız dahil olmak üzere geleneksel sabit sürücülerle ilişkili birçok farklı soruna çözüm olarak kullanılır. RAID'in en

³⁵³ Arian Ajdari, Zeynep Fenerci, Yılmaz Vural, Yavuz Canbay, “Büyük Genomik Verisinin Mahremiyetinin Korunarak İşlenmesi”, **ISCTURKEY 2018**, 17-18 Ekim 2018, p.28. (Çevrimiçi) https://www.iscturkey.org/assets/files/Bildiriler_kitab%C4%B1_2018_3.pdf 17 Aralık 2019.

³⁵⁴ IWG, **Ibid.** pp.15-16.

³⁵⁵ Bolun Wang, Yuanshun Yao, Bimal Viswanath, Haitao Zheng, Ben Y. Zhao, “With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning”. **27th USENIX Security Symposium**, USENIX Association, August 15–17, 2018, Baltimore, MD, USA, pp.1281-1297. (Çevrimiçi) <https://people.cs.uchicago.edu/~ravenben/publications/pdf/transfer-learning-sec18.pdf> 26 December 2019, p.1281.

popüler olanları 1, 5 ve 10 düzeyleridir. Bunlar arasından RAID 1, genellikle çevrimiçi verileri korumanın en güvenilir ve en hızlı yolu olarak kabul edilmektedir.³⁵⁶

3.2.1.3. Algoritmik Sistemleri Açıklama Yöntemleri

Yapay zekâlı sistemlerin haksızlığa ve ayrımcılığa neden olmaması için algoritmik şeffaflığın ve hesap verilebilirliğin sağlanmasının önemine önceki bölümlerde değinmiştik. YZ sistemlerinin neden olduğu haksızlık ve ayrımcılıklara kara kutu (black box) ve opak (opaque) olma sorunları sebebiyle nelerin sebep olduğunun ve daha sebep olmadan nasıl tespit edilebileceğinin çözümüne ilişkin birçok öneri sunulmaktadır. Açıklanabilir YZ sistemlere ilişkin araştırmalar iki ana akımda gitmektedir. İlki bir YZ sisteminin geliştirilmesinden ve uygulamaya alınmasından sonra şeffaflığının sağlanmasıyla kara kutu probleminin çözülmesine odaklanmaktadır. İkinci akım makine öğrenimi yöntemlerini değiştirerek en baştan sistemin opak olmamasını sağlayarak kara kutu probleminden kaçınmayı hedeflemektedir³⁵⁷.

YZ sistemlerinin yaptığı tahminlerin arkasında mantığın izah edilebilmesi opaklık sorununa çözüm olması bekleniyor. Kullanıcıların, etkilenen 3. Kişilerin ve düzenleyici kuruluşların algoritmik karar alma sistemlerine güveninin tesisi için nasıl ve hangi kriterlere dayalı olarak karar verilebildiğinin anlaşılabilmesine ihtiyaç duyulmaktadır. YZ sisteminin yaptığı öngörüye dayalı olarak doktorun tedavi yolunu belirlemesi, hâkimin sanık hakkında cezaya hükmedebilmesi için sistemin güvenilir değerlendirmeler yaptığının bilinmesi gerekmektedir.

Basit modellerde, modelin kendisi en iyi açıklamayı sağlamaktadır. Çünkü kendisini en mükemmel şekilde temsil ediyor ve bu yüzden de anlaşılması kolay olmaktadır. Sınıflandırıcı topluluklar (ensemble methods) veya derin öğrenme yöntemlerinde anlaşılması güç olduğu için modelin kendisi kullanılamamakta, bu

³⁵⁶ ZNetLive, “How to choose the right RAID for your Dedicated Server”, 2016, pp.1-6. (Çevrimiçi)

https://www.znetlive.com/pdf/How_to_choose_the_right_RAID_for_your_Dedicated_Server.pdf 27 December 2019.

³⁵⁷ Doran / Schulz / Besold, *Ibid.*

yüzden orijinal modele yakın yorumlanabilir olan açıklama modellerinin kullanılması gerekmektedir.³⁵⁸

ICO algoritmik sistemin açıklanabilirliğinin ölçülebilmesi için sorulabilecek soruları aşağıdaki şekilde sıralamıştır³⁵⁹:

1. Farklı bir girdi sağladığında sistemin çıktısının nasıl değişeceğini insan gözden geçirici öngörebiliyor mu?
2. Belirli bir çıktıya katkı sağlayan en önemli girdiyi insan tespit edebiliyor mu?
3. Çıktının yanlış olabileceğini insanlar tespit edebiliyor mu?

Herhangi bir sınıflandırmaya ilişkin tahminin (prediction) veya modelin güvenilir bir şekilde açıklanmasını sağlayan algoritma olan LIME (Local Interpretable Model-Agnostic Explanations), algoritmik sistemleri açıklama yöntemlerinden birisidir. Bu metot modelin genelinden ziyade belirli bir çıktının açıklamasının yapılmasını sağlamaktadır. Bir tahmindeki girdi ve çıktı arasındaki ilişkilerin özetlenmesinin yanında, LIME hataların tespit edilmesine de yardımcı olmaktadır. Algoritmik modele duyulacak güvenin sağlanması, modelin ne yaptığı hakkında bilgi sahibi olunması ve modelin geliştirilmesi ve hatalarının çözülmesi için bir öneri olarak LIME yöntemi sunulmadır.³⁶⁰

Kodun içeriğine ilişkin bir bilgi sahibi olunmadan yapılan analizlere dayalı olarak açıklama yapılan LIME yöntemi, kara kutu yaklaşımlarından (black box approach) birisidir³⁶¹. Bu yaklaşım içerisindeki diğer açıklama sistemleri; TREPAN³⁶², Anchor³⁶³, çevrimiçi reklamlara ilişkin profillemeye ve mikro hedeflemeleri

³⁵⁸ Scott M. Lundberg, Su-In Lee, "A unified approach to interpreting model predictions", **Advances in Neural Information Processing Systems**, 2017, p.2, (Çevrimiçi) <http://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions.pdf> 31 December 2019.

³⁵⁹ Binns / Gallo, **Ibid.**

³⁶⁰ Marco Tulio Ribeiro, Sameer Singh, Carlos Guestrin, "Why should i trust you?: Explaining the predictions of any classifier." Conference paper. **The 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, August 9, 2016. (Çevrimiçi) <https://arxiv.org/abs/1602.04938> 31 December 2019.

³⁶¹ EPRS, "**Understanding Algorithmic Decision-Making...**".

³⁶² Mark Craven, Jude W. Shavlik, "Extracting tree-structured representations of trained networks", Conference paper, **Conference on Advances in Neural Information Processing Systems**, 1996.

analiz eden AdFischer³⁶⁴, sağlık, dini inanç ve cinsel yönelime ilişkin hedeflemeleri belirlemede kullanılan Sunlight³⁶⁵ ve modelden bağımsız özellikle sınıflandırıcı toplumlar yöntemleri için kullanılan SHAP³⁶⁶ olarak sayılabilir.

Algoritmik sistemlerin şeffaflığının sağlanabilmesi için açıklama yöntemlerinden olan “Quantitative Input Influence” (QII) metodu girdilerin belirli bir sonuç veya sistemin davranışı üzerindeki etkisini analiz etmektedir. Belirli kişiye veya gruba ilişkin kararın açıklamasının da yapılabildiği iddia edilmektedir.³⁶⁷

Algoritmik modellerin açıklanabilirliği arttıkça isabet oranı düşmektedir. Çünkü modelin daha isabetli (accurate) olabilmesi için daha fazla karar ağaçları eklenmekte (decision trees) bu durumda da sistemin nasıl karar aldığı anlaşılamamaktadır³⁶⁸.

Harvard Üniversitesinden araştırmacılar LIME ve SHAP teknikleriyle açıklanan algoritmaların nasıl manipüle edilip bir manada hacklenebileceği tehlikesini ortaya koydu. Bu durum da Algoritmik modellere ve açıklama yöntemlerine duyulan güveni sarsabilir.³⁶⁹

Yukarıda değinildiği üzere YZ sistemlerin şeffaflığını sağlama amacıyla algoritmalara ilişkin bilgilerin açıklanmasının sistemleri saldırılara karşı daha savunmasız hale getirebileceğini ifade etmiştik. Veri sorumluları yasal yükümlülükleri

³⁶³ Marco Tulio Ribeiro, Sameer Singh, Carlos Guestrin, “Anchors: high precision model-agnostic explanations”, Conference paper, **Thirty second AAAI Conference on Artificial Intelligence**, 2018.

³⁶⁴ Amit Datta, Michael Carl Tschantz, Anupam Datta, “Automated experiments on ad privacy settings; a tale of opacity, choice, and discrimination”, Conference paper, **Conference on Privacy Enhancing Technologies**, 2015, pp.92-112.

³⁶⁵ Mathias Lecuyer, Riley Spahn Yannis Spiliopoulos, Augustin Chaintreau, Roxana Geambasu, Daniel Hsu, “Sunlight: Fine-grained targeting detection at scale with statistical confidence”, Conference paper, **Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security**, 2015.

³⁶⁶ “Shapley Additive explanations” (bkz. Lundberg / Lee, *Ibid.*, p.2.

³⁶⁷ Anupam Datta, Shayak Sen, Yair Zick, “Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems”, **IEEE symposium on security and privacy**, 2016. (Çevrimiçi) <https://www.andrew.cmu.edu/user/danupam/datta-sen-zick-oakland16.pdf> 31 December 2019.

³⁶⁸ Ribeiro / Singh / Guestrin, “**Why should i...**”.

³⁶⁹ Dylan Slack, Sophie Hilgard, Emily Jia, Sameer Singh, Himabindu Lakkaraju, “How can we fool LIME and SHAP? Adversarial Attacks on Post hoc Explanation Methods”, November 6, 2019. (Çevrimiçi) <https://arxiv.org/abs/1911.02508> 31 December 2019.

kapsamında ilgili kişilere veya herhangi bir 3. kişiye karşı açıklamada bulunmadan önce, açıklama yöntemlerinin hassas verileri sızdırma durumlarını değerlendirmeli ve ileride oluşabilecek veri güvenliğine ilişkin riskleri tespit etmelidir³⁷⁰. California'daki Berkeley Üniversitesi'ndeki araştırmacılar sisteme ilişkin açıklama yapılması sonucunda bir manada tüm algoritmanın çalınmasının mümkün olduğunu ortaya koymuştur. Kurumların makine öğrenimi modellerini gizli tutmak istemesinin birçok sebebi olabilmektedir. Ürünün veya hizmetin rekabet avantajının korunması bir yönü ancak modelin nasıl çalıştığının öğrenilmesi halinde oyuna gelmesi de mümkün olacaktır ve yapacağı tahminlerde hatalar ve isabetsizlikler görülecektir. Daha da önemli olan hususun modelin hassas verileri sızdırmasını sağlayacak saldırı yöntemleriyle karşı karşıya olabileceği üzerinde durulan konu olmuştur.³⁷¹

YZ sisteminin modeline ilişkin açıklamanın algoritmaya ilişkin gereğinden fazla bilgi vermesi oranında kötü niyetli kişiler daha fazla zarara neden olabilecektir. Sistemin iç yapısındaki çalışmanın açıklanmasının bilgi, siber veya veri güvenliği açısından risklerinin ve kurumların sorumlu tutulacakları yönlerinin hesaba katılması gerekmektedir.³⁷²

Algoritmik ayrımcılığın takibi, anlaşılması ve düzeltilmesi için ayrımcılığa duyarlı veri madenciliği alanı gelişmektedir. Ayrımcılığa duyarlı veri madenciliği yöntemlerinde; doğrudan ayrımcılığa sebep olacak kararları önlemede sınırlama odaklı (constraint-oriented) yöntemlerin, ayrımcılığa sebep olacak kararları

³⁷⁰ Reza Shokri, Martin Strobel, Yair Zick, "Privacy Risks of Explaining Machine Learning Models", arXiv preprint, December 4, 2019. (Çevrimiçi) <https://arxiv.org/abs/1907.00164> 31 December 2019.

³⁷¹ Smitha Milli, Ludwig Schmidt, Anca D. Dragan, Moritz Hardt, "Model reconstruction from model explanations." Conference paper, **The Conference on Fairness, Accountability, and Transparency (ACM)**, 2019. (Çevrimiçi) <https://arxiv.org/pdf/1807.05185.pdf> 31 December 2019.

³⁷² YZ sistemlerinin modellerinin veya algoritmalarının çalınmasına ilişkin daha detaylı bilgi için bkz. Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter, Thomas Ristenpart, "Stealing machine learning models via prediction apis", 25th USENIX Security Symposium, 2016. (Çevrimiçi) <https://arxiv.org/pdf/1609.02943.pdf> 31 December 2019; YZ sistemindeki yapılan tahminlemelerde kullanılan gizli kalması gereken değişkenlerin elde edilmesini sağlayan saldırı çeşitleri de bulunmuştur. Makine öğrenimi modelinin adına ve erişimine ulaşılmasıyla yüz tanıma teknolojilerinin içeriğinde saklanan kişilerin yüzlerine ilişkin fotoğraflar elde edilebilmektedir. Detaylı bilgi için bkz. Matt Fredrikson, Somesh Jha, Thomas Ristenpart, "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures", Conference paper, **22nd ACM SIGSAC Conference on Computer and Communications Security**, 2015. (Çevrimiçi) <https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf> 31 December 2019.

gözlemleyip ve takip etmekte kullanıcılara keşfedici (exploratory) yöntemlerin daha uygun olduğu sonucunu elde eden araştırmalar bulunmaktadır. Bu yöntemlerin de şeffaflığı ve hesap verilebilirliği artırmada bir araç olarak kullanılabileceği ifade edilmektedir³⁷³.

3.2.2. İdari Tedbirler

Bu bölümde, kişisel verilerin korunmasına ilişkin alınabilecek idari tedbirler; (1) veri koruma etki değerlendirmesi, (2) ihlali riskinin yüksek olması hâlinde bu riskin kişisel verileri koruma kurumuna ve ilgili kişiye bildirimde bulunma zorunluluğu, (3) tasarımdan itibaren kişisel verilerin korunması ve (4) veri koruma görevlisi olmak üzere dört başlık altında incelenecektir.

3.2.2.1. Veri Koruma Etki Değerlendirmesi

KVKK ve GDPR kapsamında hesap verilebilirlik çok önemli bir ilke ve diğer ilkelere uyumun ispatlanması anlamını taşıması sebebiyle de öne çıkan bir gerekliliktir. Algoritmik karar alma sistemlerindeki risklerin değerlendirildiğinin, GDPR kapsamında uyumun sağlanması için gerekli tedbirlerin alındığının ortaya koyulabilmesi için hesap verilebilirlik araçlarının kullanılmasına ihtiyaç duyulmaktadır³⁷⁴. YZ tabanlı sistemler ve hizmetlerin, yaşam döngüsünün uygun aşamalarında (örneğin geliştirme, uygulama, hizmetten çıkarma) bir gizlilik etki değerlendirmesine ve bir risk analizine tabi tutulması, bu analizler sırasında belirlenen gerekli teknik ve idari önlemlerin uygulanması gerekmektedir³⁷⁵. İşte bu noktada da Veri Koruma Etki Değerlendirmesi (VKED) (*DPIA - Data Protection Impact Assessment*) ile sürecin, hizmetin veya algoritmanın özel hayatın gizliliğini ihlal edip etmediğinin tespiti, ne gibi önlemler ve tedbirler alınabileceği, veri işleme faaliyeti başlamadan önce kurumlar tarafından değerlendirilmiş olmaktadır.

³⁷³ Bettina Berendt, Sören Preibusch, "Better decision support through exploratory discrimination-aware data mining: foundations and empirical evidence", **Artificial Intelligence and Law**, Vol.22, No.2, 2014, pp.175-209.

³⁷⁴ Article 29 Data Protection Working Party, "Guidelines on Automated...", p.29.

³⁷⁵ IWG, *Ibid.* p.14.

En basit tanımıyla, bir proje veya değişikliğin veri koruma risklerini tanımlamada ve en aza indirmede kullanılan bir süreçtir³⁷⁶. 6698 sayılı KVKK'da VKED'e ilişkin bir düzenleme bulunmamaktadır. Diğer yandan, GDPR'de bu konu, Üçüncü Bölümde yer alan "*Data protection impact assessment*" başlıklı 35. maddede³⁷⁷ kapsamlı olarak (11 fıkra altında) düzenlenmiştir. GDPR m.35/1'e göre; özellikle yeni teknolojiler kullanarak ve işlemin niteliği, kapsamı, içeriği ve amaçları göz önünde bulundurularak bir tür işlemin gerçek kişilerin hak ve özgürlükleri için yüksek bir riskle sonuçlanması halinde, veri sorumlusu, işlem öncesinde öngörülen veri işleme operasyonlarının kişisel verilerin korunması üzerindeki etkisinin bir değerlendirmesini yapar. Benzer yüksek riskler sunan bir dizi benzer veri işleme faaliyetine yönelik olarak tek bir değerlendirme yapılabilir. GDPR m.35/2'ye göre; veri sorumlusunun, bir veri koruma etki değerlendirmesi yaparken, belirtilen durumlarda veri koruma görevlisinin tavsiyesini alması gerekir. GDPR m.35/3'e göre; özellikle aşağıdaki üç temel durumda m.35/1'de atıfta bulunulan bir veri koruma etki değerlendirmesi gereklidir:

- a) Gerçek kişilerle ilgili, profillemeye de dahil olmak üzere otomatik işlemeye dayanan ve gerçek kişiye ilişkin yasal etkiler üreten veya gerçek kişiyi benzer şekilde önemli ölçüde etkileyen kararların dayandığı kişisel yönlerin sistematik ve kapsamlı bir değerlendirmesi,
- b) Özel nitelikli verilerin (m.9/1'de atıfta bulunulan veri kategorisinin³⁷⁸ veya m.10'da atıfta bulunulan cezai hüküm ve suçlarla ilgili kişisel veri kategorisinin³⁷⁹) büyük bir ölçekte işlenmesi,

³⁷⁶ İngiltere Ulusal Sağlık Servisi (NHS – National Health Service), "Data Protection Impact Assessment (DPIA) Procedure", 2018, November 7. Ref: IT-0030-001-v1, (Çevrimiçi) <https://www.tewv.nhs.uk/content/uploads/2018/12/Data-Protection-Impact-Assessment-DPIA-Procedure.pdf> 14 December 2019, pp.3.-4

³⁷⁷ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 35**, pp.53-54.

³⁷⁸ GDPR, m.9/1'e göre; Irksal veya etnik kökene işaret eden kişisel veriler, siyasi görüşleri ortaya koyan kişisel veriler, dini veya felsefi inançları açığa çıkaran kişisel veriler, sendika üyeliğini ortaya koyan kişisel veriler, genetik veriler, biyometrik veriler (tanımlama amacıyla kullanıldığı yerlerde), sağlıkla ilgili veriler, bir kişinin cinsel yaşamına ilişkin veriler ve bir kişinin cinsel yönelimi ile ilgili veriler, "özel nitelikli veriler" olarak kabul edilmiştir (bkz. Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, Article 9, pp.38-39).

³⁷⁹ GDPR, m.10'a göre; cezai hüküm ve suçlarla ilgili kişisel verilerin işlenmesi veya m.6/1 uyarınca ilgili güvenlik önlemlerinin alınması yalnızca resmi makamın kontrolü altında veya verilerin işlenmesi, ilgili kişilerin hak ve özgürlükleri için uygun güvenceler sağlayan Birlik veya Üye Devlet yasaları tarafından onaylandığında gerçekleştirilmelidir. Herhangi bir kapsamlı cezai mahkûmiyet kaydı sadece resmi makamın kontrolü altında tutulmalıdır (bkz.

c) Halka açık bir alanın büyük ölçekte sistematik olarak izlenmesi.

GDPR'ye göre veri koruma otoriteleri, m.35/1 uyarınca veri koruma etkisi değerlendirmesi gerekliliğine tabi olan işlem türlerinin bir listesini oluşturmalı ve halka açıklamalı; bu listeleri m.68'de atıfta bulunulan Kurula bildirmelidir (GDPR m.35/4). Veri koruma otoriteleri ayrıca, veri koruma etkisi değerlendirmesinin gerekli olmadığı türden işlemlerin bir listesini oluşturabilir ve halka açıklayabilir. Bu durumda da veri koruma otoritelerinin bu listeleri de Kurula bildirmesi gerekmektedir (GDPR m.35/5). Yetkili veri koruma otoritesi, m.4. ve m.5'te atıfta bulunulan listelerin kabul edilmesinden önce, m.63'te atıfta bulunulan (bu tür listelerin ilgili kişilere mal veya hizmet sunulması veya çeşitli Üye Devletlerde davranışlarının izlenmesi ile ilgili olan veya Birlik içindeki kişisel verilerin serbest dolaşımını önemli ölçüde etkileyebilecek işlem faaliyetlerini içerdiği) tutarlılık mekanizmasını uygulamalıdır (GDPR m.35/6). GDPR m.35/7'ye göre; yapılacak değerlendirme en azından şunları içermelidir:

- (a) Öngörülen veri işleme operasyonlarının ve uygun olduğu hallerde veri sorumlusu tarafından izlenen meşru menfaat dahil olmak üzere, veri işleminin amaçlarının sistematik bir açıklaması,
- (b) İşleme operasyonlarının amaçlara göre gerekliliği ve orantılılığının değerlendirilmesi,
- (c) m.35/1'de atıfta bulunulan ilgili kişilerin hak ve özgürlüklerine yönelik risklerin değerlendirilmesi,
- (d) Kişisel verilerin korunmasını sağlayacak güvenlik önlemleri ve mekanizmalar dahil olmak üzere riskleri ele almada öngörülen önlemler ile ilgili kişilerin ve ilgili diğer kişilerin haklarını ve meşru menfaatlerini dikkate alarak bu Düzenlemeye uygunluğu göstermede öngörülen önlemler.

İlgili veri sorumluları veya veri işleyenler tarafından m.40'ta atıfta bulunulan onaylanmış davranış kurallarına uygunluğun özellikle bir veri koruma etki değerlendirmesi amacıyla, bu veri sorumluları veya veri işleyenler tarafından gerçekleştirilen veri işleme faaliyetlerinin etkisinin değerlendirilmesinde dikkate alınması gerekmektedir (GDPR m.35/8). Uygun olan durumlarda veri sorumlusu,

Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, Article 10, p.39).

ticari çıkarların veya kamu çıkarlarının korunması veyahut işleme operasyonlarının güvenliği saklı kalmak kaydıyla, ilgili kişinin veya temsilcilerinin amaçlanan işleme ilişkin görüşlerini almalıdır (GDPR m.35/9). m.6/1c ve m.6/1e uyarınca veri işlemenin Birlik hukukunda veya veri sorumlusunun tabi olduğu Üye Devletin hukukunda yasal bir dayanağı varsa, bu yasa, söz konusu işlemler ve bu yasal temelin kabulü bağlamında genel bir etki değerlendirmesinin bir parçası olarak bir veri koruma etki değerlendirmesi zaten yapılmışsa, Üye Devletler işleme faaliyetlerinden önce böyle bir değerlendirme yapmayı gerekli görmedikçe, m.35'in 1'den 7'ye kadar olan fıkralarındaki hükümler uygulanmaz (GDPR m.35/10). Gerekli olduğunda veri sorumlusu (en azından veri işleme faaliyetlerine bağlı riskte bir değişiklik olduğunda), veri işlemenin veri koruma etki değerlendirmesine uygun biçimde gerçekleştirilip gerçekleştirilmediğini değerlendirmek için bir inceleme yapmalıdır (GDPR m.35/11).³⁸⁰

Özetle, VKED'ye, kişisel verilerin yeni kullanımını, süreci değiştirmeyi veya kişisel verilerin işlenme şeklini önemli ölçüde değiştirmeyi gerektiren aşağıdaki değişiklikler olduğunda başvurulması gerekmektedir:³⁸¹

- a) Kişisel verilerin toplanması ve saklanması için yeni bir belge veya elektronik bilgi sisteminin tanıtılması,
- b) Kuruluşun kişisel verileri kullanma, izleme ve rapor etme şeklini değiştirebilecek önemli bir sistemin güncellenmesi veya revize edilmesinin gerekmesi,
- c) Mevcut bir sistemin ek kişisel verilerin toplanacak şekilde değiştirilmesinin gerekmesi,
- d) Yeni bir kaynaktan veya yeni bir faaliyet için kişisel veri toplanmasının gerekmesi,
- e) Kişisel verilerin depolanmasını ve işlenmesini içeren iş süreçlerinin dış kaynaklardan sağlanmasına karar verilmesi,
- f) Bilgi varlıklarının transferini içeren hizmetlerin bir sağlayıcıdan diğerine aktarılmasının gerekmesi,

³⁸⁰ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 35**, pp.53-54.

³⁸¹ NHS, *Ibid.*, pp.3.-4

- g) Mevcut veri paylaşım sözleşmelerinin değiştirilmesi veya yenilerinin yapılmasının gerekmesi.

Otomatik karar alma mekanizmalarında veya profillemeye süreçlerinde ayrımcılığa sebep olabilecek faktörlerin önlenmesini GDPR par.71 ifade etmekle beraber nasıl yapılacağı hususunu ucu açık bırakmaktadır. Rehber ve araştırmalara göre; veri setindeki önyargının ve doğruluğun düzenli kontrolü, algoritmik denetimlerin yapılması önerilmektedir. Ancak hangi araçlarla veya yöntemlerle yapılacağı belirtilmemiştir.

Algoritmik şeffaflığın sağlanabilmesi ve daha hesap verebilir ve açıklanabilir algoritmalara ulaşılabilmesi için sistematik yönetim araçlarından olan VKED'nin kullanılarak farklı seviyelerde açıklamaların üretilbileceği düşünülmektedir. VKED'in içeriği diğer farklı etki değerlendirme analizleriyle güçlendirilerek algoritmaların ve YZ sistemlerinin insan haklarına etkilerinin de analiz edilebildiği araçlara dönüştürülebilir.

Ayrımcılığı, önyargıyı ve hakkaniyete aykırılık problemlerini çözmeyi hedefleyen diğer hukuki sistemler içerisinde önerilen algoritmik etki değerlendirmesi (algorithmic impact assessment) araçları oldukça dikkat çekmektedir³⁸². Gelecek polisliği alanında algoritmik etki değerlendirmesi analizlerinin yapılmasıyla ileride olabilecek ihmallerin önlenmesine ilişkin tedbir alınmış olacağı ifade edilmektedir. AI Now enstitüsü tarafından yapılan araştırmada tüm kamu kurumlarının otomatik karar alma mekanizmalarını kullanmayı başlayacağı döneme gelmeden algoritmik karar alma sistemlerinin satın alınmasından önce algoritmik etki değerlendirme analizlerinin yapılmasının gerekliliği ortaya konmuştur³⁸³.

VKED ilgili kişinin haklarına ilişkin sistemi, algoritmaların yönetişimine ilişkin olan sisteme bağlayan bir araç olarak görülebileceği ifade edilmektedir. VKED

³⁸² Senatör Wyden ve Booker tarafından önerilen Algoritmik Hesap Verilebilirlik düzenlemesi hakkında detaylı bilgi için bkz. Jones Day, "Proposed Algorithmic Accountability Act Targets Bias in Artificial Intelligence", June 2019. (Çevrimiçi) <https://www.jonesday.com/en/insights/2019/06/proposed-algorithmic-accountability-act> 8 January 2020.

³⁸³ Dillon Reisman, Jason Schultz, Kate Crawford, Meredith Whittaker, "Algorithm Impact Assessment: A Practical Frameworks for Public Agency Accountability", **AI Now Institute**, April 2018, (Çevrimiçi) <https://ainowinstitute.org/aiareport2018.pdf> 8 January 2019.

kurumların kendi kendini düzenlemesi (self regulation) için bir denetleme aracı olarak kullanılarak otomatik karar alma mekanizmaların alacağı kararların haksız, hatalı, önyargılı veya ayrımcı olma risklerini dikkate almaya ve sağlam adımlarla bu riskleri bertaraf etmeye yönlendirebilecektir. Ayrıca VKED sürecinde etkilenen kişilerden geri dönüş alınması, veri koruma görevlisine danışılması, gerektiğinde veri koruma otoritelerine danışılması, iç ve dıştaki uzmanlardan destek alınmasının da kurumların iç süreçlerini etkileyeceği görüşü dile getirilmektedir. İlgili kişilere yapılacak bilgilendirmeler, ilgili kişilerin erişim taleplerinde otomatik karar alma mekanizmasının çalışma mantığına ilişkin verilecek cevaplara ilişkin de VKED bir çıktı sağlayabilecektir³⁸⁴.

YZ sistemlerinin Temel insan haklarına saygılı bir şekilde çalışmasını sağlamak üzere insan hakları etki değerlendirmesi (human rights impact assessment) modelinin de VKED sürecinde kullanılabileceği araştırmacılar tarafından belirtilmektedir³⁸⁵. Birleşmiş Milletler tarafından belirlenen “human rights due diligence”³⁸⁶ yani insan hakları etki değerlendirmesi süreci, üçüncü kişi veri sorumlular tarafından veri toplayarak ve paydaşlarla, uzmanlarla ve yönetimle görüşmeler yaparak, şirketlerde uygulanacak olan bir analiz modelidir³⁸⁷. İnsan hakları etki değerlendirmesi analizlerinin şirketleri, potansiyel olarak etkilenen toplulukları ve kategorilerine bağlı olarak durumlarını belirlemeye, o gruptaki belirsiz veya hatalı etkileri tespit etmeye ve alınacak kararlarının etkilerini değerlendirmeye yönelteceği düşünülmektedir. VKED’in bireylerin temel hak ve hürriyetlerine ilişkin riskleri ve bireyler hakkında otomatik karar alma mekanizmalarının alacağı kararların önemi ve muhtemel sonuçlarına ilişkin bilgileri

³⁸⁴ Malgieri, *Ibid.*, pp.16-17.

³⁸⁵ Alessandro Mantelero, “AI and Big Data: A blueprint for a human rights, social and ethical impact assessment”, **Computer Law & Security Review**, Vol.34, No.4, 2018, pp.754-772; Sonia K. Katyal, “Private Accountability in the Age of Artificial Intelligence”, **UCLA law Review**, Vol.66, 2019, p.54, (Çevrimiçi) <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4064&context=facpubs> 8 January 2019.

³⁸⁶ İnsan haklarına ilişkin gereken özeni göstermeyi, riskleri tanımlamayı, aydınlatmayı ve bertaraf etme amacı ile araştırılması, incelenmesi ve denetlenmesini ifade etmektedir.

³⁸⁷ İnsan hakları etki değerlendirmesi analizi hakkında daha detaylı bilgi için bkz. The Office of the High Commissioner for Human Rights (UN Human Rights) (OHCHR), “Guiding Principles on Business and Human Rights”, **United Nations, Human Rights Council, Office of The High Commissioner**, 2011, pp.23–26., (Çevrimiçi) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf 8 January 2020.

içermesi gerektiği göz önünde bulundurulsa insan hakları etki analizi modelinden de faydalanmasının uygun olacağını düşünmekteyiz.

3.2.2.2. Veri İhlali Riskinin Yüksek Olması Hâlinde Bu Riskin Kişisel Verileri Koruma Kurumuna ve İlgili Kişiye Bildirimde Bulunma Zorunluluğu

GDPR'nin 84. paragrafına göre; veri işleme faaliyetlerinin gerçek kişilerin hak ve özgürlükleri için büyük bir risk oluşturma ihtimali halinde Düzenlemeye uyumu artırmak için veri sorumlusu, özellikle bu riskin kaynağını, doğasını/niteliğini, olasılığını/özgürlüğünü ve ciddiyetini değerlendirmek için öncelikli olarak bir veri koruma etki değerlendirmesi yapmalıdır. Kişisel verilerin işlenmesinin bu Düzenlemeye uygunluğunu göstermek için alınacak önlemler belirlenirken değerlendirmenin sonucu dikkate alınmalıdır. Ancak, yapılan veri koruma etki değerlendirmesinin, işleme operasyonlarının mevcut teknoloji ve uygulama maliyetleri açısından veri sorumlusunun uygun önlemler ile hafifletemeyeceği yüksek bir risk içerdiğini göstermesi halinde, veri işleme faaliyeti öncesinde veri koruma otoritesine (*supervisory authority*) danışılması gerekmektedir (GDPR, par.84)³⁸⁸.

Kişisel veri ihlalinin m.34/1'de atıfta bulunulan gerçek kişilerin hak ve özgürlükleri açısından yüksek risk doğurabileceği durumlara ilişkin olarak m.70/1e uyarınca kılavuz ilkeler, tavsiyeler ve en iyi uygulamaları yayınlama görevi Avrupa Veri Koruma Kurulu'na (*EDPB - European Data Protection Board*) ait olup bu uyarı, tavsiye ve kılavuzların yayınlanması EDPB'nin kendi inisiyatifiyle veya ilgili olduğu hallerde Komisyon'un (EC'nin) talebi üzerine gerçekleştirilebilir (GDPR, m.70/1h)³⁸⁹. Uygun önlemlerin uygulanması ve veri sorumlusu veya işleyen tarafından uygunluğun gösterilmesi konusundaki rehberlik (özellikle veri işleme ile ilgili riskin tanımlanması; kaynağı, doğası/niteliği, olasılığı/özgürlüğü ve ciddiyeti açısından değerlendirilmesi ve riski azaltmak için en iyi uygulamaların belirlenmesi), onaylanmış davranış kuralları (code of conduct), onaylanmış sertifikalar, Kurul

³⁸⁸ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, par.84**.

³⁸⁹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, m.70/1h**.

tarafından sağlanan rehberler veya bir veri koruma görevlisinin uyarıları doğrultusunda gerçekleştirilmelidir (GDPR, par.77) ³⁹⁰.

GDPR, m.34/1³⁹¹ ve par.86 uyarınca; gerçek kişinin hak ve özgürlükleri için yüksek riskle sonuçlanabilecek kişisel veri ihlali ile ilgili ilgili kişi zamanında gerekli önlemleri alabilmesi için veri sorumlusu, gereksiz bir gecikme olmaksızın, ilgili kişiye bilgi vermelidir. GDPR par.86 uyarınca bu bilgilendirme, kişisel veri ihlalinin doğasını/niteliğini tanımlamalı ve ilgili kişi üzerindeki potansiyel olumsuz etkileri azaltmaya yönelik önerileri içermelidir. İlgili kişiye yapılan bu tür bilgilendirmeler, veri koruma otoritesinin kendisi veya kolluk kuvvetleri gibi diğer ilgili makamlar tarafından sağlanan rehberlik göz önünde bulundurularak, makul ölçüde mümkün olan en kısa sürede ve veri koruma otoritesi ile yakın işbirliği içinde yapılmalıdır. Örneğin, bir hasar riskinin derhal azaltılması ihtiyacı, ilgili kişilerle vakit geçirmeden iletişim kurulmasını gerektirirken; etkisi devam eden veya benzer kişisel veri ihlallerine karşı uygun önlemlerin uygulanması ihtiyacı, iletişim için daha fazla zamanı haklı kılabilir (GDPR, par.86) ³⁹²

GDPR ile yürürlükten kalkan 95/46/EC sayılı eski Yönerge, kişisel verilerin işlenmesini veri koruma otoritelerine bildirmek için genel bir yükümlülük³⁹³ getirmişti. Bu yükümlülük idari ve mali yükler getirse de her durumda kişisel verilerin korunmasına katkıda bulunmamıştır. Bu nedenle, bu tür ayırım gözetmeyen genel bildirim yükümlülükleri kaldırılmalı ve bunların yerine, doğası/niteliği, kapsamı, içeriği ve amaçları gereği gerçek kişilerin hak ve özgürlükleri açısından yüksek riskle sonuçlanması muhtemel olan bu tür işlemlere odaklanan etkili prosedürler ve mekanizmalar kullanılmalıdır. Bu tür veri işleme faaliyetleri, özellikle yeni teknolojilerin kullanılmasını içeren veya yeni bir türden olan ve veri sorumlusu tarafından daha önce hiçbir veri koruma etkisi değerlendirmesinin yapılmadığı veya

³⁹⁰ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, par.77**.

³⁹¹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, m.34/1**.

³⁹² Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, par.86**.

³⁹³ 95/46/EC sayılı eski Yönerge'nin yürürlükten kalkmasıyla bu yükümlülük de ortadan kalkmıştır.

sistemin, hizmetin, ürünün veya sürecin tasarım aşamasında ve sonrasındaki yaşam döngüsü boyunca değerlendirmeyi sağlayan bir yaklaşımdır³⁹⁸.

6698 sayılı KVKK'da tasarımdan itibaren kişisel verilerin korunmasına ilişkin bir düzenleme bulunmamaktadır. Diğer yandan Avrupa'da bu konuya ilişkin hükümler AB ülkelerinde GDPR'nin "*Data protection by design and by default*" başlıklı 25. maddesinde düzenlenmiştir. GDPR m.25/1 uyarınca veri sorumlusu; tekniğin bilinen durumu, uygulama maliyeti ve veri işlemenin doğası/niteliği, kapsamı, içeriği ve amaçları ile işleme tabi tutulan gerçek kişilerin hak ve özgürlükleri için değişen olasılık ve ciddiye risklerini göz önünde bulundurarak, hem işleme araçlarının belirlenmesi sırasında hem de işlemenin kendisi sırasında, veri minimizasyonu gibi veri koruma ilkelerini etkili bir şekilde uygulamak ve bu Düzenlemenin gerekliliklerini karşılamak ve ilgili kişilerin haklarını korumak için gerekli önlemleri işleme entegre etmek için tasarlanmış olan "takma adlandırma" (pseudonymisation) gibi uygun teknik ve idari önlemleri uygulamakla yükümlüdür (GDPR, m.25/1). Veri sorumlusu, varsayılan olarak, yalnızca veri işlemenin her bir özel amacı için gerekli olan kişisel verilerin işlenmesini sağlamayacak uygun teknik ve idari tedbirleri uygulamalıdır. Bu yükümlülük toplanan kişisel verilerin miktarı, işlenme süreleri, depolanma süreleri ve erişilebilirlikleri için geçerlidir. Özellikle, bu tür tedbirler, bireyin müdahalesi olmadan varsayılan (default) olarak kişisel verilerinin belirsiz sayıda gerçek kişi tarafından erişilebilir olmamasını sağlayacaktır (GDPR, m.25/2). GDPR m.25/1 ve m.25/2'de belirtilen şartlara uygunluğu göstermek için m.42 uyarınca onaylanmış bir sertifikasyon mekanizması kullanılabilir (GDPR, m.25/3).³⁹⁹

Kurumlarda kişisel verilere ilişkin ilkelerin teknik ve yönetim tasarımının içine yerleştirecek, veri, süreç veya teknik mimarisini düzenleyebilecek bilgi birikiminde ve yetkinlikte "privacy engineer" olarak adlandırılan çalışanlara ihtiyaç

³⁹⁸ The University of Roehampton, "Guide to the General Data Protection Regulation GDPR 1.0 - Data protection by design and default", London, 2018, August 2. (Çevrimiçi) <https://www.roehampton.ac.uk/globalassets/documents/ethics/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> 19 December 2019.

³⁹⁹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, **GDPR, Article 25**, p.48.

duyulacaktır⁴⁰⁰. “Privacy engineer” olarak adlandırılan çalışacak kişilerin eğitilmesi için mühendislik alanında öncü olan Carnegie Mellon Üniversitesinde Bilgi Teknolojileri ve Kişisel Verilerin Korunması Mühendisliği Yüksek Lisans Programı açılmıştır⁴⁰¹. Program kapsamında “privacy engineer”; teknolojiyi anlayan ve ürün tasarımı, yazılım geliştirme, siber güvenlik, insan makine etkileşimi, işin gereklilikleri ve hukuki yönleri sisteme entegre edebilecek kişi olarak ifade edilmiştir. Ayrıca Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST: National Institute of Standards and Technology) tarafından oluşturulan kişiden ziyade bir yaklaşımı ifade eden “privacy engineering” konseptiyle; bilgi teknolojilerinin geliştirilme safhasında, bilimsel ölçüm yöntemlerinin ve sistem mühendisliği ilkelerinin uygulanmasıyla üretilen güvenilir yapıların (frameworks), risk modellerinin, rehberlerin, araçların ve standartların aracılığıyla kişisel verilerin korunmasının ve temel hak ve özgürlüklerin korunması hedeflenmektedir⁴⁰².

Uluslararası Standartları Teşkilatı (ISO: International Organization for Standardization) tarafından ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardına ek olarak tasarlanan “ISO 27701 Privacy Information Management Standart”, kişisel verilerin korunması anlamındaki ilk uluslararası standarttır⁴⁰³. ISO 27701, kişisel verilerin korunmasını sağlayan uyum ve yönetim programının kurulması, entegre edilmesi, uygulanması, korunması ve devamlı gelişimi için gereklilikleri ve rehberliği sağlamaktadır. Sistemli bir şekilde kişisel verilerin “privacy engineering” şeklinde ifade edilen yaklaşımı kurumlara entegre edebilmek için NIST’nin ön taslağını yayımlandığı “NIST Privacy Framework” takip edilebilecek yapılar (frameworks) arasındadır⁴⁰⁴. Daha ziyade teknik yönü ağırlıkta olan bu yapı, hukuki, teknik,

⁴⁰⁰ Steve Kenny, John Borking, “The Value of Privacy Engineering”, **Journal of Information, Law & Technology (JILT)**, Vol.2002, No.1, 2002 (Çevrimiçi) https://warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/ 5 January 2020.

⁴⁰¹ Daha detaylı bilgi için bkz. Master of Science in Information Technology – Privacy Engineering (MSIT-PE) Institute for Software Research, (Çevrimiçi), <https://privacy.cs.cmu.edu> 5 January 2020.

⁴⁰² Sean W. Brooks, Michael E. Garcia, Naomi B. Lefkowitz, Suzanne Lightman, Ellen M. Nadeau, “An Introduction to Privacy Engineering and Risk Management in Federal Systems” **National Institute of Standards and Technology (NIST)**, January 2017 (Çevrimiçi) <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf> 5 January 2020.

⁴⁰³ Clare Naden “Tackling Privacy Information Management Head On: First International Standard Just Published”, **International Organization for Standardization (ISO)**, 6 August 2019, (Çevrimiçi) <https://www.iso.org/news/ref2419.html> 8 January 2020.

⁴⁰⁴ Naomi Lefkowitz, “The Preliminary Draft of the NIST Privacy Framework is Here!”, **National Institute of Standards and Technology (NIST)**, 9 September 2019. (Çevrimiçi)

tasarım ve ürün ile ilgilenen takımlara ortak bir terminoloji oluşturarak uyum içerisinde verimli bir şekilde çalışabilmeleri amacıyla tasarlanmıştır.

Sistem, ürün veya hizmetlerin tasarımlarında kişisel verilerin korunmasının yanı sıra diğer değerlerin veya yasal düzenlemelerin de tasarıma yerleştirilerek uygulanması da temel hak ve hürriyetlerin korunması için “Regulation by design” konsepti önerilmektedir⁴⁰⁵. Tasarımdan itibaren kişisel verilerin korunması ve “privacy engineering” konseptleri üzerine yapılan çalışmalara ek olarak, makine öğrenimi algoritmaları üzerine yapılan çalışmamızın özellikle “3.2.1. Teknik Tedbirler” başlıklı bölümde değinilen algoritmalarındaki kara kutu ve opaklık ile önyargı sorunlarını eğitim verisini minimize ederek veya açıklama yöntemlerini kullanarak çözmeye çalışarak algoritmik şeffaflığı ve hesap verilebilirliği artırmayı ve sonuç olarak da algoritmik ayrımcılık ve haksızlığı azaltmak suretiyle kişilerin verilerinin korunması başta olmak üzere temel hak ve hürriyetlerinin korunması için yapılan araştırmalar “human rights protection by design” (tasarımdan itibaren temel insan haklarının korunması) anlayışı olarak ifade edilebilecektir⁴⁰⁶.

3.2.2.4. Veri Koruma Görevlisi

GDPR’nin temelinde olan hesap verilebilirlik ilkesi kapsamında kurum ve kuruluşların uyumlu olduklarını ispat etmede kullanabilecekleri araçlar ve alınması gereken tedbirler düzenlemede tanımlanmıştır. Kurumların kullanabileceği araçlar, yapabileceği analizler ve alması gereken tedbirler arasında sıkı bir ilişki bulunmaktadır.

GDPR m.35/2’ye göre; veri sorumlusunun, bir veri koruma etki değerlendirmesi yaparken, belirtilen durumlarda veri koruma görevlisinin tavsiyesini alması gerekir.⁴⁰⁷ Veri koruma görevlisine ilişkin hükümler, GDPR’nin “*Data protection officer*” (Veri koruma görevlisi) başlıklı Dördüncü Bölümünde (37-39.

<https://www.nist.gov/blogs/cybersecurity-insights/preliminary-draft-nist-privacy-framework-here> 8 January 2020.

⁴⁰⁵ Karen Yeung, “Design for Regulation” in M.J. Van Den Hoven, P.E. Varmaas, I. van de Poel (Eds.) Handbook of Ethics, Values and Technological Design, **Springer**, 2015. pp.447-472.

⁴⁰⁶ Yeung, “**A Study of...**”.

⁴⁰⁷ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 35/2**, p.53.

maddelerinde)⁴⁰⁸ düzenlenmiştir. “*Designation of the data protection officer*” (Veri koruma görevlisinin atanması) başlıklı 37. maddenin 1.fıkrasına göre veri sorumlusu ve işleyen aşağıdaki durumlarda bir veri koruma görevlisi atamalıdır:

- (a) İşlemin, yargı kapasitelerinde hareket eden mahkemeler hariç, bir kamu makamı veya organı tarafından gerçekleştirilmesi,
- (b) Veri sorumlunun veya Veri işleyenin temel faaliyetlerinin, yapıları gereği, kapsamı ve/veya amaçları nedeniyle, veri konularının büyük ölçekte düzenli ve sistematik olarak izlenmesini gerektiren işleme işlemlerinden oluşması,
- (c) Veri sorumlusunun veya işleyenin temel faaliyetlerinin, m.9 uyarınca büyük bir özel veri kategorisindeki ve/veya m.10'da atıfta bulunulan cezai hüküm ve suçlara ilişkin kişisel verilerden oluşması.

Daha önceki bölümlerde açıklandığı üzere kamu kurumları YZ sistemlerini en erken kullanıma alan kurumların başında geldiği, kullanım alanları itibarıyla yargı, eğitim, güvenlik, sosyal yardımların dağıtılması gibi temel hak ve hürriyetlere ilişkin risk barındıran konular olması sebebiyle kurum yapıları içerisinde sistemlerin satın alınması öncesinde ve kullanılmaya başlanmasından sonra gerekli analizleri, gözetimi ve denetlemeleri yapacak veri koruma görevlilerine ihtiyaç duyacaktır.

Sağlık verisi toplayan hastaneler, müşteri verisi toplayan banka veya sigorta şirketleri, giyilebilir cihazlar aracılığıyla GPS veya sağlık verisi toplayan, internet üzerinden cookieler aracılığıyla kişileri profilleyen ve çevrimiçi reklamcılıkta bulunan kurumların da sistemlerin temel hak ve hürriyetlere oluşturabileceği riskleri ölçmede, herhangi bir ayrımcılık veya haksızlığa sebep olma durumunun analizinde bulunacak yetkin ve gerekli bilgi birikimine sahip veri koruma görevlilerini kurumlarında istihdam edip hem rekabet avantajı hem de düzenlemelere uyum sağlamak amacıyla kişisel verilerin korunması uyum programının yürütülmesini sağlamalıdır⁴⁰⁹.

⁴⁰⁸ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 37-39**, pp.55-56.

⁴⁰⁹ Article 29 Data Protection Working Party, “Guidelines on Data Protection Officers” As last Revised and Adopted on 5 April 2017, 2017 (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 8 January 2020.

GDPR'nin "*Position of the data protection officer*" (Veri koruma görevlisinin konumu) başlıklı 38. maddesinin 1. fıkrası uyarınca veri sorumlusu ve işleyen, veri koruma görevlisinin kişisel verilerin korunması ile ilgili tüm konulara uygun ve zamanında dahil edilmesini sağlamalıdır (GDPR, m.38/1). Veri sorumlusu ve işleyen, veri koruma görevlisine bu görevleri yerine getirme, kişisel veri ve işleme faaliyetlerine erişme ve uzman bilgisini korumada gerekli kaynakları sağlayarak, m.39'da atıfta bulunulan görevleri yerine getirmesi sırasında veri koruma görevlisini desteklemelidir (GDPR, m.38/2).⁴¹⁰ Veri koruma görevlisinin m.39'da belirtilen asgari görevleri şunlardır:

- (a) Bu Düzenleme ve diğer Birlik veya Üye Devlet veri koruma hükümleri uyarınca yükümlülüklerini işlemekten geçiren veri sorumlusuna veya veri işleyene ve çalışanlara bilgilendirme ve tavsiyelerde bulunmak,
- (b) İşleme faaliyetlerinde ve ilgili denetimlerde görev almakta olan personelin, bu Düzenlemeye, diğer Birlik veya Üye Devlet veri koruma hükümlerine ve veri sorumlusunun veya veri işleyenin kişisel verilerin korunmasına ilişkin sorumluluklarının belirlenmesi, bilinçlendirilmesi ve eğitimi de dahil olmak üzere KVK politikalarına uygunluğunu izlemek,
- (c) Veri koruma etki değerlendirmesi ile ilgili istendiğinde tavsiyelerde bulunmak ve m.35 uyarınca bu etki değerlendirmesinin performansını izlemek.
- (d) veri koruma otoriteleri ile işbirliği yapmak.
- (e) m.36'da atıfta bulunulan ön istişare de dahil olmak üzere, veri işleme ile ilgili konularda veri koruma otoritesinin irtibat kişisi ve uygun olduğunda, başka herhangi bir konuda danışılacak kişi olarak hareket etmek (GDPR, m.39/1).⁴¹¹

m.39'un 2. fıkrasına göre ise veri koruma görevlisi, görevlerinin yerine getirilmesinde, işlemin niteliği, kapsamı, içeriği ve amaçları göz önünde bulundurarak işleme faaliyetleriyle ilişkili riskleri göz önünde bulundurmalıdır⁴¹². Veri

⁴¹⁰ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 38/1-2**, p.55.

⁴¹¹ Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 39/1**, p.56.

⁴¹² Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe), Regulation (EU) 2016/679, GDPR, **Article 39/2**, p.56.

koruma görevlisinin kurum içerisinde çıkar çatışmalarına girmemesi ve bağımsızlığını koruyabilmesi için doğrudan en üstteki yöneticiye bağlı olması eksikliklerin veya risklerin teşhisinde ve çözümlerin uygulanmasında kurumun ve ilgili kişilerin menfaatinin, çalışanların şahsi menfaatlerinden önde tutulmasını sağlayacaktır. Veri koruma görevlilerinin seçilmesi hususunda “International Association of Privacy Professionals” (IAPP) kuruluşunun CIPP ve CIPT gibi sertifikaları⁴¹³, İspanya veri koruma otoritesinin sertifikasyonu⁴¹⁴ ve diğer kişinin bilgi ve siber güvenliği, proje yönetimi ve kişinin üniversitede okuduğu bölüm ile iş tecrübeleri dikkate alınan hususlardan bazılarıdır.

Görüldüğü üzere veri koruma görevlisinin bulunduğu görevlerde kanunun uygulanmasını, kontrol ve denetimi sağlamak, bilinçlendirme faaliyetleri, çalışanlara eğitim vermek ve ilgili kişilerle iletişimde bulunmak gibi kilit rolleri bulunmaktadır.

3.2.2.5. Algoritmik Denetim

Sistemin uygulamaya alınmasından önce yapılması hedeflenen etki değerlendirme analizlerinden ayrı olarak algoritmik denetim teknikleri, algoritmik sistemin operasyona alınmasıyla birlikte test ve değerlendirmeye tabi tutulmasını amaçlamaktadır. Algoritmik denetim, algoritmik sistemlerin istenilmeyen olumsuz etkilerinin tespiti, incelenmesi ve teşhisini sağlamak için araştırma araçlarının ve tekniklerinin geliştirilmesi üzerine yoğunlaşan bir alan olarak öne çıkmaya başlayan bir alandır⁴¹⁵. Algoritmik denetim tekniklerinin özellikle yüksek riskli kapsamına alınabilecek algoritmik sistemlerin düzenli denetlenmesi ve alanında yetkin teknik personele sahip denetleyici bağımsız otoriteler tarafından gözetim altında tutulması için düzenlemelerde yer almasıyla yasal bir zorunluluk haline gelmesinin bir gereklilik olduğu tavsiye edilmektedir. “Algorithmists” olarak adlandırılan hukuk, tıp,

⁴¹³ International Association of Privacy Professionals” (IAPP), “From Here to DPO: Building a Data Protection Officer”, (Çevrimiçi) https://iapp.org/media/pdf/resource_center/From_Here_to_DPO_FINAL.pdf. 8 January 2020.

⁴¹⁴ International Association of Privacy Professionals” (IAPP), “Certification Scheme of Data Protection Officers From The Spanish Data Protection Agency (DPO-AEPD SCHEME)”, (Çevrimiçi) https://iapp.org/media/pdf/resource_center/AEPD_DPO-Certification-Scheme.pdf. 8 January 2020.

⁴¹⁵ Algoritmik denetim hakkında daha detaylı bilgi için bkz. Deven R. Desai, Joshua A. Kroll, “Trust but verify: A guide to algorithms and the law”, **Harvard Journal of Law & Technology**, Vol.31, 2017; Christian Sandvig, “Auditing algorithms: Research methods for detecting discrimination on internet platforms”, **Data and discrimination: converting critical concerns into productive inquiry**, 22 May 2014.

muhasabe ve mühendislik gibi alanlarda uzmanlık sahibi olmuş ve algoritmik denetim görevini üstlenebilecek ister bağımsız bir şekilde algoritmaları dışarıdan takip edecek isterse de kurumun içerisinde istihdam edilip algoritmaların gelişimini ve uygulamaya alınmasını takip edecek yeni bir meslek grubu önerilmektedir⁴¹⁶.

Algoritmik denetimin yapılmasına karşı ileri sürülebilecek itirazlar çeşitli hakların ve menfaatlerin çatışmasına dayandırılabilir. Sınıflandırma Algoritmalarında opaklığın aşılması adına doğrudan kodun kendisine bakmanın önünde engel olan husus mülkiyet hakkına müteallik korunması gereken menfaatlerdir. Kötü niyetli rakiplere karşı Rekabet avantajının korunması gibi gayeler nedeniyle kodun incelenmesi yolunun uygun olmayacağı görüşünde olanlar bulunmaktadır.

Algoritmik şeffaflığın ve hesap verilebilirliğin sağlanmasında sorumluluğu kurumlara bırakarak bir iyileşmenin beklenmesinin ilgili kişilerin haklarının ihlal edilmesinin devam etmesine neden olabilecektir. Kurumların kasten şeffaf olmamayı tercih ettiği durumlarda hukuki düzenlemeler aracılığıyla kodun tasarımının incelenmesi suretiyle müşterilerin haklarının ihlal edilmesine ve hukuka aykırı işlemlerine dair sorunlar çözülebilir⁴¹⁷. Bağımsız ve güvenilir denetleyici 3. kişiler aracılığıyla sırların korunması sağlanarak söz konusu inceleme faaliyetleri gerçekleştirilebilir⁴¹⁸.

Algoritmik sistemler kullanan uygulamalar içeriğinde çok farklı katmanlarda birbirinden farklı algoritmalar, teknikler, çok farklı grupta geliştiriciler, ilişki ağaçları kullanıyor olabilirler. Bu sebeple de sadece kodun okunmasının planlanmasıyla istenilen amaca kolaylıkla ulaşılamayacaktır. Veri setlerinin çok büyük olması ve kodun içerisindeki heterojen yapıların bulunması sebebiyle de kompleksliği artırmaktadır.

⁴¹⁶ Mayer-Schönberger, Cukier, **Ibid.**; Kate Crawford, Jason Schultz, "Big data and due process: Toward a framework to redress predictive privacy harms", **Boston College Law Review**, Vol.55, 2014, pp.93-128.

⁴¹⁷ Burrell, **Ibid.**

⁴¹⁸ Frank Pasquale, "The Black Box Society: The Secret Algorithms that Control Money and Information", **Harvard University Press**, 2015.

SONUÇ VE ÖNERİLER

Bireyler başta politik görüş, ırk ve uyrukları, dini inanç, felsefi görüş, sağlık durumları ve cinsel yönelimleri gibi özel nitelikli kişisel verileri olmak üzere genel itibarıyla kişisel verilerinin işlenmesi sonucunda üretilen profillerinin yapay zekâlı sistemlerin altyapısını oluşturduğu otomatik veya yarı otomatik karar alma mekanizmalarında kullanılması sebebiyle çeşitli haksızlık ve ayrımcılıklara uğramaktadırlar. Bu tür haksızlık ve ayrımcılıkların engellenmesi, temel hak ve hürriyetlerin korunması amacıyla inşa edilmiş başta şeffaflık ve hesap verilebilirlik olmak üzere KVK hukukundaki temel ilkelere uyumlu veri işleme faaliyetine bulunabilme adına mevcut bulunan teorileri, pratik hayattan örnekleri, çözüm önerilerini, teknik ve idari tedbirleri araştırmak amacıyla yapılan bu çalışmada; KVK hukukunun gelişimi, KVK'ya ilişkin bazı temel kavramlar, ilkeler ve konseptler, YZ sistemleri, YZ sistemleri bakımından kişisel verilerin işlenmesindeki temel ilkeler, kişisel verilerle ilgili diğer ilkeler, yapay zekâ sistemlerinde kişisel verilerin işlenmesi, algoritmalar, YZ sistemleri bakımından kişisel verilerin korunmasına ilişkin ilgili kişinin hakları ve alınması gereken tedbirler incelenmiştir.

Kişisel veri kavramı, kısaca; “tanımlanmış veya tanımlanabilir bir bireye ilişkin herhangi bir bilgi” ve/veya “kimliği belli ya da belirlenebilir olan gerçek kişilere yönelik her tür bilgi” olarak tanımlanabilir. Yaşayan bir bireyi ilgilendiren her türlü bilgi bu tanımın kapsamında olabilir. Bu nedenle kişisel verilerin neler olduğuna ilişkin liste kolayca genişletilebilir ve çeşitlendirilebilir. Avrupa Birliği düzenlemelerine göre bir bilgi/veri, belirli bir kişiyi tanımlıyorsa veya verilen bilgilerden/verilerden yola çıkıldığında o kişinin kimliğinin belirlenmesi önemli düzeyde kolaylaşıyorsa, o bilginin/verinin kişisel bilgi/veri içerdiği, dolayısıyla kişisel veri olarak değerlendirilmesi gerektiği kabul edilir. Bireyler bir takım kişisel özellikleri ve bu özelliklere ilişkin bilgilere kolay erişilebilmesi nedeniyle toplumun çeşitli kesimlerinde ayrımcılığa maruz kalabilmektedirler. Bu ayrımcılıklar ırk, doğum yeri, inanç gibi kişinin statik yani değişmez ya da değişmesi zor olan bilgileri nedeniyle veya yeme alışkanlığı, uyuma, dışarıya çıkma, konum verileri, arama motoru kullanımı, çerezler aracılığıyla tespiti gezinti yapılan web siteleri, sosyal medya hesaplarında takip edilenler, arkadaşlar ve iletişim kurulan kişiler gibi kişinin dinamik yani değişken ya da değişmesi kolay olan verileri sebebiyle uğranılan ayrımcılıklar olabilir. İşte bu noktada da özel nitelikli kişisel verilerin korunması kavramı önem kazanmaktadır.

Özel nitelikli kişisel veri, öğrenildiğinde söz konusu bireye ilişkin ayrımcılığa ya da mağduriyete yol açma olasılığı yüksek olan bilgiler olduğundan bu tür verilerin diğer kişisel verilerle kıyaslandığında daha iyi korunması gerekmektedir. Nitekim gerek GDPR’de gerekse 6698 sayılı KVKK’da özel nitelikli kişisel veriler hassas bilgiler olarak kabul edilmiş ve bunlara özel bir önem verilerek ayrı bir düzenlemeye gidilmiştir. Özel nitelikli veriler GDPR’de ve KVKK’da tanımlanarak listelenmiştir. Ayrıca GDPR ve KVKK’da özel nitelikli kişisel verilere ayrı bir önem verilerek bunlar kıyas yoluyla genişletilemeyecek şekilde dar ve sınırlı bir kapsamda tanımlanmış ve bu verilerin tanımı ve işleme şartlarına ilişkin ayrı bir düzenleme getirilmiştir. Diğer temel hak ve özgürlüklerin korunmasında mevcut bulunan sınırlı durumlar, özel nitelikli kişisel veriler için de geçerlidir. Diğer yandan bu verilere ilişkin sınırlamalarda Türkiye Cumhuriyeti Anayasası’nın 13. maddesindeki esasların dikkate alınması gereklidir. Bu maddeye göre temel hak ve özgürlüklere ilişkin sınırlamaların Anayasanın çeşitli maddelerinde geçen sebeplere bağlı olarak ve kanunla gerçekleştirilebileceği belirtilmiştir. Diğer yandan pek çok temel hak ve özgürlüğün kullanılmasında, özel nitelikli kişisel verilerin işlenmesi zorunlu olmaktadır. Bundan dolayı da bu tür verilerin işlenmesinde mutlak yasaklığın geçerli olması söz konusu değildir.

KVKK’da, veri sorumlusu ve veri işleyenin tanımları yapılmıştır. Veri sorumlusu; kişisel verileri işlemede amaç ve araçları belirleyen, verilerin kayıt sistemini kurma ve yönetmeden sorumlu gerçek ya da tüzel kişi olarak tanımlanırken veri işleyen ise; veri sorumlusu tarafından verilen yetki dahilinde ve veri sorumlusu adına kişisel verilerin işlenmesi fiilini gerçekleştiren gerçek ya da tüzel kişi şeklinde tanımlanmıştır.

Bazı yönleriyle özel hukuktan, bazı yönleriyle ise kamu hukukundan özellikler taşıyan KVKK, tarihsel süreçte yer alan birçok temel hak ve özgürlükle yakından ilişkilidir. Bunlar arasından başta gelenler özel hayatın gizliliği, insan onuru ve kişiliğin serbestçe geliştirilmesi hakkıdır. Bunlara ek olarak ifade özgürlüğü, bilgi edinme hakkı ve haberleşme özgürlüğü gibi bazı temel hak ve özgürlüklerin de zaman zaman KVKK’yı destekledikleri zaman zaman da bu hakka ters düştüğü görülmektedir. Dolayısıyla tarihsel süreçte bu hakkın hangi temel hak ve özgürlükler kapsamında değerlendirilmesi gerektiği konusunda farklı görüşler oluşmuştur. Ancak

yaygın olan görüş, temel insan haklarından biri olarak kabul edilen özel hayatın gizliliği kapsamında değerlendirilmesi gerektiği yönündedir.

Kişisel verilerin mülkiyet olarak kabul edilmesi halinde alınıp satılabilmesi ve ardından verinin ilk başta öngörülmeleyen amaçla başka birine devri veya bunun korunmasını takip etme yükünün malikine verilmesi söz konusudur. KVK'nın mülkiyet hakkı çerçevesinde değerlendirilmesinin isabetli olmayacağı, öyle yapılması halinde ise yalnızca kamu ve özel sektör sermayelerine fayda sağlayacağı anlaşılmaktadır. Tabi ki çağımızda ekseriyetle elektronik ticarete satışları arttırmak amacıyla müşteri alışkanlıklarının belirlenmeye çalışılması veya sosyal medyada kullanıcıların siyasi eğilimlerine ilişkin fikir edinilmeye ve bu eğilimlerin yönlendirilmeye çalışılması sayesinde bu veriler önemli bir ekonomik değere kavuşmuştur. Bu verilerin ekseriyetle internetin bireylerin hayatında yer almaya başladığı 1990'lı yıllar itibarıyla değerini artırdığı hatta çağın petrolü olarak adlandırıldığı göz önünde bulundurulduğunda, toplumun fertlerinin gerek kamu gerekse özel sektör kurum ve kuruluşlara karşı geçmişte olduğundan daha çok korunmaya muhtaç olduğu görülmektedir. Hiç şüphesiz bireyler, kendilerine ait bilgilerin kaderini belirleme hakkına sahip olmalıdırlar. Diğer yandan devletin de bireylerin bu hakkını korumak amacıyla düzenlemeler yapması zorunludur. Yoksa bireylerin bu yöndeki özgür iradesi kısıtlanmış ve bu irade devlet ve sermaye tarafından kullanılmış ve/veya yönlendirilmiş olacaktır.

KVK ve bu hakkı koruma sorumluluğu -kişinin insan olması nedeniyle doğuştan kazandığı, mirasla intikal etmeyen, devredilemeyen veya haczedilemeyen, kişinin manevi çıkarlarını gözetken bir hak, kısaca bir insan hakkı olan kişilik hakkı kapsamında değerlendirildiğinde- devlete yüklenen bir hak olmaktadır. KVKH, AB ülkeleri ve Kıta Avrupa Hukukunun uygulandığı ülkeler tarafından uzun yıllardır bir insan hakkı olarak görüldüğünden, kişilik hakkı görüşünü desteklemektedir. KVKH, AİHS 8. madde, EİHB 17. madde, BM Bireysel ve Siyasal Haklar Şartı'nın 12. Madde, Avrupa Birliği Temel Haklar Şartı ve bazı AB ülkelerinin Anayasa metinleri gibi birçok yeni metinde KVKH'nın özel hayatın gizliliği hakkından bağımsız olarak da ayrı bir şekilde temel haklardan kabul edilerek korunmaktadır. KVKH, özel hayatın gizliliğinin yanı sıra, ifade özgürlüğü, unutulma hakkı, insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı, bilgi edinme hakkı, özel

haberleşmenin gizliliği, bilim özgürlüğü gibi birçok insan hak ve özgürlüğüyle yakından ilişkilidir.

Yapay zekâ sistemleri, genel olarak karmaşık bir amaca ulaşmak için çevrelerini veri toplama yoluyla algılayarak, toplanmış, yapılandırılmış veya yapılandırılmamış verileri yorumlayarak, bu verilerden elde edilen bilgiyi analiz edip en iyi önlemleri almaya karar vererek fiziksel veya dijital ortamda hareket eden yazılım (ve muhtemelen donanım) sistemleridir. Ortamın önceki eylemlerinden nasıl etkilendiğini analiz ederek davranışlarını uyarlamayı öğrenmek amaçlı da tasarlanabilen YZ sistemlerinin başlıca yöntemleri; Makine Öğrenimi, Gözetimli ve Gözetimsiz Öğrenme, Derin Öğrenme ve Yapay Sinir Ağları olmak üzere dört temel grupta toplanmaktadır. YZ sistemleri; bireylerin hemen hemen her gün faydalandıkları birçok teknolojik cihaz, bilgisayarlar, akıllı cep telefonları, internete bağlı diğer cihazlar, sanal gerçeklik, artırılmış gerçeklik, sesli asistanlar, yüz tanıma sistemleri, bilgisayar kontrollü makineler, otonom araçlar, robot makineler, robot insanımsılar, ev otomasyon sistemleri, tavsiye sistemleri, özellikle İnternet üzerinden insan kullanıcılarla konuşmayı simüle etmek için tasarlanmış bilgisayar programları gibi teknolojilerde kullanılmaktadır. Bu teknolojiler gün geçtikçe insan davranışlarını daha fazla kopyalayarak ve insan hatalarını minimize ederek daha fazla bilgiyi daha hızlı analiz etmeye, internete bağlı diğer şeylerle daha fazla bilgi alışverişinde bulunmaya başladığından her geçen gün daha da yaygınlaşmaktadır.

Yapay zekâ sistemleri açısından da geçerli olacak kişisel verilerin işlenmesinde bazı temel ilkeler bulunmaktadır. Bunlar; hukuka ve dürüstlük kuralına uygun işlenmesi, doğru ve gerektiğinde güncel olma ilkesi, belirli, açık ve meşru amaçlar için işlenme ilkesi ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesidir. Hukuka ve dürüstlük kuralına uygun işlenmesi ilkesine göre kişisel verilerin işlenmesinde, veri sorumlularının ve veri işleyenlerin bu verileri dürüstlük kuralına uygun hareket ederek işleme yükümlülükleri bulunacaktır. Bunun yanı sıra kişisel verileri dürüstlük kuralına uygun işleme ilkesinin yorumlanmasında; veri sorumluları veya veri işleyenler tarafından, kişisel verileri işlemede kendilerine hukuka uygun olarak rıza gösteren bireylerin öngörebileceği biçimde hareket etmeleri gerekmektedir. Kişisel verilerin doğru olarak işlenmesi, güncel değilse güncellenmesini isteme hakkı gerek ilgili kişiler gerekse bu verilerin işlenmesinden sorumlu kişiler açısından büyük önem taşımaktadır. Ekseriyetle işlenen kişisel

verinin konusunun kişinin sağlığına yönelik veriler olduğu durumlarda, ortaya çıkması muhtemel maddi-manevi zararların ciddiyeti nedeniyle bu önem daha da artmaktadır. Ayrıca, ilgili kişinin kişisel verisinin işlenmesi, ilgili kişiyi olumsuz etkileyecek bir sonuç doğuruyorsa veri sorumlusu verilerin doğru ve güncel olması konusunda aktif özen göstermekle yükümlü tutulmaktadır. Belirli, açık ve meşru amaçlar için işlenme ilkesine göre kişisel verilerin işlenmesi ancak bu verilerin kişilerin açık rızalarının alınması ile veya yasalarda geçen haller çerçevesinde açık rızaya gerek kalmaksızın mümkün olabilecektir. Açık rıza gerektiren durumlarda kişinin açık rızasının yasalara uygun şekilde alınmış olabilmesi için verilerin işlenme amaçlarına yönelik olarak kişilerin doğru ve eksiksiz olarak bilgilendirilmiş olması gerekecektir. Bunun için de kişisel verilerin işlenme amaçları, kapsamı, sınırları ve işlenme süresinin bireylere açıkça belirtilmiş olması, verileri işlenecek kişiler bilgilendirilirken kullanılan aydınlatma/bilgilendirme/açık rıza gibi metinlerde ilgili kişi tarafından kolaylıkla anlaşılabilir terminolojik bir dilin kullanılması zorunlu olacaktır. Aksi halde, yani amaçların yeterince açık ve/veya belirli olmaması, veri sorumluları tarafından bu kişisel verilerin işlenmesi hususundaki sınırları belirsizleştireceğinden, bu ilkenin kişisel verilerin işlenmesindeki öneminin oldukça yüksek olduğu düşünülmektedir. Dolayısıyla, veri sorumlularının kişisel verileri işlemeleri, ilgili kişiye bildirdikleri amaçlarla sınırlıdır. Veri sorumlularının, bu amaçlar haricinde hangi sebeple olursa olsun kişisel verileri işlemeleri bu ilkeye ters düşeceğinden hukuken uygun değildir. Bir diğer deyişle belirli amaçlar dahilinde ilgili kişiden izni alınmış olan veri işleme faaliyetinin amaçları daha sonra genişletilir ise ve kişiden yeniden rıza alınmamış ise bu durum hukuka aykırı sayılacaktır. Öte taraftan, kişisel verilerin ilgili kişiden açık rıza alınmaksızın işlenmesi durumunda da amacın meşru, yani yasalara ve kurallara uygun olması gerekecektir. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi YZ sistemlerinde kişisel verilerin işlenmesi bakımından değerlendirildiğinde, yazılım geliştiricilerin YZ algoritmalarını geliştirirken bu algoritmaları, ihtiyaç duyacakları kişisel verilerin amaçla ilgili, sınırlı ve ne gereğinden fazla ne gereğinden az olacak şekilde modellemelerini, ona göre tasarımlarını ve bu ilkeye uygun veri işlemeyi YZ'lere öğretmelerini zorunlu kılmaktadır.

Kişisel verilere ilişkin bu ilkelere ek olarak şeffaflık ve ilgili kişileri bilgilendirme, hesap verebilirlik ve veri güvenliği gibi ilkeler de bulunmaktadır. Veri sorumlusunun ilgili kişiyi bilgilendirmede kısa, açık, sade, şeffaf, kolay ve anlaşılır bir

dil kullanması gerekmektedir. KVKK'da şeffaflık ve ilgili kişileri bilgilendirme ilkelerine ilişkin hükümlerin GDPR'de geçen hükümlerin tamamını karşılayamadığı görülmektedir. Hesap verebilirlik ilkesi, verilerin işlenmesi sırasında sağlamlık ve güvenin sağlanmasına yönelik olarak veri sorumlusuna yüklenen bir yükümlülüktür. Veri sorumlusunun; kişisel verilerin işlenmesi sırasında gereken tedbirleri alma ve talep edildiğinde en kısa süre içinde kişisel verilerin yasalarca daha önce belirlenmiş hükümlere uygun olarak işlendiğini kanıtlayan belge ve bilgilerin sunma, bunun yanı sıra hesap verebilirlik ilkesi doğrultusunda, veri işlemenin kanunda belirtilmiş diğer ilkelere de uygun olarak yürütülmesi sorumlulukları bulunmaktadır. YZ sistemlerinin kişisel verilerin korunmasını en çok ilgilendiren kullanımı ve bu konuda hesap verebilirliği en çok etkileyen husus, özel sektörden ziyade kamu kuruluşlarının yani hükümetlerin daha fazla düzeni sağlama kaygılarından ve dijital teknolojilere dayalı akıllı yönetim anlayışını daha fazla benimsemelerinden kaynaklanmaktadır. Akıllı yönetim, kamu idarelerinin sadece şeffaf olmalarını değil aynı zamanda YZ algoritmaları kullanarak aldıkları kararlardan da sorumlu olmalarını gerektirir. Hesap verebilirlik, YZ algoritmaları temelinde alınan kararları açıklama ve gerekçelendirme yükümlülüğünü ifade eder. Hesap verebilirlik yoluyla kamu idareleri, karar vermede YZ algoritmalarını kullanımlarını haklı çıkarmakta ve nasıl çalıştıklarını, hangi verileri kullandıklarını, hangi sonuçların beklendiğini ve hangi sonuçların elde edildiğini açıklamaktadırlar. Kişisel verilerin; doğal afet, siber saldırı, sistemsel arızalar, veri sisteminden sorumlu kişinin dalgın, dikkatsiz ve/veya tedbirsiz davranması veya yetkinin kötüye kullanımı gibi nedenlerle tehdit altında kalması da söz konusu olabilmektedir. Bu gibi tehditlere yönelik olarak gereken tedbirlerin alınmasında veri güvenliği ilkesi önem kazanmaktadır. Veri sorumlusu ve veri sorumlusunun kendi adına verileri işlemesine izin verdiği kişi/kişiler, kişisel verilere ilişkin hukuka uygun olmayacak şekilde işleme ve erişimin önlenmesi ile bu verilerin korunmasının sağlanması için gereken güvenliğin edinilmesine ilişkin tüm idari ve teknik tedbirlerin alınmasından sorumlu olup toplanan kişisel verilerin başkalarına açıklanmamasına ve işleme amaçları haricinde kullanılmamasına ilişkin bu yükümlülük ömür boyu devam eden bir yükümlülüktür.

YZ ve makine öğrenmesi alanındaki gelişmeler, kişilerin hak ve özgürlükleri üzerinde büyük etkileri bulunan profilleme ve otomatik karar alma mekanizmalarına yönelik kullanımlarda kolaylık ve yaygınlık sağlamaktadır. Profilleme veya profil oluşturma; bir gerçek kişiyle ilgili belirli kişisel yönleri değerlendirmek için kişisel

verilerin kullanılmasından oluşan, özellikle o gerçek insanın işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirlik, davranış, konum veya hareketlerle ilgili yönleri analiz etmek veya tahmin etmek için kullanılan, kişisel verilerin otomatik olarak işlenmesidir. Bu tanıma göre profillemeye; kişisel veri kullanan/işleyen, verileri otomatik işleyen ve bir gerçek kişi ile ilgili belirli kişisel yönleri değerlendirmek için kullanılan bir faaliyettir. Kural olarak, yasal veya benzer şekilde önemli bir etkiye sahip olan profillemeye dahil olmak üzere, tamamen otomatikleştirilmiş bireysel karar verme mekanizmaları genel olarak yasaktır. Ancak bu kuralın bazı istisnaları bulunmaktadır. Bu istisnalardan birinin geçerli olduğu durumlarda, ilgili kişinin hak ve özgürlüklerini ve meşru çıkarlarını korumak için tedbirler alınıyor olması söz konusu olmalıdır. Diğer yandan, otomatikleştirilmiş bireysel karar verme mekanizmalarına insan müdahalesi eklenmesi, kararın tamamen bir algoritma tarafından belirli kriterlere dayalı olarak alınması ve/veya bir insan etkisinin algoritmanın değerlendirdiği kriterler dışında başka kriterleri de değerlendirmeden algoritma kararını onaylaması ve/veya insan etkisinin işlevsel ve/veya anlamlı düzeyde olmaması halinde kararın tamamen otomatik karar alma mekanizmalarıyla alınmış olduğu gerçeğini değiştirmeyecektir ki bu da veri sorumlusunun bu konudaki yükümlülüklerini ve/veya ilgili kişinin bu konudaki haklarını ortadan kaldırmayacaktır. Bu istisnalar; kararın ilgili kişi ile veri sorumlusu arasında bir sözleşmeye girilmesi veya uygulanması için gerekli olması; kararın veri sorumlusunun tabi olduğu Birlik veya Üye Devlet yasaları tarafından yetkilendirilmesi ve veri konusunun hak ve özgürlüklerini ve meşru çıkarlarını korumak için uygun tedbirler getirmesi ve kararın ilgili kişinin açık rızasına dayanması hallerinde m.22/1'in hükümlerinin geçerli olmayacağı yönündedir. Yazında GDPR'nin otomatik karar alma mekanizmalarıyla ilgili bu düzenlemelerinin dar yorumlanma ve/veya sıkı bir biçimde uygulanma ihtimali nedeniyle büyük veri uygulamalarının beklenen yararlarının engellenebileceği konusunda endişe bildiren görüşler de bulunmaktadır.

Farklı hesaplama ve değerlendirmelerde kullanılan algoritmalar birçok insan aktivitesinde önemli bir rol oynamaktadır. Arama algoritmaları çevrimiçi bilgi arayışını yapılandırırken; işletme yönetimi sistemlerinde kullanılan algoritmalar çalışanların en iyi şekilde farklı görevlere ve vardiyalara nasıl tahsis edilmesi gerektiğine yardımcı olmaktadır. Birebir ticari iletişim platformlarında kullanılan algoritmalar, işgücü, beceri, bilgi ve maddi mallarda yeni tür geçici işlemlere izin verirken; trafik yönetimi gibi izleme sistemlerinde kullanılan algoritmalar olayların

tahmin edilmesine ve müdahale gerektirebilecek muhtemel durumların belirlenmesine yardımcı olmayı hedeflemektedirler. Arama, sıralama ve şifreleme algoritmalarıyla sınırlı olmamak üzere sayısız algoritma türü bulunmaktadır. İnternet üzerinden istenilen bilginin elde edilmesine yarayan arama motorlarında kullanılmasının yanı sıra gerek kişisel gerekse şirket bilgisayarlarında çevrimdışı olarak da arama yapmaya yardımcı olan arama algoritmalarının temeli istenilen bilgiye erişme, bilgiyi elde etme, bilginin geri getirilmesi fikrine dayanır. Sıralama algoritmaları; daha büyük bir öge kümesi içinden seçilen belirli sayıda bir kısa liste oluşturmayı sağlayan veya önceden belirlenmiş kriterlere göre bir dizi öğeyi sıralayan algoritmaları içerir. Hassas bilgilerin güvenliğini garanti altına almanın temel yollarından biri olan şifreleme algoritmaları ise, orijinal veri üzerinde çeşitli şifreleme ve dönüşümler gerçekleştirerek şifreli veriye dönüştürür. Kişisel verilerin korunması bağlamında şifreleme algoritmaları; takma adlandırma yani bir veri kaydındaki kişisel olarak tanımlanabilir bilgi alanlarının bir veya daha fazla yapay tanımlayıcı veya takma ad ile değiştirilmesi ve verinin şifrelenerek korunması açısından önemlidir.

Yapay zekâ sistemleri bakımından kişisel verilerin korunmasına ilişkin olarak, hakkında veri toplanan ilgili kişinin çeşitli hakları bulunmaktadır. Bunlar; bilgi edinme, düzeltme, sildirme hakkı, itiraz etme hakkı, profillemeye de dahil olmak üzere otomatik karar vermenin varlığı ve gerçekleştirilen işleme faaliyetinin kişi açısından önemi ve öngörülen sonuçları da dahil olmak üzere çalışma mantığına ilişkin anlamlı bilgilerin sunulması hakkı ve profillemeye, insan müdahalesi talep etme ve açıklama talep etme hakkıdır. Bilgi edinme, düzeltme, sildirme hakkı; kişisel veri işlenip işlenmediği, işleniyor ise bunlara yönelik bilgi verilmesi, bu verilerin hangi amaçla işlendiğini ve işlenmesinin amaca uygun olup olmadığını öğrenme, varsa bu bilgilerin aktarıldığı yerli ve yabancı kişileri öğrenme, bu verilerin yanlış işlenmesi durumunda düzeltilmelerini isteme, bu verilerin silinmesini ya da yok edilmesini talep etme, düzeltme, silme ve yok etme işlemlerinin ilgili üçüncü şahıslara da iletilmesini sağlama haklarını kapsamaktadır. Bilgi edinme, düzeltme, sildirme hakkı; GDPR’de kapsamlı ve bütünleyici istisnalarıyla birlikte düzenlenmişken, KVKK’da yeterli kapsamda değildir. Ayrıca KVKK’nın diğer maddelerinde belirtilen istisnalar ve diğer koşullar da bu hakkın kullanılabilmesini etkilemekte, kişisel verilerin silinmesine, yok edilmesine ya da anonimleştirilmesine yönelik diğer kanunlardaki hükümlerin saklı olduğu, bu konudaki usul ve esasların yönetmelik ile düzenlendiği belirtilerek bu

hakların ilgili kiři tarafından kullanılabilmesine geniş istisnalar getirilmektedir. İtiraz etme ve zararların giderilmesini isteme hakkı; verilerin işlenmesi sırasında özellikle otomatik sistemlerle analizinde ortaya çıkabilecek ilgili kiřinin aleyhine olacak sonuçlara itirazda bulunma ve bu verilerin kanuna uygun olmayan yol ve yöntemlerle işlenmesinden kaynaklı zararların giderilmesini isteme haklarını kapsamaktadır. Verileri toplanan ilgili kiřinin, kendisi hakkında profillemeye yapıldığına, bu verilerin değerlendirilmesinde bir otomatik karar alma mekanizması kullanılıp kullanılmadığına, bu sistemin nasıl çalıştığına, kişisel verileri bu yollarla işlemenin kiři açısından önemine ve kiřiye muhtemel etkilerine ilişkin veri sorumlusundan açıklama isteme hakkı bulunmaktadır. Bunun yanı sıra ilgili kiři, kendisi ile ilgili yasal etkiler veya ‘benzeri önemli etkiler’ yaratan, profil oluşturma dahil olmak üzere yalnızca otomatik işlemeye dayalı alınan bir karara tabi olmama, reddetme/itiraz etme hakkına da sahiptir. Profillemede kullanılan ve “benzer önemli etkiler” yaratan uygulamaların bir kısmının “özel nitelikli veriler”in tahmin edilmesinde kullanıldığı, yani profillemeye işlemi ile amaçlanan şeyin aslında kiřiyi önemli düzeyde etkileyebilecek “özel nitelikli verilerini” dolaylı yoldan toplama işlemi olduğu düşünülebilir. Çeřitli kuruluşları bu tür otomatik karar mekanizması uygulamalarını kullanmaya iten ana neden özel nitelikli kişisel veriler için açık rıza gerekmesi ve kişilerin böyle bir rızayı vermeye gönüllü olmayacaklarını düşünerek bu verileri başka yollarla (otomatik karar alan mekanizmalar sayesinde ÖNKV işlemeyen de ÖNKV verisi üretme) elde etmeye çalışmalarıdır. Kiřiyi önemli düzeyde etkileyebilecek diğerkonuların da dahil edilmesi gerekmektedir. Yine de doktrinde bu konuda yapılan tartışmaların son bulabilmesi için gerek GDPR’de gerekse 6698 sayılı KVK’da bu “benzeri önemli etkiler”in anlaşılabilmesi adına veri koruma otoriteleri tarafından rehberlerin, kararların ve mahkemeler tarafından kararların yayımlanması ve kriterlerin belirlenmesi ve örnek olayların üretilmesi gerekmektedir.

Kişisel verilere ilişkin hukuka uygun olmayacak şekilde işleme ve erişimin önlenmesi ile bu verilerin korunmasının sağlanması için gereken güvenliğin edinilmesine ilişkin tüm idari ve teknik tedbirlerin alınması gerekmektedir. Kişisel verilerin korunmasına ilişkin alınabilecek teknik tedbirler; eğitim verisinin minimizasyonuna ihtiyaç duyularak alınacak tedbirler (Üretken Düşmanca Ağlar, Birleşik Makine Öğrenimi ve Matris gibi) ve eğitim verisinin minimizasyonuna gerek duyulmadan alınabilecek tedbirler (Diferansiyel Gizlilik, Homomorfik Şifreleme, Transfer Öğrenimi, Bağımsız Disklerin Yedekli Dizisi gibi) şeklinde sıralanabilir.

Kişisel verilerin korunmasına ilişkin alınabilecek idari tedbirler ise VKED, ihlali riskinin yüksek olması hâlinde bu riskin kişisel verileri koruma kurumuna ve ilgili kişiye bildirimde bulunma zorunluluğu, tasarımdan itibaren kişisel verilerin korunması ve veri koruma görevlisi olarak sıralanabilir. VKED, bir proje veya değişikliğin veri koruma risklerini tanımlamada ve en aza indirmede kullanılan bir süreç olup veri işleme faaliyeti başlamadan önce kurumlar tarafından sürecin, hizmetin veya algoritmanın özel hayatın gizliliğini ihlal edip etmediğinin tespit edilmesine, ne gibi önlemler ve tedbirler alınabileceğinin belirlenmesine yardımcı olmaktadır. Ancak VKED'ye kişisel verilerin yeni kullanımını, süreci değiştirmeyi veya kişisel verilerin işlenme şeklini önemli ölçüde değiştirmeyi gerektiren belirli değişiklikler olduğunda başvurulması gerekmektedir. Veri sorumlularının kişisel verilerin işlenmesini veri koruma otoritelerine bildirme yükümlülüğü bulunurken, veri koruma otoritelerinin de özellikle yüksek ihlal riski taşıyan veriler başta olmak üzere veri koruma etkisi değerlendirmesi gerekliliğine tabi olan ve olmayan işlem türlerinin bir listesini oluşturma ve halka açıklama bu listeleri EDPB'ye bildirme yükümlülüğü bulunmaktadır. EDPB'nin ise kendi inisiyatifiyle veya EC'nin talebi üzerine kişisel veri ihlalinin gerçek kişilerin hak ve özgürlükleri açısından yüksek risk doğurabileceği durumlara ilişkin olarak kılavuz ilkeler, tavsiyeler ve en iyi uygulamaları yayınlama görevi bulunmaktadır. Kişisel verilerin tasarımdan itibaren korunması, gizlilik ve veri koruma konularını herhangi bir sistemin, hizmetin, ürünün veya sürecin tasarım aşamasında ve sonrasındaki yaşam döngüsü boyunca değerlendirmeyi sağlayan bir yaklaşım olup KVK konusunda başlı başına bir çözümdür. Tasarımdan itibaren kişisel verilerin korunmasına ilişkin GDPR'de bir düzenleme bulunurken KVKK'da bulunmamaktadır. Veri sorumlusunun, bir veri koruma etki değerlendirmesi yaparken, belirtilen durumlarda veri koruma görevlisinin tavsiyesini alması gerekir. Veri koruma görevlisinin bulunduğu görevlerde kanunun uygulanmasını, kontrol ve denetimi sağlamak, bilinçlendirme faaliyetleri, çalışanlara eğitim vermek ve ilgili kişilerle iletişimde bulunmak gibi kilit rolleri bulunmaktadır.

Genel olarak değerlendirildiğinde, 24 Mart 2016 tarihinde kabul edilerek 7 Nisan 2016 tarihinde Resmî Gazetede yayımlanan 6698 sayılı KVKK, kişisel verilerin korunmasının düzenlenmesinin yanı sıra aynı zamanda kişisel verilerle ilgilenen kişi veya kurumların uyması gereken birçok yeni zorunluluğu getirmesi yönüyle Türkiye'de türünün ilk örneğidir. Bu kanunun kabul edildiği 2016 yılına dek KVK, düzenlenmiş belirli sektörler haricinde Türkiye Cumhuriyeti Anayasasında tek

bir hüküm, TCK'da birkaç hüküm ve TMK'da kişilik hakları çerçevesindeki hükümler ile düzenlenmişti. Bu hükümlerin hiçbirisi giderek daha karmaşık hele gelen teknolojilerin ihtiyaçlarına ve her gün işlenen ve aktarılan kişisel veri miktarlarına yanıt vermede yeterli değildi. 6698 sayılı KVKK, değişen ve artan kişisel verilerin işlenmesine ilişkin gereksinimlere cevap vermeyi amaçlayan modern bir kanundur. Bu amaçla kanun, Türk mevzuatını AB mevzuatı ile uyumlu hale getirme yönünde önemli bir adımdır ve veri koruma konusunda 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Yönerge'ye dayanarak hazırlanmıştır. Ancak 6698 sayılı KVKK, 95/46/EC sayılı Yönerge'ye çok benzemekle birlikte tam bir kopyası değildir. Doktrinde, bu Kanunun 95/46/EC sayılı Yönerge'den farklı olan hükümlerinin bir kısmı, iyileştirmelerden ziyade eksiklikler şeklinde değerlendirilmektedir. Ayrıca 95/46/EC sayılı Yönerge, 24 Mayıs 2018 tarihinde yürürlükten kalkmıştır. Dolayısıyla 6698 sayılı KVKK'nın 27 Nisan 2016 tarihinde kabul edilip 25 Mayıs 2018 tarihinde yürürlüğe giren GDPR ile getirilen yeni hükümler çerçevesinde güncellenmesi gerekmektedir. Ayrıca, daha önce Türkiye'de bu konuda Anayasa'da tek bir hüküm, TCK'da birkaç hüküm ve TMK'da kişilik hakları çerçevesindeki hükümler dışında bir düzenleme olmadığı için KVKK'nın toplumun tüm kesimlerini alıştırarak ve veri koruma kültürü oluşturarak üst seviyeye çıkarılması uygun olacaktır. Son olarak, KVKK'ya yönelik yalnızca düzenlemeler yapılması da yeterli olmayacaktır. Güvenli bir ülke olabilmek için kanunun eksiksiz bir şekilde uygulanması da gerekmektedir.

KAYNAKÇA

- 4721 Sayılı Türk Medenî Kanunu (TMK): Kanun Numarası: 4721, Kabul Tarihi: 22/11/2001, Resmî Gazetede Yayımlandığı Tarih: 8/12/2001 ve Sayı: 24697. (Çevrimiçi) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.47_21.pdf 1 Aralık 2019.
- Abadi, Martín; Chu, Andy; Goodfellow, Ian; McMahan, H. Brendan; Mironov, Ilya; Talwar, Kunal; Zhang, Li: "Deep learning with differential privacy", Conference Paper, **2016 ACM SIGSAC Conference on Computer and Communications Security**, Vienna, Austria, October 24-28, 2016, (Çevrimiçi) <https://dl.acm.org/citation.cfm?id=2978318> 31 December 2019.
- Abrams, Martin: "The Origins of Personal Data and its Implications for Governance", The Information Accountability Foundation, 2014, (Çevrimiçi) <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf> 31 December 2019.
- Ağıralan, Erkan: "Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi", Yüksek Lisans Tezi, **T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü**, Ankara, 2015.
- Ajdari, Arian; Fenerci, Zeynep; Vural, Yılmaz; Canbay, Yavuz: "Büyük Genomik Verisinin Mahremiyetinin Korunarak İşlenmesi", **ISCTURKEY 2018**, 17-18 Ekim 2018, ss.26-31. (Çevrimiçi) https://www.iscturkey.org/assets/files/Bildiriler_kitab%C4%B1_2018_3.pdf 17 Aralık 2019
- Akıpek, Jale; Akıntürk, Turgut; Ateş, Derya: "Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku", **Beta Yayınları**, İstanbul, 2018.
- Akgün, Mete; Bayrak, A. Osman; Özer, Buğra; Sağıroğlu, M. Şamil: "Privacy preserving processing of genomic data: A survey", **Journal of Biomedical Informatics**, 2015, Vol.56, pp.103–111.
- Aksoy, Hüseyin Can: "Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması", **Çakmak Yayınevi**, Ankara, 2010, ss.58-59.
- Aksu, Mustafa: "Bilgisayar Programlarının Fikri Mülkiyet Hukukunda Korunması", **Beta Basım Yayım**, İstanbul, 2006.
- Altman, Andrew: "Discrimination", **The Stanford Encyclopedia of Philosophy**, Stanford University, August 30, 2015. (Çevrimiçi)

<https://plato.stanford.edu/entries/discrimination/> 31 December 2019

- Andreev, Alexei: "The Death of the Hypothesis, or, Investing in Big Data Analytics and Deep Learning", Harris and Harris Group, September 23, 2014. (Çevrimiçi) <http://www.hhvc.com/blog/death-hypothesis-investing-big-data-analytics-deep-learning/> 31 December 2019.
- Angwin, Julia; Larson, Jeff; Mattu, Surya; Kirchner, Lauren: "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks", **ProPublica**, May 23, 2016. (Çevrimiçi) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> 31 December 2019.
- Angwin, Julia; Parris Jr., Terry: "Facebook Lets Advertisers Exclude Users by Race", **PROPUBICA**, October 28, 2016. (Çevrimiçi) <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race> 31 December 2019.
- Angwin, Julia; Tobin, Ariana; Varner, Madeleine: "Facebook (Still) Letting Housing Advertisers Exclude Users by Race", **PROPUBICA**, November 21, 2017. (Çevrimiçi) <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin> 31 December 2019.
- Anyoha, Rockwell: "Can Machines Think?", **Harvard University**, (Çevrimiçi) <http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/> 31 Aralık 2019
- Article 29 Data Protection Working Party: "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", 17/EN, WP251rev.01, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 2018 (Çevrimiçi) https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826 7 December 2019, p.5.
- Article 29 Data Protection Working Party: "Guidelines on Data Protection Officers" As last Revised and Adopted on 5 April 2017, 2017 (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 8 January 2020.
- Association for Computing Machinery (ACM): "Statement on Algorithmic Transparency and Accountability", **ACM U.S. Public Policy Council & ACM Europe Policy Committee**, May 25, 2017. (Çevrimiçi) https://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf 31 December 2019.
- Aşıkoğlu, Şehriban İpek: "Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri", Yüksek Lisans Tezi, **İstanbul Üniversitesi**, İstanbul, 2018, s.142.
- Autorité de la Concurrence & Bundeskartellamt: "Algorithms and Competition", November 2019, pp.6-7, Germany & France, (Çevrimiçi) <https://www.autoritedelaconcurrence.fr/sites/default/files/algorithms-and-competition-summary.pdf> 5 December 2019.
- Avcıoğlu, Nur: "Türk Hukukunda Kişisel Verilerin Korunması Hakkı", Yüksek Lisans Tezi,

Halet:	KTO Karatay Üniversitesi , Konya, 2018.
Avrupa İnsan Hakları Mahkemesi (AİHM) (ECHR - European Court on Human Rights):	“Avrupa İnsan Hakları Sözleşmesi (The European Convention on Human Rights)”, 3 September 1953 (Çevrimiçi) https://www.echr.coe.int/Documents/Convention_TUR.pdf (Türkçe tercümesi), https://www.echr.coe.int/Documents/Convention_ENG.pdf (Orijinal versiyonu, İngilizce) 21 Kasım/November 2019.
Avrupa Komisyonu (EC - European Commission):	“Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması Sözleşmesi)”, Avrupa Birliği . 28 January 1981, (Çevrimiçi) https://rm.coe.int/1680078b37 19 November 2019.
Avrupa Komisyonu (EC - European Commission):	“Article 29 Working Party, Opinion 03/2013 On Purpose Limitation”, April 2, 2013, p.45 vd. (Online) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf 31 December 2019.
Avrupa Komisyonu (EC - European Commission):	“Draft Law for a digital Republic Impact assessment”, Avrupa Birliği . 24 November 2015, pp.1-8. (Çevrimiçi) http://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2015&num=627&iLang=EN 19 November 2019
Avrupa Parlamentosu (European Parliament):	“The Charter of Fundamental Rights of the European Union (7 Aralık 2000 tarih ve 2000/C 364/01 sayılı Avrupa Birliği Temel Haklar Bildirgesi)”, Avrupa Birliği , 7 December 2000 (Çevrimiçi) https://www.europarl.europa.eu/charter/pdf/text_en.pdf 23 November 2019.
Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe):	“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 (95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi)”, Avrupa Birliği . 24 October 1995 (Çevrimiçi) http://data.europa.eu/eli/dir/1995/46/oj 23 November 2019.
Avrupa Parlamentosu (European Parliament) ve Avrupa Konseyi (Council of Europe):	“Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data (GDPR - General Data Protection Regulation) (EU 2016/679 Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Gerçek Kişilerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Düzenlemesi (Genel Veri Koruma Düzenlemesi)), Avrupa Birliği . 27 April 2016 (Çevrimiçi)

- Europe): <http://data.europa.eu/eli/reg/2016/679/oj> 23 November 2019.
- Ayözger, Çiğdem: "Kişisel Verilerin Korunması – Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil", **Beta Yayınları**, İstanbul, 2016.
- Barocas, Solon: "Data mining and the discourse on discrimination", **Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining**, 2014. (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899 31 December 2019
- Baxter, Kathy: "Ethics in AI research papers and articles", Personal Blog, 19 November 2019, (Çevrimiçi) <https://blog.einstein.ai/ethics-in-ai-research-papers-and-articles/> 30 November 2019.
- Barocas, Solon; Selbst, Andrew D.: "Big data's disparate impact", **California Law Review**, Rev., Vol.104, 2016, pp.671-732.
- Bayamlioğlu, Emre: "Transparency of automated decisions in the GDPR: An attempt for systemisation", **SSRN**, January 7, 2018. (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097653 31 December 2019
- Bayamlioğlu, Emre: "Contesting Automated Decisions", **European Data Protection Law Review**, Vol.4, June 24, 2019, pp.433-446; Tilburg Law School Research Paper Forthcoming. **SSRN**, <https://ssrn.com/abstract=3305272> 31 December 2019.
- Bekri, M. Nedim: "Gerekçeli Karar Hakkı", **Ankara Barosu Dergileri**, Cilt.72, Sayı.3, 2014, ss.205-228. (Online) <http://www.ankarabaros.org.tr/siteler/ankarabaros/tekmakale/2014-3/6.pdf> 31 Aralık 2019)
- Bennett, Colin J.: "Regulating Privacy: Data Protection and Public Policy in Europe and the United States", **Cornell University Press**, Ithaca and London, 1992, (Çevrimiçi) https://books.google.com.tr/books?id=z6FhDwAAQBAJ&pg=PA59&lpg=PA59&dq=denmark+data+protection+1970%27s&source=bl&ots=scJlhhMOV_&sig=ACfU3U0Ymd_MSaLzMfgMbGedGbBSkCSdww&hl=tr&sa=X&ved=2ahUKEwjZvf3X5YDmAhWttIsKHW2VAE8Q6AEwAnoECAkQAQ#v=onepage&q=denmark%20data%20protection%201970's&f=false 3 November 2019.
- Berendt, Bettina: "More than modelling and hiding: towards a comprehensive view of Web mining and privacy", **Data Mining and Knowledge Discovery**, Vol.24, No.3, May 2012, pp.697-737
- Berendt, Bettina: "Better decision support through exploratory discrimination-aware data mining: foundations and empirical evidence", **Artificial Intelligence and**

- Preibusch, Sören: **Law**, Vol.22, No.2, 2014, pp.175-209.
- Binet, Alfred & Simon, Théodore: "The development of intelligence in children (the Binet-Simon scale)", In H.H. Goodard (Ed.), **Williams & Wilkins**, Baltimore, 1916.
- Binns, Reuben; Gallo, Valeria: "Automated Decision Making: The role of meaningful human reviews", **Information Commissioner's Office**, April 12, 2019. (Çevrimiçi) <https://ico.org.uk/about-the-ico/news-and-events/ai-blog-automated-decision-making-the-role-of-meaningful-human-reviews/> 31 December 2019.
- Birleşik Krallık Bilgi Komiserliği Ofisi (ICO - Information Commissioner's Office): "Big Data, Artificial Intelligence, Machine Learning and Data Protection", September 4, 2017, (Çevrimiçi) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> 31 December 2019.
- Birleşik Krallık Bilgi Komiserliği Ofisi (ICO - Information Commissioner's Office): "What methods can we use to provide privacy information", May 16, 2018. (Çevrimiçi) <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> 31 December 2019.
- Birleşik Krallık Bilgi Komiserliği Ofisi (ICO - Information Commissioner's Office): "Statement on the High Court judgement on the use of live facial recognition technology by South Wales Police", 4 September 2019 (Çevrimiçi) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/09/statement-high-court-judgement-frt-south-wales-police/> 10 October 2019.
- Birleşmiş Milletler Genel Kurulu (United Nations General Assembly) (45th sess.: 1990-1991): "Guidelines for the Regulation of Computerized Personal Data Files" (Bilgisayarlı Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Yönergeler), 14 Aralık 1990 (Çevrimiçi) <https://www.refworld.org/pdfid/3ddcafaac.pdf> 21 November 2019.
- Bolukbasi, Tolga; Chang, Kai-Wei; Zou, James; Saligrama, Venkatesh; Kalai, Adam: "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings", **Advances in Neural Information Processing Systems**, July 21, 2016. (Çevrimiçi) <https://arxiv.org/abs/1607.06520> 31 December 2019.

- Bond, Robert M.; Fariss, Christopher J.; Jones, Jason J.; Kramer, Adam D.I.; Marlow, Cameron; Settle, Jaime E.; Fowler, James H.: "A 61-million-person experiment in social influence and political mobilization", **Nature**, Vol.489, No.7415, 2012, pp.295–298.
- Borden, Bennett; Lee, Jessica; Ross, Alexandra; Hailemariam, Yodi: "Minority Report: The Ethics & Impacts of Algorithms", **MCCA Global Tec Forum**, 4-5 April, 2019, San Francisco, CA, (Çevrimiçi) <https://www.mcca.com/wp-content/uploads/2019/04/Minority-Report-The-Ethics-and-Impacts-of-Algorithms.pdf> 8 December 2019.
- Botsman, Rachel: "Big data meets Big Brother as China moves to rate its citizens", **Wired UK**, October 21, 2017. (Online) <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion> 31 December 2019.
- Brendan, McMahan; Ramage, Daniel: "Federated Learning: Collaborative Machine Learning without Centralized Training Data", 2017, April 6, <https://ai.googleblog.com/2017/04/federated-learning-collaborative.html> 11 December 2019.
- Brooks, Sean W.; Garcia, Michael E.; Lefkowitz, Naomi B.; Lightman, Suzanne; Nadeau, Ellen M.: "An Introduction to Privacy Engineering and Risk Management in Federal Systems", **National Institute of Standards and Technology (NIST)**, January 2017 (Çevrimiçi) <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf> 5 January 2020.
- Burt, Andrew: "The AI Transparency Paradox", **Harvard Business Review**, 13 Aralık 2019, (Çevrimiçi) <https://hbr.org/2019/12/the-ai-transparency-paradox> 31 December 2019.
- Burt, Andrew; Volchenbom, Samuel: "How Health Care Changes When Algorithms Start Making Diagnoses", **Harvard Business Review**, May 8, 2018, (Çevrimiçi) <https://hbr.org/2018/05/how-health-care-changes-when-algorithms-start-making-diagnoses> 31 December 2019.
- Calders, Toon; Žliobaitė, Indrė: "Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures", Discrimination and privacy in the information society. **Springer**, 2013, pp.43-57.
- Caliskan-Islam, Aylin; Bryson, "A Story of Discrimination and Unfairness Implicit Bias Embedded in Language Models", 2016. (Çevrimiçi)

- Joanna J.; Narayanan, A. R. Vijaya: <https://www.semanticscholar.org/paper/A-Story-of-Discrimination-and-Unfairness-Implicit-Caliskan-Islam-Bryson/6a0850123cefa90dbff00d2e0903bf99a9ec1c49> 31 December 2019
- Casacuberta, David: "Bias in a Feedback loop: Fuelling Algorithmic Justice", **Cultural Research and Innovation Lab**, May 9, 2018. (Çevrimiçi) <http://lab.cccb.org/en/bias-in-a-feedback-loop-fuelling-algorithmic-injustice/> 31 December 2019.
- Castelvecchi, Davide: "Can We Open the Black Box of AI?", **Nature**, November 5, 2016. (Çevrimiçi) <https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731> 31 December 2019.
- Cavoukian, Ann: "Privacy by design: 7 foundational principles", Information and Privacy Commissioner of Ontario, Canada, 2009, (Çevrimiçi) <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> 8 January 2020.
- Cerrillo i Martínez, Agustí: "How can we open the black box of public administration? Transparency and accountability in the use of algorithms", *Revista Catalana de Dret Public*, No.58, 2019, pp. 13–28, (Çevrimiçi) <http://revistes.eapc.gencat.cat/index.php/rcdp/article/download/10.2436-rcdp.i58.2019.3277/n58-cerrillo-en.pdf> 7 December 2019.
- Chen, Yongxi; Cheung, Anne S.Y.: "The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System", **The Journal of Comparative Law**, Vol.12, No.2, June 26, 2017, pp.356-378. (Çevrimiçi) <https://ssrn.com/abstract=2992537> 31 December 2019.
- Council of Europe: "Handbook on European Data Protection Law - 2014 Edition", (Çevrimiçi) https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf 11 October 2019.
- Corbett-Davies, Sam; Pierson, Emma; Feller, Avi; Goel, Sharad: "A Computer Program Used for Bail and Sentencing Decisions Was Labeled Biased Against Blacks. It's Actually Not That Clear", **Washington Post**, October 17, 2016. (Çevrimiçi) <https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas> 31 December 2019.
- Craven, Mark; Shavlik, Jude W.: "Extracting tree-structured representations of trained networks", Conference paper, **Conference on Advances in Neural Information Processing Systems**, 1996.
- Crawford, Kate; Schultz, Jason: "Big data and due process: Toward a framework to redress predictive privacy harms", **Boston College Law Review**, Vol.55, 2014, pp.93-128.

- Cuthbertson, Anthony: "China Invents Super Surveillance Camera That Can Spot Someone From Crowd of Thousands - Device's Resolution is Five-Times More Detailed Than Human Eye", The Independent, 2 October 2019, (Çevrimiçi) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/china-surveillance-camera-facial-recognition-privacy-a9131871.html> 30 November 2019.
- Çekin, Mesut Serdar: "Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu", **On İki Levha Yayıncılık**, İstanbul, 2018.
- Dash, Anil: "There is no "technology industry"", August 19, 2016, (Çevrimiçi) https://anildash.com/2016/08/19/there_is_no_technology_industry/ 31 December 2019
- Datta, Amit; Tschantz, Michael Carl; Datta, Anupam: "Automated experiments on ad privacy settings; a tale of opacity, choice, and discrimination", Conference paper, **Conference on Privacy Enhancing Technologies**, 2015, pp.92-112.
- Datta, Anupam; Sen, Shayak; Zick, Yair: "Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems", **IEEE symposium on security and privacy**, 2016. (Çevrimiçi) <https://www.andrew.cmu.edu/user/danupam/datta-sen-zick-oakland16.pdf> 31 December 2019.
- De-Arteaga, Maria; Romanov, Alexey; Wallach, Hanna; Chayes, Jennifer; Borgs, Christian; Chouldechova, Alexandra; Geyik, Sahin; Kenthapadi, Krishnaram; Kalai, Adam Tauman: "Bias in bios: A case study of semantic representation bias in a high-stakes setting." Conference paper. The Conference on Fairness, Accountability, and Transparency (ACM), January 27, 2019. (Çevrimiçi) <https://arxiv.org/abs/1901.09451> 31 December 2019.
- Desai, Deven R.; Kroll, Joshua A.: "Trust but verify: A guide to algorithms and the law", **Harvard Journal of Law & Technology**, Vol.31, 2017.
- Develioğlu, Hüseyin Murat: "6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku". **On İki Levha Yayıncılık**, İstanbul, 2017.
- Diakopoulos, "Principles for Accountable Algorithms and a Social Impact Statement for

- Nicholas;
Friedler, Sorelle;
Arenas, Marcelo;
Barocas, Solon;
Hay, Michael;
Howe, Bill;
Jagadish, H.V.;
Unsworth, Kris;
Sahuguet,
Arnaud;
Venkatasubrama
nian, Suresh;
Wilson, Christo;
Yu, Cong;
Zevenbergen,
Bendert:
- Algorithms”, **Fairness Accountability and Transparency in Machine Learning (FAT/ML)**, November 18, 2016 (Çevrimiçi) <https://www.fatml.org/resources/principles-for-accountable-algorithms> 31 December 2019.
- Dinkci, Fatih: “Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği”, Yüksek Lisans Tezi, **Ondokuz Mayıs Üniversitesi**, Samsun, 2014.
- Domingos, Pedro: “The Master Algorithm: How The Quest For The Ultimate Learning Machine Will Remake Our World”, **Basic Books**, New York, 2015.
- Doran, Derek;
Schulz, Sarah;
Besold, Tarek R.: “What does explainable AI really mean? A new conceptualization of perspectives”, October 2, 2017. (Çevrimiçi) <https://arxiv.org/abs/1710.00794> 31 December 2019.
- Doshi-Velez,
Finale; Kortz,
Mason; Budish,
Ryan; Bavitz,
Christopher;
Gershman,
Samuel J.;
O'Brien, David;
Shieber, Stuart;
Waldo, Jim;
Weinberger,
David; Wood,
Alexandra:
- “Accountability of AI Under the Law: The Role of Explanation”, Working Paper, **Berkman Klein Center Working Group on Explanation and the Law**, 2017. (Çevrimiçi) https://dash.harvard.edu/bitstream/handle/1/34372584/2017-11_aiexplainability-1.pdf?sequence=3 6 December 2019.
- Dressel, Julia;
Farid, Hany: “The accuracy, fairness, and limits of predicting recidivism”, **Science Advances**, Vol.4, No.1., 2018.

- Dölger, Murat
Volkan: "Kişisel Verilerin Korunması Hukuku", **Hukuk Akademisi**, İstanbul, 2018.
- Dwork, Cynthia: "Differential Privacy". ICALP 2006, Part II, **Springer-Verlag**, Berlin Heidelberg, 2006, pp.1–12
- Dwork, Cynthia;
Roth, Aaron: "The Algorithmic Foundations of Differential Privacy", **Foundations and Trends® in Theoretical Computer Science**, Vol.3-4, 2013. pp.1-277. (Çevrimiçi) <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf> 20 December 2019
- Ebbinghaus,
Hermann: "Psychology: An Elementary Text-book". M.F. Meyer (Ed.). **Heath**, Boston, 1908.
- Edwards, Lilian;
Veale, Michael: "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For", **16 Duke Law & Technology Review**, Vol.18, May 24, 2017, pp.18-84. (Çevrimiçi) <https://ssrn.com/abstract=2972855> 31 December 2019
- Ekonomik İşbirliği
ve Kalkınma
Örgütü (OECD -
Organization for
Economic
Cooperation and
Development): "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" **OECD** (Çevrimiçi) <http://www.oecd.org/sti/ieconomy/oecd-guidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm> (1980 version) <http://www.oecd.org/sti/ieconomy/privacy.htm> (2013 version) 20 November 2019.
- EPIC: "Algorithms in the Criminal Justice System: Pre-Trial Risk Assessment Tools", June 24, 2016. (Çevrimiçi) <https://epic.org/algorithmic-transparency/crim-justice/> 31 December 2019.
- EU Commission: "Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM (92) 422 final", October 18, 1992, (Online) <http://aei.pitt.edu/10375/1/10375.pdf> 31 December 2019.
- Eubanks,
Virginia: "Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor", **St Martin's Press**, 2018.
- European
Parliamentary
Research Service
(EPRS): "Understanding Algorithmic Decision-Making: Opportunities and Challenges", **Scientific Foresight Unit (STOA)**, PE 624.261, March 2019, (Çevrimiçi) [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) 31 December 2019
- European
Parliamentary
Research Service: "A governance framework for algorithmic accountability and transparency", **Scientific Foresight Unit (STOA)**, PE 624.262, April 2019, (Çevrimiçi) <https://www.europarl.europa.eu/RegData/etudes/STU>

- (EPRS): D/2019/624262/EPRS_STU(2019)624262_EN.pdf 31 December 2019
- Fisher, Elizabeth: "Transparency and Administrative Law: A Critical Evaluation", **Current Legal Problems**, Vol.63, No.1, 2010, pp.272–314. (Çevrimiçi) <https://doi.org/10.1093/clp/63.1.272> 31 December 2019.
- Floridi, Luciano: "Big Data and Their Epistemological Challenge", **Philosophy & Technology**, Vol.25, No.4, pp.435–437, (Çevrimiçi) <https://link.springer.com/content/pdf/10.1007%2Fs13347-012-0093-4.pdf> 31 December 2019.
- Fogel, David B.: "Defining Artificial Intelligence. In Evolutionary Computation: Toward a New Philosophy of Machine Intelligence", The Institute of Electrical and Electronics Engineers, Inc., **IEEE Press**, 2006.
- Fontana, David: "Psychology for Teachers", **Macmillan**, London, 1988.
- Fredrikson, Matt;
Jha, Somesh;
Ristenpart,
Thomas: "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures", Conference paper, 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015. (Çevrimiçi) <https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf> 31 December 2019.
- Gartner: "Information Technology, Gartner Glossary, Big Data", (Çevrimiçi) <http://www.gartner.com/it-glossary/big-data> 31 December 2019.
- Garvie, Clare: "Garbage In, Garbage Out. Face Recognition on Flawed Data", **GeorgeTown Law Center on Privacy&Technology**, May 16, 2019, (çevrimiçi) <https://www.flawedfacedata.com> 31 December 2019.
- Gemalmaz,
Haydar Burak: "Avrupa İnsan Hakları Sözleşmesinde Mülkiyet Hakkı", Doktora Tezi, **İstanbul Üniversitesi**, İstanbul, 2008.
- Gemalmaz,
Haydar Burak: "Avrupa İnsan Hakları Sözleşmesinde Mülkiyet Hakkı", **Beta Yayınları**, İstanbul, 2009.
- Gemalmaz,
Haydar Burak: "Avrupa İnsan Hakları Sözleşmesi Açısından Mülkiyet Hakkının Sınırlanmasında "Adil Denge" İlkesi", **İÜHFM**, Cilt.19, Sayı.1-2, 2011, ss.649-674.
- Gemalmaz,
Haydar Burak: "Mülkiyet Hakkı: Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 6", **Avrupa Konseyi**, Ankara, 2018, s.36
- Gerrish Legal: "The UK Court has issued a judgment on the use of live facial recognition technology by the police", 16 September 2019, (Çevrimiçi) <https://www.facebook.com/LegalBusinessPartner/posts/the-uk-court-has-issued-a-judgment-on-the-use-of-live-facial-recognition-technol/2682787115086668/> 10 October 2019.

- Gevers, Victor: “There is this company in China named SenseNets. They make artificial intelligence-based security software systems for face recognition, crowd analysis, and personal verification. And their business IP and millions of records of people tracking data is fully accessible to anyone.”, and “This database contains over 2.565.724 records of people with personal information like ID card number (issue & expire date, sex, nation, address, birthday, passphoto, employer and which locations with trackers they have passed in the last 24 hours which is about 6.680.348 records.”, **Twitter**, 13 February 2019 (Çevrimiçi) https://twitter.com/0xDUDE/status/10957025404_63820800/photo/1 20 November 2019.
- Gilbert, Francoise; Sotto, Lisa J.; Smedinghoff, Thomas J.: “Twentieth Annual Institute on Privacy and Data Security Law”, **Practising Law Institute (PLI)**, New York, 2019.
- Goldenfein, Jake: “Algorithmic Transparency and decision-making accountability: Thoughts for buying machine learning algorithms”, In Office of the Victorian Information Commissioner (Ed) **Closer to the Machine: Technical, Social, and Legal aspects of AI**, 2019. (Çevrimiçi) <https://poseidon01.ssrn.com/delivery.php?ID=75500606907000707700406802902210912405408102805005101712706808012500407306808807102705400001906202901701202107709410710909610301601303908008106400708406809608011309808600606611410310601906500016022123083104091018074123020090068083077013126071070114004&EXT=pdf> 31 December 2019.
- Goodfellow, Ian J.; Pouget-Abadie, Jean; Mirza, Mehdi; Xu, Bing; Warde-Farley, David; Ozair, Sherjil; Courville, Aaron; Bengio, Yoshua: “Generative Adversarial Nets”, Département d’informatique et de recherche opérationnelle **Université de Montréal**, France, 2014, (Çevrimiçi) <https://papers.nips.cc/paper/5423-generative-adversarial-nets.pdf> 10 December 2019.
- Goodman, Bryce; Flaxman, Seth: “European Union regulation on algorithmic decision-making and a “right to explanation”, **AI Magazine**, Vol. 38, No.3, 2017, pp.50-57.
- Göçmen-Uyarer, Sinem: “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması”, **Seçkin Yayınları**, Ankara, 2019.
- Gözübüyük, A. Şeref & Gölcüklü,

- Feyyaz: Ankara, 2009.
- Grimmelikhuijsen, Stephan; John, Peter; Meijer, Albert; Worthy, Ben: "Do Freedom of Information Laws increase transparency of government? A replication of a field experiment", **Journal of Behavioral Public Administration**, Vol.2, No.1, 2018, pp.1-10. (Çevrimiçi) <https://www.journal-bpa.org/index.php/jbpa/article/view/34> 31 December 2019.
- Göktürk, Kürşat: "Gerekçeli Karar Hakkı." **Ankara Barosu Dergisi**, Sayı.3, 2014, ss.1-224. (Çevrimiçi) <https://dergipark.org.tr/tr/download/article-file/398187> 31 December 2019)
- Gültekin, Nil Melek: "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Yüksek Lisans Tezi, **Galatasaray Üniversitesi**, İstanbul, 2012.
- Gürsel, İlke: "Protection of Personal Data in International Law and the General Aspects of The Turkish Law", **D.E.Ü. Hukuk Fakültesi Dergisi**, Cilt.18, Sayı.1, 2016, ss.33-61, (Çevrimiçi) <http://hukuk.deu.edu.tr/wp-content/uploads/2016/10/İLKE-GÜRSEL.pdf> 10 October 2019.
- H., E.: "How might your choice of browser affect your job prospects?", **The Economist**, April 11, 2013. (Çevrimiçi) <https://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-browser-affects-job-prospects> 31 December 2019.
- Hao, Karen: "There's an easy way to make lending fairer for woman. Trouble is, its illegal", **MIT Technology Review**, Nov 15, 2019. (Çevrimiçi) <https://www.technologyreview.com/s/614721/theres-an-easy-way-to-make-lending-fairer-for-women-trouble-is-its-illegal/> 31 December 2019.
- Harcourt, Bernard H.: "Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age", **University of Chicago Press**, 2007.
- Harvard Law Review: "State vs Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing." **Harvard Law Review**, March 10, 2017. (Çevrimiçi) <https://harvardlawreview.org/2017/03/state-v-loomis/> 31 December 2019.
- Hildebrandt, Mireille: "Defining Profiling: A New Type of Knowledge?", In M. Hildebrandt, and S. Gutwirth (Eds.), **Profiling The European Citizen**, Springer, 2008.
- Hildebrandt, Mireille: "Privacy as Protection of the Imcomputable Self: From Agnostic to Agnostic Machine Learning", **Theoretical Inquiries in Law**, Vol.20, No.1, 2019, p.101.
- Hill, Robin K.: "What an Algorithm Is", **Philosophy & Technology**, Vol.29, No.1, 2016, pp.35–59. (Çevrimiçi) <https://philpapers.org/rec/HILWAA> 31 December

2019.

- Hinton, Geoffrey; Sabour, Sara; Frosst, Nicholas: "Matrix capsules with em routing", Conference Paper, **ICLR 2018**, Toronto, Canada, 2018, (Çevrimiçi) <https://openreview.net/pdf?id=HJWLfGWRb> 12 December 2019.
- Hollyer, James R.; Rosendorff, B. Peter; Vreeland, James Raymond: "Democracy and Transparency", **The Journal of Politics**, Vol.73, No.4, 2011, pp.1191–1205 (Çevrimiçi) www.jstor.org/stable/10.1017/s0022381611000880 31 December 2019.
- Humphrey, Paul: "The philosophical novelty of computer simulation methods", **Synthese**, Vol.169, No.3, 2009, pp.615-626. (Çevrimiçi) https://pages.shanti.virginia.edu/Paul_Humphreys_Home_Page/files/2016/02/The-Philosophical-Novelty-of-Computer-Simulation-Methods.pdf 31 December 2019).
- International Association of Privacy Professionals" (IAPP): "From Here to DPO: Building a Data Protection Officer", (Çevrimiçi) https://iapp.org/media/pdf/resource_center/From_Here_to_DPO_FINAL.pdf 8 January 2020.
- International Association of Privacy Professionals" (IAPP): "Certification Scheme of Data Protection Officers From The Spanish Data Protection Agency (DPO-AEPD SCHEME)", (Çevrimiçi) https://iapp.org/media/pdf/resource_center/AEPD_DPO-Certification-Scheme.pdf 8 January 2020.
- International Working Group (IWG): "Working Paper on Privacy and Artificial Intelligence", 29-30 November 2018, **International Working Group on Data Protection in Telecommunications**, 64th Meeting, Queenstown (New Zealand), (Çevrimiçi) <https://epic.org/IWG/WP-AI.pdf> 9 December 2019.
- Irons, Meghan E.: "Caught in a dragnet", July 17, 2011, (Çevrimiçi) http://archive.boston.com/news/local/massachusetts/articles/2011/07/17/man_sues_registry_after_license_mistakenly_revoked/ 31 December 2019
- Işık, Muhittin: "Arama Motorları Mimarisi, Web Sayfalarının İçerik Skoru ve Google Pagerank Formülünün İncelenmesi", Yüksek Lisans Tezi, **Kadir Has Üniversitesi**, İstanbul, 2013, s.1.
- İngiltere Ulusal Sağlık Servisi (NHS – National Health Service): "Data Protection Impact Assessment (DPIA) Procedure", 2018, November 7. Ref: IT-0030-001-v1, (Çevrimiçi) <https://www.tewv.nhs.uk/content/uploads/2018/12/Data-Protection-Impact-Assessment-DPIA-Procedure.pdf> 14 December 2019.
- Jones Day: "Proposed Algorithmic Accountability Act Targets Bias in Artificial Intelligence", June 2019. (Çevrimiçi) <https://www.jonesday.com/en/insights>

/2019/06/proposed-algorithmic-accountability-act 8 January 2020.

- Joh, Elizabeth E.: "The undue influence of surveillance technology companies on policing", **NYU Law Review**, Vol.92, 2017, p.101.
- Kanada İnsan Hakları Komisyonu (CHRC - Canadian Human Rights Commission): "Human Rights in Canada". (Çevrimiçi) <https://www.chrc-ccdp.gc.ca/eng/content/human-rights-in-canada> 28 September 2019
- Karaduman, Ozan: "The New Personal Data Protection Law 2019 in Turkey", **Gün + Partners**, 14 February 2019 (Çevrimiçi) <https://gun.av.tr/tr/the-new-personal-data-protection-law-2019-in-turkey/> 24 November 2019
- Karwatzki, Sabrina; Dytnko, Olga; Trenz, Manuel; Veit, Daniel: "Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization", *Journal of Management Information Systems*, Vol.34, No.2, 2017, pp.369-400 (Çevrimiçi) <https://www.tandfonline.com/doi/abs/10.1080/07421222.2017.1334467> 31 December 2019
- Katyal, Sonia K.: "Private Accountability in the Age of Artificial Intelligence", **UCLA law Review**, Vol.66, 2019, pp.54-141, (Çevrimiçi) <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4064&context=facpubs> 8 January 2019.
- Kayser-Bril, Nicolas: "At least 10 police forces use face recognition in the EU", **AlgorithmWatch reveals**, December 11, 2019. (Çevrimiçi) <https://algorithmwatch.org/en/story/face-recognition-police-europe/> 31 December 2019.
- Kenny, Steve; Borking, John: "The Value of Privacy Engineering", **Journal of Information, Law & Technology (JILT)**, Vol.2002, No.1, 2002 (Çevrimiçi) https://warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/ 5 January 2020.
- Kişisel Verileri Koruma Kurumu: "Veri Sorumlusu Kimdir", 2017, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir> 14 Ekim 2019.
- Kişisel Verileri Koruma Kurumu: "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği", 2018, Resmî Gazetede Yayımlandığı Tarih: 10.03.2018 ve Sayı:30356, (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm> (16 Ekim 2019).

- Kişisel Verileri Koruma Kurumu: “Kişisel Verilerin İşlenmesine ilişkin Temel ilkeler”, 2018, ss.1-12, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesi-ne-Iliskin-Temel-Ilkeler> 2 Aralık 2019.
- Kişisel Verileri Koruma Kurumu: “Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi”, KVKK Yayınları, Ankara, 2018.
- Kişisel Verileri Koruma Kurumu: “Özel Nitelikli Kişisel Verilerin İşlenme Şartları”, 2018, ss.1-5, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari> 12 Ekim 2019.
- Kişisel Verileri Koruma Kurumu: “Veri Sorumlusu ve Veri İşleyen”, 2018, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf> 14 Ekim 2019.
- Kişisel Verileri Koruma Kurulu: “Facebook Hakkında Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Karar Özeti”, Karar Tarihi: 11/04/2019, Karar No: 2019/104, 10 Mayıs 2019 (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/5450/2019-104> 2 Aralık 2019.
- Kişisel Verileri Koruma Kurulu: “Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/82 sayılı Karar Özeti”, Karar Tarihi: 25/03/2019, Karar No: 2019/82, 2019 (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/5463/-Bir-market-zincirinin-sadakat-kart-uygulamasina-iliskin-ihbar-ve-sikayetler-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-25-03-2019-tarihli-ve-2019-82-sayili-Karari> 4 Aralık 2019.
- Kişisel Verilerin Korunması Kanunu (KVKK): Kanun Numarası: 6698, Kabul Tarihi: 24/3/2016, Resmî Gazetede Yayımlandığı Tarih: 7/4/2016 ve Sayı: 29677. 26 Eylül 2004 (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf> 23 Kasım 2019.
- Korkmaz, İbrahim: “Kişisel Verilerin Ceza Hukuku Kapsamında Korunması”, **Seçkin Yayıncılık**, Ankara, 2017.
- Kristian, Lum; William, Isaac: “To predict and serve?”, **Significance**, Vol.13, No.5, 2016, pp.14-19. (Çevrimiçi) <https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x> 31 December 2019.
- Kuner, Christopher: “The European Commission's proposed data protection regulation: A copernican revolution in European data protection law”, **Bloomberg BNA Privacy and Security Law Report**, February 6, 2012, pp.1-15 (Çevrimiçi) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2162781_code1213479.pdf?abstractid=2162781.&mirid=1 31 December 2019.
- Küzeci, Elif: “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, **İnsan Hakları Yıllığı**, Cilt.32, 2014, ss.53-75, (Çevrimiçi) <https://www.academia.edu/37176330/%C4%B0statistik%C3>

%AE_Birimler_ve_Bilgilerin_Gelece%C4%9Fini_Belirleme_
Hakk%C4%B1_Statistical_Units_and_Right_to_Information al_Self-
Determination 31 Aralık 2019.

- Küzeci, Elif: "Kişisel Verilerin Korunması", **Turhan Kitabevi**, Ankara, 2019.
- Langville, Amy N.; Meyer, Carl D.: "Google's PageRank and Beyond: The Science of Search Engine Rankings", **Princeton University Press**, Princeton, New Jersey, 2006, (Çevrimiçi) <http://geza.kzoo.edu/~erdi/patent/langvillebook.pdf> 8 December 2019.
- Lecuyer, Mathias; Spahn Riley; Spiliopolous, Yannis; Chaintreau, Augustin; Geambasu, Roxana; Hsu, Daniel: "Sunlight: Fine-grained targeting detection at scale with statistical confidence", Conference paper, **The 22nd ACM SIGSAC Conference on Computer and Communications Security**, 2015
- Leese, Matthias: "The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union", **Security Dialogue**, Vol.45, No.5, 2014, pp.494-511.
- Lefkovitz, Naomi: "The Preliminary Draft of the NIST Privacy Framework is Here!", **National Institute of Standards and Technology (NIST)**, 9 September 2019. (Çevrimiçi) <https://www.nist.gov/blogs/cybersecurity-insights/preliminary-draft-nist-privacy-framework-here> 8 January 2020.
- Li, Ting; Unger, Till: "Willing to pay for quality personalization? Trade-off between quality and privacy", **European Journal of Information Systems**, Vol.21, No.6, 2012, pp.621-642 (Çevrimiçi) <https://orsociety.tandfonline.com/doi/abs/10.1057/ejis.2012.13> 31 December 2019.
- Li, Yi; Vasconcelos, Nuno: "REPAIR: Removing Representation Bias by Dataset Resampling", Conference paper, **IEEE Conference on Computer Vision and Pattern Recognition**, April 16, 2019. (Çevrimiçi) <https://arxiv.org/pdf/1904.07911.pdf> 31 December 2019.
- Lundberg, Scott M.; Lee, Su-In: "A unified approach to interpreting model predictions", **Advances in Neural Information Processing Systems**, 2017, p.2, (Çevrimiçi) <http://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions.pdf> 31 December 2019.
- Lustig, Caitlin: "Algorithmic Authority of the Bitcoin Blockchain". Master's Thesis, **University of California**, Irvine, 2018, p.12 (Çevrimiçi)

<http://wtf.tw/ref/lustig.pdf> 6 December 2019.

- Lynskey, Dorian: "Alexa, are you invading my privacy?" – the dark side of our voice assistants", *The Guardian*, 9 October 2019, (Çevrimiçi) <https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants> 30 November 2019
- Lyon, David: "Surveillance as Social Sorting: Computer Codes and Mobile Bodies", In D. Lyon (Ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, pp.13–30, **Routledge**, New York, 2003.
- Malgieri, Gianclaudio: "Trade Secrets v Personal Data: a possible solution for balancing rights", **International Data Privacy Law**, Vol.6, No.2, 2016, pp.102-116.
- Malgieri, Gianclaudio; Comandé, Giovanni: "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", **International Data Privacy Law**, Vol.7, No.3, 2017, pp.243-265, (Çevrimiçi) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3088976_code2392402.pdf?abstractid=3088976&mirid=1 8 January 2020.
- Mantelero, Alessandro: "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment", **Computer Law & Security Review**, Vol.34, No.4, 2018, pp.754-772.
- Master of Science in Information Technology – Privacy Engineering (MSIT-PE) Institute for Software Research: (Çevrimiçi), <https://privacy.cs.cmu.edu> 5 January 2020.
- Matthias, Andreas: "The responsibility gap: Ascribing responsibility for the actions of learning automata", **Ethics and Information Technology**, Vol.6, No.3, 2011, pp.175–183 (Çevrimiçi) <https://link.springer.com/article/10.1007/s10676-004-3422-1> 31 December 2019.
- Mayer-Schonberger, Viktor: "Beyond Privacy, Beyond Rights- Toward a Systems Theory of Information Governance", **California Law Review**, Vol.98, 2010, ss.1853-1886, (Çevrimiçi) <https://schoharship.law.berkeley.edu/cgi/viewcontent.cgi?article=1058&context=californialawreview> 27 November 2019.
- Mayer-
- "Big Data: A Revolution That Will Transform How We Live, Work, And

- Schönberger, Viktor; Cukier, Kenneth: Think", **Houghton Mifflin Harcourt**, 2013.
- Mendos-Kuşkonmaz, Elif: "Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması", Yüksek Lisans Tezi, **İstanbul Üniversitesi**, İstanbul, 2013, s.19.
- Mendoza, Isak; Bygrave, Lee A. "The Right Not to Be Subject to Automated Decisions Based on Profiling", EU Internet Law, **Springer**, Cham, May 8, 2017, pp.77-98 (Çevrimiçi) <https://ssrn.com/abstract=2964855> 31 December 2019.
- Milli, Smitha; Schmidt, Ludwig; Dragan, Anca D.; Hardt, Moritz: "Model reconstruction from model explanations." Conference paper, **The Conference on Fairness, Accountability, and Transparency (ACM)**, 2019. (Çevrimiçi) <https://arxiv.org/pdf/1807.05185.pdf> 31 December 2019.
- Mittelstadt, Brent Daniel., Allo, Patrick, Taddeo, Mariarosaria, Wachter, Sandra, & Floridi, Luciano: "The ethics of algorithms: Mapping the debate", **Big Data & Society**, Vol.3, No.2, 2016, pp.1-21.
- Morrall, John F. III: "Regulatory Impact Analysis: Efficiency, Accountability, and Transparency", **Conference of the APEC-OECD Co-operative Initiative on Regulatory Reform**, Singapore, 2001. (Çevrimiçi) <http://www.oecd.org/governance/regulatory-policy/1901526.doc> 31 December 2019.
- Morris, Natalie: "What is unconscious name bias and why is it so damaging?", **Metro News**, 17 September 2019, (Çevrimiçi) <https://metro.co.uk/2019/09/17/unconscious-name-bias-damaging-10757825/?ito=cbshare> 30 November 2019
- Naden, Clare: "Tackling Privacy Information Management Head On: First International Standard Just Published", **International Organization for Standardization (ISO)**, 6 August 2019, (Çevrimiçi) <https://www.iso.org/news/ref2419.html> 8 January 2020.
- Ng, Irene: "Personal Data as Currency", 28 July 2018, (Çevrimiçi) <https://medium.com/hub-of-all-things/personal-data-as-currency-ab1590163ad6> (25 November 2019).
- O'Neill, Onora: "Reith Lectures 2002: A Question of Trust Lecture 4: Trust and Transparency", 27 April, 2002. (Çevrimiçi) http://downloads.bbc.co.uk/rmhttp/radio4/transcripts/20020427_reith.pdf 31 December 2019.

- O'Neil, Cathy: "Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy", **Broadway Books**, 2016.
- Obermeyer, Ziad; Powers, Brian; Vogeli, Christine; Mullainathan, Sendhil: "Dissecting racial bias in an algorithm used to manage the health of populations", **Science**, Vol.366, October 25, 2019, pp.447-453. (Çevrimiçi) <https://science.sciencemag.org/content/366/6464/447> 31 December 2019.
- Office of the Australian Information Commissioner: "Guide to Big Data and The Australian Privacy Principles", March 21, 2016. (Çevrimiçi) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/#s2-3-notification-app-5>, 1 Ocak 2020.
- Oxford Advanced Learner's Dictionary & Oxford Advanced American Dictionary: "Artificial intelligence", (Çevrimiçi) <https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence?q=artificial+intelligence> 13 November 2019.
- Özyürek, Öykü: "Kişilik Haklarına Saldırı Nedeniyle Manevi Tazminat", **İstanbul Bilgi Üniversitesi**, İstanbul, 2019.
- Pasquale, Frank: "The Black Box Society: The Secret Algorithms that Control Money and Information", **Harvard University Press**, 2015.
- Perry, Walter L.; McInnis, Brian; Price, Carter C.; Smith, Susan C.; Hollywood, John S.: "Predictive policing: The role of crime forecasting in law enforcement operations", **Rand Corporation**, 2013 (Çevrimiçi) https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf 31 December 2019.
- Prins, Corien: "Property and Privacy: European Perspectives and the Commodification of Our Identity", **Information Law Series**, Vol.16, 2006. pp.223-257.
- Purtova, Nadezhda: "Property Rights in Personal Data: Learning from the American Discourse" **Computer Law & Security Review**, Vol.25, No.6, 2009, ss.507-521, (Çevrimiçi) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1554341_code1337775.pdf?abstractid=1554341&mirid=1 (27 November 2019).
- Rabess, Cecilia Esther: "Can big data be racist?", **The Bold Italic**, March 31, 2014, (Çevrimiçi) <http://www.thebolditalic.com/articles/4502-can-big-data-be-racist> 31 December 2019.
- Rainey, Bernadette: "Jacobs, White and Ovey: the European Convention on Human Rights",

- Wicks, Elizabeth; Ovey, Clare; **Oxford University Press**, Oxford, 2017.
- Reidenberg, Joel R.: "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?", **Fed. Comm. L. J.**, No.44, 1992, pp.195-243. (Çevrimiçi) <https://pdfs.semanticscholar.org/5f5f/2fd2ff989226bd4a7a0e05c614fd7ad09a18.pdf> 18 November 2019
- Reilly, Michael: "Prediction Models Gone Wild: Why Election Forecasts and Polls Were So Wrong", **MIT Technology Review**, Nov 9, 2016. (Online) <https://www.technologyreview.com/s/602829/prediction-models-gone-wild-why-election-forecasts-and-polls-were-so-wrong/> 31 December 2019.
- Rajkoma, Alvin; Oren, Eyal; Chen, Kai; Dai, Andrew M.; Hajaj, Nissan; Hardt, Michaela; ... Dean, Jeffrey: "Scalable and accurate deep learning with electronic health records", **NPJ Digital Medicine**, Vol.1, No.1, 2018. (Çevrimiçi) <https://www.nature.com/articles/s41746-018-0029-1#citeas> 31 December 2019.
- Reisman, Dillon; Schultz, Jason; Crawford, Kate; Whittaker, Meredith: "Algorithm Impact Assessment: A Practical Frameworks for Public Agency Accountability", **AI Now Institute**, April 2018, (Çevrimiçi) <https://ainowinstitute.org/aiareport2018.pdf> 8 January 2019.
- Ribeiro, Marco Tulio; Singh, Sameer; Guestrin, Carlos: "Why should i trust you?: Explaining the predictions of any classifier." Conference paper. **The 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, August 9, 2016. (Çevrimiçi) <https://arxiv.org/abs/1602.04938> 31 December 2019.
- Ribeiro, Marco Tulio; Singh, Sameer; Guestrin, Carlos: "Anchors: high precision model-agnostic explanations", Conference paper, **Thirty second AAAI Conference on Artificial Intelligence**, 2018.
- Roberts, Andrew & Taylor, Nick: "Privacy and the DNA Database", **EHRLR**, 2005, No.4, pp.373-392.
- Robinson, David G.: "The challenges of prediction: Lessons from criminal justice", **IS: A Journal of Law and Policy for the Information Society**, Vol.14, No.2, 2017, p.151.
- Robinson David; Yu, Harlan; Rieke, Aaron: "Civil Rights, Big Data, and Our Algorithmic Future". **Social Justice and Technology**, September 2014. (Online) https://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf 31 December 2019.

- Rossi, Francesca: "A Definition of AI: Main Capabilities and Scientific Disciplines", High-Level Expert Group on Artificial Intelligence, 22 March 2019, (Çevrimiçi) http://www.pcci.gr/evepimages/0101_F483.pdf 30 November 2019.
- Ryan, Johnny: "Update on GDPR complaint (RTB ad auctions)", **Brave Insights**, Jan 28, 2019, (Çevrimiçi) <https://brave.com/update-rtb-ad-auction-gdpr/> 31 December 2019.
- Rygielski, Chris; Wang, Jyun-Cheng; Yen, David C.: "Data mining techniques for customer relationship management", **Technology in Society**, Vol.24, No.4, 2002, pp. 483–502 (Çevrimiçi) <https://www.sciencedirect.com/science/article/pii/S0160791X02000386?via%3Dihub> 31 December 2019.
- Salian, Isha: "Supervize Me: What's the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning", August 2, 2018, (Çevrimiçi) <https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/> 31 December 2019.
- Samuelson, Pamela: "Privacy as Intellectual Property", **Stanford Law Review**, Vol.52, 1999, p.1125-1173, (Çevrimiçi) <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3137&context=facpubs> 4 November 2019
- Sanders, James & Patterson, Dan: "Facebook data privacy scandal: A cheat sheet", 24 July 2019, (Çevrimiçi) <https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/> 20 November 2019.
- Sandvig, Christian: "Auditing algorithms: Research methods for detecting discrimination on internet platforms", **Data and discrimination: Converting critical concerns into productive inquiry**, 22 May 2014.
- Sandvig, Christian: "Seeing the Sort: The Aesthetic and Industrial Defence of "the Algorithm", **Journal of the New Media Caucus**, 2015. (Çevrimiçi) <http://median.newmediacaucus.org/art-infrastructures-information/seeing-the-sort-the-aesthetic-and-industrial-defense-of-the-algorithm/> 31 December 2019.
- Sandvine, "The Global Internet Phenomena Report", September 2019 (Online) https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/Internet%20Phenomena/Internet%20Phenomena%20Report%20Q32019%2020190910.pdf 31 December 2019.
- Schermer, Bart W.: "The limits of privacy in automated profiling and data mining", **Computer Law & Security Review**, Vol.27, No.1, 2011, pp. 45–52, (Çevrimiçi) <https://www.infona.pl/resource/bwmeta1.element.elsevier-a860e641-825f-3a79-9385-b2b5af42c740> 31 December 2019.
- Schwartz, John: "Giving the Web a Memory Cost Its Users Privacy", September 4, 2001. (Çevrimiçi) <https://pdfs.semanticscholar.org/77c3/88be3f57c80889e529>

1dc103f8f375718f56 .pdf 31 December 2019.

- Schwartz, Paul M.: "Property, Privacy and Personal Data", **Harvard Law Review**, Vol.117, 2004, pp.2056-2128, (Çevrimiçi) <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3150&context=facpubs> (12 November 2019).
- Seçkin, Sinan; Üstün, Gül: "İdari İşlemlerde Takdir Yetkisi ve Gerekçe İlkesi", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.21, Sayı.2, 2015, ss.509-534. (Çevrimiçi) http://dspace.marmara.edu.tr/bitstream/handle/11424/5910/2020__LEMLERDE%20TAKD__R%20YETK__S__%20VE%20GEREK__E%20__LKES__%5b%23289900%5d-273387.pdf?sequence=1&isAllowed=y 31 Aralık 2019.
- Selbst, Andrew; Powles, Julia: "Meaningful information and the right to explanation", **International Data Privacy Law**, Vol.7, No.4, November 2017, pp.233–242.
- Sentas, Vicki; Pandolfini, Camilla: "Policing young people in NSW: A study of the suspect targeting management plan", A Report of the Youth Justice Coalition, **NSW**, 2017, (Çevrimiçi) <https://www.piac.asn.au/wp-content/uploads/2017/10/17.10.25-YJC-STMP-Report.pdf> 31 December 2019
- Shokri, Reza; Strobel, Martin; Zick, Yair: "Privacy Risks of Explaining Machine Learning Models", arXiv preprint, December 4, 2019. (Çevrimiçi) <https://arxiv.org/abs/1907.00164> 31 December 2019.
- Singh, Atul: "Protecting Personal Data as a Property Right ", **ILI Law Review**, Winter Issue, 2016, pp.123-139, (Çevrimiçi) http://ili.ac.in/pdf/p9_atul.pdf 4 November 2019.
- Singh, Gurpreet; Supriya, Supriya: "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", **International Journal of Computer Applications**, Vol.67, 2013, No.19, pp.33–38 (Çevrimiçi) <https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf> 8 December 2019.
- SKW Schwarz: "The New German Federal Data Protection Act", SKW Schwarz IT-Ticker - Special Issue, 7 January, 2017. (Çevrimiçi) https://www.skwschwarz.de/fileadmin/user_upload/Artikel_Dokumente/BDSG-neu_2017-06-07_EN.pdf 31 December 2019.
- Slack, Dylan; Hilgard, Sophie; Jia, Emily; Singh, Sameer; Lakkaraju, Himabindu: "How can we fool LIME and SHAP? Adversarial Attacks on Post hoc Explanation Methods", November 6, 2019. (Çevrimiçi) <https://arxiv.org/abs/1911.02508> 31 December 2019.

- Solove, Daniel J.: "A brief history information privacy law", GWU Law School Public Law Research Paper No. 215, **Proskauer on Privacy, PLI**, 2016, p.25, (Çevrimiçi) https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications 8 January 2020.
- Stalla-Bourdillon, Sophie; Leong, Brenda; Hall, Patrick; Burt, Andrew: "Warning Signs. The Future of Privacy and Security in an Age of Machine Learning", **Future of Privacy Forum**, September 2019. (Çevrimiçi) https://fpf.org/wp-content/uploads/2019/09/FPF_WarningSigns_Report.pdf 31 December 2019
- Stanovich, Keith E.: "Assessing Cognitive Abilities: Intelligence and More", **Journal of Intelligence**, Vol.2, No.1, 2014, pp.8–11, (Çevrimiçi) http://www.keithstanovich.com/Site/Research_on_Reasoning_files/Stanovich_JOI.pdf 27 November 2019.
- Suresh, Harini; Gutttag, John V.: "A Framework for Understanding Unintended Consequences of Machine Learning", arXiv preprint, January 28, 2019. (Çevrimiçi) <https://arxiv.org/abs/1901.10002> 31 December 2019.
- Şimşek, Oğuz: "Anayasa Hukukunda Kişisel Verilerin Korunması", **Beta Basım Yayın**, İstanbul, 2008.
- Sweeney, Latanya: "Discrimination in Online Ad Delivery", arXiv preprint, 2013, (Çevrimiçi) <https://arxiv.org/abs/1301.6822> 31 December 2019
- Taneja, Hemant: "The need for algorithmic accountability", September 8, 2016. (Çevrimiçi) <https://techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/> 31 December 2019.
- Taştan, Furkan Güven: "Türk Sözleşme Hukukunda Kişisel Verilerin Korunması", Onikilevha Yayınları, İstanbul, 2017.
- Taylor, Josh: "Major breach found in biometrics system used by banks, UK police and defence firms." **The Guardian**, 14 August 2019, (Çevrimiçi) <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms> 20 November 2019.
- The Economist: "Regulating the internet giants - The world's most valuable resource is no longer oil, but data", 6 May 2017, (Çevrimiçi) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (25 November 2019).

- The Office of the High Commissioner for Human Rights (UN Human Rights) (OHCHR): “Guiding Principles on Business and Human Rights”, **United Nations, Human Rights Council, Office of The High Commissioner**, 2011, pp.23–26., (Çevrimiçi) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf 8 January 2020.
- The University of Roehampton: “Guide to the General Data Protection Regulation GDPR 1.0 - Data protection by design and default”, London, 2018, August 2. (Çevrimiçi) <https://www.roehampton.ac.uk/globalassets/documents/ethics/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> 19 December 2019.
- Thomas, Rachel: “16 Things You can Do to Make Tech More Ethical, part 1”, April 22, 2019. (Çevrimiçi) <https://www.fast.ai/2019/04/22/ethics-action-1/#risks-sweep> 31 December 2019.
- Tikkinen-Piri, Christina; Rohunen, Anna; Markkula, Jouni: “EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies”, **Computer Law & Security Reviews**, Cilt.34, Sayı.1, 2018, pp.134-153.
- Tramèr, Florian; Zhang, Fan; Juels, Ari; Reiter, Michael K.; Ristenpart, Thomas: “Stealing machine learning models via prediction apis”, **25th USENIX Security Symposium**, 2016. (Çevrimiçi) <https://arxiv.org/pdf/1609.02943.pdf> 31 December 2019.
- Tu, Stephen: “Lecture 20: Introduction to Differential Privacy”, **Advanced Topics in Data Processing**, Fall 2013, (Çevrimiçi) <https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf> 15 December 2019.
- Tutt, Andrew: “An FDA for Algorithms”, **69 Administrative Law Review**, Vol.83, 2017. (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=27479 31 December 2019.
- Türk Ceza Kanunu (TCK): Kanun Numarası: 5237, Kabul Tarihi: 26/9/2004, Resmî Gazetede Yayımlandığı Tarih: 12/10/2004 ve Sayı: 25611. 26 Eylül 2004 (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf> 23 Kasım 2019.

- Türkiye Büyük Millet Meclisi (TBMM): “Türkiye Cumhuriyeti Anayasası”, Kanun Numarası: 2709, Kabul Tarihi: 18/10/1982, Resmî Gazetede Yayımlandığı Tarih: 9/11/1982 ve Sayı: 17863. 21/1/2017 tarihli ve 6771 sayılı Kanun ile yapılan Anayasa değişikliklerinin kabul edildiği tarih: 16/4/2017, bu değişikliklerin Resmî Gazetede Yayımlandığı Tarih: 27/4/2017 ve Sayı: 30050 Mükerrer Sayı. 27 Nisan 2017 (Çevrimiçi) <https://www.anayasa.gov.tr/tr/mevzuat/anayasa/> 24 Kasım 2019.
- Van Haastert, Hugo: “Government as a Platform: Public Values in the Age of Big Data”, **Oxford Internet Institute**, 2016. (Çevrimiçi) <http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/Government%2520as%2520a%2520Platform%2520-%2520Big%2520data%2520paper.pdf> 31 December 2019.
- Van Otterlo, Martijn: “A Machine learning view on profiling”, In M. Hildebrandt, and K. de Vries (Eds.), *Privacy, Due Process and the Computational Turn - The Philosophy of Law Meets the Philosophy of Technology*, pp. 41–64, 2013, (Çevrimiçi) https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf 27 November 2019.
- Vinge, Vernor: “The coming technological singularity: How to survive in the post-human era”, **Science Fiction Criticism: An Anthology of Essential Writings**, 1993, pp.352-363.
- Yang, Hongyu; Rudin, Cynthia; Seltzer, Margo: “Scalable Bayesian Rule Lists”, **Proceedings of the 34th International Conference on Machine Learning**, Vol.70, 2017, (Çevrimiçi) <https://arxiv.org/abs/1602.08610> 31 December 2019.
- Wagner, Ben: “Efficiency vs. Accountability? – Algorithms, Big Data and Public Administration”, December 2016. (Çevrimiçi) <https://cihr.eu/efficiency-vs-accountability-algorithms-big-data-and-public-administration/> 31 December 2019.
- Wang, Bolun; Yao, Yuanshun; Viswanath, Bimal; Zheng, Haitao; Zhao, Ben Y.: “With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning”. **27th USENIX Security Symposium**, USENIX Association, August 15–17, 2018, Baltimore, MD, USA, pp.1281-1297. (Çevrimiçi) <https://people.cs.uchicago.edu/~ravenben/publications/pdf/transfer-learning-usenixsec18.pdf> 26 December 2019.
- Wang, Cunrui; Zhang, Qingling; Liu, Wanquan; Liu, Yu; Miao, Lixin: “Facial feature discovery for ethnicity recognition”, **Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery**, Vol.9, No.1, 2019. (Çevrimiçi) <https://onlinelibrary.wiley.com/doi/full/10.1002/widm.1278> 31 December 2019.

- Wang, Pei: "What Do You Mean by "AI"?", In P. Wang, B. Goertzel, and S. Franklin (Eds.), *Artificial General Intelligence 2008*, Proceedings of the First AGI Conference, *Frontiers in Artificial Intelligence and Applications*, No.171, pp.362–373. IOS Press Amsterdam, The Netherlands, 2008, (Çevrimiçi) https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf 27 November 2019.
- Warren, Samuel D.; Brandeis, Louis D.: "The Right to Privacy", **Harvard Law Review**, Vol.4, No.5, December 15, 1890, pp.193-220 (Çevrimiçi) <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> 8 December 2019.
- Wachter, Sandra; Mittelstadt, Brent; Floridi, Luciano; "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", **International Data Privacy Law**, Vol.7, No.2, 2017, pp.76-99.
- Wexler, James; Pushkarna, Mahima; Bolukbasi, Tolga; Wattenberg, Martin; Viegas, Fernanda; Wilson, Jimbo: "The What-If Tool: Interactive Probing of Machine Learning Models", **IEEE Transactions on Visualization and Computer Graphics**, Vol.26, No.1, 2019, pp.56-65. (Çevrimiçi) <https://arxiv.org/pdf/1907.04135.pdf> 31 December 2019.
- Willems, Tom; Van Dooren, Wouter: "Coming to terms with accountability: Combining multiple forums and functions", **Public Management Review**, Vol.14, No.7, 2012, pp.1011-1036.
- Winston, Ali: "Palantir has secretly been using New Orleans to test its predictive policing technology", **The Verge**, February 27, 2018. (Çevrimiçi) <https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd> 31 December 2019
- Winston, Patrick Henry: "Artificial Intelligence", Addison-Wesley Publishing Company, 1992, (Çevrimiçi) <https://courses.csail.mit.edu/6.034f/ai3/rest.pdf> 27 November 2019.
- Vries, Katya: "Identity, profiling algorithms and a world of ambient intelligence", **Ethics and Information Technology**, Vol.12, No.1, 2010, pp.71–85.

- Yeung, Karen: "A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility Within a Human Rights Framework", **Council of Europe**, November 9, 2018. MSI-AUT (2018) 05, (Çevrimiçi) https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3286027_code830937.pdf?abstractid=3286027&mirid=1 8 January 2020.
- Yeung, Karen: "Design for Regulation" in M.J. Van Den Hoven, P.E. Varmaas, I. van de Poel (Eds.) *Handbook of Ethics, Values and Technological Design*, **Springer**, 2015. pp.447-472.
- Yılmaz, Berrak: "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", Doktora Tezi, **Hacettepe Üniversitesi**, Ankara, 2019.
- Zarsky, Tal Z.: "Incompatible: The GDPR in the Age of Big Data", **Seton Hall Law Review**, Vol.47, No.4, 2017, pp.995-1020.
- ZNetLive: "How to choose the right RAID for your Dedicated Server", 2016, pp.1-6. (Çevrimiçi) https://www.znetlive.com/pdf/How_to_choose_the_right_RAID_for_your_Dedicated_Server.pdf 27 December 2019.
- Zednik, Carlos: "Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence", March 3, 2019, (Çevrimiçi) arXiv preprint arXiv:1903.04361 31 December 2019.