

**E-TİCARET SEKTÖRÜNDE KULLANILAN YAPAY ZEKA UYGULAMALARI
KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI**

Yüksek Lisans Tezi

Rümeysa TEKİN

Eskişehir 2025

**E-TİCARET SEKTÖRÜNDE KULLANILAN YAPAY ZEKA UYGULAMALARI
KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI**

RÜMEYSA TEKİN

YÜKSEK LİSANS TEZİ

Özel Hukuk Anabilim Dalı

Özel Hukuk Programı

Danışman: Prof. Dr. MESUT AYGÜN

Anadolu Üniversitesi

Lisansüstü Eğitim Enstitüsü

Temmuz 2025

Eskişehir

JÜRİ VE ENSTİTÜ ONAYI

.....'nın “.....” başlıklı tezi .../.../20.. tarihinde aşağıdaki jüri tarafından değerlendirilerek “Anadolu Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca, ... Ana Bilim/Ana Sanat dalında Programında Yüksek Lisans/Doktora/Sanatta Yeterlik tezi olarak kabul edilmiştir.

	<u>Ünvanı Adı Soyadı</u>	<u>İmza</u>
Üye (Danışman)	:	
Üye	:	
Üye	:	
Üye	:	
Üye	:	

.....
Lisansüstü Eğitim Enstitüsü Müdürü

ÖZET

E-TİCARET SEKTÖRÜNDE KULLANILAN YAPAY ZEKA UYGULAMALARI KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

Rümeysa Tekin

Özel Hukuk Ana Bilim Dalı

Özel Hukuk Programı

Anadolu Üniversitesi, Lisansüstü Eğitim Enstitüsü, Haziran 2025

Danışman: Prof. Dr. Mesut Aygün

Bu yüksek lisans tezi, e-ticaret sektöründe yaygın olarak kullanılan yapay zeka (YZ) tabanlı uygulamaların, kişisel verilerin korunması hukuku bağlamında doğurabileceği olası riskleri tespit etmeyi ve bu risklerin Avrupa Birliği (AB) ve Türk mevzuatı çerçevesinde ne ölçüde önlenebileceğini ortaya koymayı amaçlamaktadır. Zira YZ uygulamaları, hem geliştirilme süreçlerinde hem de işleyişlerinde büyük veri kümelerine ihtiyaç duymaktadır. E-ticaret sektöründe bu verilerin önemli bir bölümünü kişisel veriler oluşturmaktadır. E-ticaret platformlarında chatbot ve sanal asistanlar, kişiselleştirme, öneri sistemleri, akıllı arama sistemleri, dinamik fiyatlandırma ve stok yönetimi gibi YZ tabanlı uygulamalar bulunmaktadır. Çalışmamızda e-ticaret sektörünü şekillendiren bu dinamik yapıyı yapay zeka uygulamalarının özellikle teknik yönleri ve kullanılan YZ teknikleri kişisel verilerin korunması çerçevesinde değerlendirmesi yapılmıştır. Bu bağlamda, kişisel verilerin korunması hukukunun merkezine yerleştirilen Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve Yapay Zeka Tüzüğü (AI Act) gibi düzenlemeler ışığında, mevcut hukuki çerçevenin yeterliliği değerlendirilmiş; hem kullanıcıların korunması hem de şirketlerin yükümlülüklerini nasıl yerine getirmesi gerektiği konularında kapsamlı bir analiz yapılmıştır. Çalışmada ayrıca, YZ tekniklerini sistemlerine entegre eden e-ticaret şirketlerinin, kişisel verilerin korunmasına yönelik yükümlülüklerini yerine getirebilmeleri için uymaları gereken ilke ve kurallar ortaya konmuş; uyumun sağlanmasına yönelik hukuki ve teknik öneriler geliştirilmiştir.

Anahtar Kelimeler: Yapay Zeka, Kişisel Verilerin Korunması, E-Ticaret, GDPR, AI Act.

ABSTRACT

PERSONAL DATA PROTECTION IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE APPLICATIONS USED IN THE E-COMMERCE SECTOR

Rümeysa Tekin

Department of Private Law

Program in Private Law

Graduate School of Anadolu University, June 2025

Supervisor: Prof. Dr. Mesut Aygün

This master's thesis aims to identify the potential risks that AI-based applications, which are widely used in the e-commerce sector, may pose in the context of personal data protection law and to reveal the extent to which these risks can be mitigated within the framework of European Union (EU) and Turkish legislation. This is because AI applications require large data sets both in their development processes and in their operation. In the e-commerce sector, a significant portion of this data consists of personal data. E-commerce platforms feature AI-based applications such as chatbots and digital assistants, personalization, recommendation systems, smart search systems, dynamic pricing, and stock management. In our study, we evaluated the technical aspects and AI techniques used in these dynamic AI applications that shape the e-commerce sector within the framework of personal data protection. In this context, the adequacy of the current legal framework was assessed in light of regulations such as the European Union General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act), which are at the core of personal data protection law. A comprehensive analysis was conducted on both the protection of users and how companies should fulfill their obligations. The study also outlines the principles and rules that e-commerce companies integrating AI technologies into their systems must comply with in order to fulfill their obligations regarding the protection of personal data, and develops legal and technical recommendations for ensuring compliance.

Keywords: Artificial Intelligence, Personal Data Protection, E-Commerce, GDPR, AI Act.

TEŞEKKÜR

Bu çalışmanın yürütülmesi sürecinde desteğini hiçbir zaman esirgemeyen, bana büyük bir sabır ve hoşgörüyle rehberlik eden değerli danışmanım Prof. Dr. Mesut Aygün'e en içten teşekkürlerimi sunarım. Engin bilgisi, anlayışı ve desteği olmasaydı, bu çalışmayı yoğun iş temposu ve hayatın getirdiği sorumluluklar arasında tamamlamam mümkün olamayabilirdi. Ayrıca jüri üyelerim Doç. Dr. Nilüfer Boran Güneysu ve Dr. Öğr. Üyesi Semih Yumak'a da, çalışmamı dipnotlarına kadar dikkatle inceleyip, kıymetli tavsiye ve düzeltmeleriyle katkı sağladıkları için teşekkür ederim.

Tez çalışmalarına zaman ayırabilmem adına işten ayrıldığım dönemde bana hem maddi hem de manevi destek veren, her daim baba olduğunu hissettiren sevgili babam Ömer Tekin'e minnettarım. Onun desteği, bu sürecin en güçlü dayanaklarından biri olmuştur. Çalışmalarım sırasında bana yoldaş olan sevgili kız kardeşim Rüveyda'ya; manevi desteklerini her zaman hissettiren abim Halit Tekin'e ve kardeşlerim Yusuf ile Furkan Yiğit'e, ailem oldukları ve zor zamanlarda yanımda oldukları için teşekkür ederim. Onlar olmadan zor zamanları atlatmak çok daha güç. Annem Derya Çelik'e ise henüz küçük yaşlarımda kendi yolculuğuma ve hayallerime inanmam konusunda verdiği cesaret için teşekkür ederim. Ayrıca, uzun ve yorucu bu süreçte bana gösterdiği sabır, değer ve sürekli desteği için sevgili dostum Yusuf'a içtenlikle teşekkür ederim. Bu süreci daha katlanılır kılan diğer arkadaşlarım ve yakınlarıma da ayrıca minnettarım.

Son teşekkürüm, kendi yolculuğu boyunca yılmadan emek veren, çabalayan, elinden gelenin en iyisinden biraz fazlasını yapmaya gayret eden, içindeki umut ateşini hiç söndürmeyen ve hiçbir zaman pes etmeyen kendime; gösterdiğim sabır, kararlılık ve inanç için samimiyetle teşekkür ediyorum. Akademik hedeflerimden birini daha bu tez ile gerçekleştirdim. Dilerim ki yolum, etik değerler çerçevesinde; insanlığın ve kendimin faydasına olacak şekilde, kararlılık, cesaret ve azimle; insani değerlere bağlı ve açık bir yürekle devam etsin.

....../....../20....

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmamın Anadolu Üniversitesi tarafından kullanılan “Bilimsel İntihal Tespit Programı”yla tarandığını ve hiçbir şekilde “intihal içermediğini” beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

.....
(İmza)

.....
(Öğrencinin Adı Soyadı)

İÇİNDEKİLER

BAŞLIK SAYFASI.....	i
JÜRİ VE ENSTİTÜ ONAYI.....	ii
ÖZET.....	iii
ABSTRACT.....	iv
TEŞEKKÜR.....	v
ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ	vi
İÇİNDEKİLER.....	vii
KISALTMALAR LİSTESİ.....	xii
GİRİŞ.....	1
BİRİNCİ BÖLÜM	
1. GENEL YÖNLERİYLE YAPAY ZEKA.....	5
1.1.Genel Olarak Yapay Zeka	5
1.2. Kavramsal Çerçevede Yapay Zeka.....	6
1.3. Yapay Zeka’nın Tarihsel Yolculuğu.....	9
1.4. Yapay Zeka Türleri.....	13
1.5. Yapay Zeka Teknikleri	14
1.5.1. Makina öğrenmesi (Machine learning)	14
1.5.1.1. Pekiştirmeli öğrenme	15
1.5.1.2. Yapay sinir ağı.....	15
1.5.2. Derin öğrenme (Deep learning)	16
1.5.3. Uzman sistemler	17
1.5.4. Doğal dil işleme (Natural language processing)	17
1.5.5. Üretken AI (Gen AI).....	18
1.5.6. Robotik.....	18
1.6. Yapay Zekaya İlişkin Hukuki Düzenlemeler	19
1.6.1. Uluslararası düzenlemeler.....	19
1.6.1.1. 2024’e kadar Avrupa’daki yapay zeka alanındaki gelişmeler: belgeler, stratejiler ve danışma kurulları.	19
1.6.1.2. Avrupa birliği yapay zeka düzenlemesi: AI Act (2024).....	21
1.6.1.3. Avrupa konseyi çerçeve sözleşmesi (2024).....	25
1.6.2. Ulusal düzenlemeler	27
1.7. Veri.....	28
1.7.1. Verilerin sınıflandırılması	30
1.7.1.1. Yapılandırılmış veri	30

1.7.1.2. Yapılandırılmamış veri	30
1.7.1.3. Yarı yapılandırılmış veri	30
1.7.2. Genel olarak büyük veri	31
1.7.1.1. Büyük verinin özellikleri	32
1.7.1.1. Büyük veri ve yapay zeka ilişkisi	35
1.7.1.1. Büyük veri ve yapay zeka bağlamında kişisel veri	35

İKİNCİ BÖLÜM

2. GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI	37
2.1. Kişisel Verilerin Korunması İhtiyacı	37
2.2. Kişisel Veri Kavramı Tanımı ve Unsurları	39
2.2.1. Her türlü bilgi	40
2.2.2. Kişi	43
2.2.2.1. Tüzel kişilere ilişkin kişisel veriler	43
2.2.2.2. Cenine ilişkin kişisel veriler	46
2.2.2.3. Ölüye ilişkin kişisel veriler	47
2.2.3. Belirli veya belirlenebilir olma	49
2.2.4. İlişkili olma	52
2.3. Kişisel Verinin Hukuki Niteliği	53
2.3.1. Mülkiyet hakkı görüşü	54
2.3.2. Fikri mülkiyet hakkı görüşü	55
2.3.3. Kişilik hakkı görüşü	55
2.3.4. Günümüz “bağımsız hak” yaklaşımı	57
2.4. Kişisel Verilerin Korunması Hukuku	58
2.5. Kişisel Veri Hukukunun Sujeleri	60
2.5.1. İlgili kişi (Kişisel verileri işlenen kişi veya veri öznesi)	61
2.5.2. Veri sorumlusu	61
2.5.3. Veri işleyen	63
2.6. Kişisel Verilerin İşlenmesi	64
2.7. Kişisel Veri Türleri	65
2.7.1. Özel nitelikli kişisel veriler (Hassas kişisel veriler)	65
2.7.2. Genel nitelikli kişisel veriler (Hassas olmayan kişisel veriler)	68
2.8. Kişisel Verilerinin Korunmasına İlişkin Hukuki Düzenlemeler	68
2.8.1. Uluslararası düzenlemeler	68
2.8.1.1. Avrupa ekonomik işbirliği teşkilatı (OECD)	69

2.8.1.2. Birleşmiş milletler	70
2.8.1.3. Avrupa konseyi	72
2.8.1.4. Avrupa Birliği	73
2.8.2. Ulusal düzenlemeler	78
ÜÇÜNCÜ BÖLÜM	
3. E-TİCARET SEKTÖRÜNDE KULLANILAN YAPAY ZEKA UYGULAMALARI KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ÖZEL BİR DEĞERLENDİRME.....	82
3.1. E-Ticaret, Yapay Zeka Entegrasyonu ve Kişisel Veriler	82
3.1.1. Ticaretin dijitalleşmesi: e-ticaret.....	82
3.1.2. E-ticarete yapay zeka teknolojilerinin rolü.....	83
3.1.3. E-ticaret ve yapay zeka açısından kişisel verilerin önemi.....	84
3.2. E-Ticarete Kullanılan Yapay Zeka Uygulamaları ve Kişisel Veri İşleme Süreçleri	86
3.2.1. Genel olarak	86
3.2.2. Yapay zeka tabanlı sohbet botları (Chatbot ve sanal asistanlar)	87
3.2.2.1. Chatbotlar	87
3.2.2.2. Sanal asistanlar (Digital asistant)	89
3.2.2.3. Teknik altyapı ve kullanılan yapay zeka tekniği	91
3.2.2.4. Hukuki ve etik değerlendirme.....	92
3.2.3. Tavsiye sistemleri (Recommendation engines/Recommender systems).....	93
3.2.3.1. Tüketici segmentasyonu ve hedef kitle tespiti.....	93
3.2.3.2. Kişiselleştirilmiş müşteri deneyimi	94
3.2.2.3. Teknik altyapı ve kullanılan yapay zeka tekniği	95
3.2.2.4. Hukuki ve etik değerlendirme.....	96
3.2.4. Akıllı arama sistemleri	97
3.2.4.1. Yapay zeka tabanlı akıllı arama sistemleri	97
3.2.4.2. Teknik altyapı ve kullanılan yapay zeka tekniği	97
3.2.4.3. Hukuki ve etik değerlendirme.....	98
3.2.5. Dinamik fiyatlandırma algoritmaları ve stok yönetimi.....	99
3.2.5.1. Genel olarak dinamik fiyatlandırma (Algorithmic pricing)	99
3.2.5.2. Kişiselleştirilmiş dinamik fiyatlandırma	99
3.2.5.3. Stok yönetimi	100
3.2.5.4. Risk bakımından değerlendirme.....	100
3.2.6. E-ticarete kullanılan yapay zeka uygulamaları riskleri ile kişisel veri işleme süreçlerine ilişkin genel değerlendirme	101

3.3. E-Ticaret Sektöründe Kullanılan Yapay Zeka Uygulamaları ve Kişisel Verilerin Korunması Hukukuna Uyum	107
3.3.1. Yapay zeka uygulamalarında uyulması gereken kişisel verilerin korunması ilkeleri.....	107
3.3.1.1. Hukuka uygunluk, adalet ve şeffaflık ilkeleri.....	108
3.3.1.2. Amaçla sınırlılık ilkesi.....	110
3.3.1.3. Veri minimizasyonu ilkesi.....	113
3.3.1.4. Verilerin güncel ve doğru olması.....	113
3.3.1.5. Saklama süreleri ile sınırlılık ilkesi.....	114
3.3.2. Yapay zeka uygulamalarında kişisel verilerin işlenebilmesinin hukuki şartları	115
3.3.2.1. İlgili Kişinin Açık Rızası	115
3.3.2.1.1. Açık rızanın unsurları.....	115
3.3.2.1.1.1. sınırlı ve belirli olma	116
3.3.2.1.1.2. özgür irade şartı.....	117
3.3.2.1.1.3. bilgilendirme yükümlülüğü	117
3.3.2.1.2. Rızanın açık olması ile şekil şartı.....	118
3.3.2.1.3. Özel nitelikli kişisel veriler özelinde değerlendirme	119
3.3.2.1.4. E-ticarete kullanılan yapay zeka uygulamalarında açık rıza	120
3.3.2.2. Meşru amaçlarla kişisel verilerin işlenmesi	121
3.3.2.3. Kişisel verileri işleme yasakları.....	124
3.3.2.4.1.Profilleme	125
3.3.2.4.2. Otomatik karar verme yasağı	126
3.3.3. Yapay zeka uygulamalarında kullanıcıların(ilgili kişinin) hakları	128
3.3.3.1. Bilgi edinme hakkı.....	128
3.3.3.1.1.Veri sorumlusunun aydınlatma yükümlülüğü.....	128
3.3.3.1.1.Veri sorumlusuna müracaat ile ilgili kişinin bilgi edinmesi ve erişim hakkı	130
3.3.3.2. Kişisel verilerin düzeltilmesini isteme hakkı	132
3.3.3.3. Kişisel verilerin silinmesini ve yok edilmesini (unutulma hakkı) isteme hakkı	133
3.3.3.4. Veri taşınabilirliği hakkı	135
3.3.3.5. İtiraz hakkı.....	135
3.3.3.6. İşlemeyi kısıtlama hakkı	136
3.3.3.7. Zararının tazmin edilmesini talep hakkı.....	136
3.3.4. E-ticaret işletmesi tarafından alınacak idari ve teknik tedbirler	137
SONUÇ	141



KISALTMALAR

108 No’lu Sözleşme : Avrupa Konseyi’nin 28.01.1981 tarihli 108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

1995/46/EC VKD : Kişisel Verilerin İşlenmesine İlişkin Olarak Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımına İlişkin 24 Ekim 1995 tarihli ve 95/46/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi (*Veri Koruma Direktifi*)

2002/58/EC EVKD : Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunmasına ilişkin 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi (*Elektronik Veri Koruma Direktifi*)

AB : Avrupa Birliği

ABAD : AB Adalet Divanı (CJEU - Court of Justice of the European Union)

ABD : Amerika Birleşik Devletleri

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

Akt : Aktaran

AYM : Anayasa Mahkemesi

Bkz : Bakınız

BM : Birleşmiş Miletler

Çev : Çeviri

Dn : dipnot

Ed : editör

EDPK : Avrupa Veri Koruma Kurumu (*European Data Protection Board*)

EHSKVİY : Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik

E-ticaret : Elektronik Ticaret

GDPR : Genel Veri Koruma Tüzüğü (*General Data Protection Regulation*)

ICO : Information Commissioner’s Office

IEEE : Institute of Electrical and Electronics Engineers

KVK : Kişisel Verilerin Korunması

KVKK : 6698 Sayılı Kişisel Verilerin Korunması Kanunu

M : madde

OECD : Ekonomik İşbirliği ve Kalkınma Teşkilatı

(Organisation for Economic Co-operation and Development)

RG	: Resmi Gazete
S	: Sayılı
ss	: sayfa sayısı
T	: Tarih
TDK	: Türk Dil Kurumu
TMK	: 4721 Sayılı Türk Medeni Kanunu
TTK	: 6102 Sayılı Türk Ticaret Kanunu
UNCHR	: Birleşmiş Milletler Mülteciler Yüksek Komiserliği
Vb	: ve benzeri
Vd	: ve devamı
Yy	: yüzyıl
YZ	: Yapay Zeka

GİRİŞ

İlim tercüme ile olmaz, ilim tetkikle olur.

Mustafa Kemal Atatürk

İnsanlığın bugüne kadar dört büyük endüstri devrimi yaşadığı ifade edilmektedir. Buhar gücü ile çalışan makinaların icadı ile ilk endüstri devrimi 18. yy'da gerçekleşmiştir. İkinci endüstri devrimi elektrik gücünü kullanarak seri üretimi başlatırken; üçüncü endüstri devrimi internet ve teknoloji çağını başlatarak 20. yy'ın son çeyreğinde başlamıştır. Endüstri 4.0 veya dijital devrim olarak isimlendirilen son endüstri devriminde ise en önemli gelişme yapay zeka olmuştur¹. Günümüzde popüler bir teknoloji haline gelen yapay zeka pek çok alanda kullanılmakta; insanoğlunun yaşamını kolaylaştırmakta, hızlandırmakta ve geliştirmektedir. Yapay zeka ekonomik, sosyal ve kültürel gelişme için fırsatlar sağlamakta; enerji sürdürülebilirliği, daha iyi sağlık bakımı ve bilginin yayılması gibi alanlarda büyük katkılar sunmaktadır.

Yapay zeka bir çok disiplin altında incelenebilmektedir. Bu disiplinlerden birisi de veri bilimidir. Kişisel olmayan veriler ile çalışma konumuz olan kişisel veriler yapay zekanın çalışabilmesi için gereklidir. Dijitalleşen ve gelişen teknolojiler, insanlar hakkında çok daha büyük miktarlarda verinin toplanmasını mümkün kılmıştır. İnternetin yakıtı ve yapay zekanın hammaddesi olan kişisel veriler, özel şirketler, devletler ve kamu idarelerince sürekli olarak farklı çıkarlar için toplanılmaktadır. Kişisel veri toplama ve işleme amaçları finansal, siyasi hedefler veya suçların önlenmesi ile terörizm ile mücadele olabilmektedir. Fakat toplanan veriler, aktarımlar ve analizler ile başka bağlamlar için de kullanılabilir. Örneğin, ticari amaçlı olarak toplanan veriler sonrasında siyasi eğilim belirleme bağlamında da kullanılabilir².

Kişisel veriler, bu verileri elinde bulunduran şirketler için bir güç unsuru haline gelmiştir. Bugün sınırları çok geniş olan bir veri pazarı olduğu yönünde haklı endişeler bulunmaktadır. Sosyal medya platformlarının ticari gelir kaynağını reklamlar teşkil etse de; hiçbir reklam geliri bulunmayan Whatsapp platformunun Facebook'a on dokuz milyar dolara satın alınması bu durumu ispatlamaktadır³. Nitekim bu satın almada, bu şirketin on dokuz barındıran Meta Şirketi'nin bu satın almadaki amacı dünyada bugün 180'den fazla ülkede 2

¹ bkz. World Economic Forum (2016), The Fourth Industrial Revolution: What It Means, How to Respond, s.2-3. <https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> (Erişim Tarihi: 02.05.2025) . Dünya Ekonomik Forumu'nun (World Economic Forum) 2016 yılında yayınladığı Dünya Ekonomik Forum'u Başkanı Klaus Schwab yazısı için bkz. <https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> (Erişim Tarihi: 02.05.2025); Büyüközkan Feyzioğlu, G (2021) . Dijitalleşen dünyada yapay zeka. İçinde E. Aksoy Retornaz & O. G. Güçlütürk (Ed.), *Gelişen teknolojiler ve hukuk II: Yapay zeka* (ss.1-5) . On İki Levha Yayınları, s.1.

² Hingh, A. de (2018) . Some reflections on dignity as an alternative legal concept in data protection regulation. *German Law Journal*, 19 (5), s. 1270-1271. ABD başkanı Trump'ın seçimi kazanabilmesi için sosyal medyada yapılan profillemeye dayalı propagandalar yapıldığı ifade edilmektedir. Nitekim, 2025 haziran ayında Elon Musk, elinde bulundurduğu sosyal medya gücünü ABD başkanı Trump'ın seçimi kazanması için kullandığını itiraf etmiştir. Anadolu Ajansı (2025, 5 Haziran) . Elon Musk: Ben olmasaydım Trump seçimi kaybederdi. Anadolu Ajansı. <https://www.aa.com.tr/tr/dunya/elon-musk-ben-olmasaydim-trump-secimi-kaybederdi/3590103> , (Erişim Tarihi: 09.06.2025) .

³İlgili BBC haberi için bkz. <https://www.bbc.com/news/business-26266689> . (Erişim Tarihi: 02.05.2025) .

milyarı aşkın kullanıcıya⁴ ve verilerine erişim sağlamak istemesidir. Bu veri ambarı, kullanıcıların kimliğini, mesaj içeriklerini, iletişim bilgilerini ve çok daha fazlası ile bu verilerin analizleri ile doğan verileri içermektedir. Burada satın alınan değer kişisel verilerin analizi ile ortaya çıkan verilerin pazar değeridir⁵. Kişisel verilerin işlenmesinin herhangi bir sınırlamaya tabi tutulması verileri işleyenler ile kişiler arasındaki dengeyi kişiler aleyhine bozmaktadır. Kişisel verilerinin paylaşılması ile adeta şeffaflaşan insanlar maddi ve manevi birçok zarara uğrayabilmektedir.

21. yy insanının adeta bir yaşam alanına dönüşen internet yaşlandıkça kişisel veri ihlalleri daha tehlikeli boyutlara ulaşmaktadır. İnternet 12 Mart 2025 tarihinde 36. yaşına girmiştir⁶. İnterneti(World Wide Web) icat eden *Tim Berners-Lee*, internetin özellikle belli güç grupları elinde tutulduğu, bu grupların interneti silah olarak kullanarak kitleleri yönetilebildiğine dikkat çekmiş ve toplumsal iyiliği maksimize etmekten çok kârı maksimize etmek için kurulmuş bu şirketlerin kişisel verilerin korunması dahil olmak üzere uyması gereken yasal gerekliliklerin olduğunu altını çizmiştir⁷. 2024 yılında tehlikenin yapay zeka için de olduğunu dile getiren Lee, uyulması gereken yasal düzenlemeler konusunda çağrısını yinelemiştir⁸.

Belirtilmelidir ki, hukuk yaşamdan bağımsız değil; tersine onun bir parçasıdır. Hukuk, yaşamı takip ederek doğan ve doğabilecek ihtilaflar karşısında çözüm bulmaya çalışan bir mekanizmadır. İhdas edilen iyi kanun ve kurallar yalnızca bugünü kolaylaştırmakla kalmaz; topluluk hayatında yeni ufuklar açarak günü ve geleceği kavramayı da sağlar⁹. Bu noktada, hukukun dünyadaki güncel gelişmeleri anlaması ve onlara uyum sağlaması gerekmektedir. Kişisel verilerin korunması alanında Avrupa'da yaklaşık 40 yıldır süregelen çalışmaların ve tecrübenin ürünü olan Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) bu noktada önem arz etmektedir. 2024 yılında kabul edilen AI Act ise yapay zeka alanında dünyadaki ilk kapsamlı yasal çerçeve olma niteliğini taşımaktadır. Alanlarında ilklere imza atan bu iki gelişmenin incelemesi yapay zeka uygulamalarının, kişisel verilerin korunması hukuku bağlamında değerlendirmesi bakımından önemlidir.

Yapay zeka uygulamalarının uygulanma alanlarının geniş olması sebebi ile çalışma konusu daraltılmış ve çalışma zemini olarak e-ticaret platformları seçilmiştir. Bu bağlamda çalışmamızın amacını e-ticarete kullanılan yapay zeka uygulamalarının kişisel verilerin korunması açısından değerlendirilmesi oluşturmaktadır. Nihayetden çalışmamızda 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde Türkiye'deki durum değerlendirmesi de yapılmıştır.

⁴ WhatsApp. About. <https://www.whatsapp.com/about> (Erişim Tarihi: 02.05.2025) .

⁵ Isaac, M (2023, 8 Kasım) . Mark Zuckerberg taps the strengths of WhatsApp. *The New York Times*. <https://www.nytimes.com/2023/11/08/technology/mark-zuckerberg-whatsapp.html> diğer haberler için ayrıca bkz. Investopedia (2015, 3 Mart) . WhatsApp: The best Facebook purchase ever? *Investopedia*. <https://www.investopedia.com/articles/investing/032515/whatsapp-best-facebook-purchase-ever.asp> (Erişim Tarihi: 02.05.2025)

⁶ Kaya, M. B (2010) . *Teknik ve hukuki boyutlarıyla internete erişimin engellenmesi: 5651 sayılı kanun ve dünya uygulamaları*. XII Levha Yayınları, s.5-19.

⁷ The Guardian Haberi, <https://www.theguardian.com/commentisfree/2018/mar/12/tim-berners-lee-web-weapon-regulation-open-letter> (Erişim Tarihi: 23.02.2025) .

⁸ Davies, P (2024, 26 Aralık) . World Wide Web'in mucidi Sir Tim Berners-Lee'nin 2025 yılı için umutları: Veri hakları ve sosyal medya tepkisi. *Euronews*. <https://www.euronews.com/next/2024/12/26/world-wide-web-creator-sir-tim-berners-lees-hopes-for-2025-data-rights-and-a-social-media-> (Erişim Tarihi: 23.02.2025) .

⁹ Dönmezer, S (1957) . Hukuk ve hayat. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 21 (1-4), s.424-427.

Çalışmamızda, kişisel verilerin korunması hukuku ile e-ticarete yapay zeka (YZ) tekniklerinin ve kişisel verilerin kullanımı kapsamlı bir şekilde incelenmiş; ayrıca yapay zekanın tarihsel gelişimi ve teknik altyapısına da ayrıntılı olarak yer verilmiştir. Bilgisayar mühendisliği ana bilim dalının konusu olan yapay zeka teknolojisinin, e-ticaret sektörü bakımından işletme-iktisat disiplini kapsamında değerlendirilmesi ve ayrıca bu teknolojilerin hukuk perspektifinden ele alınması çalışmamıza disiplinlerarası bir nitelik kazandırmaktadır.

Çalışmamızın özgün yönü, e-ticaret platformlarında kullanılan YZ tabanlı uygulamaların teknik özellikleriyle birlikte, temel hak ve özgürlükler ile kişisel verilerin korunması hukuku açısından doğurabileceği risklerin tespit edilmesine dayanır. Nitekim yaptığımız literatür taramasında, e-ticaret platformlarında kullanılan uygulamaların teknik altyapısı ve kullanılan YZ yöntemleri açıklanarak bunların kişisel verilerin korunmasıyla ilişkisinin ayrıntılı şekilde ele alındığı çalışmaların sınırlı olduğu görülmüştür. Bu kapsamda, gelişmekte olan üretken yapay zeka (Gen AI) teknolojilerine ve diğer güncel gelişmelere de yer verilerek çalışmanın kapsamı genişletilmiştir. Son olarak, yapay zeka alanındaki hukuki gelişmelerin daha iyi anlaşılabilmesi amacıyla, 2024 yılında kabul edilen Avrupa Birliği Yapay Zeka Yasası (AI Act) ile yine aynı yıl kabul edilen Avrupa Konseyi'nin "Yapay Zeka ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi" ayrıntılı olarak incelenmiştir.

Yukarıda açıklanan amaçlar doğrultusunda, birinci bölümde yapay zekanın tanımı yapılmış, tarihsel gelişimi incelenmiş ve kullanılan temel yapay zeka teknikleri ayrıntılı şekilde açıklanmıştır. Ayrıca, yapay zeka türleri sınıflandırılarak bu alandaki mevcut ve gelişmekte olan hukuki düzenlemelere yer verilmiştir. Son olarak, yapay zeka teknolojisinin ayrılmaz bir unsuru olan büyük veri kavramı ele alınmış; büyük veri ile yapay zeka ve kişisel veriler arasındaki ilişki ortaya konulmuştur.

İkinci bölümde ise genel olarak kişisel verilerin korunması hukuku ele alınmıştır. Öncelikle, kişisel verilerin korunması ihtiyacının dayandığı temel gerekçeler incelenmiş; ardından kişisel verinin tanımı ve taşıdığı unsurlar açıklanmıştır. Kişisel verinin hukuki niteliği üzerine yapılan tartışmalara yer verilmiş ve bu doğrultuda kişisel verilerin korunmasına ilişkin temel kavramlar detaylandırılmıştır. Bu kapsamda, kişisel verilerin işlenmesi, kişisel veri türleri ile birlikte kişisel verilerin korunması hukukunun sınırları olan veri sorumlusu, ilgili kişi ve veri işleyen kavramları açıklığa kavuşturulmuştur. Son olarak, kişisel verilerin korunmasına ilişkin hukukun tarihsel gelişimi ve koruma kapsamı; ulusal ve uluslararası düzeyde kabul edilmiş düzenleyici metinler aracılığıyla değerlendirilmiştir.

Üçüncü ve son bölümde, çalışmamızın konusunu oluşturan e-ticaret, yapay zeka ve kişisel veri kavramları arasındaki ilişkiler saptanmış; e-ticaret platformlarında kullanılan yapay zeka tabanlı uygulamalar açıklanarak, bu uygulamalar işlevleri, teknik altyapıları ve kullandıkları yapay zeka teknikleri bakımından incelenmiştir. Ayrıca, bu uygulamaların temel hak ve özgürlükler ile kişisel verilerin korunması açısından oluşturduğu riskler değerlendirilmiştir. İncelenen yapay zeka tabanlı uygulamaları kullanan e-ticaret şirketlerinin, kişisel verilerin korunması hukukuna nasıl uyum sağladıkları detaylı şekilde ele alınmıştır. Bu kapsamda, şirketlerin kişisel verileri hukukuna nasıl uyum sağlayacağı üzerinde durularak; kişisel verilerin korunması ilkeleri açıklanmış ve hukuka uygun işleme şartlarına ilişkin ayrıntılı bir değerlendirme yapılmıştır. Son olarak, e-ticarete kullanılan yapay zeka uygulamaları çerçevesinde verileri işlenen kişilerin sahip olduğu haklar ortaya konmuş ve e-ticaret şirketlerinin veri güvenliği sağlamak adına alması gereken idari ve teknik tedbirler, yapay zeka teknolojisi özelinde değerlendirilmiştir.

Hem yapay zekanın gelişiminden en iyi şekilde yararlanılabilmesi hem de insan hakları, demokrasi ve hukukun üstünlüğü alanlarında ortaya çıkabilecek potansiyel risklere çözüm bulunabilmesi için atılması gereken en önemli ve temel adımlardan biri, yapay zeka teknolojisi ile kişisel verilerin korunmasına ilişkin mevzuatın karşılaştırmalı ve ayrıntılı biçimde incelenmesidir. Çalışmamızın konusunu işte bu çaba oluşturmaktadır.



BİRİNCİ BÖLÜM

GENEL YÖNLERİYLE YAPAY ZEKA VE VERİ

1.1.Genel Olarak Yapay Zeka

Yapay zeka, bugün genel olarak verilerden beslenen, muhakeme kabiliyeti olan, öğrenebilen, istenen görevi rasyonel davranışlarla gerçekleştirebilen sistemler veya makinalar olarak tanımlanabilmektedir. Aşağıda “*Kavramsal Çerçeve Yapay Zeka*¹⁰” başlığı altında yapay zekanın kavramsal çerçevesi detaylı şekilde incelenmiştir. Ortaya çıktığı günden bugüne popülerliğini arttıran yapay zeka uygulanma alanını genişleterek bugün hayatın pek çok alanında karşımıza çıkar hale gelmiştir¹¹. Özellikle yapay zeka sinir ağları ile derin öğrenmenin geliştirilmesi ile birlikte yapay zeka teknolojilerinde muazzam ilerlemeler kaydedilmeye başlanmıştır. Algoritmalar aracılığı ile verilerden öğrenebilen yapay zeka uygulamaları kendini sürekli geliştirmekte ve böylece her geçen gün insana özgü bilişsel yeteneklere sahip olmaya bir adım daha yaklaşmaktadır¹². Bağımsız olarak hareket edebilen yapay zeka uygulamalarının insana duyulan ihtiyacı şimdiden ortadan kaldırdığı söylenebilir. Örneğin, ABD’de yaygın olarak kullanılan sürücüsüz otomobiller kullandıkları yapay zeka uygulamaları ile insana duyulan ihtiyacı ortadan kaldırmıştır¹³. Dünya’daki insan hakimiyeti karşısında bir tehdit unsuru olarak görülen yapay zeka¹⁴ herkesin biraz korku ile karışık heyecanla beklediği teknoloji ile uyumlu insan hayatı çağını başlatmıştır. Hayatın her alanında etkilerini gösteren yapay zeka toplum 5.0¹⁵ kavramını gündeme getirerek toplum düzeni de etkilemiştir.

Disiplinlerarası bir niteliğe sahip olan yapay zeka¹⁶ düzenli olarak büyümekte ve 2023 yılındaki verilere göre yıllık bir trilyonun üzerinde değer elde etmektedir. Yapay zeka alanında uzman olan Kai-fu Lee (Microsoft Research Asia’nın kurucu ortağı ve Google Çin’in eski Başkanı) yapay zeka etkisinin “*dünyadaki diğer her şeyden*” daha etkili olacağını ifade etmiştir¹⁷.

Yapay zeka pek çok bakımdan çekicidir. Ekonomik olarak uygun olan ve gelişen teknoloji ve işlem gücü sayesinde her gün başka bir yetenek kazanan yapay zeka hayatı insanlar için daha kolay ve kazançlı hale getirmektedir. Uygulandıkları alana göre cihazları görebilen, tanımlayabilen, insan dilini anlayabilen ve yanıtlayabilen, yeni bilgiler ve deneyimlerden öğrenebilen olan yapay zeka uygulamaları, kullanıcılara ve uzmanlara hayatın neredeyse her

¹⁰ Bkz. aşağıda “3.2.Kavramsal Çerçeve Yapay Zeka” başlığı.

¹¹ Tutsal, E., & Ventura, K (2022) . Müşteri deneyimini iyileştirmede yapay zeka uygulamaları: Çevrimiçi perakende firması örneği. *Journal of Social Research & Behavioral Sciences / Sosyal Araştırmalar ve Davranış Bilimleri Dergisi*, 8 (16), s. 346.

¹² Aygün, 2023, s. 17.

¹³ IBM, What is AI? , https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai . Erişim Tarihi: 19.05.2025.

¹⁴ Turing, A. M (1950) . Computing machinery and intelligence. *Mind*, 49, 442–443. <https://courses.cs.umbc.edu/471/papers/turing.pdf> (Erişim Tarihi: 21.05.2025)

¹⁵ Japonya tarafından gündeme getirilen Toplum- 5.0 kavramı diğer adıyla “*Süper Akıllı Toplum*“, süper akıllı teknolojiler ile insanların el ele olduğu genel olarak teknoloji ile uyumlu insan hayatı düzenini ifade etmektedir. Koparan, E., & Doğan, O (2024) . Toplum 5.0 ve e-ticarete yapay zekâ odağında bakış: Tanımlar, ilişkiler ve bileşenler. *Yönetim ve Ekonomi Dergisi*, 31 (2), s. 298.

¹⁶ Yapay zekâ, biyoloji, psikoloji, fizyoloji, felsefe, mantık, bilgisayar bilimleri, matematik, fizik ve elektronik, dil bilgisi ve güzel sanatlar disiplinlerini kapsamaktadır. Büyüközkan Feyzioğlu, 2021, s. 2-3.

¹⁷ Russell, S., & Norvig, P (2024) . *Yapay zeka: Modern bir yaklaşım* (C. Öz, Çev.) . Palme Yayınları (Orijinal eser 2023’te yayımlanmıştır.) s.1.

alanında çözüm önerileri sunmaktadır¹⁸. Yapay zekanın enerjiden eğitime, finansal hizmetlerden e-ticarete ve inşaatla kadar tüm sektörlerde birçok faydası bulunmaktadır. Profesyonel alanda da hizmet veren yapay zeka uygulamaları bugün Danimarka'da, acil servisi arayan hastanın sesini analiz ederek kalp durması veya diğer hastalık durumlarının teşhis edilmesinde hayat kurtarıcı rolünde hizmet vermekte; Avusturya'da ise radyologların röntgen filmlerini büyük miktarda diğer tıbbi verilerle eş zamanları olarak karşılaştırıp analiz ederek tümörün daha doğru bir şekilde tespit edilmesine yardımcı olmaktadır¹⁹.

Yapay zekanın etkileri günlük hayatta hissedilir durumdadır. Bugün artık insanlar yapay zeka programlarını kişisel asistanları olarak kullanmakta; basit günlük hayat sorularını dahi google ya da yandex gibi internet arama motorlarına değil ChatGbt ya da OpenAI gibi yapay zeka uygulamalarına sormakta böylece ayrıntılı ve kişiselleştirilmiş cevaplar alabilmektedir. Yapay zeka uygulamalarından yemek tariflerinden rüya yorumlarına kadar birçok alanda faydalanan insanlar günlük sorunlarını yapay zeka uygulamaları ile paylaşarak internetin bilgi birikiminden hareketle yapay zekayı psikologları, dil öğrenmede öğretmenleri ve hatta günlük yeme-içme listelerini paylaşarak diyetisyenleri olarak kullanmaktadır.

Yapay zeka uygulamalarının faydalarından yararlanmak isteyen kişilerin giz alanında kalan mahremlerini yapay zeka uygulamaları ile paylaşmaları ve haklarındaki geniş hacimdeki verileri internetin sonsuz dünyasına bırakmaları kişilerin temel hak ve özgürlükleri için büyük bir tehdit halinde gelmektedir. Bu sorun çalışmamızın konusunu teşkil etmektedir. Bu bölümde kısaca yapay zekanın uygulamalarının önemi, fonksiyonları ve bugün insan hayatındaki ve hukuk dünyasındaki yerinin anlaşılması amaçlanmaktadır.

1.2.Kavramsal Çerçeve ve Yapay Zeka

Yapay zekaya ilişkin tanımların, bu kavramın ortaya çıkmasından makina öğrenmesi yaklaşımının bulunmasına kadar geçen sürede benzer şekillerde yapıldığı görülmektedir. Yapay sinir ağları ve derin öğrenme yaklaşımlarının gelişmesi ile bugüne kadar gelen dönemde yapay zekanın çalışma sistemi giderek girift bir hal almış; bu durum yapay zekanın tanımlanması da zorlaştırmıştır²⁰.

Yapay zekanın kavramsal çerçevesinin çizilmesinde öncelikle sözlüklerin yol göstericiliğinden ilerlersek; ortaya çıktığı ABD'de yapay zeka kavramından anlaşılması gereken Cambridge sözlüğüne göre: *“daha önce insan zekasına ihtiyaç duyan işlemleri gerçekleştiren bilgisayar sistemlerinin geliştirilmesi ve bunların bağlı olduğu disiplin”* veya *“insanların yapabildiği şeyleri bilgisayarlara yaptırma bilimidir”*²¹. Bu kavram benzer şekilde Oxford Advanced Learner's sözlüğünde de: *“zeki insan davranışlarını kopyalayabilen bilgisayar sistemlerinin incelenmesi ve geliştirilmesi”* şeklinde tanımlanmaktadır²². TDK Türkçe sözlüğüne göre ise bu kavramdan: *“Bir bilgisayarın, bilgisayar kontrolündeki bir robotun veya programlanabilir bir aygıtın insana benzer biçimde*

¹⁸ Büyükoçkan Feyzioğlu, 2021, s.1-2. IBM, What is AI? , https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim Tarihi: 19.05.2025.)

¹⁹ European Commission (2018) . *Artificial intelligence for Europe* (COM (2018) 237 final) . <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> . Erişim Tarihi: 20.05.2025.

²⁰ Bugün geline nokta, yapay zeka tanımı konusunda doktrinde ancak kısmi bir birlikten bahsedilebilir. Bkz. Kaplan, J (2016) . *Artificial intelligence: What everyone needs to know*. Oxford University Press.

²¹Cambridge Dictionary, “Artificial Intelligence”, <https://dictionary.cambridge.org/dictionary/english-turkish/artificial-intelligence> (Erişim Tarihi: 31.01.2025.)

²²Oxford Learner's Dictionary, “Artificial Intelligence”, <https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence?q=artificial+intelligence> (Erişim Tarihi: 31.01.2025.)

algılama, öğrenme, fikir yürütme, karar verme, sorun çözme, iletişim kurma vb. işlevleri sergileyebilme yeteneği” anlaşılmalıdır²³.

Yapay zeka kavramının isim babası olan John McCarthy, yapay zekayı, “zeki makinalar, özellikle zeki bilgisayar programları” olarak tanımlar²⁴. Yapay zeka, Sterne tarafından kısaca “insanı taklit eden sistemler olarak veya bilgisayarların insan gibi davranması” şeklinde²⁵; başka bir tanımda “bir bilgisayarın veya bilgisayar kontrolündeki bir robotun, çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyeti olarak”²⁶; bir başkasında “insan karar alma alanı içinde değerlendirilen görevleri gerçekleştiren bilgi işlem sistemleri”²⁷ ve IBM²⁸ tarafından “bilgisayarların ve makinelerin insan öğrenmesini, kavramasını, problem çözmesini, karar vermesini, yaratıcılığını ve özerkliğini taklit etmesini sağlayan teknoloji” olarak tanımlanmıştır²⁹. Yapay zeka tanımlarının kesiştiği noktanın yapay zekanın insanımsı davranış göstermesi özelliği üzerinde toplandığı ifade edilmektedir³⁰.

Yapay zeka kavramının doğrudan zeka kavramına atıf yapması karşısında insan zekasının makina zekasına yansımından ne anlaşılması gerektiği sorusu gündeme gelmektedir. Zeka çok uzun yıllardır nörobilimcilerin, psikologların ve biyologların araştırma ve inceleme konusu olmasına rağmen hala belirsizliğini koruyan bir kavramdır. Bu durum belli bir noktada önemsizleşmektedir. Çünkü, yapay zeka araştırmacılarının genellikle zeka kavramı ile kastetmek istediği “rasyonelliktir.” Rasyonellik ise en iyiyi seçme yeteneği veya doğru şeyi yapma olarak tanımlanabilir. Elbette rasyonellik zeka kavramının tek bileşeni değildir, ancak önemli bir parçasıdır³¹. Nitekim bu çıkarıma uygun şekilde McCarthy, zeka kavramını dünyada hedeflere ulaşma yeteneğinin hesaplamalı kısmı olarak tanımlamıştır³². Güçlütürk de yapay zeka tanımlamalarında insan zekası, davranışlarına veya bilişsel faaliyetlere atıf yapılmasının yanıltıcı olduğunu, yapay zeka uygulamalarının çalışma sistemlerinin düşünme, öğrenme veya yaratıcılık faaliyetleri ile değil istatistiksel temelli olduğunu ifade etmiştir³³. Diyebiliriz ki; makinelerin zeki olmasından kastedilen esasen makinanın kelimeleri bilmesi, okuyabilmesi, konuşabilmesi görebilmesi veya duyabilmesi değil; geliştirilen makinanın/programın talep

²³ Türk Dil Kurumu. *Güncel Türkçe Sözlük.*, <https://sozluk.gov.tr/> (Erişim Tarihi: 31.01.2025).

²⁴ McCarthy, J (2007) . *What is artificial intelligence*. Stanford University. s.2. <http://www-formal.stanford.edu/jmc/>, (Erişim Tarihi: 20.05.2025).

²⁵ Sterne, J (2017) . *Artificial intelligence for marketing: Practical applications*. John Wiley & Sons, s. 29-31.

²⁶ TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18 Mayıs 2025)

²⁷ GREENGARD, 2019, S (2019, May 4) . *What is artificial intelligence & how does it work?* <https://www.datamation.com/artificial-intelligence/what-is-artificial-intelligence/> (Erişim tarihi: 25 Mayıs 2025)

²⁸ IBM, bilgisayarın icadına giden yolda önemli gelişmelerden biri olan nüfus sayımı için tablolama makinası-delikli kartlar makinası (Mark I) mucidi Alman asıllı Amerikalı olan istatistikçi Herman Hollerith tarafından 1911 yılında kurulan, tarihi açıdan yapay zeka araştırmalarında büyük rol oynayan bugün hala yapay zeka teknolojilerinde araştırma ve gelişmelere öncülük eden uluslararası saygın bir şirkettir. IBM, About Us, <https://www.ibm.com/about?lnk=flatitem> (Erişim Tarihi: 24.05.2025).

²⁹ IBM, What is AI? , https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim Tarihi: 19.05.2025).

³⁰ Koparan ve Doğan, 2024, s, 297.

³¹ Russell ve Norvig, 2024, s.1,34; High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025).

³² McCarthy, 2007, s.2-3..

³³ Güçlütürk, O. G (2022) . *Yapay zeka ve verinin kullanımı*. On İki Levha Yayınları, s. 42-43.

edileni anlayabilmesi ve bağlam içinde yardım sağlayabilmesidir³⁴. Fakat yalnızca anlamak da yeterli değildir; zeki makinaların aynı zamanda yeni durumlar karşısında etkili ve güvenli şekilde nasıl davranacağını hesaplayabilmesi gerekmektedir³⁵.

Bu doğrultuda, Kaplan makinaların insan zekasına benzetilmek istenmesi tanımlamaları kusurlu bulunmaktadır. Nitekim bahsedildiği üzere, insan zekasının ölçülmesi bir yana tanımlanmasında dahi güçlük yaşanmaktadır. Bu sebeple, Kaplan insan zekasının sadece sayısal ölçümlere indirgenmesi yanlış bir tümevarım olduğunu söylemektedir³⁶. Kaplan’a göre yapay zeka; ”sınırlı verilere dayanarak zamanında uygun genellemeler yapma yeteneğidir”. Yapay zekanın uygulama alanı ne kadar genişlerse, minimum bilgi ile o kadar hızlı sonuç çıkartılır ve daha akıllı davranış çıktıları elde edilebilir³⁷.

Avrupa Komisyonu tarafından hazırlanan bir tebliğde, yapay zeka: “çevrelerini analiz ederek ve belirli hedeflere ulaşmak için - bir dereceye kadar özerklikle - eylemlerde bulunarak akıllı davranışlar sergileyen sistemler” olarak tanımlanmıştır³⁸. Daha sonra Avrupa Konseyi bünyesinde kurulan Yapay Zeka Üzerine Yüksek Düzeyli Uzman Grubu (HLEG) tarafından bu tanım geliştirilmiştir. HLEG’in yapay zekanın tanımına ilişkin hazırladığı raporda, YZ tanımını geliştirmiş ve genişletmiştir. Buna göre YZ;

”Karmaşık bir hedef verildiğinde, veri toplama yoluyla çevrelerini algılayarak, toplanan yapılandırılmış veya yapılandırılmamış verileri yorumlayarak, bilgi üzerinde akıl yürüterek veya bu verilerden elde edilen bilgileri işleyerek ve verilen hedefe ulaşmak için yapılacak en iyi eylem(ler)e karar vererek fiziksel veya dijital boyutta hareket eden, insanlar tarafından tasarlanan, yazılım (ve muhtemelen donanım) sistemleridir.”³⁹.

Dünya çapında yapay zeka konusundaki ilk kapsamlı yasal çerçeve olan Avrupa Birliği’nin Yapay Zeka Yasası’nda (“AI Act”)⁴⁰ YZ sistemi tanımlanmıştır. Buna göre:

“Açık veya örtülü hedefler için, aldığı girdilerden, fiziksel veya sanal ortamları etkileyebilecek tahminler, içerik, öneriler veya kararlar gibi çıktıların nasıl üreteceğini bilen, kullanılmaya başlandıktan sonra adaptasyon kabiliyeti gösterebilen, farklı seviyelerde bağımsız çalışabilecek şekilde tasarlanmış makine tabanlı bir sistem” YZ sistemini tanımlamaktadır.

AB tüzüğünden sadece birkaç ay sonra kabul edilen Avrupa Konseyi Yapay Zeka ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi’nde⁴¹ ise YZ; “belirli veya

³⁴SAS (2017, Kasım 15) . *An executive’s guide to cognitive computing*. https://www.sas.com/en_us/insights/articles/big-data/executives-guide-to-cognitive-computing.html (Erişim tarihi: 22 Mayıs 2025)

³⁵ Russell ve Norvig, 2024, s.1.

³⁶ Kaplan, 2016, s.1.

³⁷Kaplan, 2016, s.5-6. Fakat Kaplan, aynı zamanda gerçekten bilgisayar programının insanlardan daha zeki olabilir mi sorusuna, kameraların karanlıkta görmesi, ATM’lerin insandan daha hızlı para sayabilmesi ve arabaların daha hızlı olmasını örnek göstererek kesin bir yanıt olarak ”evet“ şeklinde cevap vermiştir. Kaplan, 2016, s.7-8.

³⁸European Commission (2018) . *Artificial intelligence for Europe* (COM (2018) 237 final) . <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Erişim tarihi: 20 Mayıs 2025)

³⁹ High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .

⁴⁰ European Parliament and Council (2024) . *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending various regulations and directives (Artificial Intelligence Act)*, *Official Journal of the European Union, L Series*, 2024/1689, Article 3 (1) . <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (Erişim tarihi: 21 Mayıs 2025) .

⁴¹European Commission, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225, Vilnius, 05.09.2024, m.2. <https://rm.coe.int/1680afae3c> Erişim Tarihi: 21.05.2025.

belirsiz hedefler doğrultusunda aldığı girdilerden yola çıkarak tahminler, içerikler, öneriler veya kararlar gibi çıktılar üretmeyi ve bu çıktılarla fiziksel veya sanal ortamları etkilemeyi amaçlayan, makine tabanlı bir sistem” olarak tanımlanmıştır.

Yapay zeka kavramının tarihsel sürecinde yukarıda açıklandığı üzere başlangıçta insan davranışlarını taklit eden sistemlerden bahsedilirken, süreç içerisinde insan davranışlarından kastedilenin robotik sistemler değil bilişsel düzeydeki insan yetenekleri olduğu vurgusu yapılmış, bugün yapay zeka alanında yaşanan gelişmeler hukuk dünyasını ilgilendiren boyutlara ulaşmış ve uluslararası düzenleyici metinlerde verilen YZ tanımlamalarında; ilk dönemde sıklıkla vurgu yapılan yapay zekanın insanımsı özelliğine hiç yer verilmemiştir. Nitekim, dikkat edilirse, HLEG raporunda, Avrupa Konseyi ve Avrupa Birliği düzenlemelerinde verilen yapay zeka tanımlamalarında insana benzeyen, insanımsı veya insan ile ilişkilendirilecek hiçbir kavram bulunmamaktadır. Bu durumun, her ne kadar yapay zeka gelişmeleri için başlangıçta hedef insan kabiliyetlerine ulaşmak olsa da; bugün bazı insan kabiliyetlerini ve kapasitesini aşan yapay zeka programları karşısında yapay zeka algısının değişmekte olması ve bu sebeple daha üst bir tanım yapılması gerekmesinden ileri geldiği kanaatindeyiz.

Her ne kadar McCarthy, yapay zekanın amacının, dünyadaki sorunları çözebilen ve hedeflere insanlar kadar kolay ulaşabilen bilgisayar programları yapmak olduğunu ifade etse de⁴²; derin öğrenme yaklaşımı ile birlikte YZ alanında birçok atılımın yaşandığı, alanda aşağıda açıkladığımız üzere hatırı sayılır gelişmenin olduğunu⁴³ ve bugün insan ötesi yapay zeka programlarının yapılmasının amaçlandığını belirtmek gerekir. Ezcümle, yapay zekanın gelişmesinde artık hedefin insan kabiliyetleri olmadığı söylenebilir.

1.3. Yapay Zeka’nın Tarihsel Yolculuğu

Yapay zeka kavramından nispeten uzun bir gelişim tarihine sahip ve sürekli olarak yeni gelişmeler ile ilerlemeye devam eden teknolojiler bütününe anlaşılmalıdır⁴⁴. Dolayısıyla, yapay zekanın tam olarak anlaşılabilmesi için tarihsel gelişimi incelenmelidir.

Her ne kadar “*Düşünen Makina*” kavramı antik Yunana dayansa da; yapay zekayı basit bir şekilde, yaklaşık 80 yıldan uzun bir süredir ortaya çıkan bir dizi iç içe geçmiş kavramlar bütünü olarak düşünebiliriz. İlk YZ kabul edilen çalışma 1943 yılında öne sürülen Warren McCulloch ve Walter Pitts’in “yapay nöronlar” tasarımıdır. Bu sistem, her bir nöron yeterli sayıda koşu nöron tarafından uyarılması ile meydana gelen “açık anahtar” ile nöronların açık veya kapalı olarak nitelendirildiği bir nöron sistemidir. Ardından, 1945 yılında, Vannevar Bush “*As We May Think*” isimli çalışmasında insanların kendi bilgi ve anlayışlarını güçlendirebilecekleri bir sistem önerisinde bulundu. 1950 yılında Alan Turing’in, “*Computing Machinery and Intelligence*” başlıklı makalesinde “Makinalar düşünebilir mi?” diye bir soru sordu böylece yapay zeka yolculuğunu başlattı⁴⁵.

⁴² McCarthy, 2007, s.5.

⁴³ Bugün bir bilgisayar, bir beyinden milyon kat daha hızlı bir çevrim süresine sahiptir. Russell ve Norvig, 2024, s.12.

⁴⁴ Atalan, S. E (2024) . *Uluslararası hukuk bağlamında Avrupa’da yapay zekaya ilişkin düzenlemeler ve kişisel verilerin korunması* (Yayımlanmamış yüksek lisans tezi) İstanbul Üniversitesi. s.5.

⁴⁵ Turing, A. M (1950) . Computing machinery and intelligence. *Mind*, 49, s. 433–460. <https://courses.cs.umbc.edu/471/papers/turing.pdf> (Erişim tarihi: 21 Mayıs 2025); McGuire, B (2006) . The Turing test (pp. 5–9) . In C. Smith (Ed.), *The history of artificial intelligence*. University of Washington., Russell ve Norvig, 2024, s.17-18, Smith, C (Ed.) (2006) . *The history of artificial intelligence*. University of Washington.

"Yapay zeka" terimi ise ilk defa 1956 yılında, Dartmouth College'daki konuyla ilgili konferansında John McCarthy tarafından kullanıldı. Henüz YZ ismi yeni konulsa da, ufuk açıcı gelişmeler çoktan yaşanmıştır. Nitekim, bu konferansta, makinaların dili kullanması, soyutlamalar yapması, insana özgü problemleri çözmesi ve kendilerini geliştirmeleri üzerine alanında uzman kişilerin katılımı ile konuşmalar yapılmıştır⁴⁶. Aynı yılın ilerleyen zamanlarında Allen Newell, JC Shaw ve Herbert Simon, çalışan ilk yapay zeka programı olan Logic Theorist'i⁴⁷ geliştirdiler. Her ne kadar başlangıçta geliştiricilerin hayal ettikleri insan gibi düşünebilen, öğrenebilen ve akıl yürütebilen makinalar inşa etmek olsa da; ilk yapay zeka uygulamaları oldukça emek isteyen, "*sorunu bul-çöz-çözümü kodla- uygula*" yöntemiyle çalışan, geleneksel programlamaların kullanıldığı kural tabanlı yaklaşımlar içeren kısıtlı uygulamalardı. Bu yaklaşıma GOFAI (Good Old-Fashioned AI), yani "*Güzel, Nostaljik Yapay Zeka*" dendi ve 1970-1990 dönemi "*Birinci Dalga*" olarak isimlendirildi⁴⁸.

New York, Buffalo'daki Cornell Havacılık Laboratuvarı'nda, daha sonra Biyoloji Bilimleri Bölümü'nde nörobiyoloji ve davranış doçenti olacak olan araştırma psikoloğu ve proje mühendisi Frank Rosenblatt, deneme yanılma yoluyla "*öğrenen*" bir sinir ağına dayalı ilk bilgisayar olan Mark 1 Perceptron'u⁴⁹ oluşturmuştur. Bilgisayar ve Bilişim Bilimleri profesörü olan Thorsten Joachims, bu gelişmeyi "*Tüm bu yapay zekanın temelleri Cornell'de atıldı.*" şeklinde yorumlamaktadır. 1969 yılında, Marvin Minsky ve Seymour Papert, hem sinir ağları

<https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf> (Erişim Tarihi: 23.05.2025); McCarthy, 2007, s. 4; IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18.05.2025). İngiliz matematikçi Alan Turing, Alman enigma kodunu kıran ünlü bir bilim adamıdır. "Turing Testini" geliştirmesi ile bilgisayar sunucusu ile insan arasında ayırım yapabilen bir program geliştirmiştir. Buna göre, eğer makina bilgi sahibi bir gözlemciye insan gibi davranmayı başarabilirse zeki kabul edilmelidir. Yapay zeka tarihi için bir mihenk taşı olan bu test birçok güncelleme ile hala kullanılmaktadır. Turing, A. M (1950). Computing machinery and intelligence. *Mind*, 49, s. 433-460. <https://courses.cs.umbc.edu/471/papers/turing.pdf> (Erişim tarihi: 21 Mayıs 2025); 1950 yılında sunulan Turing Testi, 2014 yılına kadar çözülemedi. Rus Vladimir Veselov, Ukraynalı Eugene Demchenko ve Sergey Ulasen isimli üç program yazılımcı tarafından geliştirilen "Eugene Goostman" isimli yapay zeka programı, 7 Haziran 2014 tarihinde Turing Testi'ni geçebildi. Böylece "Eugene" tarihte Turing testini geçebilen ilk program oldu. Bkz. Bilişim Dergisi (2014, Temmuz). Bilgisayar yazılımı ilk kez testi geçti. *Bilişim Dergisi*, 167, 74-75. <https://www.bilisimdergisi.org.tr/s167/pdf/74-75.pdf> (Erişim tarihi: 23.05.2025)

⁴⁶Russell ve Norvig, 2024, s.17-18; Smith, 2006, s. 5; IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); Güçlütürk, 2022, s.31.

⁴⁷Smith, 2006, s. 5; IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); Ayrıntılı bilgi için bkz. Newell, A., and Simon, H. A (1956). The logic theory machine—A complex information processing system. *IRE Transactions on Information Theory*, 2 (3), 61-79.

⁴⁸Tübitak Bilgem. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18.05.2025).

⁴⁹Mark I Perceptron'un ilk versiyonunu 1958 yılında, bir oda büyüklüğünde ve 5 tona karşılık gelen IBM 704 ile bir dizi delikli kartla oluşturuldu. 50 denemeden sonra, bilgisayar kendisine soldaki işaretli kartları sağdaki işaretli kartlardan ayırt etmeyi öğrendi. Sistemin yaratıcısı Frank Rosenblatt'a göre bu, "orijinal bir fikre sahip olabilen ilk makine" olan "perceptron"un bir gösterimiydi. Lefkowitz, M (2019, September). Professor's perceptron paved the way for AI – 60 years too soon. *Cornell Chronicle*. <https://news.cornell.edu/stories/2019/09/professors-perceptron-paved-way-ai-60-years-too-soon> (Erişim tarihi: 24 Mayıs 2025). Ayrıca bkz. Rosenblatt, F (1960, March). Perceptron simulation experiments. *Proceedings of the IRE*, 48 (3), 301-309.

üzerine çığır açan bir çalışma hem de en azından bir süreliğine gelecekteki sinir ağı araştırma girişimlerine karşı bir argüman haline gelen “*Perceptrons*” isimli bir kitap yayınladılar⁵⁰.

Ne var ki, heyecanla yaklaşıl原因 yapay zeka alandaki gelişmeler beklenenden oldukça yavaş ilerledi. 1970 sonrasında gelişen bu duraklama dönemine “*Yapay Zeka Kışı*” denilmiştir. Bir görüşe göre bu durum, başlangıçta geliştiricilerin insan zekasının karmaşıklığını hafife almalarından ileri gelmektedir⁵¹. Gelişmelerin yavaşlaması sonucunda, hükümetler tarafından sağlanan fonlar kesildi. Bu dönemde “*Makine Öğrenimi*”, “*Enformatik*”, “*Bilgi tabanlı sistem*” ve “*Örüntü tanıma*” gibi yapay zekaya ilişkin disiplinler yapay zeka ismi kullanılmadan ortaya çıkartıldı. Böylece, yapay zeka araştırmacıları, araştırma konularını gizleyerek fon almaya çalıştılar⁵². Bilgi işlem gücünde yaşanan gelişmeler ve World Wide Web’in (İnternet) kurulması oluşturulan büyük veri kümeleri, makina öğrenme algoritmalarının geliştirilmesini sağladı. Büyük veri sayesinde geliştirilen makinelerin öğrenmesi yaklaşımı yapay zekanın ticari yönünün tekrar canlanmasını sağlamıştır⁵³.

1970’li yıllarda başlayan çalışmalar nihayetinde ilk uzman sistem yapay zeka programlarından biri olan MYCIN, 1974 yılında kandaki bakteriyel enfeksiyonları tespit eden ve tedavi yöntemleri öneren bir program olarak piyasaya sürüldü. Bu programın etkili, kolay kullanılabilen ve güvenilir sonuçlar verdiği iddiası, MYCIN yapay zeka programının çıktılarının birçok tıp öğrencisi ve pratisyen hekimden daha doğru sonuçlar vermesi ile ispat edildi⁵⁴. 1997 yılına gelindiğinde makineler için tarihi bir an yaşandı. IBM tarafından geliştirilen Satranç Programı, daha önce hiçbir makinanın yapamadığı bir şeyi yaptı. Dünya şampiyonu satranç maçında Garry Kasparov’u hem oyunda hem de altı oyunluk maçta hem de maçın rövanşında yenen Bilgisayar Programı yapay zekaya karşı bakışları değiştirerek bir makinanın strateji gerektiren kararlarda insanları yenebileceğini tüm dünyaya gösterdi⁵⁵. Bu gelişme satranç dünyasının sınırlarını aştı ve kullanılan teknoloji, makinelerin yeni ilaçlar keşfetmek, finansal riski değerlendirmek, devasa veri tabanlarındaki kalıpları ortaya çıkarmak ve insan genlerinin iç işleyişini keşfetmek için gereken karmaşık hesaplamaları ele alma yeteneklerinin geliştirilmesinde kullanıldı⁵⁶. Yapay zekanın insan karşısındaki durumunu tespit

⁵⁰ Lefkowitz, 2019, <https://news.cornell.edu/stories/2019/09/professors-perceptron-paved-way-ai-60-years-too-soon> (Erişim Tarihi: 24.05.2025); IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025).

⁵¹ Huang, T (2006) . Expert systems. In C. Smith (Ed.), *The history of artificial intelligence*. University of Washington, s.16.

⁵² Yang, G (2006) . AI winter and its lessons. In C. Smith (Ed.), *The history of artificial intelligence*. University of Washington. s. 17-21; Smith, 2006, s.4-5. Turing, 1950, s. 433-460; McCarthy, 2007, s. 4; IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18.05.2025) .

⁵³ Russell ve Norvig, 2024, s.26, 83.

⁵⁴ Shortliffe, E. H (1977) . Mycin: A knowledge-based computer program applied to infectious diseases. In *Proceedings of the Annual Symposium on Computer Application in Medical Care*, s.66-69; McCarthy, 2007, s.11.

⁵⁵ IBM. *Deep Blue*. <https://www.ibm.com/history/deep-blue> (Erişim tarihi: 20.05.2025); Smith, C (2006) . History of AI applied to chess. In C. Smith (Ed.), *The history of artificial intelligence* (s. 10) . University of Washington. s. 10. Deep Blue, satranç becerisini hesaplama yeteneği ile elde etti. Bir dizi koordineli, yüksek hızlı hesaplamayı aynı anda gerçekleştirmek için 32 işlemci kullandı. Deep Blue, saniyede 200 milyon satranç pozisyonunu değerlendirebildi ve saniyede 11,38 milyar işlem hızına ulaşabildi. IBM, *Deep Blue*, <https://www.ibm.com/history/deep-blue> (Erişim Tarihi: 20.05.2025) .

⁵⁶ IBM, *Deep Blue*, <https://www.ibm.com/history/deep-blue> (Erişim Tarihi: 20.05.2025) .

etmek veya sergilemek için daha birçok oyunda yapay zeka ve insan taraflar yarıştırmış, yapay zeka bu oyunlardan da galibiyetle ayrılmıştır⁵⁷.

Birinci dalga yapay zeka sistemlerinin gelişimlerinin kısıtlı olduğu fark edildikten sonra geliştirilen insan gibi düşünen makinaların üretimi için insanların sahip olduğu nöron yapısını temel alan ve taklit eden “*yapay sinir ağı*” yaklaşımı geliştirildi ve yapay zeka uygulamalarında yaygın olarak kullanılmaya başlandı. 2000’li yıllardan başlayan; 2010’lu yıllarda teknoloji ve işlemci gücünde gerçekleşen gelişmelerle çok katmanlı yapay sinir ağlarının geliştirilmesine izin veren derin öğrenme yaklaşımıyla güçlenen ve günümüze kadar devam eden süreç “*ikinci dalga*” denilmiştir. Bu dönemde ayrıca, yapay zekanın eğitilmesinde kullanılacak büyük veri ve bulut bilişim çağları başlamış böylece veri bilimi popüler bir disiplin haline gelmiştir. İkinci dalgada, derin öğrenme kullanılarak geliştirilen dar kapsamlı yapay zeka uygulamaları, bugün özellikle karmaşık verileri ve ilişkilerin çözülmesinde, iyi tanımlanmış belirli görevlerde özelleştirilmiş çözümlere sahiptir⁵⁸.

2022 yılına gelindiğinde; Open AI ve ChatGPT gibi LLM gibi yapay zeka uygulamalarında büyük dil modellerinin kullanılmasındaki artış, kurumsal değerlendirme yönlendirme potansiyelinde değişiklik yaratmaya başlamıştır. Bugün kullanılan yapay zeka trendlerinin devam eden Yapay Zeka Rönesansının bir göstergesi olduğu ifade edilmektedir. Günümüzden 2030’lara uzanan dönem “*üçüncü dalga*” olarak isimlendirilmiştir. Dar kapsamlı yapay zeka uygulamaları ile istenilen sonuca ulaşılmayacağının görülmesi ile yapay zeka uygulamalarına bağlamsal adaptasyon yeteneği kazandırılarak, derin pekiştirmeli öğrenme sağlanması ve etiketli veri ile çalışma bağımlılığını böylece büyük veri kümelerine olan ihtiyacı ortadan kaldırabilmesi amaçlanmıştır⁵⁹. İnsan düzeyi yapay zeka uygulamalarına giden bu yolda bilişsel mimari yeteneklerini kazanan uygulamalar, insanların nasıl öğrendiklerine çok daha benzer bir şekilde öğrenme yeteneğine sahip olacakları umulmaktadır⁶⁰.

⁵⁷2011 yılında IBM tarafından geliştirilen Watson programı, ABD yarışma programı bilgi yarışması olan *Jeopardy!*’de şampiyonlar Ken Jennings ve Brad Rutter’ı yendi; 2015 yılında Baidu’nun Minwa süper bilgisayarı, özel bir derin sinir ağı kullanarak verilen görüntüleri ortalama bir insandan daha yüksek bir doğruluk oranıyla tanımladı ve kategorilere ayırdı. 2016 yılında, DeepMind’in derin bir sinir ağıyla desteklenen AlphaGo programı, beş oyunluk bir maçta dünya şampiyonu Go oyuncusu Lee Sudo’lu yendi. Böylece yapay zeka uygulamaları, insanlara fark atmaya devam etti. Smith, 2006, s. 10-11; IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025)

⁵⁸TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18.05.2025) . IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025) . Gösterdikleri başarılar ile göz kamaştıran bu yapay zeka uygulamalarına, birden çok dar kapsamlı yapay zeka uygulamasının birleştirilmesi ile meydana gelen sürücüsüz otomobiller güzel bir örnektir Bu yapay zeka uygulamalarının algı, karar verme ve kontrol olarak üç ana yetenekleri bulunmaktadır. İkinci dalga yapay zekanın bir başka sınırlaması, çok miktarda eğitim verisine bağımlı olmasıdır. Örneğin, kedileri tanımak için geliştirilecek bir derin öğrenme algoritmasının kabul edilebilir bir doğruluk seviyesinde sonuç verebilmesi için on binlerce kedi fotoğrafıyla eğitilmesi gerekir. Bu aslında üç yaşındaki bir çocuğun sadece birkaç örnek gördükten sonra başarabileceği bir şeydir. TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18.05.2025) .

⁵⁹Böylelikle, yapay zeka uygulamaları yalnızca kediyi tanımakla kalmayacak, aynı zamanda neden bir kedi olduğunu ve bu sonuca nasıl ulaştığını açıklayabilecektir. TÜBİTAK BİLGEM, *Üçüncü Dalga Yapay Zeka Teknolojileri*, https://b3lab.org/sayfalar/yapay_zeka-12/ . Erişim Tarihi: 18.05.2025.

⁶⁰IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18.05.2025) .

1.4. Yapay Zeka Türleri

Yapay zeka gelişmişlik düzeyine göre ayrılmıştır. Bunlar: Zayıf Yapay Zeka diğer adıyla Dar Kapsamlı Yapay Zeka (*Artificial Narrow Intelligence*), Güçlü Yapay Zeka diğer adıyla Genel Yapay Zeka (*İnsan Düzeyi*) Yapay Zeka (*Artificial General Intelligence*) ve Süper Yapay Zeka (*İnsan Ötesi*) Yapay Zekadır (*Artificial Super Intelligence*)⁶¹.

Dar yapay zeka uygulamaları belirli bir görevi ya da birkaç görevi yerine getirmek için geliştirilmiştir. Amazon markasının Alexa asistanı, Apple markasının Siri asistanı, bir sosyal medya sohbet robotu veya Tesla'nın otonom araçlar gibi "akıllı" sesli asistan uygulamaları ile Trendyol'un öneri algoritması ile sevebileceğinizi düşündüğü t-shirtleri önermesi dar yapay zeka uygulamalarına örnektir. Bu uygulamalar görevleri dışında bir şey yapamazlar, zayıflardır. Güçlü Yapay Zeka ise insan zekasına eşit veya onu aşan çok çeşitli bilgiyi anlama, öğrenme ve uygulama yeteneğine sahip olan yapay zeka türüdür. Bu tür kendini farkındadır, sağduyulu muhakeme yeteneğine sahiptir, insanlar gibi düşünebilir, genel bilgidan faydalanır, kendi amacını tanımlayabilir ve dünyayı ele geçirmede tehdit olarak algılanır. Güçlü yapay zeka uygulamalarının günümüzde hala bir idea olduğunu söyleyebiliriz. Nitekim, bugün bilinen YZ sistemleri bu türün yanından dahi geçememektedir. Şu anda kullanılan YZ sistemleri dar yapay zeka türüne örnektir. Süper yapay zeka ise insan kabiliyetleri ve zekasını aşan, insan ötesi yapay zeka uygulamalarını ifade etmektedir⁶². Henüz güçlü yapay zeka uygulamalarına erişemeyen teknoloji için süper yapay zeka teknolojisi uzak bir gelecek gibi gözükmemektedir.

Yapay zekanın fiziksel bir donanıma sahip olup olmamasına göre bir ayrıma tabi tutulmadığını belirtilelim. Nitekim, yapay zeka programları yazılım tabanlı olabileceği gibi sistem sadece sanal dünyada da var olabilirler(örneğin sesli asistanlar) veya donanım cihazlarına yerleştirilebilir(robotlar, sürücüsüz arabalar ve dronlar örnek olarak verilebilir). Fakat yapay zeka ayrımlarında fiziken var olma faktörü bir ayrım sebebi olarak görülmemiştir. Bu özellik yalnızca teknikler ve yaklaşımlar yönünden gözetilmiştir⁶³.

1.5. Yapay Zeka Teknikleri

Yapay zeka aslında büyük bir şemsiyedir. YZ, makine öğrenimi (derin öğrenme, pekiştirmeli öğrenme), makine yorumlaması (planlama yapma, bilgi temsili ve muhakeme, arama ve optimizasyon) ve robotik (siber-fiziksel sistemlere entegrasyonunu sağlayan kontrol,

⁶¹ Sterne, 2017, s.30-31; TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. <https://b3lab.org/sayfalar/yapay-zeka-12/> (Erişim tarihi: 18.05.2025); IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025). Bugüne kadar birlikte yaşadığımız zayıf yapay zeka uygulamalarının, yapay zekanın olgunluk dönemini yansıttığı söylenebilir. Aygün, 2023, s.33; Sterne, 2017, s.30 High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019). *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025).; Russell ve Norvig, 2024, s.22.

⁶² Sterne, 2017, s.30-31; TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. <https://b3lab.org/sayfalar/yapay-zeka-12/> (Erişim tarihi: 18.05.2025); IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025). Bugüne kadar birlikte yaşadığımız zayıf yapay zeka uygulamalarının, yapay zekanın olgunluk dönemini yansıttığı söylenebilir. Aygün, 2023, s.33; Sterne, 2017, s.30 High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019). *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025).; Russell ve Norvig, 2024, s.22.

⁶³ bkz. "Robotik" başlığı.

algılama, sensörler ve aktüatörler ve diğer teknikler) gibi birçok yaklaşım ve teknikleri kapsamaktadır. Yapay zeka programları bugün genellikle tek bir sistemden değil; pek çok sistemin birleşmesiyle oluşmaktadır⁶⁴.

Yapay zekanın besisi kaynağı verilerdir. Nitekim YZ, veriler vasıtası ile eğitilir, öğrenir ve şema oluşturabilir⁶⁵. Genel olarak yapay zeka sistemlerinde, bulunduğu çevreyi anlama, verileri toplamaya bilgi haline getirme ve bu bilgileri işleyerek yorumlama yapma, karar verme ve karar sonucunu uygulama(harekete geçme) aşamaları ve özellikleri bulunmaktadır. Sistemin öğrenen bir sistem olması halinde hareket aşamasından sonra yanıt bekleme ve olumlu geri bildirimde hareketi pekiştirme ve olumsuz geri bildirim halinde sistemin kendini uyarlaması aşamaları da bulunur⁶⁶. Aşağıda yapay zeka tekniklerinden öne çıkan ve en çok uygulanan yaklaşımlardan birkaçı incelenmiştir.

1.5.1. Makina öğrenmesi (Machine learning)

Makina öğrenmesi genellikle yapay zeka ile eş anlamlı şekilde kullanılmaktadır. Makina öğrenmesi, bir algoritmayı verilere dayalı tahminler veya kararlar üretmesi için eğitilerek yeni modeller oluşturulmasını ifade etmektedir. Başka bir anlatımla, bir sistemin, belirli bir görevi nasıl çözebileceğini anlamasına makina öğrenmesi denilmektedir. Makina öğrenmesi, katı kuralları içeren bir sistem değildir; tersine sisteme öğrenmesi için alan tanınmıştır. Çünkü burada amaçlanan makinanın kendi kendine öğrenmesidir. Öncelikle sistemin eğitilmesi için veri setleri oluşturulur ardından model oluşturulur. Model oluşturulduktan sonra eğitim veri setinde yer alan veriler modele girdi olarak verilir. Bu teknikte açık programlama olmadan örüntüleri keşfetmek ve tahminlerde bulunmak veya kararlar almak amacıyla sistemleri "eğitmek" için istatistiksel yöntemler ve algoritmalar kullanılır⁶⁷. Algoritmalar, kedi resimlerini tanımlamaktan müzik tercihlerini tahmin etmeye kadar, karar vermek için kullandıkları dünyaya ilişkin perspektifler geliştirir⁶⁸.

Makina öğrenmesi, makinanın verilerden öğrenmesini ve çıkarımlar yapabilmesini sağlayan bir dizi teknik yelpazeyi kapsamaktadır. Başlangıçta sisteme girilen veriler ve belirli bir görev vardır. Burada sistem, verilerden hareketle algılama, veriyi yorumlama, bilgi işleme,

⁶⁴ Sterne, 2017, s.20; Büyüközkan Feyzioğlu, 2021, s. 5 High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .

⁶⁵ IBM. *Unstructured data*. <https://www.ibm.com/think/topics/unstructured-data> (Erişim tarihi: 19.05.2025)

⁶⁶ High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .

⁶⁷ S Sterne, 2017s.29-31, GREENGARD, 2019, Büyüközkan Feyzioğlu, 2021,, s. 6, Russell ve Norvig, 2024, s.651 vd., IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); Güçlütürk, 2022, s. 58-68; IBM, *What is AI?* , https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai . Erişim Tarihi: 19.05.2025; High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .

⁶⁸ European Parliament (2020, Haziran) . *Artificial intelligence: How does it work, why does it matter, and what can we do about it?* Panel for the Future of Science and Technology. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU\(2020\)641547_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf) (Erişim tarihi: 20.05.2025) .

bugün için kısıtlı karar alma ve harekete geçme adımlarını takip eder. Sistemin görevi tamamlamasının ardından, muhakeme yaparak yapmaya karar verdiği ve gerçekleştirdiği eylem nihayetinde ne kadar başarılı olduğunun geri dönüş yanıtını kullanıcı veya geliştiriciden alması gereklidir. Geri dönüş pozitif ise, program, bu çözümü benzer görevlere de uygular. Geri dönüşün negatif olması durumunda, sistemin nereye yanlış yaptığına dair bilgilendirilmelidir. Bilgilendirme akabinde yapay zeka sistemi, muhakeme kurallarını ve karar verme yönetimini verilen bildirim doğrultusunda yeniden uyarlar⁶⁹.

Her bir makina öğrenmesi türü farklı türden sorunlara ve verilere uygundur⁷⁰. Sahte mesajları, kredi kartı yolsuzluklarını ve Amazon, Netflix, Youtube, Facebook gibi birçok şirket kullanıcının geçmiş deneyimlerden ve benzer kullanıcı deneyimlerden yararlanarak tercihleri kişiselleştirmesinde ve kullanıcının neyi sevebileceği film veya ürünler hakkında önerilerde bulunmasında makina öğrenmesi teknikleri kullanılmaktadır⁷¹.

1.5.1.1. Pekiştirmeli öğrenme

Makina öğrenimi yaklaşımlarından pekiştirmeli öğrenme sisteminde sistem zaman içinde kararlarını vermekte özgür bırakılır. Sistemin her bir karar çıktısında sisteme iyi veya kötü bir karar aldığına ilişkin bir ödül sinyali verilir. Sistemin amacı, alınan ödülü maksimize etmektir. Bu yaklaşım, örneğin tavsiye sistemlerinde (kullanıcılara ne satın almak isteyebileceklerini öneren çeşitli çevrimiçi tavsiye sistemleri gibi) veya pazarlamada kullanılır⁷².

1.5.1.2. Yapay sinir ağı

Günümüzde en popüler makina öğrenmesi türlerinden biri Yapay Sinir Ağı'dır. Yapay sinir ağı, insan beyninin yapısı ve işlevine taklit edilerek insan sinir sisteminde var olan nöron ağı modellemesinin yapay zeka programlarına uygulanması ile oluşturulmuştur. Katmanlar(Nöron) birbiri ile bağlantılı olacak şekilde tasarlanmıştır. Böylece yapay zeka sistemleri öğrenebilir, hafızasına bilgiyi yerleştirebilir ve veriler arasındaki ilişkiyi ortaya çıkarabilir. Yapay sinir ağı tekniği ile bu yetenekler ve çok daha fazlasının YZ'ya kazandırılmasını sağlamıştır⁷³. Birçok karmaşık görevi çözebilen ve bu çözümleri otomatikleştirebilen yapay sinir ağları yapısında, girdi, çıktı ve bu iki katman arasında kalan gizli katmanlar bulunmaktadır. Yapay sinir ağları özellikle sınıflandırma, teşhis, örüntü tanıma,

⁶⁹ Sterne, 2017s.29-31, GREENGARD, 2019, IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .

⁷⁰IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .

⁷¹Russell ve Norvig, 2024, s.29; Büyüközkan Feyzioğlu, 2021, s. 6.

⁷²High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025); Russell ve Norvig, 2024, s.789.

⁷³TÜBİTAK BİLGEM. *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18.05.2025) . IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); Büyüközkan Feyzioğlu, 2021, s. 8.

veri sıkıştırma, optimizasyon, veri madenciliği, optimum rota belirleme, iş çizelgesi hazırlama gibi görevler için kullanılmakta ve bu görevlerde başarı göstermektedir⁷⁴.

1.5.2. Derin öğrenme (Deep learning)

Derin öğrenme esasında bir makine öğrenimi alt kümesidir. Fakat klasik makine öğrenimi türlerinde kullanılan yapay sinir ağı yaklaşımının üst segmenti olarak karşımıza çıkmaktadır⁷⁵. Görevler karmaşık hale geldiğinde makina öğrenmesi yeterli olmamakta; derin öğrenme methodu devreye girmektedir. Derin öğrenme, büyük veri setlerini analiz etmek, görüntü ve ses tanıma, doğal dil işleme, tahmin ve sınıflandırma gibi birçok yapay zeka fonksiyonun gerçekleştirilmesinde kullanılmaktadır⁷⁶.

Çok geniş teknikleri içeren derin öğrenme yaklaşımı ile yapay zeka alanında adeta oyunun kuralları tekrar yazılmıştır. Görüntü veya konuşma tanıma veya makine çevirisi gibi belirli görevler için performansta muazzam bir iyileşme sağlayan ve sürekli öğrenen derin öğrenme algoritmasının eğitilebilmesi için çok sayıda etiketli veriye ihtiyaç duyulmaktadır. Algoritmalar eğitildikten sonra, daha önce hiç görmedikleri nesneleri doğrulukla sınıflandırabilirler. Yapay zekanın bu fonksiyonunun bazı durumlarda insan yeteneklerini aştığını belirtilmelidir⁷⁷. Limitsiz veri ve işlem gücü, yeni algoritmalar ve açık sistemlerle desteklenen derin öğrenme, 2010 yılından bu yana yapay zeka uygulamalarının itici gücünü oluşturmuştur⁷⁸.

İnsan beyninin karmaşık karar verme gücünü daha yakından taklit eden ve derin sinir ağları olarak adlandırılan çok katmanlı sinir ağlarını kullanan derin öğrenmenin bir giriş katmanı ve en az üç olmak üzere yüzlerce gizli katmanı ve bir çıkış katmanı bulunmaktadır. Klasik modellerde ise genellikle yalnızca bir veya iki gizli katmana sahip sinir ağları bulunmaktadır. Bu fonksiyon sayesinde derin öğrenme, gözetimsiz öğrenmeye olanak tanır. Böylece uygulamalar derin öğrenme metodunu kullanarak büyük, etiketlenmemiş ve yapılandırılmamış veri kümelerinden özelliklerin çıkarılmasını otomatikleştirebilir ve verilerin neyi temsil ettiğine dair kendi tahminlerini yapabilirler. Büyük ölçüde güçlü bir donanıma ihtiyaç duyan derin öğrenme, minimum insan müdahalesini mümkün kılmaktadır⁷⁹.

Derin öğrenmenin güzel örneklerinden biri olarak Google Translate verilebilir. Hem metin tabanlı hem de görsel çeviri yapabilen bu sistem, evrimsel bir sinir ağı yaklaşımını

⁷⁴ Büyüközkan Feyzioğlu, 2021, s. 8.

⁷⁵IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .; Büyüközkan Feyzioğlu, 2021, s. 6.

⁷⁶ Sağtaş, S (2023) . Yapay zeka uygulamalarının e-ticarete kullanımı. In T. Yolcu & K. Özkaynar (Ed.), *Yapay zeka ve pazarlama* .Nobel Yayıncılık, s.53.

⁷⁷ European Commission (2018, April 25) . *Artificial intelligence for Europe* (COM (2018) 237 final) . <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Erişim tarihi: 20.05.2025); Russell ve Norvig, 2024, , s.750 vd., Büyüközkan Feyzioğlu, 2021, s. 6.

⁷⁸ Büyüközkan Feyzioğlu, 2021, s. 7.

⁷⁹IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025); High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) . Russell ve Norvig, 2024, s.27.

uygulanmaktadır. Özellikle görsel çeviride bizleri şaşırtan sistem kirli ve bulanık metinleri bile algılamakta ve çevirilerini gerçekleştirebilmektedir. Yapay zeka programı öncelikle büyük bir veri kümesi ile eğitilmekte, girdi yapılan harf ve kelimeleri algılayabilir hale getirilmekte, tespit edilenlerin sözlük vasıtası ile en yakın anlamı tespit etmekte ve istenilen çeviriyi orjinal dilde sunabilmektedir⁸⁰.

1.5.3. Uzman sistemler

Uzman sistemler, bir veya daha fazla bilgi alanında insan uzmanlığını modellemeyi amaçlayan sistemlerdir. Bu sistemlerin genellikle üç temel bileşeni bulunmaktadır: veri tabanı (insan bilgi ve deneyimi içeren bilgiler ve kurallar), çıkarım motoru (değerlendirmenin yapıldığı ve çıkarımların nasıl yapıldığını belirleyen sistem) ve giriş ve çıkış arayüzü (kullanıcı ile etkileşimin sağlanması için). Uzman sistemlerin temel motivasyonu, uzmanların beyin gücünden yararlanarak insanlara yardımcı olmaktır⁸¹. Nitekim, bu güdü, yapay zekanın en olumlu potansiyellerinden biridir. Sağlık hizmetleri, kimyasal analiz, kredi yetkilendirme, finansal yönetim, kurumsal planlama, petrol ve maden arama, genetik mühendisliği, otomobil tasarımı ve üretimi ve hava trafiği kontrolü gibi geniş bir yelpazede uzman sistemler kullanılmaktadır⁸².

1.5.4. Doğal dil işleme (Natural language processing)

Doğal Dil İşleme(NLP), temelde makinelerin insan dilini okumasını, anlamasını ve yorumlamasının sağlanması amacıyla kullanılmaktadır. Modern dil biliminin ve yapay zekanın doğuşu aynı zaman aralığında gerçekleşmiştir. Bu iki disiplin doğal dil işleme(NLP) veya hesaplama dil bilimi de denilen disiplin altında birlikte gelişteler. Bilginin programlarda akıl yürütmeye yarayacak bir hale getirilmesi dile bağlıydı bu sorunun çözülmesinde dilbilim araştırmaları etkin rol oynadı. Bu oldukça zor bir uğraş oldu çünkü dili anlamak, yalnızca cümle yapılarını anlamayı değil; aynı zamanda konuyu ve bağlamı da anlamayı gerektiriyordu⁸³. Yapay zeka dil modelleri genellikle bir temel ile başlar. Bir temel model oluşturmak , genellikle internetten gelen büyük hacimli yapılandırılmamış veriler üzerinde derin öğrenme algoritması ile eğitilerek gerçekleştirilir. Bu yapılandırılmamış veriler zengin ve çeşitlidir ve YZ modellerine bağlam ve nüans öğretmektedir³.

Doğal dil işleme sistemlerini kullanmasının üç temel ana sebebi vardır. Bunlar: sistemlerin insanlar ile iletişim kurmasının sağlanması, sistemin öğrenilmesinin sağlanmak istemesi (sistemin öğrenilmesi isteniyorsa doğal dili iyi anlamalıdır çünkü doğal dil kullanılarak birçok bilgi yazılı hale getirilmiştir) ve son olarak yapay zekanın dil biliminin gelişimine katkıda bulunması amacı. Bu yapay zeka sisteminin metin çevirisi, duygu analizi, konuşma gibi görevleri bulunmaktadır.⁸⁴

⁸⁰ Good, O (2015, July 29) . *How Google Translate squeezes deep learning onto a phone*. Google AI Blog. <https://ai.googleblog.com/2015/07/how-google-translatesqueezes-deep.html> (Erişim tarihi: 26.05.2025)

⁸¹ Huang, T (2006) . Expert systems. In C. Smith (Ed.), *The history of artificial intelligence* (s. 12–15) . Seattle: University of Washington., s.12-15; Büyüközkan Feyzioğlu, 2021, s. 9.

⁸² Huang, 2006, s.12.

⁸³Russell ve Norvig, 2024, s.16-17; Greengard.

⁸⁴Russell ve Norvig, 2024, s.823; Greengard.

1.5.5. Üretken AI (Gen AI)

Üretken Yapay Zeka diğer bir adıyla Gen AI, bir kullanıcının istemine veya isteğine yanıt olarak uzun biçimli metinler, yüksek kaliteli resimler, gerçekçi video veya ses ve daha fazlası gibi karmaşık orijinal içerikler oluşturabilen derin öğrenme modellerini ifade eder. Üretken yapay zeka modelleri, temelde yapay zekaya temel bir eğitim modeli oluşturulması, modeli belirli bir uygulamaya uyarlayarak ve son olarak doğruluk ve işlerliğini arttırmak için üretim, değerlendirme ve daha fazla ayarlama yapılması ile oluşturulur⁸⁵. Üretken Yapay Zeka insanlar tarafından üretilmesi zaman alacak nitelik ve kalitede içerikleri çok kısa sürede üretebilmektedir⁸⁶. Üretimin gerçekleştirilmesinde dijital görüntüdeki yer, nesne, insan ve diğer faktörleri tespit edebilen yapay zeka sistemleri ile görüntünün elde edilmesi ve işlenmesi gibi becerilere sahip olan görüntü işleme yapay zeka sistemleri kullanılabilir⁸⁷.

En yaygın temel modeller metin içerikleri üreten LLM yani büyük dil modelleridir. Bundan başka ses, müzik, görüntü ve çok çeşitli başka modeller üretilmesi için çok biçimli temel modeller de bulunmaktadır. Bir temel model oluşturmak için uygulayıcılar, internetten terabaytlarca veya petabaytlarca veri, metin veya resim veya video gibi büyük hacimli ilgili ham, yapılandırılmamış, etiketlenmemiş veriler üzerinde derin öğrenme algoritması eğitir. Böylece milyarlarca *parametrelili* bir sinir ağı üretilir ve bu da taleplere yanıt olarak bağımsız bir şekilde içerik üretilebilmesini sağlar. Eğitim süreci oldukça pahalı, zaman alan ve yoğun emek isteyen bir süreçtir. Daha sonra, model belirli bir içerik oluşturma görevine göre ayarlanır. Böylece etiketli veriler, uygulamanın alması muhtemel soruları ve istenen formata karşılık gelen cevapların ayarlanması yapılır. Son kısım, uygulamanın performansını geliştirmek için kullanıcılar ve geliştiriciler Üretici Yapay Zeka uygulamasının çıktılarını düzenli olarak değerlendirir ve bu kapsamda uygulama düzenli olarak güncellenir⁸⁸.

1.5.6. Robotik

Robotik yapay zeka uygulamaları kısaca fiziksel dünyada var olan eylem halindeki yapay zeka sistem ve donanımlarıdır. Algılama, muhakeme, öğrenme gibi diğer yapay zeka sistemlerinde var olan özelliklerin yanı sıra eylem ve var olan diğer sistemler ile etkileşim yetenekleri de robotik yapay zeka uygulamalarının kontrol mimarisine eklenir. Bu tür, çevrelerini algılamaları için sensörlerle donatılmıştır. Yapay zeka yalnızca bilgisayar bilimi disiplini içinde yer alırken; robotik YZ dışında kalan disiplinlerden de yardım alır. Örneğin, robotik, yapay zekaya ek olarak fiziki sistemin mevcudiyeti de gerekli olduğu için tasarım konusunda makina mühendisliğine ihtiyaç duyulmaktadır. Günümüzde kullanılan robotik yapay zekaya örnek olarak; sürücüsüz arabalar, dronlar, uçaklar, robotik süpürgeler örnek verilebilir⁸⁹. Esasen yapay zekanın dünyayı ele geçirdiğine ilişkin filmlerde (örneğin, 2004

⁸⁵IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025).

⁸⁶Güçlütürk, O. G (2023, Temmuz) . Üretken yapay zeka, riskler ve mahremiyet üzerine bir değerlendirme. *KVKK Bülten*, s. 9.

⁸⁷Büyükoçkan Feyzioğlu, 2021, s. 10.

⁸⁸IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim tarihi: 19.05.2025).

⁸⁹ High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A definition of AI: Main capabilities and scientific disciplines*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20 Mayıs 2025) .Russell ve Norvig, 2024, s.28; 925.

yapım I, Robot filmi) insanlığı yok eden yapay zeka türü robotik yapay zekaya örnek teşkil etmektedir.

1.6. Yapay Zekaya İlişkin Hukuki Düzenlemeler

Yapay zeka alanındaki gelişmeler ve gelişmelere paralel olarak farkındalıkların artması ile uluslararası alanda düzenlemeler yapılmaya başlanmıştır. Bu düzenlemelerin etkileri ise yavaş yavaş Türk Hukukunda hissedilmekte ve bu alanda farkındalığın oluşmasına yardımcı olmaktadır. Henüz Türk Hukukunda YZ alanında bir hukuki düzenleme mevcut değilse de bu alanda politik adımlar atılmaya başlanmıştır. Bu hususlar aşağıda açıklanmıştır.

1.6.1. Uluslararası düzenlemeler

Yapay zeka alanındaki gelişmeler ve bu gelişmelere paralel olarak artan farkındalıkla birlikte, uluslararası alanda hukuki düzenlemeler yapılmaya başlanmıştır. Bu çerçevede, aşağıda OECD, BM, Avrupa Birliği ve Avrupa Konseyi tarafından gerçekleştirilen düzenlemelere yer verilmiştir.

1.6.1.1. 2024'e kadar Avrupa'da yapay zeka alanındaki gelişmeler: belgeler, stratejiler ve danışma kurulları

Yapay zeka (YZ) teknolojisinin gelişimi ve yaygınlaşması ile bu teknolojilerin hukuki sınırları ve etik kullanımı uluslararası alanda önemli bir konu haline gelmiştir. 1990'lı yıllarda başlayan teknolojinin hukuki ve etik sınırları tartışmaları ancak 2010'lu yıllarda yasal düzenlemeler ve kılavuzların oluşturulmasını sağlamıştır⁹⁰. Bu bakımdan yapay zekaya ilişkin hukuki düzenlemeler oldukça yeni tarihlidir ve uygulamaları bakımından yeteri tecrübe henüz bulunmamaktadır.

Avrupa Birliği yapay zeka alanında, *kişisel verilerin korunması alanında olduğu gibi*, en etkili ve kapsamlı düzenlemelere imza atmıştır⁹¹. Hatta yapay zekanın hukuki düzenlemeleri anlamında dünyada öncü olduğu söyleyebiliriz. Avrupa Komisyonu'nun 25.04.2018 tarihinde yayınladığı yapay zeka stratejisi genel olarak yapay zekanın kullanımının ve bu alana yatırımın teşvik edilmesi ile etik ve yasal sınırların çizilmesi gerektiği çıkarımlarını içeriyordu⁹². Bundan sonra 10.04.2018 tarihinde 25 Avrupa ülkesi Yapay Zeka (YZ) konusunda bir iş birliği Bildirgesi imzaladı⁹³. Ardından, Avrupa Konseyi bünyesinde, Yapay Zeka Üzerine Yüksek Düzeyli Uzman Grubu (HLEG) kurulmuştur. HLEG görevleri kısaca, güvenilir yapay zeka için etik ilkelerin belirlenmesi, politika ve yatırım önerilerinin oluşturulması, alana ilişkin sektörel değerlendirmelerin yapılmasıdır⁹⁴. Bu Uzman Grup, 08.04.2019 tarihinde "*Güvenilir*

⁹⁰ Ergül, E (2025, Şubat), *Türkiye'nin yapay zeka hukuku: Uluslararası standartlar ve mukayeseli yaklaşımlar* (Sayı 437), SETA, s.10, <https://www.setav.org/assets/uploads/2025/02/a437.pdf> (Erişim Tarihi: 26.07.2025).

⁹¹ AB bünyesinde yapay zekaya ilişkin önemli kilometre taşları hakkında detaylı bilgi bkz European Commission. *European approach to artificial intelligence*. <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> (Erişim tarihi: 20.05.2025)

⁹² European Commission (2018, April 25) . *Artificial Intelligence for Europe* (COM (2018) 237 final) . <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Erişim tarihi: 20.05.2025) .

⁹³ European Commission (2018, April 10) . *Declaration of Cooperation on AI*. <https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence> (Erişim tarihi: 19.05.2025)

⁹⁴European Commission. *Yapay Zeka Üzerine Yüksek Düzeyli Uzman Grubu (HLEG)* . <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> (Erişim tarihi: 20.05.2025)

Yapay Zeka için Etik Kuralları” çalışmasını ortaya koymuştur. Böylece, yapay zekanın insanlar üzerindeki etkilerini, önyargıların engellenmesi ve veri gizliliği gibi konuları ele alınmıştır. Alınan geri bildirimlere dayanarak, HLEG, 2020 yılında Güvenilir Yapay Zeka (ALTAI) için nihai bir değerlendirme listesini sundu. ALTAI, Etik Yönergelerinin, kendi kendine değerlendirme sağlayabilen, erişilebilir ve dinamik kontrol listesi ve pratik bir araç olduğu ifade edilmektedir⁹⁵.

Avrupa Ekonomik İşbirliği Örgütü (OECD), İnsan haklarına ve demokratik değerlere saygılı, yenilikçi ve güvenilir YZ’yı teşvik etmek için AI Principles (Yapay Zeka İlkelerini)⁹⁶ 2019 yılında kabul etmiştir. 2024 yılında bu ilkeler güncellenmiştir. Bu ilkeler genel olarak sürdürülebilir kalkınma ve refah, insan hakları ve demokratik değerler, şeffaflık, güvenlik, açıklanabilirlik, güvenlik ve hesap verebilirlik gibi temel prensiplere dayanmaktadır.

Yapay zeka alanında ilk uluslararası standart ise 2021 yılında BM bünyesinde bulunan UNESCO tarafından “*Yapay Zeka Etiğine İlişkin Tavsiyeleri*”⁹⁷ olarak yayınlanmıştır. Bu düzenlemeler, yapay zekanın güvenli, şeffaf ve adil bir şekilde geliştirilmesini ve uygulanmasını sağlamak amacıyla sürekli olarak güncellenmiş ve geliştirilmiştir⁹⁸. Son olarak, bir diğer uluslararası örgüt olan Avrupa Konseyi’nin yapay zeka alanında yaptığı çalışmalara ve düzenlemelere değinilmesi gerekmektedir. Nitekim, 2019 yılında Avrupa Konseyi bünyesinde yapay zekaya ilişkin bir CAHAI isimli *ad hoc* (geçici) bir komite kurulmuştur. CAHAI’nin görevini (2019-2021) tamamlaması ardından yerini Yapay Zeka Komitesi’ne (CAI) bıraktı. Komite, yapay zekanın geliştirilmesi, tasarlanması ve uygulanması için Avrupa Konseyi’nin insan hakları, demokrasi ve hukukun üstünlüğü standartlarına dayalı bir yasal çerçevenin uygulanabilirliğini ve potansiyel unsurlarını, tüm paydaşlarla geniş kapsamlı istişarelerle incelemektedir⁹⁹.

1.6.1.2. Avrupa birliği yapay zeka düzenlemesi: AI Act (2024)

Dünya çapındaki en önemli gelişme sayılabilecek yapay zeka konusundaki ilk kapsamlı yasal çerçeve Avrupa Birliği’nin Yapay Zeka Yasası (“AI Act”)¹⁰⁰ olmuştur¹⁰¹. Bu yasa 01.08.2024 tarihinde kabul edilmiştir. Bu regülasyon kabul tarihinden iki yıl sonra, 02.08.2026

⁹⁵High-Level Expert Group on Artificial Intelligence (AI HLEG) (2020) . *The Assessment List for Trustworthy Artificial Intelligence (ALTAI)* . <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim tarihi: 20.05.2025) ayrıca bkz. High-Level Expert Group on Artificial Intelligence (AI HLEG) . *Ethics Guidelines for Trustworthy AI*. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (Erişim tarihi: 20.05.2025) .

⁹⁶Organisation for Economic Co-operation and Development (OECD) . *AI Principles*. <https://www.oecd.org/en/topics/ai-principles.html> (Erişim tarihi: 25.05.2025)

⁹⁷ United Nations Educational, Scientific and Cultural Organization (UNESCO) (2021, November 23) . *Recommendation on the Ethics of Artificial Intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000381137> (Erişim tarihi: 21.05.2025)

⁹⁸UNESCO tavsiyeleri 2021 yılında güncellenmiştir.

⁹⁹CAHAI - Ad hoc Committee on Artificial Intelligence (t.y.) . Detaylı bilgi için bkz. <https://www.coe.int/en/web/artificial-intelligence/cahai> (Erişim tarihi: 19.05.2025) .

¹⁰⁰ European Parliament & Council (2024, July 12) . *Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence and Amending Various Regulations and Directives (‘Artificial Intelligence Act’)* . Official Journal of the European Union, L Series, 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (Erişim tarihi: 21.05.2025)

¹⁰¹Burada dikkat edilmesi gereken AI Act’ın dünyadaki ilk yasal çerçeve olmadığıdır. Örneğin, Güney Kore’de akıllı robotların geliştirilmesini ve gelişimi için bir politika oluşturma amacı taşıyan 9014 Sayılı “The Robot Special Act” henüz 28.05.2008 tarihinde kabul edilmiştir. Kore Mevzuat Araştırma Enstitüsü (2008, May 28) . *Intelligent Robots Development and Distribution Promotion Act (9014 Sayılı Kanun)* . https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=17399&type=sogan&key=13 (Erişim tarihi: 19.05.2025)

tarikhinde bazı istisnalar dıřında tam olarak y r rl ge girecektir. Bununla birlikte, AI Act kapsamında yasaklar ve yapay zeka okuryazarlıęı y k ml l kleri 2025 yılında uygulanmaya bařlanmıřtır. D zenlenmiř  r nlere yerleřtirilen y ksek riskli yapay zeka sistemlerine iliřkin kurallar ise 02.08.2027'ye kadar uzatılmıř bir geiř s resine sahiptir. Hen z hatırı sayılır bir uygulama tecr besi bulunmayan bu d zenleme getirdięi risk tabanlı yaklařım ile yeni bir ufuk amıřtır¹⁰². Belirtmek isteriz ki, literat re "*Yapay Zeka Yasası*" olarak geen bu d zenleme, teknik anlamda bir yasa deęil; Avrupa Birlięi'nin doęrudan etkili bir reg lasyonu (t z k) nitelięindedir. Bu alıřmada, literat rdeki kullanıma ve AB belgelerine sadık kalmak amacıyla "*AI Act*" terimi tercih edilmiřtir.

AB  lkeleri aısından baęlayıcı olan AI Act; g venlięi, temel hakları ve insan merkezli YZ'yi ve AB genelinde YZ kullanımını, yatırımını ve teřvik etmek, inovasyonu, yatırımı teřvik etme amacı g tmektedir (*giriř*, para. 1). AI Act, yalnızca AB  lkelerindeki yapay zeka sistem saęlayıcılarını etkilememektedir; Avrupa Birlięi pazarına sunan AB  yesi olmayan  lkeler ile saęlayıcısı veya kullanıcısı AB sınırları ierisinde yer almasa da yapay zeka sistemi tarafından  retilenlerin AB ierisinde kullanılması durumunda bu kiřiler bakımından da uygulama alanı bulacaktır (*giriř*, para. 22; m.2/1-a) . Bu baęlamda AI Act T rkiye'nin tarafı olmadıęı bir reg lasyon olması sebebi ile T rk hukuku bakımından bir baęlayıcılık tařımamakla birlikte, AB vatandařlarına hizmet eden T rk YZ uygulamalarının bu yasaya uyum g stermesi gerekmektedir. Dięer yandan YZ sistemlerine iliřkin hukuki d zenlemeler yapılması, politik adımlar atılması ve akademik bakıř aılarının oluřması bakımından bu yasa  nem teřkil etmektedir.

AI Act'in  ye devletler genelinde tutarlı bir řekilde uygulanması, genel amalı yapay zeka kurallarının y r rl ge konulması ve g venilir YZ'nin geliřtirilmesi ve kullanımının g lendirilmesi iin AB yapısı iinde AI Office¹⁰³ (Yapay Zeka Ofisi) kurulmuřtur. 04.02.2025 tarihinde Avrupa Komisyonu, yasaklı yapay zeka uygulamalarına iliřkin bir kılavuz yayınladı¹⁰⁴. Bu y nergede  zellikle zararlı manip lasyon, sosyal puanlama ve gerek zamanlı uzaktan biyometrik tanımlama gibi uygulamaları ele alındı ve temel haklar aısından potansiyel riskler tařınması nedeniyle kabul edilemez g r len yapay zeka uygulamaları listelendi. Yapay zeka alanında k resel lider olmak isteyen AB'nin hedefini gerekleřtirmesi iin hazırlanan Avrupa Kıtası Yapay Zeka Eylem Planı¹⁰⁵ 2025 yılı nisan ayında yayınlanmıřtır.

AI Act, yapay zekanın, belirli uygulama, kullanım ve teknolojik geliřim d zeyine iliřkin kořullara baęlı olarak, hukuken korunan kamu ıkarlarına ve temel haklara riskler oluřturabileceęini ve zarar verebileceęini ifade etmiřtir. Bu zararların, fiziksel, psikolojik, toplumsal veya ekonomik zararlar da dahil olmak  zere maddi veya manevi řekilde

¹⁰² Karadeniz, S (2025). Avrupa Birlięi Yapay Zek  Kanunu'nun risk grupları ve ilgililerin y k ml l kleri baęlamında incelenmesi. *Ankara Hacı Bayram Veli  niversitesi Hukuk Fak ltesi Dergisi*, 29 (1), 307–366. <https://doi.org/10.34246/ahbvuhfd.1541455> .

¹⁰³ European Commission. AI Office. <https://digital-strategy.ec.europa.eu/en/policies/ai-office> (Eriřim tarihi: 21.05.2025)

¹⁰⁴ European Commission (2025, February 4) . Approval of the content of the draft Communication from the Commission — Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) . <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> (Eriřim tarihi: 22.05.2025)

¹⁰⁵European Commission (2025, April 9) . Communication from The Commission To The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, AI Continent Action Plan (COM (2025) 165 Final) . <https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan> (Eriřim tarihi: 22.05.2025) .

olabileceğine dikkat çekmiştir (*giriş*, para. 5) . Esasen yapay zeka üzerindeki kısıtlamaları bertaraf etmek isteyen düzenleme (*giriş*, para.1), insan merkezli olması ve insana hizmet etmesi arzu edilen bu teknolojinin aktif kullanımının toplum üzerindeki etkisi ve olası risk ve tehlikeleri karşısında güven oluşturma ihtiyacı göz önüne alınarak; hukuki güvenceler ile donatılması ile mümkün olduğu kanaatindedir (*giriş*, para. 5) . Bu sebeple AB kapsamında temel insan hakları YZ sistemleri karşısında korunmalı olduğu görüşü düzenlemeye hakimdir. Bu düzenleme kapsamında yapay zeka sistemleri için ortak kurallar oluşturulmuştur. Ayrıca, AB üyesi ülkelerin, YZ geliştiricilerinin ve uygulayıcılarının AI Act yanında “*Dijital On Yıl için Dijital Haklar ve İlkeler Bildirgesi*”¹⁰⁶ ile Yapay Zeka Yüksek Düzeyli Uzman Grubu'nun (YZ HLEG) güvenilir yapay zeka için Etik ilkelerini¹⁰⁷ de dikkate alması gerektiğinin altı çizilmiştir (*giriş*, para.7) .

YZ birçok faydası yanında temel hak ve özgürlüklere, insan onuruna, demokrasiye ve hukukun üstünlüğüne zarar verici fonksiyon göstermesinin mümkün olduğuna AI Act düzenlemesinde işaret edilmiştir. Kötüye kullanılan bu YZ uygulamalarının sömürücü ve toplumu kontrol etmeye yönelik davranışları zararlı ve istismar edici olabilmektedir. AI Act'ın bu uygulamalar karşısında bulduğu çözüm bu tür uygulamaların tespit edilerek yasaklanmasıdır (*giriş*, para.28) . Bu kapsamda, düzenleme kapsamında belirli YZ uygulamaları yasaklanmıştır. Bunlar: kişilerin hür iradesini baltalayan manipülasyon ve aldatma içeren YZ uygulamaları (haksız tüketici uygulamaları da bu kapsamdadır) (*giriş*, para.29) , güvenlik açıklarının istismarı, toplandığı bağlamla ilgisi olmayan sosyal bağlamlarda gerçek kişilere veya gruplarına yönelik olumsuz veya zararlı muamele veya sosyal davranışlarının ciddiyetine göre orantısız, haksız veya ayırmacı bir olumsuz muamele yol açabilen sosyal puanlama sistemleri , bireysel suç riski değerlendirmesi veya tahmini, yüz tanıma veri tabanlarını oluşturmak veya genişletmek için internet veya CCTV materyalinin hedefsiz bir şekilde toplanması, işyerlerinde ve eğitim kurumlarında duygu tanıma, yüz veya parmak izi gibi gerçek kişilerin biyometrik verilerine dayanan ve bir bireyin siyasi görüşlerini, sendika üyeliğini, dini veya felsefi inançlarını, ırkını, cinsel yaşamını veya cinsel yönelimini çıkarsamak veya tahmin etmek için kullanılan biyometrik kategorizasyon, bilimsel temeli konusunda endişe duyulan duygu tanıma sistemleri ve kamuya açık alanlarda kolluk kuvvetleri amaçları için gerçek zamanlı uzaktan biyometrik tanımlama amacı günden (istisnası terörizm ve suç ilişkisidir) YZ tabanlı uygulamalarıdır (*giriş*, para.29 vd.) .

AI Act kapsamında ayrıca masumiyet karinesi doğrultusunda, yalnızca profillemeye veya kişilik özellikleri ve niteliklerinin değerlendirilmesine dayanarak suç işleme olasılığını değerlendirmek veya gerçek veya potansiyel bir suç işlenmesini öngörmek amacıyla gerçek kişilerle ilgili olarak yapılan risk değerlendirmeleri yasaklanması gerektiği belirtilmiştir (*giriş*, para.42) .

Ayrıca birtakım yapay zeka uygulamalarının, karar alma sürecini önemli ölçüde etkilememesi veya bu çıkarlara esaslı bir zarar vermemesi nedeniyle, korunan yasal çıkarlara önemli bir zarar riski oluşturmadığı belirli durumların olabileceğinin altını çizen AI Act düzenlemesi, bu duruma dört örnek vermiştir. Bunlardan ilki, yapay zeka sisteminin, yapılandırılmamış verileri yapılandırılmış verilere dönüştüren veya çok sayıda uygulama

¹⁰⁶ Council of the European Union, & European Parliament (2023, January 23). *European Declaration on Digital Rights and Principles for the Digital Decade* (2023/C 23/01). Publications Office of the EU. <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> (Erişim tarihi: 20.07.2025) .

¹⁰⁷ High-Level Expert Group on Artificial Intelligence (AI HLEG) (t.y.) . *Ethics Guidelines for Trustworthy AI*. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (Erişim tarihi: 20.05.2025) .

arasında yinelenenleri tespit etmek için kullanılan bir yapay zeka sistemi gibi dar bir prosedürel görevi yerine getirmek üzere tasarlanmış olmasıdır. İkincisi, bir görevin gerçekleştirilmesi için yüksek riskli YZ sistemleri açısından önemli olabilecek, daha önce tamamlanmış bir insan faaliyetinin sonucunu iyileştirmeyi amaçlayan YZ sistemleridir. Bu tür YZ, insan faaliyetine yalnızca daha düşük riskli ek bir katman sağlamaktadır. Üçüncüsü, YZ sistemlerinin, karar alma kalıplarını veya önceki karar alma kalıplarından sapmaları tespit etmeyi amaçlamasıdır. Bu YZ uygulamaları sayesinde, ikinci bir kontrol sağlanarak oluşabilecek risk azaltılır. Dördüncü ve sonuncusu, kullanılan YZ sisteminin yalnızca bir değerlendirmeye hazırlık niteliğinde bir görevi yerine getirmek üzere tasarlanmış olmasıdır. Bir test sürüşü gören bu sonuncu tür risk oluşturma açısından çok düşüktür (*giriş*, para.53 ; m.6/3).

Ürettiği YZ sisteminin yüksek riskli olmadığını düşünen bir sağlayıcı, söz konusu YZ uygulaması piyasaya arz edilmeden veya hizmete sunulmadan önce değerlendirmenin belgelerini hazırlamalı ve talep üzerine bu belgeleri ulusal yetkili makamlara sunmalıdır. Ayrıca sağlayıcı, söz konusu YZ sistemini AI Act kapsamında oluşturulan AB veri tabanına kaydetmekle yükümlü olacaktır (*giriş*, para.53).

AI Act, YZ geliştiricileri ve YZ tabanlı uygulamaları kullananlar kurum, kuruluş ve şirketler için YZ'nın belirli kullanımları konusunda risk tabanlı bir yaklaşım benimsemiş ve içerdikleri risklere göre gruplar oluşturmuştur. Nitekim, YZ sistemleri için bağlayıcı kuralların öngörülebilmesi, açıkça tanımlanmış risk grupları çerçevesinde oluşturulabilecektir. Risk gruplarının ayırımında, YZ sistemlerinin doğurabileceği riskler, bu risklerin yoğunlukları ve kapsamı gözetilmiştir (*giriş*, para.26) . AI Act kapsamında belirlenen gruplar şunlardır: minimal risk, sınırlı risk, yüksek risk ve kabul edilemez risk grupları¹⁰⁸.

AI Act özellikle *Yüksek riskli AI sistemlerini*¹⁰⁹ önceleyerek bu sistemlerin uyması gereken yükümlülükleri detaylandırmıştır (m.8 vd.). Yüksek riskli YZ uygulamalarına¹¹⁰; kişilerin işe alınması ve seçilmesinde, iş ilişkisinin şartlarını etkileyen kararların alınmasında, iş sözleşmesi ilişkilerinin terfi ettirilmesinde ve sona erdirilmesinde, bireysel davranış, kişisel özellik veya karakteristiklere göre görev dağılımı yapılmasında ve iş sözleşmesi ilişkilerindeki kişilerin izlenmesi veya değerlendirilmesinde kullanılan YZ sistemleri örnek olarak verilebilir. Nitekim bu YZ sistemleri, ayrımcılık yasağına ve eşit davranma ilkesine aykırı sonuçlara sebep olabileceği gibi çalışanların performans ve davranışlarını izlemek için kullanılan yapay zeka sistemleri, aynı zamanda kişilerin veri koruma ve gizlilik konusundaki temel haklarını da zedeleyebilmektedir (*giriş*, para.57) . Adaletin temini ve demokratik süreçlerin yönetilmesi için

¹⁰⁸ Detaylı bilgi için ayrıca bkz. Karadeniz, S (2025). Avrupa Birliği Yapay Zekâ Kanunu'nun risk grupları ve ilgililerin yükümlülükleri bağlamında incelenmesi. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 29 (1), 307–366. <https://doi.org/10.34246/ahbvuhfd.1541455> .

¹⁰⁹ Kritik altyapılardaki güvenliğe yönelik YZ uygulamaları (örneğin ulaşım), eğitim kurumlarında kullanılan, bir kişinin eğitime erişimini ve mesleki yaşam seyrini (örneğin sınav puanlaması) belirleyebilecek yapay zeka uygulamaları, İstihdam, çalışanların yönetimi ve serbest mesleklere erişim için kullanılan yapay zeka sistemleri (örneğin işe alım için özgeçmiş sıralama yazılımı), Özel ve kamu hizmetlerine erişim sağlamak için kullanılan belirli yapay zeka kullanım örnekleri (örneğin kredi notunun vatandaşların kredi alma fırsatını engellemesi), uzaktan biyometrik tanımlama, duyu tanıma ve biyometrik kategorizasyon için kullanılan yapay zeka sistemleri (örneğin, bir hırsız geriye dönük olarak tanımlayan yapay zeka sistemi), insanların temel haklarına müdahale edebilecek kolluk kuvvetlerinde kullanılan YZ sistemleri (örneğin kanıtların güvenilirliğinin değerlendirilmesi), göç, iltica ve sınır kontrol yönetiminde kullanılan yapay zeka sistemleri (örneğin vize başvurularının otomatik olarak incelenmesi) ve son olarak adalet ve demokratik süreçlerin yönetiminde kullanılan yapay zeka çözümleri (örneğin mahkeme kararlarının hazırlanmasında kullanılan yapay zeka çözümleri) yüksek riskli YZ sistemleridir.

¹¹⁰ Yüksek riskli yapay zeka uygulamalarının kapsamı için bkz. Artificial Intelligence Act, ANNEX III , High-risk AI systems referred to in Article 6 (2).

hazırlanan yapay zeka sistemleri de yüksek riskli sınıf kategorisindedir. Nitekim, özellikle hukukun üstünlüğü, bireysel özgürlükler ve adil yargılanma hakkı kapsamında olası önyargı ve hata risklerinin doğuracağı sonuçlar gözetildiğinde bu alandaki YZ uygulamalarının ayrıca bir özen, dikkat ve tedbir gereksindiği ortadadır (*giriş*, para.61) . Göç, iltica ve sınır kontrol yönetimine ilişkin YZ uygulamaları da yüksek riskli YZ uygulamalarıdır. Ayrıca kişisel verilerin korunması için ihlal niteliği taşıyabilecek uygulamalar, yüksek riskli yapay zeka kategorisi içinde sayılmaktadır.

AI Act kapsamında ayrıca yüksek riskli YZ uygulamalarının, piyasaya sürülmeden önce uyması gereken yükümlülükler öngörülmüştür. Bunlar: yeterli risk değerlendirmesi ve azaltma sistemlerinin sağlanması, ayrımcı sonuçların risklerini en aza indirmek için sistemi eğiten veya girdi olan büyük veri kümelerinin yüksek kaliteli olması, sürecin denetiminin sağlanması için faaliyetlerin kaydedilmesi, yetkililerin uyumluluğunu değerlendirmesi için sistem ve amacı hakkında gerekli tüm bilgileri sağlayan ayrıntılı belgeler kayıt edilmesi, kullanıcılara açık ve yeterli bilgilerin sağlanması, insani gözetim önlemlerinin alınması ve son olarak yüksek düzeyde sağlamlık, siber güvenlik ve doğruluğun sağlanmasıdır (m.8; m.15) . Ayrıca yüksek riskli yapay zeka sistemleri piyasaya sürülmeden veya hizmete sunulmadan önce şeffaflık sağlanmalıdır. Böylece, uygulayıcı ve kullanıcıların YZ sistemlerinin nasıl çalıştığını anlamalarını, işlevselliğini değerlendirmelerini ve güçlü ve zayıf yönlerini kavramaları sağlanmalıdır (*giriş*, para.72; m.13) .

AI Act, insan onuru, temel insan hakları ve demokrasiye ilişkin riskler barındırma tehlikesi olan YZ sistemleri için risk temelli bir yaklaşım benimsemiştir. Olası zararın önlenmesi için yüksek riskli YZ sistemleri için uyulması gereken ortak kurallar öngörmekle kalmamış(m.16 vd.); yukarıda belirtildiği üzere birtakım YZ uygulamalarını hem özel sektör hem de idari alanda kullanımını yasaklamıştır. Ayrıca YZ okuryazarlığını teşvik etmiş ve YZ sistem sağlayıcı ve uygulayıcıların idari ve teknik tedbirler kapsamında personeli bu konuda eğitmesi hususunda yükümlü kılmıştır (m.4).

YZ sistemlerinin meydana getirebileceği tehlikelere ilişkin, geliştirici ve sağlayıcıların risk değerlendirmesinin (m.9) önemine sıklıkla vurgu yapan AI Act, risk yönetiminin yüksek riskli YZ sistemlerinin yaşam döngüsü süresince planlanıp yürütülen sürekli yinelen bir süreç olduğunun altını çizmektedir (*giriş*, para.65) . Risk yönetimi süreci, YZ sistemlerinin özellikle temel haklar, güvenlik ve sağlık üzerindeki ilgili risklerini belirlemeyi ve azaltmayı hedeflemelidir. En uygun risk yönetimi önlemlerini belirlerken, sağlayıcı yapılan seçimleri belgelemeli ve açıklamalı ve gerektiğinde uzmanları ve dış paydaşları dahil etmelidir. Son olarak, risk yönetim sistemi, sürekli etkinliğini sağlamak ve alınan önemli karar ve eylemlerin gerekçelendirilmesi ve belgelendirilmesi için düzenli olarak gözden geçirilmeli ve güncellenmesi gerektiğine vurgu yapılmıştır (*giriş*, para.65) . Ayrıca, yüksek riskli YZ sistemlerinin çalışma usulleri, gelişimleri ve performansları üzerinde bilgi sahibi olmak da risk faktörlerinin belirlenmesi ve azaltılmasında etkili olacağı ifade edilmiştir (*giriş*, para.71). YZ uygulamalarının, gerçek kişilerin denetimine imkan tanıyan şekilde tasarlanması ve geliştirilmesi risk faktörlerini azaltılmasına yardımcı bir diğer mekanizmadır (m.14) . Bu kapsamda YZ sistemi ile ilgili teknik dokümantasyonu, sistem piyasaya arz edilmeden veya hizmete sunulmadan önce hazırlanmalı ve güncel olarak tutulmalıdır (m. 11) . Gelişen teknolojinin YZ sistemlerinde risk önleme mekanizmalarına yardımcı olması ile temel insan hakları, onuru ve demokratik değerlerin korunması güçlenecektir (*giriş*, para.75 vd.) .

Çalışma konusu bakımından, Genel Veri Koruma Tüzüğü (GDPR) kapsamında yapay zeka teknolojilerinden doğrudan bahsedilmediğini belirtmek isteriz. Ancak, GDPR düzenlemesinin kişisel verilerin işlenmesine ilişkin genel hükümleri, yapay zeka sistemlerinde işlenen kişisel veriler için doğrudan bağlayıcıdır. Bu nedenle, GDPR, yapay zeka sistemlerinde kişisel verilerin işlenmesi ve korunması için temel hukuki çerçeveyi oluşturmaktadır. Bu kapsamda YZ sistemlerinin GDPR’da düzenlenen veri koruma gerekliliklerine uyması gerekmektedir¹¹¹. Bu durum AI Act düzenlemesinin giriş kısmı paragraf 10’da açıkça düzenlenmiştir.

1.6.1.3. Avrupa konseyi çerçeve sözleşmesi (2024)

Avrupa Konseyi Yapay Zeka ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi’ni¹¹² AI Act’in kabul edilmesinden yalnızca birkaç ay sonra 05.09.2024 tarihinde kabul etmiştir. Sözleşme, yapay zeka alanında hukukten bağlayıcı olan ilk uluslararası anlaşma niteliğini haizdir. Yapay zeka alanında uluslararası standartları koyan Sözleşme hızlı teknolojik gelişmelerden kaynaklanabilecek yasal boşlukları doldurmayı amaçlamaktadır. Sözleşme ile bir yandan yapay zeka teknolojisinin geliştirilmesi ve üye devletlerin işbirliği teşvik edilmiş diğer yandan yapay zeka sistemlerinin yaşam döngüsü içindeki belirli faaliyetlerin insan onurunu ve bireysel özerkliği, insan haklarını, demokrasiyi ve hukukun üstünlüğünü zedelemesinden hareketle insan haklarını koruyucu ve uygulanabilir bir yasal çerçeve oluşturulması gerektiği düşüncesi hakim olmuştur¹¹³.

Avrupa Konseyi Çerçeve Sözleşmesi, yaşam döngüsü içerisindeki insan faaliyetlerinin insan hakları, demokrasi ve hukukun üstünlüğü ile tamamen uyumlu olmasını amaçlamaktadır (m.1) . Bu Sözleşme uyarınca devletler, yapay zeka sistemlerinin yaşam döngüsü içindeki faaliyetleri kapsamında temel ilkelere uyumlu olmasını sağlamakla yükümlüdürler. Bu temel ilkeler; insan onuru ve bireysel özerklik, eşitlik ve ayrımcılık karşıtlığı, gizliliğe ve kişisel verilerin korunmasına saygı, şeffaflık ve denetim, hesap verebilirlik ve sorumluluk, güvenilirlik ve güvenli inovasyon ilkeleridir (III.Bölüm, m.7-13) .

Yapay zeka sistemlerinin kamu otoriteleri (onlar adına hareket eden özel aktörler dahil) ve özel aktörler tarafından kullanımını kapsayan Sözleşme, birtakım çözüm yolları, haklar ve güvenceler getirmiştir. Nitekim YZ sistemlerini kullanan aktörler, uygulamalarında kullandıkları yapay zeka sistemleri ve sistemin işleyişi ile ilgili bilgileri belgeleyerek bunları kullanıcıların erişimine sunmakla yükümlü tutulmuşlardır. Bu bilgiler kişilerin YZ sistemleri ile haklarında alınan kararlara itiraz haklarını, itiraz usulünü ve YZ sistemi kullanımını kullanımına itirazlarını içermelidir. Ayrıca bu müracaat ve itiraz yolları etkin ve erişilebilir olmalıdır (m.14). AI Act ve Çerçeve Sözleşme’nin getirdiği en önemli yenilik kullanıcının bir YZ sistemi ile karşı karşıya olduğunu ve bu durumun kendi menfaatini nasıl etkileyeceği konusunda bilgilendirilmesi yükümlülüğüdür. Şikayet ve itiraz haklarının da bilgilendirme

¹¹¹ Çavuşoğlu, G. F (2021) . *Kişisel verilerin yapay zekayla işlenmesinden doğan özel hukuk sorunları* (Yayımlanmamış yüksek lisans tezi), Ankara Üniversitesi, s.16.

¹¹²Avrupa Konseyi (2024, Eylül 5) . *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225, m.2) . Vilnius. <https://rm.coe.int/1680afae3c> (Erişim tarihi: 21.05.2025) .

¹¹³ Council of Europe. *The Framework Convention on Artificial Intelligence*. <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> .

yükümlülüğü kapsamında olması kullanıcıların kişisel verilerini etkin şekilde korumalarına ve akıbetleri konusunda karar vermelerine imkan tanımaktadır.

Avrupa Konseyi Çerçeve Sözleşmesi'nde ayrıca yapay zeka sistemlerinin tehlike ve risk doğurabileceğine dikkat çekilerek; yapay zekanın pek çok faydası yanında özellikle insan hakları, özerkliği ve insan onurunun korunmasında tehlikeler doğurabileceği belirtilmiştir. Yapay zeka sistemlerinin eşit muamele ve ayrımcılık yasağına aykırı sonuçlar doğurabileceğini belirten sözleşme özellikle kadınların ve hassas durumda bulunan kişiler hakkında eşitsizlik yaratılabileceği veya var olan eşitsizliğin ağırlaştırılabileceğini vurgulamaktadır. Özellikle keyfi ve yasadışı gözetleme ve sansür uygulamaları veya diğer şekillerde yapay zeka sistemlerinin kötüye kullanımları sonucunda kişilerin mahrem ve özerk alanlarının ihlal edilebileceği ifade edilmektedir (*giriş*). Engelli bireylerin ve çocukların haklarının ayrıca gözetilmesi gerektiğinin altını çizen Çerçeve Sözleşmesi, bu kişilerin haklarının sağlanması için gerekli olan her türlü özel ihtiyaç ve hassasiyetin gösterilmesi gerektiğini belirtmektedir (m.18).

Avrupa Konseyi Çerçeve Sözleşmesi'ne göre YZ bağlamındaki risk ve tehlikelerin önlenmesi için ilk önce yapılması bu tehlike ve risklerin belirlenmesi, yorumlanması ve azaltılması için özellikle sorumlu olanlar ile toplumun tüm kesimleri için dijital okuryazarlık ve becerilerin edinilmesinin sağlanması gerekmektedir (m.20). YZ sistemlerinin yaşam döngüsü içindeki faaliyetleri kapsamında yasal bir çerçeve çizilmesi de bir zorunluluktur. Ayrıca, Sözleşmeden doğan yükümlülüklerin yerine getirilmesinin denetlenmesi için en az bir veya daha fazla etkin gözetim mekanizmaları oluşturulmalıdır (m.26). Ayrıca risk ve etki yönetimi çerçevesinde her bir YZ sistemi çerçevesinde sistemin kullanılma amacı, bağlamı, potansiyel risk durumu, etkileri, YZ sistemi bağlamında hakları etkilenecek kişilerin ve bu kişilerin bakış açılarının belirlenmesi, sistemin insan haklarına, demokrasiye, hukukun üstünlüğüne yönelik risklerin belirlenmesi ve olumsuz etkilerinin izlenmesi yapılmalıdır. Tüm bu tespitlerin ve bunlara karşı oluşturulan risk yönetimi yaklaşımının belgelenmesi de önem taşımaktadır. Özellikle YZ sistemleri ilk kullanımlarından önce risk yönetimi bakımından teste tabi tutularak risk ve tehlikeler azaltılmalıdır (m.16).

Avrupa Konseyi Çerçeve Sözleşmesi'nde yapay zeka sistemlerinde kişisel verilere ilişkin hususlarda kişisel verilerin korunması mevzuatının uygulanması gerektiği belirtilmiştir (*giriş*). Son olarak belirtmek isteriz ki; Avrupa Konseyi'nde bulunmayan ülkelerin katılıma açık olan Sözleşme (m.30) henüz Türkiye tarafından imzalanmamıştır¹¹⁴.

1.6.2. Ulusal düzenlemeler

Yapay Zeka'nın ekonomik değerinin her geçen gün artması devletlerin ve bölgesel birlikleri bu alanı teşvik etmek için yapay stratejisi yapmaya itmiştir. Nitekim, Avrupa Birliği de 2018 yılında Yapay Zeka Stratejisini yayınlamıştır¹¹⁵. Türkiye ise 24.08.2021 tarihinde 5

¹¹⁴ İmza eden devletler için ayrıca bkz. Council of Europe. *The Framework Convention on Artificial Intelligence*. <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>.

¹¹⁵ European Commission (2018, April 25). *Artificial Intelligence for Europe* (COM (2018) 237 final). Brussels. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Erişim tarihi: 20.05.2025).

yıllık (2021-2025) Ulusal Yapay Zeka Stratejisini yayınlamıştır¹¹⁶. Bu eylem planı, YZ alanında son dönemde yaşanan gelişmeler ve ülke ihtiyaçları göz önünde bulundurularak, 2024-2025 Eylem Planı olarak güncellenmiştir¹¹⁷. Ayrıca 2021/18 sayılı Cumhurbaşkanlığı Genelgesi ile, Ulusal Yapay Zeka Stratejisi Yönlendirme Kurulu kurulmuştur. Cumhurbaşkanı yardımcısının başkanlık ettiği bu kurulda Dijital Dönüşüm Ofisi ve Sanayi ve Teknoloji Bakanlığı temsilcileri yer alır. Gündeme göre diğer yetkililer de davet edilebilir. Kurulun görevi, yapay zeka teknolojilerinin gelişimini destekleyecek ulusal politikaları koordine etmek ve stratejinin uygulanmasını üst düzeyde izlemektir¹¹⁸. TBMM bünyesinde 02.10.2024 tarihinde yapay zekaya ilişkin fırsatların değerlendirilmesi, hukuki altyapının oluşturulması ve risklerin azaltılması amacıyla bir Araştırma Komisyonu kurulmuştur. Komisyon, 7 Ocak 2025'te çalışmalarına başlamıştır¹¹⁹.

Türkiye'de henüz ulusal bir yapay zeka kanunu veya yönetmeliği bulunmamaktadır. Bununla birlikte, yapay zeka farkındalığı her geçen gün artmaktadır. Yapay zeka sistemlerinde kişisel verilerin işlenmesi hallerinde 6698 sayılı Kişisel Verilerin Korunması Kanunu(KVKK)¹²⁰ uygulama alanı bulacaktır¹²¹.

Kişisel Verileri Koruma Kurumu'nun "*Yapay Zeka Alanında Kişisel Verilerin Korunmasına İlişkin Tavsiyeleri*"¹²² yapay zeka alanında bilincin oluşturulması bağlamında önem arz etmektedir. Yapay zeka alanında faaliyet gösteren, geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcılar için hazırlanan bu yayımda öncelikle YZ sistemlerine ilişkin genel tavsiyelerde bulunulmuştur. Bu tavsiyeler genel olarak; YZ sistemlerinin oluşturulmasında ve geliştirilmesinde insan onuruna ve temel insan haklarına saygı gösterilmesi, kişisel verileri işleme ilkelerine uyum sağlanması, potansiyel risklerin önlenmesi ve azaltılması çalışmalarının yapılması, tasarımdan itibaren kişisel verilerin korunması mevzuatına uyum sağlanması, YZ sistemleri yüksek risk kategorisine göre değerlendirilmeli ve bu sınıfta olduğu düşünülen YZ sistemleri için mahremiyet etki değerlendirmesinin yapılması, işletme veya kurum tarafından risk ve tehlikelere karşı gerekli idari ve teknik tedbirlerin alınması ve kişisel verilerin korunması mevzuatına uyum sağlanmasıdır. Geliştirici ve sağlayıcılar için özel tavsiyelerde bulunan bu yayımın YZ mevzuatının geliştirilmesinde bilinç oluşturulması bakımından önemli bir adım olduğu kanaatindeyiz.

¹¹⁶bkz. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi & T.C. Sanayi ve Ticaret Bakanlığı (2021) . *Ulusal Yapay Zeka Stratejisi 2021-2025*. <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf> (Erişim tarihi: 17.05.2025) .

¹¹⁷ bkz. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi & T.C. Sanayi ve Ticaret Bakanlığı (2021) . *Ulusal Yapay Zeka Stratejisi 2021-2025*. <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf> (Erişim tarihi: 17.05.2025) .

¹¹⁸ Ergül, 2025, s. 19.

¹¹⁹ Ergül, 2025, s. 19-20.

¹²⁰ R.G. 29677 S. ve 07.04.2016 T.

¹²¹ Çavuşoğlu, 2021, s.16.

¹²² Kişisel Verileri Koruma Kurumu (2025). *Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler* , KVKK Yayınları, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf> . Erişim Tarihi: 01.06.2025.

1.7. Veri

Yapay zeka ile veri (*data*) arasında yakın bir ilişki bulunmaktadır. Nitekim, yapay zeka sistemlerinin işlevlerini gerçekleştirebilmeleri için veri kümelerine ihtiyaçları vardır. Çalışma konumuz kapsamında veriden anlaşılması gerekenin açıklanması ihtiyacı doğmuştur.

Avrupa Birliği, veri odaklı ekonomiye ilişkin yayımladığı bir bildirisinde veriyi ISO/IEC 2382¹²³ kaynak göstererek; *"iletişim, yorumlama veya işlemeye uygun, biçimselleştirilmiş bir biçimde bilginin yeniden yorumlanabilir bir temsili"* şeklinde tanımlamıştır¹²⁴. Türk Dil Kurumu Sözlüğünde ise veri teknik olarak *"Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi"* şeklinde tanımlanmaktadır¹²⁵. Avrupa komisyonu bildirisinde özellikle dijital verilerin üretildiği, işlendiği ve kullanıldığı yöntemlerin arttığına ve birçok kararın alınmasında veri analitiğine güvenildiğine vurgu yapılmıştır¹²⁶. Bu çerçevede veri; bilgisayarlara işlenebilen herhangi bir sayı veya metin veri olarak da ifade edilmiştir¹²⁷.

Genel olarak veri kavramı sezgisel anlamı olan, bilinen gerçeklerin kaydedilen halidir¹²⁸. Veri, belirsiz olmayan, nesnel ve determinist ekosistemde karşılığı bulunan bir kavramdır¹²⁹. Nitekim tek başına veri bir anlam ifade etmez. Bu sebeple mantıksal olarak ilişkili bulunan veriler özel olarak tasarlanan ve oluşturulan belirli veri tabanlarında muhafaza edilir¹³⁰. Veri analizi yöntemleri ile veri tabanlarında anlamlı örüntüler oluşturularak; verinin bilgiye dönüştürülmesi sağlanır. Böylece veriye anlam kazandırılarak amaç doğrultusunda fayda sağlanır¹³¹. Aksi halde analiz edilmeyen veri yalnızca rakamlardan, sembollerden, ölçümlerden genel olarak ham yani anlamlandırılmayan gerçeklerden ibaret kalır¹³².

Veri anlamlandırılabilen bir kayıt olabileceği gibi anlam çıkartılamayan gelişigüzel şekilde oluşmuş bir şey de olabilir. Bu durum verinin niteliğini etkilemeyecektir. Veri kullanılma amacına, kaynağına ve niteliğine (örneğin verinin eser niteliğinde olması) göre ekonomik değer taşıyabilir. Verinin değiştirilmesi, kopyalanması, çoğaltılması veya silinmesi dijital ortamlarda mümkündür. Bu sebeple siber saldırılara ve erişime ilişkin gerekli tedbirlerin alınması gereklidir¹³³.

Veriler insanlar tarafından doğrudan sağlanan ve makinalar tarafından üretilen veriler olarak ayrıma tabi tutulabilse de bu ayrım keskin değildir. Nitekim, makinalar tarafından

¹²³ International Organization for Standardization (2015). *Information technology – Vocabulary* (ISO/IEC 2382:2015). <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:ed-1:v2:en> (Erişim Tarihi: 15.07.2025).

¹²⁴ European Commission (2014). *Towards a circular economy: A zero waste programme for Europe* (COM (2014) 442 final). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014DC0442> Erişim Tarihi: 15.07.2025.

¹²⁵ Bkz. Türk Dil Kurumu. *Büyük Türkçe Sözlük*. <https://sozluk.gov.tr/> (Erişim tarihi: 31.01.2025).

¹²⁶ European Commission (2014). *Towards a circular economy: A zero waste programme for Europe* (COM (2014) 442 final). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014DC0442> Erişim Tarihi: 15.07.2025.

¹²⁷ Tüzüntürk, S (2010). Veri madenciliği ve istatistik. *Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 29 (1), 65.

¹²⁸ Kahramanlı, H (2008), *Hibrit bulanık sinir ağını kullanarak bir sınıflandırma ve kural çıkarma sisteminin geliştirilmesi* (Yayımlanmamış Doktora Tezi), Selçuk Üniversitesi, s.1.

¹²⁹ Güçlütürk, 2022, s.13.

¹³⁰ Kahramanlı, 2008, s.1.

¹³¹ İnan, O (2015), *Veri madenciliği uygulamaları için veri indirgeme algoritmalarının geliştirilmesi ve resim madenciliğine uygulanması* (Yayımlanmamış doktora tezi), s.15.

¹³² Atalan, 2024, s.25.

¹³³ Güçlütürk, 2022, s. 18.

üretile verilerin mutlaka doğrudan veya dolaylı bir insan kaynağı bulunmaktadır. Örneğin, bir arabanın motoruna ilişkin veriler kullanıcı insan davranışları hakkında bilgi sağlayabilmektedir¹³⁴. Makina üretimi verinin anlaşılabilmesi için makineden kastedilen bilgisayarların veya yazılımların verileri nasıl oluşturduğunu anlamak gerekir. Bilgisayarlar verileri 1 ve 0 kodlarını kullanarak gösterir. Faaliyet gösterilen birim ise bit olarak ifade edilir. Klasik bir bilgisayar sisteminde, verileri işlenmesi için bir ikili bit, yalnızca 0 veya 1 gibi tek bir ikili değeri temsil edebilir; bu da yalnızca iki olası durumdan birinde olabileceği anlamına gelmektedir¹³⁵. Bilgisayarların 0 ve 1 kullanarak işledikleri verileri okumakta zorlanan insanlar için veriler ile etkileşime girebilmelerini sağlamak amacıyla arayüzler oluşturulmuştur. Yani insanlar tarafından arayüzler vasıtası ile ses, görüntü veya metin olarak görülen verilerin arkasında bilgisayar 0 ve 1 verileri vardır. Bu veriler yukarıda bahsedildiği üzere gerçekliğin temsiliidir. Diğer bir ifade ile gerçeklik bilgisayar tarafından kendi dili kullanılarak işlenir ve insanlara gösterilmek için dönüştürülür. Bu kapsamda, makina tarafından sunulan algılayabildiğimiz veriler makina üretimi veridir. Bu verilerin insan kaynağından ayrı düşünülmesi bu bakımdan da güçtür¹³⁶.

Bilindiği üzere yapay zekanın eğitilmesi ve sonrasında işletilebilmesi için çok sayıda veriye ihtiyaç duyulmaktadır¹³⁷. Yapay zeka bağlamında kullanılan veriden bahsedildiği zaman anlaşılması gereken dijital verilerdir. Yani yapay zekanın geliştirilmesinde model eğitiminde kullanılacak veya sonrasında sisteme girdi olarak verilecek olan bahsi konu verinin dijital ortamda temsili olan bir veri olması gerekmektedir. Ancak bu halde, veri YZ algoritmaları tarafından okunabilir ve işlenebilir. Bu sebeple, YZ tarafından yorumlanacak olan veya YZ modelinin geliştirilmesi için kullanılacak video ve fotoğraf görüntü verileri elde edildikten sonra elektronik ortama aktarılarak kullanılır¹³⁸.

1.7.1. Verilerin sınıflandırılması

Veri, yapılandırılmış veri (*structured data*), yapılandırılmamış veri (*unstructured data*) ve yarı yapılandırılmış (*semi-structured data*) olmak üzere üç temel ayrıma tabi tutulur¹³⁹.

1.7.1.1. Yapılandırılmış veri

Yapılandırılmış veriler, önceden tanımlanmış bir şemaya sahiptir. Bu tip verilere, rehberde kaydedilen telefon numaraları ve ürün gönderimi için alınan müşteri verileri örnek olarak verilebilir¹⁴⁰. Bu tür verilerden analiz yolu ile elde edilen çıkarımlar daha hızlı şekilde elde

¹³⁴ Duch-Brown, N., Martens, B., and Mueller-Langer, F (2017). *The economics of ownership, access and trade in digital data* (JRC Digital Economy Working Paper 2017-01; JRC104756). European Commission, Joint Research Centre, s.7.

¹³⁵ Microsoft, *What is a qubit?* Microsoft Azure, <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit/> (Erişim Tarihi: 17.07.2025); Güçlütürk, 2022, s.16; Duch-Brown, Martens, and Mueller-Langer, 2017, s. 7.

¹³⁶ Güçlütürk, 2022, s.16-17; Duch-Brown, Martens, and Mueller-Langer, 2017, s. 6-7.

¹³⁷ European Commission (2018, April 25) . *Artificial intelligence for Europe* (COM (2018) 237 final) . <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Erişim tarihi: 20.05.2025); Russell ve Norvig, 2024, s.750 vd., Büyüközkan Feyzioğlu, 2021, s. 6.

¹³⁸ Güçlütürk, 2022, s.13-14.

¹³⁹ SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html (Erişim Tarihi: 18.07.2025); Retornaz ve Güçlütürk, 2021, s.9; IBM. *Unstructured data*. <https://www.ibm.com/think/topics/unstructured-data> (Erişim tarihi: 19.05.2025).

¹⁴⁰ IBM. *Unstructured data*. <https://www.ibm.com/think/topics/unstructured-data> (Erişim tarihi: 19.05.2025).

edilebilmektedir. Öyle ki, bir alışveriş merkezinde satış verilerinin toplanması örneğinde özellikle hangi saatlerde satış hacminin fazla olduğu ve düşük olduğunun tespiti ürün, alışveriş saati ve adeti gösteren ürün satım verileri sayesinde hızlı şekilde öğrenebilmektedir¹⁴¹.

1.7.1.2. Yapılandırılmamış veri

Yapılandırılmamış verilerin önceden tanımlanmış bir şeması yoktur. Bu verilerle tablolastırmaya henüz uygun değildir. Öncelikle tasnif edilmesi veya etiketlenmesi gerekmektedir¹⁴². Bu verilerin çoğu metinseldir: mesajlar, Word belgeleri, PDF'ler, bloglar ve sosyal medya gönderileri. Ancak, metin dışı yapılandırılmamış veriler de bulunmaktadır. Bu grubun yaygın örnekleri arasında görüntü dosyaları (JPEG, GIF ve PNG gibi), multimedya dosyaları, video dosyaları, mobil etkinlik ve Nesnelerin İnterneti (IoT) cihazlarından gelen sensör verileri bulunur¹⁴³.

1.7.1.3. Yarı yapılandırılmış veri

Yarı yapılandırılmış veriler, yapılandırılmış ve yapılandırılmamış verilerin özelliklerini taşır. Bu verilerin önceden tanımlanmış bir şeması bulunmasa da indeksleme ve analiz imkanı sağlayan etiketler ve anlamsal işaretleyicilere sahiptir. Bu veriler, geleneksel ilişkisel veri tabanının katı yapısına uyum göstermez. JavaScript Nesne Gösterimi (JSON), CSV ve Genişletilebilir İşaretleme Dili (XML) dosyaları örnek olarak verilebilir.¹⁴⁴ Başka bir örnek e-postalardır. E-postalar her ne kadar bir şemaya sahip olmasalar da alıcı, gönderici, gönderi saati ve tarihi gibi belli birtakım sınıflandırılabilir etiketleri bulunmaktadır¹⁴⁵.

1.7.2. Genel olarak büyük veri

Büyük veri, "geleneksel yöntemlerle işlenmesi zor veya imkânsız olacak kadar büyük, hızlı veya karmaşık olan verileri" ifade etmektedir¹⁴⁶. Bu tanım temelde büyük verinin geleneksel veri setlerinden farkını ortaya koymaktadır¹⁴⁷. Avrupa Birliği bildirisinde büyük veri, çok sayıda farklı kaynaktan yüksek hızda üretilen büyük miktarda farklı veriler olarak tanımlanmıştır. Bu bildiride teknolojinin sağladığı güçlü işlemciler, yazılımlar ve algoritmalar aracılığıyla farklı kaynaklardan ile gerçek zamanlı olarak çok çeşitli ve hacimli veri kümeleri işlenebildiği belirtilerek, büyük veri özelliklerine vurgu yapılmıştır¹⁴⁸.

İnsanoğlunun tarih boyunca kayıtlar tutarak ürettiği veriler, bilgisayarların yaygınlaşması ile elektronik ortama aktarılmış ve gelişen teknoloji ile verinin üretimini,

¹⁴¹ Retornaz ve Güçlütürk, 2021, s.10.

¹⁴² Retornaz ve Güçlütürk, 2021, s.10-11; IBM. *Unstructured data*. <https://www.ibm.com/think/topics/unstructured-data> (Erişim tarihi: 19.05.2025).

¹⁴³ IBM. *Unstructured data*. <https://www.ibm.com/think/topics/unstructured-data> (Erişim tarihi: 19.05.2025).

¹⁴⁴ IBM. *Unstructured data*. <https://www.ibm.com/think/topics/unstructured-data> (Erişim tarihi: 19.05.2025).

¹⁴⁵ Retornaz ve Güçlütürk, 2021, s.11.

¹⁴⁶ SAS Institute, *What is big data?*, SAS, https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html (Erişim Tarihi: 18.07.2025).

¹⁴⁷ Retornaz, E. A., & Güçlütürk, 2021, s.2.

¹⁴⁸ European Commission (2014). *Towards a circular economy: A zero waste programme for Europe* (COM (2014) 442 final). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014DC0442> Erişim Tarihi: 15.07.2025.

toplanmasını, aktarılmasını, birleştirilmesini yani işlenmesini kolaylaştırmıştır. Bilgi işlem gücünde yaşanan gelişmeler çok büyük veri kümelerinin oluşturulmasını olanak tanımıştır. Büyük veri olarak isimlendirilen bu veri kümeleri, trilyonlarca kelime metni, milyarlarca görüntü milyarca saatlik konuşma de videonun yanı sıra genomik, sosyal ağ, tıklama verisi ve daha birçok veri türünü içermektedir¹⁴⁹. Nitekim, büyük veri, yukarıda açıklanan teknik olarak ayırma tabii tutulan üç veri grubunu da kapsamaktadır¹⁵⁰.

Özellikle internetin (World Wide Web) icadı, büyük verinin gelişimine önemli katkılar sağlamıştır. Nitekim internet, erişim sağladığı milyarlarca cihaz üzerinden büyük miktarda veri üretmektedir. Sosyal medyayı da kapsayan veri toplama faaliyetleri kapsamında, dünya genelindeki milyarlarca kullanıcının verilerine erişilmekte ve bu veriler, Google Cloud gibi küresel bulut hizmet sağlayıcılarında depolanarak analiz edilmektedir. Her ne kadar bu merkezi veri depoları, verilerin daha hızlı işlenmesine ve küresel ölçekte analizine olanak tanısa da; verilerin yetkisiz erişim veya siber saldırılar yoluyla kötüye kullanılması ihtimali, temel hak ve özgürlükler açısından ciddi riskler barındırmaktadır¹⁵¹.

Büyük veriye ilişkin olarak Türk hukukunda özel bir yasal düzenleme bulunmamaktadır. Ancak, yapay zeka teknolojilerinde olduğu gibi, büyük verinin kişisel veri ya da veriler içermesi durumunda, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) hükümlerinin uygulanacağı konusunda herhangi bir tereddüt bulunmamaktadır.

1.7.2.1. Büyük Verinin Özellikleri

Büyük verinin temelde üç ana özelliğinin bulunduğu kabul edilmiştir. Bu özellikler ilk defa 2001 yılında Loug Laney tarafından ortaya konulmuş ve 3V olarak adlandırılmıştır. Bunlar “yüksek hacim (*volume*)”, “yüksek hız (*velocity*)” ve “yüksek çeşitlilik (*variety*)”’dir. Daha sonra bu özelliklere farklı yazarlar veya otoriteler tarafından görece birtakım eklemeler yapılmış olsa da¹⁵² bugün doktrinde çoğunluğun büyük verinin 5 özelliğinin (5V olarak adlandırılan) bulunduğunu kabul ettiğini görmekteyiz. Temel özelliklerin yanına eklenen diğer iki özellik “doğruluk (*veracity*)” ve “değer (*value*)” unsurlarıdır¹⁵³. Bu unsurlardan, ilk üç temel

¹⁴⁹ Russell ve Norvig, 2024, s.26, 83; Retornaz, E. A., ve Güçlütürk, 2021, s.1.

¹⁵⁰ SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html (Erişim Tarihi: 18.07.2025); Retornaz ve Güçlütürk, 2021, s.9; IBM. *Unstructured data*. <https://www.ibm.com/think/topics/unstructured-data> (Erişim tarihi: 19.05.2025).

¹⁵¹ Atalan, 2024, s.33-34.

¹⁵² Örneğin, Ayata, *Stucke ve Grunes* yolundan giderek büyük verinin, “4V” olarak ifade edilen 4 özelliği olduğunu ifade etmektedir. Bunlar: verinin hacmi (*volume*), verinin hızı (*velocity*), verinin çeşitliliği (*variety*) ve verinin geçerliliği (*veracity*) unsurlarıdır. Bkz. AYATA, Z., Büyük Yenilik Büyük Değişiklik Gerektirir mi? Avrupa Birliği Rekabet Hukukunun Büyük Veri ile İmtihani, *Banka ve Ticaret Hukuku Dergisi*, 34 (4), s. 207; ayrıca bkz. Stucke, M., and Grunes, A (2016), *Big data and competition policy*, Oxford University Press, s.15. Özcan, 3 temel özelliğin yanına değer (*value*) özelliğini ekleyerek 4V kanaatini ortaya koymuştur. Özcan, A (2021). *Büyük veri: Fırsatlar ve tehditler*. TRT Akademi, 6 (11), <https://doi.org/10.37679/trta.818569>, s.16. SAS, 5V özelliğini vurgulamakta bunların 3 temel özelliğinin yanında doğruluk (*veracity*) ve değişkenlik (*variability*) olduğunu ifade etmektedir. Ayrıca bkz. Yıldız, A (2022). Büyük verinin V’leri ve veri analitiği. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (51), 361–378. <https://doi.org/10.30794/pausbed.111>.

¹⁵³ Retornaz, E. A., ve Güçlütürk, 2021, s.3.

özellik teknik oluşumu itibariyle büyük verinin sahip olduğu özellikler iken; sonradan eklenen iki özellik büyük veriden amaçlanan değer elde edilebilmesi için büyük verinin taşınması istenen özelliklerdir¹⁵⁴. Dolayısıyla bugün geldiğimiz noktada büyük verinin özelliklerini şu şekilde sayabiliriz¹⁵⁵.

- **Yüksek Hacim (Volume) :** Büyük verinin yüksek hacimli olması ilk özelliğidir. Bugün yaşadığımız bilgi ve teknoloji çağında; şirketler, işletmeler, nesnelerin interneti, internet, endüstriyel ekipmanlar, kameralar ve daha çok daha fazla kaynak sürekli olarak farklı kanallardan veri toplamaktadır. Dijital kanalları kullanan tüm kurum ve kuruluşların veri ürettiğini söyleyebiliriz. Bunun yanı sıra internette yapılan her işlem örneğin e-postalar, mesajlaşmalar ya da arama motorlarından yapılan taramalar da internet teknolojisine sahip nesnelerin birbiri ile iletişim ile de veri üretilmektedir¹⁵⁶. Tüm bu toplanan ve üretilen veriler nihayetinde çok büyük miktarda ve dolayısıyla hacimde veri kümeleri ortaya çıkmaktadır. Öyle ki, veri hacimlerinin büyümesi ve genişlemesi ile veri hacmini ifade etmek için her geçen gün yeni ifadelerle ihtiyaç duyulmaktadır. Veri hacmini ifade etmek için kullanılan kavramlara; bit, byte, kilobyte, megabyte, gigabyte yanında petabyte (1000 terabyte), exabyte (1000 petabyte), zettabyte (1000 exabyte) ve yottabyte (1000 zettabyte) ifadeleri örnek olarak verilebilir¹⁵⁷. Büyük miktarda verinin toplanması ve muhafaza edilmesi her ne kadar zor olsa da; teknolojinin sağladığı veri havuzları ve bulut sistemleri sayesinde yüksek hacimde veri toplanabilmesi geçmişe kıyasla maaliyeti büyük ölçüde hafifleterek büyük verinin oluşmasını kolay ve ucuz hale getirmiştir¹⁵⁸. Böylece büyük veri teknolojisinin geliştirilmesine imkan tanımıştır. 5G'nin hemen arkasından dünyanın kapısını çalan 6G teknolojisi, getirdiği yenilik ve gelişmeler ile daha büyük ölçekte verinin toplanmasına hizmet edecektir. Bir 6G teknolojisi türü olan dijital ikizler bu duruma örnek olarak verilebilir. Nitekim, şehirlerin sanal ikizlerini oluşturan bu teknoloji, şehirdeki farklı lokasyonlardan eş zamanlı olarak veri toplanması ve sanal dünyanın sürekli güncellenerek alınan kararların mevcut durumlara ve değişen koşullara göre alınmasını sağlamayı amaçlamaktadır. Bu da çok büyük miktarda ve dolayısıyla hacimde veriye karşılık gelmektedir¹⁵⁹. Diğer yandan hacim, büyük verinin değerini arttıran bir unsurdur. Nitekim, çok miktarda ve hacimde verinin analiz edilmesi daha doğru çıkarımlar elde edilebilecektir¹⁶⁰. Bugün devletlerin yanı sıra Amazon, Google, Meta gibi büyük şirketler de dünyada çok büyük hacimde veri toplayan şirketlerdir

- **Yüksek Hız (Velocity) :** Verilerin toplanması bugün tarihte eş benzeri görülmemiş bir hızda gerçekleştirilmektedir. Nesnelerin interneti teknolojisinin bu gelişmesinin ve

¹⁵⁴ Retornaz, E. A., ve Güçlütürk, 2021, s.3.

¹⁵⁵ SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html (Erişim Tarihi: 18.07.2025); Retornaz, E. A., ve Güçlütürk, 2021, s.3-9.

¹⁵⁶ Ayata, 2018, s.207-209.

¹⁵⁷ Özcan, 2021, s. 17.

¹⁵⁸ SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html (Erişim Tarihi: 18.07.2025); Retornaz, E. A., ve Güçlütürk, 2021, s.3-5.

¹⁵⁹ Özparlak, B.O. ve Yılmaz, S.S. (2021), 6G kablosuz teknolojisi ve veri: yeni hukuki tartışmalar, İçinde O. Güçlütürk & E. Retornaz (Ed.), *Gelişen teknolojiler ve hukuk III: Büyük veri* (1. baskı, s. 167-220), On İki Levha Yayınları, s.186-187.

¹⁶⁰ Ayata, 2018, s.209.

kapsamını arttırmasının bu hızın gerçekleşmesinde pay sahibidir. Özellikle, nesnelerde bulunan bazı sensörler ve akıllı sayaçlar neredeyse gerçek zamanlı olarak verileri toplayabilmektedir¹⁶¹. Bundan 10 yıl önce 2015 yılında OECD, neredeyse tüm medya, sosyal ve ekonomik faaliyetlerin internete (e-ticaret ve elektronik devlet hizmetleri dahil) taşınmasıyla birlikte, her saniye petabaytlarca veri üretildiğini belirtmiştir¹⁶². Verilere gerçek zamanlı olarak erişebilmek ise büyük bir değer yaratmaktadır. Öyle ki, bir yol haritası uygulamasındaki trafik bilgilerine anlık olarak erişmek kullanıcıya geleneksel verinin gecikmeli veri akışına kıyasla büyük bir fayda sağlamaktadır¹⁶³. Yüksek hızdan yalnızca verilerin hızlı şekilde toplanması değil, veriye ilişkin her türlü işlemin yapılması ifade edilmektedir. Bu verilerin analiz edilmesi sürecini kapsamaktadır. Kamera görüntülerinde anlık olarak yüz tanıma yapılabilmesi bu duruma örnek olarak verilebilir¹⁶⁴. E-ticaret kapsamında, şirketlerin sistemlerini her yeni değişiklikte anlık olarak optimize ederek fayda sağlaması da yüksek hızlı veri toplama ve işleme teknoloji sayesinde.

- **Yüksek Çeşitlilik (Variety) :** Büyük veriden bulunan verilerin birçok farklı kaynaktan toplanmasını, yapısal olarak farklı olmasını ve ayrı konulara ilişkin olması, büyük verinin çeşitlilik unsuruna ilişkindir¹⁶⁵. Öyle ki Büyük veri kapsamındaki veriler, geleneksel veri tabanlarındaki gibi yapılandırılmış sayısal verilerden, yapılandırılmamış metin belgelerine, e-postalara, videolara, ses kayıtlarına, borsa verilerine ve finansal işlemlere kadar her türlü formatta olabilir¹⁶⁶. Geleneksel veri toplama yönteminde hedefe yönelik ve sınıflandırılmış veriler toplanırken; büyük veride veriler amacına ve içeriğine bakılmaksızın adeta rastgele şekilde toplanmaktadır. Bu da büyük bir miktarda yapılandırılmamış veri anlamına gelmektedir. Bu verilerin analiz edilmesi ile anlamlanması mümkündür. Bu bir iş yükü olmasının yanı sıra bu verilerin maliyet olmadan ilgili pek çok başka amaçlarla da analizini mümkün kıldığı için aynı zamanda fayda da sağlamaktadır¹⁶⁷. Böylece birçok fonksiyonu kolaylıkla yerine getiren büyük veri, çeşitliliği sayesinde özellikle tüketiciler hakkında çok çeşitli bilgi edinilmesi ve analiz edilmesi profillemeye faaliyetlerini kolaylaştırarak şirketlere kazanç sağlamaktadır¹⁶⁸.
- **Değer (Value) :** Değer teknik olarak büyük verinin yapısal olarak sahip olduğu bir nitelik değildir. Daha ziyade, büyük veri analizinin daha isabetli ve kıymetli olması için

¹⁶¹ SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html (Erişim Tarihi: 18.07.2025).

¹⁶² OECD (2016), *Big Data: Bringing Competition Policy to the Digital Era* (OECD Roundtables on Competition Policy Papers, No. 193), OECD Publishing, s.6.

¹⁶³ OECD (2016). *Big Data: Bringing Competition Policy to the Digital Era* (OECD Roundtables on Competition Policy Papers, No. 193). OECD Publishing, s.6.

¹⁶⁴ Retornaz, E. A., ve Güçlütürk, 2021, s.6.

¹⁶⁵ Retornaz ve Güçlütürk, 2021, s.6.

¹⁶⁶ SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html Erişim Tarihi: 18.07.2025; Özcan, 2021, s.17-18.

¹⁶⁷ Ayata, 2018, s.210; Retornaz ve Güçlütürk, 2021, s.7.

¹⁶⁸ OECD (2016), *Big Data: Bringing Competition Policy to the Digital Era* (OECD Roundtables on Competition Policy Papers, No. 193), OECD Publishing, s.6.

olması arzu edilen bir özelliktir¹⁶⁹. Değerden kastedilen, verinin başlı başına bir ürün olması ve ekonomik değere sahip olmasıdır¹⁷⁰. 2012 yılında Dünya Ekonomik Forumu(OECD) veriyi bir ekonomik değer olarak ifade etmiştir¹⁷¹. Veriyi esasen kullanım amacı yani analizi ile ulaşılmak istenen amaç değerli kılmaktadır. Ne var ki, analizin gerçekleşmesi için birçok veri kümesine ihtiyaç duyulmaktadır. Bu veri kümelerinin elde edilmesi gerekir. Varılmak istenen yer için gereken büyük veri böylece tek başına bir değeri ifade eder hale gelmiştir¹⁷². Büyük verinin bir ekonomik değerinin olması her şeyin veri'ye dönüştürülme çabasını doğurmuştur. Bu da haberli veya habersiz pek çok kanaldan kişilere ilişkin veya olmayan verilerin toplanmasını ve işlenmesini ve bundan doğan tehlikeleri beraberinde getirmiştir¹⁷³. Her geçen gün büyük veri teknolojisinin ekonomik artması karşısında e-ticaret platformları, devletler ve ekonomik birlikler bu teknolojileri daha da geliştirmek için büyük çapta yatırımlar yapmaktadır¹⁷⁴.

- **Doğruluk (Veracity)** : Değerde yapısal özellik bakımından ifade ettiklerimiz aynen burada da geçerlidir. Doğruluk büyük veride istediğimiz bir özelliktir; yapısı içinde barındırdığı bir özellik değildir. Verinin ilgili bulunduğu durumu isabetli şekilde ifade etme halinde “doğruluk” denilmektedir. Verinin doğru olması, veri analizi ile elde edilecek karar/çıkarımın daha isabetli olması sonucunu doğuracaktır. Bu sebeple önemlidir¹⁷⁵. Doğruluk aynı zamanda verinin kalitesini ifade etmektedir. Birçok farklı kaynaktan tabiri caizse rastgele şekilde elde edilmiş farklı türden verilerin işletmelerce kategorize edilmesi, sınıflandırılması ve belli bir sistematik içinde ilişkilendirilmesi gerekmektedir. Aksi halde veriler kontrolden çıkabilir¹⁷⁶.

1.7.2.2. Yapay zeka ve büyük veri ilişkisi

Yapay zeka teknolojisinin gelişmiş bir veri analizi sistemi olduğu söylenebilir. Nitekim, YZ teknolojisinin, büyük verinin bir tamamlayıcısı olma ve anlamlandırılmasına aracılık eden işlevsel bir fonksiyonu bulunmaktadır¹⁷⁷. Bu iki teknoloji birbirine karşılıklı olarak yardım etmektedir. Nitekim, büyük veri sayesinde geliştirilebilen makinaların öğrenmesi yaklaşımı yapay zekanın canlanmasını ve gelişmesinin önünü açmıştır¹⁷⁸. Veri ihtiyacı yüksek olan makina öğrenimi yeteneğine sahip yapay zeka sistemlerinin gelişmesi ile ise verinin değeri

¹⁶⁹ Retornaz ve Güçlütürk,2021, s.3,7.

¹⁷⁰ Ayata, 2018, s.210; Retornaz ve Güçlütürk,2021, s.7.

¹⁷¹ OECD, (2012), *OECD Economic Outlook, Volume 2012 Issue 2*, OECD Publishing. Ayrıca bkz. Bkz. Sholtz 2001, “Redefining the Market for Privacy” başlığı; Özparlak ve Yılmaz, 2021, s.169.

¹⁷² Ayata, 2018, s.210; Retornaz ve Güçlütürk,2021, s.7.

¹⁷³ Retornaz ve Güçlütürk,2021, s.7-8.

¹⁷⁴ Başalp, N (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun temel yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21 (1), 78.

¹⁷⁵ Retornaz ve Güçlütürk,2021, s.2-3,8.

¹⁷⁶SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html (Erişim Tarihi: 18.07.2025).

¹⁷⁷ Köksal, D. ve Konukpay, C (2021), Büyük veri kullanımının temel hak ve özgürlükler üzerindeki etkileri, İçinde O. Güçlütürk & E. Retornaz (Ed.), *Gelişen teknolojiler ve hukuk III: Büyük veri* (1. baskı, s. 15–89), On İki Levha Yayınları, s.15-16; Atalan, 2024, s.27.

¹⁷⁸ Russell ve Norvig, 2024, s.26, 83.

giderek artmıştır. Bu gelişmeler neticesinde; ürün ve hizmet tasarlanmasında, pazarlanmasında ve geliştirilmesinde veri üretimi ayrıca gözetilmiş ve gelinen noktada yeni nesil ürün ve hizmetlerin kendileri de birer veri toplama ve işleme aracına dönüşmüştür¹⁷⁹. Örneğin, bir robot süpürge sensörleri vasıtası ile bulunduğu evin haritasını ve eşyaların yerlerinin verisini toplayabilmekte ve sistemine işleyebilmektedir.

Hukuki perspektiften büyük verinin özellikle de temel hak ve özgürlükler bakımından doğurduğu tehlike ve risklerin analizi, yapay zeka teknolojileri ile birlikte ele alınmalıdır. Nitekim günümüzde yapay zeka teknolojileri, büyük veri analizinde kullanılan en etkili araçlardır. Yapay zeka gözetilmeden yapılan hukuki değerlendirme bu kapsamda eksiktir. Bu iki teknoloji yalnızca birbirini desteklemekle kalmamakta, aynı zamanda ortak amacın gerçekleştirilmesinde birbirini tamamlayıcı nitelik taşımaktadır¹⁸⁰.

1.7.3. Veri'nin bir alt kümesi olarak: kişisel veri

Büyük verinin bir kısmını kişilere ilişkin veriler yani kişisel verilerden oluşturmaktadır. Belirli veya belirlenebilir -kişiye ilişkin her türlü veri, kişisel veridir. Kişisel veri tanımı ve unsurlarına ilişkin ikinci bölümde detaylı bir inceleme yapılmıştır. Ayrıca yapay zeka ve kişisel veri ilişkisi üçüncü bölümde işlenmiştir.

Yapay zekanın modellerinin oluşturulması ve sisteminin çalışması için ihtiyaç duyduğu verilerin de bir kısmını büyük verinin bir parçası olan kişisel veriler oluşturmaktadır. Yapay zeka sistemlerinde kişiye ilişkin veriler yani kişisel veriler ile üç aşamada karşılaşılır: YZ modellerinin eğitilmesi için kullanılan eğitim setlerinde (örneğin YZ modeline yüzleri tanıması için verilecek kişilere ilişkin yüz fotoğraflarını içeren eğitim setleri), YZ algoritmalarından karar vermeleri istenmesi halinde sisteme verilen girdilerde (örneğin YZ algoritmasının tanıması istenen kişiye ilişkin yüz fotoğrafının sisteme girdi olarak verilmesi) ve son olarak YZ algoritmalarının verdiği kararların kişiye ilişkin bir çıkarım olması halinde sonucun/kararın (örneğin YZ algoritmasının fotoğrafı tanımlayıp ilişkin olduğu kişiye ait ismi çıktı olarak vermesi) doğrudan kişisel veri özelliğinin bulunması halinde¹⁸¹.

Yapay zeka sistemlerinin, kişisel veriler bakımından iki önemli fonksiyonundan bahsedilebilecektir. Bunlardan ilkinde YZ, belirli teknikler kullanılarak anonim hale getirilmiş veya kişisel veri özelliğinden arındırılmış veri setlerindeki bilgileri birtakım başka bilgiler ile birleştirmek sureti ile verisi işlenen kişiyi belirli kılabilmeyi mümkün hale getirebilecektir¹⁸². İkinci olarak YZ sistemine girdi olarak dahil edilen kişiye ilişkin bilgilerin işlenmesi ile algoritmaların ilgili kişi hakkında çıkarımda bulunması halidir. Bu durumda YZ kişiye ilişkin bilgilerden hareketle ilgili kişi hakkında yeni bir kişisel veri üretmektedir¹⁸³. Bu durumda YZ algoritmasının kişisel veri çıkarımı kesin ve doğru sonuç olmayabilir, nitekim algoritma bu çıkarımı verileri analiz ederek üretir. Verinin eksik, yanlış veya güncel olmaması hallerinde üretilen çıkarım verinin bu özelliklerinden etkilenecektir¹⁸⁴.

¹⁷⁹ Retornaz ve Güçlütürk, 2021, s.1.

¹⁸⁰ Köksal ve Konukpay, 2021, s.15-16.

¹⁸¹ Güçlütürk, 2022, s.285.

¹⁸² Bkz. aşağıda "2.1.3. Belirli veya belirlenebilir olma" başlığı.

¹⁸³ Ayrıca bkz. aşağıda "Profilleme" Başlığı.

¹⁸⁴ Güçlütürk, 2022, s.281-282.

Son olarak belirtmek isteriz ki, uygulama alanı oldukça geniş olan büyük veri ve yapay zeka teknolojileri, hangi amaca ve sektöre hizmet ettikleri belirlenerek; bu belirlenen alanlar gözetilmek suretiyle hukuki perspektiften özel bir değerlendirmeye tabi tutulmalıdır. Nitekim hizmet ettikleri sektöre göre farklı teknik özellikler barındıran yapay zeka teknolojileri ile farklı türde veriler içeren büyük verinin, tek bir hukuk dalı kapsamında ve tüm sektörleri kapsayacak şekilde ele alınması yetersiz ve eksik bir yaklaşım olacaktır.



İKİNCİ BÖLÜM

GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI

2.1. Kişisel Verilerin Korunması İhtiyacı

Kişisel verilerin korunması alanındaki hukuki tartışmalar 1960'lı yıllarda hızla gelişen bilgisayar teknolojileri karşısında özel hayatın korunması düşüncesi ile ele alınmaya başlanmıştır. 20. yüzyılda bilgi ve teknoloji alanındaki gelişmeler kişisel verilerin işlenmesini ciddi şekilde arttırmış, internetin bulunması ise meseleyi kritik bir noktaya taşımıştır¹⁸⁵. Teknolojik gelişmeler bir yandan globalleşmeyi tetiklemiş bir yandan da bilgi toplumuna geçiş yapılmasını sağlamıştır. Kişisel verilerin korunması sorunu ise bugünkü bilgi toplumunun oluşun sürecinin bir ürünüdür. Bugün yaşadığımız veri tabanlı toplumda insanlar hakkındaki bilgiler sosyal ve ekonomik yandan faydalı ve hayati öneme sahiptir. Güç ile özdeşleştirilen kişisel veriler hem kamu kuruluşları hem de özel sektör tarafından toplanmakta ve çeşitli amaçlar için işlenmektedir. Nitekim, sağlık hizmetleri, sosyal yardımlar, vergilendirme, suç tespiti ve terörizmin önlenmesinde, şirketler açısından pazarlama ve ticaret stratejilerinin yürütülmesinde kişisel verilere ihtiyaç duyulmaktadır¹⁸⁶.

Devlet ya da özel bir şirketin kişiler hakkında öğrendikleri ve işlemeye aldıkları veri sayılamaz hale gelmiştir. Gelineen noktada bir kişiye ait veriler toplanarak ve karşılaştırılarak, kişilerin özeli, alışkanlıkları ve tercihleri hakkında bilgi olunabilir ve yüksek tahminler yapılabilir hale gelmiştir. Örneğin, kredi kartı alışkanlıkları takip edilerek bir kişinin alışveriş alışkanlıkları öğrenebileceği gibi, internet kullanımı sırasında kullandığı çerezler (cookies) yolu ile ilgi alanları kolaylıkla öğrenilebilir hale gelmiştir¹⁸⁷.

Modern teknoloji, bilginin toplanarak, depolanmasını, işlenmesini ve aktarılmasını hızlandırmış ve çok kolaylaştırmıştır. Böylelikle, veriler kurumlar, şirketler ve devletler arasında kolaylıkla aktarılabilir hale gelmiştir. Özellikle kişisel verilere erişimin kolaylaşması ile veri sahiplerinin maddi ve manevi olarak zarar görmeye başlamış ve bu sebeple kişisel verilerin korunması ihtiyacı doğmuştur¹⁸⁸. Teknolojinin gelişmesi ile bireyin tüm verilerini kayıt altına alabilen, onu adeta şeffaflaştıran, özel hayatının gizliliğini ortadan kaldıran, bireyi basit bir veri objesi haline getiren ve işlediği veriler neticesinde bireyin olası davranışlarını tahmin edebilme imkanı yaratan sistemler bireylerin temel hak ve özgürlüklerini ihlal etmektedir. Öyle ki, çoğunlukla ihlal edilen değer yalnızca kişisel verilerin korunması hakkı olmamaktadır. Nitekim, yukarıda bahsedildiği üzere kişisel verileri ihlal edilen bireyin ilişkili diğer hakları da ihlal edilebilmektedir^{189 190}.

¹⁸⁵ Akgül, 2014, s. 345-346; Ayözger Öngün, 2019, s.76.

¹⁸⁶ Prins, 2006, s. 273; Aksoy, 2010, 2-4, 75, 119, KVKK Gerekeç s.6.

¹⁸⁷ Develioğlu, 2017, s. 1.

¹⁸⁸ Ayözger Öngün, 2019, s.1.

¹⁸⁹ bkz. aşağıda "Günümüz "2.3.4.Bağımsız Hak" Yaklaşımı" başlığı.

¹⁹⁰ Şimşek, 2008, s. 218-219.

Bireyin bir toplantı veya gösteri yürüyüşüne katılmak istemesi, derneğe üye olmak istemesi veya bir sivil toplum örgütünün etkinliklerine katılmak istemesi durumlarında faaliyetlerinin kapsamlı şekilde kayıt altına alındığını bilmesi ve bu kayıtların olası riskler içermesi karşısında muhtemel bu temel hak ve özgürlüklerini (örneğin toplantı ve gösteri yürüyüşü hakkı, dernek üyeliği hakkı) kullanmaktan vazgeçecektir. Nitekim, somut olay bakımından, bireyin katıldığı toplantının niteliğine göre bireyin değişik özelliklerini ortaya koyan verilerin de oluşturulabilmesi mümkün olabilecektir. Çağdaş ve insan haklarını temel alan hukuk düzenlerinde bu durum istenmeyen bir tablo olarak kendini gösterir. Bu bakımdan, kişisel verilerin korunması temel hakkı bireyin diğer hak ve özgürlüklerini etkin ve efektif şekilde kullanması için de son derecede önemlidir¹⁹¹. Kişisel verilerin korunması hakkının kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması hakkı ile ilişkili olduğu ifade etmek gerekir¹⁹². Kişisel verilerin korunmadığı bir toplumda, mahremiyete saygı duyulduğundan veya özel hayatın gizliliğinin korunduğundan söz edilemeyeceğinin altını çizmek gerekir¹⁹³.

Kişisel verilerin kural olarak kişilerin rızası olmadan toplanması bile yasaklanmış olmasına rağmen, uygulamada veri bankalarının oluşturulduğuna ve özellikle pazarlamacı ile özel teşebbüslere dağıtılması veya diğer bir deyişle satılarak ticaretinin yapılması ile şirketlerin potansiyel müşteri olarak belirlediği kişilere rızaları olmaksızın ulaşmaları yaygın hale gelmiştir¹⁹⁴. İnsanlara “daha iyi hizmet sunmak için” görüşmeleri; doğru teşhis için mahrem sağlık bilgileri, işyeri giriş çıkışları ile bugün devlete ait KYK yurtlarında biyometrik veriler(parmak izi), algoritmanın kişisel tüketici hizmeti sunması için alışveriş verileri işlenmektedir. Bu verilerin, kimler tarafından toplandığı çoğu zaman bugün bilinebilmekte ise de kişisel verilerin akıbetinin ne olacağı, daha sonra hangi amaçlarla ve kimler tarafından da kullanılacağı soruları endişe vericidir. İsimlerden beğenilere, düşüncelerden tercihlere kadar kişinin gerçekte kim olduğunu yansıtan kişisel verilere sınırsız erişim kişinin kendi olmasının önünde bir engel teşkil edebileceği yönünde haklı endişeler bulunmaktadır. Zira, sürekli izlenip gözetlenme ihtimali insanı benzersiz kılan “*kişilik*”in geliştirilmesi önünde önemli bir engeldir¹⁹⁵.

Bilgi toplumu ekonomisi kişisel verilere ihtiyaç duymaktadır. Kişisel verilere duyulan ihtiyaç, devletin sosyal devlet ilkesini yerine getirmesinden kaynaklandığı gibi Şirketlerin endüstriyel üretiminin temini ve tüketici taleplerin karşılanması süreçlerinin yönetilmesinden de kaynaklanabilmektedir. Modern iletişim araçları vasıtası ile hızlı ve masif büyüklükte kişisel verilerin toplanması ve işlenmesi dengeyi bireyler aleyhine bozmaktadır¹⁹⁶. Bu bakımından,

¹⁹¹ Şimşek, 2008, s. 113, 218-219. ”Nitekim özgürlükçü bir demokrasinin işlemesi topluma katılma ve toplum içerisinde işlev görebilme becerisine bağlıdır. Bir başka anlatımla demokratik düzen ancak özgürce kişiliğini geliştirebilmiş yurttaşların varlığı ile sürdürülebilir. Demokratik toplumun sürekliliğinin sağlanabilmesi, devlet tarafından kişisel verilerin sınırsız bir şekilde toplanması, kaydedilmesi, kullanılması ve aktarılması karşısında bireyin korunmasına bağlıdır.” Küzeci, 2014, *İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı*”, s.57.

¹⁹²Kişisel Verileri Koruma Kurumu (2025) . *Madde ve gerekçesi ile kişisel verilerin korunması kanunu (Bilgi notu) ve kişisel verilerin korunmasına ilişkin terimler sözlüğü* (KVKK Yayınları) . Ankara, s.7.

¹⁹³ Selek, 2021, s.94.

¹⁹⁴ Develioğlu, 2017, s. 1; Aksoy, 2010, 78.

¹⁹⁵ Küzeci, 2014, ” *Anayasal Bir Hak: Kişisel Verilerin Korunması*“, s.142-149.

¹⁹⁶Aksoy, 2010, s.4; Akgül, 2014,, s. 343. Bir kişinin alışveriş alışkanlıklarından kişilere çeşitli reklamlar gönderip maddi kazanç sağlayabileceği gibi kişinin cinsel yaşamına ilişkin elde edilen bilgiler ile tehdit ile kişiden birtakım taleplerde bulunulabilir ve kişiye manevi olarak zarar verebilir. Aksoy, 2010, s.3.

bireyin özerkliği ile hak ve hürriyetleri bu bilgi akışına hukuki müdahaleyi gerektirmiştir¹⁹⁷. Bireylerin kişisel verilerinin akıbeti ve işlenen verilerin tehdit potansiyeli üzerinde duydukları endişe tespiti kişisel verilerin korunması alanında özel düzenleyici metinlerin oluşturulmasında etkili olmuştur¹⁹⁸. Nitekim, genel hükümler kişisel verilerin korunmasına özgü düşünceden yoksun olmaları sebebi ile artan ihtiyacı karşılayamamaktadır¹⁹⁹. Doktrinde özel yaşamın gizliliğinin artık bittiğine inanılan bu çağda elimizde kalan en güçlü silahlardan birinin kişisel verilerin korunması olduğu ifade edilmiştir²⁰⁰.

2.2. Kişisel Veri Kavramı Tanımı ve Unsurları

Kişisel veri kavramı, ulusal ve uluslararası metinlerde yer aldığı şekliyle; “*belirli veya belirlenebilir bir kişiye ait her türlü veri*” olarak tanımlanabilir²⁰¹.

Kişisel veri kavramının tanımından hareketle gerçek bir kişiye ilişkin “*her türlü bilginin*” kişisel veri kapsamında olduğunu söylemek mümkündür. Dolayısıyla kavramın kapsamının epey geniş tutulmuştur. Kişisel veriye örnek olarak, doğum yılı, ev adresi, isim, etnik köken, meslek, yaş, cinsiyet, fiziksel özellikler, eğitim bilgileri, sağlık verileri, malvarlığı bilgisi, bilgisayar log kayıtları, adli sicil, sendikal faaliyetleri, görüntü, fatura bilgileri, trafik cezaları, boş zaman uğraşları, IP adresleri, bağımlılıkları, sosyal medya beğeni ve paylaşımları veya alışveriş alışkanlıkları verilebilir²⁰². Yaşadığımız teknoloji ve internet çağında var olabilmenin bir ön koşulu haline gelen kişisel verilerin örnekleri saymakla bitmeyecektir.

Yukarıda verilen kişisel veri tanımdan hareketle kişisel verilerin unsurlarını belirlemek mümkün olsa da bu unsurlara ilişkin doktrinde bir görüş birliği bulunmamaktadır²⁰³.

¹⁹⁷Schwartz, 2004, “*Right of Informational Self-Determination*”, s.677, 701.

¹⁹⁸European Commission (2012, January 25) . *Press release: GDPR regulation*. https://ec.europa.eu/commission/presscorner/detail/en/memo_14_186 (Erişim Tarihi: 04.05. 2025) .

¹⁹⁹Aksoy, 2010, s.120.

²⁰⁰Küzeci, 2014, “*Anayasal Bir Hak: Kişisel Verilerin Korunması*”, s.142-149.

²⁰¹ Kişisel veri, Avrupa Birliği (1995) . *Veri Koruma Direktifi* (95/46/EC), m.2/a: “tanımlanmış veya tanımlanabilir gerçek kişiye (veri sahibi) ilişkin her türlü bilgi.” olarak tanımlanmıştır. Bu tanım kişisel veri kavramına ilişkin temel tanım teşkil etmektedir. Birçok iç hukuk düzenlemesi ve Avrupa Birliği düzenleyici metinleri bu tanıma kullanmıştır. Öyle ki, kişisel veri söz konusu direktif ile aynı doğrultuda Avrupa Birliği (2016) . *Genel Veri Koruma Tüzüğü* (GDPR), m.4/1: “tanımlanmış (identified) veya tanımlanabilir (identifiable) gerçek kişiye ilişkin her türlü bilgi.” olarak tanımlanmıştır. Benzer şekilde, Türk hukukunda veri korunmasına ilişkin temel kanun olan 6698 sayılı *Kişisel Verilerin Korunması Kanunu* (Kabul Tarihi: 24 Mart 2016, Resmi Gazete Sayısı: 29677, Resmi Gazete Tarihi: 07.04.2016) m. 3/1-d’de bu kavram “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” şeklinde ifade edilmiştir.

²⁰² GDPR, m.4/1; KVKK m.3 gerekçesi. European Union (2007, June 20) . *Opinion 4/2007 on The Concept of Personal Data, Article 29 Working Party*, s.6-17. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf (Erişim tarihi: 30.01.2025) . Avrupa Adalet Divanı’nın 6.11.2003 tarihli C-101/01 sayılı kararı (Lindqvist), §24: Kişisel veri, kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgiyi kapsamaktadır. Bu terim kuşkusuz bir kişinin telefon koordinatlarıyla birlikte adını ya da çalışma koşulları veya hobileri hakkındaki bilgileri de kapsamaktadır. Karar için bkz. Avrupa Adalet Divanı (2003, November 6) . C-101/01 (Lindqvist), <https://curia.europa.eu/juris/recherche.jsf?language=fr> (Erişim tarihi: 29.04.2025) .

²⁰³Nitekim doktrinde; kişisel veri kavramının “bilgi” ve “belirli veya belirlenebilir kişi” olarak iki unsurdan oluştuğu bkz. Ayözger Öngün, Ç (2019) . *Kişisel verilerin korunması hukuku: Elektronik haberleşme sektörüne ilişkin özel düzenlemeler dahil* (Genişletilmiş 2. baskı) . Beta Yayınları, s.7-8); “kişi”, “belirli veya belirlenebilir olma”, “bilgi” ve “ilişkin olma” olmak üzere dört unsurdan oluştuğu bkz. Develioğlu, 2017, s.30 veya “belirli veya belirlenebilir gerçek kişi”, “bilgi” ve “bilginin kişiye ilişkin olması” olarak üç unsurdan oluştuğu şeklinde belirlemeler yapılmıştır, bkz. Taştan, F. G (2017) . *Türk sözleşme hukukunda kişisel verilerin korunması* (2. basım)

Çalışmamıza Avrupa Birliği'nin bağımsız danışman organı olan Article 29 Working Party²⁰⁴,nin kişisel veri kavramına ve unsurlarına ilişkin hazırladığı Kişisel Veri Kavramı Hakkında Görüş (Opinion 4/2007 on The Concept of Personal Data)²⁰⁵ isimli rapor temel alınmıştır. Bu raporda, kişisel veri kavramı dört ana unsur çerçevesinde incelenmiş ve bu unsurların birbirleriyle yakından bağlantılı olduğu ve birbirini tamamladığı ifade edilmiştir. Bunlar: “Her türlü bilgi”, “İlgili olmak”, “Kimliği belirli veya belirlenebilir Olma” ve “Gerçek kişi” unsurlarıdır. Tüzel kişilerin kişisel veri korumasından faydalanması hususunun doktrinde tartışmalı olması sebebi²⁰⁶ ile “Gerçek Kişi” unsuru Çalışmamızda “Kişi” unsuru olarak ele alınmıştır. İşlenen verinin aşağıda detaylı şekilde açıklanan kıstasları karşılamaması halinde söz konusu veri, “kişisel veri” olarak kabul edilmeyecek ve kişisel verilerin korunması hukuku kapsamında bir korumadan bahsedilemeyecektir.

2.2.1. Her türlü bilgi

Kişisel verilere ilişkin düzenleyici metinlerde kişisel veri (“personal data”)²⁰⁷ kavramına yer verilse de; kişisel veri hukuku ve literatürünü anlamada Avrupa Birliği danışmanlık organı görevini yerine getirmiş olan 29. Working Party Çalışmasına bakıldığında; kişisel veri tanımlamasını yaparken unsur olarak veri(data) kavramının değil; bilgi-enformasyon (information) ifadesinin kullanıldığı görülecektir²⁰⁸. Bu sebeple bu kavramların kapsamlarına kısa bir bakış atılması faydalı olacaktır.

Bilgi, bilişim parantezinde “Verinin anlam kazanmış biçimi” olarak tanımlanmaktadır²⁰⁹. Veri, tek başına bir anlam ifade etmeyen veya kullanılamayan ve analiz

. Onikilevha Yayınları, s.27-28 aynı ayırım için bkz. Aksoy, H. C (2010) . *Medeni hukuk ve özellikle kişilik hakkı yönünden kişisel verilerin korunması*. Çakmak Yayınları, s.13.

²⁰⁴ Article 29 Working party (Art. 29 WP), Avrupa Birliği 95/46/EC sayılı Direktifinin 29. maddesi uyarınca kurulmuştur. Bu çalışma grubu, kişisel verilerin korunması ve mahremiyet konuları üzerinde çalışan bağımsız bir Avrupa Birliği danışma organıdır. Bu kapsamda, Avrupa Komisyonu'nun bir pozisyonunda değildir. Görevleri, 95/46/EC sayılı Direktif'in 30. maddesinde ve 2002/58/EC sayılı Direktif'in 15. maddesinde belirtilmiştir. Article 29 Working Party (Art. 29 WP) tarafından yayınlanan materyaller (görüşler, çalışma belgeleri, mektuplar vb.) yalnızca Article 29 Working Party görüşlerini yansıtmaktadır. Dolayısıyla bu materyallerin Avrupa Birliği üye devletlerine ilişkin esasen bağlayıcılığı bulunmamakla birlikte Avrupa Birliği'nin veri koruması ve mahremiyete ilişkin yayımladığı düzenleyici metinlerin anlaşılması ve yorumlanmasında rehberlik etmektedir. 25 Mayıs 2018 tarihinden sonra (GDPR'nin uygulamaya girmesi) Article 29 Working Party yerini ve görevlerini Avrupa Veri Koruma Kurumu'na (European Data Protection Board “EDPB”) bırakmıştır. Article 29 Working Party (Art. 29 WP) (t.y.) . *Who we are: Legacy of Article 29 Working Party*. European Data Protection Board. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en (Erişim tarihi: 30.01.2025)

²⁰⁵ Opinion 4/2007 on The Concept of Personal Data, 20.06.2007 tarihinde kabul edilmiştir. Bu rapor ile kişisel veri kavramına ortak bir anlayış getirmek amaçlanmıştır. Kişisel veri kavramının ortak bir tanımına ulaşarak amaçlanan hangi bilgilerin veri koruma kuralları kapsamında değerlendirileceğini belirlemektir. Böylece, Avrupa genelinde kişisel veri kavramına nasıl yaklaşılması gerektiğine dair rehberlik sağlanmış ve böylece Article 29 Working Party'nin temel işlevlerinden biri olan veri koruma kurallarının tutarlı şekilde uygulanması sağlanmaya çalışılmıştır. İlgili raporunun İngilizce tam metni için bkz. European Union (2007, June 20) . Opinion 4/2007 on the concept of personal data. Article 29 Working Party. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf (Erişim tarihi: 30.01.2025) .

²⁰⁶bkz. “Kişi” başlığı.

²⁰⁷ bkz. 95/46/EC nolu Veri Koruma Direktifi m.2/a; GDPR m.4/1; KVKK m.3/1-d.

²⁰⁸ Aynı yönde bkz. Ayözger Öngün, 2019; . Develioğlu, 2017, s.36, Taştan, 2017, s.36. Selek, ise kişisel veri unsuru olarak farklı olarak “Her Türlü Veri” ifadesini kullanmıştır. Selek, O (2021) . *Kişisel verilerin korunması ve verileri yok etme suçu (TCK m.138)* . Onikilevha Yayınları, s.6.

²⁰⁹Bkz. Türk Dil Kurumu. *Büyük Türkçe Sözlük*. <https://sozluk.gov.tr/> (Erişim tarihi: 31.01.2025)

edilmeye muhtaç olunan ham bilgiyi ifade etmektedir²¹⁰. Veri, enformasyona ve bilgiye temel oluşturmaktadır. Verinin kendisinden ve yorumlanması birlikte ele alınarak bilgiye ulaşılır²¹¹. Bilginin ortaya çıkabilmesi için veriye anlam yüklenmesi gerekmektedir. İlgili ve ilişkili verilerin, belli bir amaç doğrultusunda bir araya getirilmesi ile ise enformasyon ismi verilir. Böylece bilgide olduğu gibi veriler anlam kazanarak enformasyona temel oluştururlar. Bilgi, insan beyninde ve/veya zihninde bulunduğundan soyut bir varlığa işaret etmektedir. İnsan zihnindeki bilgiler elektronik ya da basılı bir kayıt ortamına aktarıldığında veya birileriyle paylaşıldığında enformasyona dönüşebilir. Bu kavramlar birbirleriyle doğrudan ilişkili olmalarına karşın aralarında içeriksel ve anlamsal birtakım ayırt edici farklılıklar vardır. Bu farklılıklara karşın, bu kavramların özellikle Türkçe literatürde genellikle birbirlerinin yerine kullanıldığı görülmektedir²¹². Kişisel verilerin korunması hukuku bakımından da benzer şekilde, kavramlar arasındaki farklar olduğu kabul edilmekle birlikte, uygulamada zorluklara sebep olacağı sebep gösterilerek; birbirinin yerine kullanılmalarında bir sakınca görülmediği yönünde görüş birliği oluşmuştur²¹³.

Kişisel veri kavramına ilişkin düzenleyici metinlerde verilen tanıma göre bir kişiye ilişkin “*her türlü veri*” kişisel veri kapsamındadır. Kavramın kapsama alanı kasıtlı şekilde geniş tutularak bir bireyle bağlantılı olabilecek tüm bilgiler kişisel veri olarak kabul edilmiştir²¹⁴. Bu cihetle her bir bilgi özelinde kişisel veri değerlendirmesi yapılmalıdır.

Verinin niteliği açısından bakıldığında, verinin kişisel veri olarak tanımlanabilmesi için öznel veya nesnel olmasının bir önemi bulunmamaktadır. Bu kapsamda isim, tc kimlik numarası, işyeri, meslek, malvarlığı, kan tahlilleri, hastalıklar, sınav notları gibi nesnel bilgilerin yanı sıra bir çalışanın performansı ile ilgili amirince yapılan kişisel değerlendirmeler, kişinin güvenilir olup olmamasına ilişkin yapılan yorumlar, kişilik üzerine yapılan saptamalar ve kişinin kendi yorum ve düşünceleri gibi öznel bilgiler de kişisel veri kapsamına girmektedir.

Kişisel veri; bireyin özel yaşamıyla ilgili olabileceği gibi, iş hayatına²¹⁵, sosyal ilişkilerine veya kamusal yaşamına²¹⁶ dair bilgiler de olabilir²¹⁷. Öyle ki, şahsi yazışmaların yapılmadığı şirket çalışanlarının ticari/şirket mailleri kişisel veri niteliğindedir. Bu durum Şirket’in bu mailleri kaydetmesi ve aktarmasında kişisel verilerin korunması mevzuatına uygun

²¹⁰ Veri hakkında daha fazla bilgi için bkz. yukarı “1.8 Veri” Başlığı.

²¹¹ İnan, 2015, s.15.

²¹² Yılmaz, M (2009) . Enformasyon ve bilgi kavramları bağlamında enformasyon yönetimi ve bilgi yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49 (1), 97–98, s. 113–114. “*Bilgi Toplumu parantezinde ‘bilgi’ kavramı doksanlı yılların başından itibaren başlangıçta veri, enformasyon ve bilgi üçlemesindeki enformasyonun (information) yerine kullanılmakta idi. Ancak internetin yarattığı gelişme, çok geçmeden aslolan terimin bilgi (knowledge) olması gereğini ortaya koydu. Her ne kadar bu üç kavram birbirlerinden ayrı kavramlar olarak gözükseler de her birinin tanımının yapılabilmesi için aslında birbirlerine ihtiyaç duyulduğu da bir gerçek.*” Medeni, İ. T., ve Aktaş, Z (2010) . Veri toplumundan bilgi toplumuna dört düzeyli bir toplum modeli. 3. *Ağ ve Bilgi Güvenliği Ulusal Sempozyumu*, s. 5–6.

²¹³ bkz. Küzeci, E (2010) . Kişisel verilerin korunması. Turhan Kitabevi, s.9; Selek, 2021, s.7.

²¹⁴ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.4-5.

²¹⁵ Avrupa Adalet Divanı, 09.11.2010 tarihli Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09) contre Land Hessen kararında, internet ortamında paylaşılan kişilerin iş yaşamına ilişkin bilgiler kişisel veri olarak kabul edilmiştir. Bkz. Avrupa Adalet Divanı (2010, November 9) . *Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09) v. Land Hessen*. <https://curia.europa.eu/juris/recherche.jsf?language=fr> (Erişim tarihi: 29.04.2025) .

²¹⁶ Aksoy, 2010, s.63.

²¹⁷ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.6.

hareket etmesini zorunlu kılmaktadır²¹⁸. Gizli ve gizli olmayan kişiye ilişkin her veri kişisel veri olarak kabul edilir. Bu bakımdan kişinin cinsel tercihi veya kredi kartı şifresi bilgileri gibi kamusal alanda giydiği kıyafet veya arabasının markası gibi herkesin kolaylıkla ulaşabileceği bilgiler de kişisel veridir²¹⁹.

Bir verinin, kişisel veri olarak kabul edilmesi için doğru veya doğruluğu kanıtlanmış olması gerekmemektedir. Kişiye ilişkin yanlış bilgiler de kişisel veri kapsamındadır. Nitekim, kişisel verilerin korunmasına ilişkin düzenlemelerde, kişisel bilgilerin yanlış veya hatalı olması ihtimali karşısında ilgili kişilere veri sorumlusuna müracaat yolu ile kişisel verilerine erişim hakkı ve yanlış işlenen bilgilerinin düzeltilmesi haklarının tanınması bunu göstermektedir²²⁰. Bir iş adamının kara para akladığını iddia edildiğinde medyada yer alan bilgi, gerçek olmasa da kişisel veridir. Somut olayda, şan, şeref ve haysiyeti yani kişilik hakları saldırıya uğrayan iş adamının haberin düzeltilmesini talep hakkı bulunur²²¹.

Kişiye ilişkin bilginin hangi format veya ortamda saklandığı da kişisel veri sınıflandırmasında bir önem taşımaz. Bu kapsamda, bilgilerin kağıt üzerinde olması ile bilgisayar belleğinde bulunması arasında sınıflandırma açısından bir fark bulunmamaktadır. Bilgiler alfabetik, sayısal, grafiksel, fotografik veya akustik şekilde olabilir. Bu bilgiler bir bireye ilişkilendirilebildikleri ölçüde, kişisel veri kapsamındadır²²². İnsan dokuları tek başına kişisel veri olarak kabul edilmese de, bu dokulardan elde edilen biyometrik veriler kişisel veri olarak kabul edilir. Örneğin parmak izi biyometrik veri²²³ yani kişisel veridir, ancak parmağın

²¹⁸Ayözger Öngün, 2019, s. 35. Şirket maillerinin, KVKK m.5/2-c maddesinde yer alan bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerden olması, diğer bir ifade ile Şirket ile aralarında bulunan sözleşme yükümlülüklerini yerine getirmek için kendilerine atanan şirket e-maili sözleşmenin ifası ile doğrudan doğruya ilişkili olması sebebi ile bu verilerin işlenmesi için çalışanın rızası aranmayacaktır. Ne var ki, bu durum Şirketin çalışanı aydınlatma yükümlülüğünü ortadan kaldırmayacaktır. Ayözger Öngün, 2019, s. 36.

²¹⁹Aksoy, 2010, s.14.

²²⁰Develioğlu, 2017, 37; Kişisel verilere erişim ve bu verilerin düzeltilmesini talep hakkı anayasal bir haktır. Nitekim, Anayasa'nın *Özel hayatın gizliliği* başlıklı m. 23/3 şu şekilde düzenlenmiştir: « Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir ». Bu hususa ilişkin diğer düzenlemeler için bkz. GDPR m.13/2-b ; KVKK m. 11/1-d.

²²¹Selek, 2021, s.7.

²²²Raporda özellikle kişilerin ses ve görüntülerinin kişisel veri kapsamında olmasına vurgu yapılmakta ayrıca bir çocuk tarafından yapılan ve velayet davasında mahkemeye sunulan resim ve çizimlerin de çizen çocuğun psikiyatrik açıdan sağlık durumunu göstermesi sebebi ile kişisel veri olarak kabul edilebileceğinin altını çizmektedir. Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.7-8.

²²³Kişilerin tanımlanması için parmak izleri veya iris taramaları gibi biyometrik verilerin kullanımı, yaşadığımız teknoloji çağında giderek yaygınlaşmaktadır. European Union Agency for Fundamental Rights (FRA), Council of Europe, & European Data Protection Supervisor (EDPS) (2018) . *Handbook on European data protection law* (s. 90) . Luxembourg: Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (Erişim tarihi: 25.03.2025) . Biyometrik verilerin korunması ile ilgili ayrıca bkz. Darendeli, F (2023) . *The protection of biometric data in the era of artificial intelligence technology in EU law*. Yetkin Yayınları. Biyometrik verilere örnekler şu şekilde çoğaltılabilir: retina deseni, yüz yapısı, ses, el geometrisi ve derinlemesine kökleşmiş bazı beceriler veya diğer davranışsal özellikler (el yazısı imza, tuş vuruşları, belirli bir yürüyüş veya konuşma şekli vb.) Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.8-9.

kendisi değildir²²⁴. AB hukuku kapsamında metaveriler de kişisel veri olarak kabul edilmiştir²²⁵.

2.2.2. Kişi

Kişisel veri olarak kabul edilen bilginin, kimliği belirli veya belirlenebilir bir kişiye ilişkin olmasından, bu kavramın ikinci unsuru “kişi”dir.

Kişi denilince aklımıza ilk olarak insan gelmektedir. Fakat kişiler yalnızca insanlardan ibaret değildir. Hukuk dilinde kişi, hak sahibi olabilen ve borç altına girebilen varlıkları ifade etmektedir. Bu cihetle, kişi hak ehliyetine sahip kişidir ve hakkın öznesidir. Kimlerin kişi olarak sayılabileceğini kanun koyucu belirler. Türk Medeni Kanunu, iki tür kişi kabul etmiştir: gerçek ve tüzel kişi²²⁶. Gerçek kişi, kişi kavramında ilk aklımıza gelen yani insandır. Belli bir amacın gerçekleştirilmesi amacıyla bağımsız bir varlık olarak o amaç etrafında toplanan kişi ve mal topluluklarına tüzel kişi denilmektedir. Tüzel kişiler de gerçek kişiler yani insanlar gibi hak sahibi olabilir ve borç altına girebilir²²⁷.

Kişisel verilerin korunması alanındaki ulusal ve uluslararası mevzuatta sadece gerçek kişiler korunma altına alınmıştır. Nitekim, kişisel verilerin korunması kapsamında esas aldığımız GDPR, 95/46/EC AB Yönergesi ve KVKK düzenlemelerinde gerçek kişilerin koruma altında alındığını, tüzel kişilerin açık şekilde kişisel verilerin korunması kapsamı dışında bırakıldığını görmekteyiz²²⁸.

2.2.2.1. Tüzel kişilere ilişkin kişisel veriler

Kişisel verilerin korunmasından tüzel kişilerin de yararlandırılması gerekip gerekmediği konusunda doktrinde bir görüş birliği bulunmamaktadır. Birtakım görüşe göre toplumsal gereklilikler ile ortaya çıkan tüzel kişilerin faaliyetleri esnasında oluşan kişisel verilerinin tıpkı gerçek kişiler gibi korunmaya ihtiyacı bulunmaktadır²²⁹. Ayrıca, tüzel kişilerin

²²⁴ Biyometrik verilere örnekler şu şekilde çoğaltılabilir: retina deseni, yüz yapısı, ses, el geometrisi ve derinlemesine kökleşmiş bazı beceriler veya diğer davranışsal özellikler (el yazısı imza, tuş vuruşları, belirli bir yürüyüş veya konuşma şekli vb.) Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.8-9.

²²⁵ Article 29 Working Party (2014, December 10) . *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, s.5. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf (Erişim tarihi: 18.03.2025) .

²²⁶ Antalya, G., ve Topuz, M (2024) . *Medeni hukuk (Giriş, temel kavramlar, başlangıç hükümleri)* (Cilt 1, Genişletilmiş 5. Baskı) . Seçkin Yayıncılık, s.92-93.

²²⁷ Antalya ve Topuz, 2024, s.92-93; Akıntürk, T., & Ateş, D (2024) . *Medeni hukuk* (28. Baskı) Beta Yayınları, s. 107-110; 180.

²²⁸ 95/46/EC AB Yönergesi, GDPR ve KVKK düzenlemelerinde “kişisel veri” kavramına ilişkin verilen tanımlarda ise açık şekilde “gerçek kişiyi ilişkin her türlü bilgi” ifadesi ile düzenlemelerin kapsamı noktasında tüzel kişilerin dışlandığını anlaşılmaktadır. GDPR, giriş kısmı 14. paragrafında bu husus açık şekilde de ifade edilmiştir: “ (14) Bu Tüzük, tüzel kişinin adı ve türü ile irtibat bilgileri dâhil tüzel kişilere ve özellikle tüzel kişi olarak kurulmuş teşebbüslere ilişkin kişisel verilerin işlenmesini kapsamaz.” European Union Agency for Fundamental Rights (FRA), Council of Europe, & European Data Protection Supervisor (EDPS) (2018) . *Handbook on European data protection law*, Publications Office of the European Union, s. 85., https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (Erişim tarihi: 25.03.2025) . Ayrıca bkz. 95/46/EC AB Yönergesi m.2/1-a, KVKK m. 3/1-d.

²²⁹ Ayözger Öngün, 2019, s.5, s.313; Nitekim kişisel veriler de kişilik hakkının bir parçasını oluşturmaktadır ve tüzel kişilerin de bazı alanlar ile ilgili kişilik hakkına sahip olduğu kabul edilmektedir. Akgül, A (2014) . *Danıştay*

kişilik hakkı²³⁰ çerçevesinde kişisel verilerin korunmasından faydalandırılması gerektiği belirtilmektedir²³¹. 95/46/EC AB Yönergesi, üye ülkelerin kişisel verilerin korunması mevzuatını tüzel kişilerin dahil edilmesine engel bulunmadığını kabul etmektedir²³². Her ne kadar Türk Hukuk sisteminde tüzel kişiler kişisel veri korunması kapsamına dahil edilmemişse de, AYM bir kararında tüzel kişilerin kişisel verilerin korunması kapsamında değerlendirilmesi gerektiği ifade edilmiştir²³³.

Diğer bir görüş, tüzel kişilerin türlerine göre kazanç paylaşma amacı güden ve gütmeyen tüzel kişiler şeklinde bir ayrıma gidilmesi gerekmektedir. Buna göre, kazanç paylaşma amacı güden tüzel kişilerin(örneğin, ticari şirketler) verileri ticari gizliliğin korunması kapsamında değerlendirilmeliyken; kazanç paylaşma amacı gütmeyen tüzel kişilerin(örneğin, dernek, vakıf ve siyasi partiler) verilerinin TMK²³⁴ m. 48 hükmü kapsamında kişilik hakkının genel korunması kapsamında kişisel verilerin korunmasından yararlanması gerektiğini savunmaktadır²³⁵.

Son görüşe göre ise bireyler yanında devletler, şirketler ve başkaca gruplar da veri öznesi olabilmektedir fakat başka birtakım hukuki düzenlemeler kapsamında korunmaları (devlete ait veriler “Devlet Sırrı“, ticari şirketler ilişkin verileri “ticari sır“ kapsamında korunur), kişisel verilerin esas olarak temel insan hakkı olması, insan kişiliğini ve özel alanını koruması sebepleri ile tüzel kişiler kişisel verilerin korunması kapsamı dışında bırakılmalıdır²³⁶.

ve Avrupa İnsan Hakları Mahkemesi kararları ışığında kişisel verilerin korunması (s. 15) . Beta Yayınları, s.15; Şen, E (2009) . Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri çerçevesinde değerlendirilmesi. *İstanbul Barosu Dergisi*, 83 (3), s.1201-1202.

²³⁰Bkz. 2.3. Kişisel Veri Kavramının Hukuki Niteliği Başlığı.

²³¹Selek, 2021, s.9 ; Ayözger Öngün, 2019, s.5, s.313. Tüzel kişilerin de verilerinin işlenmesi ile mağdur edilebileceğini, örneğin aynı sektördeki şirketlerin sınıflandırılması ile profillemeye yapılmasının, iletişim bilgilerinin ve verilerinin bedel karşılığı veya olmadan paylaşılmasının kişilik hakkına yönelik bir saldırı olarak kabul edilmesi ve tüzel kişilerin kişisel verilerin korunması kapsamında olması gerektiği yönündeki görüş için bkz. Gönen, D (2011) . *Tüzel kişilerde kişilik hakkı ve korunması*,. XII Levha Yayıncılık, s.99-100.

²³² 95/46/EC AB Yönergesi, Giriş, 24. Paragraf.

²³³ AYM kararında: ” (...) Esasen her ne kadar 95/46/EC sayılı Avrupa Veri Koruma Direktifinde yer alan tanım, tüzel kişilere ilişkin verileri dışlamakta ve kişisel veriler kapsamına yalnızca gerçek kişilere ilişkin bilgilerin gireceğini kabul etmekte ise de, gerek elektronik haberleşme sektöründe kişisel bilgilerin işlenmesi ve gizliliğin korunması hakkında 12.07.2002 gün ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifinde, yalnızca haberleşme sektörüne ilişkin olarak, hem gerçek kişilerin hem de tüzel kişilerin veri sahibi kabul edileceğinin ifade edilmesi; gerekse son yıllarda kabul edilen bazı ülke kanunlarında tüzel kişilerin de kişisel verilerinin koruma alanına dahil edilmesi bir bütün olarak dikkate alındığında, Avrupa ve Dünyadaki gelişimin kişisel verilerin korunmasında tüzel kişilerin de kapsamında yer alması gerektiği yönünde olduğu görülmektedir (...) ” Anayasa Mahkemesi (AYM) (2015) . E. 2013/84, K. 2014/183, Karar Tarihi: 13.03.2015. Resmî Gazete, 13.03.2015, Sayı: 29294. <https://www.resmigazete.gov.tr/eskiler/2015/03/20150313-12.pdf> . Bununla birlikte şu hususun belirtilmesinde fayda görmekteyiz. 2008 yılında TBMM’ye sunulan Kişisel Verilerin Korunması Kanunu Tasarı’sında, “tüzel kişilere ilişkin tüm bilgiler“ kişisel verilerin korunması kapsamına alınmıştı. 24/03/2016 tarihinde kabul edilen KVKK m.3/1-ç’de ise “İlgili kişi”, kişisel verisi işlenen “gerçek kişi“ olarak tanımlanmış ve tüzel kişi tanımdan dışlanmış. Kişisel verilerin korunması kanun tasarısının söz konusu AYM kararını etkisi düşündürücüdür.

²³⁴4721 sayılı Türk Medeni Kanunu (Kabul Tarihi: 22.11.2001, RG. Tarihi: 08.12.2001, RG Sayısı: 24607) .

²³⁵ Taştan, 2017, s.30.

²³⁶ Kişisel verilerin korunması hakkı, temelde özel yaşamın gizliliği hakkından doğmuştur. Bu hak gerçek kişilere özgü bir hak türüdür. Develioğlu, 2017, s.30 ; Küzeci, 2010, s.5-6; Şimşek, O (2008) . *Anayasa hukukunda kişisel verilerin korunması*. Beta Yayıncılık, s. 123; Dolayısıyla kişisel veri kavramı esasen özü itibari ile gerçek kişilere özgü bir kavram olması yanında tüzel kişiler için bu bağlamda ticari sır kavramından bahsedilebilecektir. Ayözger Öngün, 2019, s.5,10. ŞEN ise bu konu hakkında Ticarî Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu ile kişisel verilerin korunması ihlallerine ilişkin düzenlenen suçların korunan hukuki menfaatlerinin farklı olduğunu; ilk suç için ekonomi, sanayi ve ticarete dair hukuki menfaat korunurken;

Bizim de görüşümüz bu doğrultudadır. Nitekim halihazırda tüzel kişiler ve tacirler için mahremiyetten çok “*aleniyet prensibini*” benimsenmektedir ve bu kapsamda tüzel kişilerin neredeyse tüm bilgilerinin kamuya açık olması gereklidir^{237 238}. Diğer yandan “ticari sır” olarak kabul edilen bilgiler için halihazırda bankacılığa, rekabete ilişkin özel hukuki düzenlemeler²³⁹ mevcuttur ve uygulamada şirketler arası gizlilik sözleşmeleri yapılmaktadır. Tüm bu haller karşısında tüzel kişilerin kişisel verilerinin sektörel bazda korunmasında hukuki menfaatleri bulunmamaktadır²⁴⁰. Bu durum, gereklilik dolayısıyla tüzel kişilerin kişisel verilerin korunması hakkında yararlandırılması halini yasaklamaz²⁴¹.

Doktrinde bazı Avrupa ülkelerinde tüzel kişilerin kişisel verilerinin korunmasına ilişkin kanuni düzenlemeler mevcut olduğu belirtilmekteyse de; yaptığımız araştırma sonucunda örnek gösterilen ülke düzenlemlerinde her ne kadar ilk başta kişisel verilerin korunması kapsamına tüzel kişiler de dahil edilmişse de güncel değişikliklerle kapsamın yalnızca “gerçek kişileri” içerecek şekilde daraltıldığı görülmüştür²⁴². Dolayısıyla, genel olarak, ulusal ve uluslararası

kişisel verilerin korunmasında özel hayatın giz alanının korunduğunu ve tüzel kişilerin, gerçek kişiler kadar olmasa da özel hayat kapsamında verilerinin (ticari veri) olduğu görüşündedir. Şen, 2009, s.1202.

²³⁷6102 Sayılı Türk Ticaret Kanunu (TTK) (Resmî Gazete, 14.02.2011, Sayı: 27846) m.35/2 gereği, ticari işletmelerin ve şirketlerin yerleşim yeri bilgisi ve diğer bilgileri ile birlikte kayıt olma yükümlülüklerinin bulunduğu “ticaret sicili” alenidir. Bu nedenle herkes (ilgili sıfatı aranmaksızın), ticaret sicilinin içeriğini ve sicilde saklanan bütün senet ve belgeleri inceleyebilir, bunlardan onaylı suret alabilir ve bir hususun sicilde kayıtlı olup olmadığına ilişkin onaylı belge verilmesini isteyebilir. Ticaret siciline, ticari işletmenin adı ve ticaret unvanı, işletme merkezinin ve şubelerinin bulunduğu yer (TTK m.40) 1163 Sayılı Kooperatifler Kanunu (Resmî Gazete, 10.05.1969, Sayı: 13195) m.3 uyarınca kooperatif merkezinin bulunduğu yer, ticari mektuplarda ve ticari defterlere yapılan kayıtların dayandığı belgelerde tacirin sicil numarası, ticaret unvanı, işletmesinin merkezi ile tacir internet sitesi gösterilir (TTK m. 39). Vakıfların yerleşim yerleri ile birlikte Resmi Gazete’de ilan edilmeleri ile derneklerin sicile kaydedilmesi zorunludur. Kamu tüzel kişilerinde ise görev ve yetkilerinin mevzuat ile belirlenmesi ile görevlerini yürütecekleri adreslerin ve diğer bilgilerinin kamuya açık olması gerekliliği bulunmaktadır.

²³⁸Ticaret sicilinin kişisel veriler kapsamında değerlendirilmesi için bkz. Korkmaz, A (2024) . Ticaret sicili kapsamındaki faaliyetlerin kişisel verileri koruma hukuku çerçevesinde değerlendirilmesi. *Ticaret ve Fikri Mülkiyet Hukuku Dergisi*, (10), 297–316.

²³⁹4982 Sayılı Bilgi Edinme Hakkı Kanunu (Resmî Gazete, 24.10.2003, Sayı: 25269) kapsamında bilgi edinme hakkına getirilen istisnalar özel hayatın gizliliği ile ilişkili olarak madde 21’de ticari sırlara ilişkin bilgi ve belgelere ilişkin istisnalar madde 23’de ayrı ayrı olarak düzenlenmiştir. *T.C. Anayasası* (1982) (Resmî Gazete, 09.11.1982, Sayı: 17863) m. 20’de “Özel Hayatın Gizliliği” başlığı altında düzenlenen “Kişisel Verilerin Korunması” bilgi edinme hakkı çerçevesinde özel hayatın gizliliği başlığı altındaki istisnalara tabii olacaktır. Buradan, ticari hayattaki tüzel kişilerin kişisel verilerin korunması dışında korunduğu görülecektir.

²⁴⁰Aynı yönde bkz. Aşıkoğlu, İ. Ş (2018) . *Avrupa Birliği ve Türk hukukunda kişisel verilerin korunması ve büyük veri*, Onikilevha Yayınları, s.16-17.

²⁴¹Ayözger Öngün, 2019, s.10.

²⁴²Örneğin, İsviçre Veri Koruma Kanunu, kişisel verilerin korunması kapsamına tüzel kişileri de dahil etmekteyken 1 Eylül 2023 tarihinden sonra kanundan tüzel kişi ibaresini çıkartarak sadece “gerçek kişileri” koruma kapsamına dahil etmiştir. Kanun değişikliği ve eski kanun karşılaştırması için bkz. Federal Department of Justice and Police (2023) . *New Federal Act on Data Protection (nFADP)* . <https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html> Erişim Tarihi: 21.02.2025. İsviçre Veri Koruma Kanunu İngilizce metni için bkz. The Swiss Confederation (2023) . *Federal Act on Data Protection (FADP)*, RS 235.1. <https://www.fedlex.admin.ch/eli/cc/2022/491/en> Erişim Tarihi: 21.02.2025. Benzer şekilde, Türkiye’de 2008 tarihli Kişisel Verilerin Korunması Kanunu Tasarısı m. 2’de kişisel verilerin korunması kapsamı tüzel kişileri de kapsama dahil ederken kanunlaşma ile tüzel kişiler kapsamdan çıkarılmıştır. Nitekim, KVKK yalnızca gerçek kişilerin kişisel verilerinin Kanun kapsamında korumaktadır (m.2) . Avrupa dışında yer alan Avusturya hukuk sisteminde de veriler, kişisel verilerin korunmasından ancak gerçek kişilere ait olduğu müddetçe faydalanabileceği düzenlenmiştir. Bkz. Australian Government (1988) . *Privacy Act 1988*, article 6. <https://www.legislation.gov.au/C2004A03712/latest/text> Erişim Tarihi: 29.04.2025. Benzer şekilde Türk

hukukun yaklaşımı, tüzel kişilerin kişisel verilerin korunması kapsamı dışında bırakılması yönünde olduğu çıkarımı yapılabilir. Bu durum yukarıda belirttiğimiz üzere elbette gereksinim duyulan hallerde istisnai düzenlemeler yapılmasına engel teşkil etmeyecektir. Nitekim, Avrupa Birliği'nin 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi²⁴³, sektörün kendine özgü şartları sebebi ile kişisel verilerin korunması kapsamında, tüzel kişilerin de dahil edildiği görülecektir²⁴⁴. Benzer şekilde, Türk hukukunda Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik (EHSKVİY)²⁴⁵ kullanıcı ve abone sıfatlarını haiz olan tüzel kişi, kişisel verilerin korunmasından faydalandırmıştır.

Bahsedilmesi gereken önemli bir konu, tüzel kişilere ilişkin verilerin gerçek kişiye ilişkin veriler içermesi halidir. Örneğin limited şirket verilerinde ortaklara veya müdürlere ilişkin verilere ulaşılması durumunda tüzel kişiye ait veri gerçek kişiye ilişkin verileri içermekte ve gerçek kişiyi belirli veya belirlenebiliyor kılmaktadır. Bu durumda kişisel verilerin korunması devreye girmelidir²⁴⁶.

2.2.2.2. *Cenine ilişkin kişisel veriler*

Kişi unsuruna ilişkin değinilmesi gereken bir diğer husus, henüz tam ve sağ doğumu gerçekleşmemiş yani hukuk nazarında kişiliği oluşmamış²⁴⁷ anne karnındaki çocukların ("ceninin") kişisel verilerinin korunması meselesidir²⁴⁸. AB'nin kişisel verilerin korunmasına ilişkin düzenlemelerinde cenine dair bir koruması mevcut değildir. Article 29 Working Party, AB üye devletlere, kişisel veri koruma kurallarının amacının bireyi korumak olmasını temel alarak iç hukuklarında bu konu hakkında düzenleme yapabileceklerini belirtmiştir. Bununla birlikte doğmamış çocukların durumunun hamilelik dönemiyle sınırlı olmadığı, dondurulmuş embriyolarda örneğinde olduğu gibi aslında çok daha uzun süreyi kapsadığına dikkat çekmiştir²⁴⁹. Avrupa Konseyi'nin, Rec 97/5 sayılı Tıp Verilerinin Korunmasına İlişkin Tavsiye

hukukunda, KVKK tasarısında da kişisel verilerin korunması gerçek ve tüzel kişileri kapsayacak şekilde oluşturulmuş olsa da; kanunlaşma aşamasında tüzel kişiler korumanın kapsamı dışında bırakılmıştır.

²⁴³ Council of the European Union (2002) . *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* . Official Journal of the European Communities. <https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng> Erişim Tarihi: 18.04.2025.

²⁴⁴Fakat söz konusu Direktifin 12. Paragrafında bu istisnai korumanın ancak "kamuya açık bir elektronik haberleşme hizmetine abone olan" tüzel kişiler için öngörüldüğü ve Direktifin üye devletlere iç hukuklarında, tüzel kişilerin meşru menfaatlerinin korunmasına ilişkin genişletme yükümlülüğü getirmediği özel olarak ifade edilmiştir.

²⁴⁵*Resmî Gazete*, 04.12.2020, Sayı: 31324.

²⁴⁶ Şimşek, 2008. 123; Faal bir şirketin yetkilisi ya da pay sahibi olarak gözüken gerçek kişinin şirket ile ilişkisi sona ermiş ya da şirketin faaliyetinin sona ermiş olması hallerinde ticaret sicilindeki verilerinin, KVKK kapsamında bir ihlal teşkil edip etmediği hususu için ayrıca bkz. Balkan, N (2024) . Kişisel veri koruma hukuku ile ticaret sicilinin aleniyet fonksiyonu arasındaki menfaat dengesi. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, (28), 207–240.

²⁴⁷4721 Sayılı *Türk Medeni Kanunu (TMK)* (Resmî Gazete, 08.12.2001, Sayı: 24607)madde 28- Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer.

Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder.

²⁴⁸ Kişiliğin başlangıcı öncesinde ceninle ilgili veriler, ana rahmindeki ultrason görüntüleri olabileceği gibi; henüz ana rahminde bile olmayan in vitro (tüpteki) embriyolara uygulanan testler sonucu elde edilen genetik veriler de olabilir. Doğmamış çocuklar adına açılan sosyal medya hesapları, dijital üyelikler, alan adları doğmamış çocuğa ilişkin verilerden birkaçıdır.

²⁴⁹Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.23.

Kararında²⁵⁰ doğmamış çocuklarla ilgili tıbbi verilerin kişisel veri olarak kabul edilmesi ve böylece kişisel veri korumasından yararlandırılması gerektiğini ayrıca bu halde ebeveynlerin doğmamış çocuk adına hareket etme yasal yetkisine sahip olması gerektiğini belirtmiştir. Diğer yandan, aynı zamanda annenin kimliğini belirleyen veriler olması sebebi ile cenine ait veriler, ceninin anne karnında bulunması şartı ile hem cenin hem de anne açısından kişisel verilerin koruması altındadır²⁵¹.

Türk hukuku bakımından ise tam ve sağ doğması ile hukuken gerçek kişi sıfatını alan tarafın, ceninken kendisi hakkında toplanan ve hukuka aykırı olarak işlenen kişisel verilerine dair kişisel veri korunmasından faydalanması önünde bir engel bulunmamaktadır. Bu kapsamda, doğum ile birlikte kişilik kazanan kişiler hakkında doğum öncesinde edinilen bir bilgi, kişiliğin başlamasındaki sonraki dönemde kişiyi belirli veya belirlenebilir kılıyor ise, kişisel verilere ilişkin koruma kapsamında yer alır. *Örneğin, tüpte oluşturulan bir embriyo üzerinde, ebeveynlerin rızası dışında, yapılan genetik testlerden elde edilen bulgular çocuğun tam ve sağ doğumu ile kişisel veri hakkının ihlalini oluşturur*²⁵².

2.2.2.3. Ölüye ilişkin kişisel veriler

Kişinin ölmüş olmasının kişisel verilerin korumasını ortadan kaldırıp kaldırmayacağı hususu bir diğer tartışma konusunu oluşturmaktadır. Bu konuda genel kanı, kişisel verilerin ilke olarak kimliği belirli veya belirlenebilir yaşayan bireylere ilişkin veriler olduğu ve ölü bireylere ilişkin bilgilerin, ölümlerin artık medeni hukuk kapsamında artık bir kişiliği olmadığından hareketle²⁵³, kişisel veri koruması kapsamında olmadığı yönündedir²⁵⁴. GDPR konu hakkında ölen kişilerin Tüzük kapsamında olmadığı fakat bu durumun üye devletlerin kendi iç hukuklarında koruyucu tedbirler almasına yönelik bir engel teşkil etmediğini belirtmektedir²⁵⁵. Bu doğrultuda, Danimarka²⁵⁶ ve Estonya²⁵⁷ gibi ülkeler iç hukuklarında ölen bireylerin kişisel verilerini koruma altına alınırken, örneğin Almanya Veri Koruma Kanunu²⁵⁸,’nda bu hususa yer verilmemiştir. Ayrıca İngiltere’nin Veri Koruma Kanunu’nun kişisel verinin tanımı yapılırken,

²⁵⁰Council of Europe (1997) . *Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data*. <https://rm.coe.int/16806af967> Erişim Tarihi: 22.02.2025.

²⁵¹ bkz. Rogers, A (1997) . European data protection to give unborn children rights? *The Lancet*, 349 (9045), s.550. [https://doi.org/10.1016/S0140-6736\(97\)80110-9](https://doi.org/10.1016/S0140-6736(97)80110-9).

²⁵²Badur, E (2023) . Kişisel verilerin kişiliğin başlangıcı ve sonu ötesinde korunması. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 27 (3), s. 14-15. Fakat, cenin ultrason fotoğrafı, kişilik hakkı kapsamında değerlendirilmez. Nitekim, burada ultrason fotoğrafı tam ve sağ doğan kişiyi belirli veya belirlenebilir kılammamaktadır. Bu veri anneyi belirli veya belirlenebilir kıldığı ölçüde, annenin kişisel verisidir. Badur, 2023, s.15.

²⁵³ Ölümle kişilik sona erer (TMK m. 28) Dolayısıyla kişiliğe bağlı haklar ölüm ile birlikte ortandan kalkar. Benzer şekilde ölüm karanesinde ve gaiplik kararında da kişilik sona ermekte ve gaiplik kararı geçmişe etkili olarak sonuç doğurmaktadır. Ölenin şeref ve haysiyetinin korunması bağlamında istisnai olarak korumalar bulunmaktadır. Örneğin: cesede saldırıda bulunulması. Arat, A (2014) . Gerçek kişilerde kişiliğin sona ermesi. *Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi*, 9, s. 263, 272-273; Badur, 2023, s.7.

²⁵⁴Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.22; Develioğlu, 2017, s.31.

²⁵⁵ GDPR, Giriş, başlangıç, 27. Ayrıca başlangıç Kısımının 158 ve 160. paragraflarında da ölen kişilerin verileri hakkında Tüzüğün uygulanmasının mümkün olmadığı belirtilmiştir.

²⁵⁶ Danimarka Kişisel Veri Kanunu İngilizce tam metni için bkz. Danish Data Protection Agency. *Danish Data Protection Act*. <https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf> (Erişim tarihi: 23.02.2025)

²⁵⁷ Estonya Kişisel Veri Kanunu İngilizce tam metni için bkz. Estonian Ministry of Justice. *Personal Data Protection Act*. <https://www.riigiteataja.ee/en/eli/523012019001/consolide> (Erişim tarihi: 23.02.2025) .

²⁵⁸ Almanya Kişisel Veri Kanunu İngilizce tam metni için bkz. Federal Ministry of Justice and Consumer Protection. *Federal Data Protection Act (BDSG)* . https://www.gesetze-im-internet.de/englisch_bdsch/englisch_bdsch.html#p0014 (Erişim tarihi: 23.02.2025) .

“yaşayan (*living*)” denilmek sureti ile ölen bireylerin kişisel veri koruması altında olmadığı vurgulanmıştır²⁵⁹. Türk-İsviçre hukukunda kural olarak, ölen kişilerin kişisel verilerinin korunması mümkün değildir²⁶⁰.

Ölü bireylerin kişisel verilerinin de koruma altında olduğu bazı durumlar olabilir. Nitekim, veri sorumlusunun verisini işlediği kişinin sağ veya ölü olmasının bilemeyebilir ve bilse dahi hukuktan doğan yükümlülüklerini ayırım yapmaksızın bu veriler için de uygulayabilir. Burada ölü kişinin verileri sağ gerçek kişiler gibi veri sorumlusunca korunmaktadır. Diğer bir durum, ölü kişiye ilişkin bilgilerin sağ gerçek kişilere ilişkin bazı bilgilere işaret etmesi halidir. Kural olarak, ölüm halinde kişiye bağlı haklar sona da sona ereceği için, ölen kişinin mirasçıları ölü adına kişisel verilerin korunması ile ilgili haklardan yararlanamayacaktır²⁶¹. Fakat ölünün verilerinin mirasçılarının kişilik haklarına hanelerinde örneğin, ölüye ait genetik hastalık bilgilere ilişkin mirasçıları hak iddiasında bulunabilir. Ölünün hastalığına ilişkin verilerin sağ çocuklarına ilişkin bir hastalığı (kişisel veriyi) işaret etmesinde bu kişisel veriler hukuken koruma altındadır²⁶².

Türk hukuku bakımından, KVKK’da konuya ilişkin bir hüküm bulunmamakla birlikte, genel kanı ölen kişinin kişisel verilerinin koruma altında olmadığı yönündedir²⁶³. Bu noktada ölü bireylerin kişisel verilerinin korunmasının (sağlık verileri dışında kalan²⁶⁴) ancak yakınlarının kişilik hakkının korunmasının çerçevesinde mümkün olabilecektir²⁶⁵. Diğer yandan, kişisel veri koruma mevzuatı dışındaki kurallar tarafından sağlanan özel korumalar vasıtası ile ölü kişinin kişisel verileri korunabilir. Örneğin, ölüm halinde sağlık personelinin sır

²⁵⁹ İngiltere Kişisel Veri Kanunu İngilizce tam metni için bkz. UK Government (2018) . *Data Protection Act 2018*. <https://www.legislation.gov.uk/ukpga/2018/12/enacted> (Erişim tarihi: 23.02.2025) . Birleşik Krallık’ta kişisel veri koruma kuralları yalnızca tanımlanabilir yaşayan bir bireyle ilgili bilgiler için geçerlidir. Vefat etmiş bir kişiye ilişkin bilgiler kişisel veri teşkil etmez. Bkz. bkz. Information Commissioner's Office. *Personal information: what is personal data?* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/#pd6> (Erişim tarihi: 06.05.2025) .

²⁶⁰Taşan, 2017, s.32.

²⁶¹Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.22; Selek, 2021, s.10; Develioğlu, 2017, s.32.

²⁶² Örneğin, hemofili, X kromozom ile taşınan bir genetik hastalık olması sebebi ile, ölen kişinin hemofili hastası olduğu bilgisi, kişinin oğlunun da bu hastalığı taşıdığı bilgisini vermektedir. Bu durumda sağ kişiye ilişkin kişisel veriler açığa çıktığı için bu kişisel korunmalıdır. Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.22.

²⁶³Kişisel Verileri Koruma Kurumu 18.09.2019 tarihli ve 2019/273 sayılı Kararında ölen eşinin verilerini talep eden eşin talebi “talep edilen kişisel verilerin talep eden gerçek kişiye ilişkin olmaması ve ölmüş kişiye ait olması sebebiyle” reddedilmiştir. Kişisel Verileri Koruma Kurumu (2019) . *Karar No: 2019/273 - Talep edilen kişisel verilerin ölmüş kişiye ait olması sebebiyle reddi*. <https://www.kvkk.gov.tr/lcerik/6710/2019-273> (Erişim tarihi: 22.02.2025) .

²⁶⁴ Nitekim, Kişisel Sağlık Verileri Hakkında Yönetmeliğinin (RG. 21.06.2019 T. ve 30808 S.) 11. maddesinde: “Ölünün Sağlık Verilerine Erişim” başlığı altında; “Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle mirasın yasal mirasçıları münferit olarak yetkilidir. Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır.” hükmü düzenlenmiştir.

²⁶⁵Badur, 2023, s.27; Uçak, M (2021) . Kişisel verilerin ölümden sonra korunması. *İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi*, 6 (10), s. 105-106.

saklama yükümlülüğünün devam etmesi böyledir^{266 267}. Son olarak, kişisel veri korumasından cinsiyet, yaş, vatandaşlık ayırt etmeksizin herkesin yararlanabileceğinin altını çizmek gerekir²⁶⁸.

2.2.3. Belirli veya belirlenebilir olma

Kişisel veri tanımında gerçek kişinin, belirli veya belirlenebilir (*identified or identifiable natural person*) olması koşulu bulunmaktadır. Bu sebeple kişisel veri kavramının üçüncü unsuru “belirli veya belirlenebilir olma”dır.

Kişinin belirli olması doğrudan doğruya ayırt edilebilmesi anlamına gelmektedir. Örneğin, kişinin kimlik numarası ile kişi doğrudan doğruya başka bir araca ihtiyaç duyulmaksızın ulaşılması hali belirli olma halidir. Belirlenebilir olma ise henüz tespit edilmemiş kişinin yardımcı vasıtalar ile ayırt edilmesinin mümkün olmasını ifade etmektedir²⁶⁹. 95/46/EC sayılı Direktif ile GDPR düzenlemesinde belirlenebilir kişinin, tanımlayıcılar²⁷⁰ (“*identifier*”) vasıtası ile doğrudan veya dolaylı olarak tanımlanabilen gerçek kişi olduğu belirtilmiştir (95/46/EC sayılı direktif m.2/1-a; GDPR m.4/1) ²⁷¹. Gerçek kişiyi, belirlemeye yarayan tanımlayıcılara (“*identifier*”) örnek olarak isim, kimlik numarası, çevrimiçi tanımlayıcılar ya da fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü veriler örnek verilebilir (95/46/EC sayılı direktif m.2/1-a; GDPR m.4/1). Bu bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilmek özellikleri nedeniyle kişisel veridir²⁷². Bu bilgilerin kullanılması ile somut olayın koşullarında kişi “belirli” hale gelecektir²⁷³.

²⁶⁶Hekimlerin sır saklama yükümlülüğü, *Tıbbi Deontoloji Nizamnamesi'nin* 4. maddesi (Tıbbi Deontoloji Nizamnamesi, 1960), *Türk Tabipler Birliği Hekimlik Meslek Etiği Kuralları'nın* 9. maddesi (Türk Tabipler Birliği, 1998) ve 01.08.1998 tarihli, 23420 sayılı Resmî Gazete’de yayımlanan *Hasta Hakları Yönetmeliği'nin* “Mahremiyete Saygı Gösterilmesi” başlıklı 21. maddesinde düzenlenmiştir (Hasta Hakları Yönetmeliği, 1998). Nitekim söz konusu Yönetmeliğin 21. maddesi şu şekildedir:

“Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir. Mahremiyete saygı gösterilmesi ve bunu istemek hakkı;

a) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini,
b) Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini,
c) Tıbben sakınca olmayan hallerde yanında bir yakınının bulunmasına izin verilmesini,
d) Tedavisi ile doğrudan ilgili olmayan kimselerin, tıbbi müdahale sırasında bulunmamasını,
e) Hastalığın mahiyeti gerektirmedikçe hastanın şahsı ve ailevi hayatına müdahale edilmemesini,
f) Sağlık harcamalarının kaynağının gizli tutulmasını, kapsar.

Ölüm olayı, mahremiyetin bozulması hakkını vermez.

²⁶⁷Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.22.

²⁶⁸ Develioğlu, 2017, s.32.

²⁶⁹ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.12.

²⁷⁰95/46/EC sayılı Direktif’te tanımlayıcı (“*identifier*”) yerine atıf ifadesi kullanılmış GDPR düzenlemesinde ise atfın da bir tanımlayıcı olduğu ifade edilmiştir. 95/46/EC sayılı direktif m.2/1-a; GDPR m.4/1). 95/46/EC sayılı Direktif’i esas alan KVKK düzenlemesinde ise tanımlayıcı ifadesine yer verilmemiş; kişisel veri tanımında yer verilen belirlenebilir kişi olma kistası Kanun Gereğesinde 3. madde başlığı altında açıklanmıştır.

²⁷¹Yani, bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade etmektedir. KVKK m.3 Gereğesi.

²⁷²KVKK m.3 Gereğesi.

²⁷³ Aksoy, 2010, s.23.

Kişinin belirlenebilir olmasından kastedilen, işlenen veriler ile basit bir bağlantı ile ilgili kişinin (veri öznesinin) kimliğini ortaya çıkarılmalıdır²⁷⁴. Belirli kişi, bir grup içerisinde ek bir bilgiye ihtiyaç duyulmadan doğrudan ayırt edilebilen kişi iken; belirlenebilir kişi henüz tanımlanmamış fakat ek bilgi veya bilgilerle (*tanımlayıcılarla*) tanımlanması mümkün olan kişidir²⁷⁵. Bir kişinin isminin en önemli tanımlayıcı olduğu söylenebilir. Fakat bazı durumlarda sadece isim tanımlanabilir olmak için yeterli değildir²⁷⁶. Örneğin, bir futbol takımında birden fazla aynı isme sahip olan oyuncunun olması halinde bu isim kişiyi belirlenebilir hale getirmezken; tek kişinin bu isme sahip olması halinde soyismi olmadan yalnızca isim kişiyi belirlenebilir kılmaktadır²⁷⁷. Bu bakımdan, bilginin ilgili olduğu kişinin kimliğinin tespit edip etmemesi hususu durumun özellik ve şartlarına bağlıdır²⁷⁸. Kişinin ait olduğu grup alanı daraltıldıkça tanımlayıcının gerçek kişiyi işaret etmesindeki işlevi artacaktır²⁷⁹.

Birey maddi ilişkileri içerisinde de belirlenebilir olabilir. Kişiyi belirlenebilir kılan adres, fotoğraf, gerçek kişinin saç rengi, göz rengi gibi fiziksel özellikler²⁸⁰, pasaport numarası, vergi borcu²⁸¹, hastalık, IP adresi²⁸², ses kaydı gibi bilgiler kişisel veri olarak değerlendirilir²⁸³. Barınma kurumunda gerçek isimlerini gizleyen sığınmacılara bir idari amaçlarla kod numarası verilmesi ve bu kod numarasına kişiye ilişkin bilgilerin yüklenmesinde, söz konusu idari kod kişinin diğer sığınmacılardan ayırt edilmesine ve ona atfedilen farklı bilgi parçalarını içermesi sebebi ile kişisel veri ve somut olayda idari kod atanan sığınmacı "tanımlanabilir" kişidir²⁸⁴.

²⁷⁴Şimşek, 2008, s. 121-122. Gerçek kişiler, kullandıkları cihaz, uygulama, araç ve protokollerin, internet protokolü adresleri, çerez tanımlayıcıları veya radyo frekansı ile tanımlama etiketleri gibi diğer tanımlayıcılar şeklinde sağlamış olduğu çevrim içi tanımlayıcılarla ilişkilendirilebilir. Bu; tanımlayıcılar, özellikle sunuculardan edinilen emsalsiz tanımlayıcılar ve diğer bilgiler ile birleştirildiğinde, gerçek kişilerin profillerini oluşturmak ve onları tanımlamak için kullanılacak izler bırakabilir (GDPR, *giriş*, para. 30) .

²⁷⁵Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.12. Bu ek bilgi, halihazırda elinizde bulunan bir bilgi olabileceği gibi, başka bir kaynaktan edinmeniz gereken bir bilgi de olabilir. ICO, Information Commissioner's Officer bkz. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-information-a-guide/> .Erişim Tarihi: 16.05.2025.

²⁷⁶ Develioğlu, 2017, s.33.

²⁷⁷ Selek, 2021, s.12.

²⁷⁸Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.13. Aynı şekilde mavi ceket giyen kadın bilgisinde mevcut koşullarda örneğe uygun tek bireyin olması durumunda kişi doğrudan tanımlanabilir olacaktır. Resmi üniformanın mavi ceket olduğu bir okulda ise bu bilgi kişiyi belirlemeye tek başına yeterli değildir. Ancak başka bir ve birkaç tanımlayıcı bilginin eklenmesi ile kişi tanımlanabilir hale gelecektir.

²⁷⁹ Develioğlu, 2017, s.33.

²⁸⁰Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.12.

²⁸¹Avrupa İnsan Hakları Mahkemesi (AİHM) (2023, 9 Mart) . *L.B. v. Hungary (Grand Chamber)*, Başvuru No: 36345/16. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-222437%22%7D> (Erişim Tarihi: 21.02.2025) .

²⁸² IP adreslerinin kişisel veri sayılmasına ilişkin değerlendirme için bkz. Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.16-17.

²⁸³ KVKK madde 3 gerekçesinde: "Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilecek özellikleri nedeniyle kişisel verilerdir."

²⁸⁴Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.14. Aynı şekilde istatistik enstitüleri tarafından işlenen kişisel bilgilere bir anahtar kod atanır ve burada bilgiler toplanır (örn. X1234 kodlu haftada 3 kereden fazla bir kadeh şarap içiyor) . Bu anahtar kodun "makul olarak kullanılması muhtemel" olması ve tüketicilerin "makul olarak mümkün olabilecek tüm araçlar dikkate alınarak" belirlenebilir olması sebepleri ile kişinin bilgi seti kişisel veri kapsamındadır. Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.18-19.

Eşyaya ilişkin veriler örneğin maliki olunan bir araca ilişkin plaka bilgisi vasıtası ile basit bir bağlantı kurularak gerçek kişinin belirlenmesi mümkün olduğundan araç plakası kişisel veri olarak kabul edilir²⁸⁵.

Bir verinin, “*tanımlanabilir kişi*”den bahsedilebilmesi ve kişisel veri olarak kabul edilebilmesi için “*makul olarak kullanılması muhtemel tüm araçların kullanılması*” kriteri bulunmaktadır. Buna göre verisi işlenen bireyi tespit etmek için herhangi bir diğer kişi tarafından kullanılabilecek makul tüm araçlarla elde edilen ek bilgiler kullanarak kişi belirlenebiliyorsa “*kişisel veri*” ve “*tanımlanabilir kişiden*” bahsedilebilir²⁸⁶. Aksi halde, veri, kişisel veri korumasından faydalanamaz. Araçların kullanılmasının makul ve muhtemel olmasında, işleme sırasında mevcut olan teknoloji ve teknolojik gelişmeler göz önünde bulundurulmalıdır²⁸⁷. Ayrıca araştırmayı yapacak olan kişinin konumu da önemlidir. Bu durum kişisel verilerin göre bir kavram olup olmadığı hususunda tartışılmaktadır. Nitekim, aynı veri bir gazeteci için araştırma yöntem ve teknikler uygulanarak ilgili kişiye ulaşmayı mümkün kılarken bu yöntemleri bilmeyen ve basın kartı ile ayrıcalığı olmayan bir vatandaş için ilgili kişiye ulaşmak güç olabilir. İlgili kişi ile veri arasında bağlantıyı kurulamayan durumda veri, kişisel veri olarak kabul edilmeyecektir²⁸⁸.

Günümüzde algoritmalar, kişinin adını dahi bilmeye ihtiyaç duymadan kullanıcı davranışlarını tanımlamakta, bunları biraraya getirerek kişinin davranış desenini belirleyebilmektedir. Böylece kişinin sosyo-ekonomik ve kültürel düzeyini belirleyebilmekte ve psikolojik durumunu belirleyebilmektedir. Dolayısıyla, bir kişinin kimliğini ve kişiliğinin belirlenmesi artık günümüzde bireyin adını bilmeden dahi yapılabilmektedir²⁸⁹. Bugünkü teknoloji araçları ile belirlenemeyen kişiler teknolojinin gelişimi ile birlikte belirlenebilir hale gelebilir. Bu bakımdan söylenebilir ki, bugün kişisel veri olarak kabul edilmeyen veriler teknolojinin gelişimi ile birlikte kişisel veri olarak kabul edilebilir²⁹⁰.

²⁸⁵ Şimşek, 2008, s. 121-122.

²⁸⁶ Kişilere verilen takma isimler başka kaynaklar ile birleştirildiğinde kişiyi tanımlamayabilecek işlevde ise kişisel veri olarak kabul edilebilecektir. KVKK (2025) . 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Rehberi,) s. 21. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf> (Erişim: 18 Nisan 2025 Erişim Tarihi: 18.04.2025. Örneğin, Boğaziçi Üniversite’sinin x tarihindeki rektörü” verisinden makul ve erişilebilir araçlar yani teknoloji, internet ve üniversite yıllıkları vasıtası ile ulaşılabilir olduğundan bu veri ile isim verilmeden tanım yapılmış olur ve gerçek kişi tespit edilebilir. Küzeci, 2010, s.9; Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.13. Bireylerin tespit edilip edilemeyeceğini değerlendirirken, ilgili ve yeteri kadar kararlı bir kişinin kullanabileceği araçları değerlendirmeniz gerekir. ICO, Information Commissioner’s Officer bkz. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-information-a-guide/> .Erişim Tarihi: 16.05.2025. 95/46/EC sayılı Direktif, giriş, para. 26; Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.15.

²⁸⁷ ICO (Information Commissioner’s Office) (2025) . Personal information: What is personal information? A guide. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-information-a-guide/> (Erişim: 16 Mayıs 2025) . Örneğin, bugün teknolojinin geldiği noktada ses algılama teknolojisi ile kişilerin seslerinden kimlikleri tespit edilebilmektedir. Fakat, bu durum bir gerçek kişiye ait sesin her halükarda kişisel veri olarak kabulünü gerektirmez. Nitekim, kişinin bir restoranda rezervasyon yapmak için telefon görüşmesi yapmasında kişinin sesi tanımlayıcı niteliğinde değilken; ses tanıma sistemi bulunan bankanın müşteri temsilcisi ile yapılan görüşmede kişinin sesi kişisel veri niteliğindedir. Develioğlu, 2017, s.35.

²⁸⁸ Aksoy, 2010, s.27.

²⁸⁹ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.14.

²⁹⁰ GDPR, giriş paragraf 26; Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.15; Aksoy, 2010, s.26-27.

Son olarak belirtmek gerekir ki, veriler, veri sahibinin artık tanımlanamayacağı şekilde anonim hale getirildiğinde kişisel verilerin korunması hukuku kapsamında korunmaz. Bir verinin anonim veri olarak kabul edilebilmesi için, gerçek kişinin belirlenebilmesini sağlayan hertürlü özellikten arınmış olması gerekir²⁹¹. İstatistik veya araştırma amaçları ile işlenen ve anonim hale getirilmiş veriler böyledir²⁹². Anonim verilere benzeyen psödonim verilerde ise farklı olarak kişisel veri olarak kabul edilmektedir. Psödonim veriler, GDPR düzenlemesinde, kişisel verilerin ek bilgiler kullanılmadan ilgili kişi(veri öznesi) ile ilişki kurulamayacak şekilde işlenmesi olarak tanımlanmıştır(m.4/5). Kodların listeleştirilmesi marifeti ile veya iki yönlü kriptolama algoritması kullanılarak psödonimleştirme yapılabilir. Örneğin, bir okulda öğrencilerin verilerinin işlendiği bir listede öğrencilerin isimleri yerine bir kodlama kullanılması halinde, o kodun hangi öğrenciye ait olduğu bir anahtar vasıtası ile belirlenebiliyor ise veri psödonimdir²⁹³. Aslında, psödonim veriler, bireye geri dönmek mümkün olduğu anlamına gelir, ek bilgiler kullanıldığında verisi işlenen kişinin kimliği keşfedilebilir. Bu sebeple ek bilgilerin psödonim verilerden ayrı tutulması ve veri sorumlusu tarafından gerekli idari ve organizasyonel tedbirlerinin alınması gerekmektedir²⁹⁴.

2.2.4. İlişkili olma

İşlenen verinin bir gerçek kişi ile “*ilişkili olması*” diğer bir ifade ile “*bağlantılı*” olması kişisel verilerin nitelendirilmesi bakımından önemlidir. Bu sebeple “ilişkili olma” kişisel veri kavramının son unsuru olarak ele alınmıştır. Bu unsur özellikle nesneler ve yeni teknolojilerle ilgili olarak kavramın maddi kapsamını saptamak ve ayırt edebilmede kritik bir rol oynamaktadır²⁹⁵.

Pek çok durumda bilgi ile kişi arasındaki bağlantı çok kolay kurulmaktadır. Örneğin, çalıştığı işyerinde, kendisine ait özlük dosyasındaki bilgiler ile işçinin ilişkisini saptamak oldukça kolaydır. Bazı durumlarda ise bu bağlantının kurulması nispeten zor olabilmektedir. Örneğin, satışa sunulan bir evin ekonomik değeri esasen eşyaya ilişkin bir veri olduğu için esasen kişisel veri değilken; malikin bazı vergileri ödeme yükümlülüğünün belirlenmesi için kullanıldığında bir kişisel veri niteliğinde olmaktadır. Maliki olunan bir araca ilişkin plaka bilgisi de esasen araca ilişkin bir veri iken basit bir bağlantı kurularak gerçek kişinin (“*malikin*”) belirlenmesi mümkün olduğundan araç plakası kişisel veri olarak kabul edilebilir²⁹⁶. Dolayısıyla, verilerin bir kişiyle ilgili olması o kişiye “odaklanılmasını” zorunlu kılmamaktadır. Önemli olan bilgi ile gerçek kişi arasındaki ilişkinin/bağlantının kurulabilmesidir²⁹⁷.

²⁹¹ Develioğlu, 2017, s.35; Ayözger Öngün, 2019, s.13. 29. Çalışma Grubu’nun anonimleştirme teknikleri hakkındaki değerlendirmeleri için bkz. Article 29 Working Party (2014, 10 Nisan) . *Opinion 05/2014 on anonymisation techniques*. European Commission. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (Erişim: 30 Nisan 2025) .

²⁹² 95/46/EC sayılı Direktif, *giriş*, para. 26; GDPR, *giriş*, para. 26. Anonimleştirilen araştırma ve istatistiki verilerin ayrıntılı kişisel veri değerlendirmesi için ayrıca bkz. Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.18-21. Örneğin, katılanların isminin toplanmadan sokakta bir anektöre doldurulan beslenme alışkanlıklarına ilişkin bir anket formundaki bilgiler anonim veridir ve kişisel veri kapsamında değildir. Develioğlu, 2017, s.35; Ayözger Öngün, 2019,

²⁹³ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.18; Develioğlu, 2017, s. 36.

²⁹⁴ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.18; GDPR m.4/5.

²⁹⁵ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s. 25.

²⁹⁶ Şimşek, 2008, s. 121-122; Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.9-11.

²⁹⁷ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.9-11.

Veriler, içerik, amaç ve sonuç bağlamında kişiye ilişkin olabilir. İçerik yönünden kişiye ilişkin olma hali doğrudan hakkında olma şeklindedir. Örneğin, bir kişinin özgeçmişindeki veriler o kişi hakkındadır ve “içerik” yönüyle kişi ile ilişkidir. Kimi veriler ise “amaç” unsuru ile yani toplanma sebepleri ile bir gerçek kişiye ilişkindir. Kişinin davranışlarının, performanslarının veya durumunun değerlendirilmesi için veri toplanılmasında böyledir. Bu duruma kişinin özlük haklarının belirlenmesi için işçinin giriş çıkış saatlerinde parmak izinin alınması böyledir. Kimi veriler ise “sonuç” bağlamında bir kişiye ilişkin olabilir. Örnek olarak hizmeti optimize etmek için taksilerin konumunun izlenmesi verilebilir. Bu servis esasen taksinin bulunduğu konumu tespit için kullanıldığı için sürücüyü değil; araca yani eşyaya ilişkin bir veridir. Fakat, taksinin sürücü tarafından kullanıldığı durumlarda, sürücünün hız sınırına uyup uymadığı veya direksiyon başında olup olmadığı bilgilerini de içerdiği için bu bilgiler kişisel veri niteliğini haiz olur²⁹⁸. İçerik, amaç ve sonuç unsurları alternatif şartlardır, yalnızca birinin varlığı halinde veri kişiye ilişkin kabul edilecektir²⁹⁹.

2.3. Kişisel Verilerin Hukuki Niteliği

Kişisel verilerin hukuki niteliğinin belirlenmesi uygulanacak hukuk rejiminin belirlenmesi açısından önem arz etmektedir³⁰⁰. Kişisel verilerin hukuki niteliğine ilişkin farklı yaklaşımlar bulunmaktadır. Bu başlık altında kişisel verilerin hukuki nitelendirmesi bakımından temel olarak Anglo-Amerikan ve Kıta Avrupası hukuk sistemlerinde bugüne kadar kabul edilen görüşlerin değerlendirmesi yapılarak günümüzde kabul edilen hukuki nitelendirme üzerinde durulacaktır.

Anglo-Amerikan hukuk sisteminde Kıta Avrupası sisteminde olduğu gibi merkez bir düzenleme ile koruma mevcut olmadığını belirtmek gerekir³⁰¹, sektörel bazlı korumaların³⁰² olduğunu söylemek mümkünse de kişisel verilerin korunması özelinde mevzuatın yetersiz kaldığı ifade edilmekte ve eleştirilmektedir³⁰³. Bu sistemde kişisel veri hukukuna ekonomik-iktisadi temelli yaklaşılmakta ve kişisel veri kavramı kişiden soyutlaştırılarak bağımsız bir ürün (iktisadi bir değer) gibi değerlendirilmektedir. Bu yaklaşımda, kişisel verilerin “mülkiyet hakkı” veya “fıkri ve sınai haklar” çerçevesinde değerlendirmesi gerektiği yönünde iki farklı görüş bulunmaktadır³⁰⁴.

²⁹⁸ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.10-11.

²⁹⁹ Aksoy, 2010,, s.29.

³⁰⁰ Kişisel verilerin hukuki nitelendirmesi hususunda ayrıca bkz. Akkurt, S. S (2020) . Kişisel veri kavramının hukuki niteliğine ilişkin yaklaşımlara mukayeseli bir bakış. *Kişisel Verileri Koruma Dergisi*, 2 (1), 20-32.

³⁰¹ Lemley, M. A (2000) . Private property: A comment on Professor Samuelson’s contribution. *Stanford Law Review*, 52, s.1545.

³⁰² Örneğin, sağlık sektöründe kişisel verilerin işlenmesine ilişkin olarak Health Insurance Portability and Accountability Act (HIPAA); Kaliforniya eyaletinde yaşayan bireylerin kişisel verilerini kontrol etme ve satılmasına karşı haklara ilişkin tüketici kişisel verileri ile ilgili olarak California Consumer Privacy Act (CCPA) düzenlemeleri mevcuttur.

³⁰³ Schwartz, P (1989) . The computer in German and American constitutional law: Towards an American right of informational self-determination. *The American Journal of Comparative Law*, 37 (4), s.676, 694-698.

³⁰⁴ Akkurt, 2020, s. 22; Prins, C (2006) . When personal data, behavior and virtual identities become commodity: Would property rights approach matter? *SCRIPTed: Journal of Law, Technology and Society*, 3 (4), s. 273 vd. ; Aksoy, 2010, s.57 vd.

2.3.1. Mülkiyet hakkı görüşü

Kişisel verilerin mülkiyet hakkı çerçevesinde değerlendirildiği görüşte, kişisel verileri eşya hukuku bağlamında “şey” veya “meta” olarak kabul edilmektedir³⁰⁵. Buna göre, kişisel veriler, ait olduğu kişiden bağımsız olarak bir iktisadi değeri olan bir ürün olan görülümde alınıp satılmakta³⁰⁶ ve devredilebilmektedir³⁰⁷. Kişisel verilerin ekonomi için değerli bir emtia(mal) olduğunu belirten Sholtz, kişisel bilgilerin tüm biçimleri ya da kullanımlarının mülkiyet hakkı çerçevesinde değerlendirmesi gerektiğini ifade etmiştir³⁰⁸. Buna göre, kişi malik sıfatı ile kişisel verileri üzerinde tasarrufta bulunma, kullanma ve yararlanma haklarına sahiptir. Bu demektir ki, bireyler kişisel verilerini bedel karşılığı satabilir veya üçüncü kişiye karşılıksız(ivazsız) olarak devredebilir. Bu yaklaşımı eleştiren HINGH, kişisel verilerin ticari değeri temsil ederek metalaştırılmasına ve varoluşun ve gündelik yaşamın tüm yönleri ile alınır satılır metalara dönüştürülmesine karşı çıkmış ve kişisel verilerin satılmasını, kişilerin bu verileri gönüllülük esasına göre vermiş olması durumunda dahi, bu durumun insan onuru ile bağdaşmayacağı dile getirmiştir³⁰⁹. Anayasal haklar en yüksek fiyat verene satılabilir mi? sorusu ile etkileyici bir soru soran PRINS, bireyleri kişisel verileri üzerindeki mülkiyet hakkından mahrum bırakmanın kişileri verileri üzerinde daha az pazarlık yapabilir bir konuma soktuğunu ve böyle daha dezavantajlı olduklarını ifade eder. Bu noktada başka bir soru şu olmalıdır: Hangisi daha önemlidir; kişi özerkliği mi anayasa ile güvence altına alınan insan haklarını?³¹⁰ Mülkiyet hakkı teorisinin kişisel verilerin korunmasındaki maaliyetleri arttıracığı ve kişisel verilerinin işlenmesi ile mevcut sistemler hakkında bilgi sahibi olmayan bireyin kişisel verileri üzerindeki mülkiyet hakkından bilinçsizce vazgeçmesine sebep olabileceği, dezavantajlı konumda bulunan bireyin korunması ile bu teorisinin bağdaşmayacağını söyleyen PRINS, diğer yandan bir hakkın temel insan hakkı olarak değil mülk olarak görülmesinin sağlanan koruma sebebi ile bugün Amerika’da daha büyük korumaya ulaştıracağını ifade

³⁰⁵ bkz. Sholtz, P (2001) . Transaction costs and the social cost of online privacy. *First Monday*, 6 (5), 1 vd. <https://firstmonday.org/article/view/887/823> . Schwartz, 1989, s. 2076 vd. SHOLTZ, kişisel veri mülkiyet hakları sisteminin mahremiyeti korumanın çok daha güçlü olduğunu ifade eder. bkz. Sholtz, 2001, “*Clarifications on Personal Information Property Rights*” başlığı. Türk Hukuku bakımından doktrinde Akkurt, Türk eşya hukukunda mülkiyet hakkının korunmasına ilişkin hukuki çare ve davaların kişisel verilerin korunmasına doğrudan hizmet edecek elverişlilik ve nitelikte olmadığını ifade etmiştir. Bkz. Akkurt, 2020, s. 23.

³⁰⁶2001 yılında, ABD Massachusetts eyaletinde, Toysmart Şirketi’nin 250.000 müşterisinin isim listesi ile diğer kişisel verilerini (e-mail, adresler, işlem detayları) 50.000 USD karşılığı olarak yaptığı satış yargıç tarafından hukuken geçerli olarak kabul edilmiştir. akt. Prins, 2006, 271. SHOLTZ, kişisel verilerin satın alınması meselesine eleştiri getirmektedir. Bu noktada, müzik CD’si örneğini vermekte ve CD’yi satın aldığımızda, plak şirketinin içinde bulunan müzik üzerindeki mülkiyet haklarını elinde tutmaya devam edeceğini tıpkı bu örnekte olduğu gibi kişisel veri aktarımı yapıldığında ve her halde kişisel verinin mülkiyetinin ilgili kişide kalması gerektiğini savunmaktadır. Bkz. Sholtz, 2001, “*Clarifications on Personal Information Property Rights*” başlığı.

³⁰⁷PRINS, anayasal bir hak devredilebilir mi sorusu ile devredilebilirliği sorgularken, mülkiyet hakkının kişilere kişisel verilerinin işlenmesine ilişkin pazarlık imkanı tanıdığının altını çizmektedir. Buna göre, bireysel özerkliğin mi yoksa anayasal insan haklarının mı önemli olduğu tartışması gündeme gelmektedir. Prins, 2006, s.287. Amerikan doktrininde veri ticaretine ilişkin yasal sınırlandırma ve devredilmezliğe ilişkin tartışmalar için ayrıca bkz. Schwartz, 1989, s.2057.

³⁰⁸Sholtz, 2001, bkz. “*Property rights over personal information*” s.9 vd.

³⁰⁹Hingh, 2018, s.1272. Aynı yönde bkz. Aksoy, 2010, s.69.

³¹⁰Prins, 2006, s. 287. Bugün her ne kadar akademik dünyada kişisel verilerin bir meta olduğuna karşı çıkılsa da; yaşamın gerçekliğinde kişisel verilerin karşılığında fayda sağlanması karşılığı işlenen metalara dönüştüğü eleştirisi, Avrupa düzenlemelerinin mülkiyet hakkı teorisine daha elverişli bir ortam yarattığı ve piyasanın sadece kişisel verileri kötüye kullanan işletmeleri disipline etmekte yetersiz kalmadığı aynı zamanda aşırı veri kullanımı için teşvik yarattığı hakkında ayrıca bkz. Prins, 2006, s. 276 vd.

etmiştir³¹¹. Türk doktrinde ise kişisel verilerin niteliği gereği alınıp satılmasının; bu haklardan feragat edilmesinin ve devredilmesinin mümkün olmadığı dile getirilmiştir³¹².

2.3.2. Fikri mülkiyet hakkı görüşü

Kişisel verilere ilişkin bir diğer hukuki nitelendirme fikri mülkiyet hakkıdır. Bu görüşe göre, fikri hakkın korunmasını amaçlayan fikri mülkiyetin amacı ile kişisel verilerin korunması amacı arasında amaçsal bir benzerlik bulunmaktadır. Öyle ki, iki disiplinin de ortak amacının bilginin korunması ve dağılımının kontrol altında alınmasının sağlanması olduğu iddia edilmektedir³¹³. Ne var ki, bu görüş doktrinde yeterli desteği bulamamıştır ve eleştirilmiştir³¹⁴. Nitekim, Lemley, kişisel veriler üzerinde fikri mülkiyet kapsamında sağlanacak bir korumanın verilmek istenenden daha az bir korumaya dönüşebileceğini, her bir kişisel verilerin her birinin lisanslanmasını ve bu kapsamdaki çabanın ve maaliyetin göz korkutucu olduğunu ve son olarak meşru fayda ve kamu yararı gibi saikler işlenmesi gereken verilerin işlenmesinin bu koruma ile imkansız hale geleceğini ifade etmiştir³¹⁵. Akkurt, fikir eserlerinin aksine kişisel verilerin, iradi üretiminin eseri olmadığı, dolayısıyla fikri hakka konu olan değerler eser olarak nitelendirilirken, kişisel verilerin teknik anlamda eser olarak nitelendirilmelerinin mümkün olmadığı eleştirisini getirmektedir³¹⁶. Benzer şekilde PRINS, fikri mülkiyete konu eserler kasıtlı bir çabanın ürünü iken aksine kişisel veriler doğal varoluşlar sonucu meydana geldiğini, kasıtlı çabaların meyveleri olmadığını dile getirmiştir³¹⁷. Ayözger Öngün ise iki hukuk dalı arasındaki farkı dile getirirken, fikri mülkiyet hukukunun ekonomik kaygılar taşıması yanında kişisel verilerin korunmasında önemli olanın ekonomik kaygılar olmadığına vurgu yapmıştır³¹⁸.

2.3.3. Kişilik Hakkı Görüşü

Kıta Avrupası hukuk sisteminde, kişisel verilerin korunması ile kişi temel hak ve özgürlüklerinin korunmasının amaçlandığı, kişisel verilerin korunmasının hakkı temelde bir kişilik hakkı³¹⁹ olarak olduğu değerlendirilmekte ve kişisel verilerin korunması hakkının gerçek kişilerin özel hayatının gizliliğinin şemsiyesi altında olduğu ifade edilmektedir³²⁰. Diğer

³¹¹ Prins, 2006, s. 274-278; 295-297.

³¹² Akkurt, 2020, s. 28. Mülkiyet hakkı görüşünün belirli yönlerden ilgili kişinin haklarını koruduğu savunulsa da bu görüş esasen veri işleyen kişilerin menfaatine hizmet etmektedir. Aksoy, 2010, s.69.

³¹³ Prins, 2006, s. 279. Detaylı bilgi için ayrıca bkz. Zittrain, J (2000) . What the publisher can teach the patient: Intellectual property and privacy in an era of trusted privication. *Stanford Law Review*, 52, s. 1201-1251.

³¹⁴ Lemley, M. A (2000) . Private property: A comment on Professor Samuelson's contribution. *Stanford Law Review*, 52, s.1554; Akkurt, 2020, s. 24, Ayözger Öngün, 2019, s. 17-18.; Prins, 2006, s. 284; Aksoy, 2010., s.69.

³¹⁵ Lemley, 2000, s.1551-1552.

³¹⁶ Örneğin kişinin dış görünüşü, yara izleri, biyometrik verileri gibi kişisel veriler "eser" olarak nitelendirilemez. Akkurt, 2020, s. 24.

³¹⁷ Prins, 2006, s. 296.

³¹⁸ Ayözger Öngün, 2019, s.18. Aynı yönde bkz. Prins, 2006, s. 296.

³¹⁹ "Kişilik hakkı, bir bireyin hukuk düzenince korunan kişisel değerleri üzerinden sahip olduğu ve herkese karşı ileri sürebileceği dokunulmazlık ve hakimiyet alanını ifade eder. Bu haklardan tümüyle vazgeçilmesi, bu hakların devredilmesi yahut hukuka veya ahlaka aykırı şekilde aşırı ölçüde sınırlandırılması sonucunu doğuran hukuki işlemler yapılamaz. Bu hukuki işlemler kesin hükümsüzdür ve hukuki sonuç doğurmaz." Antalya ve Topuz, 2024, s. 121-122. "Kişilik, insanı insan kılan, onu diğerlerinden ayıran; bu nedenle de insana ayrılmaz ve vazgeçilmez bir şekilde bağlanan değerler bütünüdür." Badur, 2023, s. 11. Yargıtay, HGK 05.11.1997 tarihli, 1997/7-690 esas ve 1997/893 karar sayılı ilamında: "Kişilik hakkı, kişisel varlıkların korunmasıyla ilgilidir." ifadesine yer verilmiştir. Akt. Aksoy, 2010, s.38, dp.3.

³²⁰ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.21-22; Avrupa İnsan Hakları Mahkemesi, Handbook on European Data Protection Law, Data Protection Terminology, s. 85. Ayözger Öngün, 2019, s.5,14, 313; Develioğlu, 2017, s.30. Ayrıca, KVKK m.1'de açık şekilde kanunun amacının başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunması olduğunu belirtilmiştir. Nitekim

yandan, AİHM de kişisel verilerin korunması hakkının kişiliğin bir parçası olduğunu ifade etmektedir³²¹ ³²². Kişilik hakkı görüşüne göre, mahremiyet³²³ kişisel verilerin korunması hakkının bir görünümüdür ve bu sebeple kişisel verilerin korunmasına hizmet etmektedir³²⁴. Bu görüşe getirilen en büyük eleştiri, özel hayatın gizliliğinin yalnızca mahrem bilgileri koruması ve kamuya açık alandaki bilgilerin bu hak kapsamında korunmamasıdır³²⁵. Kişilik hakkı görüşü, kişisel verilerin en geniş bir biçimde korunmasına hizmet etse de; kişilik hakkı kapsamında olmayan gerçek kişiler hakkında gizli olmayan hatta gerçek olmayan veriler de kişisel verilerin korunması kapsamında korunmaması³²⁶ sebebiyle kişilik hakkı görüşü, kişisel veriler üzerinde arzu edilen tam korumayı sağlayamadığı ifade edilmektedir. Nitekim, kişisel veriler bugün kişilik hakkının koruduğu kişilik değerlerinden daha fazla bir alana yayılmış durumdadır³²⁷.

AİHM içtihatlarına göre de, kişinin özel hayatına yönelik bilgi depolanmasına ilişkin hususlar, “Özel Hayatın ve Aile Hayatının Korunması” başlığını taşıyan AİHS m. 8/1 kapsamına girer. Örneğin bkz. “Leander v. İsveç”, (Başvuru No. 9248/81), Karar Tarihi 26 Mart 1987; “S. ve Marper v. Birleşik Krallık”, (Başvuru No. 30562/04 ve 30566/04), Karar Tarihi 4 Aralık 2008; Şimşek, kişisel verilerin korunması hakkının anayasal temellerinin kişinin maddi ve manevi varlığını geliştirme hakkı yani kişiliğin serbestçe geliştirme hakkı (AY. M. 17), insan onuru ilkesi ve yine özel yaşamın gizliliği hakkı (AY m.20) olduğu görüşündedir. Şimşek, sürekli gözetlenen, yaşamına ilişkin tüm kişisel verileri kayıt altına alınan ve kişisel verileri üzerinde bir hakkı olmayan bireyin, kişiliğini serbestçe geliştirmesinin mümkün olmadığı ve bu kişinin özgür kişiliğinin gereğini değil ancak ondan beklenen davranış tarzı ile hareket edebileceğinin altını çizmektedir. Şimşek, kişisel verilerin korunması hakkını temel olarak özel hayatın gizliliği hakkından çok insan onuru kavramı ile ve kişinin maddi ve manevi varlığını koruma temel hakkı ilişkilendirmektedir. Şimşek, 2008, s. 111-112; 128-158. İnsan onuru kavramı ile ilişkilendirilmesi gerektiği hakkında bkz. Hingh, 2018, s.1269. Kişisel verilerin kişilik hakkı bağlamında ayrıntılı değerlendirilmesi için bkz. Aksoy, 2010,, s.38 vd.

³²¹bkz. Mehmedovic v. Switzerland, 11.12.2018, European Court of Human Rights (ECHR), Factsheet – Personal Data Protection. https://www.echr.coe.int/documents/d/echr/fs_data_eng . Erişim Tarihi: 23.02.2025.

³²² 11.12.1985 tarihli LUNDVALL v. SWEDEN kararında AİHM, vergi borçları olan kişilerin aleni olarak ilan edilmesini özel hayatın gizliliğinin ihlali olduğuna karar vermiştir. European Court of Human Rights (1985, 12 11) . *Lundvall v. Sweden* (Başvuru No: 45293/79) . <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-72432%22%5D%7D> (Erişim tarihi: 14.05.2025) . 07.07.1989 tarihli GASKIN v. UNITED KINGDOM davasında AİHM, hükümet nezdinde tutulan kişisel verilere ilişkin kayıtların özel hayatın gizliliği kapsamında değerlendirmiştir. bkz. European Court of Human Rights (1989, 07 07) . *Gaskin v. United Kingdom* (Başvuru No: 10454/83) . <https://hudoc.echr.coe.int/tur#%7B%22itemid%22:%5B%22001-57491%22%5D%7D> (Erişim tarihi: 14.05.2025) . Detaylı bilgi ile güncel kararlar için bkz. European Court of Human Rights (2025) . *Factsheet – Personal Data Protection*. https://www.echr.coe.int/documents/d/echr/fs_data_eng (Erişim tarihi: 23.02.2025) .

³²³Avrupa düzenleyici metinlerde kişisel verilerin korunmasında amaçlanan mahremiyet hakkının korunması olduğu ifade edilmiştir. Kıta Avrupası metinlerinde sıkça karşılaştığımız bu kavramın, Türk hukukunda bağımsız görünüm türlerinden birisi özel hayattır. Aksoy, 2010, s.47.

³²⁴ Aksoy, 2010, s.47; Ayözger Öngün, 2019, s. 15; Akgül, 2014, s. 45.

³²⁵Ayözger Öngün, 2019, s.18; Taştan, 2017, s.62-63.

³²⁶ bkz. “Her Türlü Bilgi” başlığı. Nitekim, kişinin kamuya açık bilgilerinin işlenmesi halinde de zarar görmesi mümkündür. Örneğin, Türkiye’de vatandaşlar katıldığı toplantı ve gösteri yürüyüşleri ile veya bir örnek olarak devamlı suretle gittiği ibadethanelerin kayıt altına alınması ile fişlenebilmekte ve ayrımcılığa maruz kalabilmektedir. Aksoy, 2010, s.70.

³²⁷ Taştan, 2017, s. 63. Kişinin kamusal alanda gerçekleştirdiği davranışlar gizliliği bulunan davranışlar olmasa da tıpkı gizli verilerde olduğu gibi toplanıp belli amaçlar dahilinde işlenmesi halinde kişi zarar görebilir. Örneğin, bir kimsenin siyasi parti toplantılarına, toplantı veya gösterilere katılması ile kişinin düzenli olarak bir ibadethaneye gittiği bilgisi gizlilik taşımaya da, bu verilerin belli amaçlar dahilinde işlenmesi, veri sahibine karşı ayrımcı davranış sonucunu doğurabilecek ve bu cihetle bu cihetle zarar verebilecektir. Bu nedenle kişisel verileri, yalnızca özel hayat kavramı ile ilişkilendiren kişilik hakkı görüşünün kabul edilmesi mümkün değildir. Aksoy, 2010, s.63-64.

2.3.4. Günümüz “bağımsız hak” yaklaşımı

Kişilik hakkının bir görünümü olan kişisel verilerin korunması hakkının hukuki nitelendirilmesi açısından, Federal Alman Anayasa Mahkemesi’nin 1983 yılında verdiği “Nüfus Sayımı(Census) Kararı” çok önemlidir. Nitekim, Federal Alman Anayasa Mahkemesi bu kararı ile kişisel verileri salt kişilik hakkı bağlamında değil; herkesin kendisine ait verilerin kullanımını ve devri konusunda esas olarak belirleme hakkına sahip olması şeklinde tanımladığı “bilginin geleceğini belirleme hakkı” kavramını ortaya atmış ve bu cihetle, bilgi toplumuna hediye edilen bu hak, kişisel verilerin korunması hakkının ortaya çıkmasında büyük bir adım olmuştur³²⁸.

Günümüzde kişisel verilerin korunması hakkının, insan haklarının özel hukuktaki görünümü olan kişilik hakkı kapsamında fakat yalnızca özel hayatın gizliliği ile ilişkilendirilemeyen inanç özgürlüğü, insan onuru, inanç özgürlüğü ve düşünce özgürlüğünü ile bir dizi temel hak ve özgürlük ve ayrıca iktisadi varlık ve hürriyet, enformasyonel özerklik (self – determinasyon) gibi pek çok kişisel değerle bağlantısı olan fakat kendine özgü koruma alan başlı başlına koruma alanı içinde bulunan bağımsız bir anayasal hak olarak tanımlanmaktadır.³²⁹

Kanaatimiz de kişisel verilerin kişilik hakkı bağlamından,³³⁰ insan onuru ve özel hayatın gizliliği, haberleşme özgürlüğü, düşünce özgürlüğü, unutulma hakkı, bilgi edinme

³²⁸Federal Almanya Anayasa Mahkemesi, 15 Aralık 1983 tarihli Nüfus Sayımı (Census) Kararında (BverfGE 65, 1-Volkszählung, 15 Aralık 1983) daha önce tanımlanmayan ve bu karardan sonra yaygın kullanıma sahip olan bir hak tanımlandı: “bilgilerin geleceğini belirleme hakkı” (“Informationelle Selbst-bestimmung”; “right of informational self-determination”). Alman halkının geniş ölçekteki soruları cevaplamasını isteyen ve böylece vatandaşının nüfus bilgilerinin yanı sıra gelir bilgilerini, çalışma saatlerini ve eğitim durumlarını da öğrenerek özellikle seçime yönelik politikalar yürütmek isteyen hükümet kararını Anayasa’ya aykırı bulan Alman Anayasası Kararına göre, “bilgilerin geleceğini belirleme hakkı”, insan onurunun ve “kişiliği serbestçe geliştirme haklarının bir gereğidir. Bu hak, kişisel verilerin sınırsız bir şekilde toplanmasından, kontrolsüz şekilde işlenmesinden (kayıt edilmesinden, kullanılmasından ve aktarılmasından) koruma görevi görmektedir. Alman Anayasa Mahkemesi, bilgisayar gibi otomatik veri işleme araçlarının kullanıldığı durumlarda ihmallerin ve kişilerin zarar görme tehlikesinin daha ciddi bir hale büründüğünün altına çizmiştir. Nitekim, bu kaynaklar sınırsız ve hazır erişime olanak tanımakta, veriler arasında ilişki kurulmasına olanak tanıyarak profillemeyi kolay hale getirmekte ve veri kayıt hacmini çok geniş tutabilmektedir. Alman Anayasa Mahkemesi Kararı, esasen kamu-birey güç dengesinin korunması amacı gütmüştür. Schwartz, 1989, “Right of Informational Self-Determination”, s. 686-692; Küzeci, E (2014). İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı. *İnsan Hakları Yıllığı*, 32, 1-23. Ayrıca bkz. Ayözger Öngün, 2019, s.19. Bilginin geleceğini belirleme hakkı, insan onuruna ve kişiliğin serbestçe geliştirilmesi hakkını temel alarak türetilmiş bir hak türüdür. Buna göre, kişinin kendisi ile ilişkili olan verilerin kaderini tayin hakkı bulunmaktadır. Dolayısıyla, verilerin işlenmesine ve aktarılmasına dair karar hakkı ilgili kişide yani verisi işlenen gerçek kişidedir. Ayözger Öngün, 2019, s.313. Alman Anayasa Mahkemesi’nin 1973 tarihli Lebach Kararında bir hükümlünün adının açıkça anıldığı ve işlediği suça ilişkin kişinin belgeselinin yayımlanmasını karşısında söz konusu belgeselin televizyondan kaldırılmasına ilişkin verdiği karar, kamu menfaati ile birey menfaatinin çatıştığı noktalardan birini konu almaktadır. Kişinin kendi bilgisinin geleceğini belirleme hakkına ilişkin değerler belirlenmesinde ve değerlendirilmesinde Lebach Kararı da önem teşkil etmektedir. SCHWARTZ, “Right of Informational Self-Determination”, s. 694. Self-determinasyon hakkı kişisel verilerin korunmasındaki sebeplerden olan verilerin serbest dolaşımına da imkan tanımaktadır. Aksoy, 2010, s.72.

³²⁹ Aksoy, 2010, s.72; Ayözger Öngün, 2019, s.18,313; Şimşek, 2008, s. 147-148; Akkurt, 2020, s. 27-30; SELEK, s.15; Taştan, 2017, s. 65-66; Akgül, 2014, s. 343-344. Kişilik hakkının bağımsız bir görünüm şeklinde kişisel verilerin korunması kişisel verilerin kişilik hakkından soyutlandığı anlamına gelmez. Nitekim, ne teknolojinin ne de toplum dinamiklerinin değişmesi kişisel verilerin kişi varlığı değerleri içinde gerçeğini değiştirmeyecektir. Taştan, 2017, s. 65-66. Konu ile ilgili olarak ayrıca bkz. Akkurt, S. S (2020). *Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış. Kişisel Verileri Koruma Dergisi*, 2 (1), 20-32.

³³⁰ Dolayısıyla kişisel verilerin ihlali durumlarında kişilik hakkını korumaya yönelik kanun hükümlerine dayanılabilir. Ayözger Öngün, 2019, s.53.

hakkı³³¹ gibi birçok temel hak ve hürriyet³³² ve self – determinasyon ile bağlantılı olan bağımsız bir hak olarak kabul edilmesi gerektiği yönündedir.

Doktrinde kimi görüş kişisel verilerin korunması hakkının kişiye sıkı sıkıya bağlı olması gerektiğini ifade ederken³³³, kimisi bu özelliğin yerine kişisel verilerin mülkiyet hakkında olduğu gibi devrinin mümkün olduğunu ifade etmektedir³³⁴. Diğer yandan, kişisel verilerin korunması hakkı, ilgili kişinin(verisi işlenen gerçek kişinin) sınırsız hakimiyetinin olduğu mutlak bir hak türü değildir. Yani, sınırsız olarak korunmamaktadır ve bu hakka müdahale mümkündür³³⁵.

2.4. Kişisel Verilerin Korunmasının Hukuku

Bir yanda hızla gelişen teknoloji ile özgürce akan bilgi akışı ve bilginin belli çıkar ve amaçlar doğrultusunda devletler, kişi toplulukları, kişiler veya şirketler tarafından toplanması, işlenmesi ve değerlendirilmesi ile kişisel hak ve özgürlükler ile özel olarak bireysel özerkliğin gerektirdiği kişilerin bilgi üzerindeki denetim hakkı sürekli bir çatışma halindedir. Burada bir dengenin sağlanması çok önemlidir. Üretilen veri sayısının çoğalması gibi veri işleme amaçlarına da her geçen gün bir yenisi eklenmektedir. Genel çerçevede, devletler yönetim, planlama, planlama, güvenlik gibi saikler ile kişisel veri işlemekteyken, şirketlerin amacı ise müşterilerine daha iyi hizmet sunabilmek ve kar marjını arttırmadır. Bu noktada kişisel verilerin

³³¹Bilgi edinme hakkının bir temel hak ve özgürlük olarak kabul edilmesi ile bu hususa ilişkin maddi ve usulü belirlemek için 4982 Sayılı Bilgi Edinme Kanunu (R.G. 24.10.2023 T., 25269 S.) çıkarılmıştır. Söz konusu hak, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinde, demokratik ve şeffaf yönetimin gereği olarak bireylerin bilgilendirilmesi amacını gütmektedir (Kanun m.1-2) . Kanun'un 21. maddesi 1. fıkrasında :” Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.” düzenlemesine yer verilerek kişisel veriler korunmuştur. Aynı maddenin 2. fıkrasında ise yalnızca kamu yararının olduğu durumlarda kişilere ilişkin verilerin paylaşılabileceği fakat bu hallerde ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşulu getirilmiştir.

³³² Detaylı bilgi için bkz. Ayözger Öngün, 2019, s.39-67; Şimşek, O (2008) . *Anayasa hukukunda kişisel verilerin korunması*. Beta Yayıncılık.

³³³ Selek, 2021, s.15.

³³⁴ Ayözger Öngün, 2019, s.313. Kişisel verilerin devredilemez olması gerektiği hakkında ise bkz. Selek, 2021, s.15.

³³⁵ Kişisel verilerin korunması hakkına kamusal organlar tarafından yapılan müdahale ancak kişinin rızası veya kamu yararı doğrultusunda ve ancak kanuni bir temelle mümkün olabilir. Şimşek, 2008, s. 127. GDPR m. 23’de kişisel verilerin korunması hakkının belli koşul ve şartlarda kısıtlanabileceği düzenlenmiş ve söz konusu sebepler şu şekilde düzenlenmiştir: milli güvenlik, savunma, kamu güvenliği, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi; Üye Devletlerin önemli ekonomik veya mali çıkarı başta olmak üzere, parasal hususlar ile bütçe ve vergilendirmeye ilişkin hususlar, halk sağlığı ve sosyal güvenlik de dâhil, Birlik ya da bir Üye Devlet’in genel kamu yararına yönelik diğer önemli amaçlar, yargı bağımsızlığının ve yargısal süreçlerin korunması, düzenlenmiş mesleklere ilişkin etik kuralların ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması, nadiren olsa dahi, resmi yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevi, veri öznesinin veya başkalarının hak ve özgürlüklerinin korunması, medeni hukuktan kaynaklanan hak iddialarına ilişkin kararların icrası. AT Kişisel Verilerin Korunması Yönergesi (95/46/AT) de kişisel veriler bakımından Yönerge’deki koruma alanlarına ilişkin birtakım sınırlar ve istisnalar getirilmesine olanak tanımaktadır. Nitekim, Yönerge m. 13’te üye devletlerin devlet güvenliği, ülke savunması, kamu güvenliği, suçtan korunma ve suçların soruşturulması ve kovuşturulması, üye devletlerin önemli finansal yararı, ilgili kişinin korunması, diğer kişilerin hak ve özgürlükleri sebepleri ile kişisel verilerin korunması hakkına birtakım sınırlamalar ve istisnalar getirilebilecektir. KVKK m. 28’de benzer şekilde Kanun’un uygulama istisnalarına yer verilmiştir.

korunması hakkı veri akışının ortadan kaldırılması değil, bu büyük veri akışında verisi üzerindeki hakimiyetini ve kontrolünü kaybetmiş olan kişiye, işlenen verileri üzerindeki denetim hakkının sağlanmasına hizmet etmek ve bu bakımdan bir denge unsuru işlevini görmektedir. Bu bakımdan kişisel verilerin korunması hukuku, hızla gelişen teknolojik gelişmelerin sağladığı olanaklar ile kişi hak ve özgürlükleri arasındaki teraziye sağlanmaya çalışılan denge unsurlarından biridir³³⁶. Bu noktada, belirtilmelidir ki, söz konusu veri işleme faaliyetlerinin meşru nedenlere dayanması ile belli amaçlara hizmet etmesi sebepleri ile veri koruma kurallarının gereksiz şekilde genişletilmesinin önüne geçilmeli ancak kişisel veri kavramını gereksiz yere kısıtlamaktan da kaçınılmalıdır.³³⁷

Kişisel verilerin korunması hakkı temelini Anayasa'dan alan bireyin hak ve özgürlüklerinin korunmasını amaçlayan yukarıda belirtildiği üzere teknolojinin gelişmesi ve bilginin işlenmesi ile akışının hızlanması ile ortaya çıkan bir temel hak ve özgürlüktür. Sadece verinin korunması veri güvenliğine ilişkin bir meseledir fakat kişiye ait verilerin kişinin özel alanını ile hak ve özgürlüklerinin korunması amacı doğrultusunda korunması, kişisel verilerin korunması hukukunun bir parçasıdır. Kişisel verilerin korunması hukuku, özel yaşamın gizliliği, haberleşme özgürlüğü, inanç özgürlüğü, ifade özgürlüğü gibi daha pek çok Anayasal hak ve özgürlüğün garanti altına alınmasına da hizmet etmektedir³³⁸. Kişisel verilerin korunması hukuku, verinin kaderi tayin noktasında ilgili kişiye(verisi işlenen gerçek kişiye/ "veri öznesine") karar verme özgürlüğü tanımaktadır. Bu kapsamda, ilgili kişi işlenen verisi hakkında bilgi alma, aktarılan kişileri öğrenme, işlenme amaçlarını öğrenme, eksik veya yanlış işlenen verisinin düzeltilmesini isteme, kanunda belirtilen koşullar altında silinmesini isteme, işlenen verisi sebebi ile uğradığı zararı isteme gibi haklara sahiptir³³⁹.

Kişisel verilerin korunması hukuku, genel olarak kişisel verilerin işlenmesinde hangi ilke ve kurallara uyulması gerektiğini açıklar³⁴⁰. Bunun yanı sıra kişisel verilerin işlenmesinde rol alan süjelerin hak ve yükümlülüklerini tespit ederek birlikte bunların etkin ve işlevsel olarak kullanımı için gerekli denetim mekanizmalarını ve ihlal halindeki yaptırımları belirler. Birçok hukuk alanına ilişkin hükümlerin de uygulandığı ve bu surette hem özel hem de kamu hukuk hükümlerinin uygulandığı kişisel veri hukuku, karma nitelikli bir hukuk dalıdır. Nitekim, kişisel verilerin korunması hakkı 1982 Anayasa'sı 20. madde ile güvence altına alınmış bir anayasal hak olmasının yanında TCK m. 135 vd. maddelerinde bu hakkın ihlal edildiği bazı durumlar suç olarak kabul edilmiştir. Bu yönüyle kamu hukukunun ilgilendirmesinin yanı sıra, kişilik hakkı kapsamında koruma alanı bulan bu hakkın ihlalinde TMK ve TBK hükümlerine de gidilebilmektedir. Bu durum da bu hukukun özel hukuk boyutunu ortaya koymaktadır. Dolayısıyla, hem kamu hukuku hem de özel hukuk düzenlemelerinin uygulanabildiği kişisel veri koruma hukuku karma nitelikli bir hukuk dalıdır³⁴¹.

Kişisel verilerin korunmasına ilişkin belirtilmesi gereken bir husus, bu konunun teknoloji ile yakın ilişkili olması ve doğal olarak teknoloji üretenin, dilini de belirlemesinden pek çok yabancı kökenli terim ile karşılaşılacağıdır. Nitekim GDPR ve KVKK metinlerinde

³³⁶Küzeci, 2010, s.3.

³³⁷Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.25.

³³⁸Şimşek, 2008, s. 217, 128-153.

³³⁹GDPR m. 15-18; KVKK m.11.

³⁴⁰ Develioğlu, H. M (2017) . 6698 sayılı Kişisel Verilerin Korunması Kanunu ile karşılaştırmalı olarak Avrupa Birliği veri koruma tüzüğü uyarınca kişisel verilerin korunması hukuku, Onikilevha Yayınevi, s.29.

³⁴¹Taştan, 2017, s. 8-9.

“kişisel veri” olarak tanımlanan kavram, özellikle Anglo-Amerikan sistemine dahil ülkelerde “özel hayatın gizliliği (privacy protection)” başlığı altında incelenmiştir³⁴². Dolayısıyla konu ile ilgili Anglo-Amerikan hukuk sisteminde yapılacak araştırmalarda; akademik çalışmalarda, mahkeme kararları vesair ilgili hukuk kaynaklarından yapılacak tarama kişisel veri kavramı ile değil; Mahremiyet ve Veri Mahremiyeti-Veri gizliliği (information privacy-intimacy) kavramları kullanılarak yapılmalıdır³⁴³.

Bireyin kişisel verilerinin korunması hakkı, bireye devlet karşısında bir savunma hakkı vermekle kalmaz. Bununla birlikte bütün devlet güçlerinin uyması gereken bir devlet düzeni yaratma konusunda devlete bir ödev yükler. Dolayısıyla kişisel verilerin korunması hakkı hem subjektif bir hak hem de objektif değer düzeninin bir unsurudur³⁴⁴. Belirtmek gerekir ki, kişisel verilerin korunması hukuku her ne kadar birey temel hak ve özgürlüklerinin korunması amacı ile ortaya çıkarılmış olsa da diğer bu alanın yaratılmasındaki ikinci amaç verilerin serbest dolaşımının sağlanmasıdır³⁴⁵. Nitekim, bu hususa uluslararası metinlerde açıkça yer verilmiştir³⁴⁶.

Kişisel veri hukukuna bakıldığında, kişi haklarını tehlike altında bırakan sujenin ilk bakışta “Devlet” olarak düşünüldüğü görülecektir. Nitekim, birçok kaynakta bireyin devlet karşısındaki savunmasız durumu, devlet tarafından tüm verilerinin kontrolsüz ve anayasal denetim hakkı olmadan işlenmesi ile bireyin kendini gerçekleştiremeyeceği ve kişi hak ve özgürlüklerine müdahale olacağı gerekçeleri ile bireyin işlenen kişisel verileri hakkında bilgi edinme, denetim ve müdahale haklarını sağlayan kişisel verilerin korunması hakkının anayasal koruma altına alınması gerektiği ifade edilmiştir³⁴⁷. Ne var ki, bugün devletlerden daha güçlü konumlarda bulunabilen şirketlerin kişilerin verilerini işlemesi ve aktarmasındaki tehlike çok daha riskli ve kapsamlıdır. Çalışmamızda bu kapsamda temel olarak e-ticaret platformları ele alınmıştır.

2.5. Genel Olarak Kişisel Veri Hukukunun Sujeleri

Kişisel verilerinin korunmasına duyulan ihtiyaç, bu kavramın tanımı ve unsurları ile hukuki niteliği anlaşıldıktan sonra bu verilerin kimler tarafından nasıl işleneceği meselesi gündeme gelmektedir. Çalışmamız kapsamında, özellikle e-ticarete veri işleyenlerin sorumluluğu ile verisi işlenen kişinin müracaat, itiraz ve şikayet hakları kapsamında kişisel verilerin korunması hukukunun sujelerini belirlenmesinde fayda bulunmaktadır. Aşağıda kişisel veri hukukunun temel üç öznesi açıklanmıştır.

³⁴²bkz. Sholtz, P. (2001) . Transaction costs and the social cost of online privacy. *First Monday*, 6 (5) .; Schwartz, P. M. (2004) . Property, privacy, and personal data. *Harvard Law Review*, 114 (7), 2055–2128.; Gostin, L. O. (1995) . Genetic privacy. *Journal of Law, Medicine & Ethics*, 23, s. 320-330; Küzeci, 2010, s.14-15.

³⁴³Küzeci, 2010, s.14-15; Schwartz, 2004, “Right of Informational Self-Determination”, s. 675-676.

³⁴⁴Şimşek, 2008, s. 113.

³⁴⁵Aksoy, 2010, s.75.

³⁴⁶bkz. GDPR, giriş, 13,21, 166 ve m.1/3: ” Kişisel verilerin Birlik içinde serbest dolaşımı, kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ile bağlantılı sebeplerle kısıtlanmaz ve yasaklanmaz.”

³⁴⁷bkz. Şimşek, 2008, s. 113.

2.5.1. İlgili kişi (kişisel verileri işlenen kişi veya veri öznesi)

İlgili kişi, kişisel verisi işlenen kişiyi ifade etmektedir³⁴⁸. Avrupa Birliği tüzük ve yönetmeliklerinde bu kişi “veri öznesi” olarak geçmektedir. İlgili kişi çalışmamızda yukarıda kişisel verinin “Kişi”³⁴⁹ unsuru başlığı altında detaylandırıldığından burada ayrıca incelenmeyecektir.

2.5.2. Veri sorumlusu

Veri sorumlusu (“controller”) yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve yollarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder(GDPR m.4/7)³⁵⁰. Yani, kişisel verilerin işlenmesi konusunda ne, nasıl, niçin, hangi sürelerle sorularının cevabını belirleyen, veri koruma sisteminin temel değişkenlerini belirleyen ve karar veren gerçek veya tüzel kişi, veri sorumlusudur³⁵¹. Kişisel verilerin korunması kurumu, veri sorumlusunun tespiti noktasında dikkat edilmesi gereken kriterler listesi oluşturmuştur. Buna göre, veri sorumlusunun tespiti için, kişisel verilerin toplanması ve toplama yöntemine, toplanacak kişisel veri türlerine, toplanan verilerin hangi amaçlarla kullanılacağına, hangi bireylerin kişisel verilerinin toplanacağı, toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı, verilerin ne kadar süreyle saklanacağı hususlarında kimin karar aldığıın tespit edilmesi gerekir³⁵². Veri sorumlusu kişisel verileri elinde bulundurmakla bu sıfatı kazanmamakta; bu verilerin işleme amaçlarını ve vasıtalarını belirleyen kişi olması sebebi ile veri sorumlusu sıfatını haiz olmaktadır³⁵³.

Tüzel kişilerde veri sorumlusu her halükarda tüzel kişiliğin kendisidir³⁵⁴. Avukatlık veya mali müşavirlik ofislerinde ise gerçek kişiler veri sorumlusudur³⁵⁵. Bir şirket bünyesinde yer alan birimler tüzel kişi sıfatını haiz değildir. Bu sebeple bu birimlerin veri sorumlusu olduğundan da bahsedilemez. Diğer yandan, bir şirketler topluluğunu oluşturan her bir şirket tüzel kişiliğe sahiptir. Bu sebepler şirketler topluluğunu oluşturan her bir şirketin ayrı ayrı veri

³⁴⁸KVKK, m. 3/1-ç.

³⁴⁹bkz. yukarıda ”2.2.2.Kişi” başlığı.

³⁵⁰ Avrupa Konseyi (1981) . *108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi* [108 Sayılı Sözleşme], m. 2-d. Erişim adresi: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatyid=108> (Erişim Tarihi: 14.03.2025) . KVKK m. 3/1-ı’da veri sorumlusu; “Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade eder.” şeklinde düzenlenmiştir.

³⁵¹Taşan, 2017, s.67.

³⁵² Bununla birlikte, veri sorumlusu yapacağı kişisel veri işleme sözleşmesi ile kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı, kişisel verilerin hangi yöntemle saklanacağı, kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları, kişisel verilerin aktarımının hangi yöntemle yapılacağı, kişisel verilerin saklanması ile ilgili sürelerin doğru uygulanabilmesi için kullanılacak metot, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemlerine ilişkin hususlarda karar verme yetkisini veri işleyene bırakabilir. Kişisel Verileri Koruma Kurumu. *Veri Sorumlusu ve Veri İşleyen Rehberi*, s. 2-3.

³⁵³ Develioğlu, 2017, s. 42.

³⁵⁴30.12.2017 tarihli 30286 sayılı Resmi Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik, m. 11.

³⁵⁵25.11.2001 tarihinde 24594 sayılı Resmi Gazete’de yayımlanan Türkiye Barolar Birliği Avukatlık Ortaklığı Yönetmeliği m.9/2 uyarınca ”Avukatlık Ortaklığı” tüzel kişiliği haizdir.

sorumlusu olarak kabul edilecektir³⁵⁶. Şirketin, sorumluluktan kaçmak için bir yönetim kurulu üyesini veya çalışanını veri sorumlusu olarak ataması mümkün değildir³⁵⁷.

Elektronik ortamda toplanan veriler ile alakalı veri sorumlusunun belirlemesini yapmak giderek zorlaşmaktadır. Bir şirkete örneğin Koç Holding'in Arçelik markasına ait websitesindeki veri sorumlusunun Koç Holding olduğunu tespit etmek kolaydır. Fakat örneğin, yapay zekaya uygulamaları olan web 3.0 uygulamalarında veri sorumlularının tespiti güç bir hal alır. Bu noktada, yapay zekanın veri toplamasını gerçekleştirdiği, veriden kimin istifade ettiğinin tespiti yapılarak veri sorumlusuna ulaşılabilir³⁵⁸. Avrupa Birliği Adalet Divanı (ABAD), arama motoru işleticisinin de veri sorumlusu olduğunu belirlemiştir³⁵⁹.

Veri sorumlularının tespiti, ilgili kişilerin haklarını kim veya kimlere karşı ileri sürebileceği noktasında önem taşımaktadır. Kamu makamı, kamu kurumu veya diğer organlar da veri sorumlusu olabilir(GDPR m.4/7). Veri sorumlusu, veri işlemeye başlamadan önce veri soruluları siciline(VERBİS) kayıt olmak zorundadır(KVKK m.16/2). Ayrıca Kurum'un tesis edeceği düzenleyici işlemler ile kararlara uymak mecburiyetindedir (KVKK m.22).

³⁵⁶Kişisel Verileri Koruma Kurumu. *Veri Sorumlusu ve Veri İşleyen Rehberi*, s. 2-3.s.1. <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen> (Erişim Tarihi: 26.04.2025) .

Buna karşılık, anonim şirketlerde TTK m.367 uyarınca veri sorumlusunun yapacağı işlerin yönetim yetkilerini, yönetim kurulundan birine devredilmesi mümkündür. Taştan, 2017, s.68.

Memiş, T (2017) . Veri sorumlusu ve veri işleyen arasındaki ilişkiler ve sorumluluk düzeni. *Beykent Üniversitesi Hukuk Fakültesi Dergisi*, 3 (6), s.10-11.

13.05.2014 tarihli İspanya vatandaşı Mario Costeja Gonzales'in evinin evinin 1998'de cebrî icra yoluyla açık artırmaya çıkarıldığına dair bir gazete ilanının kişilik hakkını ihlal etmesi sebebi ile 2010 yılında İspanyol Ulusal Veri Koruması Otoritesi'ne başvurması akabinde arama motorunun veri sorumlusu olup olmayacağına ilişkin sorulan görüşte, ABAD 13.05.2014 tarihinde google arama motorunun veri sorumlusu olduğunu tespit etmiştir. AB yaklaşımı, örneğin arama motorlarında kişisel verileri uzun süre tutulması karşısında bireylerin lehine karar verdikleri gözlemlenmektedir. Örneğin: Avrupa Birliği Adalet Divanı (ABAD) (2014) . *Google/İspanya kararı*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131> (Erişim Tarihi: 22.03.2025) . Kararın Türkçe Çevirisi için bkz. Kaya, M. B (2015) . Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 tarihli Google Unutulma Hakkı kararı çevirisi. <https://dergipark.org.tr/en/download/article-file/1671800> (Erişim Tarihi: 22.03.2025) . Daha detaylı bilgi için bkz. Akgül, A (2016) . Kişisel verilerin korunmasında yeni bir hak: Unutulma hakkı ve AB Adalet Divanı'nın Google kararı. *TBB Dergisi*, (116), 27-32; Başalp, N (2015) . Avrupa Birliği Veri Koruması Genel Regülasyonu'nun temel yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21 (1), 99-101.

³⁵⁷Buna karşılık, anonim şirketlerde TTK m.367 uyarınca veri sorumlusunun yapacağı işlerin yönetim yetkilerini, yönetim kurulundan birine devredilmesi mümkündür. Taştan, 2017, s.68.

³⁵⁸ Memiş, T (2017) . Veri sorumlusu ve veri işleyen arasındaki ilişkiler ve sorumluluk düzeni. *Beykent Üniversitesi Hukuk Fakültesi Dergisi*, 3 (6), s.10-11.

³⁵⁹ 13.05.2014 tarihli İspanya vatandaşı Mario Costeja Gonzales'in evinin evinin 1998'de cebrî icra yoluyla açık artırmaya çıkarıldığına dair bir gazete ilanının kişilik hakkını ihlal etmesi sebebi ile 2010 yılında İspanyol Ulusal Veri Koruması Otoritesi'ne başvurması akabinde arama motorunun veri sorumlusu olup olmayacağına ilişkin sorulan görüşte, ABAD 13.05.2014 tarihinde google arama motorunun veri sorumlusu olduğunu tespit etmiştir. AB yaklaşımı, örneğin arama motorlarında kişisel verileri uzun süre tutulması karşısında bireylerin lehine karar verdikleri gözlemlenmektedir. Örneğin: Avrupa Birliği Adalet Divanı (ABAD) (2014, 13 Mayıs) . *Google/İspanya kararı*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131> (Erişim Tarihi: 22.03.2025) . Kararın Türkçe Çevirisi için bkz. Kaya, M. B (2015) . Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 tarihli Google Unutulma Hakkı kararı çevirisi. <https://dergipark.org.tr/en/download/article-file/1671800> (Erişim Tarihi: 22.03.2025) . Daha detaylı bilgi için bkz. Akgül, A (2016) . Kişisel verilerin korunmasında yeni bir hak: Unutulma hakkı ve AB Adalet Divanı'nın Google kararı. *TBB Dergisi*, (116), 27-32; Başalp, N (2015) . Avrupa Birliği Veri Koruması Genel Regülasyonu'nun temel yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21 (1), 99-101.

Yapay zeka tabanlı uygulamalarda işlenen kişisel verilerde, yapay zekaya ilişkin sistemin geliştiricisi ve/veya sahibinin veri sorumlusudur³⁶⁰. Konuya e-ticaret platformlarında kullanılan YZ tabanlı uygulamalar bakımından yaklaşıldığında söz konusu e-ticaret şirketlerinin veri sorumlusu olduğu ve verilerin YZ uygulamasında eğitim veri setleri oluşturmak için saklanması durumlarında veya bu verilerle uygulama sürümlerinin güncellendiği durumlara ilişkin YZ geliştiricilerinin de veri sorumlusu olduğu söylenebilir.

Dikkat çekmek istediğimiz bir nokta, KVKK'da veri sorumlusunun “kişi” olarak tanımlanmış olduğudur. GDPR ve 95/46/EC sayılı Yönerge’de ise birlikte veri sorumlusu kavramına yer verilmiştir. Bu durum, Avrupa bünyesinde şirketler topluluğunda veri paylaşımı yapılabilme yolunun açıkken Türk hukuku bakımından böyle olmadığı çıkarıma götürülebilir³⁶¹.

2.5.3. Veri işleyen

Veri işleyen(“*processor*”), veri sorumlusu adına kişisel verileri işleyen bir gerçek veya tüzel kişidir(GDPR, m. 4/8; KVKK, m. 3/1-ğ.). Yani veri işleyen, veri sorumlusunun kişisel verilerin işlenmesi konusunda belirlediği ne, nasıl, niçin, hangi sürelerle sorularının cevaplarını oluşturan parametreler doğrultusunda verileri işleyen kişiyi ifade etmektedir³⁶². Kişisel verileri ancak veri sorumlusunun verdiği yetki ve talimatlarla işleyebilen veri işleyen, mevzuat gerekliliklerinin yerine getirilmesini ve veri öznesinin haklarının korunmasını sağlayacak biçimde uygun teknik ve kurumsal tedbirler uygulamakla yükümlüdür (GDPR, m.28/1).

Veri işleyen tanımından hareketle her ne kadar veri sorumlusu ile hiyerarşik bir altlık üstlük ilişkisi varmış gibi gözükse de; böyle olmadığı durumlar da vardır. Nitekim, veri işleyen, veri sorumlusunun çalışanı olabileceği gibi veri sorumlusunun organizasyonu dışında hizmet sunan gerçek veya tüzel kişi de olabilir³⁶³. Veri sorumlusu organizasyon bakımından tektir fakat veri işleyen aynı anda birden fazla şirketin veri işleyeni olabilmektedir³⁶⁴. Bunun yanı sıra bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu, hem de veri işleyen olabilir. Örneğin, bir muhasebeci kendi çalışanları hakkında işlediği kişisel verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin işlediği kişisel veriler bakımından veri işleyen olarak kabul edilir³⁶⁵.

Elektronik ticaret yapan bir şirketin satış gerçekleştirebilmek için bir ödeme hizmeti şirketi ile anlaşması durumunda, söz konusu ödeme hizmeti şirketi, satıcının veri işleyeni değildir. Ödeme şirketi, işlediği veriler bakımından veri sorumlusu olarak sorumlu olur. Nitekim, ödeme hizmeti şirketi; müşterilerden hangi verilerin toplanması gerektiğine karar vermekte, toplanan verilerin hangi amaçla kullanılacağı konusunda kontrol sahibi olmakta,

³⁶⁰Badur, E (2024) . Yapay zeka sistemleri kullanılarak yapılan işleme faaliyetlerinde kişisel verilerin korunması. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 32 (4), s.2525-2560.

³⁶¹Memiş, 2017, s.12-13.

³⁶² Taştan, 2017, s.68.

³⁶³Bu durum, kişisel verilerin işlenmesi bağlamında akdi ve haksız fiil sorumluluğun belirlenmesi açısından önemlidir. Nitekim, veri işleyenin organizasyon dışında bir üçüncü kişi olması durumunda, veri sorumlusu ile veri işleyen arasında veri işleme sözleşmesi gündeme gelecektir. Diğer yandan, veri işleyenin, veri sorumlusunun bir çalışanı olması durumunda, ilgili kişi KVKK'da düzenlenen hakları yanında, 6098 sayılı TBK m.66 uyarınca adam çalıştırmanın sorumluluğuna da gidebilecektir. Taştan, 2017, s. 69.

³⁶⁴ Memiş, 2017s.10-11.

³⁶⁵KVKK Gerekçesi, m.3; Kişisel Verileri Koruma Kurumu (2025) . *Madde ve gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve kişisel verilerin korunmasına ilişkin terimler sözlüğü*. KVKK Yayınları, s.11 ; Kişisel Verileri Koruma Kurumu. Veri Sorumlusu ve Veri İşleyen, KVKK Rehberi, s.2.

satıcıdan bağımsız olarak doğrudan kişisel verileri işlenen müşterilere uyguladığı kendi hüküm ve şartları bulunmakta ve son olarak satıcı Şirketten bağımsız olarak tabi olduğu hukuki yükümlülükler(örneğin; kredi kartı bilgilerinin silinmesi) bulunmaktadır³⁶⁶.

Veri işleyen veri işlenmesi konusunda karar mekanizması değildir, verilerin işlenmesindeki teknik kısım ile faaliyetleri sınırlıdır³⁶⁷. Uygulamada veri işleyenler, bu alanda uzmanlaşmış bilişim şirketleri olduğu görülmektedir. Veri sorumlusu şirketler genellikle bu alanda faaliyet gösteren bilişim şirketleri ile anlaşır. Bu bağlamda, bilişim şirketleri, veri işleyen olarak kabul edilirler. Örneğin, bir şirketin, kurum e-posta hesaplarının yedeklenmesi amacıyla sözleşme yaptığı bulut bilişim şirketi(Google Drive, Onedrive, Dropbox) şirketten aldığı talimatla verileri işleyen, veri kişisidir³⁶⁸.

2.6. Kişisel Verilerin İşlenmesi

Kişisel verilerin hukuki korumadan faydalanabilmesi için tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi gerekmektedir(GDPR m.2; KVKK m.2.). Kişisel verilerin işlenmesinden, bu verilerin toplanması, kaydedilmesi, düzenlenmesi, yapılandırılması, depolanması, silinmesi veya tahrip edilmesi, uyarlanması veya değiştirilmesi, bu verilere erişilmesi, verilerin geri getirilmesi, yayılması veya başka bir şekilde ulaşılabilir hale getirilmesi, kullanılması, iletim yoluyla açıklanması, uyumlaştırılması ya da birleştirilmesi, kısıtlanması, kalıcı olarak silinmesi veya imha edilmesi gibi işlemler anlaşılmalıdır. Bu işlemler sınırlı(“*tahdidi*”) şekilde sayılmamış, veriler üzerinde gerçekleştirilen her türlü eylemin işleme olarak kabul edileceği ifade edilmiştir (GDPR, m.4/2; 95/46/EC sayılı Direktif m. 2/b; KVKK m.3/1-e.). Anlaşılan odur ki, kişisel verilerin işlenmesi kavramı geniş bir alanı kapsamaktadır. Öyle ki, bu kavram, kişisel verilerin ilk defa elde edilmesinden(toplanmasından) başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ve imha edilmesi sürecini de kapsamaktadır³⁶⁹. Ezcümle, kişisel veriler üzerinde yapılan her türlü işlem, kişisel verilerin işlenmesi kapsamına girerek hukuki korumadan faydalanır.

Otomatik, kısmen otomatik veya bir veri sisteminin parçası olmak şartıyla otomatik olmayan yöntemler kullanılarak verilerin işlenmesi mümkündür. Burada otomatik ve otomatik olmayan yöntemlerden ne anlaşılması gerektiğinin tespiti gereklidir. Otomatik işleme, 108 sayılı Sözleşme³⁷⁰'sine göre, “*kısmen veya tamamen otomatik yöntemlerle verilere aritmetik işlemler uygulanması, verilerin değiştirilmesi, silinmesi veya dağıtılması*” işlemidir. Buna göre, günümüzde yaygın olarak kullanılan bilgisayarlar, tabletler veya akıllı telefonlar vasıtası ile yapılan veri işleme faaliyeti otomatik yöntemle yapılan işlemeye örnek verilebilir³⁷¹.

Diğer yandan, kişisel verilerin işlenmesi yalnızca teknoloji ile ilişkili değildir. Elle (manuel olarak) yani geleneksel olarak işlenen verileri de kişisel verilerin korunması kapsamına

³⁶⁶ Kişisel Verileri Koruma Kurumu.Verdi Sorumlusu ve Veri İşleyen, KVKK Rehberi, s.7.

³⁶⁷Veri işlemenin neden ve nasıl yapılacağına “*Veri Sorumlusu*” karar verir. Kişisel Verileri Koruma Kurumu. Veri Sorumlusu ve Veri İşleyen, KVKK Rehberi, s.2.

³⁶⁸ Selek, 2021, s.125, Taştan, 2017, s.69; Kişisel Verileri Koruma Kurumu.Verdi Sorumlusu ve Veri İşleyen, KVKK Rehberi, s.10.

³⁶⁹bkz. KVKK, m.3 gerekçesi.

³⁷⁰ Council of Europe (1981) . *Convention for the protection of individuals with regard to automatic processing of personal data (No. 108)* . Strasbourg. m. 2/1-c. <https://rm.coe.int/1680078b37> (Erişim tarihi: 19.03.2025)

³⁷¹Selek, 2021, s.22.

95/46/EC sayılı Direktifi, m.8/1'de: "Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır." ifadesine yer vererek tahdidi surette sayarak hassas nitelikteki kişisel verilerin kapsamını belirlemiştir. Sayılanlara ek olarak, GDPR m.9/1'de "kişilerin ticari birliklere üyeliğini ortaya koyan bilgiler" ile "biyometrik verileri" de kapsama dahil edilmiş ayrıca m.10'da mahkumiyet kararlarına, işlenen suçlara ve kişiye ilişkin güvenlik tedbirlerine ilişkin özel bir düzenleme getirilmiştir. Türk hukuku bakımından, KVKK m.6/1 ile " vakıf veya dernek üyeliği", " kılık kıyafet", " mezhep" ve "ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler" de hassas nitelikli veri olarak sayılmıştır. Dolayısıyla, ulusal ve uluslararası düzenleyici metinlerden hareketle³⁸⁰ kişinin "ırkı, etnik kökeni, siyasi görüşü, felsefi inancı, dini, mezhebi veya diğer inançları, sendika üyeliğini"³⁸¹ açığa çıkaran verileri ve bir gerçek kişinin kimliğini benzersiz bir şekilde belirleyen genetik veriler ile biyometrik verileri, sağlık verileri veya bir cinsel yaşamı veya cinsel eğilimine ilişkin verileri, ceza mahkumiyeti ve güvenlik tedbirleri, genetik ve biyometrik verileri" hassas nitelikte kişisel veridir. Özel nitelikli kişisel veriler, tahdidi olarak sayılmıştır. Dolayısıyla yoruma dayalı olarak kapsamının genişletilmesi mümkün değildir³⁸².

Avrupa düzenlemelerinde yer almayan "kılık ve kıyafet" verisinin Türkiye coğrafyasında özel nitelikli veri olarak kabul edilmesi, meseleye coğrafi ve tarihsel bir yaklaşımla bakıldığında oldukça isabetlidir. Nitekim, kılık kıyafeti sebebiyle ayrımcılığa maruz kalınan bu coğrafyada gerçek kişilerin bu verilerinin işlenmesi fişlenmeye yol açacak ve ayrımcılık yasağına aykırılık meydana getirebilecektir. Bununla birlikte, bir e-ticaret şirketinin pazarlama analiz çalışmalarının yürütülmesi kapsamında tüketicilerin satın aldığı kıyafet verilerinin işlenmesi bu verilerin özel nitelikli veri olması sebebi ile daha sıkı bir koruma altında ve sınırlı amaçlar ile işlenebilecektir³⁸³.

Genetik veriler³⁸⁴ ile biyometrik veriler³⁸⁵ kişisel verilerin korunması başlığı altında ayrıca incelenmelidir. Genetik veriler, kişinin biyolojik özelliklerini ortaya koyduğu gibi öz ebeveynleri, kardeşleri ve çocukları hakkındaki özelliklerin yanı sıra kan bağı olan akrabalarına(biyolojik aile) ve ait olduğu etnik gruba ilişkin de bilgi vermektedir³⁸⁶. Günümüzde genetik bilgi, hastalıkların önlenmesi ve iyileştirilmesinde sağlık alanında

özgürlüklere yönelik önemli riskler oluşturabileceğinden özel korumayı hak eder... Üye Devletlerin hukukunda veri korumaya ilişkin spesifik hükümlerin olabileceği dikkate alınarak, bu Tüzük'te belirtilen özel durumlarda işlemeye izin verilmedikçe, bu tür kişisel veriler işlenmemelidir. "; KVKK m. 6/3: "Özel nitelikli kişisel verilerin işlenmesi yasaktır. " şeklinde düzenlenmiştir.

³⁸⁰GDPR, m.9/1; KVKK m.6/1; 95/46/EC sayılı Direktif m.8; 108 nolu Avrupa Konseyi Sözleşmesi m.6.

³⁸¹ Ancak işçinin işe alınmasından sonra sendikal haklarından yararlanması için Sendika üyeliğinin sorulması hukuka aykırı değildir. Selek, 2021, s.30.

³⁸² Kaya, 2011, s. 319.

³⁸³bkz. GDPR m.9 ve KVKK m.6.

³⁸⁴Genetik veri, bir bireyin kalıtsal özelliklerine veya ilgili bir birey grubu içinde bu özelliklerin kalıtım modeline ilişkin her türlü veri olarak tanımlanabilir. Council of Europe (1997, 13 Şubat) . Recommendation No. R (97) 5 on the protection of medical data (m. 1) . <https://rm.coe.int/cmrec-97-5-on-the-protection-of-medical-data/1680a43b64> .

³⁸⁵ Biyometrik veriler; yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin kimliğinin benzersiz şekilde belirlenmesini sağlayan veya bunu teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak belirli teknik işleme ile ortaya çıkan kişisel verilerdir. GDPR m.4/14.

³⁸⁶ Article 29 Working Party, Working Document on Genetic Data, 17.05.2004, s.4; İngilizce tam metin için bkz. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf . Erişim Tarihi: 22.03.2025. ; Gostin, L. O (1995) . Genetic privacy. *Journal of Law, Medicine & Ethics*, 23, s.320.

insanlığın yaşam kalitesini artırmak için sahip olduğu en güçlü araçlardan biridir³⁸⁷, ne var ki bu bilgiler insan haklarını ihlal etmek için de kullanılabilir³⁸⁸. Örneğin, sigorta şirketleri, genetik ve sağlık verilerini isteyerek; kişilerin sağlık bilgileri ve hastalık teşhisleri ile risk analizi yaparak kişilerin tahmini yaşam sürelerini hesaplamakta bu da kişinin sigorta için fahiş fiyatlar ödemesine veya hiç sigortalanamamasına sebep olarak genetik verilere dayanan ayrımcılığı ortaya çıkarmaktadır³⁸⁹. Genetik bilgilerin ifşası, potensiyel damgalanmayı ve ayrımcılığı beraberinde getirir. İhlale uğrayan kişiler, işini, evini veya sigorta kaybı yaşayabilir ayrıca bu durum utanç ile beraber sosyal izolasyon ve özsaygı kaybına yol açabilir. DNA bilgilerinden erişilebilen uyuşturucu bağımlılığı, zeka geriliği, alkol bağımlılığı gibi durumlarda ise kişinin sosyal hayatında mağdur olmasının etkisi daha büyüktür³⁹⁰. Açıkçası, genetik verilerin kullanımı genişletir; araştırma, analiz ve diğer sebepler ile aktarılan genetik kişilerin verilerinin olası kullanımına ilişkin kişiler gerekli ve yeterli bilgilendirme yapılmaması ve bu sebeple uygun açık rıza alınmaması da ihlale sebebiyet verir³⁹¹.

Bugün üniversiteler bünyesinde araştırmalardan elde edilen genetik veriler depolanabildiği gibi ticari şirketler de genetik veri bankacılığı yaparak genetik verileri araştırmacılara ve bireylere bir hizmet olarak sunmaktadır³⁹². Böylece kişinin kendisi ve ailesine ilişkin bilgileri içeren ve kişilik hakları ile ilişkili olan veriler metalaştırılmakta ve pazar malzemesi haline gelmektedir. Bir defa elde edilen genetik verinin yeniden kullanım riskleri ve

³⁸⁷Nitekim, genetik hastalıklarda, Kalıtsal hastalıklarda, ebeveyne ait hastalık verisi çocuğun da hastalığına işaret edebilir. Örneğin Huntington hastalığı (HD) ile ilgili olarak, ebeveynlerden biri HD hastasıysa, çocuk bu ebeveynin HD kalıtım riski %50'dir. Selita, F (2019) . Genetic data misuse: Risk to fundamental human rights in developed economies. *Legal Issues Journal*, 7 (1), s.62. Genetik bilgi, bunun yanı sıra tedavi, beslenme alışkanlığı ve düzeni, yaşam tarzı ve üreme tercihleri gibi konularda hayati öneme sahiptir. Gostin, 1995, s.323.

³⁸⁸Gostin, 1995, s. 320-321. Askeri gelişim için de genetik veriler kullanılabilir. Örneğin, Amerikan ordusunda genetik veriler askerlerin stres seviyelerini, tahammül seviyelerini, sağlığını, fiziksel ve psikolojik durumlarını tespit etmek ve performanslarını arttırmak için kullanılmaktadır. Genetik bilgiler, potansiyel sağlık veya davranış sorunlarına yönelik erken müdahalelerin uygulanması için kullanılmaktadır. Örneğin, suçla mücadele bunlardan biridir. Antisozyal davranışa genetik eğilimi sebebiyle müdahale edilebilmesi ve suç işlenmesinin böylece önüne geçilmesidir. Bu durumlar, insan hakkı ihlallerini ortaya çıkarabilmektedir. Nitekim, genetik faktörler olasılıklar üzerine kuruludur. Bir bireyin suç işleme riskinin %50, %70 veya daha fazla olması durumunda insan haklarının ihlal edilerek kişi hakkında gözetleme yapılabilir mi? Selita, 2019, s.57-58. Kanaatimizce bu yaklaşım bir cadı avına dönüşebilir ve dogmatik tehlike suçluları yeniden tarih sayfasında kendini göstererek, insan hakları çoğu zaman bir hiç uğruna ihlal edilebilir hale gelir.

³⁸⁹Selita, 2019, s. 58-59, 74-75; Article 29 Data Protection Working Party (2004) . *Working document on genetic data*. Brussels: European Commission. Retrieved from, s.10. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf . Bu konudaki Amerika'daki ve Birleşik Krallık'taki mevzuat yetersizliği eleştirilmiştir. Selita, 2019, s. 74-75. Genetik verilere dayanan her türlü ayrımcılık yasaklanmıştır. Bu husus, Avrupa Konseyi, Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi, 1997, m.11 'de düzenlenmiştir. İlgili Sözleşme'nin İngilizce tam metni için bkz. Council of Europe (1997) . *Convention for the protection of human rights and dignity of the human being with regard to the application of biology and medicine: Convention on human rights and biomedicine (Oviedo Convention)* . Retrieved from <https://rm.coe.int/168007cf98> . Aynı yönde bkz. Unesco, İnsan Genomu ve İnsan Hakları Evrensel Bildirgesi, m.6. Bildirinin Türkçe metni için bkz. UNESCO (1997) . *Universal Declaration on the Human Genome and Human Rights*. Retrieved from <https://www.unesco.org.tr/Pages/459/73/%C4%B0nsan%20Genomu%20ve%20%C4%B0nsan%20Haklar%C4%B1%20Evrensel%20Bildirgesi>. Benzer şekilde işverenler, işçilerin beyan edilen veya testler neticesinde tespit edilen hastalıklar sebebi ile işçileri istihdam etmekten kaçınabilmektedir. Nitekim Uygulamada, işverenler çalışanın sağlık masrafları ve emekliliğine ilişkin kendisine yük olup olmayacağı riskini değerlendirmek için hukuka aykırı olsa da bu uygulamayı yapabilmektedir. Gostin, 1995, s.321; Article 29 Working Party, Working Document on Genetic Data, s.10.

³⁹⁰Gostin, 1995, s.324.

³⁹¹ Article 29 Working Party, Working Document on Genetic Data, s.7; Selita, 2019, s.56;

³⁹² Gostin, 1995, s.322.

ait olduğu kişiyi uyumsuz kullanımlarda ifşa tehlikeleri vardır³⁹³. Kişiyi ait fotoğrafın işlenmesi tek başına hassas kişisel verilerin işlenmesi anlamına gelmemektedir. Fotoğraf, yalnızca bir gerçek kişinin kimliğinin benzersiz bir şekilde belirlenmesine veya doğrulanmasına izin veren belirli bir teknik yolla işlendiğinde biyometrik verilerin tanımı kapsamında yer alırlar³⁹⁴.

2.7.2. Genel nitelikli kişisel veriler (Hassas olmayan kişisel veriler)

Özel nitelikli kişisel verilerin dışında kalan veriler genel nitelikli (hassas olmayan) kişisel veriler olarak sınıflandırılır³⁹⁵. Esasen düzenleyici metinlerde bu ifade kullanılmamış olsa da tasnifte ve dolayısıyla uygulamada kolaylık olması açısından bu ayrıma gidilmiştir. Çalışmamızda "Kişisel Veri Tanımı ve Unsurları" başlığı altında yaptığımız açıklamalar, genel nitelikli veriler için aynen geçerlidir.

2.8. Kişisel Verilerinin Korunmasına İlişkin Hukuki Düzenlemeler

1970'li yıllarda bilişim teknolojilerinin gelişmeye başlaması ile devlet ve kamu tüzel kişiliklerinin yanında özel şirketlerin de artan hızla kişisel verileri işlemesi karşısında kişisel verilerin korunması alanında düzenleme yapılmasına ihtiyaç duyulmuştur³⁹⁶. Uluslararası düzenlemeler ve ulusal çapta mevzuat çalışmaları yapılmış; bağlayıcı hukuk normları ile kişisel verilerin korunması hakkı tanınmıştır. Aşağıda bu hususlar detaylandırılmıştır.

2.8.1. Uluslararası düzenlemeler

Kişisel verilerin korunmasına ilişkin ilk düzenlemeler, 1970'li yıllarda Batı Avrupa'da baş göstermiştir. Bu tarih, bilgisayarın ve merkezi veri tabanlı sistemlerin vatandaşların verilerini işlemeleri ile aynı zamana denk gelmektedir³⁹⁷. Bu tarihten sonra kişisel verilerin korunması alanında başta Avrupa olmak üzere birçok çalışma ve düzenleme yapılmıştır. Çalışmamız kapsamında temel olarak kapsam olarak Kıta Avrupası düzenlemeleri ele alınsa da kişisel verilerin korunmasına ilişkin düzenlemelerle bugün dünyanın her yerinde karşılaşmaktayız³⁹⁸. Bu başlık altında, özellikle Avrupa düzenlemeleri ele alınmıştır³⁹⁹.

³⁹³ Article 29 Working Party, Working Document on Genetic Data, s.6-11. Bir diğer mesele, DNA dizilimi yapıldıktan sonra genotipleme bilgilerinin güvenliği meselesidir. Nitekim, tek bir genom, saklanması (ve muhtemelen yedeklenmesi) gereken ve bireyin yaşamı boyunca ve sonrasında kullanılabilecek yaklaşık 725 megabaytlık veriyi temsil etmektedir. Bu verilerin güvenliğinden ve gizliliğinin sağlanamaması için kişisel veri işleme amaçlarının kesin ve açık şekilde ortaya konması gerekmektedir. Selita, 2019, s.57. Ayrıca kişinin verisinden, genetik bağlamda açığa çıkan akrabaların da "ilgili kişi (veri öznesi)" kabul edilmesi ile veya ilgili kişinin haklarına sahip olması ya da farklı nitelikteki bir bilgi edinme hakkı ile bu veri üzerinde söz sahibi olması sağlanmalıdır. Article 29 Working Party, Working Document on Genetic Data, s.8-9,14; Prins, 2006, s. 295.

³⁹⁴ GDPR, giriş, para. 51.

³⁹⁵ Selek, 2021, s. 26.

³⁹⁶ Develioğlu, 2017, s. 6.

³⁹⁷ Küzeci, E (2011) . Anayasal bir hak: Kişisel verilerin korunması. *Türkiye Bilişim Derneği Bilişim Dergisi*, s.143-144.

³⁹⁸ Pek çoğu yeni tarihli olan bu düzenlemelerin bir kısmını şu şekilde saymak mümkündür: California Tüketici Gizliliği Yasası (CCPA); Kanada Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (PIPEDA); Avustralya Kişisel Verilerin Korunması Yasası (Privacy Act); Japonya Kişisel Bilgilerin Korunması Yasası (APPI); Güney Kore Kişisel Verilerin Korunması Yasası (PIPA); Çin Kişisel Bilgilerin Korunması Yasası (PIPL); Endonezya Kişisel Verilerin Korunması Yasası (PDP Law) .

³⁹⁹ Ayrıntılı bilgi için bkz. Kişisel Verileri Koruma Kurumu (2025) . *Kişisel Verilerin Korunması Kanunu'na İlişkin Uygulama Rehberi* (Yay. No. 58, ss. 16–19) . KVKK Yayınları. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF> (Erişim Tarihi: 25.03.2025); Kişisel Verileri Koruma Kurumu. *Kişisel verilerin korunması alanında uluslararası ve ulusal*

2.8.1.1. Avrupa ekonomik işbirliği örgütü (OECD)

1980 yılında Avrupa Ekonomik İşbirliği Örgütü (OECD), kişisel verilerin otomatik işlenmesine ilişkin *"Mahremiyetin Korunmasına ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri"*⁴⁰⁰ yayımlaması ile kişisel veri hukuku gelişme göstermiştir. Esasen bağlayıcılığı olmayan bu ilkeler dünya çapında kişisel verilerin korunması konusunda kabul edilen ilk düzenleyici belgedir⁴⁰¹. Bu belge ile kişisel verilerin sınır ötesi dolaşımına ilişkin temel ilkeler belirlenmiştir⁴⁰². Ulusal yasaların ve politikaların farklılık göstermesi karşısında mahremiyetin ve bireysel özgürlüklerin korunması için ülkelerin ortak çıkara sahip olması ve veri akışına ilişkin temel asgari prensipleri kabul edilmesinin gerekliliğine yapılmıştır. OECD Rehber İlkelerinde, kişisel verilerin korunmasına ilişkin 8 prensip kabul edilmiştir⁴⁰³:

1. Verilerin Toplanması Sınırlı Olması (m.7): Kişisel verilerin toplanması bazı sınırlara tabi olmalıdır. Bu veriler ancak yasal ve adil koşullar altında, hukuka ve dürüstlük kuralına uygun şekilde ve ilgilinin rızası ile toplanmalıdır.

2. Verilerin Kaliteli Olması (m.8): Kişisel veriler toplanma amaçları ile uygun şekilde işlenmeli, gerekli olduğunda ölçülü şekilde kullanılmalı ve doğru, tam ve güncel olmalıdır.

3. Veri İşleme Amacının Belirli Olması (m.9): Kişisel verilerin işleme amacı belirli olmalı ve bu amaç en geç veri toplanması esnasında ilgili kişiye ve bilmesinde hukuki menfaati bulunan kişilere belirtilmelidir. Veri işleme amacının değişmesi halinde bu değişiklik ilgili kişiye bildirilmeli ve sonraki amaç değiştirilen amaç ile açık şekilde bağdaşmaz olmamalıdır.

4. Veri Kullanımının Sınırlı Olması (m.10): Kişisel veriler ifşa edilemez ve başkasının erişimine açılmaz. Kişisel veriler toplama amacı dışındaki sebepler ile işlenemez. Ancak yasaların belirmesi veya ilgili kişinin rızası söz konusu olduğunda kişisel veriler m.9'da belirlenen ve açıklanan amaçlar dışında da işlenebilmesi hali saklıdır.

5. Veri Güvenliğinin Sağlanması (m.11): Veri sorumlusu, kişisel verilerin kaybolması, bu verilere yetkisiz şekilde erişilmesi, verilerde değişiklik yapılması, imha edilmesi, kullanılması ifşa edilmesi gibi risklere karşı makul güvenlik önlemlerini almakla yükümlüdür.

6. Verilerin Açık ve Anlaşılabilir Olması (m.12): İlgili kişinin bilgi edinme hakkı karşısında işlenen kişisel veri türleri, kapsamı, nitelikleri ve işleme amaçları hazır bulundurulmalıdır. Ayrıca, veri sorumlusu ile iletişime geçilme yolları açılmalı ve bu kapsamda veri sorumlusunun adı ve olağan ikamet adresi ilgili kişinin erişimine açık bulundurulmalıdır. Veri açıklığı ilkesi, sayılan hususların kolaylıkla belirlenebilir olması anlamını taşımaktadır.

7. İlgili Kişinin Katılımı (m.13): İlgili kişi, hangi verilerinin işlendiğini öğrenme ve kişisel verilerinin silinmesi, düzeltilmesi, tamamlanması veya değiştirilmesini talep haklarına sahiptir.

düzenlemeler. KVKK Rehber Yayınları. <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Düzenlemeler> (Erişim Tarihi: 24.04.2025).

⁴⁰⁰Organisation for Economic Co-operation and Development (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing. https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html (Erişim Tarihi: 23.04.2025).

⁴⁰¹Aksoy, 2010, s.4; Taştan, 2017, s. 10.

⁴⁰²Aygözer Öngün, 2019, s.67; Şimşek, 2008, s.12; Develioğlu, 2017, s. 6-7.

⁴⁰³ŞİMŞEK, s.15-16; Selek, 2021, s.35-37; Aygözer Öngün, 2019, s.68-69; Develioğlu, 2017, s. 7-8.

8. Hesap Verilebilirlik İlkesi (m.14): Veri sorumlusu, veri güvenliğine ilişkin alınan önlemlerin uygunluğu ve sayılan 7 prensibin işlerliği noktasında hesap verebilir olmalıdır. Bu prensiplere uyulması veri sorumlusunun sorumluluğundadır.

2.8.1.2. Birleşmiş milletler

Birleşmiş Milletler (BM) nezdinde 1948'de "İnsan Hakları Evrensel Beyannamesi"⁴⁰⁴ kabul edilmiş böylece kişisel mahremiyeti koruma ilkesini benimsemiştir. Bu ilke ile özellikle kişilerin özel yaşamına yapılan keyfi müdahaleleri yasaklamıştır. Nitekim, Beyanname 12. madde: "Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır." şeklinde düzenlenmek sureti ile kişisel veriler de özel yaşam kapsamı içinde koruma altına alınmıştır⁴⁰⁵. 04.12.1990 tarihinde ise BM Genel Kurulu, "Bilgisayar Ortamındaki Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Yönerge"⁴⁰⁶ (BM Rehber İlkeleri) yayımlanmıştır. Yönergede, hukuka uygunluk, dürüstlük, belli amaçlar ile işleme, ayrımcılık yasağı gibi ilkelere ve kamu ve özel sektöre ilişkin düzenlemelere yer verilmiştir⁴⁰⁷. Kişisel verilere ilişkin kabul edilen her ilkeyi ayrıntılı şekilde açıklayan Yönerge'de 9 temel ilke kabul edilmiştir⁴⁰⁸:

1. Yasallık ve dürüstlük: Kişisel veriler kanuna aykırı ve dürüstlük kuralına aykırı şekilde toplanmamalıdır. Veriler toplanma amacına ve temel hak ve özgürlüklere aykırı şekilde kullanılmamalıdır (m.1)
2. Doğruluk: Kişisel verilerin toplanmasından, saklanmasından ve işlenmesinden sorumlu olanlar verilerin doğruluğunu kontrol etmekle ve eksiksiz şekilde saklamakla yükümlüdür. İşlenme sırasındaki kontrolden sonra düzenli aralıklarla bu verilerin doğruluğu ve güncelliği kontrol edilmelidir (m.2)
3. Amacın Belirli, Açık ve Haklı Olması: Veri işleme sırasında verisi işlenen kişi, verilerin işlenme amacı hakkında bilgilendirilmelidir. Kişisel veriler ancak amaçla bağlantılı olarak işlenebilir, bu amaç meşru sebeplere dayandırılmalıdır. Kişisel verilerin saklanma süreleri, amacın gerçekleştirilmesi için gereken süreyi geçemez (m.3)

⁴⁰⁴ United Nations (1948) . *Universal Declaration of Human Rights*. <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (Erişim Tarihi: 25.03.2025) . Türkçe çevirisi için bkz. HSK. *İnsan Hakları Evrensel Beyannamesi* [Türkçe çeviri]. <https://www.hsk.gov.tr/eklentiler/dosyalar/9a3bfe74-cdc4-4ae4-b876-8cb1d7eeae05.pdf> (Erişim Tarihi: 25.03.2025) .

⁴⁰⁵Selek, 2021, s.37.

⁴⁰⁶ United Nations General Assembly (1990, December 14) . *Guidelines for the regulation of computerized personal data files*. <https://www.refworld.org/policy/legalguidance/unga/1990/en/13761> (Erişim Tarihi: 25.03.2025) .

⁴⁰⁷Şimşek, 2008, s.16.

⁴⁰⁸İlkeler ve açıklamaları için bkz. ayrıca bkz. Aygözer Öngün, 2019, s.70-71.

4. İlgili Kişinin Erişim Hakkı: Kişisel verileri işlenen kişiler kimliğini kanıtlamak koşulu ile kişisel verilerine erişme, hangi kişisel verilerinin işlendiğini öğrenme, doğru veya güncel olmayan kişisel verilerini düzeltme veya koşullarının varlığı halinde kişisel verilerinin yok edilmesini isteme hakkına sahiptir. İlgili kişinin bu talepleri karşısında masraf yapması gerekmez ve taleplerine gecikmeksizin cevap verilir. Bu ilkenin uygulanmasında ilgili kişinin uyruğu veya ikamet yerine ilişkin ayrım yapılamaz (m.4)
5. Ayrımcılık Yasağı: Ayrımcılığa yol açabilecek kişilerin ırkı ve etnik kökeni, cinsel yaşamı, siyasi görüşü, dini ve felsefî inançları ile denek ve sendika üyeliğine ilişkin veriler ancak kanunun izin verdiği ve gerekli hallerde işlenebilir (m.5)
6. İstisna Koyma Yetkisi: 1-4 numaralı ilkelere istisnalar ancak kamu düzeni, milli güvenlik, halk sağlığı, genel ahlak sebepleri ile veya temel hak ve özgürlükleri korumak için özellikle zulüm gören kişileri koruma için (insani yardım) gerekli olduğu durumlarda ve ancak kanun ile getirilebilir (m.6)
7. Güvenlik: Kişisel veri dosyaları hem yetkisiz erişim, verilerin kötüye kullanılması veya virüslerin kontaminasyonu gibi insani hem de sistemin çökmesi veya arızalanması kaynaklı silinme veya imha gibi bilgisayardan kaynaklı tehlikelere ve doğal afetlere karşı korunma altına alınmalı, gerekli ve yeterli tedbirler sağlanmalıdır (m.7)
8. Denetim ve Yaptırım: BM Rehber İlkelerine uyumun denetlenebilmesi için her ülke kendi iç hukuk düzenlemesinde yasal olarak yetkili denetim mekanizmaları oluşturmaktadır. Bu demetin organları adil, tarafsız ve yetkin olmalıdır. Sayılan ilkelere aykırılığın tespit edilmesi durumunda konuya özgü oluşturulacak güvenlik tedbirleri ve cezai müeyyideler uygulanmalıdır (m.8)
9. Sınır Ötesi Veri Akışı: Kişisel verilerin işlendikleri ülkeden başka bir ülkeye transferleri ancak bu iki veya daha fazla ülkede kişisel verilerin genel ve özgü anlamında transferine izin verilen düzenlemenin mevcut olması gereklidir. Transfer ülkedeki kişisel verilerin korunması düzeyi işlenen ülkedeki korumadan daha aşağıda olmamalıdır (m.9)

BM Rehber ilkeleri yukarıda sayılan ilkelerin kural olarak gerçek kişilere ait kişisel veriler için geçerli olduğunu fakat korumanın tüzel kişi verilerini de kapsayacak şekilde genişletilebileceğini düzenlemiştir (m.10). Ayrıca, hükümet dışı uluslararası kuruluşların da ilkelere uyum sağlaması gerektiğinin altı çizilmiştir. Bu belge ile kişisel verilerin korunmasına ilişkin bağımsız bir denetleyici mekanizma olmasının öngörülmesi ise ayrı bir önem taşımaktadır.

2.8.1.3. Avrupa konseyi

Avrupa Konseyi, 04.11.1950 tarihinde Roma’da imzalanıp 3 Eylül 1953’te yürürlüğe giren Avrupa İnsan Hakları Sözleşmesi’ni (AİHS)⁴⁰⁹ doğrudan doğruya kişisel verilerin korunmasına ilişkin bir düzenleme içermese de Avrupa Konseyi’nin yasal aracı olan AİHM geliştirdiği içtihatlarla AİHS m.8 ”Özel Hayata ve Aile Hayatına Saygı Hakkı” kapsamında kişisel verilerin korunması hakkını koruma altına almıştır. AİHS’in ”Özel ve Aile Hayatına Saygı Hakkı” başlıklı 8. maddesi:

“ 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.” şeklindedir.

Esasen AİHS 8. madde ile kişisel verilerin korunmasına doğrudan doğruya bir düzenleme yapılmamakla birlikte, özel hayata ve aile hayatına saygı hakkı kapsamında yer alan kişisel veriler hukuken koruma altına alınmıştır⁴¹⁰.

Avrupa Konseyi’nin 1970’li yıllardan itibaren kişisel verilerin korunması alanında yaptığı çalışmaların bir neticesi olarak⁴¹¹ 28.01.1981 tarihinde Strazburg’da “108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesini”⁴¹² kabul edilmiş ve 1985 yılında yürürlüğe girmiştir. Önemli nokta, 108 No’lu Sözleşme’nin kişisel verilerin korunması alanında ayrıntılı olarak hazırlanan ve hukuken bağlayıcılığı olan ilk belge olmasıdır. Bu Sözleşme Avrupa Konseyi’ne üye olan tüm ülkeler tarafından imzalanmakla birlikte Avrupa Konseyi olmayan ülkelerin katılımına da açık tutulmuştur⁴¹³.

Sözleşmeyi imzalayan taraf devletlerden her biri, ülke sınırlarında yaşayan bütün gerçek kişilerin kişisel verilerini ayırım yapmaksızın korumakla (m.1) ve Sözleşme hükümlerini iç hukuklarına aktarmakla yükümlü tutulmuşlardır (m.4). Hem özel sektör hem de kamu kurumlarına yönelik olarak hazırlanmıştır⁴¹⁴. Avrupa Konseyi’ne üye olmayanların da

⁴⁰⁹Council of Europe (1981) . *Convention for the protection of individuals with regard to automatic processing of personal data* (No. 108) . <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108> (Erişim Tarihi: 25.03.2025) .

⁴¹⁰ bkz. Akgül, 2014, s.76 vd. Konu ile ilgili ayrıca bkz. European Court of Human Rights (ECHR), Factsheet – Personal Data Protection. https://www.echr.coe.int/documents/d/echr/fs_data_eng (Erişim Tarihi: 23.02.2025) .

⁴¹¹ Selek, 2021, s.38 ; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanuna İlişkin Uygulama Rehberi, s.16.

⁴¹²Avrupa Konseyi (1981) . *108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*, m. 2-d. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108> (Erişim Tarihi: 14.03.2025) .

⁴¹³ bkz. Council of Europe. *Convention No. 108, Summary*. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108> (Erişim tarihi: 24.04.2025); 108 sayılı Sözleşme, veri koruma alanında yasal bağlayıcılığı olan tek uluslararası belgeydi ve halen yürürlükte. Council of Europe (2018) . *Handbook on European data protection law* (2018 edition, s. 17) . https://www.echr.coe.int/documents/d/echr/Handbook_data_protection_ENG (Erişim tarihi: 04.05.2025) . Türkiye, 28 Ocak 1981 tarihinde bu sözleşmeyi imzalayan ilk ülkelerden biri olmuştur. Sözleşme, 17 Mart 2016 tarihli ve 29656 sayılı Resmî Gazete’de yayımlanarak iç hukuka dahil edilmiştir.

⁴¹⁴Aksoy, 2010, 99.

katılımına açık olan(m.23) Sözleşme'nin temel amacı; kişisel verilerinin otomatik işlemlerle işlenmesi karşısında gerçek kişilerin, mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerinin korunmasıdır(m.1). Üzerinde durulması gereken nokta ise bu Sözleşme'nin sadece otomatik yollarla işlenen verilere ilişkin bir koruma sağlamasıdır. 108 nolu Sözleşme'nin uygulanması için Avrupa Konseyi tarafından bugüne kadar pek çok tavsiye karar alınmış ve 1999 yılında Sözleşme'de değişiklikler yapılmıştır⁴¹⁵.

OECD ve BM Rehber İlkeleri ile neredeyse aynı düzenlemeleri içeren Sözleşme yalnızca otomatik işleme tabi verileri kapsamaktadır. Ayrıca Rehber İlkelere ek olarak başka yenilikler de getirmiştir. Örneğin, "Hassas verilerin" işlenmesini kural olarak yasaklanmış(m.6); bu verilerin işlenmesi birtakım güvencelerinin olması şartına bağlanmıştır. Kişisel verilerin işlenmesinde istisna tutulan alanlar Sözleşme ile genişletilerek, verilerin devlet güvenliğinin, kamu emniyetinin, devletin parasal çıkarlarının korunması, cezai suçların bastırılması, veri sahibinin veya başkalarının hak ve özgürlüklerinin korunması ile istatistik veya bilimsel araştırma amacıyla kullanılması hallerinde kanunla öngörülmesi şartı ile işlenebileceği öngörülmüştür(m.9).

181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol⁴¹⁶, 08.11.2001 tarihinde kabul edilmiştir. Bu protokol ile taraf ülkelere, tarafsız ve bağımsız, kararlarına karşı temyiz yoluna gidilebilen denetleyici veri koruma organlarının kurulmasını zorunlu hale getirmiştir(m.1). Ayrıca, yeterli hukuki korunmasının varlığı halinde ve veri aktarılmasına kanunda izin verilmesi hallerinde sınır ötesi veri akışının mümkün olacağı düzenlenmiştir(m.2-3).

2.8.1.4. Avrupa Birliği

Avrupa Birliği, II. Dünya Savaşı'ndan sonra Avrupa'da barış ve güvenliği sağlamak, teşvik etmek, insan hak ve özgürlüklerini korumak ve geliştirmek, ekonomik, sosyal ve politik birliğin sağlanması amacı güden bir kuruluştur⁴¹⁷. Avrupa Birliği, "AB Temel Haklar Şartı"⁴¹⁸ Fransa'nın Nice şehrinde 2000 yılında imzalanmıştır. AB vatandaşlarının temel haklarını ve AB'nin vatandaşlarına karşı sorumluluklarını düzenleyen metin, 8. maddesinde kişisel verilerin korunması hakkını düzenlemiştir. Buna göre: *"Herkes, kendisine ilişkin kişisel bilgilerin korunmasını isteme hakkına sahiptir. Kişisel bilgiler, belirtilen amaçlar için ve ilgili kişinin rızasına veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme*

⁴¹⁵Ayözger Öngün, 2019, s.73-74.

⁴¹⁶Council of Europe (2001) . *Convention No. 181 on the Protection of Individuals with regard to Automatic Processing of Personal Data* (08.11.2001) . <https://rm.coe.int/1680080626> (Erişim tarihi: 25.03.2025)

⁴¹⁷Avrupa Birliği Resmi Web Sitesi için bkz. European Union Official Website: European Union, https://european-union.europa.eu/index_en Erişim Tarihi: 25.03.2025. Avrupa'da kişisel verilerin korunması alanındaki gelişmeler de yine ikinci dünya savaşının etkileri sebebi ile ortaya çıkmıştır. Nitekim, II. Dünya Savaşı sırasında ırk ve etnik köken temelli soykırım faaliyetlerinin trajik sonuçları, özel hayatın, giz alanının ve kişisel verilerin devletler nezdinden çok daha sıkı şekilde korunması gerektiğini bilincini oluşturmıştır. Aynı yönde bkz. Şimşek, 2008, 39-40.

⁴¹⁸ AB Temel Haklar Şartı, AB hukukunun uygulanmasında hem Avrupa Birliği (AB) hem de AB ülkeleri tarafından gözetilmesi gereken temel hakları ortaya koymaktadır. Avrupa İnsan Hakları Sözleşmesi'nden daha geniş olan bu sözleşme, AB vatandaşları ve AB'de ikamet edenler için onur, özgürlük, eşitlik, dayanışma, vatandaşlık ve adalet ile ilgili ilkeler ve haklar belirler. Sivil ve siyasi hakları korumanın yanı sıra, çalışanların sosyal haklarını, veri korumasını, biyoetiği ve iyi yönetim hakkını da kapsar. Daha fazla bilgi için bkz. Charter of Fundamental Rights of the European Union: European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT> (Erişim Tarihi: 26.03.2025) .

yaptırma hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir”⁴¹⁹.

Avrupa Birliği Konseyi⁴²⁰’nin ve Avrupa Parlamentosu tarafından ”*Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunmasına ve Serbest Veri Akışının Sağlanmasına İlişkin 24/10/1995 tarihli 95/46/EC sayılı Veri Koruma Direktifi*”⁴²¹ hazırlanmış ve 95/46/EC sayılı bu Direktif 1998 yılında yürürlüğe girmiştir⁴²². 108 No’lu Avrupa Konseyi Sözleşmesi ile yalnızca otomatik işleme faaliyetlerinde kullanılabilirdi; bu Direktif ile kapsam genişletilmiş ve kişisel verilerin her türlü araç ile işlenmesinde koruma alanı içine dahil edilmiştir⁴²³. AB tarafından kişisel veri koruma konusunda danışmanlık yapması için 29. Çalışma Grubu görevlendirilmiş(m.30), bu çalışma grubu AB üyelerinin iç hukuklarındaki veri koruma mevzuatlarını uyumlu hale getirmeleri için rehberlik sağlamıştır. 95/46/EC sayılı Direktif’de bulunan maddelerin 04.05.2016 tarihinde kabul edilen Çalışmamız konusunu teşkil eden GDPR metninde de bulunması ile GDPR’ın esasen Direktif’in değişen yeni koşullara uyarlanmış halinden ibaret olması⁴²⁴ sebepleri ile 95/46/EC sayılı Direktif’ten kısaca bahsedilecektir.

95/46/EC sayılı Direktif, temel olarak iki amacı olduğu belirtilmektedir: temel hak ve özgürlüklerin korunması ile kişisel verilerin özellikle iç pazarda serbest akışının sağlanması⁴²⁵. Kişisel veri kurallarının uygulanmasına ilişkin kamu-özel ayrımı yapılmamış olsa da kişisel verilerin işlenmesinde hukuka uygunluk sebebi olarak kamu yararı ve kamu düzeni gibi ifade yer verilmesi kamu idaresinin genel kurallardan istisna sayılabileceğini göstermektedir. Direktif, otomatik veya otomatik olmayan yollarla işlenen kişisel verilere uygulanabilecektir. Bununla birlikte Direktif m.3’te uygulama istisnalarına yer verilmiştir. Buna göre, ceza hukuku alanındaki devlet faaliyetleri, devlet güvenliği, savunma ve kamu güvenliğine ilişkin faaliyetler kapsamında 95/46/EC sayılı Direktif uygulanmayacaktır. Bunun yanı sıra bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti esnasında işlenen kişisel verilere ilişkin de Direktif uygulanmaz⁴²⁶. Son olarak belirtmek gerekir ki, AB’de 95/46/EC sayılı Direktif’ine dayanan sektörel bazı düzenlemeler de mevcuttur. Bu düzenlemelerden en önemlisi;

⁴¹⁹ Avrupa Şartı, veri koruma alanında yasal olarak bağlayıcı bir uluslararası araçtır ve halen yürürlüktedir. Council of Europe, Handbook on European Data Protection Law, s. 27-28.

⁴²⁰Avrupa Birliği Konseyi, Avrupa Konseyi’nin değil; Avrupa Birliği’nin bir organıdır. Avrupa Birliği Resmi Web Sitesi için bkz. European Union Official Website: European Union. https://european-union.europa.eu/index_en (Erişim Tarihi: 25.03.2025).

⁴²¹Avrupa Birliği’nin 1995/46/EC nolu direktifi tam metin için bkz. European Union (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, L281, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046> (Erişim Tarihi: 31.01.2025).

⁴²² Ayözger Öngün, 2019, s.78.

⁴²³ Şimşek, 2008, s.23.

⁴²⁴ Selek, 2021, s.46-47.

⁴²⁵ bkz. Avrupa Komisyonu, Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions, A Comprehensive Approach on Personal Data Protection in The European Union, Brüksel, 04.11.2010, s. 2. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF> . Erişim Tarihi: 25.04.2025.

⁴²⁶Benzer bir düzenleme 95/46/EC sayılı Direktif, giriş, m.12’de de düzenlenmiştir. Bu düzenleme ile adres kayıtlarını tutma ve yazışma gibi özellikle şahsi veya ailevi olan aktiviteler esnasında, bir gerçek kişinin gerçekleştirdiği veri işleme faaliyetlerinin Direktif kapsamında korunmadığı belirtilmiştir.

2002/58/EC sayılı “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif”⁴²⁷’tir.

Hızla gelişen teknolojinin ve küreselleşmenin dünyayı derinden değiştirmesi ve yeni çatışma ve ihtiyaçların giderilmesinde çözümler getiremeyen 95/46/EC sayılı Direktif’in gelişmeler karşısında yetersiz kaldığı ve geliştirilmesi gerektiği hakkında Avrupa Komisyonu 2010 yılında görüş bildirmiştir⁴²⁸. Komisyon görüşü kapsamında yapılan çalışmalar neticesinde⁴²⁹ kişisel verilerin korunması alanında çeyrek asrı aşan uygulama tecrübesi ile bu alandaki bugüne kadarki en etkili düzenleme için 04.05.2016 tarihinde adım atılarak, Avrupa Birliği Resmi Gazetesinde yayımlanan 2016/679 sayılı Avrupa Birliği Veri Koruma Tüzüğü (“GDPR”)⁴³⁰ kabul edilmiştir. 25.05.2018 tarihinde yürürlüğe giren GDPR, 95/46/EC sayılı Direktif’in yerine geçmiş ve böylece Direktifin uygulanmasına son vermiştir. Belirtmek gerekir ki, üye ülkeler bakımından bağlayıcı kurallar öngören GDPR, esasen kaynağını Direktifin kendisinden almaktadır. Diğer bir ifade ile pek çok yenilik olmakla birlikte GDPR esasen 95/46/EC sayılı Direktif’in yeni teknolojiye ve ihtiyaçlara uyarlanmış halinden ibarettir⁴³¹.

GDPR düzenlemesinin “tüzük” olmasının büyük bir önemi bulunmaktadır. Nitekim Avrupa Birliği’nde 95/46/EC sayılı Yönergesi gibi “yönergelerin” uygulanabilmesi, taraf devletlerin bu düzenlemeleri iç hukuklarına aktarması ile mümkünken; “tüzüklerin” doğrudan doğruya uygulanabilmesi mümkündür. Bu durum, kişisel verilerin korunmasına ilişkin 95/46/EC sayılı Yönergesi çerçevesinde kurulmuş olsa da birbirinden farklı iç hukuk düzenlemeleri oluşmasına sebep olmuştur fakat bağlayıcılığı bulunan GDPR düzenlemesi ile Avrupa’da yeksanak bir uygulama sağlanması mümkün olmuştur⁴³². Nitekim, Avrupa Birliği İşleyişi Hakkında Antlaşma m. 288 uyarınca direktifler, her üye devleti, ulaştırılması gerekli sonuçları itibarıyla bağlarken; tüzükler, üye ülkeler için bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanmalıdır⁴³³. Bilgi teknolojilerinin ve özellikle internetin gelişimi

⁴²⁷ 12.07.2002 tarihli Direktif’in İngilizce metni için bkz. European Parliament & Council (2002, July 12) . *Directive 2002/58/EC on privacy and electronic communications*. <https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng> (Erişim Tarihi: 18.04.2025) .

⁴²⁸bkz. European Commission (2010, November 4) . *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union* [COM (2010) 609 final]. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF> (Erişim Tarihi: 25.04.2025) . Bu noktada kişisel verilerin kesin ve ayrıntılı şekilde düzenlenmesinden ziyade katı bir yaklaşımdan uzaklaşarak teknolojinin de gelişimi göz önüne alınarak geleceğe de uygulanabilir hükümler ile düzenlenmesi gerektiğinin de altı çizilmelidir. Zira sıkı ve katı yaklaşım, kullanılan uygulamalardan istenilen verimin alınması yanında kişisel verilerin korunmasının sağlanması bakımından da bir engel teşkil etmektedir. Aşıkoğlu, 2018, s.212. Teknoloji ve toplumun değişen yapısına uyum sağlamak için Avrupa Konseyi ve Avrupa Komisyonu’na 2012 yılında başlanan tüzük görüşmeleri 4 yıl süren çalışmanın ardından 04.05.2016 yılında tamamlanmış ve GDPR bu tarihte Resmi Gazete’de yayımlanmıştır. Taştan, 2017, s. 15.

⁴²⁹Develioğlu, 2017, s.12.

⁴³⁰ Avrupa Parlamentosu ve Konseyi (2016, 27 Nisan) . *Genel Veri Koruma Tüzüğü (EU) 2016/679 (GDPR)* . <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (Erişim Tarihi: 25.03.2025) . T.C. Avrupa Birliği Başkanlığı (2025, Ocak 31) . *Genel Veri Koruma Tüzüğü (GDPR) Türkçe çeviri*. <https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf> (Erişim Tarihi: 25.03.2025) .

⁴³¹ Selek, 2021, s.46-47.

⁴³²Avrupa Komisyonu’nun GDPR düzenlemesi hakkında 25.01.2012 tarihli basın açıklaması için bkz. European Commission (2012, January 25) . *Why do we need an EU data protection reform?* https://ec.europa.eu/commission/presscorner/detail/en/memo_14_186 (Erişim Tarihi: 04.05.2025) . Nitekim, 95/46/EC sayılı Direktifi esas alan iç hukuk kuralları her ne kadar aynı prensiplere sahip olsalar da, AB üyesi devletin bu yasal düzenlemelerinde önemli farklar vardır. GDPR ile bu durum ortadan kaldırılmıştır. Develioğlu, 2017, s.12; Selek, 2021, s.46-47.

⁴³³ bkz. Avrupa Birliği İşleyişi Hakkında Antlaşma (“The Treaty on The Functioning of The European Union”), C 326/47, 26.10.2012, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF> .

ile böylesi AB’de etkin bir veri koruma standartlarının oluşturulması özellikle bu gelişimlerin meyvesi olan dijital ekonomi ve elektronik ticaret için çok önemli bir gelişmedir⁴³⁴.

GDPR, kişisel veri koruma konusunda en kapsamlı düzenlemeyi getirerek, diğer metinlerde yer verilen şeffaflık(m.12), veri sahiplerinin onayını alma(m.8-9), veri ihlali bildirimleri yapma(m.33) ve kişisel verilerin güvenliğini sağlama(m.32 vd.) gibi yükümlülükler getirmesinin yanı sıra birçok yeni hak ve kavramı da düzenlemiştir. Çalışmamızın konusunu GDPR’ın kendisinin oluşturması ile ilgili konu başlıkları altında bağlantılı hükümlerinin Çalışmada incelenmesi sebebi ile bu kısımda yalnızca Tüzüğün getirdiği başlıca yeniliklere kısaca değinilmiştir⁴³⁵:

Öncelikle belirtmek gerekir ki, GDPR’ın uygulama alanı 95/46/EC sayılı direktife göre daha geniştir. Her ne kadar, GDPR bir AB Tüzüğü olsa da, AB bünyesinde yaşayan kişilerin verilerini işlemesi koşulu ile AB coğrafi sınırları dışında kurulan fakat AB içinde ödeme talep edilip edilmesine bakılmaksızın mal ve hizmet sağlanması halinde Tüzük uygulama alanı bulacaktır((m.3/2-a). Bu durum, AB’de ikamet eden bir gerçek kişinin profillemesi, internette takip edilmesi ile kendisi ile ilgili kararlar almak veya kişisel tercihlerini, davranışlarını ve tutumlarını analiz veya tahmin etmek amacıyla verilerinin işlenmesi durumunda da böyledir(m.3/2-b). Bu koşulları sağlayan Şirketlerin GDPR’a uyum sağlamasını zorunlu kılmaktadır(m.3). Örneğin, ABD merkezli Amazon’un internet hizmet sağlayıcı Google’ın ve bir sosyal medya platformu olan Facebook’un AB sınırları içerisinde hizmet sunmaları sebebiyle GDPR’a uyum sağlamaları gerekmektedir⁴³⁶. Ayrıca, Türkiye’deki mevzuata tabi veri sorumlularının AB vatandaşlarına mal ve hizmet faaliyetlerini yürütmesinde bir yandan da GDPR’a uyum göstermesi gerekecektir. Aksi halde, bu Şirketler Tüzük tarafından belirlenen cezai müeyyide ve tedbirlere tabii olacaktırlar⁴³⁷. Kişisel veri akışının Avrupa Birliği dışındaki ülkelere yapılması halinde kısıtlayıcı hükümler öngören düzenlemeler karşısında, kişisel verilerin akışında herhangi bir kesinti yaşanmasını önlemek amacıyla Amerika Birleşik Devletleri Ticaret Bakanlığı (DOC) Avrupa Birliği ile müzakere sürecini başlatmış ve taraflar arasında kişisel verilerin korunmasına ilişkin güvence sağlayan ve Avrupa kişisel veri koruma direktifleri ile uyumu teşvik eden Safe Harbor İlkeleri üzerine 2000 anlaşmaya varılmıştır.

Erişim Tarihi: 04.05.2025. Antlaşmanın Türkçe çevirisi için bkz. <https://www.ab.gov.tr/files/pub/antlasmalar.pdf>. Erişim Tarihi: 04.05.2025.

⁴³⁴ Ayözger Öngün, 2019, s.89.

⁴³⁵ Ayözger Öngün, 2019, 87-89; Selek, 2021, s.53-56. Ayrıca bkz. BAŞALP, Nilgün, " Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Dergisi, 2015, C.21, S.1, s.77-105.

⁴³⁶ Ayözger Öngün, 2019, s.88, Selek, 2021, s.53, Taştan, 2017, s. 16; Develioğlu, 2017, s. 17-18; Başalp, 2015, s. 88. Develioğlu, internet ortamında sunulan mal ve hizmetin hedef kitle olmamasına rağmen sadece internette bulunması sebebi ile ulaşılabilir olduğu durumların GDPR kapsamı dışında bulunduğunu söylemektedir. Buna göre, Yunanistan’daki bir taşınmaza ilişkin Türkiye’de mukim bir Türk Emlak Şirketi’nin Türkçe ve TL cinsinden vereceği ilan kapsamında hedef kitlenin Türk Vatandaşları olduğu varsayımı ile GDPR uygulanmayacaktır. Ters bir durum ise Türkiye’de örneğin Antalya’daki bir taşınmaza ilişkin Alman muhiti denilerek, Almanca ve Euro cinsinden verilen bir ilanda GDPR hedef kitlenin AB vatandaşı olması sebebi ile uygulanacaktır. Develioğlu, 2017, s. 18.

⁴³⁷ Bu halde, verisi işlenen ilgili kişi, veri ihlali durumunda GDPR m.79’da düzenlenen yargı yollarına başvurabileceği gibi; bu şirketler aynı zamanda KVKK’ya tabii olduğundan Kişisel Verilerin Korunması Kurumu’na veya genel hükümler çerçevesinde genel mahkemelere başvuruda bulunabilir. Develioğlu, 2017, s. 19.

Ancak bu ilkeleri sağlayan veri sorumlularının yeterli korumaya sahip olduğu kabul edilecek ve aktarım yapılabilir olacaktır⁴³⁸.

Pek çok yeni hak tesis eden GDPR, kişisel verilerin korunması alanında “Unutulma Hakkını” (*the right to be forgotten*) gündeme getirerek bir ilke imza atmıştır. Unutulma Hakkı çerçevesinde, ilgili kişi, kişisel verilerinin işlenmesi amaçları bakımından işlenen kişisel verilerinin artık gerekli olmaması, rızasını geri alması veya itiraz etmesi ile kişisel verilerinin işlenmesinin Tüzük ile uyumlu olmaması hallerinde, kişisel verilerini kalıcı olarak silme ve daha fazla işlenmemesini talep hakkına sahiptir (GDPR, “giriş”, para. 65; m.17). Bu hak temelde bireylerin mahremiyet hakkı ile ilişkilidir⁴³⁹.

Çocukların kişisel verilerinin korunmasına ilişkin hükümlere ilk defa⁴⁴⁰ Tüzük’te yer verilmiştir. Giriş kısmı 75. Paragrafta çocukların savunmasız gerçek kişilerden (“*vulnerable natural person*”) olduğunun altı çizilerek çocuklara ait verilerin işlenmesinde velayet makamının rızası veya yetkisi aranmıştır(m.8). “*Privacy by Design*”⁴⁴¹ ilkesini benimseyen GDPR, AB sınırları içerisinde satılacak ürünlerin, tasarım ve üretim aşamalarında diğer bir ifade ile tasarımlarından itibaren korunmasını düzenlemiştir(m.25)⁴⁴². Aynı maddede düzenlenen, varsayılan ayarla veri koruma (“*Privacy by Default*”) ise herhangi başka bir ayarlamaya ihtiyaç duyulmadan, kişisel verilerin korunmasının sağlanmasını ifade etmektedir(m.25/2)⁴⁴³. Tüzüğün getirdiği yeniliklerden biri de veri taşınabilirliği hakkına(“*right to data portability*”) yer vermesidir. Veri taşınabilirliği hakkı, ilgili kişinin

⁴³⁸ Blanke, J. M (2000) . "Safe Harbor" and the European Union's directive on data protection. *Albany Law Journal of Science & Technology*, 11, s.101-134. Avrupa Birliği ile kararlaştırılan bu ilkelere uyan ve uyum sağlamayanların listesi Amerika Birleşik Devletleri Ticaret Bakanlığı (DOC) bünyesinde tutulmaktadır. Böylece kişisel verilerin korunmasına ilişkin Amerika Birleşik Devletleri bünyesinde esasen ekonomik kaygılarla sağlam bir lobi çalışması yapılmaktadır. Safe Harbour kapsamında anlaşılan 7 ilke kısaca şunlardır: bireyler verilerinin toplandığı ve nasıl kullanılacağı konusunda ve veri sorumlusuna müracaat hakları hakkında bilgilendirilmelidir “bildirim ilkesi”; kişilerin verilerinin toplanmasında, daha sonra başka amaçlarla kullanılmasına ve üçüncü taraflara aktarılmasında vazgeçme hakkının verilmesi gerekmektedir “seçim ilkesi”; kişisel verilerin üçüncü taraflara aktarımının yalnızca yeterli veri koruma ilkelerini izleyen diğer kuruluşlara yapılabileceği güvencesini verilmelidir “ileri aktarım ilkesi”; kişisel verileri işleyen kurum ve kuruluşları, bu verileri ihlallere karşı korunmasını sağlamakla yükümlüdür “güvenlik ilkesi”; İlkelerle tutarlı olarak, kişisel bilgiler kullanılacakları amaçlarla ilgili olmalıdır, veriler toplanma amaçlarına uygun olmayan şekilde ve ilgili kişiden alınan rıza kapsamında olmayan amaçlarla işlenemez “veri bütünlüğü ilkesi” ; ilgili kişilere işlenen kişisel verilerine ilişkin bilgilendirme yapılmalı ve veri sorumlusuna müracaat ile verisinin düzeltilmesini ve silinmesini talep etme hakkı tanınmalıdır “erişim ilkesi” ve son olarak bu ilkelerin etkin şekilde uygulanması için yeterli araçların olması gerektiğini ifade eden “uygulama ilkesi”. Blanke, 2000, s.123 vd.

⁴³⁹ bkz. European Commission (2015) . *Data Protection Reform – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/pt/memo_15_6385 . Erişim Tarihi: 06.05.2025.

⁴⁴⁰ Selek, 2021, s.54.

⁴⁴¹ Bu ilke, bir ürünün kişilerin gizliliğine hanel getirmeyecek şekilde tasarlanması veya gizliliğin henüz tasarım aşamasında dikkate alınması olarak ifade edilebilir. Taştan, 2017, s. 18.

⁴⁴² Örneğin, kullanıcı profilinin erişilebilirliği en baştan sınırlandırılmalı ve varsayılan olarak belirsiz sayıda kişi tarafından erişilebilir olmamalıdır. Bkz. European Commission. *What does data protection by design and by default mean?* https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (Erişim Tarihi: 16.06.2025) . Kullanıcının gizlilik ayarlarını değiştirerek bilgilerini herkese açık hale getirmesinde bu kural ihlal edilmiş olmaz. Taştan, 2017, s. 19.

⁴⁴³ “*Tasarımla veri koruma*” ve “*varsayılan ayarla veri koruma*” artık AB veri koruma kurallarında temel ilkeleri haline gelmiştir. Bu ilkelere göre, veri koruma önlemleri, geliştirilmenin en erken aşamasından yani tasarımından itibaren ürün ve hizmetlere yerleştirilecek ve gizlilik dostu varsayılan ayarlar norm haline gelecektir. bkz. European Commission (2015) . *Data Protection Reform – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/pt/memo_15_6385 (Erişim Tarihi: 06.05.2025) .

kişisel verilerini bir veri sorumlusundan bir diğerine taşımasına olanak vermektedir⁴⁴⁴ (m.20). Bu hak, Türk mevzuatına alınmamış ve Kişisel Verilerin Korunması Kanunu("KVKK")'da düzenlenmemiştir. Benzer şekilde "ortak veri sorumluluğu"⁴⁴⁵ müessesesi de GDPR'ın 26. maddesinde düzenlenmekle birlikte; KVKK metninde yer almamaktadır. Son olarak, Direktif'te yalnızca özel nitelikli kişisel verilerin işlenmesinde aranan ilgilinin konuya ilişkin açık rızası alınması şartı, tüzük ile genel nitelikli veriler için de uygulanması kararlaştırılmıştır⁴⁴⁶.

GDPR, veri sorumlusunun yükümlülüklerini arttırmış ve detaylandırmıştır. Hesap verilebilirlik ilkesi(m.3/2) kapsamında, veri sorumlusuna bir ihlalin varlığının öğrenilmesinden en geç 72 saat içinde, söz konusu kişisel veri ihlalinin denetim makamına (*giriş*, 58) bildirimde bulunma yükümlülüğü getirilmiştir. Kişisel verilerin işlenmesinin, temel hak ve özgürlükler açısından yüksek bir riske sebebiyet vermesinin olası olduğu hâllerde, veri sorumlusu, işleme öncesinde, "*Veri Koruma Etki Değerlendirmesi*" yapmakla yükümlü kılınmıştır(m.35). Ayrıca, ilk kez veri koruma görevlisinden⁴⁴⁷ (*data protection officer*) ve bu meslek grubunu istihdam etmek zorunda olan kurum ve kuruluşlardan bahsedilmiş(m.37 vd.), yüksek para cezalarıyla(m.83) veri güvenliğini teşvik etmiştir.

GDPR'ın en önemli özelliklerinden birisi bağımsız bir tüzel kişiliğe sahip olan AB Veri Koruma Otoritesi kurulmasını öngörmesidir. Avrupa Veri Koruma Kurumu (European Data Protection Board); ("EDPK"), 95/46/EC sayılı Direktif ile kurulan 29. Çalışma Grubu'nun yerini alarak; 29. Çalışma Grubu'nun faaliyetlerini sona erdirmiştir. Kurul, her Üye Devlet'in denetim makamının başkanı ile Avrupa Veri Koruma Denetçisi veya bunların her birinin temsilcilerinden oluşmaktadır. "*One Stop Shop*" ilkesi çerçevesinde uygulama yeknesaklaştırılması amacı ile kurulan Veri Koruma Otoritesi AB içinde yalnızca bir otorite ile muhatap olunması amaçlanmıştır⁴⁴⁸.

2.8.2. Ulusal düzenlemeler

Türk hukukunda, kişisel verilerin korunmasına ilişkin yolculuk 1981 tarihli 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireyin Korunmasına dair Avrupa Konseyi Konvansiyonu'nun 28.01.1981 tarihinde imza edilmesi ile başlamış fakat bundan sonraki

⁴⁴⁴ Bu hak, bireylerin kişisel verilerinin hizmet sağlayıcılar arasında iletilmesini kolaylaştırılmasını ifade etmektedir. EU Press Release: Data Protection Reform – Questions and Answers, https://ec.europa.eu/commission/presscorner/detail/pt/memo_15_6385 . Erişim Tarihi: 06.05.2025.

⁴⁴⁵ GDPR m.26'ya göre; iki ya da daha fazla veri sorumlusunun ortak bir şekilde kişisel veri işleme amaç ve yöntemlerini belirlediği hallerde, bu veri sorumluları ortak (birlikte) veri sorumlularıdır. Örneğin, pek çok banka için işlem verileri depolayan SWIFT kurumu, SWIFTNet FIN hizmeti kapsamında işlenen verileri için iş ortağı bankalar ve SWIFT kurumu ortak veri sorumlularıdır. Article 29 Working Party (2006, November 22) . Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) s. 2 vd. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf . Erişim Tarihi: 02.05.2025) .

⁴⁴⁶ Başalp, 2015, s. 102.

⁴⁴⁷ Veri koruma görevlisinin temel görevi, veri güvenliğini sağlamak için bulundukları kuruluştaki gizlilik politikaları ile uygulamaların GDPR ile uyumlu olup olmadığının denetimi yapmaktır. Taştan, 2017, s. 20.

⁴⁴⁸ Buna göre, farklı ülkelerin veri otoritelerinin aynı konuya ilişkin farklı kararlar almalarının önüne geçmek için yalnızca bir ülkeyi ilgilendiren ihlallerde o ülkenin veri otoritesinin yetkili olacağı; fakat birden fazla ülkede ihlalin söz konusu olduğu hallerde AB Veri Koruma Kurumu'nun yetkili olacağı düzenlenmiştir. GDPR, "*giriş*", para. 127-128. Bu kurumun başlıca görevleri: üçüncü ülkelerde veya uluslararası kuruluşlardaki koruma düzeyi konusunda Komisyona tavsiyede bulunma ve AB genelinde denetim makamları arasında işbirliğini teşvik etme dâhil, Tüzük'ün Birlik genelinde tutarlı bir şekilde uygulanmasına katkı sağlamaktır. GDPR, "*giriş*", para. 139.

adımlar oldukça yavaş atılmıştır. Öyle ki, Türkiye bu Sözleşme’yi ilk imzalayan ülkeler arasında bulunmasına rağmen iç hukukuna dahil etmesi yaklaşık 35 yıl sürmüştür⁴⁴⁹. Türkiye’de ilk kez kanun düzeyinde düzenleme, 2004 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu⁴⁵⁰ ile yapılmış; bu kapsamda kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi, yayılması gibi fiiller suç olarak tanımlanmıştır (TCK m. 135–140).

Anayasa’da kişisel verilerin korunması ile bağlantılı birçok hak ve özgürlük bulunmaktadır⁴⁵¹. Fakat doğrudan bir düzenleme 2010 yılı değişikliği ile Özel Hayatın Gizliliği Hakkını düzenleyen 20. maddesi 3. fıkrasına eklenen “Kişisel Verilerin Korunması Hakkı” eklenmesi ile meydana gelmiştir⁴⁵². Anayasa m.20/3’de, kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceği hüküm altına almıştır. Bu doğrultuda hazırlanan ve GDPR düzenlemesini değil 95/46/EC sayılı Direktifi esas alan⁴⁵³ 6698 Sayılı Kişisel Verilerin Korunması Kanunu(“KVKK”)⁴⁵⁴, 07.04.2016 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

KVKK, günümüzde, Türk hukukunun temel kişisel verilerin korunması kanunudur. Esasen, AB üyelik sürecinin tamamlanması için kabul edilen Kanun⁴⁵⁵ ile temel hak ve özgürlükler alanında bir gelişme olması ve uluslararası alanda kabul edilen prensiplerin iç hukuka dahil olması sebepleri ile olumlu bir gelişme olsa da; ucu açık şekilde düzenlenen ve keyfi uygulamalara imkan tanıyan geniş istisnai hükümleri bakımından düşündürücüdür⁴⁵⁶. Kanun’un amacı, kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasal hakların güvence altına alınması ile kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların da düzenlenmesidir⁴⁵⁷.

KVKK kapsamında düzenleyici ve denetleyici bir kurum olan idari ve mali özerkliği bulunan Kişisel Verilerin Korunması Kurumu(“Kurum”) 30.01.2017 tarihinde kurulmuştur. Kişisel Verilerin Korunması Kurumu görev ve yetkileri ile teşkilatlanması Kanun’un 3. bölümünde 19. madde vd. sayılmıştır. Kişisel verilerin korunması kurumu kararları ile KVKK düzenlemesinde mevcut olmayan hususlara ilişkin de ilke kararlar alma yetkisine sahiptir (KVKK m.15/6). Örneğin, KVKK metninde GDPR düzenlemesinde olduğu gibi çocuklara ait kişisel verilere ilişkin özel bir düzenleme bulunmamaktadır. Kurul, bu konuda kişisel verilerin şahsa sıkı sıkıya bağlı bir hak olduğu fakat küçüğün ayırt etme yeteneğine sahip olması ve ebeveyni ile rızanın örtüşmesi koşulu ile ebeveyninin küçük adına şikayet ve itirazda

⁴⁴⁹ Onay süreci 6669 sayılı Kanun’un 30.01.2016 tarihinde kabul edilmesi ile tamamlanmıştır. Bu Kanun 17.03.2016 tarih ve 29656 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

⁴⁵⁰ R.G. 12.10.2004 T., 25611 S.

⁴⁵¹ bkz. başlık “*Kişisel Verilerin Korunması Hukuku*” : Nitekim, kişisel verilerin korunması hakkı ile bağlantılı olan hukuk devleti ilkesi (m.2), kişinin maddi ve manevi varlığını serbestçe geliştirme hakkı (m.17), özel hayatın gizliliği hakkı (m.20), haberleşme özgürlüğü (m.22), haberleşme hürriyeti (m.22); din ve vicdan hürriyeti (m.24), düşünce ve kanaat hürriyeti (m.25) Anayasa’da düzenlenmiştir.

⁴⁵² Çağdaş devletlerde bir hakkın anayasa ile güvence altına alınması, bu hakkın en üst düzeyde koruma altına alındığı anlamına gelmektedir. Akgül, 2014, s. 347.

⁴⁵³ Aksoy, 2010, 115, Taştan’a göre, kişisel veri kavramı ile veri koruma kuralları alanında 2016 yılında hala tecrübesi bulunmayan Türkiye’nin, 2018 yılında yürürlüğe girecek olan ve dolayısıyla AB içinde uygulanma tecrübesi bulunmayan GDPR düzenlemesinin değil; yirmi iki yıldır uygulaması bulunan 95/46/EC sayılı Direktif’in KVKK düzenlemesinde esas alınması isabetlidir. Taştan, 2017, s. 24-25.

⁴⁵⁴ R.G. 29677 S. ve 07.04.2016 T.

⁴⁵⁵ bkz. Kanun gerekçesi, s.5.

⁴⁵⁶ Ayözger Öngün, 2019, s.111; Şimşek, 2008, s.215; Şen, 2009, s.1213.

⁴⁵⁷ bkz. KVKK Gerekçe, m.1.

bulunabileceği kararını vermiştir⁴⁵⁸. Çocukların kişisel verileri konusundaki usul belirsizliği doktrinde eleştirilere yol açmıştır⁴⁵⁹.

Kişisel Sağlık Verileri Hakkında Yönetmelik⁴⁶⁰ 21.06.2019 tarihinde yürürlüğe girerek 20.10.2016 tarih ve 29863 sayılı Resmi Gazete’de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetin Sağlanması Hakkında Yönetmeliğin yürürlükten kaldırmış ve eski düzenlemelerde yer almayan hususlara ilişkin açıklık getirmiştir (Örneğin, açık veri, açık sağlık verisi gibi kavramlar yeni tarihli yönetmelikte açıklanmıştır). 10.04.2024 tarihinde çıkarılan Kişisel Verilerin Yurtdışına Aktarılmasına İlişkin Esaslar Hakkında Yönetmelik⁴⁶¹ yanında Kurum tarafından çıkarılan diğer yönetmelikleri şu şekilde sıralayabiliriz: Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği; Veri Sorumluları Sicili Hakkında Yönetmelik; Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Ünvan Değişikliği Yönetmeliği; Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği; Kişisel Verileri Koruma Uzmanlığı Yönetmeliği; Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

Kişisel verilere ilişkin ulusal mevzuattan bahsederken, kişisel veriler ile ilgili diğer kanunlarda yer alan hükümlerin de bulunduğundan bahsetmek gereklidir⁴⁶². 5651 Sayılı

⁴⁵⁸ Kişisel Verileri Koruma Kurulu (2020, 11 Ağustos). *18 yaşını doldurmamış ilgili kişiye ait sağlık raporunun imha edilmesine yönelik ilgili kişinin babası tarafından veri sorumlusuna başvurulması ve cevap alınamaması üzerine ilgili kişinin kendisi tarafından Kurul’a yapılan şikayet* (Kurul Kararı No. 2020/622). Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/6816/2020-622> (Erişim Tarihi: 26.07.2025).

⁴⁵⁹ Dülger, M. V., Kahraman, C. C., ve Yalçın, S. (2021). *GDPR ve KVKK bakımından kişisel verilerinin korunması ve konuya ilişkin kurul kararının değerlendirilmesi (Çocukların kişisel verilerinin GDPR ve Kişisel Verilerin Korunması Kanunu açısından korunması ve Yargıtay incelemesi)*. <https://doi.org/10.2139/ssrn.3792410>

⁴⁶⁰ R.G. 21.06.2019 T. ve 30808 S.

⁴⁶¹ R.G. 10.04.2024 T. ve 32598 S.

⁴⁶² Kişisel verilerin korunmasına ilişkin düzenlemeleri bulunan Kanunları Çalışma Konusu Kapsamı itibari ile tek tek incelemek mümkün değildir. Bu Kanunları tahdidi olmamak üzere şu şekilde saymak mümkündür: 23/01/2004 tarih ve 25355 sayılı Resmi Gazete ile yürürlüğe giren 5070 Sayılı Elektronik İmza Kanunu m.12, elektronik sertifika hizmet sağlayıcısının, elektronik sertifika talep eden kişinin veya kullanan kişinin kişisel verilerini koruma yükümlülüğü; 10.06.2003 tarih ve 25134 sayılı Resmi Gazete ile yürürlüğe giren 4857 İş Kanunu m.75’te işverenin, işçi özlük dosyasına ilişkin bilgileri saklama yükümlülüğü; 30.06.2012 tarih ve 28339 sayılı Resmi Gazete ile yürürlüğe giren 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu m. 15 ile işverene işçi sağlık bilgilerini gizli tutma yükümlülüğü; 29.04.2006 tarih ve 26153 sayılı Resmi Gazete ile yürürlüğe giren 5490 Sayılı Nüfus Hizmetleri Kanunu m.9 ile nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan bilgi ve belgelerin gizli olduğu düzenlenmiş, memurlara bilgileri gizli tutma yükümlülüğü; 01.11.2005 tarih ve Mükerrer 25983 sayılı Resmi Gazete ile yürürlüğe giren 5411 Sayılı Bankacılık Kanunu m. 73 ile banka çalışan ve yetkililerine müşterileri ile ilgili öğrendikleri kişisel verileri koruma yükümlülüğü getirilmiştir. 10.11.2008 tarih ve Mükerrer 27050 sayılı Resmi Gazete ile yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu m.12 ile “*Kişisel Verilerin Korunması*” açık şekilde işletmecilerin yükümlülüğü olarak düzenlenmiştir. Kanun’un 59. maddesinde: “*Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz.*” hükmüne yer verilmiş ve “Cezai Hükümler” başlıklı 63. maddesinde bu yükümlülüklerle aykırı şekilde hareket edilmesi halinde uygulanacak adli para cezaları belirlenmiştir. 12.03.2020 tarih ve 31066 sayılı Resmi Gazete ile yürürlüğe giren 7223 Sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu m. 23 ile kişisel verilerin korunması yükümlülüğü getirilmiştir. Diğer yandan, kişisel verilerin korunması hakkını da kapsayacak şekilde bireylerin kişilik haklarına, özel hayatın gizliliğine ve diğer temel hak ve özgürlüklere aykırı

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlar ile Mücadele Edilmesi Hakkında Kanun⁴⁶³, internet trafiği bilgilerinin⁴⁶⁴ saklanması da düzenlemesi sebebi ile kişisel verilerin korunmasını ilgilendirmektedir. İnternet trafiği bilgilerinin saklamasını öngören bu kanun düzenlemelerini kişisel verilerin korunması hakkına karşı ölçüsüz bir müdahale teşkil etmesi sebebi ile eleştirilmektedir⁴⁶⁵. 7253 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun⁴⁶⁶ ile sosyal ağ sağlayıcı terimi eklenerek düzenlenmeler getirilmiştir(m.1).

Çalışma konumuz ile ilgili olan 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun⁴⁶⁷(“ETDK”) 01.05.2015 tarihinden itibaren yürürlüktedir. Kanun kapsamında belirtilen elektronik ticaret hizmet sağlayıcısı: “*Elektronik ticaret pazar yerinde ya da kendine ait elektronik ticaret ortamında mal veya hizmetlerinin teminine yönelik sözleşme yapan ya da sipariş alan hizmet sağlayıcıyı*” ifade etmektedir (ETDK m.2/1-g). E-ticaret platformlarında KVKK kapsamında yükümlülüklerden sorumlu olan suje elektronik hizmet sağlayıcılarıdır. Bu Kanun, özellikle müşterilere izinsiz elektronik ticari mail gönderilmesini yasaklaması(m.6)⁴⁶⁸ ve ihlallere ilişkin olarak getirdiği para cezaları(m.12) bakımından değerlidir. ETDK'nın "Kişisel Verilerin Korunması" başlıklı 10. maddesi, 2022 yılında mülga olmuştur. Böylece, kişisel verilerin korunmasına dair yetki ve sorumluluk, daha kapsamlı bir şekilde KVKK'ya devredilmiştir.

yahut çocukların fiziksel ve psikolojik gelişimlerine zarar verici şekilde internet kullanımının önlenmesi amacıyla alınan tedbirler ile yapılan iş ve işlemler hakkında inceleme, görüşme, raporlama, tavsiye ve görüş bildirme işlemlerini yürütmek amacıyla 28.07.2020 tarih ve 31199 sayılı Resmi Gazete ile yürürlüğe giren 7252 Sayılı Dijital Mecralar Komisyonu Kurulması ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun ile Türkiye Büyük Millet Meclisi bünyesinde “Dijital Mecralar Komisyonu” kurulmuştur. 12.10.2004 tarihli ve 25611 Sayılı resmi gazete ile yürürlüğe giren 5237 Sayılı Türk Ceza Kanunu’nun (“TCK”), “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” bölümünde kişisel verilere ilişkin m.135 vd. düzenlenen suç türleri; 17.12.2004 tarihli ve 25673 sayılı Resmi Gazete ile yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanunu (“CMK”) m.75 vd. düzenlenen şüpheli, sanık veya üçüncü kişilerin beden muayeneleri, vücutlarından alınan örnekler neticesinde elde edilen veriler, soybağı testleri, soruşturma ve kovuşturmalar kapsamında yapılan moleküler genetik incelemelerine ilişkin düzenlemeler kişisel verilerin korunması kapsamındaki Kanun hükümlerindendir. Genel hükümler çerçevesindeki düzenlemelere ise, 08.12.2001 tarihli ve 24607 sayılı Resmi Gazete ile yürürlüğe giren 4721 Türk Medeni Kanunu (TMK) “*Kişilik Haklarını*” düzenleyen 24 vd. maddeleri ile 14.02.2011 tarihli ve 27846 sayılı Resmi Gazete ile yürürlüğe giren 6102 sayılı Türk Ticaret Kanunu’nun (TTK) haksız rekabet hükümleri kişisel verilerin korunmasına ilişkin Kanunlara örnek gösterilebilir. Son olarak, 04.02.2011 tarihli ve 27836 Sayılı Resmi Gazete ile yürürlüğe giren 6098 Sayılı Türk Borçlar Kanunu da kişisel verileri, kişilik hakkı bağlamında koruma altına almıştır (m.58) .

⁴⁶³ R.G. 23.05.2007 T., 26530 S.

⁴⁶⁴ İnternet kullanıcısının, giriş-çıkış saatleri, adı-soyadı, kimlik bilgileri, iletişim bilgileri, IP adresi, bağlantı noktaları gibi veriler ve ilgili diğer veriler trafik bilgisi olarak sayılabilir. Yetim, S (2009) . 5651 sayılı yasa kapsamında tutulan internet trafik bilgilerinin özel hayat ve hayatın gizliliği kapsamında değerlendirilmesi. *Terazi Hukuk Dergisi*, 4 (36), s. 55-56.

⁴⁶⁵Selek, 2021, s. 70-71; ayrıca bkz. Yetim, 2009, s. 55-63.

⁴⁶⁶ R.G. 31.07.2020 T, 31202 S.

⁴⁶⁷ R.G. 05.11.2014 T. ve 29166 S.

⁴⁶⁸İngiltere ve Alman hukukunda da doğrudan pazarlama mesajları için opt-in (istek içi) sistem benimsenmekte ve alıcının bu mesajın gönderilmesi için rızası aranmaktadır. Bu hususta ispat yükü mesajın göndericisine aittir. Alman Mahkemeleri çift opt-in (istek içi) prosedürünü zorunlu kılmaktadır. Ayözger Öngün, 2019, s.92-93.

ÜÇÜNCÜ BÖLÜM

E-TİCARET SEKTÖRÜNDE KULLANILAN YAPAY ZEKA UYGULAMALARI KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ÖZEL BİR DEĞERLENDİRME

3.1. E-Ticaret, Yapay Zeka Entegrasyonu ve Kişisel Veriler

3.1.1. Ticaretin dijitalleşmesi: e-ticaret

İnternet zamanla onu geliştirenlerin hiç öngöremedikleri bir hale gelmiştir. Öyle ki, ilk amaç olarak iletişim düşünülmüş olsa da zaman içinde ticaretin en önemli araçlarından birisi hale gelmiştir. Başlı Amazon, Ebay, Yahoo gibi büyük hacimli şirketler çekmiş ve bugün internet bir ticaret platformu haline gelmiştir⁴⁶⁹. Dolayısıyla 1990'lı yılların ortalarında internetin kullanılması ile birlikte ortaya çıkan e-ticaret platformları özellikle; fazla çeşit sunması, ürünün aranma maliyetini azaltması, uygun fiyatlar sunması gibi özellikler sebebi ile tercih edilmiş⁴⁷⁰ ve Kovid-19 pandemisi sonrası insan hayatının ayrılmaz ve vazgeçilmez bir parçası haline gelmiştir⁴⁷¹. Pandemi döneminde e-ticaret platformlarının tüketicilere sağladığı kolaylıklar sayesinde dünya genelinde olduğu gibi Türkiye'de de e-ticaret hacminde inanılmaz artışlar yaşanmıştır. Öyle ki, 2019 yılında ülkemizin e-ticaret hacmi 136 Milyar Türk Lirası iken 2022 yılında bu rakam 800 Milyar Türk Lirasına yükselmiştir⁴⁷².

E-ticaret kavramından kısaca *“ticaret işlemlerinin internet sağlayıcıları vasıtası ile elektronik ortamda gerçekleşen biçimi”* anlaşılabılır. Bu platformlarda ürün ve hizmetlerin satışından, reklamlarına ve ödeme işlemleri de dahil olmak üzere tüm ticari pazarlama ve satış süreci dijital kanallar ile sağlanmakta ve bu faaliyetler web siteleri, uygulamalar gibi sanal pazar yerlerinde gerçekleşmektedir. Genel olarak e-ticarete, ticari işlemlerin dijitalleşmesi veya çevrimiçi olarak yapılan ticari işlemleri ifaden eden terim olarak nitelendirmek mümkündür⁴⁷³. Nitekim, 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun⁴⁷⁴,un 2/1-b maddesinde e-ticaret *“ Fiziki olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyet”* olarak tanımlanmıştır. Birçok uzmanın e-ticaret tanımından hareketle, e-ticaretin bilişim sistemleri ve online kanallar üzerinden yürütülen fiziki koşulların dezavantajlarından arındırılmış ticari bir olgu olduğu söylenebilir⁴⁷⁵. Gelecek günlerde e-ticaretin sanal ve arttırılmış gerçeklik ile daha fazla kişiselleştirilmiş, çok daha hızlı ve otonom teslimat seçenekleri sunan bir pazar olacağı ifade edilmektedir⁴⁷⁶.

⁴⁶⁹Kaya, 2011, s.17,153.

⁴⁷⁰Deliçay, M (2021) . *Perakende e-ticaretin yükselişi: Fırsatlar, sorunlar ve öneriler*. Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, s.5-6.

⁴⁷¹Koparan, E., ve Doğan, O (2024) . Toplum 5.0 ve e-ticarete yapay zekâ odağında bakış: Tanımlar, ilişkiler ve bileşenler. *Yönetim ve Ekonomi Dergisi*, 31 (2), s. 305.

⁴⁷²bkz. ETBİS. *İstatistikler*. <https://www.eticaret.gov.tr/istatistikler> .Erişim Tarihi: 19.05.2025.

⁴⁷³ Koparan ve Doğan, s. 296-299 ayrıca bkz. Ticaret Bakanlığı. *E-ticaret bilgi platformu: E-ticarete giriş eğitimi*. <https://www.eticaret.gov.tr/cevrimiciegitim/e-ticarete-giris-egitimi-12>, Erişim Tarihi: 16.05.2025.

⁴⁷⁴ R.G. 05.11.2014 T. ve 29166 S.

⁴⁷⁵Koparan ve Doğan, 2024, S. 305. S. 305.

⁴⁷⁶Koparan ve Doğan, 2024, s. 306.

3.1.2. E-ticarette yapay zeka teknolojilerinin rolü

E-ticaret platformlarının bugünkü büyüme ve satış hacmini yapay zekaya borçlu olduğu söylenebilir. Nitekim, e-ticaret ve pazarlama alanları yapay zekanın en çok kullanıldığı alanlardan biridir. Chatbotlardan müşteri taleplerinin tahmin edilerek satışları arttıracak yöntemler sunan öneri sistemlerinden, tedarik ve lojistik süreçlerini eş zamanlı olarak bilgi paylaşımları ile destekleyen akıllı programlardan, insan hata riskini sıfırlayan güvenli ödeme sistemlerine kadar birçok alanda yapay zeka uygulamaları e-ticaret platformlarına destek olmaktadır⁴⁷⁷. Bu uygulamalar özellikle iş süreçlerinin optimize edilmesi, verimliliğin artırılması ve karar verme süreçlerinin iyileştirilmesi bakımından büyük potansiyellere sahiptir⁴⁷⁸.

Yapay zeka endüstriler ve uygulamalar için birçok fayda sunmaktadır. Veri toplama, girme ve ön işleme gibi dijital görevler ve depo stok seçimi ve üretim süreçleri gibi fiziksel görevler de dahil olmak üzere birçok rutin sıkıcı görevleri otomatik hale getirerek insanların yüksek değerli yaratıcı işler için serbest kalmalarına imkan tanınmıştır. Daha az insan hatası ile fiziksel riskleri azaltan yapay zeka teknolojileri gelişmiş karar alma teknolojileri sayesinde daha doğru ve verilere dayalı daha güvenilir kararlar ve sonuçlar alınmasını sağlar. 7/24 ulaşılabilirlik sağlayan bu uygulamalar için mesai kavramı söz konusu değildir, dahası çıktıları arasında bir tutarlılık bulunmaktadır⁴⁷⁹.

2030 yılına kadar yapay zekanın, küresel ekonomiye 15.7 trilyon dolar katkıda bulunacağı ve ülke ekonomilerini ortalama %26 oranında büyüteceği beklenmektedir. Gelişmiş ülkeler, bu muazzam pazarda paylarını muhafaza etmek ve daha da genişletebilmek için üniversiteler, araştırma merkezleri, teknoloji lideri şirketler ve girişimler aracılığıyla yapay zeka teknolojileri konusunda çalışmalar yapmaktadır⁴⁸⁰. Yapay zeka'nın gelir büyüme oranında %25'ten fazla bir iyileşme sağladığı belirtilirken 2024 yılında en çok verim alınan uygulamaların müşteri deneyimi, BT operasyonları, sanal asistanlar ve siber güvenlik olduğu ifade edilmektedir⁴⁸¹. Yapılan bir diğer araştırma, yapay zekayı kullanan birçok şirketin insan kaynaklarından yazılıma, bilişim departmanından ürün ve hizmet gelişimine ve servis operasyonlarından risk ve uyum alanlarına kadar birçok alanda maaliyetlerinin düştüğünü ifade etmektedir. Maaliyetleri azaltan, verimliliği ve etkililiği arttıran yapay zeka uygulamaları yüksek talep görmeye devam etmektedir. Nitekim, 2017 yılında en az bir yapay zeka uygulamasını kullanan şirketlerin oranı %20 iken, bu oran 2022'de %50'ye, 2024 yılında ise %72'ye yükselmiştir. Bu artış, yapay zekanın iş süreçlerinde yaygın ve stratejik bir araç haline geldiğini açıkça göstermektedir⁴⁸².

⁴⁷⁷ Smith, 2006, s.4; Koparan ve Doğan, 2024, s. 300.

⁴⁷⁸ Aygün, 2023, s.13.

⁴⁷⁹ IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim Tarihi: 19.05.2025).

⁴⁸⁰ TÜBİTAK BİLGEM (n.d.). *Üçüncü dalga yapay zeka teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ (Erişim tarihi: 18 Mayıs 2025).

⁴⁸¹ IBM (2024). *AI in action 2024*. <https://www.ibm.com/think/reports/ai-in-action#AI+roadmap> (Erişim tarihi: 19 Mayıs 2025).

⁴⁸² McKinsey & Company (2025). *The state of AI: How organizations are rewiring to capture value*. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/> (Erişim tarihi: 24 Mayıs 2025.)

Gelecek perspektifinde yapay zekaya duygusal zeka, doğal yetenek, yaratıcılık, karmaşık sorunlara ilişkin çözüm önerilerini ve etik kavramının ekleneceği öngörülmektedir. Yapay zeka işlevleri ve hacmi ile kimileri için korkutucu ve heyecan verici iken kimileri için ise etik sınırlar içerisinde kontrol altında tutulduğu sürece tehlikeli olmadığı çıkarımları yapılmaktadır⁴⁸³. Diğer yandan, yapay zekanın geliştirilmesi sürecinde etiğe ve yasal gerekliliklere gereken önem verilmezse yapay zeka uygulamaları etik kuralları ve kanunları ihlal edebilir, veri koruma kurallarını çiğneyebilir, uygulamaların kullanılmasında operasyonel riskler çıkabilir bu siber güvenlik açıklarına sebep olabilir⁴⁸⁴.

3.1.3. E-ticaret ve yapay zeka açısından kişisel verilerin önemi

Günümüz ekonomisinde bireylerin kişisel ve fiziksel özelliklerinin önemli bir potansiyel gücü bulunmaktadır. Şirketler bu verileri toplayarak ve işleyerek hedef kitlelerini kolaylıkla tespit eder, ilgi duyulan ürün ve hizmetleri belirler ve geliştirir ayrıca teşebbüsler reklam faaliyetlerini ürün ve hizmeti alan ve alma potansiyeli olan tüketicinin arama ve beğeni verilerine göre tasarlayarak özgüleştirebilir ve böylece satış hacimlerini artırır. Bireylerin, çevrimiçi işletmeler kişisel verilerini toplayıp dağıtırken gerçekte neler olup bittiğini anlamaları, gerçekte neler olup bittiğini doğrulayabilmeleri ise oldukça zordur. Bu durum, kişisel verilerin hakkının ihlalini oluşturur. Kişiselleştirme hizmetlerinin artması ile birlikte kişisel verilere ilişkin ihlallerin devamı hiç kuşkusuz gelecektir⁴⁸⁵. E-ticaretin gelecek vizyonuna olumlu bakılsa dahi e-ticaretin yaygınlaşmasının daha çok kişisel veri ihlaline, siber saldırılara, güvenlik ve etik ile ilgili tehlikeleri arttıracığına ilişkin endişeler de dile getirilmektedir⁴⁸⁶.

E-ticaretin güçlü askeri yapay zeka sistemlerinin çalışabilmesi ve kendilerini geliştirebilmeleri için büyük miktarda veriye ihtiyaç duymaktadırlar. Veri setleri ne kadar büyük olursa yapay zekanın o kadar iyi öğrenebilir ve böylece kendini daha iyi geliştirebilir. Çünkü algoritmanın çevre ile iletişimi ve bilgi edinmesi ancak veriler aracılığı ile mümkün olabilmektedir. Örneğin, bir fabrikada tüm makinalar ve süreçlerin sürekli veri üretmesi halinde, yapay zeka sayesinde daha fazla otomasyon ve optimizasyon elde edilebilir⁴⁸⁷.

Daha 10-15 yıl önce bilgisayarların, telefonların, e-maillerin hayatımızı ele geçirmesi ve bu teknolojik gelişmelerle yapılan faaliyetlerden veri üretilmesinden doğan endişeler dile getirilirken⁴⁸⁸; bugün yapay zeka kavramı günlük hayatımızın ücra köşelerine dahi girmiş durumdadır. İnternet teknik yapısının, profil oluşturma teknikleri ve diğer gelişmiş uygulamalar ile birlikte miktar ve hız bakımından ivme göstermesi ve veri toplama ve işleme faaliyetleri ise şirketler açısından da her zamankinden daha kolay ve ucuz hale gelmiştir⁴⁸⁹.

⁴⁸³Koparan ve Doğan, 2024, s. 308.

⁴⁸⁴IBM. *What is AI?* https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai (Erişim Tarihi: 19.05.2025).

⁴⁸⁵ Prins, 2006, s. 275.

⁴⁸⁶Koparan ve Doğan, 2024, s. 315.

⁴⁸⁷Tersi durumda, örneğin analog bir ortamda ve dijitalleştirilmiş verilerin olmadığı ortamlarda yapay zekanın etkililiğinden bahsedilemez. European Commission (2018, April 25) . *Artificial intelligence for Europe* (COM (2018) 237 final) . <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Erişim Tarihi: 20.05.2025).

⁴⁸⁸ bkz. Küzeci, 2011 , s.142-149.

⁴⁸⁹Prins, 2006, s. 273; Akgül, 2014, s. 346.

Avrupa dünyasında akademik hayatta genel olarak kişisel verilerin meta olarak kabul edilmeyeceği ifade edilse de⁴⁹⁰ uygulamada durum tam tersi yönde işlemiştir⁴⁹¹. Nitekim, kişisel veriler sanal süpermarketlerde indirim veya belirli çevrimiçi hizmetlerine erişim imkanı sunarak fayda karşılığı alınabilen bir meta haline dönüşmüştür. Veri pazarlamacıları ve ticari şirketlerce veri toplanması ve işlenmesine büyük yatırımlar yapılmakta; internet üzerinde tüketici davranışları izlenmekte, kaydedilmekte, incelenmekte ve diğer faktörlerle ilişkilendirilmektedir. Böylece pazarlama ve ticari stratejilere dönüştürülen ve şirketlerin hizmet kalitesini arttıran işlenen kişisel veriler karşısında yatırımcılar büyük kazançlar elde etmektedir. Bunların yanı sıra kişisel verilerin bir güç haline geldiği günümüz dünyasında birçok şirket, elinde bulundurduğu müşteri kişisel listeleri ile veri tabanlarını satarak doğrudan kazanç elde etmeye başlamıştır⁴⁹². Bu durumda en iyi ihtimalde müşteriler bilgilendirilmektedir. Google'ın gizlilik politikasında yer alan: *“Google başka bir şirketle birleşme, şirket satın alma veya varlık satma faaliyetinde bulunursa, kişisel bilgilerinizin gizliliğini sağlamaya devam ederiz ve kişisel bilgiler devredilmeden ya da farklı bir gizlilik politikasına tabi olmaya başlamadan önce, bu durumdan etkilenecek kullanıcılara bildirimde bulunuruz.”* ifadesi de bu gerçeği yansıtmaktadır⁴⁹³.

Günümüzde ticari bakımdan büyük öneme sahip olan kişisel verilerin ekonomiye katkı sağlayabilmelerinin yani serbest dolaşımlarının öncelikli koşulu korunmalarıdır⁴⁹⁴. Yapay zeka teknolojisine gerek işletmeler gerekse bireylerin güvenebilmeleri; bu teknolojinin doğurduğu risklere karşı haklarının güvence altına alındığından emin olmaları ve hakları ihlal edildiğinde müracaat makamlarını bilmeleri ile mümkündür. Örneğin YZ uygulamalarının ilk kullanımları esnasında öngörülemeyen şekilde çalışması, yapay zeka algoritmalarının yanlış kullanımı veya sistemden kaynaklı sıkıntılara karşı ortaya çıkacak kişisel verilerin korunması ihlallerinde tazminat mekanizmaları ve çözüm yollarının ilgili kişilerce bilinmesi halinde YZ aktif şekilde kullanılabilir. Hukuki öngörülebilirliğin olmadığı hallerde yapay zekanın grift yapısı insanları yalnızca kendisinden uzaklaştıracaktır.

Dijital teknoloji çağında, kimi zaman bireylerin kişisel verilerinin toplanmasından haberi dahi olmamaktadır. Bu veriler genellikle kurumların ve şirketlerin veri tabanlarında muhafaza edilmektedir. Bu ise bir başka kişisel veri ihlalini oluşturmaktadır. Sholtz, bu durumu şu şekilde açıklamıştır: *“İşin püf noktası, bilgi akışını yöneten kısıtlamaları tam olarak doğru şekilde elde etmektir. Aşırı kısıtlayıcı kontroller ekonomik değeri azaltır; ancak diğer yandan tamamen açık ve özgür bilgi ticareti (bugünün ekonomisinde kişisel bilgi alışverişinde olduğu gibi) genellikle çok verimsizdir. Bilgi üreticilerinin hakları ile bilgi tüketicilerinin ihtiyaçlarını dengeleyen mutlu bir ortam gereklidir”*⁴⁹⁵.

Yapay zeka algoritmalarının eğitilmesi ve fonksiyonlarını gerçekleştirmesi için büyük veri setlerine ihtiyaç duyması karşısında temel insan hakkı olarak nitelendirilen kişisel verilerin akıbetinin ne olacağı üzerinde durulmalıdır. Avrupa Komisyonu, AB içinde yapay zeka

⁴⁹⁰bkz. yukarıda ”2.3.Kişisel Verilerin Hukuki Niteliği” başlığı.

⁴⁹¹ Beklenenin aksine, Avrupa düzenlemelerinin esasında tarafların Avrupa veri koruma rejiminin herhangi bir müdahalesi olmaksızın kişisel verilerini ticari olarak kullanmalarına izin verdiğine ilişkin eleştiri için bkz. Prins, 2006, s. 289.

⁴⁹² Prins, 2006, s. 275-276; Aksoy, 2010, s.68.

⁴⁹³bkz. Google gizlilik prosedürü için bkz. Google. *Privacy & terms: Privacy policy.* <https://policies.google.com/privacy> . (Erişim tarihi: 10 Mayıs 2025) .

⁴⁹⁴ Prins, 2006, s. 287, 297, Aksoy, 2010, 79; Akgül, 2014, s. 343.

⁴⁹⁵ Bkz. Sholtz 2001, “Redefining the Market for Privacy” .

uygulamalarının geliştirilmesi için gereken veri havuzunun sağlanmasının teşvik edilmesini ve kişisel olmayan verilerin serbest akışının sağlanması gerektiğini belirtirken diğer yandan da yapay zeka bağlamındaki uygulamalar kapsamında kişisel veriler niteliği haiz veriler hakkında GDPR'ın uygulama alanı bulacağını belirtmektedir. Nitekim AI Act, giriş, para. 27 ve 28'de bu husus düzenlenmiştir⁴⁹⁶.

3.2. E-Ticarette Kullanılan Yapay Zeka Uygulamaları ve Kişisel Veri İşleme Süreçleri

3.2.1. Genel olarak

Ticaretin rekabetçi dünyasında ayakta kalmak isteyen e-ticaret işletmelerine bugün uzmanlarca önerilen yapay zeka teknolojisini sistemlerine entegre etmeleri ve bu teknolojinin sağladığı imkan ve kolaylıklardan faydalanmalarıdır⁴⁹⁷. Müşterilere verilen hizmetleri kişiselleştirme, verileri doğru işleme ve müşterilerinin güvenini kazanma gibi konularda, YZ uygulamalarına erkenden yatırım yapan e-ticaret işletmelerinin rakiplerinin önüne kolaylıkla geçebileceği; aksi halde sektörün ve rakiplerin gerisinde kalınacağını ise kaçınılmaz olduğu ifade edilmektedir⁴⁹⁸.

Dijitalleşen dünyada, insanlar her alanda hız, kolaylık ve çeşitlilik beklentisi içindedir. Bugün şirketler bu beklentileri karşılamak, müşteri deneyimini zenginleştirmek ve marka imajlarını yükseltmek için pazarlama stratejilerinden, müşteri temsilcilerine, lojistik sevkiyatlarından depo kontrollerine kadar birçok alanda yapay zeka teknolojisinden yararlanmaktadır. Böylece karşılaştıkları problemleri minimize ederek tüketici ihtiyaçlarını karşılayabilmekte, yapay zekanın eş zamanlı birden fazla işlem yapabilme becerisini kullanarak daha kaliteli hizmet sunabilmekte, görevleri otomatikleştirerek süreçleri hızlandırabilmekte ve potansiyel müşteriye çekmek için doğru stratejiler oluşturabilmektedir. YZ teknikleri sayesinde insan kaynaklı hataları minimuma indirerek verimliliği arttıran e-ticaret işletmeleri, bu teknoloji sayesinde maliyetleri de düşürerek kazanç sağlamaktadır⁴⁹⁹.

Belirtilmelidir ki; her geçen gün yapay zekanın e-ticaret piyasası üzerindeki etkisi artmakta ve uygulanma alanı genişlemektedir. Ne var ki, e-ticarette kullanılan yapay zeka uygulamaları sunduğu birçok faydanın yanı sıra teknik yapısı ile işlediği büyük veri kümeleri ile tüketici mahremiyeti, temel hak ve özgürlükler(başta kişisel verilerin korunması hakkı olmak üzere) ile etik ilkeler bakımından riskler barındırmaktadır⁵⁰⁰. E-ticaret sektörünü şekillendiren dinamik yapıyla yapay zeka uygulamalarının⁵⁰¹ çalışma konumuz olan kişisel verilerin korunması çerçevesinde değerlendirilmesi ve taşıdığı risklerin boyutunun anlaşılabilmesi için bu uygulamaların teknik altyapısının, kullanılan YZ tekniklerinin ve çalışma mekanizmalarının bilinmesi gerekmektedir. Çalışmamızın bu bölümünde e-ticaret

⁴⁹⁶Benzer şekilde, Avrupa Konseyi, Yapay Zeka ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi'nde Sözleşme'nin Avrupa Konseyi kişisel mevzuatı gözetilerek hazırlanmıştır. Council of Europe (2024, September 5) . *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225) . Giriş, para. 16. <https://rm.coe.int/1680afae3c> Erişim Tarihi: 21.05.2025.

⁴⁹⁷Tutsal ve Ventura, 2022, s. 357-364; Sağtaş, 2023, s.54-57; Güven, H., & Güven, E. T. A (2023) . Yapay zekâ uygulamalarının e-ticarette kullanımı. *International Journal of Management and Administration*, 7 (13), s. 89.

⁴⁹⁸Güven ve Güven, 2023, s. 89.

⁴⁹⁹Tutsal ve Ventura, 2022, s. 357-364; Sağtaş, 2023, s.54-57; Güven ve Güven, 2023, s. 69,88-89; Gülşen, İ (2019) . İşletmelerde yapay zeka uygulamaları ve faydaları: Perakende sektöründe bir derleme. *Tüketici ve Tüketim Araştırmaları Dergisi*, 11 (2), s.425.

⁵⁰⁰ Sağtaş, 2023, s.58; Güven ve Güven, 2023, s. 81,88-89.

⁵⁰¹ Koparan ve Doğan, 2024, s. 301.

sektöründe kullanılan YZ tabanlı uygulamalar tespit edilerek; bu uygulamaların teknik altyapıları, kullandıkları YZ teknikleri ve taşıdıkları riskler anlaşılmaya çalışılmıştır.

E-ticaret platformlarında chatbot ve sanal asistanlar, kişiselleştirme, öneri sistemleri, akıllı arama sistemleri, dinamik fiyatlandırma ve stok yönetimi gibi YZ tabanlı uygulamalar bulunmaktadır⁵⁰². E-ticaret sektörünü şekillendiren dinamik yapıyla yapay zeka uygulamalarının⁴³⁰ kişisel verilerin korunması çerçevesinde değerlendirilmesi için söz konusu uygulamalar özelinde değerlendirme yapmak daha anlamlı olacaktır. Bu bakımdan aşağıda e-ticaret platformlarında kullanılan yapay zeka tabanlı uygulamaların teknik altyapıları, kullanılan yapay zeka teknikleri ile oluşturdıkları riskler açıklanmıştır.

3.2.2. Yapay zeka tabanlı sohbet botları (Chatbot ve sanal asistanlar)

E-ticaret işletmeleri müşteri memnuniyetinin artırılması ve kaliteli hizmet standartlarının sağlanması için gün geçtikçe daha çok chatbotlar ve sanal asistanlara yönelmektedir. Bugün bu programlar işletmeler tarafından müşteriler ile etkin iletişimde kullanılan en popüler yapay zeka tabanlı uygulamalar olarak karşımıza çıkmaktadır⁵⁰³. Nitekim, her geçen gün başka bir markanın sanal asistanının piyasaya sürülmektedir. Önceden temel olarak e-ticaret platformlarında gördüğümüz chatbotlar da banka ve telekomünikasyon servis sağlayıcıları uygulamalarında çevrimiçi destek hizmetlerinde kullanılır hale gelmiştir⁵⁰⁴. Yapay zeka temelli bu uygulamalar, müşterilerin talep ve ihtiyaçlarının anlayabilmekte, insan hatasını ortadan kaldırdıktan sonra sistem arızalarının kolayca tespit edebilmekte, 7/24 müşteri desteğinin sağlamakta ve maaş külfetini kaldırarak işletme maliyetlerini düşürmeye yardımcı konumdadır. Daha birçok fayda sağlayan ve giderek popülerleşen chatbot ve sanal asistan uygulamalarının hizmet sağlayan bütün platformlara entegre edilmesinin kaçınılmaz olduğu kanaatindeyiz.

3.2.2.1. Chatbotlar

Chatbot insanlar ile sesli veya yazılı olarak iletişime geçen uygulamaları ifade etmektedir⁵⁰⁵. "Chat" (*sohbet*) ve "bot" (*robot*) kelimelerinden oluşmuştur. Yani Chatbot, sohbet eden/konuşan robot veya sohbet robotu anlamlarına gelmektedir. Sesli konuşma ve mesajlaşma arayüzleri bu uygulamaların insanlar ile iletişime geçebilmesine yardımcı olur. Chatbotlar bugün e-ticaret, bankacılık, sigorta, sağlık, eğitim ve daha birçok sektörde farklı amaçlara ulaşmak için kullanılmaktadır. Yapay zeka teknolojisinden yararlanarak kullanıcı deneyiminde bir devrim yaratan bu uygulamanın geliştirilmesindeki temel amaç; kullanıcıların işletmenin kendisi ve işletme ürün ve hizmetleri hakkındaki talep ve soruları karşısında bir çalışana ihtiyaç duymadan hızlı ve etkili şekilde çözüm bulunmak istenmesidir⁵⁰⁶.

⁵⁰² Güven ve Güven, 2023, s. 81,88-89.

⁵⁰³ Özgür, N (2023) . *Sohbet botları ve yapay zeka etiği* (Yüksek lisans bitirme projesi) İzmir Kâtip Çelebi Üniversitesi. <https://acikerisim.ikcu.edu.tr/yayin/1742489&dil=3&q=> (Erişim Tarihi: 30.05.2025); Güven ve Güven, 2023, s.86.

⁵⁰⁴ Başkaya, F., ve Karacan, H (2022) . Yapay zekâ tabanlı sistemlerin kişisel veri mahremiyeti üzerine etkisi: Sohbet robotları üzerine inceleme. *Bilişim Teknolojileri Dergisi*, 15 (4), s.487.

⁵⁰⁵ İşeri, İ., Aydın, Ö., ve Tutuk, K (2021) . Müşteri hizmetleri yönetiminde yapay zeka temelli chatbot geliştirilmesi. *European Journal of Science and Technology*, (29), s. 358.

⁵⁰⁶ İşeri, 2021, s.358; Özgür, 2023, s.1; Sağtaş, 2023, s.56; Başkaya ve Karacan, 2022, s. 487 vd; Türkiye Cumhuriyeti Ticaret Bakanlığı, Chatbot Kurgusunun Yapılması, <https://www.eticaret.gov.tr/cevrimiciegitim/chatbot-kurgusunun-yapilmasi-64> (Erişim Tarihi: 02.06.2025) .

Chatbotlar, kullanıcı arayüzünün kolaylığına algoritmalara ve kullanılan teknolojilere göre üç ana gruba ayrılmaktadır. Bunlar: Menü/Buton Tabanlı Chatbotlar, Anahtar Kelime Tanıma Tabanlı Chatbotlar ve Bağlamsal Chatbotlar'dır⁵⁰⁷:

- **Menü/Buton Tabanlı Chatbotlar:** menüler ve butonlardan oluşur. Karar ağacı ilkelerini uygulayan sohbet robotları burada nihai davranışı/cevabı bulmak için müşterinin verdiği kararları takip eder. Yapay zeka teknolojisi kullanılmayan bu türde, menüden seçenekleri seçmek sureti ile müşterilerin daha derine inmesi sağlanır. En yaygın ve en basit olan chatbot uygulaması olmasına rağmen uygulamadan yanıt alınma süresi yavaştır ve talep edilen çözümün sunulmasında tam anlamıyla tatmin sağlamaz. Yapay zeka teknolojisi kullanılmadığı için derinlemesine bir iletişim mümkün değildir ancak kısıtlı çerçevede cevaplar alınabilir. Bu doğrultuda uygulamadan alınan cevaplar zengin ve özgülenmiş olmayacaktır.
- **Anahtar Kelime Tanıma Tabanlı Chatbotlar:** tanımlanmış anahtar kelimeleri kullanarak çalışır. Müşterilerin söylediklerini dinler, özelleştirilmiş anahtar kelime listesi yardımıyla ve algoritmalara aracılığıyla uygun tanımlanmış cevabı verir. Sınırlı hizmet kabiliyetine sahip olan bu sistemin çalışması için basit kurallar yeterlidir. Her ne kadar gelişmiş olsa da verebileceği yanıtlar yalnızca belirlenen anahtar kelimelere karşılık hazırlanmış basmakalıp cevaplardır. Birbirleriyle ilişkili birkaç soru sorulduğunda “*anahtar kelimelerin*” çoğalması sebebiyle sistem başarısız olmaya başlayabilir. Bu türde ileri yapay zeka teknolojisi uygulamaya entegre edilmemekte; YZ teknolojisinden ancak kısmen faydalanılmaktadır.
- **Bağlamsal Chatbotlar:** bugün piyasadaki en gelişmiş Chatbot türüdür. Müşterinin talep ve şikayetlerinin tam olarak anlaşılması ve konu ile ilgili cevabın düşünceli olarak verilmesi amaçlanır. Müşteri ile etkileşimlerinden, geri bildirimlerden ve deneyimlerinden öğrenebilen bu Chatbot türü zamanla kendini daha da geliştirir. Müşterilerin, örneğin bir yemek dağıtımı uygulamasında, ödeme seçenekleri, adresleri, beğenileri, yemekleri inceleme süreleri veri tabanlarında saklanır. Bu veriler analiz edilerek kullanıcıya bir sonraki siparişi için önerilerde bulunulur. Yapay zeka teknolojisine entegre edilen bu chatbot türü çalışmamızın konusunu ihtiva etmektedir. E-ticaret platformlarında bugün kullanılan bağlamsal Chatbot uygulamaları; gelen taleplere ve sorulan sorulara zekice cevaplar verebilir hale gelmiştir. Müşteriler ile daha karmaşık ve esnek sohbetler gerçekleştirebilen günümüz Chatbot uygulamaları sanki bir makina ile değil bir insan ile konuşuyor izlenimi yaratmaktadır⁵⁰⁸. Yeni nesil chatbot çözümleri, her diyalogdan yeni şeyler

⁵⁰⁷ Gupta, A., Hathwar, D., & Vijayakumar, A. (2020). Introduction to AI chatbots. *International Journal of Engineering Research and Technology*, 9 (7), s. 255-256; Özgür, 2023, s.9-10.

⁵⁰⁸ Güven ve Güven, 2023, s.86; Sağtaş, 2023, s.56.

öğrenebilirler ve farklı tip sorulara uyum sağlayabilmesinin yanında ayrıca yazım hatalarını ve hazırlıksız soruları anlamaya odaklanmıştır⁵⁰⁹.

İletişim tabanlı hizmet veren Chatbot uygulamaları, sahip oldukları büyük veri havuzu ile müşteri soru ve taleplerine hızlı şekilde cevap verebilmektedir. Müşterilerin 7/24 kesintisiz erişim sağlayabildiği ve istedikleri zaman anlık destek bulabildikleri Chatbot uygulamalarının amacı, var olan müşteri ihtiyaçlarını karşılamak ve daha iyi bir kullanıcı deneyimi sunmaktır⁵¹⁰. Satış öncesi ve sonrası destek sunan Chatbotlar, ürün tanıtımı da yaparak satış danışmanları gibi hizmet verebilmekte ve tüketicileri satın alma sürecine kadar götürebilmektedir. Siparişin oluşturulmasında da etkin rol oynayan ve sepette kalan ürünü müşterilere hatırlatan bu uygulamalar; e-ticaret işletmeleri için canla başla çalışmaktadır. Özellikle değişim ve iade işlemleri desteği ile satış sonrası müşteri hizmetlerine de destek olan Chatbotlar birbirini tekrarlayan işleri otomatikleştirerek; işletmelere özellikle zaman ve para yönünden tasarruf sağlamaktadır. Bu işlemlerin gerçekleştirilmesi sırasında geleneksel müşteri hizmetlerine bağlanmadaki bekleme sürelerinin olmaması ise bu uygulamaları daha verimli hale getirmektedir⁵¹¹.

Belirtilmelidir ki; Chatbot uygulamalarının tahmin edildiğinden daha çok yeteneği bulunmaktadır⁵¹². Müşteri hizmetleri bu uygulamanın çıkış yaptığı alandır. Chatbotlar ayrıca satış ve pazarlama için etkili birer araçtır; potansiyel müşteri ve ziyaretçi bilgilerini toplayarak analiz eden bu uygulamalar doğru hedef kitlesi ile doğru iletişim stratejilerinin geliştirilmesinde pay sahibidir⁵¹³. Chatbot uygulamaları ayrıca, halihazırdaki müşterileri verilerinin toplanmasında böylece kişiselleştirilmiş kullanıcı yaklaşımın sağlanmasında önemlidir⁵¹⁴. Chatbot uygulamasına verilebilecek güzel örneklerden biri Getir markasının “*Getir Destek*”⁵¹⁵ uygulamasıdır.

3.2.2.2. Sanal asistanlar (Digital asistant)

Sanal asistanlar, yapay zeka yardımıyla insan diyaloglarını taklit eden ses ve metin temelli komutları gerçekleştirebilen böylece insanları asiste edebilen, görevlerini otonom şekilde gerçekleştirebilen yazılımları ifade etmektedir. Günümüzde özellikle sesli sanal asistanlar giderek popülerleşmektedir. Nitekim, yapılan bir araştırmada, kullanıcıların konuşmadan metin tabanlı etkileşime göre daha yüksek verim alındığını, daha düşük bilişsel çaba gösterildiğini, kullanıcının daha büyük keyif aldığını ve daha yüksek hizmet memnuniyeti

⁵⁰⁹Türkiye Cumhuriyeti Ticaret Bakanlığı, Chatbot Kurgusunun Yapılması, <https://www.eticaret.gov.tr/cevrimiciegitim/chatbot-kurgusunun-yapilmasi-64> . Erişim Tarihi: 02.06.2025.

⁵¹⁰ Gupta, Hathwar & Vijayakumar, 2020, s. 256, Özgür, 2023, s.1; Sağtaş, 2023, s.56.

⁵¹¹ Özgür, 2023, s.6-7,11.

⁵¹² E-ticaret sektörü dışındaki alanlarda örneğin, mizahçı chatbotları kullanıcının mizah seviyesini yorumlamak için şakaları dinleme özelliğine sahiptir, şakaları anlayarak, görüntü veya metinsel karşılıklar verir. Bunun yanı sıra güvenlik ve protokoller ile ilgilenen chatbotlar da vardır. Bkz. Gupta ve ark., 2020, s. 257.

⁵¹³ Gupta ve ark., 2020, s. 256.

⁵¹⁴ Özgür, 2023, s.1; Sağtaş, 2023, s.56.

⁵¹⁵ CBOT, En İyi Chatbot Ödülü Haberi, <https://www.cbot.ai/tr/getir-destek-alfa-awards-2023te-en-iyi-sanal-asistan-chatbot-odulunun-sahibi-oldu/> (Erişim Tarihi: 31.05.2025) .

gösterdiğini ortaya konulmuştur⁵¹⁶. Sesi, konuşmayı ve metni anlayarak cevap veren sanal asistanlar, metinden sese(TTS) ve sestten metne(STT) dönüştürme yeteneğine sahiptir⁵¹⁷.

Bugün birçok hizmet sektöründe sanal asistanlar kullanılmaktadır. Örneğin sigorta sektöründe sanal asistanlar, müşteriler tarafından paylaşılan görüntüleri görüntü tanıma ve sınıflandırma teknolojisini kullanmak sureti ile inceleyerek “uzaktan hasar tespiti” yapmak için kullanılmaktadır⁵¹⁸. E-ticarete kullanılan sanal asistanlar ise ürünler, platformun işleyişi ve siparişleri hakkında müşterilere bilgi vermekte ve platformun sistem organizasyonu dahil olmak üzere karşılaştıkları tüm sorunlara anlık ve hızlı çözümler sağlayabilmektedir. Hızlı sipariş ve ödeme işlemlerine yardımcı olan sanal asistanlar işletmeler için yoğun rekabet ortamında bir avantaj unsuru haline gelmiştir. Satış öncesi ve satış sonrası destek sağlayan YZ tabanlı bu uygulama sayesinde müşteri ile e-ticaret platformu alışveriş deneyiminin her adımında irtibatla kalmakta öylece müşteri ile marka arasındaki bağ kopmamaktadır. Bu durum, müşteri deneyimini pozitif şekilde etkilemektedir⁵¹⁹.

Sanal asistan uygulamalarının, e-ticaret işletmeleri tarafından kullanılma amaçları kısaca: kullanıcı deneyimlerinin iyileştirilmesi ve satışların arttırmasının sağlanmasıdır. B uygulamaların en önemli yeteneklerinden biri, aşağıda açıklayacağımız öneri sistemlerini kullanarak kişiselleştirilmiş ürün hizmeti sunmasıdır. Böylece, işletmenin hedeflerini gerçekleştirip gelir elde etmesinde ve alışverişin tüketiciler için daha kolay hale gelmesinde etkili olmaktadır⁵²⁰. Diğer yandan, kişisel veriler analiz edilerek; müşteriye sunulan kişiselleştirilmiş kampanya ve indirimler, müşteri sadakatini pozitif yönde etkilemektedir⁵²¹. Sanal asistanlara; Apple’ın “Siri”si, Amozon’un Alexa’sı, Microsoft’un Cortana’sı ve Google Asistan örnek verilebilir⁵²². Başka bir örnek olarak Trendyol markasının “Trendyol Asistanı” verilebilir.

Akademik literatürde Chatbot ve sanal asistanların sıklıkla birlikte ve hatta birbirinin yerine kullanıldıkları⁵²³ görülmektedir. Donanımsal yazılımlara yüklenebilen ve hayatın her yerinde insanlara yardımcı olan sanal asistanların kullanım alanı chatbot uygulamasına göre daha geniştir. Fakat her iki uygulamanın, teknolojinin gelişmesi ile elde ettiği benzer kazanımlar arasındaki farkı belirsizleştirebilmektedir. Nitekim, *IBM Watson Başkan Yardımcısı Ruob High*, bu teknolojiler arasında ince ama belirgin farklılıklar olduğunu; bu farklılıkların genellikle

⁵¹⁶Rzepka, C., Berger, B., & Hess, T (2022) . Voice assistant vs. chatbot – Examining the fit between conversational agents’ interaction modalities and information search tasks. *Information Systems Frontiers*, 24, s.839–856. <https://doi.org/10.1007/s10796-021-10226-5> .

⁵¹⁷ Text to Speech (TTS) ve Speech to Text (STT) teknolojilerinin incelemesi için bkz.ORACLE, <https://www.oracle.com/tr/artificial-intelligence/speech/> (Erişim Tarihi: 02.06.2025) .

⁵¹⁸ bkz. AXA Sigorta, AXA’dan Dijital Asistan ile Hızlı Hasar Tespiti, <https://www.axasigorta.com.tr/basin-bultenleri/axa-dijital-asistan-ile-hizli-hasar-tespiti> . Erişim Tarihi: 31.05.2025. Bankacılık sektöründe sanal asistan teknolojisi yoğun olarak kullanılmaktadır. Her geçen gün artan sana asistanlara; Ugi (Garanti BBVA), Maxi (İş Bankası), Bankacıbot (Yapı Kredi) örnek olarak verilebilir. Özgür, 2023, s. 14.

⁵¹⁹ Deligöz, K (2024) . E-ticarete yapay zekâ ile kişisel asistanların rolü. In T. Yolcu (Ed.), *Elektronik ticaret ve dijitalleşme* (ss. 31–32) . Özgür Yayınları, s.31-32; Arık, A., ve Zeren, D (2023) . Tüketicilerin sanal asistanları kullanma niyetinde etkili faktörlerin araştırılması. *Alanya Akademik Bakış*, 7 (1), s 27-49.

⁵²⁰ Örneğin, Netflix, kullanıcıların izleme geçmişi ve beğenilerini analiz ederek kullanıcının sevebileceği düşünülen kişiselleştirilmiş film ve dizi önerileri sunmaktadır.

⁵²¹ Deligöz, 2024, s.24-26.

⁵²² Özgür, 2023, s.6.

⁵²³ Özgür, sanal asistan uygulamalarını chatbotlar olarak nitelendirmektedir. Bkz. Özgür, 2023, s.6. Benzer şekilde bkz. Gupta ve ark., 2020, s. 257.

kullanıcıyı ne şekilde etkiledikleri ile ilişkili olduğunu ifade etmiştir. *Forrester Research başkan yardımcısı Thomas Husson*, Chatbotların temelde dinamik sıkça sorulan sorulara (SSS) karşılık geldiğini; sanal asistanların ise birçok chatbot ve sanal asistan deneyimlerinin bir araya getirilmesi ile oluştuğunu belirtmiştir. Daha geniş kapsamda ve yetenekte olan sanal asistanlar tüketiciler adına üçüncü taraflardan gelen araçları ve hizmetleri düzenlemekle görevlidir. Bu teknoloji kalitesini iyileştirmek için bağlama (kullanıcı girişi, veritabanlarından bilgilere erişim) güvenir ve kullanıldıkça daha yetenekli hale gelirler⁵²⁴.

3.2.2.3. Teknik altyapı ve kullanılan yapay zeka tekniği

Chatbot ve sanal asistanlarda; uygulamaların karmaşıklık seviyelerine ve müşterilere sunduğu potansiyel hizmetlerin kapsamına göre farklı yapay zeka tekniklerini kullanılmaktadır. Bugün yaygın olarak kullanılan Kurumsal düzeyde bir sohbet robotu, müşteriler veya çalışanlarla yaptığı görüşmelerdeki yapılandırılmamış metin verilerini analiz edebilir ve bunlardan içgörüler çıkarabilir. Analiz genellikle doğal dil işleme (NLP) ve makine öğrenimi gibi teknikler kullanılarak gerçekleştirilir. Analiz edilen metin verilerinden elde edilen içgörüler, müşteri davranışını bilgilendirmeye ve sohbet robotu performansını iyileştirmeye yardımcı olur⁵²⁵. Sanal asistanlar temel olarak doğal dil işleme (NLP) algoritmasını kullanılarak geliştirilen ve sesli komutlar verebilen uygulamalardır⁵²⁶. Müşterilerin talep ve isteklerinin tam olarak anlaşılabilmesi için müşterinin duyguları da anlaşılmalı çalışılır. Bu uygulamalar ayrıca ses tanıma, sesi metne dönüştürme teknolojilerinden de faydalanmaktadır⁵²⁷.

2018 yılında IEEE Uluslararası Veri Madenciliği Çalıştayı Konferansında, iş yoğunluğuna bağlı olarak mevsimlik müşteri temsilcisi çalıştıran B2C şirketleri için diyalog tabanlı yapay zeka teknolojisi temel alınarak geliştirilen “*Isa: Intuit Smart Agent*” isimli chatbot uygulamasında ise Chatbot uygulamalarında temel olarak kullanılan⁵²⁸ makina öğrenmesi, doğal dil işleme(NLP) gibi yapay zeka tekniklerinin yanı sıra farklı olarak yapay sinir ağı tekniğinin bu chatbot sisteminde kullanılacağı belirtilmiştir⁵²⁹. Geldiğimiz noktada, chatbot ve sanal asistan uygulamalarında öncelikle ve özellikle çeşitli doğal dil işleme(NLP)

⁵²⁴Techtarget, *What's the difference between chatbots and virtual assistants?*, https://www.techtarget.com/searchcio/answer/Whats-the-difference-between-chatbots-and-virtual-assistants?utm_source=chatgpt.com (Erişim Tarihi: 01.06.2025). Her iki uygulamada sohbet robotu uygulaması olmasına rağmen bu uygulamalar esasen farklı iş ve işlevlerde kullanılmaktadır. Chatbotları daha çok sıkça sorulan sorular üzerinde yoğunlaşmışken; sanal asistanlar kullanılan programları yönetme, hatırlatıcı ayarlama ve akıllı cihazları kontrol etme gibi görevlerde kişisel asistan görevi görerek daha geniş bir yetenek yelpazesi sunar. Chatbotları, karar ağaçlarına veya komutlara da dayanabilirken; sanal asistanlar karmaşık istekleri anlamak için doğal dil işleme (NLP) gibi gelişmiş yapay zekayı kullanır. Upwork, *AI Chatbot vs. AI Virtual Assistant: What's the Difference?*, <https://www.upwork.com/resources/ai-chatbot-vs-virtual-assistant>. Erişim Tarihi: 31.05.2025.

⁵²⁵ IBM, *Unstructured Data*, <https://www.ibm.com/think/topics/unstructured-data>, Erişim Tarihi: 19.05.2025.

⁵²⁶Özgür, 2023, s.6.

⁵²⁷Gupta ve ark., 2020, s. 255-256;

⁵²⁸Güven ve Güven, 2023, s.86; Sağtaş, 2023, s.56.

⁵²⁹Xue, Z., Ko, T.-Y., Yunchen, N., Wu, M.-K. D., & Hsieh, C.-C (2018). *Isa: Intuit smart agent, a neural-based agent-assist chatbot*. In *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, s.1423-1428. Ayrıca görev odaklı geliştirilen chatbot uygulamasının sahip olduğu özellikler sayesinde hizmet kalitesini koruyacağı ve müşteri temsilcilerinin iş yükünü önemli ölçüde azaltacağı belirtilmiştir. Xue, Ko, Yunchen, Wu & Hsieh, 2018, s. 1423.

tekniklerinin ve genel olarak derin öğrenme, makina öğrenimi ve son günlerde Gen AI⁵³⁰ yapay zeka tekniklerinin kullanıldığı görülmektedir⁵³¹.

Chatbot ve sanal asistan modelleri geliştirilirken ilk olarak modelde kullanılacak veriler hazırlanır. Daha sonra modelin bu veriler kullanılarak eğitilmesi aşaması gelir. Veri girdilerini alacakları platform ile model bağlantısı kurulur(örneğin, şirket whatsapp hattı ile şirket web sayfası bağlantısının kurulması), model eğitilirken bir yandan başarıları/kazanımları kontrol edilir. Daha sonra model canlıya alınarak, gerçek kullanıcı ile buluşturulur. Modelin öğrenme özelliğinin gerçekleştirilebilmesi için kullanıcı tarafından sorulan yeni sorular ve olası cevapları ile model tekrar eğitilir. Bu öğrenim sürekli tekrarlanmak sureti ile uygulamalar geliştirilir⁵³².

3.2.2.4. Hukuki ve etik değerlendirme

Veri gizliliği, kullanıcı verilerinin korunması ve etik sorunlar bu uygulamalar bakımından kritik sorunlardır⁵³³. Chatbot ve sanal asistanların kullanım özelliklerine bakıldığında özellikle gerçek zamanlı veri işleme özelliklerinin olduğunu görmekteyiz. Özellikle sesli komut sistemi kullanıldığında bu durum kullanıcıyı içinde bulunduğu alan da dahil olmak üzere kullanıcının sesinin tanınması, çevre koşulları, kullanıcının karakteristik ses yapısı özellikleri vs. ile istenmeyen üçüncü kişi konuşmalarının YZ veri tabanlarında saklanması sonucunu doğurabilir. Bu durumlar kişinin alışveriş deneyimi esnasında işlenmesine izin verdiği kişisel veriler kapsamında olmadığından hak ihlali doğurabilecektir.

Online servis hizmeti sunarak müşteri hizmet yönetimini gerçekleştiren Chatbotlar ve Sanal Asistanlar; müşteri ile birebirde kurdukları ilişki neticesinde müşterilere ilişkin kişisel verileri toplamada büyük bir potansiyele sahiptir. Kullanıcı ile etkileşimli olan bu sistemler topladığı kişisel veriler ile kullanıcıya daha iyi bir hizmet kalitesi sunmayı amaçlasa da; bu verilerin toplanma amaçları dışında işlenmesi ve analiz edilmesi de mümkündür⁵³⁴. Bu durum amaçla sınırlılık ilkesine aykırılık teşkil etmektedir (GDPR m.5-6, KVKK m. 4-5). Bu veriler her ne kadar şirket içi uygulamalarda kullanılarak daha kontrollü ortamlarda işlense de; müşteri verilerinin (isim, sipariş bilgisi, ödeme tercihi vb.) veri ihlallerine karşı korunması gerekmektedir. Bu bakımdan işletmelerin hangi tüketici verilerini işledikleri, hangi sürelerle muhafaza ettikleri (GDPR m.5; KVKK m.4), hangi kurum ve kuruluşlarla paylaştığı ve aktarım ve işleme amaçlarının neler olduğunu (GDPR m.44-50; KVKK m.8-9) belirten şeffaf veri işleme politikalarının oluşturulması ve bu konular hakkında müşterilerin aydınlatılması (GDPR m.12-13; KVKK m.10) gerekmektedir. Bu politikalar e-ticaret platformlarına karşı kullanıcı güvenini arttıracaktır⁵³⁵.

Sohbet robotları güvenlik ihlaline de vücut verebilir. Sürekli dinleme, ses verisi toplama ve kişisel cihazlara erişim halleri kişinin özel hayatına müdahale sonucunu doğurur. Bu müdahale hukuka aykırı olabileceği gibi hukuka uygun şekilde de yapılabilir. Her iki durumda

⁵³⁰ bkz. CBOT, *CBOT Chatbot Platformu ve Üretici Yapay Zeka Teknolojisi*, *CBOT | Türkiye'nin Lider Yapay Zeka Şirketi | Kurumsal Chatbot Projeleri* (Erişim Tarihi: 30.05.2025). Ayrıca bkz. Kirazlı, Ş. N (2024). *Chatbot özelinde üretken yapay zeka ve kişisel verilerin hukuka uygun işlenmesi / Processing of personal data in compliance with the law and generative artificial intelligence in the context of chatbots* (Yayımlanmamış yüksek lisans tezi). Sakarya Üniversitesi.

⁵³¹ İşeri, 2021, s.358; Güven ve Güven, 2023, s.86; Sağtaş, 2023, s.56; Sağtaş, 2023, s. 257.

⁵³² İşeri, 2021, s.360.

⁵³³ Deligöz, 2024, s.31-32.

⁵³⁴ Başkaya ve Karacan, 2022, s. 487.

⁵³⁵ Deligöz, 2024, s.31-32.

da kullanıcı kişiliğinin korunması bakımından risk teşkil etmektedir. Hukuka uygun müdahalede işletmelerce uygun teknik ve idari tedbirlerin(GDPR m.32; KVKK m.12) alınması temel hak ve özgürlüklerin korunması anlamında hayatidir. Hukuka aykırılık hallerinde veri sorumlusu ilgili kişiye maddi-manevi tazminat(GDPR m.82; KVKK m.14), idari para cezası(GDPR m.83; KVKK m.18) ve TCK⁵³⁶ m.135-138 kapsamında^[OBJ] cezai yaptırımlar(müeyyideler) ile karşılaşacaktır.

3.2.3. Öneri sistemleri (Recommendation engines/Recommender systems)

Daha önce insanlar tarafından uzun zaman ve büyük maliyetlerle gerçekleştirilen tüketicilere ilişkin büyük miktardaki verinin toplanması ve analiz edilmesi faaliyetleri artık yapay zeka tarafından yapılmaktadır. Yapay zeka, algoritmalar aracılığı ile bu işlemleri çok kısa sürelerde, düşük maliyetlerle ve otomatik olarak gerçekleştirmektedir. Ayrıca daha rasyonel ve kesin çıkarımlar elde edebilmektedir⁵³⁷. Bu işlemlerden birisi de öneri sistemleridir.

Öneri sistemleri, makine öğrenimi tekniği kullanılan, büyük veri analizi sayesinde duyulan ihtiyaçlar hakkında tahmin yürütebilen bir uygulama türüdür. Sistem temel olarak kullanıcı davranışlarını gözeterek olasılığı tahmin etmeye çalışan bilgi filtreleme sistemi ile çalışır. Böylece sonucun yani “tahminin” doğruluk yüzdesi yüksek olur⁵³⁸.

Finansal hizmetler, sigorta, restoranlar, tekstil, çevrimiçi flört siteleri de dahil olmak üzere birçok alanda kullanılan öneri sistemleri, ticaret alanında da yoğun olarak kullanılmaktadır⁵³⁹. Müşteri verilerinin analizine dayanan yapay zeka tabanlı öneri sistemlerinin e-ticaret sektöründe temel olarak iki hayati görevi gerçekleştirdiğini söyleyebiliriz. Bunlar: Tüketici Segmentasyonu ile Hedef Tespiti ve Kişiselleştirilmiş Müşteri Deneyimidir.

3.2.3.1. Tüketici segmentasyonu ile hedef kitle tespiti

Yapay zeka, e-ticaret pazarını daha iyi anlamak ve etkili şekilde pazar stratejisi belirlemek adına tüketici segmentasyonu yapmaktadır. Tüketici segmentasyonu ile tüketiciler farklı gruplara ayrılarak benzer ihtiyaç, davranış, tercihlere sahip tüketiciler gruplandırılmaktadır. Müşteri segmentasyonu işleminde; coğrafi, sosyo-demografik, sosyal, psikolojik, ekonomik, müşteri davranışı gibi kriterler gözetilir⁵⁴⁰. Segmentasyon, kişiselleştirilmiş ve etkili pazarlama stratejilerinin oluşturulması ve uygulanmasında ayrıca işletmeye daha fazla müşteri çekilmesinde ve sadık müşteri tabanının oluşturulması bakımından önemlidir⁵⁴¹.

⁵³⁶ 5237 Sayılı Türk Ceza Kanunu (R.G. 12.10.2004 T., 25611 S.)

⁵³⁷ Belhadj, M (2022) . *Pazarlama hizmetinde yapay zeka: Netflix öneri sistemi örneği / Artificial intelligence in the service of marketing: Case of Netflix recommendation system* (Yayımlanmamış yüksek lisans tezi) . Necmettin Erbakan Üniversitesi, s.12.

⁵³⁸ Chate, P. J (2019) . The use of machine learning algorithms in recommender systems: A systematic review. *IJRAR – International Journal of Research and Analytical Reviews*, 6 (2), s. 671.

⁵³⁹Chate, 2019, s. 671.

⁵⁴⁰Beane, T. P., & Ennis, D. M (1989) . La segmentation des marchés: Une revue de la littérature. *Recherche et Applications en Marketing*, s.14.

Aktaran: Irina, I (2016) . What is marketing automation and how could it be used for business? *Yearbook of the 'Gheorghe Zane' Institute of Economic Researches, Jassy / Anuarul Institutului de Cercetări Economice 'Gheorghe Zane' Iași*, 25 (1), 11–28.

⁵⁴¹ Sağtaş, 2023, s.54; Irina, 2016, s. 14.

Segmentasyon faaliyetinde yapay zeka kullanımının avantajı aynı davranış ve ihtiyaçlara sahip olan grupları belirlemede geleneksel araçlardan daha verimli ortam sunmasıdır. Örneğin, 20-25 yaş alışveriş bağımlısı grupların, gösterilen topuklu ayakkabılara ilgi duyması verisi karşısında; bu grubun orta sınıfın biraz üstünde kalan lüks markalara daha fazla ödeme yapacağı çıkarımını oluşturabilen segmentasyon ticari işletmelere kar elde ettirmektedir⁵⁴². Diğer yandan hamile veya çocuklu kadın gruplara satış hedefini gerçekleştirmek için e-ticaret sitesinde genellikle çocuk kıyafetleri gösterilmesi de segmentasyonun etkinlerindendir.

Öneri sistemleri, e-ticaret platformlarının doğru hedef kitlesini belirlemesine yardımcı olmaktadır. Nitekim, ürün ve hizmet satışlarının gerçekleştirilebilmesi için müşteri profilinin diğer bir ifade ile hedef kitlenin işletmelerce iyi bilinmesi gerekmektedir⁵⁴³. Doğru ve etkili hedefleme yaparak doğru demografiye öneriler sunmak doğru müşteriye ulaşarak işletmenin kar elde etmesini ve böylece ticari hayatta başarıyı getirmektedir⁵⁴⁴.

3.2.3.2. Kişiselleştirilmiş müşteri deneyimi

Öneri sistemi, veri filtreleme sistemlerinin bir alt sınıfıdır. Öneri sistemlerinin genel amacı; bir kullanıcının hangi tercihleri yapabileceğini önceden öngörmektir. Sistem, kullanıcıya ürün kataloğundan tercih edebileceğini kişiselleştirilmiş bir ürün seçkisi sunarak ürünleri bulmada ve satın almada müşteriye kolaylık sağlar⁵⁴⁵. Kullanıcı geçmişine dayalı kişiselleştirilmiş ürün öneri sistemleri özellikle son on yıldır işletmeler tarafından sıkça kullanılmaktadır⁵⁴⁶.

Öneri sistemlerinin çalışabilmesi için müşterilerin etkileşimi; gönderilen/alınan e-postalar, açılan/açılmayan e-postalar, müşterinin özellikleri, girilen kampanyalar, önceki satışlar, ürün üzerinde gezinme süreleri, etkinliklere katılımlar, izlenen web seminerleri, indirilen varlıklar gibi faktörler değerlendirilir⁵⁴⁷. Temel olarak tüketicilerin yalnızca alışveriş davranışları dikkate alınır⁵⁴⁸. Bağlamsal kullanıcı davranışı ve verilerinden yararlanan bu sistemde, kişilerden bir şeyler öğrenmek istenir. Davranış analizi ve diğer kullanıcı profilleriyle karşılaştırmalar yoluyla kişilerin seçebilecekleri içerik hakkında doğru tahminler sunulmaya çalışılır⁵⁴⁹. Örneğin bir sonraki satın almanın tahmin edilmesi için bir e-ticaret platformunda alışveriş yapan müşterinin davranışları sistem tarafından bir süre izlenir. Bu veriler aşağıdaki davranışlar gözetilerek değerlendirilir ve bu sayede sistem bir tahmin geliştirebilir⁵⁵⁰:

- Bu ürünler birlikte satın alındı verisi ile bu ürünleri satın alan kişiler bu gibi benzer satın alma işlemleri yapabilir çıkarımı elde edilebilir.
- Bu ürüne ilgisi olan kişiler bilgisinden ilişkili başka ürünlere de ilgi duyabilir çıkarımı yapılabilir.

⁵⁴² Belhadj, 2022, .12-13.

⁵⁴³ Güven ve Güven, 2023, s.81-82.

⁵⁴⁴ Karaman, Ö (2021) . Yapay zeka destekli kişiselleştirme algoritmalarının tüketici zihninde filtre balonu yaratma etkisinin incelenmesi. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 12 (32), s.1344.

⁵⁴⁵ Belhadj, 2022, s.15; Güven ve Güven, 2023, s.80.

⁵⁴⁶ Deligöz, 2024, s.24-26.

⁵⁴⁷ Irina, 2016, s. 14.

⁵⁴⁸ Sağtaş, 2023, s.54; Tutsal ve Ventura, 2022, s. 364.

⁵⁴⁹ Belhadj, 2022, s.16.

⁵⁵⁰ Belhadj, 2022, s.15.

- Ürüne yüksek puan veren kişiler kimlerdir tespit edilerek bu veriden, ürünü beğenen kişiler ile benzer profillere sahip kişilerin bu ürünleri satın alma olasılığı yüksektir çıkarımı yapılabilir.

Tahmine dayalı analitik karmaşık bir süreçtir ve en iyi sonuçları elde edilmesi için müşteri geçmişine ilişkin verilerin toplanması çok önemlidir⁵⁵¹. Veri toplama, web sitesindeki çerezler⁵⁵² (web sitesi ziyaretçisinin tarama bilgilerini kaydeden dosyalardır) ve e-ticaret platformları aracılığıyla yapılır. Oluşturulan veritabanı sayesinde yapay zeka tabanlı sistem, müşterilerin ihtiyaçlarını anlamak için toplanan verilerini analiz eder. Yapay zeka sayesinde, veri analizlerinin çok hızlı ve konu bakımından tutarlı olması sayesinde hiper bir kişiselleştirme yapılır. Hiper kişiselleştirme başka bir deyişle hiperpersonalizasyon, her müşteriyle özel olarak ilgilenilmesi; diğer müşterilerden bağımsız olarak iletişim kurulabilmesi anlamına gelir. Bu hiper-kşiselleştirme, ihtiyaçların gerçek zamanlı olarak tespit edilmesi yoluyla kalite hedeflemesine (mikro-segmentasyon) dayanır ve her müşteri için benzeri olmayan kişiselleştirilmiş bir deneyim yaratır⁵⁵³. Yapay zeka tabanlı chatbotlar ve sanal asistanlar müşteri deneyimini zenginleştirmek için bu teknolojiden yararlanır⁵⁵⁴.

3.2.3.3. Teknik altyapı ve kullanılan yapay zeka tekniği

E-ticarete müşterileri hizmetleri çerçevesinde sunulan öneri sistemlerinin ham maddesi kişisel verilerdir. Öneri sistemleri, bilinmeyen durumlar ve gelecek tahminleri için mevcut ve geçmiş verileri analiz eden veri madenciliği, modellemeler ve makina öğrenmesi gibi teknikler kullanmaktadır. Öneri sistemlerinin, bu tahminleri yapabilmesi için çok sayıda kişisel veri gereklidir. Sonrasında veriler arasındaki ilişki ve kalıplar çıkartılarak bu verilerin analizi sağlanmalıdır. Böylece müşteri davranışlarına ilişkin anlamlı örüntüler keşfedilebilir ve sistem tahmin yürütebilir hale gelir. Hiç geçmişi olmayan kullanıcılara sunulan öneriler, etkileşim benzerliklerinin güvenli şekilde ölçülmesi için yeterli olmadığından başarısız olabilir. Fakat kullanıcının platformda etkinliklerini sürdürmesi ile bu öneriler kendisini geliştirir⁵⁵⁵. Böylece sistem, müşterilerine daha kişiselleştirilmiş ve doğruluk yüzdesi yüksek tahminler sunabilir.

Öneri sistemlerinde, tahminlerin oluşturulması büyük veri ile doğal dil işleme(NLP), görüntü ve ses tanıma ve özellikle makine öğrenmesi gibi yapay zeka teknikleri kullanılarak gerçekleştirilmektedir⁵⁵⁶. Birden fazla ürün içerisinde müşteriye satın almada yardımcı olunmasında uzman sistem yapay zeka tekniğinin de kullanıldığı belirtilmiştir⁵⁵⁷. Böylece konu ile ilgili uzmanlaşan sistemler doğal dil işleme(NLP), görüntü ve ses tanıma teknikleri ile elde edilen veriler ile makina öğrenmesi kullanılarak sürekli kendilerini geliştirmektedir. Kullanılan

⁵⁵¹ Örneğin, sistem bir kullanıcının sürekli belirli tipte dondurma markası aldığını tespit ettiğinde diğer marka dondurmalarında indirim yaparak o markaların satışının da artmasını sağlıyor. Belhadj, 2022, s.14.

⁵⁵² Google Chrome'un websitelerindeki çerezleri adım adım kaldıracağı açıklaması karşısında; RTB House, çerezlerin yerini alması için bir yapay zeka uygulaması geliştirdiklerini duyurdu. RTB House'un yapay zeka çözümü ContentGPT, önceden eğitilmiş dönüştürücüler (generative pre-trained transformers, GPT) ve geniş / büyük dil modellerinden (LLMs) yararlanarak, web sayfalarını ziyaret eden kullanıcıların site içeriğini analiz ederek, özel ilgi alanları ve niyetleri hakkında bilgiler sağlamaktadır. Bkz. Oksijen (2023, Aralık 21) . *RTB House: 2024'te çerezlerin yerini yapay zeka dolduracak*. <https://gazeteoksijen.com/bilim-ve-teknoloji/rtb-house-2024te-cerezlerin-yerini-yapay-zeka-dolduracak-195788> (Erişim tarihi: 1 Haziran 2025) .

⁵⁵³ Belhadj, 2022, s.13-14.

⁵⁵⁴ Deligöz, 2024, s.24-26.

⁵⁵⁵ Chate, 2019, s. 672-673,675; Güven ve Güven, 2023, s.81-82; Belhadj, 2022, s.14-16.

⁵⁵⁶Güven ve Güven, 2023, s.80; Belhadj, 2022, s.15-16; Chate, 2019, s. 673-674.

⁵⁵⁷Güven ve Güven, 2023, s.80.

YZ teknikleri sayesinde müşterilerinin satın alma süreçleri derinlemesine araştırabilmekte; işleme, araştırma, inceleme aşamalarından elde edilen bulgulara göre pazarlama stratejileri oluşturabilmektedir⁵⁵⁸.

3.2.3.4. Hukuki ve etik değerlendirme

Öneri sistemlerinin, veri analizleri ve toplanan büyük ölçekteki kişisel veri havuzları ile müşterilerin mahremiyetlerini ihlal edilebilecek niteliktedir⁵⁵⁹. Nitekim, e-ticaret sitesi tarafından platform geçmişi sürekli olarak izlenen, kendisi hakkındaki kişisel veriler korumak amacıyla toplanan, kullanılan ve analiz edilerek kendisi hakkında daha fazla bilgiler elde edilen kişiyi şeffaflaştırabilir. Bu durum, kişinin maddi ve manevi varlığını geliştirme hakkı, özel hayatın gizliliği hakkı ile ilgili diğer temel hak ve özgürlüklerini ihlal eder niteliktedir. Müşteriler hakkında edinilen bilgilerin kişisel veri koruma kurallarına uygun şekilde elde edildiğinin, muhafaza edildiğinin ve saklama sürelerine uyulduktan sonra meşru menfaati bulunmadığı için yok edildiği hakkında e-ticaret platformlarının açıklanmalıdır⁵⁶⁰. Aksi halde kişisel verilerin korunması hakkı da ihlal edilecektir. Bu durum GDPR m.5 ve KVKK m.4’de belirtilen ‘belirli, açık ve meşru amaçlar için işleme’ ve ‘ilgili mevzuata uygun süre zarfında muhafaza edilme’ ilkeleriyle doğrudan ilişkilidir.

Kişisel verilerin korunması kurallarına uyulsa dahi gerçek kişi müşterilere ilişkin bu büyük veri havuzunun tehlikeli durumu işletmelerce gözetilmelidir. Nitekim, öneri sistemleri çok sayıda kişisel veriye eriştiğinden, bu verilerin kötü niyetli üçüncü kişilerin eline geçmesi veya sızdırılması ihtimali, ciddi bir risk oluşturmaktadır. İşletmelerce bu hususa ilişkin alınacak tedbirler dezavantajlı konumda bulunan bireyin korunması için gereklidir. Ayrıca, veri odaklı segmentasyon süreçlerinin belirli demografik gruplara karşı sistematik ayrımcılık yaratma potansiyeli karşısında şeffaf algoritmaların geliştirilmesi ve şirket içi teknik ve etik denetimin periyodik olarak sağlanması gerekmektedir. Müşterilere ilişkin veriler işletme için kararlar alınmasında anonimleştirilse dahi, büyük veri kümeleriyle bağlantılar kurularak geri tanımlama yapılabilir. Geri alınmanın mümkün olduğu ve kişinin veriler kullanılarak belirlenebildiği hallerde veri sorumlusu tarafından gerekli idari ve organizasyonel tedbirlerinin alınmalıdır⁵⁶¹.

Potansiyel riskleri sebebiyle ırk veya etnik köken, siyasi görüş, din veya inançlar, sendika üyeliği, genetik durum veya sağlık durumu, kılık kıyafeti veya cinsel yönelime ve diğer özel nitelikli kişisel verilere⁵⁶² dayanan kişiselleştirme faaliyetleri kural olarak yasaktır. Bu verilerin kişiselleştirme için kullanılmasına sadece özel koşullar altına izin verilebilir(GDPR, giriş, para.71). Bu kapsamda, bir e-ticaret şirketinin ticari stratejilerinin belirlenmesinde veri analiz çalışmalarının yürütülmesi kapsamında tüketicilerin satın aldığı kıyafet verilerinin işlenmesi halinde; bu veriler özel nitelikli veri olduğu için daha sıkı bir koruma altında olacaktır ve ancak sınırlı amaçlar ile işlenebilecektir(GDPR m.9 ve KVKK m.6.). Doktrinde bu durum

⁵⁵⁸Güven ve Güven, 2023, s.82.

⁵⁵⁹ Belhadj, 2022, s.14.

⁵⁶⁰ Müşterilerin bu konuların açıklanmasını konu alan ”Aydınlatma Yükümlülüğü“; KVKK m.10 ve GDPR, giriş, 32. paragrafında düzenlenmiş ve aşağıda ”3.3.2.1.1.3.Bilgilendirme Yükümlülüğü“ başlığı altında incelenmiştir.

⁵⁶¹Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.18; GDPR m.4/5.

⁵⁶² bkz. yukarıda ”2.7.1.Özel nitelikli kişisel veriler (Hassas kişisel veriler)” başlığı.

eleştirilerek bu sıkı uygulamanın katma değerli hizmetin üretimini engelleyebileceği bu sebeple katma değer gözetilerek istisna getirilmesi gerektiği belirtilmiştir⁵⁶³.

3.2.4. Akıllı arama sistemleri

E-ticaret işletmeleri için büyük bir öneme sahip olan arama optizasyonu; marka görünürlüğü arttırmanın yanı sıra tüketici eğilimlerinin çözülmesi, e-ticaret platformunun ihtiyaçlarının tespit edilmesi ile pazarlama stratejisi planlarının yapılması gibi faydalar sunmaktadır⁵⁶⁴.

3.2.4.1. Yapay zeka tabanlı akıllı arama sistemleri

Yapay zeka algoritmalarının en sık kullanıldığı alanlardan biri akıllı arama sistemleridir. Arama motorları, algoritmalar aracılığı ile milyonlarca veriyi tarayarak anahtar kelimler için ipucu araması yapar. Daha sonra arama sonuçlarını düzenleyerek kullanıcıya sunar. Bu sonuç listesinden bir seçim yapan kullanıcının bundan sonraki her eylemi arama motorunun öğrenmesini beslemektedir⁵⁶⁵.

Akıllı arama motorları kişiselleştirilmiş dijital reklamların oluşturulmasında da etkilidir. E-ticaret platformlarında gezinerek ürün arama ve fiyat karşılaştırması yapan kullanıcı, bıraktığı dijital ayak izlerinin yani ilgilendiği konulara ilişkin verilerin ve ilgilenme süresi verilerinin analiz edilmesi ile yapılan kişiselleştirme faaliyeti ile ilgisini çekebilecek reklamlarla karşılaştırılır. Örneğin arama motorunda “siyah demir döküm tava” araması yapan bir kullanıcı, sonraki internet gezinmeleri sırasında, sosyal medya da dahil olmak üzere, tava içerikli hedefli reklamlarla karşılaşır. Bu reklamlar kişinin satın alım aşamasına geçmesine yardımcı olarak işletmeye kazanç sağlar⁵⁶⁶. Bu durum müşterilerin YZ teknolojileri ile kişiselleştirilmesi ve öneri sistemlerinin kullanılması ile de ilişkilidir. Dolayısıyla e-ticaret platformlarında yer alan yapay zeka temelli uygulamaların ve tekniklerin birbirinden beslendiği çıkarımı yapılabilir.

3.2.4.2. Teknik altyapı ve kullanılan yapay zeka tekniği

Akıllı arama sistemlerinin çalışması için öncelikle sistem; yapılandırılmış ve yapılandırılmamış verileri içeren bir içerik kaynağına bağlanır. Ardından, tek bir ardışık içerik dizini oluşturulur ve doğal dil işleme(NLP) yapay zeka tekniği kullanılarak veriler içerik ve duygu analizi kullanılarak kategorilere ayrılır. Böylece içerikler arasında anlamsal ilişki kurulur. Akıllı puanlama algoritmaları ile kullanıcının sorgusuna cevap olarak en ilgili pasaj veya parçacık sağlanır⁵⁶⁷.

Akıllı arama sistemlerinde öncelikle insan dilinin anlaşılması için doğal dil işleme(NLP) yapay zeka tekniği kullanılır. Anlamsal arama ve bağlamsal anlayış sayesinde akıllı arama günlük dilde ve karmaşık belgelerde bulunan dilsel nüansları, eş anlamlıları ve ilişkileri parçalayabilir ve anlaşılır hale getirir. Ayrıca bu sistemlerde, birçok veri kaynağını aynı anda

⁵⁶³ Taştan,2017, s. 42.

⁵⁶⁴ Karaman, 2021, s.1344; IBM, *What is Intelligent Search?*, <https://www.ibm.com/think/topics/intelligent-search> , (Erişim Tarihi: 02.06.2025) .

⁵⁶⁵ Karaman, 2021, s.1344; IBM, *What is Intelligent Search?*, <https://www.ibm.com/think/topics/intelligent-search> , (Erişim Tarihi: 02.06.2025) .

⁵⁶⁶ Başalp, 2015,, s.78; Karaman, 2021, s.1345.

⁵⁶⁷ IBM, *What is Intelligent Search?*, <https://www.ibm.com/think/topics/intelligent-search> , (Erişim Tarihi: 02.06.2025) .

anlayabilecek bir belge anlama yapay zeka teknolojisi bulunmaktadır. Makina öğrenimi yapay zeka tekniği sayesinde, akıllı arama sistemleri, e-ticaret işletmelerine özgü belgeleri, grafik ve tabloları, sözleşme ve faturaları öğrenebilir. Derin öğrenme YZ tekniği sayesinde ise; kullanıcıya kusursuz ve eşzamanlı sorgu önerileri oluşturur ve arama sorgusu sonucu alaka düzeyini zaman içinde sürekli olarak iyileştirerek, hangi bilginin kullanıcılara en fazla değeri sağlayacağını tahmin eder. Yönlü ve filtrelenmiş arama sayesinde kapsam daraltılır ve veriler içinde aranan bilgi sistem tarafından bulunur⁵⁶⁸.

3.2.4.3. Hukuki ve etik değerlendirme

Akıllı arama motoru sisteminin işlevini gerçekleştirebilmek için kişisel verilerden yararlanılır. Örneğin, dünyanın en yaygın kullanılan arama motorlarından biri olan Google, kullanıcının aradığı bilgiyle en alakalı sonuçları; öncelikle arama terimi ile ilişkili verileri, resim veya video yüklenmesi halinde burada çözümlenen verileri, web'deki diğer veriler ile bağlantılarını, kullanıcının konumunu, kullanıcının arama ayarlarındaki kullandığı güncel dil ve ülke hatta bölge, güncel gelişmeleri dikkate alarak listelediğini ifade etmektedir⁵⁶⁹. Google'ın çalışma sisteminde kullanılan güncel konum, yaşanan bölge ve ülke ile kullanıcılar tarafından kullanılan dil kişisel verilerdir. Kimi zaman da arama motorlarına girilen verilerin analizi ile de kişi hakkında bilgi edinilebilir. Örneğin, 0-1 yaş bebek ürünlerini takip eden ve satın alan kişinin bebek sahibi olduğu veya yakın zamanda olacağı çıkarımı yapılabilir. Ayrıca tüketicilerin arama motorlarından arattığı hizmet ve ürünlerden kişilerin cinsel yönelimlerinin, hobileri, alışkanlıkları veya sosyal statüsü tahmin edilebilir.

Kullanıcılar yapay zeka tabanlı akıllı arama teknolojilerinde hangi verilerinin kullanıldığını ve verilerinin toplanarak hangi amaçlarla işlendiğini genellikle bilmez. Bu durum, kişisel verilerin korunması hakkı ve ilişkili diğer temel insan haklarının ihlalini ortaya çıkarabilir. Bu konuda, e-ticaret işletmelerin özellikle dikkat etmesi gereken husus şeffaf veri politikalarının oluşturulması ve hangi müşteri kişisel verilerin toplandığı ve kullanıldığına ilişkin müşterilerin aydınlatılmasıdır. Her ne kadar kişisel veriler müşterilerin açık rızaları olmadan işlenemezse de; sözleşmenin kurulması ve ifasının gerektirdiği hallerde kişisel veriler açık rıza olmadan da işlenebilecektir(GDPR, *giriş*, para.40, m.6/1-b m.7/4; KVKK m.5/2-c). Özel nitelikli kişisel verilerin⁵⁷⁰ (örneğin sağlık, cinsel yönelim, dini inanç verileri) işlenmesi ise kural olarak yasaktır. E-ticaret platformlarında arama motorlarının işleminde kullanılan veya arama motorları aracılığıyla elde edilen kişisel verilerin özel nitelikli kişisel veri türünde olması halinde, verisi işlenen müşterinin(İlgili kişinin) belirli, bilgilendirilmiş ve açık rızasının alınması gerekmektedir(GDPR, *giriş*, para.51; KVKK m.6). Kişisel verilerin anonimleştirilmesi korunması için bir seçenek olsa da; anonimleştirme çalışmalarının geri alınamayacak şekilde gerçekleştirilmesi gerekmektedir. Aksi halde, yani kişinin veriler kullanılarak belirlenebildiği hallerde e-ticaret işletmeleri kişisel verilerin işlenmesinden doğan ihlallerden sorumlu olur⁵⁷¹.

⁵⁶⁸ IBM, *What is Intelligent Search?*, <https://www.ibm.com/think/topics/intelligent-search> , (Erişim Tarihi: 02.06.2025) .

⁵⁶⁹ Google (t.y.) . *Arama ipuçlarını ve sonuçların Google'daki aramanızla ne şekilde ilgili olduğunu öğrenin.* Google Arama Yardım. <https://support.google.com/websearch/answer/10563935?hl=tr#zippy=%2Cm%C3%BCstehcen-sonu%C3%A7lar%C2Carama-terimleri-ve-ilgili-terimler> (Erişim Tarihi: 02.06.2025) .

⁵⁷⁰ bkz. yukarıda "2.7.1.Özel nitelikli kişisel veriler (Hassas kişisel veriler)" başlığı.

⁵⁷¹ Article 29 Working Party, Opinion 4/2007 on The Concept of Personal Data, s.18; GDPR m.4/5.

3.2.5. Dinamik fiyatlandırma ve stok yönetimi algoritmaları

Kapsamlarının nispeten dar olması sebebi ile dinamik fiyatlandırma ve stok yönetimi e-ticaret uygulamaları bir başlık altında toplanarak aşağıda kısaca işlenmiştir.

3.2.5.1. Genel olarak dinamik fiyatlandırma (algorithmic pricing)

Rekabet durumu, talep yoğunluğu, güncel gelişmeler ile özel günler ve müşteri sadakati gibi koşulları gözetilerek ile ürün fiyatlarının devamlı olarak güncellenmesi ve belirlenmesinde (böylece gereksiz indirim ve şişkin fiyatların önlenmesinde) dinamik fiyatlandırma olarak isimlendirilmektedir⁵⁷². Bu ifade, elektronik ortamda mal ve hizmet sağlayanların arz ve talepte meydana gelen en ufak değişimler doğrultusunda sunulan mal veya hizmetin fiyatını anında değiştirme becerisini ifade etmektedir. Öyle ki, dinamik fiyatlandırma sisteminin kullanıldığı platformlarda ürün veya hizmetin fiyatı gün içerisinde dalgalanabilmektedir. Çevrimiçi ürünün fiyatı talep ve arz durumları ile yukarıda belirtilen diğer koşullara bağlı olarak örneğin akşam, sabahki fiyattan daha düşük veya yüksek olabilmektedir⁵⁷³. Gelişmiş bir fiyatlandırma algoritmasına sahip bir firma, ürünlerini her gün, hatta günde birkaç kez yeniden fiyatlandırabilir.

Dinamik fiyatlandırma algoritmaları, fiyatlandırmaları tespit etmek için diğer çevrimiçi mağazaları(e-ticaret platformlarını) incelemektedir. Fiyatlandırma stratejilerini belirlemek ve neyin işe yaradığını öğrenmek için bu algoritmalar yazılımsal olarak bu şekilde kurgulanmalarına rağmen istemeden de olsa amaçlarını gerçekleştirmek için birbirleri ile konuşurlar. Bu durum, karı maksimize etmek sistemlerin bir e-ticaret platformundaki ürün artışından sonra diğerlerinde de artmasına sebebiyet verir. Bu da anlaşılmamış bir işbirliğine sebep olur⁵⁷⁴. Avrupa Birliği, bu işbirliğinin tüketicilerin e-ticarete daha fazla seçenek ve daha düşük fiyatlardan faydalanmasını engelleyerek onlara zarar vereceği ve dinamik fiyatlandırma algoritmaları ile otomatik olarak uygulanan fiyatlandırma yazılımının rekabet yasağını ihlal ettiği gerekçeleri ile bu yazılımların işbirliğini engelleyici şekilde yazılması gerektiğinin altını çizmiştir⁵⁷⁵.

3.2.5.2. Kişiselleştirilmiş dinamik fiyatlandırma

Ürün satımı için en doğru yöntem indirim yapmak gibi görünse de kimi zaman indirim yapılmasına gerek duyulmadan ürünün müşteri tarafından satın alınabileceği anlaşılabilmektedir. Bu durum kişiselleştirilmiş dinamik fiyatlandırmayı gündeme getirmektedir. Kişiselleştirilmiş dinamik fiyatlandırma, dinamik fiyatlandırmanın özel bir biçimi olarak karşımıza çıkmaktadır. Burada, müşterinin kişisel özelliklerine ve satın alım

⁵⁷² Sağtaş, 2023, s.58.

⁵⁷³ McLean, G (2019, February 25) . *Algorithms are maximising profits for online retailers by colluding to keep prices high*. The Conversation. <https://theconversation.com/algorithms-are-maximising-profits-for-online-retailers-by-colluding-to-keep-prices-high-112179> (Erişim tarihi: 02.06.2025)

⁵⁷⁴ McLean, 2019. Le, C., Mislove, A., & Wilson, C (2016) . An empirical analysis of algorithmic pricing on Amazon Marketplace. In *Proceedings of the 25th International Conference on World Wide Web*, s.1339-1349. <https://doi.org/10.1145/2872427.2883089>

⁵⁷⁵ bkz. European Commission (2017, February 2) . *Antitrust: Commission opens three investigations into suspected anticompetitive practices in e-commerce* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_17_201 (Erişim tarihi: 02.06.2025) .

davranışlarına göre fiyatlandırma yapılır ve satışın gerçekleşmesi hedeflenir⁵⁷⁶. Örneğin Amazon'un Echo ev içi sesli asistanı gibi asistanlar ile zaman içinde kullanıcıları hakkında bilgi edinip, çalışma biçimlerini bu bilgilere göre değiştirebilmektedir⁵⁷⁷. Nitekim, sadakatini kazandığı düzenli müşterilere Amazon diğer müşterilerine kıyasla daha yüksek fiyatlarla ürün sattığı gözlenmiştir⁵⁷⁸.

Kişiselleştirilmiş dinamik fiyatlandırmanın uygulanabilmesi özellikle müşteri davranış tahmini yapan YZ teknolojilerinin gelişmesi, bu ticari uygulamanın gizlenmesinin nispeten kolay olması ve tüketicilerin fiyatlandırma ve reklamcılık yöntemleri aracılığıyla rekabetçi alternatifleri ayırt etmelerinin zorluğu sayesinde mümkün olmuştur. Kişiselleştirilmiş dinamik fiyatlandırmada, kişiselleştirmenin yapılabilmesi için öneri sistemleri ve akıllı arama sisteminde olduğu gibi müşterinin dijital ayak izleri takip edilir ve satın alım davranışları analiz edilir. Dijital ayak izi, ticari işlemleri, hobileri, kişisel özellikleri, sosyal ağları, çalışma platformlarını kapsamaktadır⁵⁷⁹.

3.2.5.3. Stok yönetimi

E-ticarete stok yönetimi; müşteri talepleri karşısında stok optimizasyonunu sağlamak için kullanılmaktadır⁵⁸⁰. Gelişen kamera teknolojisi ile birleştirilen yapay zeka algoritmaları ile bugün görüntü tanıma teknolojisi ticari hayatta da kullanılmaya başlanmıştır. Nitekim, zincir marketler, mağaza ve depolarda raflar boşaldığında; ürünler eksildiğinde görüntüleri analiz eden YZ teknolojileri yetkili birimleri uyarabilmektedir⁵⁸¹. Stok yönetiminde, stok optimizasyonu yapılırken özellikle örneğin market alışveriş platformları bakımından mevcut müşterilerin konum verileri kullanılabilir.

3.2.5.4. Risk bakımından değerlendirme

Dinamik fiyatlandırmada, davranış tahmini için makina öğrenimi yapay zeka tekniğinden faydalanılmaktadır. Kişiselleştirilmiş dinamik fiyatlandırma bakımından kişisel verilere ilişkin riskler, riskin “kişiselleştirmeye” dayanması sebebi ile öneri sistemleri ile akıllı arama sistemlerindeki gibidir. Müşterinin dijital ayak izleri izlenir, konumu işlenir, satın alım davranışlarına göre fiyat belirlemesi kişiye özel olarak yapılır. Bu durum kişisel verilerin işlenmesi yönünden ayrı riskler barındırdığı gibi işinin davranışları ve kişisel özellikleri gözetilerek belirlenen fiyat eşit davranma ilkesi ile ayrımcılık yasağı ilkelerine aykırılık teşkil eder niteliktedir⁵⁸².

Otomatik kişiselleştirilmiş fiyatlandırma uygulaması doğası gereği, tüketicilerin özelliklerine göre (örneğin, alan kodu, sokak adresi, satın alma işlemi için kullanılan cihaz türü, satın alma geçmişi, cinsiyet ve yaş) dayalı olarak ayırım yapmaktadır. Bu durum eşit davranış ilkesi bakımından düşündürücüdür. Nitekim, fiyat ayrımcılığının ağırlıklı olarak tüketicinin kişisel özelliklerinden kaynaklandığı; eşitlik, tedarik maaliyeti veya tüketiciye sunulan artı

⁵⁷⁶ Duran, C (2021) . Yapay zekâ temelli pazarlama: Geleneksel pazarlamanın sonu mu? In N. Ö. İyigün & M. K. Yılmaz (Eds.), *Yapay zekâ: Güncel yaklaşımlar ve uygulamalar*. Beta Yayınları. s.42; Chapdelaine, P (2020) . Algorithmic personalized pricing. *New York University Journal of Law & Business*, 17 (1), s. 3.

⁵⁷⁷ McLean, 2019.

⁵⁷⁸ Chapdelaine, 2020, s.13.

⁵⁷⁹ Chapdelaine, 2020, s.10,18.

⁵⁸⁰ Gülşen, 2019, s.423,428.

⁵⁸¹ Duran, 2021, s.45.

⁵⁸² Chapdelaine, 2020, s.5-9.

değer(örneğin ürüne eklenen özellikler) gibi objektif kriterlere dayandırılmadığında fiyatların ancak keyfiliğinden bahsedilebilir. Bu da eşit davranış ve ayrımcılık yasağına vücut verir. Burada ayrımcılık yasağının yanı sıra adalet ilkesinin ihlalden de bahsedilebilir. Tüketicilere diğerlerine nazaran keyfi ve eşitlik ilkesine aykırı olarak yapılan fiyatlandırmanın kendisinin adil olmadığı söylenebilir de; kişisel verilerin kullanılmasındaki potansiyel kötüye kullanım ile ilgili adaletsizlikten de bahsedilmelidir. Adil olmayan bu yaklaşım kişisel verilerin ancak belirlenen amaçlarla işlenmesi kuralının ihlal edilmesi ile işletmecilerin tüketiciler aleyhine orantısız ve haksız kazanç sağlamasından da ileri gelmektedir. Nitekim, tamamen her bir kişinin ödeme gücüne bağlı olarak aynı ürün için iki kişiye farklı fiyatlar verilmesini haklı çıkarmak epey zordur⁵⁸³.

Yapay zeka temelli, özel olarak kişiselleştirilmemiş, rakip e-ticaret platformlarının analizi ile elde edilen dinamik fiyatlandırma sistemleri ve müşteri konum bilgisi kullanmayan stok yönetim uygulamaları bakımında kişisel verilerin korunması riskleri diğer uygulamalara göre nispeten hafiftir.

3.2.6. E-ticarette kullanılan yapay zeka uygulamaları ve kişisel veri işleme süreçlerine ilişkin genel değerlendirme

Yapay zeka araştırmalarına sağlanan destek fonları her geçen gün artmakta ve yapay zeka her geçen gün geliştirilmektedir. Finans, ticaret, sağlık, eğitim ve daha birçok konuda fayda sağlayan yapay zeka uygulamalarının faydası olduğu kadar, kasıtlı veya kasıtsız olarak (örneğin yanlış kullanım, hata veren sistemler vb.) doğuracağı riskler bulunmaktadır. YZ sistemleri daha zeki hale geldikçe insanların toplumsal rollerini de üstlenecek ve daha önce insanlar tarafından gerçekleştirilen ihlaller YZ tarafından gerçekleştirilebilecektir⁵⁸⁴. YZ'nın bu ihlalleri gerçekleştirmesi halinde geniş ölçekteki etkililiği sebebi ile YZ tarafından verilen zarar daha ağır olabilecektir. Bunun yanı sıra YZ sistemlerinden kendine has özelliklerinden kaynaklanan ihlaller de mümkündür⁵⁸⁵.

Yapay zeka uygulamaları, çalışmamız konusu olan kişisel verilerin korunması hakkını ihlal riski taşımaktadır. Bu risk, YZ uygulamalarının sahip olduğu beceriler(örneğin; konuşma, anlama, doğal dili algılama ve anlama, yüz tanıması, bilgisayar görmesi) ile insana ilişkin bilgiler gözetleme yolu ile elde edilmesi böylece hukuka aykırı şekilde veri toplaması faaliyeti şeklinde gerçekleşebileceği gibi kişisel verilerin korunmasına korunan menfaatlerden biri olan ayrımcı davranış yasağının ihlal edilmesi ile de olabilir.

Yukarıda açıklandığı üzere, e-ticaret platformlarında en çok kullanılan yapay zeka teknikleri genel olarak; doğal dil işleme(NLP), makina öğrenmesi, yapay sinir ağları, uzman sistemler ve derin öğrenmedir. Bu sistemlerin ne şekilde çalıştığı “1.5. Yapay Zeka Teknikleri” başlığı altında detaylı şekilde açıklanmıştır. Bütün yapay zeka uygulamaları için var olan temel aşamalar veri ile öğrenme, veri girdisi, gizli katmanlar vasıtası ile makinanın öğrendiklerinden hareketle veri üzerinde yorum yapması, karar vermesi ve karar davranışını gerçekleştirmesi şeklindedir. Sistemin öğrenen bir sistem olması halinde ise bu aşamalar geliştirici veya

⁵⁸³ Chapdelaine, 2020, s.30-39.

⁵⁸⁴ Russell ve Norvig, 2024, s.31.

⁵⁸⁵ Yapay zeka çalışma alanlarına göre farklı alanlarda risk doğurabilir. Örneğin, ölümcül otonom silahlar insan hayatını tehdit ederken; YZ kullanımının yaygınlaşması ile istihdam yönünde insanlar için riskler oluşabileceği yönünde endişeler bulunmaktadır. Yüksek risk içeren alanlarda (örneğin araba sürmek) YZ'nın hayatı tehdit edebileceği de ifade edilmektedir. Russell ve Norvig, 2024, s.31-32.

kullanıcının geri dönüşünün beklenmesi ve cevaba göre pekiştirme veya kendini düzeltme/uyarlama şeklindedir⁵⁸⁶.

Son yıllarda müşteri deneyiminin zenginleştirilmesi; müşteri davranış ve tercihlerinin tahmin edilerek daha iyi hizmet kalitesinin sunulması adına kişisel veriler etrafında bir ekonomi geliştirilmiştir⁵⁸⁷. Anlaşılan odur ki; e-ticaret platformlarında kullanılan uygulamalar kapsamında yapay zeka tekniklerinin; müşteriye tanınması, potansiyel müşteriye işletmeye çekebilmesi, müşteri ihtiyaç ve taleplerini anlayabilmesi ile sorunlarına çözüm bulabilmesi, müşteriye kişiselleştirilmiş önerilerde bulunabilmesi ancak müşteri alışveriş hareketlerini takip etmesi ve müşterilere ilişkin tüm verileri toplaması, analiz etmesi, yorumlaması, karar vermesi ve bu kararı davranışa dönüştürmesi ile mümkündür. Dolayısıyla, yapay zekanın e-ticaret platformları için yararlı çıktıları (dijital strateji planları, analizler ve doğru kararlar) ancak genel tabir ile müşterilerin geniş ölçekteki verilerinin toplanması ve analiz edilmesi ile mümkündür.

E-ticaret platformlarının tüketici davranışlarını tahmin etmek ve etkilemek için yararlandıkları üç ana kişisel veri kaynağı bulunmaktadır. Bunlardan birincisi, platformun belirli bağlamlarda edindiği veriler(örneğin online alışveriş verisi). Bunlar tüketici tarafından gönüllü olarak verilir. İkinci veri kaynağı, tüketici tarafından serbestçe sunulan ve kamuya açık hale getirilen veriler(açık profile sahip olan kişinin sosyal medya beğenileri) ve üçüncüsü ise belirsiz hizmet koşulları aracılığıyla izin verildiği iddia olunan veri analizi şirketlerine sunulan bilgilerdir⁵⁸⁸.

E-ticaret platformlarında kullanılan yapay zeka uygulamalarının çalışması için gerekli olan müşterilere ilişkin kişisel veriler; chatbotlar vasıtası ile elde edilen mesaj içerikleri ile yazılı, görüntülü görüşmeler veya fotoğraflar ile görsel, sanal asistanlar veya chatbotlarda yapılan sesli görüşmeler ile işitsel veya müşterilere kişiselleştirmiş hizmetlerin sunulabilmesi ve öneri sistemlerinin işletilebilmesi için internet adımlarının, cookieilerin, takip edilmesi ile elektronik formatta olabilir.

YZ, birden fazla kanaldan otomatik olarak ve anında veri toplama, analiz etme ve harekete geçme yeteneği ile tüketiciler için tatmin edici çözümler sunmakta ve müşteri deneyimini iyileştirmektedir⁵⁸⁹. Fakat müşterilerin kişisel verilerin korunması hakkı üzerindeki etkisi bu kadar olumlu olduğu söylenemez. Nitekim, veri işleme, toplama ve paylaşma süreçlerini içeren yapay zeka algoritmaları, özellikle bireylerin mahremiyeti ve verilerin gizliliği ihlallerine yol açabilir. E-ticaret platformlarını kullanan müşteriler çoğunlukla kullandıkları uygulamaların arkasında yapay zeka olduğunu bilmezler⁵⁹⁰. Dahası, çoğunlukla müşteriler kişisel verilerinin toplanmasından dahi haberi dahi olmamaktadır. Kullanılan yapay zekanın ve işletmelerin veri tabanlarında muhafaza edilen bu verilerin nasıl işlendiğinin, kiminle paylaşıldığının veya satıldığının, bunlardan hangi sonuçların çıkarılabileceğinin ve hangi kararların bu verilere dayandığının farkında değildirler⁵⁹¹. Nitekim, Gazi

⁵⁸⁶bkz. yukarıda ” 1.5. Yapay Zeka Teknikleri” başlığı.

⁵⁸⁷Chapdelaine, 2020, s.9.

⁵⁸⁸Chapdelaine, 2020, s.11.

⁵⁸⁹ Duran, 2021, s.46.

⁵⁹⁰ Özgür, 2023, s.21.

⁵⁹¹ Küzeci, 2011, s.142-149. “Isa: Intuit Smart Agent” isimli chatbot uygulamasında, uygulama geliştiricileri chatbot uygulamaları aracılığı ile edinilen bilgilerin alandaki araştırma ve uygulamaların geliştirilmesi için YZ sistemlerinde biriktirildiğini ifade edilmiştir. Bkz. Xue vd., 2018,s. 1423. Gupta da benzer şekilde, müşterilerin, örneğin bir yemek dağıtım uygulamasında, ödeme seçenekleri, adresleri, beğenileri, yemekleri inceleme süreleri

Üniversitesi'nde kullanıcıların sohbet robotlarında kullanılan yapay zeka uygulamalarına ve kişisel verilerine ilişkin farkındalığının ölçülmesi için yapılan bir çalışmada kullanıcıların %62,1'inin bu online servislerin kişisel verileri kaydedip işleyebileceğini bilmediğini belirtmiştir⁵⁹². İsimlerden beğenilere, düşüncelerden tercihlere, ses dokusundan görüntüsüne kadar müşterinin ticaret platformu dışında da gerçekte kim olduğunu yansıtan kişisel verilerin akıbeti bu noktada endişe vermektedir. Nitekim, kişisel verilerinin işlendiğini farkında olan tüketicilerin bu verilerin kullanımına ilişkin makul beklentileri ile verileri toplayan ve kullananların gerçekte bu verileri nasıl kullandığı arasında uçurumlar bulunmaktadır⁵⁹³. Bu durum verileri işlenen kişiler ile verileri kullananlar arasında çatışma yaratmaktadır⁵⁹⁴.

Yapay zeka tabanlı uygulamaların temel hak ve özgürlükler bakımından risk oluşturmamasının ana sebeplerinden biri müşterilerin kullandıkları uygulamaların arkasında yapay zeka olduğunu fark etmemeleri, yapay zeka algoritmalarının işleyişi ve kişisel verilerin korunması hakları hakkında bilgi sahibi olmamalarıdır. Nitekim, bu hususa ilişkin Avrupa Birliği AI Act("Yapay Zeka Yasası") YZ sistemleri ile etkileşime giren kişilerin bu konuda bilgilendirmeleri gerektiği dair bir yükümlülük getirilmiştir⁵⁹⁵. Aynı doğrultuda, Avrupa Konseyi, 108 numaralı Kişisel Verilerin Otomatik İşleme Danışma Komitesi (Consultative Committee of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) tarafından 2019 yılında hazırlanan "*Yapay Zeka ve Veri Korumasına İlişkin Kılavuzu*"⁵⁹⁶, m.11 ve 12'de; ilgili kişilerin(konumuz bağlamında müşterilerin) bir YZ uygulaması ile etkileşimden bulunmaları halinde bilgilendirilmeleri, kendilerine uygulanan YZ tabanlı veri işleme işlemlerinin altında yatan mantık hakkında bilgi edinme hakkına sahip olmaları gerektiği belirtilmektedir. Ayrıca bireylere(müşterilere) kişisel gelişimlerini etkileyen teknolojilere dayalı işlemeye ilgili olarak itiraz hakkı, kendilerine uygulanan YZ işlemlerinin sonuçlarını ve bu sonuçların kendileriyle nasıl ilişkili olduğunu anlamak için gerekli bilgileri elde etme hakkı sağlanmalıdır. Dolayısıyla verisi işlenen müşteriler e-ticaret site ve uygulamalarında gezinirken temel hak ve özgürlüklerine ilişkin olası risklerin bilincinde olarak ve yasal haklarını bilerek hareket edebilir hale gelecektir.

ile ilişkili diğer verilerinin; veri tabanlarında saklanacağını ve bu verilerin analiz edilerek kullanıcıya bir sonraki siparişi için önerilerde bulunulacağını ifade etmiştir. GUPTA vd. , 2020, s. 256.

⁵⁹² Başkaya ve Karacan, 2022, s. 489.

⁵⁹³Chapdelaine, 2020, s.11.

⁵⁹⁴ Lemley, 2000, s.1547; Schwartz, 2004, s. 2055, 2127.

⁵⁹⁵ European Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brüksel, C (2025), 04.02.2025, giriş, para.132 <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> . Erişim Tarihi: 22.05.2025. Aksi halde, yani yapay zeka sistemlerin uygulamalar arkasında gerçeği gizleyecek şekilde sunulması halinde (örneğin chatbotlarda), kullanıcılar yapay zeka sistemini insansı bir varlık olarak algılayarak kişisel verilerini paylaşmaktan çekinmemektedir. Güçlütürk, 2023, s.9-10. Amerika'da yapılan bir araştırmada, şirket çalışanlarının %10,8'i iş yerinde ChatGPT'yi kullandığını ve çalışanların %4,7'sinin şirketlerin gizli verilerini ChatGPT ile paylaştığını göstermiştir. ChatGPT ise materyalleri herkese açık bilgi tabanına dahil etmekte ve paylaşmaktadır. Bu sebeple, JP Morgan ve Verizon gibi şirketler, gizli verilere yönelik riskler nedeniyle şirket faaliyetlerinde ChatGPT kullanılmasını engellemiştir. Bkz. Coles, C (2023, February 28) . 11% of data employees paste into ChatGPT is confidential. *Cyberhaven News*. <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt> (Erişim Tarihi: 05.06.2025) .

⁵⁹⁶ Council of Europe (2019, January 25) . *Guidelines on artificial intelligence and data protection*. Directorate General of Human Rights and Rule of Law. <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8> (Erişim Tarihi: 02.06.2025) .

Yapay zeka öğrenmek, müşteri deneyimini iyileştirmek ve daha doğru ve iyi kararlar alabilmek için hep daha fazla kişisel veriye ihtiyaç duyacaktır. Örneğin YZ uygulamaları ile tüketici segmentasyonu faaliyetinin tam olarak gerçekleştirilmesi ve kişiselleştirme ile tam eşleşmeler sağlanabilmesi için müşterilerin demografik, psikografik, coğrafi, sosyoekonomik düzey gibi tüm bilgilerinin bilinmesi gerekmektedir. Şu an kullanılan YZ uygulamalarında ise yalnızca müşterinin alışveriş davranışları göze alınmaktadır⁵⁹⁷. İşletme-İktisat bilimi perspektifinden e-ticaretin geliştirilmesi için işletmelerin tüketicileri daha iyi tanınması gerektiği ve bu sebeple müşteriler hakkındaki tüm özellikleri keşfedecek yazılımların geliştirilmesi önerilmiştir⁵⁹⁸. Bu öneriye temel hak ve hürriyetler nazarından bakıldığında ise önerilen durumun başta kişisel verilerin korunması ve özel hayatın gizliliği olmak üzere temel insan haklarını ihlal edeceği, kişinin mahrem alanına müdahale teşkil edeceği, veri işleyen ile ilgili kişi arasındaki menfaat dengesini ilgili kişi aleyhine bozacağı, ilgili kişiyi maddi ve manevi zararlara uğrama tehlikesi altında bırakarak kişiliğini geliştirmesine engel teşkil edeceği açık şekilde ortadadır. Dolayısıyla bu öneri insan hakları nazarından kabul edilemez gözükmektedir. Belirtmek isteriz ki; bugün yaşadığımız teknoloji çağının günlük sorunları disiplinler arası bir bakış açısını zorunlu kılmaktadır. Devletler ve şirketler karşısında güçsüz konumda olan bireyin temel insan hakları ve menfaatlerinin karşılaşılan her somut olayda gözetilmesi hukukun görevi olmalıdır.

Son olarak yapay zeka uygulamaları için en büyük risklerin kötü yapılandırılmış algoritmalar aracılığı ile ortaya çıkabileceği belirtilmelidir. Kullanıcılar bu algoritmaları kullandığında genellikle yanlış ve hatta tehlikeli sonuçlar ortaya çıkar. İnsan toplumları yapısal önyargılara ve eşitsizliklere sahip olduğundan, makine öğrenimi araçları da kaçınılmaz olarak bunları öğrenmektedir. Yapay zeka sisteminin çalışabilme şartı olan verilerin önyargılı olması halinde yani dengeli veya kapsayıcı olmaması halinde yapay zeka davranışının da önyargılı olması sonucu doğacaktır. Sorunun tek kesin çözümü önyargı ve eşitsizliği toplumdan kaldırmak olsa da, yapay zeka bu misyon için yalnızca sınırlı bir destek sunabilir. Bununla birlikte, YZ'nin eşitsizlikleri pekiştirmek yerine bunlara karşı koymasını sağlamak önemlidir. Diğer bir ihtimalde yapay zeka algoritmasının önyargılı şekilde oluşturulması veya ayrımcı müdahale yapmaya imkan tanınması halinde de yapay zeka çıktısı bazı grupları bir diğerine tercih edecek ve adil bir düzene hizmet etmeyecektir. Bu durumlar uygulama bakımından risk teşkil etmektedir. Diğer yandan, söylemek gerekir ki, yapay zeka programlarında önyargının tespit edilmesi ve azaltılması için başka YZ algoritmaları üzerine çalışılmaktadır⁵⁹⁹.

Kişisel veriler e-ticaret platformlarınca yalnızca hizmet ilişkisinden doğan edimlerin yerine getirilmesinde amacıyla değil sonrasında diğer başka sebeplerle de işlenebilmektedir. Nitekim, ticari amaçlı olarak toplanan veriler daha sonra birçok farklı sebeple örneğin, siyasi

⁵⁹⁷ Sağtaş, 2023, s.54; Tutsal ve Ventura, 2022, s. 364.

⁵⁹⁸ Tutsal ve Ventura, 2022, s. 364.

⁵⁹⁹ High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) . *A Definition of AI: Main Capabilities and Scientific Disciplines*. European Commission, Brussels. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (Erişim Tarihi: 20.05.2025); Russell ve Norvig, 2024, s.31-32; Greengard, 2019, European Parliament (2020, January) . *Artificial intelligence: How does it work, why does it matter, and what can we do about it?* Panel for the Future of Science and Technology, s. 60. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU\(2020\)641547_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf) (Erişim tarihi: 20.05.2025)

eğilim analizi ve manipölasyon için kullanılabilir⁶⁰⁰. Bir başka örnek ise; mevcut kişisel verilerin toplanması ve analiz edilmesi ile yaratılan olası kullanıcı profillerinin reklamcılık sektöründe kullanılarak doğrudan pazarlama stratejileri belirlenmesinde faydalı olmasıdır. Yapay zeka ile büyük veri teknolojileri ile ekonomik değerinin büyümesi karşısında e-ticaret platformları bu teknolojileri daha da geliştirmek için verileri toplayan yazılımlara yatırım yapmaktadır⁶⁰¹.

Yapay zeka tabanlı uygulamaların işleyişi ve teknik yapısı ile riskleri bakımından yapılan değerlendirmemiz kapsamında yapay zeka ile ilgili etik durumlar(kişisel verilerin korunması bağlamı üçüncü kısımda işlenecektir) aşağıdaki gibi sıralanabilir⁶⁰²:

1) Şeffaflık: Kullanıcılar, bir insanla değil, yapay zeka sistemi ile etkileşim kurduklarının farkında olmalıdır. Yapay zeka programları kendilerini açık şekilde ifşa etmeli; işlevleri, kabiliyetlerinin sınırları hakkında kullanıcıyı bilgilendirmelidir. Kişisel verilerin nasıl toplandığı ve kullanıldığına dair bilgilerin açıklanmasını zorunlu kılınması temel hak ve özgürlükler bakımından bu riskli uygulamaların kesin olarak yasaklanmasından daha olumlu bir şekilde tüketicilere fayda sağlayabilir⁶⁰³.

2) Önyargı: Yapay zeka temelli uygulamalar eğitildikleri verilerin yanlı veya ayırıcı olması ile geliştiricilerin önyargılı algoritmalar geliştirmesi ile eşit davranma ilkesine aykırı şekilde hareket edebilir ve belli kullanıcı gruplara karşı ayrımcı davranabilirler. Böylece, bazı bireylerin veya grupların sistem sonucundan dezavantajlı duruma düşmesi tehlikesi ile karşılaşılır. “Privacy by design” ilkesi(GDPR m.78) işletilerek söz konusu uygulamanın tasarımdan itibaren varsayılan ayarla kişisel verilerin korunması hakkının etkin şekilde sağlanması ve düzenleyici kişisel veri koruma mevzuatına uyum göstermesi gerekmektedir.

3) Gizlilik: Yukarıda başlıklar altında detaylıca açıklandığı üzere yapay zeka tabanlı e-ticaret uygulamaları müşterilerin ve potansiyel müşterilerin çok sayıda kişisel verisini toplamakta, analiz etmekte ve diğer şekillerde kullanmaktadır. Bu veriler yalnızca müşterilerin rızası ile işlenmelidir. Ayrıca kişisel verilerin işlenmesinden sorumlu e-ticaret işletmelerince gerekli idari ve teknik tedbirler alınarak müşteri verilerine yetkisiz erişim veya verilerin ifşası engellenmelidir.

4) Hesap Verebilirlik: Yapay zeka teknolojisini kullanarak kişisel verileri işleyen veri sorumluları eylemlerinden ve kararlarından sorumlu olmalıdır. Ayrıca, kullanıcının müracaat hakkı kapsamında kişisel verilerine ilişkin bilgilendirme yapılmalıdır. Yapay zeka sistemlerinin anlaşılır ve net şekilde mekanizması/nasıl işlediğine ve kişisel verilerin yerine ilişkin müşterilere açıklama yapılmalıdır.

5) Gözetim: Yapay zeka uygulamaları tamamen insan etkileşiminin yerini almamalıdır. Düzenli aralıklarla insan gözetimi sağlanarak yapay zeka sisteminin kişisel veriler aleyhine işlemediğinden emin olunmalıdır.

⁶⁰⁰ Hingh, 2018, s. 1270-1271. Facebook kullanıcılarının kişisel verileri ABD’deki başkanlık seçimleri sürecinde Donald Trump’ın seçimi kazanabilmesi için, siyasi amaçlı, kullanılmış ve kullanıcılar seçim sürecinde kişilik özellikleri bilgileri vasıtasıyla manipüle edilmiştir. Grasseger, H., and Krogerus, M (2017, January 28) . The data that turned the world upside down. *VICE*. <https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win> (Erişim tarihi: 05.06.2025)

⁶⁰¹ Başalp, 2015, s.78.

⁶⁰² Özgür, 2023, s. 24-25.

⁶⁰³ Chapdelaine, 2020, s.40.

Kişisel verilerin korunması konusu son yıllarda önem verilen konulardan biri olarak gözüke de Avrupa Birliği düzenleyici metinlerinde dahi esas sağlanmak istenenin kişisel verilerin serbest dolaşımı sağlanarak yapay zeka uygulamalarının geliştirilmesi ve böylece ekonomik kazançlar elde edilmesi olduğunu görmekteyiz. Bu durum yapay zeka algoritmalarının hukuka aykırı şekilde veri işlemlerini ve böylece verisi işlenen kişilerin zor durumda kalmasına yol açabilmektedir. İşlenen veriler; veri sahibi konumundaki kişi veya kurumları, kişisel verilerin ifşa edilmesi, yetkisiz üçüncü kişilere aktarılması, fidye amacıyla kullanılması ve daha birçok şekilde zor duruma düşürebilmektedir⁶⁰⁴.

E-ticaret platformlarının gelir eğrisini yükselten yapay zeka programlarının çalışması için gereken kişisel verilerin serbest dolaşımı; kişisel veri işleyenlere duyulan güven ile doğru orantılıdır. Kişisel verilerinin kendilerine zarar verebilecek şekilde işlenebileceği ve hukuka aykırı şekilde kullanılabilmesi endişesinde olan kişiler yapay zeka uygulamalarını kullanmaya çekineceklerdir. Buna en güzel örnek *Whatsapp* gizlilik sözleşmesinin yenilendiği esnada milyarlarca kullanıcının alternatif örneğin *Signal* gibi kanallara yönelmesidir⁶⁰⁵. Yapay zeka uygulamalarının gelişimine destek verilmesi, serbest veri akışının sağlanması aynı zamanda temel insan hak ve hürriyetlerinin korunması için yapay zeka uygulamaları tarafından işlenen kişisel verilerin hukuki güvenceler çerçevesinde korunması gerekmektedir.

E-ticarete kullanılan yapay zeka tabanlı uygulamalar kapsamında temel hak ve özgürlüklere yönelik risklerin ortadan kaldırılabilmesi için öncelikle yapılması gereken bu uygulamaların kişilik haklarına aykırı bir durum teşkil etmeden tasarlanmasıdır(data protection by design). Bu şekilde, uygulamadaki varsayılan ayarlar gizliliği koruyacak şekilde yapılandırılarak(data protection by default)⁶⁰⁶; uygulamanın tasarlanması sırasında temel hak ve özgürlükler dikkate alınacak ve kişisel verilerin toplanması aşamasından önce sistemin işleyici kişisel verilerin korunması mevzuatına uygun hale getirilecektir. Böylece kişiler sistemden kaynaklanabilecek ihlallere karşı başlangıçtan itibaren korunması sağlanacaktır(GDPR m.25). Ayrıca, kişisel verilerin işlenmesinde “*amaca bağlılık ilkesi*” uyarınca müşterilere, verilerinin hangi amaçla alındığı kaydedildiği ve işlendiği açık ve doğru bir şekilde açıklanmalı ve amaçla bağdaşmayan türden veriler toplanılmamalıdır. E-ticaret işletmelerinin veri koruma politikasına uygun şekilde hazırladığı aydınlatma metinleri ile ilgili kişiler(müşteriler ve potansiyel müşteriler), e-ticaret platformlarıncı yapay zeka temelli uygulamalar ile hangi verilerinin hangi amaçla ve ne kadar süre işleneceğine dair bilgilendirilmelidir. Kişisel verilerin toplanmasında açık rıza ilkesi gereği verisi işlenecek kişilerden konuyla sınırlı ve açık olmak üzere rızaları alınmalı⁶⁰⁷; özel nitelikli kişisel verilerin işlenmesi konusunda hukukun öngördüğü hassasiyet gözetilmelidir.

E-ticaret platformlarındaki YZ tabanlı uygulamaların açıklanan risklerin ortadan kaldırılması için işletmelerce alınması gereken önlemler, kişisel verilerin korunması hukuku

⁶⁰⁴ Başkaya ve Karacan, 2022, s. 489.

⁶⁰⁵BBC, Whatsapp'ın Yeni Kullanıcı Sözleşmesi Gizlilik Açısından Ne Anlama Geliyor?, <https://www.bbc.com/turkce/haberler-dunya-55610827> (Erişim Tarihi: 05.06.2025) .

⁶⁰⁶ Bugün yaygın olarak kullanılan yapay zeka uygulamaları ChatGBT, bu ilkeye aykırı olarak, kullanıcıların verilerin gelecekte kullanılmaması için açıkça bir seçim yapmadığı hallerde, varsayılan ayarlı olarak kullanıcıların girdiği her türlü veri sisteme dahil edildiği görülmektedir. İtalyan Veri Koruma otoritesi ChatGBT yapay zeka uygulamasının kişisel verileri hukuka uygun olarak işlememesi sebebi ile erişimine 2023 yılında kullanıldığını engellemiştir. bkz. Burges, M., ChatGPT Has a Big Privacy Problem, Wired, <https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/> (Erişim Tarihi: 05.06.2025) .

⁶⁰⁷ bkz. aşağıda ”3.3.2.1.İlgili Kişinin Açık Rızası” başlığı.

kapsamında uyması gereken kurallar ve dikkat etmesi gereken ilkeler ile genel olarak YZ uygulamalarını kullanan e-ticaret işletmelerinin kişisel veriler hakkındaki düzenleyici metinlere(özellikle GDPR ve KVKK) nasıl uyum sağlayacakları aşağıda (üçüncü kısımda) detaylı olarak açıklanmıştır.

3.3. E-Ticaret Sektöründe Kullanılan Yapay Zeka Uygulamaları ve Kişisel Verilerin Korunması Hukukuna Uyum

Yapay zeka teknolojinin gelişmesi ve büyük veri setlerinin oluşması ile kişilerin özel hayatlarına ilişkin bilgilerin makinalar tarafından açığa çıkarılması ile kişilerin bu durumdan zarar görmesi riski ortaya çıkmıştır⁶⁰⁸. Bu durumun bertaraf edilmesi için çalışmamız kapsamında e-ticaret platformları bünyelerinde kullanılan YZ tabanlı uygulamaların kişisel verilerin korunması hukukuna uyum sağlamaları gerekmektedir. Bu doğrultuda şirketler kişisel verilerin korunması ilkelerini benimsemeli, kişisel verilerin işlenmesi şartlarını gerçekleştirmeli, veri sorumlularına yüklenen yükümlülükleri yerine getirmeli ve yasaklanan YZ tekniklerinden kaçınılmalıdır. Yasal yükümlülüklerin gerçekleştirilmesinin yanı sıra YZ tabanlı uygulamaları kullanan şirketlerin kişisel verilerin korunması bilincinin oluşması ve bu alanı gözeten; özenli ve dikkatli politikalar geliştirmeleri ile işlemlerini bu bilinçle gerçekleştirmeleri temel hak ve özgürlüklerin korunmasına yönelik büyük bir katkı sağlayacaktır. Bu çalışmamızla amacımız bu bilincin oluşmasında pay sahibi olmaktadır.

3.3.1. Yapay zeka uygulamalarında uyulması gereken kişisel verilerin korunması ilkeleri

Yapay zeka teknolojisine dayanan uygulamalarda, kişisel veri işleme faaliyetinde bulunurken hangi hususların göz önünde bulundurulması gerektiği belirlenmelidir. Nitekim, YZ teknolojisini kullanan e-ticaret işlemleri ile YZ teknolojisini geliştiren ve üretenlerin uyması gereken temel ilkelerin belirlenmesi bu teknolojinin geliştirilmesinden kullanılmasına kadar her aşamada kişisel verilerin korunmasının sağlanması bakımından önemlidir. Konu ile ilgili Avrupa Konseyi, 108 numaralı Kişisel Verilerin Otomatik İşleme Danışma Komitesi (Consultative Committee of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) tarafından 2019 yılında hazırlanan “*Yapay Zeka ve Veri Korumasına İlişkin Kılavuz*⁶⁰⁹’ında”, aşağıda belirtilen hususlara yer verilmiştir:

- YZ geliştiricileri, üreticileri ve hizmet sağlayıcıları veri koruma ilkelerini esas almalıdır. Kişisel verilerin işlenmesine dayanan yapay zekanın geliştirilmesinde kişisel verilerin korunması ilkeleri uygulanmalıdır. Kişisel verilerin korunması ilkeleri temel olarak: adalet, amaçla sınırlılık, orantılılık, tasarımdan itibaren ve varsayılan ayarla gizlilik, hesap verilebilirlik, şeffaflık, veri güvenliği ve risk yönetimidir.
- Yapay zekanın inovasyonun gerçekleştirilmesinde kişisel verilerin işlenmesinin potansiyel risklerinden kaçınılmalıdır. Veri toplama faaliyeti de dahil olmak üzere kişisel verilerin tüm aşamalarında insan hakları yaklaşımı benimsenmelidir. İlgili

⁶⁰⁸ Retornaz, E. A., ve Güçlütürk, O. G (2021) . Yapay zekanın kişisel veri kavramı ve kişisel verilerin işlenmesinde temel ilkelerle ilişkisi. İçinde E. A. Retornaz & O. G. Güçlütürk (Ed.), *Gelişen teknolojiler ve hukuk II: Yapay zeka* (ss. 275-302) . On İki Levha Yayınları, s.275.

⁶⁰⁹Council of Europe (2019, 25 January) . *Guidelines on artificial intelligence and data protection*. Directorate General of Human Rights and Rule of Law. <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8> (Erişim tarihi: 02.06.2025)

kişinin haklarına saygı gösterilmeli; İlgili kişilere, açık, doğru ve anlaşılır bir şekilde işlenen kişisel verileri hakkında bilgilendirmeler yapılmalıdır. Verisi işlenen kişilerin kişisel verileri üzerindeki denetimi etkin bir şekilde sağlanmalıdır. Veri sahipleri, bir YZ uygulaması ile etkileşime girdiklerinde bilgilendirilmeli ve kendilerine uygulanan YZ veri işleme operasyonlarının altında yatan mantık hakkında bilgi edinme hakkına sahip olmalıdır. Bireylerin kişisel gelişimlerini etkileyen veri işlemlerine itiraz hakkı sağlanmalıdır.

- Yapay zeka teknolojisinin temel insan hakları üzerindeki olası olumsuz etkileri(riskler) gözetilerek geliştirilen YZ teknolojisi üzerinde geliştiriciler ve uygulayıcılar tarafından risk analizi yapılmalıdır. Bu analizler yapay zeka teknolojisinin kendine has özellikleri göz önüne alınarak özenli bir şekilde yapılmalıdır.
- Veri minimizasyonu ilkesi gözetilmeli, gereksiz ve aşırı veri işleme faaliyetinden kaçınılmalıdır. Amaç dışı veri işleme faaliyetinde bulunulmamalıdır. YZ teknolojinin geliştirilmesinde, üretilmesinde ve hizmet verilmesindeki paydaşlar hesap verebilir olmakla yükümlü tutulmalıdır.

Kişisel verilerin korunması hukuku bazı temel prensipler üzerine kuruludur. Kişisel verilerin işlenmesi genel ilkeleri bunlardan biridir. Kişisel verilerin işlenmesi, kanuna uygun şekilde gerçekleşmiş olsa dahi, kişisel verilerin işlenmesi genel ilkelerine uyulmadan yapılması halinde hukuka aykırılık teşkil eder⁶¹⁰. E-ticaret işletmelerinin YZ tabanlı uygulamalar kapsamında kişisel verilerin kullanılması kapsamında uyması gereken bu genel ilkeler GDPR m.5 ve KVKK m.4'de sayılmıştır. Kişisel veriler, ancak öngörülen bu usul ve esaslara uygun olarak işlenebilir. Çalışmamıza konu düzenleyici metinlerde kişisel verilerin işlenmesine ilişkin ilkeler kısaca: Hukuka Uygunluk, Adalet ve Şeffaflık, Belirli, Açık ve Meşru Amaç (Amaçla Sınırlılık), Veri Minimizasyonu, Verilerin Güncel ve Doğru Olması ve Saklama Süreleri ile Sınırlılık olarak sayılabilir. Bu ilkeler ve kapsamaları aşağıda açıklanmıştır.

3.3.1.1. Hukuka uygunluk, adalet ve şeffaflık ilkeleri

Kişisel verilerin işlenmesine ilişkin ilkeler kapsamında GDPR düzenlemesinde sayılan ilk ilke hukuka uygunluk, adalet ve şeffaflık prensibidir. KVKK m.4/2'de bu ilke, “*hukuka ve dürüstlük kurallarına uygun olma*” şeklinde ifade edilmiştir. Hukuka uygunluğun sağlanması, kişisel verilerin işleme faaliyetlerinin KVKK ve GDPR düzenlemeleri ile ilgili diğer yasal düzenlemelerde belirtilen işleme şartlarına uyum sağlaması ile alakalıdır. Buna göre, kişisel verilerin işlenmesi GDPR m. 6 ve KVKK m.5 ile m.6 düzenlemelerinde yer alan kişisel verilerin işleme şartlarından biri kapsamında gerçekleşmesi halinde hukuka uygundur⁶¹¹. Hukuka uygunluk prensibi ayrıca işlemenin açık ve şeffaf olması ile diğer kişisel veri işleme ilkelerine uyumlu olmasını da kapsamaktadır⁶¹².

⁶¹⁰ Develioğlu, 2017, s. 44.

⁶¹¹ Develioğlu, 2017, s. 44.

⁶¹² Selek, 2021, s.79.

Türk hukukunda belirtilen “*Dürüstlük Prensibi*” ile ifade edilmek istenen; veri işlemede ulaşılmak istenen hedefe ilerlenirken; ilgili kişi menfaatlerinin ve makul beklentilerinin dikkate alınmasıdır. Bu ilke veri işleminin şeffaf olması ile ilgili kişinin bilgilendirilmesi yükümlülüklerini de kapsamaktadır. Hukuki bir sebebe dayanmadan yapılarak işleme ile kişisel verilerin gizli olarak(örneğin açıklanmayan/gizli kayıt ile) işlenmesi dürüstlük ilkelerine aykırılık oluşturmaktadır⁶¹³. Dürüstlük ilkesi karşısında e-ticarete kullanılan YZ tabanlı uygulama kullanıcılarının kişisel verilerinin uygulamanın arkasındaki YZ sistemi tarafından işlendiğini bilmemesi düşündürücüdür.

Kişisel verilerin işlenmesinde “*Şeffaflık Prensibinin*” anlaşılması bakımından GDPR yol göstericidir. Nitekim, GDPR gerekçesine göre Şeffaflık ilkesi:

*“kamuya veya veri öznesine iletilen her türlü bilginin kısa, kolay erişilebilir ve anlaşılabilir olmasını ifade etmektedir. Ayrıca kullanılan dil açık ve basit olmalı ve uygun olduğu hallerde, anlaşılabilirliğin sağlanması için görseller kullanılmalıdır. Bu durum özellikle uygulamanın teknolojik karmaşıklığı nedeniyle veri öznesinin kendisi ile ilgili kişisel verilerin toplanıp toplanmadığını, kim tarafından ve hangi amaçla toplandığını bilmesi ve anlamasının zor olduğu hallerde geçerlidir”*⁶¹⁴ (GDPR, giriş, para.58).

Belirtilmelidir ki, yapay zeka uygulamaları teknolojik altyapısı ve çalışması bakımından karmaşık sistemlerdir. Konuda uzmanlığı olmayan kimseler tarafından anlaşılması güçtür. Bu sebeple ilgili kişilere sistemin açıklanmasında ve kişisel verilerin işlenmesinin anlatılmasında görsellerden, tablolardan ve şablonlardan faydalanılması gerektiği düşüncesindeyiz.

Belirtilmelidir ki, uzmanlar dahi yapay zeka sistemleri hakkında her zaman her şeyi bilemeyebilirler. Yapay zekanın verileri yorumlaması sonrasında aldığı karar süreci her zaman net değildir. Özellikle teknik yapı itibari ile sürecin karar aşamasına kadar izlenemediği yapay sinir ağlarını kullanan makina öğrenimi teknikleri gibi “kara kutu” denilen sistemler için geçerlidir. Bu tür sistemler opaktır. Kararın neden ve ne şekilde alındığının tam olarak açıklanamadığı bu sistemler şeffaflık ilkesi ile uyumlu değildir⁶¹⁵.

Kişisel verilerin işlenmesi amaçları ile süreçleri hakkında ilgili kişinin bilgi alma hakkı “Adalet ve Şeffaflık” ilkelerinin gereğini oluşturmaktadır. Adil ve şeffaf bir veri işleminin temin edilebilmesi için ilgili kişiye veri işlenmeye ilişkin kişisel verilerin işlendiği özel koşullar da dikkate alınarak, anlaşılabilirliğin sağlanabilmesi için ilgili kişiye ilave ek bilgiler verilmelidir(GDPR, giriş, para.60). YZ uygulamalarında kişisel veri işleme faaliyetlerinin olumsuz etkilerinden kurtulmak ve etkin denetimlerin sağlanması bakımından bu ilke hukuki dayanak oluşturmaktadır⁶¹⁶. Nitekim, YZ sistemleri ve işlenen kişisel veriler hakkında tüketicinin bilgisizliği, kişisel verilerinin çevrimiçi kullanımındaki sahip olduğu denetim eksikliğinin bir yansıması olduğu ifade edilmektedir⁶¹⁷.

Çalışmamıza konumuz olan GDPR ve KVKK düzenlemelerinde yapay zekaya ilişkin bir hüküm bulunmamaktadır. Fakat otomatik karar alma sistemlerinde adalet ve şeffaflık ilkelerinin bir gereği olarak kişilerin itiraz etme ve bilgilendirme haklarının gerçekleştirilmesi

⁶¹³ Küzeci, 2010, s. 197; Şimşek, 2008, s.85.

⁶¹⁴ Ayrıca işlemin çocuklara yönelik olduğu durumlarda, her türlü bilgi ve bilgilendirme, çocukların kolaylıkla anlayabileceği kadar açık ve sade bir dilde olmalıdır (GDPR, giriş, para.58) .

⁶¹⁵ Özgür, 2023, s. 22

⁶¹⁶ Atalan, 2024, s.54.

⁶¹⁷Chapdelaine, 2020, s.11

için sistem hakkında spesifik olarak bilgilendirilmeleri gerektiği belirtilmiştir (GDPR, *giriş*, para.71). Bunun sağlanabilmesi için yapay zeka sistemlerinin e-ticaret platformları içindeki yerinin ve işlevinin anlaşılabilir ve erişilebilir olması gerekmektedir⁶¹⁸.

Uygulamaya bakıldığında; e-ticaret platformlarındaki kullanıcıların YZ sistemlerine ve kişisel verilere ilişkin farkındalığının olmadığı görülmektedir. Bunun nedeninin şirketlerin şeffaf olmamaları olması gösterilmektedir. Şirketler bilinçli şekilde belirsiz, yanıltıcı ve kafa karıştırıcı bir dil kullanmakta ve kişisel verilerin işlenmesi hakkında tüketicileri eksik, yanlış veya hiç bilgilendirmemektedir⁶¹⁹. Yapay zeka sistemlerinin anlaşılması için yapılan yasal düzenlemelerden olan AI Act(Yapay Zeka Yasası) ve Çerçeve Sözleşmesi bu kapsamda önemlidir.

3.3.1.2. Amaçla sınırlılık ilkesi

Kişisel veriler, veri sorumlusu tarafından belirtilen, açık ve meşru amaçlarla toplanır ve bu amaçlara uygun olmayacak şekilde sonradan işlenemez(GDPR m.5/1-b). Bu kural kişisel verilerin “*Amaçla Sınırlı*” olması prensibini ifade etmektedir. Bu prensip, KVKK m.4/1-c’de aynı şekilde “*belirli, açık ve meşru amaçlar için işlenme*” olarak ifade edilmiştir.

Belirli, açık ve meşru amaçlar için işlenme ilkesi, e-ticaret şirketlerinin, veri işleme amacını açık ve kesin olarak belirlemesini zorunlu kılmaktadır⁶²⁰. Bildirilen belirli amaç kapsamında toplanan kişisel veriler, toplanma amacı dışında başka bir amaç ile işlenemez⁶²¹. Bu ilke uyarınca, veri sorumlusu, ilgili kişiye toplanan veya aktarılan kişisel verilerinin hangi amaçlarla işleneceğini; planlanan tüm işleme planını içerecek şekilde bildirmekle yükümlüdür. Amacın belirsiz şekilde açıklandığı, tam olarak anlaşılamadığı, olası amaçların bulunduğu haller bu ilkeye aykırılık teşkil eder⁶²².

Amacın açık olması, amacın veri öznesi tarafından anlaşılabilecek şekilde ifade edilmesi anlamına gelmektedir⁶²³. Amacın meşru olması ise e-ticaret platformu tarafından işlenen kişisel verilerin, işletme konusu iş veya hizmetle bağlantılı ve gerekli olması anlamına gelmektedir. Örneğin, bir hazır giyim mağazasının, müşterilerinin iletişim ve adres bilgilerini işlemesi meşru amaç kapsamındayken, adli sicil kayıtlarını işlemesi meşru amaç kapsamında değerlendirilemeyecektir⁶²⁴. Kişisel verilerin, GDPR m. 6 ve KVKK m.5 ile m.6 düzenlemelerinde belirtilen kişisel verilerin işlenmesi halleri kapsamında işlenmesi; kişisel verilerin işlenme amacının meşru olması anlamına gelmektedir⁶²⁵. Kişisel verilerin toplanma amacı henüz verilerin toplanması aşamasında ilgili kişilere bildirilmelidir(GDPR m.13 ve m.14). Dolayısıyla, bir e-ticaret platformu müşterileri hakkında topladığı kişisel verilere ilişkin bilgilendirmeyi henüz kişisel verileri toplamadan kullanıcıya gerçekleştirmelidir.

“*Amaçla Sınırlılık*” prensibinin yansıması olarak kişisel veriler yalnızca toplanmaları aşamasında değil; daha sonra gerçekleştirilen işlemelerinde de toplanma amacı dışında

⁶¹⁸ Atalan, 2024, s.55.

⁶¹⁹ Karaman, s.1346.

⁶²⁰ bkz. KVKK m.4 gerekçesi.

⁶²¹ Akgül, 2014, s. 129.

⁶²² Atalan, 2024, s.55.

⁶²³ Retornaz ve Güçlütürk, 2021, s. 291.

⁶²⁴ bkz. KVKK m.4 gerekçesi.

⁶²⁵ Ayözger Öngün, 2019, s.140.

işlenememektedir⁶²⁶. Kişisel verilerin yeniden kullanımına ilişkin GDPR m.6/4'te özel bir düzenleme öngörmüştür. Buna göre; kişisel verilerin toplandıkları (veya işlemeden önce bildirilen) amaç kapsamı dışında yeniden kullanımı ancak kanuni düzenlemede açık şekilde belirtilmesi ile veya ilgili kişinin rızası hallerinde mümkün olmaktadır. Rıza'nın olmadığı hallerde, yeni amaca yönelik işlemenin kişisel verilerin asıl toplanma amacına uygun olup olmadığını değerlendirilir. Bu değerlendirmede⁶²⁷: kişisel verilerin toplanma amacı ile yeni amaç arasındaki olası bağlantılar, veri öznelere ve veri sorumlusu arasındaki ilişki noktasında kişisel verilerin toplandığı bağlam; kişisel verilerin toplandığı bağlam ve ilgili kişilerin daha fazla kullanımına ilişkin makul beklentileri, kişisel verilerin niteliği ve daha fazla işlemenin ilgili kişi üzerindeki etkisi; adil işlemeyi sağlamak için veri sahipleri üzerinde herhangi bir uygunsuz etkiyi önlemek için koruma önlemleri ile verilerin şifrelenmesi veya psödonimleştirilmesini içerebilecek uygun güvencelerin mevcut olması kriter olarak yer alır. Sıralanan kriterler sonucunda yeniden kullanımın uygunluğu(*compatibility*) belirlenir. Bu kavram, kişisel verilerin ilk toplandığı amaçla uyumlu olmasını ifade etmektedir⁶²⁸.

Amaçla Sınırlılık prensibinin istisnası, kişisel verilerin sonradan işlenmesinin bilimsel veya tarihi araştırma amaçları veya istatistiki amaçlarla gerçekleştirilmesidir(GDPR, m.5/1-b).

Açıklananlar ışığında amaçla bağlılık ilkesi için 4 ihtimal ile karşılaşıldığı anlaşılmaktadır:

- Birinci ihtimalde kişisel veriler toplanma amaçları çerçevesinde toplanır ve bu amaç doğrultusunda ve ilgili kişiye açıklanan faaliyet kapsamında işlenir. Bu durum hukuka uygundur.
- İkinci ihtimalde, toplanma amacı çerçevesinde kişisel veriler toplanır fakat ilgili kişiye bilgi verilmeden benzer veya aynı durumlar için tekrar işlenir. Örneğin, bir müşterinin, her hafta evine organik sebze kutusu teslim etmesi için bir çevrimiçi e-ticaret şirketi ile anlaştığı yaptığı örnekte; müşterinin adresi ve banka bilgilerinin ilk toplanmasından sonra, bu veriler ödeme ve teslimat için perakendeci tarafından her hafta tekrarlanması halidir. Bu durum da hukuka uygundur çünkü, yeniden işleme toplanma amacı ile uyumludur. Bu nedenle, yeniden yapılacak işleme, başlangıçta tüm ayrıntılar tam olarak ifade edilmemiş olsa bile, veri sahiplerinin makul beklentilerini açıkça karşılamaktadır⁶²⁹.
- Üçüncü durumda, kişisel veriler toplanma amacından farklı bir amaç için fakat ilişki kurabilecek alanlarda işlenmektedir. Bir e-ticaret şirketinin, müşterinin e-posta adresini ve satın alma geçmişini kullanarak, organik süt ürünleri dahil olmak üzere benzer ürünler için kişiselleştirilmiş teklifler ve indirim kuponları göndermek istemesi hali bu duruma örnektir. Ayrıca, müşterinin adı, e-posta adresi, telefon numarası ve satın alma geçmişi gibi verilerini, mahallede organik kasaplık işi açan

⁶²⁶ European Data Protection Supervisor (2012) . *Opinion of the European Data Protection Supervisor on Data Protection Reform Package*, Brüksel, para. 115.

⁶²⁷Article 29 Working Party, (2013, April 2) *Opinion 03/2013 on Purpose Limitation*, s.40. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . (Erişim Tarihi: 05.06.2025) .

⁶²⁸Atalan, 2024, s. 57.

⁶²⁹Article 29 Working Party, (2013, April 2) *Opinion 03/2013 on Purpose Limitation*, s.22. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . (Erişim Tarihi: 05.06.2025) .

bir iş ortağına aktarmak istemektedir. Her iki durumda da, şirketin kişisel verileri yeniden kullanımın uyumlu olduğunu söylenemez. Bu durumda yukarıda sayılan GDPR m.6/4 hükmündeki kriterler değerlendirilmelidir⁶³⁰.

- Dördüncü yani son ihtimalde, kişisel veriler yine toplanma amaçları dışında işlenmektedir. Fakat burada ilgili kişiyi veri sorumlusu karşısında dezavantajlı duruma koyan ve toplanma amacı ile hiçbir şekilde bağdaşmayan veri işleme faaliyetleri bulunmaktadır. Örneğin, bir e-ticaret platformunda müşteriye organik ürün satılmasında, şirketin müşteriye haber vermeden, kişiselleştirilmiş dinamik fiyatlandırma YZ teknolojisinin kullanması halinde böyledir. Bu durum kişinin satın alma amacı ile bağdaşmamaktadır. Buradaki müşterinin gizli fiyat ayrımcılığına maruz bırakılması ile ilgisiz amaç kapsamında kişisel verilerin yeniden işleme hali hukuka aykırılık teşkil etmektedir⁶³¹.

Yapay zeka işleyişine “amaçla sınırlılık” ilkesi kapsamında bakıldığında nispeten karışık bir düzen ile karşılaşılacaktır. Nitekim, kişisel verilerin yapay zeka sistemlerinde birden fazla fonksiyonları vardır. Kişisel veriler yapay zeka sistemlerine girdi olarak dahil olabileceği gibi sistemin eğitilmesinde de kullanılabilir. Ayrıca elde edilen kişisel veriler YZ sistemlerinde daha sonra başka bağlamlarda da kullanılabilir.

Kişisel verilerin sisteme girdi olarak katılmasında YZ sisteminin fonksiyonu ve sistem ile elde edilmek istenen amaç hakkında kullanıcının bilgilendirilmesi hali “amaçla sınırlılık” ilkesi ile uyumludur. Diğer bir ihtimal olarak YZ sistemlerine dahil olan kişisel verilerin başka fonksiyonları gerçekleştirmek ve kazanımları elde etmek için kullanılmasıdır. Örneğin, bir e-ticaret şirketinden spor ayakkabıları satın alan müşterinin dijital ayak izlerinin takip edilmesi ve teslimat konum bilgisi kullanılarak “kişiselleştirme” yapılması ve böylece öneri sistemleri ile (kullanıcının önceki satın alım davranışlarından çıkarımlar elde edilerek) kullanıcının karşısına sevebileceği ve mevsime uygun olan spor ayakkabıların çıkarılması(davranışsal reklamcılık) halinde bu böyledir. Somut olayda müşteri(İlgili kişi) kişisel verilerini satış sözleşmesi ve teslimat için paylaştığı kişisel verilerin, müşterinin satın alma davranışlarının arttırılması ile kişiselleştirilmesi için kullanılması “amaçla sınırlılık” ilkesi ile örtüşmez⁶³².

Son ihtimal, kişisel verilerin YZ sisteminin eğitilmesi için kullanılma ihtimalidir. Burada kişisel veriler büyük veri setlerinin istatistiksel bir parçası olarak bulunurlar⁶³³. “Amaçla Sınırlılık” prensibinin istisnası, kişisel verilerin sonradan işlenmesinin bilimsel veya tarihi araştırma amaçları veya istatistiki amaçlarla gerçekleştirilmesidir(GDPR, m.5/1-b). Dolayısıyla, bu ilkeye uyum sağladığı söylenebilir.

⁶³⁰Article 29 Working Party, (2013, April 2) *Opinion 03/2013 on Purpose Limitation*, s.23. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . (Erişim Tarihi: 05.06.2025) .

⁶³¹Article 29 Working Party, (2013, April 2) *Opinion 03/2013 on Purpose Limitation*, s.23. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . (Erişim Tarihi: 05.06.2025) .

⁶³² Burada şirket, yeni veri işleme işleme faaliyetinin yasal dayanağı olarak işini geliştirmek ve daha uygun sağlamak ile hizmet kalitesinin iyileştirilmesi gibi sebepler ile meşru menfaat ilkesine başvurabilir. Atalan, 2024, s. 59.

⁶³³ Atalan, 2024, s. 58.

3.3.1.3. Veri minimizasyonu ilkesi

Veri minimizasyonu ilkesi GDPR m. 5/1-c’de: “kişisel verilerin işleme amaçlarına uygun, işleme amaçlarıyla ilgili ve bunlarla sınırlı olması.” şeklinde; KVKK m.4/1-ç’de ise “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olunması” şeklinde ifade edilmiştir.

Avrupa Birliği Adalet Divanı, 2023 tarihli “*Norra Stockholm Bygg AB v Per Nycander*” kararında kişisel verilerin orantılılık prensibine uygun şekilde işlenmesi gerektiği belirtmiştir⁶³⁴. Bu kapsamda, kişisel verilerin toplanmasında ve veri sorumlularınca tutulmasında gerekli olan kadar verinin toplanması asıldır⁶³⁵. Veri minimizasyonu prensibi ile işleme amacının gerçekleştirilmesinde gerekli olandan fazla verinin talep edilmemesi olarak anlaşılmaktadır. Kişisel veriler gerekli olan asgari düzeyde tutulmalı ve işleme amacı başka yollarla gerçekleştirilemediği takdirde işlenmelidir⁶³⁶. Mevcutta olmayan ve sonradan gerçekleşmesi düşünülen amaçlarla kişisel veri toplanmamalı veya işlenmemelidir⁶³⁷. “İleride lazım olursa” mantığı kişisel verilerin işlenmesi bu ilkeyle bağdaşmadığından hukuka aykırıdır⁶³⁸. Bu doğrultuda öncelikle, kişisel verilerin kullanılmasının mutlaka gerekli olup olmadığı değerlendirilerek⁶³⁹; kişisel verilerin işlenmesi amacının gerçekleştirilmesi için gereken en az sayıda kişisel veri kullanılmalıdır. Teknolojik araçlar ile sağlanan kişisel veri işlemlerinde de bu kural sağlanmalıdır. Nitekim, *örneğin*, mağaza içinin güvenliğini sağlamak için yerleştirilen kameranın görüş açısının mağaza dışını da kapsamaması halinde veri minimizasyonu ilkesi ihlal edilmiş ve hukuka aykırı şekilde işleme gerçekleştirilmiş olacaktır⁶⁴⁰.

Yapay zeka bağlamında bu ilkenin çalıştırılabilmesi esasen güçtür. Çünkü, yapay zeka sistemlerinin işleyebilmesi ile doğru ve yerinde karar alabilmeleri büyük veri kümeleri ile çalışabilmeleri koşuluna bağlıdır⁶⁴¹. Bu ilke, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması yani; veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına gelmektedir⁶⁴². Dolayısıyla mesele az sayıda veri işleme değil amaç ile orantılı olacak ölçüde verinin işlenmesidir⁶⁴³. Yapay zeka sistemlerine de bu bakış açısı ile yaklaşılmalıdır. Veri minimizasyonu ilkesinin uygulanması ile kişisel veri ihlallerinin önemli ölçüde azalacağı ifade edilmektedir⁶⁴⁴.

3.3.1.4. Verilerin güncel ve doğru olması ilkesi

GDPR m.5/1-d bendinde, kişisel verilerin doğru olması ve gerektiğinde güncel tutulması gerektiği düzenlenmiştir. Kişisel verilerin işleme amaçları göz önünde tutularak,

⁶³⁴ ABAD (Avrupa Birliği Adalet Divanı), 2023, *Norra Stockholm Bygg AB v Per Nycander* Kararı, C-268/21, Para. 4, 49, 54. Karar tam metni için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0268> (Erişim Tarihi: 12.07.2025).

⁶³⁵ Akgül, 2014, s.131.

⁶³⁶ European Data Protection Supervisor (2012). *Opinion of the European Data Protection Supervisor on Data Protection Reform Package*. Brüksel. para. 114.

⁶³⁷ Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Uygulanması, s.47.

⁶³⁸ Akgül, 2014, s. 128.

⁶³⁹ Küzeci, 2010, s.203-205.

⁶⁴⁰ Akgül, 2014, s.133.

⁶⁴¹ Başalp, 2015, s.78.

⁶⁴² Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Uygulanması, s.48.

⁶⁴³ Atalan, 2024, s.60.

⁶⁴⁴ Selek, 2021, s.83.

doğru olmayan kişisel verilerin gecikmeksizin ve kalıcı olarak silinmesi veya düzeltilmesi adımları atılmalıdır. KVKK m.4/2-b’de benzer şekilde: “*kişisel verilerin doğru ve gerektiğinde güncel olması*” gerektiği düzenlenmiştir. İlgili kişilerin, doğru olmayan kişisel verilerinin düzeltilmesini isteme hakkı bu ilke ile ilişkilidir⁶⁴⁵.

İşlenen kişisel verilerin doğruluğu özellikle ilgili kişinin menfaatini korumaktadır. Aksi durumda, yani kişisel verilerin gerçeği yansıtmaması ilgili kişinin temel insan haklarına, ekonomik çıkarlarına ve manevi bütünlüğüne zarar verebilir⁶⁴⁶. Kişisel verilerin doğru ve güncel olmaması veri sorumlusu tarafından işleme amacına ulaşılmasını engelleyebilmekte ve tarafları zarara uğratabilmektedir. Nitekim, bir GSM şirketinin müşterilerine ilişkin kişisel verileri doğru ve güncel tutmaması karşısında şahsa değil, şahsın ortağı olduğu şirket numaralarına kişinin borç durumuna ilişkin kısa mesaj atılması sureti ile kişinin borcunun diğer çalışanlar tarafından öğrenilmesine ilişkin olayda Kişisel Verilerin Korunması Kurumu söz konusu GSM şirketinin kişisel verileri doğru ve güncel tutmaması sebebiyle kusurlu bularak hakkında 85.000-TL idari para cezasına hükmetmiştir⁶⁴⁷. Dolayısıyla, kişisel verilerin doğru ve güncel olması hem veri sorumlusu hem de ilgili kişi bakımından önem teşkil etmektedir.

Yapay zeka bakımından değerlendirildiğinde ise karşımıza yapay zekanın besini olan verilerdeki yanlış bilgilerin YZ sistemi çıktısının da yanlış olması sonucunu doğuracağı çıkmaktadır⁶⁴⁸. Bu durumda YZ sistemi beklenen faydayı sağlayamayacaktır. Dolayısıyla verilerin güncel ve doğru olması YZ sisteminin doğru şekilde çalışabilmesi için gereklidir. Kişisel verilerin doğru ve güncel olması veri sorumluları tarafından gerçekleştirilecek denetimlerle sağlanabileceği gibi; bu durumu fark eden ilgili kişinin müracaatı ile kişisel verilerindeki yanlışlıkların düzeltilmesini istemesiyle de gerçekleştirilebilir.

3.3.1.5. Saklama süreleri ile sınırlılık (“depolamanın sınırlandırılması”)

Depolamanın sınırlandırılması prensibi, kişisel verilerin yalnızca kişisel verilerin işleme amaçlarının gerektirdiği sürece ilgili kişinin kimliğinin belirlenmesini sağlayan bir şekilde tutulmasını ifade etmektedir(GDPR, m.5/1-e). KVKK düzenlemesinde bu hususta kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiği ifade edilmiştir(KVKK m.4/2-d).

Depolamanın Sınırlandırılması ilkesi gereği, kişisel veriler toplanma amacının gerçekleştirecek süre kadar muhafaza edilmeli ve bu sürenin sonunda silinmeli veya anonim hale getirilmelidir. Örneğin, bir telekom şirketine yapılan şikayete ilişkin ses kaydının, şikayet sonuçlandırıldıktan ve varsa mevzuat süresi akabinde silinmesi gerekmektedir. İlgili kişilerin

⁶⁴⁵ bkz. aşağıda ”3.3.3.2.Kişisel verilerin düzeltilmesini isteme hakkı” Başlığı.

⁶⁴⁶ Develioğlu, 2017, s. 48.

⁶⁴⁷ Kişisel Verileri Koruma Kurulu (2023, 19 Ocak). “İlgili kişinin borç bilgisinin ortağı olduğu şirketin kurumsal numaralarına kısa mesaj olarak gönderilmesi” hakkında Kurul Kararı No. 2023/78. Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/7596/2023-78> (Erişim Tarihi: 26.07.2025) . KVKK ve insan hakları kapsamında ilgili kararın değerlendirmesi için ayrıca bkz. Egemen, E. E (2023). Kişisel verilerin işlenmesinde “doğru ve gerektiğinde güncel olma” ilkesi ve Kişisel Verileri Koruma Kurulunun 2023/78 sayılı kararı. *Trabzon Üniversitesi Hukuk Fakültesi Dergisi*, 1 (1), 105–133.

⁶⁴⁸ Retornaz ve Güçlütürk, 2021, s.282, 290.

amaçla ilgili olarak artık gerekli olmayan verilerinin silinmesi hakkı bu ilke ile ilişkilidir(GDPR m.17)⁶⁴⁹.

Kişisel verilerin ancak mevzuatta yer alan süreler kadar şirket ve YZ veri depolarında saklanabileceği anlaşılmaktadır. E-ticaret platformlarında kullanılan yapay zeka uygulamalarında kişisel verilerin depolanmanın sınırlandırılması ilkesinin işletilmesinde güçlükler ile karşılaşılabilir. Nitekim, müşterilerden toplanan kişisel veriler şirketler ve YZ uygulamaları veri tabanlarında ticari stratejilerin belirlenmesi ve uygulamaların geliştirilmesi için muhafaza edilmektedir⁶⁵⁰. Dolayısıyla ilk olarak söz konusu kişisel veri ile ilgili mevzuat araştırması yapılmalıdır. Diğer bir husus ise, kişisel verilerin, mevzuatta belirtilen süreden sonra ilişkili oldukları kişileri işaret edecek şekilde tutulmamasıdır. Bu süreler genellikle ulusal kanunlarda belirlenmiştir. Mefhumi muhalifinden anlaşılan odur ki, kişisel veriler ait oldukları gerçek kişinin ortaya çıkarılmasını engelleyecek şekilde ilişkisi bertaraf edilerek e-ticaret şirketlerince ve YZ uygulamasınca ticari stratejilerin belirlenmesi ve uygulamaların geliştirilmesi için muhafaza edilmeye devam edilebileceklerdir. Kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla işlendikleri sürece, daha uzun sürelerle depolanabilecektir(GDPR m.5/1-e).

3.3.2. Yapay zeka uygulamalarında kişisel verilerin işlenebilmesinin hukuki şartları

Kişisel verilerin hukuka uygun şekilde işlenebilmesi için yalnızca kişisel verilerin korunması ilkelerine uyumlu olması yeterli değildir. Nitekim, bu verilerin şirketler bünyesinde işlenebilmesi ancak mevzuattaki koşulların yerine getirilmesi ve öngörülen yasaklardan kaçınılmasıyla, işlemenin yasal dayanaklara dayandırılması ile, hukuka uygun hale gelmektedir. Bu şartlar, yükümlülükler ve kısıtlamalar aşağıda açıklanmıştır.

3.3.2.1. İlgili kişinin açık rızası

Kişisel verilerin hukuka uygun olarak işlenmesi şartları GDPR m.6'da ve KVKK m.5'te düzenlenmiştir. Buna göre, kişisel verileri işleyen e-ticaret platformlarının dikkat etmesi gereken ilk unsur ilgili kişinin rızasıdır. Nitekim kişisel verilerinin işlenmesine, verisi işlenen kişinin rıza vermesi durumunda bu işleme hukuka uygun hale gelir. İlgilinin rızası olmadığı durumlarda işleme kural olarak hukuka aykırıdır.

Açık rıza kavramı kişisel verilerin işlenmesinin ayrılmaz bir parçasını teşkil etmektedir. Nitekim, kişisel veriler için veri ve özel nitelikli(hassas) veri ayrımı yapılmakta ve her ikisinin de işlenebilmesi için ilgilinin rızası aranmaktadır(GDPR m.6/1-a; m.9/2-a; KVKK m.5/2-a; m.6/3-a). Kişisel verilerin üçüncü kişilere ve yurtdışına aktarımında da ise açık rıza şartı bulunmaktadır(KVKK m.8). Kişisel verilerin işlenmesi için büyük bir öneme sahip olan açık rıza kavramının ne olduğu ve ne olmadığının tespiti gerekmektedir.

3.3.2.1.1. Açık Rızanın Unsurları

Kişisel verilerin işlenmesi kapsamında ilgili kişiden rıza alınması, GDPR düzenlemesinde; *“veri öznesinin, kişisel verilerinin bir ya da daha fazla spesifik amaca yönelik olarak işlenmesine rıza vermesi”* olarak ifade edilmiştir(GDPR m.6/1-a). Açık Rıza kavramı ise; *“veri öznesinin, bir beyanla ya da açık bir onay eylemiyle kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini belirttiği, özgür bir şekilde, spesifik, bilinçli ve açıkça ifade edilen*

⁶⁴⁹ Develioğlu, 2017, s.49; Şimşek, 2008, s. 84-85.

⁶⁵⁰ Küzeci, 2014, s.142-149; Xue vd., 2018, s. 1423; Gupta vd., 2020, s. 256; Özgür, 2023, s.9-10.

istekleri” (GDPR m.4/11); benzer şekilde KVKK m. 3/1-a’da “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak tanımlanmıştır.

Bu tanımlardan hareketle “açık rıza” kavramından, ilgili kişinin kendisiyle ilgili veri işlenmesine, konuyla ilgili yeterli bilgi sahibi olarak ve sadece o işlemle sınırlı olarak, spesifik, bilinçli, açıkça ve özgürce verdiği onay beyanı anlaşılmalıdır. Dolayısıyla “*açık rızanın*” dört unsuru içerdiğini söyleyebiliriz. Bunlar Rızanın; Sınırlı olarak belirlenmiş bir konu özelinde verilmesi, Bilgilendirmeye dayalı olması, Özgürce verilmiş olması ve Tereddüt oluşturmayacak açıklıkta verilmiş olmasıdır⁶⁵¹. Rıza mekanizması ile genel olarak, verisi işlenen kişinin verilerinin üzerinde hakimiyet kurabilmesini sağlamaya çalışılmaktadır⁶⁵²(GDPR, giriş, para.42).

3.3.2.1.1.1. sınırlı ve belirli olma

Açık rızadan bahsetmek için öncelikle hakkında rıza verilen konunun sınırlarının çizilmesi gerekmektedir⁶⁵³. Böylece, kişisel verilerin hangi amaçlar ile işleneceği belirlenir ve ilgili kişi bildirilir. Başkaca konulara ilişkin kişisel verilerin işlenmesi halinde, bu konular hakkında ilgili kişiden tekrar rıza alınmalı ve sonradan eklenen konular rıza talebinde açıkça ayırt edilebilecek nitelikte sunulmalıdır⁶⁵⁴. Veri işlemenin tam amacını belirtmeyen genel rıza beyanları kabul edilemez⁶⁵⁵. Son olarak amaçlar tek tek belirtilmeden ilgili kişi tarafından verilen genel onay açık rıza kapsamında değerlendirilemez⁶⁵⁶.

Rızanın sınırlı ve belirli olması için anlaşılabilir olması gerekir: rıza açık ve kesin bir şekilde kapsamına ve veri işlemenin sonuçlarına atıfta bulunmalıdır. Açık uçlu bir dizi işleme faaliyeti için geçerli değildir. Kişisel veri işleme amaçlarının açıkça tanımlanmış olması halinde “*Spesifik(sınırlı ve belirli) Rıza*” kavramından bahsedilebilecektir. Nitekim, sınırlı ve belirli konularda verilmiş rıza özünde bilgilendirilme kriteri ile bağlantılıdır. Rızanın izlenen “*tüm meşru amaçları*” kapsamı mümkün değildir. Rıza, belirtilen amaca ilişkin olarak makul ve gerekli olan işlemeye verilmektedir. Kişisel verilerin toplanma amacı karşısında ilgili kişinin “makul beklentisi” çerçevesinde gerçekleşen kişisel veri işlemleri hakkında rıza verilmiş sayılır; rıza verilen amacı aşan işleme faaliyetlerinde verilmiş bir rızadan bahsedilemez⁶⁵⁷.

⁶⁵¹ Akgül, 2014, s.149.

⁶⁵²Article 29 Working Party (2014) . *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, s. 16. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim Tarihi: 08.06.2025) .

⁶⁵³ Küzeci, 2010, 239.

⁶⁵⁴Develioğlu, 2017, s.53; Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 18. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025)

⁶⁵⁵Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 17. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁵⁶Develioğlu, 2017, s.53; Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 17,34-35.https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁵⁷Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 17. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

3.3.2.1.1.2. özgür irade şartı

Kişisel verilerin işlenmesinde ilgili kişinin vereceği rıza hiçbir baskı altında kalmadan mevcut durumun bilincinde olarak verilmelidir⁶⁵⁸. İlgilinin kişinin rızanın özgürce verilip verilmediği değerlendirmesinde ilgili kişilerin rıza vermede zorunda bırakılıp bırakılmadıkları değerlendirilmelidir. Kişinin tehdit, aldatma ve korkutma ile verdiği rıza hukuki şartı sağlamaz⁶⁵⁹. Taraflar arasında güç dengesizliği olduğu durumlarda kişinin özgürce rızasını verip vermediği ayrıca değerlendirilmelidir. Nitekim, aralarında hiyerarşi veya güç dengesizliği bulunan kişilerde, örneğin, işçi-işveren ilişkilerinde, özgür iradeye çekince ile bakılacaktır⁶⁶⁰. Rızanın özgürce verilmesi değerlendirmesinde gözetilecek diğer husus koşulluktur. Nitekim GDPR m.7/4'e göre: bir sözleşmenin ifasının, söz konusu sözleşmenin ifası için gerekli olmayan kişisel verilerin işlenmesine rıza verilmesine bağlı olup olmadığı dikkate alınmalıdır. Burada sözleşmenin gerçekleşmesi için rıza talep edilen kişisel verinin gerekli olup olmaması incelenmelidir.

Son olarak, farklı kişisel veri işleme işlemlerine ayrı ayrı rıza verilmesi uygun olduğu halde buna izin verilmiyorsa bu durumda da kişisel verilerin işlenmesine özgürce rıza verildiğinden bahsedilemeyecektir(GDPR, *giriş*, m.34). İnternette yapılan bir işlem neticesinde alınan açık rıza da bir diğer tartışma konusudur. Nitekim, ilgili kişi rızasını verirken bu rızayı internette var olabilmenin bir şartı olarak görmekte böylece sebep ve sonuçlarını anlayarak bilinçli olarak bir rıza değil bir bedel olarak açık rızasını yapılan işlem neticesinde veya sırasında vermektedir. Bu durumda bu rızaların özgür iradelerin bir sonucu olmadığı açıktır⁶⁶¹. Rızanın gerçekten yeterince özgür olup olmadığını değerlendirmek için her bir vaka bazında ayrı bir değerlendirme yapılmalıdır⁶⁶².

Belirtilmelidir ki; rızanın özgür irade ürünü olması karşısında GDPR ile ilgili kişiye verdiğini rızasını istediği zaman geri çekme hakkı tanınmıştır. Rızanın geri çekilmesi işlemi, rızanın verilmesi kadar kolay olmalıdır. Bu kolaylığı sağlama ödevi veri sorumlusu üzerindedir. Rızanın geri alınması, bundan önce rızaya dayalı olarak yapılan işlemlerin hukuka uygunluğunu etkilemez, bu cihetle geçmişe dönük bir etkisi yoktur. Rıza bundan sonraki işlemler için yok sayılır(GDPR, m.7/3.).

3.3.2.1.1.3 bilgilendirme yükümlülüğü

Veri sorumlusunun bilgilendirme yükümlülüğü ile açık rıza şartının tamamlanması arasında sıkı bir ilişki mevcuttur. Kişisel verilerin işlenmesinde rızanın geçerliliği için ilgili kişiye yeterli açıklamanın yapılması gerekmektedir. Nitekim, bir kişi ancak sebepleri ve

⁶⁵⁸ Akgül, 2014, s.149.

⁶⁵⁹ Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 34. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁶⁰ European Data Protection Supervisor (2012) . *Opinion of the European Data Protection Supervisor on Data Protection Reform Package*, Brüksel, para.127; Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 16. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁶¹ Ayözger Öngün, "Açık Rıza".

⁶⁶² Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 18. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

sonuçlarını iyi şekilde anladığı bir konuya rızasını sağlıklı şekilde verebilir. Hukuken muteber olan rıza, ilgili kişiye bildirim yapıldıktan sonra alınan rızadır⁶⁶³.

Rızanın hukuken geçerli olabilmesi için her zaman rızanın ne için alındığına ilişkin bilgi verilmesi gerekmektedir. Bu da pratikte şu anlama gelmektedir: veri sahibinin rızası, bir eylemin gerçeklerinin ve sonuçlarının takdir edilmesi ve anlaşılmasına dayanır. İlgili kişiye, açık ve anlaşılır bir şekilde, işlenen verilerin niteliği, işleme amaçları, olası aktarımların alıcıları ve veri sahibinin hakları ile ilgili tüm konular hakkında doğru ve tam bilgi verilmelidir. GDPR m. 10 ve 11 hükümlerinde bilgilendirme mutlaka yer verilmesi gereken hususlar sayılmıştır; bilgilendirme metni belirtilen bu bilgileri içermelidir. Böylece ilgili kişiye vereceği rızası karşısında yapılacak işleme faaliyetlerinin sonucuna ilişkin farkındalık kazandırılarak⁶⁶⁴ verilecek rızanın bilinçli şekilde verilmesi amaçlanmaktadır.

Kullanıcılara yapılan bildirimin gözden kaçmaması için açık ve yeterince dikkat çekici şekilde bulundurulması gerekmektedir. Bilgilendirmede anlaşılır ve basit bir dil kullanılmalıdır. Bu durum şeffaflık ilkesinin de bir sonucudur. Bilgilendirme çok uzun olmamak koşulu ile anlaşılabilir şekilde yapılmalı ve bilgiler açıkça görülebilir (yazı tipi ve boyutu) ve belirgin şekilde yazılmalıdır. Gerekli görülmesi halinde resim ve tablolardan faydalanılmalıdır⁶⁶⁵. Bilgilendirme yükümlülüğünün baştan savma ve göstermelik olarak yapıldığı hallerde açık rızadan bahsedilemez. İlgili kişinin, verisinin işlenmesine açık rızasını verdiğini ispat yükü veri sorumlusunun üzerindedir⁶⁶⁶.

3.3.2.1.2. Rızanın açık olması ile şekil şartı

GDPR, rızanın açık Her iki rızanın şüpheye yer bırakmayacak açıklıkta verilmesi gerekmektedir⁶⁶⁷. Rızanın birden fazla konuyu içermesi halinde rıza; her bir konu için verildiği ayırt edilecek şekilde verilmelidir⁶⁶⁸.

Açık rızanın verilmesi için bir şekil şartı bulunmamaktadır. Bu rıza beyan ile veya onay eylemi ile verilebilir. Bu, bir internet sitesini ziyaret ederken bir kutunun işaretlenmesini, bilgi toplumu hizmetleri için teknik ayarların seçilmesini ya da veri öznesinin kişisel verilerinin önerilen biçimde işlenmesini kabul ettiğini bu bağlamda açıkça gösteren başka bir beyan veya davranışı içerebilir. Sükût, önceden işaretlenmiş kutular ya da hareketsizlik rıza teşkil etmez(GDPR, giriş, para.32).

⁶⁶³ Akgül, 2014, s.149-150; Develioğlu, 2017, s.57; Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 19. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁶⁴ Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 19. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁶⁵ Akgül, 2014, s.149; Küzeci, 2010, s.224-225; Develioğlu, 2017, s.53; Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 20,34.. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁶⁶ European Data Protection Supervisor (2012) . *Opinion of the European Data Protection Supervisor on Data Protection Reform Package* , Brüksel, para.127.

⁶⁶⁷ Akgül, 2014, s.150; Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 35. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁶⁸ Develioğlu, 2017, s.53.

3.3.2.1.3. Özel nitelikli kişisel veriler özelinde değerlendirme

Özel nitelikli kişisel verilerin⁶⁶⁹ işlenmesi kural olarak yasaktır(GDPR m.9, KVKK m.6). Ancak bu yasak mutlak olarak uygulanmamaktadır. Uluslararası düzenleyici metinlerde özel nitelikli kişisel verilerin işlenmesinde hukuka uygunluk sebeplerine yer verilmiştir. Özel nitelikli kişisel veriler, öncelikle ilgili kişinin açık rızasının olması halinde işlenebilecektir. Fakat rıza olmadığı hallerde de bu veriler işlenebilecektir. Özel nitelikli kişisel verilerin işlenebileceği bu istisnai haller sınırlı olarak belirlense de kapsamı geniş tutulmuştur⁶⁷⁰. Kıta Avrupası metinlerinde istisnaların geniş tutulması karşısında, KVKK kapsamı daha da genişletmiştir. Nitekim, GDPR ve 95/46/EC Direktif’inde istihdam kanunu, sosyal güvenlik ile sosyal koruma hukuku alanındaki yükümlülüklerinin yerine getirilmesi ve spesifik haklarının kullanılması amacıyla verilerin işlenebileceği öngörülmüşken; KVKK m.6/3-b

⁶⁶⁹ bkz. yukarıda ”2.7.1.Özel nitelikli kişisel veriler (Hassas kişisel veriler)” başlığı.

⁶⁷⁰ Kaya, 2011, s. 333. 95/46/EC Direktifi (m.8/2) ve GDPR (m.9/2) düzenlemelerine göre, verisi işlenen kişi, hassas nitelikli verilerinin işlenmesine açık şekilde rızasını vermesi halinde bu veriler işlenebilmektedir. Açık rızanın olmadığı hallerde ise genel olarak istihdam kanunu, sosyal güvenlik ile sosyal koruma hukuku alanındaki yükümlülüklerinin yerine getirilmesi ve spesifik haklarının kullanılması amacıyla denetleyicinin yükümlülüklerini ve özel haklarını yerine getirme amacı için gerekli olduğunda; veri öznesinin rızasını vermesinin fiziksel veya yasal olarak elverişsiz olduğu durumda diğer bir kişinin veya veri öznesinin hayati menfaatlerini korumak için; işleme bir vakıf, dernek veya siyasi, felsefi, dini veya ticaret birliği amaçlı başka bir kar amacı gütmeyen kuruluş tarafından uygun teminatlı meşru faaliyetler esnasında yapılırsa, veya veri öznesi tarafından alenileştirilen verilere ilişkinse ya da hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulması için veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ederken işlemenin gerekli olması halinde, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi amacıyla gerekli olması, işlemenin, koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, halk sağlığı alanında kamu yararına ve diğer kamu yararına yönelik nedenlerden dolayı işlemenin gerekli olması ile kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda gerekli olması durumlarında ilgili kişinin açık rızası olmadan da işlenebileceğini düzenlemiştir. Türk hukuku bakımından, hassas nitelikteki verilerin ancak rıza ile işlenebileceği belirtilmiş; rıza aranmayan haller ise KVKK m.6’da düzenlenmiştir. KVKK, m.6/3: Özel nitelikli kişisel verilerin işlenmesi yasaktır. Ancak bu verilerin işlenmesi;

- a) İlgili kişinin açık rızasının olması,
- b) Kanunlarda açıkça öngörülmesi,
- c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,
- d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,
- e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,
- f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,
- g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması halinde mümkündür.

bendinde genel bir ifade olarak "kanunlarda açıkça öngörülmesi"⁶⁷¹ istisnasını kapsama dahil etmiştir. Bu durum, doktrinde eleştirilmiş⁶⁷² ve KVKK'nın hassas nitelikli veriler ile hassas olmayan nitelikteki ayrımı belirsizleştirdiği ifade edilmiştir⁶⁷³.

Genel nitelikteki veriler bazen özel nitelikteki verilerle ilişkili olabilir. Örneğin, bir bireyin sağlıkla ilgili verilerle ilişkilendirilebilen web sitelerine yaptığı ziyaretlere ilişkin gezinme verilerinde bu böyledir. İlgili kişinin vereceği rızanın etkileri gözetilerek duruma uygun olduğu hallerde rıza özel nitelikli kişisel veri kapsamında dolayısıyla daha sıkı koşullar altında alınmalıdır⁶⁷⁴.

Belirtilmelidir ki, özel nitelikli kişisel veriler yüksek riskli yapay zeka sistemlerinde ancak, önyargıların tespiti ve düzeltilmesinde gerekli olduğu ölçüde kullanılabilir (AI Act m.10/5). Veri sorumluları, yapay zeka sistemlerinde, sistemin kendisinden doğan özel nitelikteki kişisel verilerin işlenmesinde temel hak ve özgürlükleri koruyucu önlemleri almalıdır.

3.3.2.1.4. E-ticarete kullanılan yapay zeka uygulamalarında açık rıza

E-ticaret platformlarında kullanılan YZ uygulamaları kapsamında açık rıza kavramı değerlendirilmesinde belirtilmesi gereken ilk mesele: Yapay zeka uygulamalarında kişisel verilerin işlenmesi sisteminin oldukça karmaşık olduğudur. Bu durum şeffaflık ilkesi bölümünde detaylandırılmıştır. Rızanın verilmesi için ön koşul verisi işlenecek kişinin veri işleme amaçları ve yöntemleri hakkında bilgilendirilmesidir. Veri işleme ne kadar karmaşık ise veri sorumlusundan da o kadar fazla şey beklenmelidir. Ortalama bir birey için veri işlemenin tüm unsurlarını denetlemek ve anlamak ne kadar zorlaşırsa, veri sorumlusunun rızanın belirli, anlaşılabilir bilgilere dayalı olarak alındığını gösterme çabaları da o kadar büyük olmalıdır⁶⁷⁵. Açık rızanın verilmesi için ön koşul olan bilgilendirme direk kişisel verisi işlenen kişiye doğrudan yapılmalıdır. Bu bilgilendirmenin platformun bir yerinde beklemesi ile bilgilendirme şartı gerçekleşmez⁶⁷⁶.

Belirtilmelidir ki, kişisel verilerin işlenmesinin rızaya dayanması bu teknolojilerin işlenmesi ve geliştirilmesi için bir engel teşkil edebilir. Nitekim, büyük veri teknoloji sayesinde çok büyük miktarda ve hızla toplanan kişisel veriler için ilgili kişilerden hukuka uygun bir rıza

⁶⁷¹ Kanunlarda açıkça öngörülen hallerde açık rıza aranmaksızın kişisel veri işlenebilecektir. Örneğin, kolluk tarafından bir suç soruşturması sebebiyle, 2559 sayılı Polis Vazife ve Salahiyet Kanununun 5 inci maddesi uyarınca şüphelilerin parmak izlerinin alınması, 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetlerine ilişkin verilerini işleme gibi durumlarda açık rızaya gerek yoktur.

⁶⁷² KVKK düzenlemesinin bu yaklaşımı açık şekilde AB direktifleriyle çatışmaktadır, diğer yandan bu düzenleme temel hak ve özgürlüklere müdahale kapısını aralayabilir. Özel nitelikteki kişisel verilere ilişkin kesin işlem yasağına getirilen bu geniş ve belirsiz istisna sebebi ile ihdas edilen her kanun sektör bazında ölçülülük, meşruluk ve belirlilik tartışmalarını gündeme getirecektir. Aygözer Öngün, 2019, s.24-25; Kaya, 2011, s. 333. KVKK'da yer alan istisnalar o denli geniştir ki, kişisel verilerin sahibinin rızası çerçevesinde işlenebileceği ilkesi adeta istisnai bir hal almıştır. Bu yönüyle AB düzenlemeleri ile çatışan Kanun'un veri koruma yasalarından beklenen işlevini gerçekleştirebileceğini ummak gerçekten güçtür. Aksoy, 2010, 121.

⁶⁷³ Aygözer Öngün, 2019, s. 34

⁶⁷⁴ Prins, 2006, s. 291.

⁶⁷⁵ Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 21. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁷⁶ Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 35. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

alınmasının güç olması karşısında yapay zeka tabanlı bu uygulamalarda hukuka uygun rızanın alınıp alınmadığı bir soru işareti taşımaktadır. Yapay zeka uygulamalarının kişisel verilere ilişkin alması gereken rıza iki şekilde olabilir: bu verilerin bir eğitim setine dahil edilmesi için rıza ile kişiselleştirilmiş yanıtlar sunmayı amaçlayan algoritmik bir sisteme girdi olarak sağlanmasına verilmesi gereken rızadır⁶⁷⁷.

Kullanıcılar e-ticaret platformlarında kişisel verilerinin işlenmesine rıza vermek için özgür olmalıdır. Sözleşmenin ifasının, sözleşmenin ifası için gerekli olmayan bir şarta bağlanması durumu özgür irade şartına aykırılık teşkil edecektir. Örneğin, bir e-ticaret şirketinde satış sözleşmesinin yapılması akabinde şirket tarafından tüketicinin e-postasının reklam gönderimi için saklanması bu durum böyledir⁶⁷⁸. Rıza kişisel verilerin işlenmesine başlamadan önce verilmelidir. Ancak yeni bir amaç doğrultusunda kişisel verilerin işlenmesi gerekmesi halinde işlenme sırasında da verilebilir⁶⁷⁹.

Açık rıza her ne kadar şekle bağlanmamışsa da; rızanın anlamlı bir eylem ile gerçekleşmesi gerekmektedir. Çevrimiçi ortamlarda verilen rızalarda sessizlik veya eylemsizlik ile rıza verilemeyeceğine dikkat etmek gereklidir. Bu özellikle varsayılan ayarlara alakalı bir konudur. Önceden verilerin toplanması için gerekli olan kutucuğun önceden işaretli olmasında bu böyledir⁶⁸⁰. Örneğin, ChatGBT, kullanıcıların verilerin gelecekte kullanılmaması için açıkça bir seçim yapmadığı hallerde, varsayılan ayarlı olarak kullanıcıların girdiği her türlü veri sisteme dahil etmesi rıza koşuluna aykırılık teşkil etmektedir. Yapılan veri işleme faaliyeti hukuka aykırıdır⁶⁸¹. Özel nitelikli kişisel veriler bakımından YZ uygulamaları bu verilerin özelliğinden kaynaklanan çift kat korumaya uygun şekilde işleme faaliyetleri daha özenli şekilde yapılmalıdır⁶⁸².

3.3.2.2. Meşru amaçlarla kişisel verilerin işlenmesi

Kişisel verilerin işlenmesinde rıza koşul olsa da; ilgilinin rızası olmadan da kişisel verilerin işlenilebileceği düzenlenmiştir. Bu istisnai haller GDPR m.6/1 ve KVKK m.5/2 düzenlemelerinde sayılmıştır. GDPR düzenlemesinde kişisel verilerin işlenmesi rıza olmasa da hukuka uygun sayılabilen haller şu şekilde sayılmıştır:

- Verisi işlenen kişinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce kişinin talebiyle adımlar atılması için işlemenin gerekli olması;
- Veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uyulması amacıyla işlemenin gerekli olması;
- Gerçek bir kişinin hayati menfaatlerinin korunması amacıyla işlemenin gerekli olması;

⁶⁷⁷Atalan, 2024, s.63.

⁶⁷⁸ Develioğlu, 2017, s.53.

⁶⁷⁹Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 34. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁸⁰Article 29 Working Party (2011) . *Opinion 15/2011 on the definition of consent* , s. 35. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf . (Erişim tarihi: 24.03.2025) .

⁶⁸¹ bkz. Burges, 2023.

⁶⁸² Taştan, 2017, s.41.

- Kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için işlemenin gerekli olması;
- Veri öznesinin menfaatleri veya temel hak ve özgürlüklerinin bir veri sorumlusu veya üçüncü kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu meşru menfaatler doğrultusunda işlemenin gerekli olması⁶⁸³.

KVKK düzenlemesinde de benzer amaçlara yer verilse de istisna kapsamları genişletilmiştir. Nitekim, KVKK m. 5/2 düzenlemesinde ilgili kişinin rızası olmasa da:

- Kanunlarda açıkça öngörülmesi.
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumlarında işlenmesi mümkündür.

Görüldüğü üzere KVKK düzenlemesinde GDPR düzenlemesindeki istisnai haller genişletilmiştir. Nitekim, kişisel verilerin veri sorumlusunun yükümlü olduğu yasal yükümlülükler haricinde de kanunda düzenlenmesi ile işlenebileceği öngörülmüştür. Ayrıca KVKK, kişisel verilerin bir hakkın tesisi, kullanılması veya korunması için işlenmesini hukuka uygun saymaktadır. Ne var ki, burada kullanılacak ölçütlerden bahsedilmemiştir. Nitekim, GDPR düzenlemesinde temel hak ve özgürlüklerin korunması bakımından; veri sorumlusu ile ilgili kişi hak ve menfaatleri tartılmakta ve ancak veri sorumlusunun hak ve özgürlükleri baskın geldiği durumlarda ilgili kişinin kişisel verilerinin işlenmesine müsaade edilmektedir. Herhangi bir ölçüt verilmeden kişisel verilerin işlenmesine izin veren bu geniş istisnai hallerin; kişisel verilerin ancak rıza ile işlenebileceği kuralını anlamsızlaştırdığı düşüncesindeyiz. Son olarak KVKK düzenlemesi, kişisel verilerin ilgili kişi tarafından alenileştirilmesi halinde işlenmesinin hukuka aykırı olmayacağını belirtmiştir. Ne var ki, GDPR düzenlemesinde bu yönde bir hüküm bulunmamaktadır.

Kanun lafzında “*mümkündür*” ibaresinin kullanılması sayılan istisnai durumlarda somut olayın şartlarına özgü bir değerlendirmeyi gerekli kılmaktadır. Diğer bir ifade ile sayılan durumlarda dahi kişisel verilerin işlenmesi hukuka aykırı bulunabilir. Burada ilgili kişi ile veri sorumlusu arasındaki menfaat dengesi gözetilmelidir⁶⁸⁴. Kişisel verilerin meşru menfaatler kapsamında işlenmesi halleri çalışmamız kapsamında değerlendirilecektir.

⁶⁸³Bu madde kamu makamlarının, görevlerini yerine getirirken veri işlemlerinde uygulanmaz.

⁶⁸⁴Develioğlu, 2017, s.58-59.

Bir sözleşmenin ifası için kişisel verilerin işlenmesi ilgili kişinin rızası olmasa dahi hukuka uygun olarak kabul edilmiştir. Bu durumun iki uygulama alanı vardır: sözleşme öncesi ve sözleşme ifası için gereken işlemler. Bu işlemler kapsamında gerçekleştirilecek işlemlerin hukuka uygun olabilmesi için koşul bu amaçlara hizmet için gerekli olmasıdır⁶⁸⁵.

Sözleşme öncesi kişisel veriler; veri sorumlusunun isteği veya üçüncü kişinin inisiyatifi ile değil ancak ilgili kişinin taleplerinin gerçekleştirilmesi için işlenebilir. Bu duruma örnek olarak, kişilerin perakendeciden fiyat teklifi talep etmesi üzerine, şirket tarafından isim, soyisim ve adres bilgilerinin teklifin gönderilmesi için işlenmesi gösterilebilir. İlgili kişinin sözleşmenin ifası için kişisel verilerinin gerekli olduğu durumlara örnek olarak, çevrimiçi olarak satın alınan malların teslim edilebilmesi için veri sahibinin adresinin işlenmesi veya ödemeyi gerçekleştirmek için kredi kartı bilgilerinin işlenmesi gibi durumları verilebilir⁶⁸⁶. Ancak, bu satış sözleşmesinden kaynaklanan uyumsuzluklar dolayısıyla şirket tarafından kişi ad, soyad ve adresinin örneğin dava açmak için kullanılması sözleşme konusu ile bağdaşmadığı için istisnai hüküm kapsamında değerlendirilemez. Fakat burada şirketin üstün menfaati istisnası işlemler ve bu durumda işleme yine hukuka uygun olarak kabul edilir⁶⁸⁷. İstisna olarak, sözleşme konusunun sağlık verilerini (özel nitelikteki verileri) ihtiva etmesi halinde açık rıza gerekmektedir.

Satış sözleşmesi için işlenen kişisel verilerin kişiselleştirme, dinamik fiyatlandırma, öneri sistemleri ve kişiselleştirilmiş reklamcılık için kullanılması hukuka uygun değildir. Nitekim bu işlemler satış sözleşmesinin ifası için değil; işletmenin ticari stratejilerinin belirlenmesi ve geliştirilmesi ile pazarlama hedeflerini gerçekleştirmesi amaçları ile yapılmaktadır. Bu durumlar sözleşmenin ifası için rıza aranmayacak haller olarak değerlendirilemez. Fakat müşterilerin toplanan kişisel verilerinin örneğin dolandırıcılığın önlenmesi kapsamında işlenmesi hallerinde veri sorumlusunun yasal yükümlülüklerinden veya meşru menfaatinden yani diğer istisnai hallerden bahsedilebileceği için veri işleme hukuka uygun kabul edilebilir⁶⁸⁸.

Veri sorumluların yasal yükümlülüklerini yerine getirmek için kişisel verileri işlemesi hukuka uygundur. Örneğin, şirketin çalışanlarının maaşını ödemesi için iban bilgilerini kaydetmesinde bu böyledir. Bu durumda, ilgili kanun maddesi kişisel verilerin işlenmesi için yeterince açık olmalıdır. Ayrıca, veri sorumlusunun yükümlü olduğu yasal yükümlülüğü gerçekleştirmesi zorunlu olmalı yani veri sorumlusunun yasal yükümlülüğü yerine getirme ve bu çerçevede kişisel verileri işleme konusunda bir seçeneği olmamalıdır⁶⁸⁹. Ayrıca vergi

⁶⁸⁵Develioğlu, 2017, s.62; Article 29 Working Party (2014) . *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, s.16, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim tarihi: 08.06.2025) .

⁶⁸⁶Article 29 Working Party (2014) . *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, s.17-18, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim tarihi: 08.06.2025) .

⁶⁸⁷Develioğlu, 2017,, s.61-62.

⁶⁸⁸ Article 29 Working Party (2014) . *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, s.17, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim tarihi: 08.06.2025) .

⁶⁸⁹Article 29 Working Party (2014) . *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, s.18-19,

bildirimi ve ilgili kişilerin hukuki yollara müracaat etmesi hali için kişilerin satın alım makbuzlarının ve ödeme bilgilerinin saklanması da yasal yükümlülük gerçekleştirildiği için işleme hukuka uygundur.

Kişisel verilerin yapay zeka tarafından kullanılmasında meşru menfaat kavramı kavramı işletilebilir mi? Yapay zeka tabanlı uygulamalar ile kullanıcı deneyimlerinin zenginleştirildiği, işletmelere katma değer sağlandığı, işletmenin gelir elde etmesine yardımcı olunduğu bilinmektedir⁶⁹⁰. Bu durumların veri sorumlusunun meşru menfaati kapsamında değerlendirilerek ilgili kişinin temel hak ve özgürlüklerine baskın geldiği iddia edilerek YZ uygulamaları kapsamında kişisel verilerin rıza olmadan işlenebileceği iddia olunabilir mi? Bu soru esasen çalışmamız kapsamında değerlidir. Veri sorumlusunun meşru menfaatinden yukarıda bahsedildiği üzere hukuki çarelere başvurusu hallerinde ve dolandırıcılığın önlenmesi kapsamında bahsedilebilecektir.

YZ tabanlı uygulamalarda kişisel verilerin kullanılmasına ilişkin değerlendirmede; kişisel veriler iki gruba ayrılarak incelenmelidir. Bunlar: YZ'nın öğrenmesi için eğitim setlerinde kişisel verilerin kullanılması ve YZ uygulamasına girdi olarak kullanılması halleridir. Kişisel verilerin eğitim setlerinde kullanılmasında güçlü güvenlik önlemleri alınması halinde, verilerin psödonimleştirilmesi ve model tamamlandığında anonimleştirilmesi, veri sahibinin çıkarları ciddi şekilde etkilenmemektedir. Dolayısıyla, YZ tabanlı uygulamaların kişisel veriler ile eğitilmesi halinde ilgili kişinin çıkarlarının doğrudan etkilendiğinden bahsedilemeyeceği için bu teknolojiye elde edilecek faydalar gözetildiğinde terazinin veri sorumlusundan yana ağır bastığından söz edilebilir. Altı çizilmesi gereken mesele, burada YZ uygulamalarının öğrenmesi için veri setlerine katılan veriden, kişiyi doğrudan etkilemeyen ve güçlü önlemler alınan işleme faaliyetinden bahsedilmektedir⁶⁹¹.

Veri sahiplerinin verileri, algoritmik bir modelde veri sahibi hakkında sonuçlar çıkarmak için kullanıldığında ise durum çok farklıdır. Böyle bir durumda, veri sahibinin menfaati onun değerlendirmesine göre öncelikli olmalıdır. Bu nedenle, veri sahibinden onayı istenmeli ve reddetme fırsatı verilmelidir⁶⁹². Kanaatimizce de ticari amaçlarla gerçekleştirilen, YZ uygulamalarına girdi olarak kullanılan ve kişilere ilişkin doğrudan çıkarımlar yapmaya sağlayan işleme faaliyetlerinin kişiyi dezavantajlı konuma sokacağı göz önüne alındığında kişinin temel hak ve özgürlüklere baskın çıktığından bahsedilemez.

3.3.2.3. Kişisel verileri işleme yasakları

Teknolojinin gelişmesi ve insan müdahalesi olmadan algoritmik sistemler tarafından kişiler hakkında karar verilmesi uygulamaları yaygınlaştıkça kişilerin dezavantajlı konumda bulunma riskleri ve ayrımcı davranış yasağına aykırı edilebilmesi ihtimali karşısında bazı kişisel veri işlemlerine karşı daha sıkı kurallar getirilmesi zorunluluğu doğmuştur. Aşağıda

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim tarihi: 08.06.2025).

⁶⁹⁰ bkz. yukarıda "3.2.E-Ticarete Kullanılan Yapay Zeka Uygulamaları ve Kişisel Veri İşleme Süreçleri" başlığı.

⁶⁹¹ European Data Protection Supervisor (2012). *Opinion of the European Data Protection Supervisor on Data Protection Reform Package*. Brüksel.s.50; Atalan, 2024, s.69.

⁶⁹² European Data Protection Supervisor (2012). *Opinion of the European Data Protection Supervisor on Data Protection Reform Package*. Brüksel.s.50.

kişisel verilerin işlenmesi kural olarak yasaklanmış hususlara ilişkin açıklamalara yer verilmiştir.

3.3.2.4.1. profillemeye

Profillemeye faaliyeti genel olarak; bilgileri tanımlamak, tahminlerde bulunmak ve son olarak da çıkarımda bulunmaktır⁶⁹³. GDPR m.4/4'te profillemeye: “*kişisel verilerin, bir gerçek kişiyle ilgili bazı kişisel özellikleri değerlendirmek, özellikle söz konusu gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususları analiz etmek veya tahmin etmek amacıyla kişisel verilerin kullanılmasını içeren her türlü otomatik işlenmesi biçimi*” olarak tanımlanmıştır. KVKK düzenlemesinde ise bu kavram tanımlanmamıştır. Fakat, Kişisel Verilerin Korunması Kurumu tarafından hazırlanan KVKK'ya ilişkin rehberde profillemeye tanımına yer verilmiş ve GDPR düzenlemesindeki tanım aynen burada kullanılmıştır⁶⁹⁴.

Profil oluşturma faaliyeti üç unsurdan oluşur. Öncelikle otomatik bir işleme biçimi olmalıdır; algoritmik faaliyet kişisel veriler üzerinde gerçekleştirilmelidir ve son olarak bu faaliyetin amacı, bir gerçek kişi hakkındaki kişisel özellikleri değerlendirmek olmalıdır⁶⁹⁵. Profillemeye faaliyeti genel profillemeler, otomatik karar mekanizmalarından yararlanan profillemeler ve sadece otomatik karar mekanizmalardan oluşturulan profillemeler olmak üzere üçe ayrılabilir. Yani profillemeler yalnızca otomatik karar mekanizmaları ile oluşturulmazlar; insan müdahalesi ile de profillemeye yapılması mümkündür⁶⁹⁶.

Profillemeye faaliyeti üç aşamadan oluşur: İlk aşama gözlem aşamasıdır. Bu aşamada kişisel veya anonim veriler toplanarak bir veri ambarı oluşturulur. Veriler tanımlanabilir veya tanımlanmış bir kişiye aitse, genellikle bu aşamada anonim hale getirilir. Bir pazarlama şirketinin, alışveriş yapanların kimlikleri belirlenmeden büyük süpermarket zincirlerinin “*alışveriş sepetleri*” listesini edinmesi birinci aşamaya örnek olarak verilebilir. İkinci aşamada, belirli bir hata payı ile belirli gözlemlenebilir değişkenler arasındaki ilişkileri belirlemek amacıyla istatistiksel yöntemlerle gerçekleştiren veri madencileri bulunmaktadır. İkinci aşama faaliyeti ile benzer şekilde veri madenciliği olarak da isimlendirilmektedir. Bu aşamanın somut sonucu, bireylerin gözlemlenebilir bazı özelliklerine göre kategorize edilmesidir. Üçüncü ve son aşamada algoritma bir çıkarım elde eder. Dolayısıyla profil oluşturma faaliyeti; tanımlanmış veya tanımlanabilir bir kişiye ait verilere dayanarak, aslında o kişinin ait olduğu kategorinin verileri olan yeni verileri elde etmek için uygulanmaktadır⁶⁹⁷.

Profillemeye akabinde algoritma tarafından, kişi hakkında yeni bir kişisel veri üretilmektedir. Bu üretim çıkarım elde edilerek meydana gelir. Kişisel verilerin, doğru olup olmaması, objektif olması gibi unsurlar sınıflandırma bakımından önemli olmadığından

⁶⁹³Pap, A. L (2009) . Profiling, data mining and law enforcement: Definitions. *Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae: Sectio Iuridica*, 50, s. 278.

⁶⁹⁴ bkz. Kişisel Verileri Koruma Kurumu (2025) . *Madde ve gerekçesi ile kişisel verilerin korunması kanunu (Bilgi notu) ve kişisel verilerin korunmasına ilişkin terimler sözlüğü* (KVKK Yayınları) . Ankara, s.127.

⁶⁹⁵Article 29 Data Protection Working Party (2018,. *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, s.6-7. <https://ec.europa.eu/newsroom/article29/items/612053/en> (Erişim Tarihi: 09.06.2025) .

⁶⁹⁶ Aşıkoğlu, 2018, s.153.

⁶⁹⁷ Pap, 2009, s. 278-279.

profilleme nihayetinde gerçek kişiye ilişkin elde edilen bu çıkarımlar kişisel veri niteliğini haizdir⁶⁹⁸. Fakat bireyler, genellikle kendileri hakkında profil oluşturulduğunu bilmez ya da bilse dahi bu ifadenin ne anlama geldiğini neleri kapsadığını anlayamaz⁶⁹⁹.

Her profilleme faaliyeti otomatik bir veri işleme sürecinin sonucunu oluşturur⁷⁰⁰. Bugün e-ticaret platformları, teknoloji platformları, ve diğer hemen hemen bütün şirketler gelir elde etmek için büyük miktarda veriyi toplamakta ve analiz etmektedir. Verilerin toplanması ve analizi şirketlerin, müşterilerin profillerini çıkarmalarına yardımcı olmaktadır. Böylece kişiselleştirilmiş hizmetler sağlayabilen şirketler, daha fazla gelir elde edebilmektedir⁷⁰¹. E-ticarette kullanılan üçüncü bölüm ve ikinci kısımda açıkladığımız YZ tabanlı uygulamalarda(stok yönetimi hariç olmak üzere) profilleme faaliyeti uygulanmaktadır.

3.3.2.4.2. otomatik karar verme yasağı

Doktrinde “ilgili kişinin otomatik kararlara tabi olmama hakkı” olarak da tanımlanabilen bu yasak GDPR m.22’de şu şekilde düzenlenmiştir: “*Veri öznesinin kendisiyle ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen, profilleme de dâhil olmak üzere yalnızca otomatik işlemeye dayalı bir karara tabi olmama hakkı bulunur.*” KVKK düzenlemesinde, kararların salt algoritmalar tarafından insan müdahalesi olmadan gerçekleştirilmesine bir hukuki sonuç bağlanmamıştır. Dolayısıyla salt algoritmalar ile işlenen kişisel veriler yasak değildir ancak genel hükümlere tabidir. Bu durum KVKK’nın modern düzenlemeler ile uygun olmaması ile sunduğu çözümlerin yetersiz olması sebepleri ile eleştirilmiştir⁷⁰².

Otomatik karar verme, insan müdahalesi olmaksızın teknolojik araçlarla karar verme yeteneğidir⁷⁰³. Otomatik karar alma mekanizmaları insan faktörü bakımından profilleme tanımından ayrışır⁷⁰⁴. Bu yasak, ilgili kişinin profillemeye dahil olmak üzere otomatik karar alma mekanizmalarının varlığı, işlemede izlenen yöntem ve olası sonuçlar ile ilgili bilgilendirilmesini sağlamaktadır⁷⁰⁵.

Otomatik karar verme yasağı ilgili kişinin hukuki sonuçlar doğuran⁷⁰⁶ veya kayda değer bir şekilde(ciddi şekilde) ilgili kişiyi etkileyen algoritma kararlarında uygulanmaktadır. Veri

⁶⁹⁸ Badur, 2024, s.2538.

⁶⁹⁹ Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, revised and adopted on 06.02.2018, s.5 . <https://ec.europa.eu/newsroom/article29/items/612053/en> . Erişim Tarihi: 09.06.2025.

⁷⁰⁰ Badur, 2024, s.2537.

⁷⁰¹ Hingh, 2018, s. 1278.

⁷⁰² Büyüksağış, E (2021) . Yapay zeka karşısında kişisel verilerin korunması ve revizyon ihtiyacı. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, 18 (2), s. 532,538-539; Aksoy, H. C (2022) . Kişisel verilerin korunması yönüyle algoritmik karar verme. *Kişisel Verileri Koruma Dergisi*, 4 (2), s.83.

⁷⁰³ Article 29 Data Protection Working Party (2018, February 6) . *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (revised), s.8. <https://ec.europa.eu/newsroom/article29/items/612053/en> (Erişim tarihi: 09.06.2025)

⁷⁰⁴ Otoyollarda bulunan kameraların otomatik olarak aracın hızını hesaplayarak trafik cezası hesaplama yapması örnek olarak verilebilir. Aşıkoğlu, 2018, s.151.

⁷⁰⁵ Badur, 2024, s.2542.

⁷⁰⁶ Bu durumda ilgili kişinin yasal hakları etkilenir. Bu haklar oy kullanma, dava açma gibi haklar olabileceği gibi kişinin yasal statüsünü etkileyen sözleşmenin feshi gibi sonuçlar doğuran durumlar da olabilir. Article 29 Data Protection Working Party (2018, February 6) . *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (revised), s. 21. <https://ec.europa.eu/newsroom/article29/items/612053/en> (Erişim tarihi: 09.06.2025) .

işlemenin bir kişiyi önemli ölçüde etkilemesi için, işlemenin etkileri yeterince büyük veya önemli olmalı ve dikkate değer olması aranır. Kişisel verileri üzerinde işlem yapan yapay zeka teknolojisi hakkında bilgi alma ve itiraz etme hakkının hukuki veya önemli sonuç doğurma ön koşulu, bilgi alma hakkını önemli ölçüde engellediği gerekçesi ile doktrinde eleştirilmiştir⁷⁰⁷. İlgili kişilerin koşullarını, davranışlarını veya seçimlerini önemli ölçüde etkileyen, veri sahibine uzun süreli veya kalıcı bir etki yapan ve kişilerin dışlanmasına veya ayrımcılığa maruz kalmasına yol açan algoritmik kararlar kural olarak yasaktır. Bu durumlar ilgili kişinin ciddi şekilde etkilenmesinde koşul olarak gözetilirler⁷⁰⁸.

Teknolojideki gelişmeler ve büyük veri, yapay zeka ve makine öğrenimi yetenekleri, bireylerin hak ve özgürlüklerini önemli ölçüde etkileyebilecek profiller oluşturmayı ve otomatik kararlar almayı kolaylaştırmıştır⁷⁰⁹. Otomatik karar verme yasağı özellikle otomatik karar alma sistemine sahip olan YZ uygulamaları bakımından önem arz etmektedir. YZ sistemlerinin, ilgili kişiyi ciddi şekilde etkilediği durumlarda ilgili kişinin bu işlemeye itiraz hakkı bulunmaktadır. Özellikle, şeffaf olmayan algoritmalar sebebi ile ilgili kişiler verileri üzerindeki hakimiyetlerini kaybedebilirler. Bu durum ilgili kişinin verisi üzerindeki kontrol hakkını ihlal etmektedir. İtirazın ötesinde veri sorumlusu işlemeyi rıza olmadan gerçekleştirmiş ise kural olarak yasak olması sebebi ile hukuka aykırılık meydana gelmiş olacaktır⁷¹⁰.

Ne var ki, salt otomatik karara tabii olmama hakkı, sanıldığından daha dar kapsamlıdır. Örneğin, Ankara'nın Çiğir mahallesindeki suç işleme eğilimini gösteren bir karar alma süreci, otomatik karar alma yasağı kapsamında değildir. Nitekim, madde hükmünde ifade edildiği üzere kişiye ilişkin karar almalarında uygulanır; topluluğa veya bir grup insan için karar almalar bu sebeple koruma kapsamı dışında kalmaktadır⁷¹¹. Ayrıca, otomatik olarak alınan kararın veri öznesi ve bir veri sorumlusu arasında bir sözleşme yapılması veya söz konusu sözleşmenin uygulanması için gerekli olması, veri sorumlusunun tabi olduğu ve veri öznesinin hak ve özgürlükleri ile meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtildiği ulusal hukuk tarafından verilen yetkiye dayanması veya veri öznesinin açık rızasına dayanması halleri bu yasağın istisnalarını oluşturmaktadır. Bu hallerde kişiler hakkında profillemeye yapılabilir ve otomatik karar alınabilir.

“Kişisel verilerin işlendiği özel koşulları ve bağlamı göz önünde bulundurarak, veri öznesi ile ilgili adil ve şeffaf bir veri işleme faaliyeti gerçekleştirilmesinin temini amacıyla, veri sorumlusu, profillemeye için uygun matematiksel ve istatistikî usulleri kullanmalı, özellikle kişisel verilerde yanlışlıklara yol açan unsurların düzeltilmesini ve hata riskinin en aza indirilmesini sağlamak için uygun teknik ve kurumsal tedbirleri uygulamalı, kişisel verileri, veri öznesinin menfaatleri ve hakları bakımından ortaya çıkabilecek potansiyel riskleri göz önünde bulunduracak ve diğerlerinin yanı sıra, ırk veya etnik köken, siyasi görüş, din veya inançlar; sendika üyeliği, genetik durum veya sağlık durumu veya cinsel yönelim temeline dayanan ya da

⁷⁰⁷ Demirtaş, 2024, s.19.

⁷⁰⁸ Article 29 Data Protection Working Party (2018, February 6) . *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (revised), s.21-22. <https://ec.europa.eu/newsroom/article29/items/612053/en> (Erişim tarihi: 09.06.2025)

⁷⁰⁹ Article 29 Data Protection Working Party (2018, February 6) . *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (revised), s.5. <https://ec.europa.eu/newsroom/article29/items/612053/en> (Erişim tarihi: 09.06.2025)

⁷¹⁰ Badur, 2024, s.2541.

⁷¹¹ Demirtaş, A (2024) . ChatGBT gölgesinde kişisel verilerin korunması. *Kişisel Verileri Koruma Dergisi*, 6 (1), s.16.

böyle bir etkiye sahip tedbirlerle sonuçlanan, gerçek kişiler üzerindeki ayrımcı etkileri önleyecek bir şekilde korumalıdır(GDPR, giriş, para.71).”

YZ uygulamaları, temel hak ve özgürlükleri temel alan koruyucu yaklaşım ve gerekli teknik düzenlemeler ile otomatik karara tabii olmama hakkı ile uyumlu hale getirilebilir. Nitekim, YZ uygulamalarının hukuki sonuç doğuran veya kayda değer bir şekilde(ciddi şekilde) ilgili kişiyi etkileyen kararlar verme ihtimali yüksektir. Bu uyumun gerçekleştirilmesi için örneğin, kişiye ilişkin doğrudan bir kararın YZ tabanlı uygulama tarafından alınması talep edildiğinde bu talebin GDPR m.22 kapsamında algoritmik karara tabi olma çerçevesinde verileceği uyarısı ile bu kararın alınmasından kaçınma hakkına ilişkin etkin bir vazgeçme sistemi işletilebilir. Diğer bir olasılık, algoritmanın bu kararın neden alınması istendiğini sorgulama halidir. Bu ihtimalde algoritma, hukuki sonuç doğuran veya ilgili kişiyi ciddi şekilde etkileyen kararı almaktan çekinebilir veya verdiği kararın bağlayıcı olmaması gerektiğine vurgu yapabilir. Bu sistemlerin işletilmesi için teknik yapının oluşturulması halinde otomatik karara tabi olmama hakkı etkin şekilde korunur⁷¹².

Otomatik karar almanın meşruluğunun veri öznesi ve bir veri sorumlusu arasında bir sözleşme yapılması veya söz konusu sözleşmenin uygulanması için gerekli olması ile veri öznesinin açık rızasına dayanması hallerinde veri sorumlusu, müdahalesini temin hakkı başta olmak üzere, veri öznesinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki hak ve özgürlükleri ile meşru menfaatlerini güvence altına almak için uygun tedbirleri almakla yükümlüdür(GDPR m.22/4).

3.3.3. Yapay zeka uygulamalarında kullanıcıların(ilgili kişinin) hakları

Kişisel verilerin hukuka uygun şekilde kişisel verilerinin işlendiğinin teminatı olarak ilgili kişiye birtakım haklar tanınmıştır. GDPR m.12 ile 22 arasında ve KVKK m.11’de ilgili kişinin hakları düzenlenmiştir. Ne var ki, GDPR düzenlemesinde ilgili kişiye tanınan birtakım haklar KVKK düzenlemesine dahil edilmemiştir. Bu hususlar aşağıda detaylandırılmıştır.

E-ticaret platformlarında YZ tabanlı uygulamaları kullanan kullanıcıların veri sorumlusu olan e-ticaret şirketine başvurarak aşağıdaki haklarını kullanabilir.

3.3.3.1. Bilgi edinme hakkı

YZ uygulamalarının ve kişisel veri işleme sistemlerinin karmaşık yapısı ile ilgili kişi üzerindeki dezavantajlı etkileri karşısında ilgili kişinin kendisine ait hangi kişisel verilerin işlendiğini bilmesi büyük bir öneme sahiptir. Bu sayede ilgili kişiler, tanınan haklarını kullanabilecek ve kişisel verileri üzerinde söz sahibi olabileceklerdir⁷¹³. İlgili kişinin bilgi edinme hakkı, veri sorumlusunun aydınlatma yükümlülüğü ve müracaat ile bilgi edinme hakkı çerçevesinde iki kısımda incelenebilir⁷¹⁴.

3.3.3.1.2. Veri sorumlusunun aydınlatma yükümlülüğü

GDPR, veri sorumlusunun aydınlatma yükümlülüğüne ilişkin bir ayrıma giderek; kişisel verilerin doğrudan ilgili kişiden toplanıp toplanmamasına göre paylaşılması gereken bilgileri

⁷¹² Demirtaş, 2024, s.22.

⁷¹³Develioğlu, 2017, s. 83.

⁷¹⁴Develioğlu, 2017, s.83; Selek, 2021, s.87.

ayrı ayrı düzenlemiştir⁷¹⁵. Bu bilgiler neredeyse aynı olmakla aktarım yapılan bilgilerde aktarım yapılan şirkete ilişkin yükümlülükleri içeren eklemeler yapılmıştır.

GDPR hükümlere göre, veri sorumlusu kimlik ve irtibat bilgileri (ve varsa temsilcisinin bu bilgileri), (varsa) veri koruma görevlisinin irtibat bilgileri, kişisel verilerin işleme amaçları, işlemenin yasal dayanağı, (varsa) veri sorumlusu veya üçüncü kişi tarafından gözetilen meşru menfaatler, (varsa) kişisel verilerin alıcıları veya alıcı kategorileri hakkında bilgilendirmeyi ilgili kişiye sağlamakla yükümlüdür. Bilgilendirme metninde ayrıca, kişisel verilerin depolanacağı süre veya bunun mümkün olmaması hâlinde, bu sürenin belirlenmesi amacıyla kullanılan kriterler, veri sorumlusundan kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da kalıcı olarak silinmesini veya veri öznesi ile ilgili işlemenin kısıtlanmasını talep etme ya da işlemeye itiraz etme hakkının yanı sıra veri taşınabilirliği hakkının belirtilmelidir (GDPR m.13-14). Belirtilmelidir ki; KVKK düzenlemesinde ilgili kişinin veri taşıma hakkı düzenlenmemiştir.

İlgili kişi ayrıca rızanın geri çekilmesinden önce rızaya dayalı olarak gerçekleştirilen işlemenin hukuka uygunluğu etkilenmeksizin, her zaman rızayı geri alma hakkının varlığı; denetim makamına şikâyetle bulunma hakkı; otomatik karar almanın varlığı ve en azından bu hâllerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri öznesi açısından önemi ve öngörülen sonuçları hakkında en az veri işleme esnasında veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmesi ile bilgi sahibi olmalıdır (GDPR m.13-14).

KVKK m.10 düzenlemesine göre aydınlatma yükümlülüğü çerçevesinde kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, ilgili kişinin kanunda sayılan diğer hakları konusunda bilgi vermekle yükümlüdür.

Yapay zeka uygulamaları bakımından aydınlatma yükümlülüğüne ilişkin münhasıran belirtilmesi gereken hususlarda otomatik işlemeyi konu alan GDPR m.13/2-f hükmü dikkate alınmalıdır. Nitekim, bu maddede; profillemeye dahil olmak üzere otomatik karar almanın sistemlerinde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri öznesi açısından önemi ve öngörülen sonuçlarının ilgili kişiye bildirilmesi gerektiği belirtilmiştir. Buna göre yapay zekanın çalışma sistemi, işlenen kişisel veriler, kişisel verilerin işleme amaçları, YZ uygulamalarında işlenecek kişisel verilerin neden önemli olduğu ve işleme sonucu elde edilebilecek çıkarımlar basit ve anlaşılır bir dil ile ilgili kişiye YZ tarafından henüz kişisel veriler işlenmeden veya işleme sırasında açıklanmalıdır.

YZ tabanlı uygulamaları kullanıcılarına işlenen kişisel verilerin ilişkin açıklamaların YZ modeli merkezli, ilgili kişi merkezli, demografik yapı merkezli yaklaşımların benimsenebileceği belirtilmiştir⁷¹⁶. Kanaatimiz, YZ tabanlı uygulamalar bakımından kişisel verilerin işlenmesi hakkında ilgili kişi odaklı konu merkezli açıklamaların yapılması ile

⁷¹⁵ bkz. GDPR, m.13-14.

⁷¹⁶Edwards, L., and Veale, M (2019) . Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for. *Duke Law and Technology Review*, 16, .s.58.

uygulanan modelin işleyiş taslağının çizilmesidir. YZ uygulamalarında kişisel verilerin işlenmesine ilişkin ilgili kişiye (*kullanıcıya*) aşağıdaki bilgiler sağlanmalıdır⁷¹⁷:

- İlk olarak sistemin dikkate aldığı girdi verileri belirtilmelidir. Örneğin, bir kredi başvurusu için başvuranın geliri, cinsiyeti, varlıkları, işi vb. gibi sonuç alınması için sisteme girilen veriler. Ayrıca farklı veri öğelerinin başvuranın umduğu sonucu olumlu mu yoksa olumsuz mu etkilediği açıklanmalıdır.
- Sistemin hesaplaması gereken hedef değerler bilgilendirme metninde yer alması gereken bir diğer öğedir. Kredi değerliliği düzeyi ve muhtemelen kredinin onaylanması için ulaşılması gereken eşik değeri örnek olarak verilebilir.
- Otomatik değerlendirme/kararın öngörülen sonucu da aydınlatma metninde gösterilmelidir. Kredi başvurusunun onaylanması veya reddedilmesi gibi sistem kararları bu sonuçlara örnek olarak verilebilir.

Veri sorumlusu ilgili kişiyi bünyesinde işlenen kişisel verileri hakkında bilgilendirirken kullandığı ifadeler açık ve anlaşılır olmalı ve belirsiz ifadelerden kaçınmalıdır. “*Size daha iyi bir hizmet vermek için kişisel verilerinizi işliyoruz*” şeklinde beyan ile aydınlatma yükümlülüğünün yerine getirildiğinden bahsedilemez⁷¹⁸. Kişisel verilerin işlenmesi detayları asgari olarak GDPR ve KVKK düzenlemelerinde yer alan bilgilerin açıklanması şeklinde detaylandırılmalıdır.

Kişisel veriler ilgili kişiden doğrudan elde ediliyorsa veri sorumlusu tarafından yapılacak bildirim en geç verilerin işlenmesi sırasında yapılmalıdır. Aksi halde, veri sorumlusu, kişisel verileri elde ettikten makul bir süre veya en geç bir ay içinde ilgili kişiye sağlamakla yükümlüdür. Veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmemesi hallerinde kişisel verilerin işlenmesi hukuka aykırılık teşkil edecektir. Fakat ilgili kişi aydınlatma metninde yer alan bilgilere zaten sahipse aydınlatma yükümlülüğünün yapılması için bir gereklilikten bahsedilemeyecektir.

3.3.3.1.1. veri sorumlusuna müracaat ile ilgili kişinin bilgi edinmesi ve erişim hakkı

Erişim hakkı, ilgili kişinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme ve işlemenin var olduğu hallerde kişisel verilere erişim sağlama hakkını ifade etmektedir (GDPR m.15) . İlgili kişi, erişim hakkını kullanarak, veri sorumlusuna müracaat ile kişisel verilerinin işleme amaçları, kişisel veri kategorileri; üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri, kişisel verilerin depolanması için öngörülen süre

⁷¹⁷European Parliament (2020) . *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (Panel for the Future of Science and Technology) . Brussels, s.55.

⁷¹⁸ Selek, 2021, s.88.

veya bunun mümkün olmaması hâlinde, bu sürenin belirlenmesi amacıyla kullanılan kriterler hakkında bilgi talep edebilir.

Veri sorumlusu(e-ticaret işletmesi) ilgili kişinin talebi üzerine kişisel verilerin düzeltilmesi veya kalıcı olarak silinmesini ya da söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işlemeye itiraz etme hakkı bulunduğu, denetim makamına şikâyetle bulunma hakkını ve kullanılma usulünü; kişisel verilerin bir üçüncü ülke ya da bir uluslararası kuruluşa aktarılması durumunda, veri öznesinin aktarımla ilgili olarak alınan uygun güvenceler hususunda bilgilendirme yapar. Ayrıca, ilgili kişi kişisel verilerin kendisinden doğrudan toplanmaması halinde(yani aktarımla kişisel verilerin elde edinmesinde), bu verilerin kaynaklarına ilişkin mevcut bilgiler hakkında bilgi edinme hakkına sahiptir.

KVKK m.11 kapsamında “bilgi edinme hakkı” ise şu şekilde düzenlenmiştir:

“Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme haklarına sahiptir.”

Bilgi edinme hakkı, ilgili kişilerin hukuki haklarını kullanabilmek için gereken en temel haklarıdır. Nitekim, kişiler hangi verilerinin işlendiğini öğrendikten sonra hukuki diğer haklarını kullanabilecektir. Bilgilendirme hakkı ile bilgi edinme/erişim haklarının birbirinin mütemmim cüzü olduğunu; bir madalyonun iki yüzü olduğunu söyleyebiliriz⁷¹⁹.

Teknik olarak bilgi edinme hakkının mümkün olmaması iddiası doktrinde kabul görmemektedir⁷²⁰. Nitekim, veri sorumlularının(e-ticaret şirketleri) ilgili kişinin yukarıda verilen taleplerini karşılamak için ilgili kişiye ait tüm verileri veri tabanından tespit edebilecek donanımına sahip olması gerekmektedir⁷²¹. İlgili kişinin bilgi edinme hakkı bir kere kullanılmakla tükenmez. Kişisel verileri üzerinde hakimiyetini sürdürmek isteyen ilgili kişi aralıklarla bilgi edinme hakkını kullanarak, veri sorumlusuna müracaat edebilir⁷²². Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kişisel Verilerin Korunması Kurumu tarafından belirlenen tarifiedeki ücret alınabilir(KVKK m.13/2). OECD Rehber İlkeleri 13. maddede alınan bu ücretin aşırı olmaması ve makul olması gerektiği belirtilmiştir. Öte yandan, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ⁷²³’de ilgili kişinin veri sorumlusuna başvuru usul ve yöntemleri açıklanarak m.7’de veri sorumlusunun, ilgili kişinin başvurusuna yazılı olarak cevap vermesi halinde, on sayfaya kadar ücret almayacağı; on sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabileceği düzenlenmiştir. Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçmeyecektir.

YZ uygulamaları bağlamında bilgi edinme/erişim hakkı kapsamında dikkat edilmesi gereken husus GDPR m.15/1-h’da düzenlenen “*profilleme de dâhil olmak üzere otomatik karar almanın varlığı ve en azından bu hâllerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra*

⁷¹⁹ Selek, 2021, s.87.

⁷²⁰ Demirtaş, 2024, s.17.

⁷²¹ Aygözer Öngün, 2019, s.206.

⁷²² Akgül, 2014, s.142.

⁷²³ R.G. 10.03.2018 T. ve 30356 S.

söz konusu işlemenin veri öznesi açısından önemi ve öngörülen sonuçları” hakkında ilgili kişinin bilgi edinme hakkıdır. Ne var ki, ilgili kişiye gerçekleştirilecek sistemde yürütülen mantığa ilişkin açıklama kapsamında belirtilmelidir ki; yaygın olarak kullanılan ve isabetli sonuçlar verebilen, yapay sinir ağlarına tekniği kullanan YZ uygulamaları kara kutu (black box) mantığıyla çalışmakta ve karar alma süreçleri tam olarak açıklanamamaktadır. Teknik imkansızlık sebebi ile ilgili kişiye yapılacak bilgilendirmenin en ufak detaylarına kadar tüm mekanizmaları içerecek şekilde yapılması gerekli değildir⁷²⁴. Doktrinde, çözüm olarak ilgili kişinin makine öğrenmesi ile işlenen kişisel verilerine ilişkin talebine eğer veri sorumlusu tarafından geçerli bir hukuki sebebe dayanılarak tutulmaya devam ediliyorsa verinin orijinal haline erişim sağlanarak; eğer böyle bir durum yoksa hangi kişisel verilerinin modele girdi olarak verildiğine yönelik bir açıklamayla cevap verilebileceği belirtilmiştir⁷²⁵.

Kanaatimiz, YZ teknolojinin kullanıldığı hakkında ilgili kişinin bilgilendirilmesinin yeterli olmadığı, her ne kadar sistemin tam olarak açıklanması mümkün değilse de uygulanan modelin genel işleyiş taslağının çizilerek, kullanılan YZ tekniklerinin açıklanması ve bu model için hangi kişisel verilerin kullanıldığını ve çıktı olarak alınabilecek diğer kişisel verilere ilişkin açıklamalarda bulunması gerektiği yönündedir.

E-ticaret platformları kullanıcılarının bilgi edinme haklarını kullanmaları için gerekli sistemsel araçları sağlamakla yükümlüdür. Müşterilerin toplanan ve kullanılan kişisel verileri hakkında bilgi sahibi olmaları en az işlenmeleri kadar kolay hale getirilmelidir. Nitekim bilgi edinme hakkı, kişisel verilerin korunması hakkının gerçekleşebilmesi için bir önkoşul niteliğindedir.

3.3.3.3. Kişisel verilerin düzeltilmesini isteme hakkı

E-ticaret kullanıcılarının kendileriyle ilgili doğru olmayan veya eksik olan kişisel verilerin fazla gecikmeksizin düzeltilmesini söz konusu e-ticaret şirketinden talep etme hakları bulunmaktadır (GDPR m.16; KVKK m.11/1-d)). Ayrıca işleme amaçları dikkate alınarak, ilgili kişinin(kullanıcının), ek beyan yoluyla yapılması da dahil olmak üzere, eksik kişisel verileri tamamlama hakkı bulunur(GDPR m.16). Kişisel verilerin düzeltilmesi hakkı, bilgi alma hakkının bir uzantısıdır. Kişisel verilerin üçüncü kişilere aktarılması durumunda, düzeltilme taleplerinin bu kişilere bildirilmesi e-ticaret şirketi veri sorumlusunun yükümlülüğüdür⁷²⁶.

Yapay zeka bağlamında kişisel verilerin düzeltilmesi hakkının yararlı olduğu düşüncesindeyiz. Nitekim, ancak tam ve doğru bilgilerle YZ uygulamalarının sağlıklı ve tatminkar sonuçlar elde edilebilir. Ve böylece YZ kullanılan uygulamalar amaçlarına ulaşılabilir. Bu cihetle, ilgili kişinin kişisel verilerinin düzeltilmesini talep hakkı YZ tabanlı uygulamalarının amaçlarını gerçekleştirmelerine ve YZ'nın geliştirilmesine hizmet eder niteliktedir. Ne var ki, bizim görüşümüz YZ uygulamalarına girdi olarak işlenene kişisel veriler hakkındadır. Diğer yandan doğru ve güncel verilerin YZ tabanlı uygulamalara girdi olarak işlenmesi ile kişiler(kullanıcılar) hakkında ortaya çıkarılan bilginin (çıktı/karar) düzeltilmesinin istenmesi YZ modelinin tekrar oluşturulması anlamına geleceğinden düzeltilme talebinin reddedilmesi gerektiği yönünde görüş bulunmaktadır⁷²⁷.

⁷²⁴ Güçlütürk, 2022, s.332.

⁷²⁵ Güçlütürk, 2022, s.333.

⁷²⁶ Aygözer Öngün, 2019, s.212.

⁷²⁷ Güçlütürk, 2022,, s.335.

3.3.3.4. Kişisel verilerin silinmesini ve yok edilmesini (unutulma hakkı) isteme hakkı

Kişisel verilerin silinmesi, “*kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi*”; yok edilmesi, “*kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi*” ve son olarak anonim hale getirilmesi, “*kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemi*” olarak tanımlanmaktadır⁷²⁸.

İlgili kişinin e-ticaret platformlarınca işlenen kişisel verilerinin, işleme hukuka uygun olarak gerçekleşmiş olsa dahi, silinmesini isteme hakları bulunmaktadır (KVKK m.11/1-e). Öyle ki, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu e-ticaret şirketi tarafından silinir, yok edilir veya anonim hâle getirilir (KVKK m.7/1). Veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer. Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlü tutulmuştur. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır⁷²⁹. Veri sorumlusu bu işlemleri gerçekleştirirken kişisel verilerin işlenmesi ilkelerine uygun hareket etmek ve gerekli idari ve teknik tedbirleri⁷³⁰ almakla yükümlüdür.

Kişisel verilerin silinmesi (right to erasure) ve unutulma hakkı(right to be forgotten) GDPR m.17’de düzenlenmiştir. Kişisel verilerin işlenme amaçlarının ortadan kalkması sebebi KVKK ile paralellik göstermektedir. Ayrıca ilgili kişi tarafından verilen rızanın geri çekilmesinde işlemeye ilgili başka bir hukuki dayanak bulunmaması durumunda kişisel veriler veri sorumlusu veri tabanından imha edilmelidir. Yasal bir yükümlülüğün bulunması, ilgili kişinin itiraz etmesi veya kişisel verilerin hukuka aykırı biçimde işlenmiş olması hallerinde de kişisel veriler silinmelidir. Son olarak, bir çocuğa bilgi toplumu hizmeti sunulması amacıyla kişisel verilerin işlenmesi durumunda; talep halinde bu verilerin silinmesi gerekmektedir.

Unutulma hakkı, esasen 2014 yılında ABAD(Avrupa Birliği Adalet Divanı) Google/İspanya kararında ortaya çıkmıştır⁷³¹. Bu kararın ardından unutulma hakkı GDPR

⁷²⁸ bkz. 28.10.2017 tarih ve 30224 sayılı Resmi Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m.8, m.9 ve m.10.

⁷²⁹ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m.7.

⁷³⁰ İlgili İdari ve Teknik Tedbirler için bkz. KVKK m.12.

⁷³¹ 13.05.2014 tarihli İspanya vatandaşı Mario Costeja Gonzales’in evinin evinin 1998’de cebri icra yoluyla açık artırmaya çıkarıldığına dair bir gazete ilanının kişilik hakkını ihlal etmesi sebebi ile 2010 yılında İspanyol Ulusal Veri Koruması Otoritesi’ne başvurması akabinde arama motorunun veri sorumlusu olup olmayacağına ilişkin sorulan görüşte, ABAD 13.05.2014 tarihinde google arama motorunun veri sorumlusu olduğunu tespit etmiştir. AB yaklaşımı, örneğin arama motorlarında kişisel verileri uzun süre tutulması karşısında bireylerin lehine karar verdikleri gözlemlenmektedir. Örneğin: ABAD (Avrupa Birliği Adalet Divanı) (2014) . *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12) . İngilizce tam metin için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131> (Erişim tarihi: 22.03.2025) . Kararın Türkçe Çevirisi için bkz. Kaya, M. B (2015) . Avrupa Birliği Adalet Divanı’nın 13 Mayıs 2014 tarihli Google unutulma hakkı kararı çevirisi. <https://dergipark.org.tr/en/download/article-file/1671800> (Erişim tarihi: 22.03.2025) . Daha detaylı bilgi için bkz. Akgül, A (2016) . Kişisel verilerin korunmasında yeni

düzenlemesine eklenmiştir. Unutulma hakkının çevrimiçi platformlarda değerlendirilmesi bakımından Google/İspanya kararında bireylerin arama motorlarında kendileri ile ilgili yer alan bazı linklerin belirli şartlar altında kaldırılmasını talep edebileceğine işaret edildiğinin ve unutulma hakkının mutlak olmadığını vurgulandığının belirtilmesinde fayda vardır. Nitekim bu kararda, unutulma hakkına özellikle diğer temel haklar (örneğin ifade özgürlüğü, basın özgürlüğü) karşısında oluşacak menfaatler dengesi temelinde bir değerlendirme yoluyla yer verilebileceğine özellikle işaret etmiştir. Dolayısıyla, unutulma hakkının uygulanmasında kişisel verilerin korunması, ifade hakkı ve basın özgürlüğü arasındaki dengenin iyi kurulması gerekmektedir⁷³².

GDPR düzenlemesinde yer alan “Unutulma Hakkı” ile KVKK düzenlemesinde yer alan “Silinme Hakkı” arasındaki fark verinin geri alınıp alınmaması meselesidir. Nitekim, GDPR düzenlemesi yalnızca veri sorumlusunun veriyi silmesini öngörmemekte aynı zamanda verinin yayıldığı diğer veri sorumlularının da aynı şekilde davranmasını sağlamak için harekete geçmesi gerektiğini öngörmektedir. Nitekim, unutulma hakkı aynı zamanda kişisel verilerin üçüncü kişilere aktarılması durumlarında bu kişilere e-ticaret şirketi olan veri sorumlusu tarafından bildirim yapılması yükümlülüğünü de içermektedir. Bu sayede kişiye gerçekten bir unutulma hakkı tanınmaktadır⁷³³. Veri sorumlusu, mevcut teknoloji ve mevcut araçları dikkate alarak alacağı teknik tedbirler ile birlikte unutulma hakkının tam olarak kullanıldığının güvencesini vermelidir(GDPR, *giriş*, para.66).

YZ uygulamaları bakımından silinme ve unutulma hakkına bakıldığında iki sonuç ile karşılaşılacaktır: YZ uygulamalarının eğitilmesi için eğitim setlerin katılan kişisel verilerin işlenmesi ve YZ çıktısının kişisel veri ihtiva etmesi hali. Kişisel verilerin eğitim setlerine katılması ile kişi ile doğrudan ilişkisinin kurulmaması durumlarında⁷³⁴ ilgili kişinin çıkarlarının doğrudan etkilendiğinden bahsedilemeyeceği için silinme talebinin diğer durum ve koşullar da değerlendirilerek reddedilmesi kanaatindeyiz. Yapay zeka çıktısı olarak yine kişi ile doğrudan ilişki kurulamayacak şekilde ”25-30 yaş grubu erkekler, sağlıklı atıştırma grubundan fıstık ezmesini tercih ediyor.” gibi bir çıkarım kişisel veri olarak kabul edilemeyeceği için ilgilinin silinme talebi bu verinin YZ algoritmasından silinmesini gerektirmeyecektir⁷³⁵. Fakat, anonim verilerin, yeni sistemlerle yeniden kimliklendirilebilir hale gelmesi halinde ne yapılacağı belirsizdir. Bu gibi hallerde modelin silinmesiyle beraber kullanılması gerektiği için orantısız bir müdahale olabilecektir⁷³⁶. Kişisel verilerin YZ uygulamalarına girdi olarak henüz dahil edilmediği durumlarda unutulma ve kişisel verilerin silinmesi hakları uygulanmalıdır.

bir hak: Unutulma hakkı ve AB Adalet Divanı’nın Google kararı. *Türkiye Barolar Birliği Dergisi*, (116), 27–32.; Başalp, 2015, 99-101.

⁷³² Aygözer Öngün, 2019, s.212. Unutulma hakkı ile zihinlerde kişinin kriminal geçmişinden aklanması gibi bir olgu husule gelse de, bu hak teknolojinin gelişmesi ile günümüzde farklı bir anlam daha kazanmıştır. Kişinin bir defa ortaya çıkartılmış başka bir deyişle ifşa edilmiş verilerinin tekrar gündeme getirilmesinde ilgili kişinin menfaatinin bulunmamasından hareketle, kişiye unutulma hakkı ile kişisel verilerinin unutulmasını isteme ve bundan doğan zarar veya doğabilecek olası zarardan kaçınma hakkı tanınmıştır. Aygözer Öngün, 2019, s.46.

⁷³³ Develioğlu, 2017, s.91-93; Aygözer Öngün, 2019, s.212.

⁷³⁴ European Parliament (2020) . *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (Panel for the Future of Science and Technology) . Brussels, s.50.

⁷³⁵ Atalan, 2024, s.81.

⁷³⁶ Atalan, 2024, s.118; Güçlütürk, 2022, s.337.

3.3.3.5. Veri taşınabilirliği hakkı

GDPR m.20’de düzenlenen “*Veri Taşınabilirliği Hakkı*” (“*right to data portability*”) KVKK düzenlemesinde bulunmamaktadır. Bu hak uyarınca, ilgili kişinin(kullanıcı) kendisi ile ilgili olarak bir veri sorumlusuna sağladığı kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı ve bu verileri başka bir veri sorumlusuna iletme hakkı bulunmaktadır. E-ticaret şirketi olan veri sorumlusu bu konuda hiçbir zorluk çıkartamaz. Dünya düzeninin elektronik ortamda devam ettiği ve internette yaşandığı günümüz dünyasında bu hak ilgili kişilere kolaylık sağlamaktadır. Bu hakkın kullanılması, başkalarının hak ve özgürlüklerini olumsuz yönde etkilememelidir. İlgili kişinin veri taşınabilirliği hakkı; kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması için gereken işlemlere uygulanamaz.

3.3.3.6. İtiraz hakkı

İlgili kişinin itiraz hakkı GDPR m.21’de düzenlenmiştir. Buna göre; verisi işlenen kişilerin her zaman itiraz hakları bulunmaktadır. Bu itirazdan sonra veri sorumlusu veri öznesinin menfaatleri, hakları ve özgürlüklerine veya hak taleplerinin oluşturulması, hakkın yerine getirilmesi veya savunulmasına ağır basan zorlayıcı meşru bir dayanak göstermediği sürece artık kişisel verileri işleyemez hale gelir(GDPR m.21/1). Bununla birlikte, kişisel verilerin, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlenmesi durumunda, işleme kamu yararı sebebiyle gerçekleştirilen bir görevin yürütülmesi için gerekli olmadığı sürece, veri öznesinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, kendisi ile ilgili kişisel verilerin işlenmesine itiraz hakkı bulunmaktadır(GDPR m.21/6). Kişiler(kullanıcılar) kişisel verilerinin işlenmesine itiraz edilebileceği hakkında en geç veri sorumlusu ile ilk iletişime geçtikleri anda bilgilendirilir. Bu bilgi diğer bilgilerden açık ve ayrı bir şekilde sunulmalıdır(GDPR m.21/4).

Pazarlama alanında özel bir düzenleme öngörülmüştür. Buna göre, ilgili kişinin pazarlama amaçlarına yönelik işlemeye her zaman itiraz edebilir ve itirazın gerçekleşmesi halinde, veri sorumlusu bu verileri artık pazarlama amacıyla işlemeye devam edemez (GDPR m.21/3). GDPR hükmünde profil çıkarma işleminde de itiraz edilebileceği ayrıca ve açık şekilde vurgulanmıştır. Buna göre, e-ticaret alanında müşterilerin kişisel verilerinin işlenerek pazarlama amacıyla profillemeye yapılması halinde müşteriler ilgili işlemeye itiraz edebilir. Ve bu itirazdan sonra veri sorumlusu veri işlemeye devam edemez.

YZ tabanlı uygulamaların verdiği kararlara ilişkin ilgili kişi tarafından yapılan itirazlar sonucunda veri sorumlusunca izlenecek yol şu şekildedir: ilgili kişisel verinin münhasıran otomatik sistemleri barındırmayan bir şekilde yeniden işlenmesi ve ilgili kişi hakkındaki kararın yeniden insan müdahalesi ile gözden geçirilmelidir⁷³⁷. Örneğin münhasıran otomatik ve makine öğrenmesi destekli sistemlerle verilen kredi başvurusu kararının gerçek kişilerin de dahil olduğu bir süreçle tekrar değerlendirilmesi gerekmektedir. Ancak bu işlemin maaliyeti kimi zaman çok büyük olabilmektedir. İnsan tabiatından doğan hata payı da burada gözetilmelidir. Eğer modelin karar verme mekanizması açıklanamıyor ise bu durumda nasıl bir yol izleneceği de belirsizdir⁷³⁸.

⁷³⁷ Güçlütürk, 2022, s.337; Demirtaş, 2024, s.16.

⁷³⁸ Güçlütürk, 2022, s.337.

3.3.3.6. İşlemeyi kısıtlama hakkı

GDPR m.18’de düzenlenen “İşlemeyi Kısıtlama Hakkı” (“right to restriction of processing”) KVKK düzenlemesinde bulunmamaktadır. Bu hak kapsamında ilgili kişi veri sorumlusundan verilerinin işlenmesinin kısıtlanmasını talep edebilir. İşlemenin kısıtlanması, depolanan kişisel verilerin gelecekte işlenmelerinin sınırlandırılması amacıyla işaretlenmesini ifade etmektedir(GDPR m.4/3). Yani, ilgili kişinin talebi üzerine işlenmesinin kısıtlanmasına karar verilerek işaretlenen veriler, bir süre işlenemeyecek, kaderleri tayin olunduğunda karar göre hareket edilecektir⁷³⁹.

İlgili kişilerin kişisel verilerinin doğruluğuna veya güncelliğine itiraz ettiği hallerde, veri sorumlusunun kişisel verilerin doğruluğunu teyit etmesine imkân veren sürede kişisel verilerin işlenmesi kısıtlanacaktır. Kişisel verilerin işlenmesine bir itirazın gerçekleşmesi halinde, veri sorumlusunun meşru gerekçelerinin veri öznesinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar ilgili kişi işlemenin kısıtlanmasını talep edebilir.

Kişisel verilerin işlenmesinin hukuka aykırı olması halinde de işlemeyi kısıtlama argümanından yararlanabilecektir. Bunun için ilgili kişi kişisel verilerin kalıcı olarak silinme yerine kişisel verilerinin kullanımının kısıtlanmasını talep etmelidir. Kimi zaman veri sorumlusunun işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaz ancak ilgili kişinin bazı talepleri, hakkının yerine getirilmesi veya savunulması amacıyla söz konusu verileri veri sorumlusu bünyesinde tutulmasına ihtiyaç duyabilir. Bu durumda kişisel verilerin kısıtlanmasını talep edebilir. Kişisel verilerinin işlenmesine kısıtlama getirilen ilgili kişilere, işlemeye ilişkin kısıtlama kaldırılmadan önce veri sorumlusu tarafından bilgi verilir.

3.3.3.7. Zararının tazmin edilmesini talep hakkı

Veri sorumlusu, veri işlemeye ilişkin mevzuatta belirtilen veri toplama, işleme ve aktarmaya ilişkin tüm ilkelere uyum sağlanmasında ve ilgili diğer yükümlülüklerin muhatabı olmasının yanı sıra müracaat mercii ve meydana gelen zararların sorumlusudur⁷⁴⁰. Veri sorumlusu veya veri işleyen, kişisel verileri işleme faaliyetinin sonucunda çıkan zararı tazmin etmelidir. Bu bakımdan zarara uğrayan ilgili kişinin zararının giderilmesini talep etme hakkı bulunmaktadır(KVKK m.11/1-ğ; GDPR m.82).

GDPR, kişisel verilerinin korunması hakkı ihlal edilen ilgili kişilerin bundan doğan zararlarını veri sorumlusu veya veri işleyenden alabileceğini düzenlemiştir(GDPR, m. 82/1).

“Veri sorumluları veya veri işleyenler aynı işleme faaliyetine dâhil olduklarında, her veri sorumlusu veya veri işleyen zararın tamamından sorumlu tutulmalıdır. Tam tazminat ödemiş olan herhangi bir veri sorumlusu veya veri işleyen daha sonra, aynı işlemde yer alan diğer veri sorumluları veya veri işleyenler aleyhine rücu davası açabilir. Veri sorumlusu veya veri işleyen ilgili kişinin kişisel verilerinin işlenmesinden doğan zararından hiçbir şekilde sorumlu olmadıklarını kanıtlamaları halinde zararı gidermekten kurtulur”(GDPR, giriş, para.146).

Kişisel verilerinin korunması ihlal edilen ve bu cihetle kişilik hakkı ihlal edilen kişiler, maddi ve manevi olarak zarara uğramaktadır⁷⁴¹. Türk hukuku bakımından bir değerlendirme

⁷³⁹ Develioğlu, 2017, s.93.

⁷⁴⁰ KVKK Gereğesi, m.3; Memiş, 2017, s.10-13. Ayrıca bkz. Memiş, T (2017) . Veri sorumlusu ve veri işleyen arasındaki ilişkiler ve sorumluluk düzeni. *Beykent Üniversitesi Hukuk Fakültesi Dergisi*, 3 (6), 9–23.

⁷⁴¹ Aksoy, 2010, s.2.

yapılacaktır. 6098 Sayılı Türk Borçlar Kanunu⁷⁴² da kişilik hakkı ihlal edilen kişinin manevi tazminat talep edebileceğini hüküm altına almıştır(m.58). Kişi malvarlığında eksilme ile maddi(TBK m.49 vd), duyduğu derin elem ve keder karşısında manevi tazminat açabileceği gibi(TBK m.56-58), ilgili kişinin elde edemeyeceği bir kazancın kişisel verilerin korunması hakkını ihlal eden tarafından elde edilmesi halinde saldırıdan elde edilen kazancın verilmesi davası açabilecektir⁷⁴³.

GDPR, veri sorumlusu ve veri işleyen arasındaki sorumluluğun düzenlenmesini esas olarak devletlerin iç hukuk düzenlemelerine bırakmıştır. Kanun'da ise tedbirlerin alınması hususunda veri sorumlusunun ve veri işleyenin müştereken sorumlu olduğu düzenlenmiştir(KVKK m.12/2). Zararın giderilmesinde ise; veri sorumlusu ihlal oluşturan işlemenin sebep olduğu zarardan doğrudan sorumlu olmakla birlikte veri işleyen, kendi yükümlülüklerini yerine getirmemesi halinde zarardan sorumlu olacaktır.

Türkiye'de bulunan bir veri sorumlusunun veya veri işleyenin gerçekleştirdiği kişisel verileri işleme faaliyetinin, AB'de ikamet eden gerçek kişilere mal veya hizmet sağlaması ile AB sınırları içinde davranışların gözlemlenmesine ilişkin kişisel veri işleme faaliyetinin olması durumunda, veri sorumlusu ve/veya veri işleyen konumunda bulunan Şirketler, hem GDPR hükümlerine hem de KVKK hükümlerine uyum sağlamalıdır. Fakat, zaten, GDPR hükümlerine uyum sağlayan bir Şirket zaten KVKK hükümlerine uygun hareket etmiş olacaktır. Nitekim, GDPR düzenlemesi KVKK'ya göre çok daha geniş kapsamlı olmakla birlikte çok daha fazla hak öngörülmüş ve veri sorumlusu ile veri işleyene daha fazla sorumluluk yüklemiştir⁷⁴⁴.

3.3.4. E-ticaret işletmesi tarafından alınacak idari ve teknik tedbirler

Kişisel verilerin korunmasına yönelik uygun teknik ve kurumsal tedbirleri uygulamak ve tedbirleri günün ihtiyaçlarına göre gözden geçirip güncellemek veri sorumlusunun yükümlülüğüdür (GDPR, m. 24/1; KVKK m.12/1-c). Söz konusu tedbirler veri güvenliğinin sağlanması bakımından önemlidir.

Veri sorumluları, teknolojik gelişmeleri göz önüne alarak; işlemenin gerçek kişilerin hak ve özgürlüklere yönelik, değişen olasılık ve ağırlıktaki riskleri dikkate alarak, uygun teknik ve kurumsal tedbirleri hem işleme yönteminin belirlenmesi hem de işleme esnasında uygulamak ve veri öznelinin haklarını korumakla yükümlüdür(GDPR m.25/1). Şirketlerin veri güvenliği sağlama yükümlülüğü kişisel verilerin korunmaso hukukunun tamamlayıcı unsurlarından birini oluşturmaktadır. Nitekim, Kişisel Verileri Korum Kurumu da veri güvenliğine ilişkin şikayetlerde caydırıcı kararlar vermektedir. Nitekim, bir hazır giyim e-ticaret şirketinde kayıtlı olan müşteriye ilişkin kişisel verilerin sistem arızasından kaynaklı olarak verilerin başka müşterilere görünür olması olayında veri sorumlusu şirket veri güvenliğini sağlamada kusurlu bulunmuş ve hakkında idari para cezası yaptırım uygulanmıştır⁷⁴⁵. Burada önemli olan mesele,

⁷⁴² R.G. 04.02.2011 T. ve 27836 S.

⁷⁴³ Aksoy, 2010, 90,97. Kişisel verilerin hukuka aykırı şekilde işlenmesi yani toplanması, kullanılması, paylaşılması hallerinde kar mevcut ise gerçekolmayan vekaletsiz iş görme hükümleri çerçevesinde bu karın ilgili kişi tarafından taleo edilmesi mümkündür. Ayrıntılı bilgi için bkz. Aksoy, 2010, 80 vd. , 98.

⁷⁴⁴ Develioğlu, 2017, s. 20.

⁷⁴⁵ Kişisel Verileri Koruma Kurulu (2018, 26 Temmuz). “*Kişisel verilere hukuka aykırı erişilmesini önleme*” yükümlülüğünü yerine getiremeyen veri sorumlusu hakkında Kurul Kararı No. 2018/91. Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/5365/2018-91> (Erişim Tarihi: 26.07.2025).

bahse konu şirketin ihlali fark etmesinden sonra gerekli tüm tedbirleri almış olmasına rağmen kusurlu bulunmasıdır. Nitekim, veri güvenliğinin sağlanmasında ver sorumluları çok geniş bir risk sorumluluğu kapsamında değerlendirilmektedir. Bu durum; Kişisel Verilerin Korunması Hakkı'nının ihlal edilmesinin genellikle klasik hukuk sisteminde karşılaşılan tarzda bir zarar ve mağduriyet yaratmıyor olmasından kaynaklanmaktadır⁷⁴⁶.

Veri güvenliği yükümlülüğü kapsamında, YZ uygulamaları varsayılan ayarlar gizliliği koruyacak şekilde yapılandırılarak(data protection by default); uygulamanın tasarlanması sırasında temel hak ve özgürlükler dikkate alınmalı ve kişisel verilerin toplanması aşamasından önce sistemin işleyici kişisel verilerin korunması mevzuatına uygun hale getirilmelidir. Böylece ilgili kişilerin sistemden kaynaklanabilecek ihlallere karşı başlangıçtan itibaren korunması sağlanabilmektedir (GDPR m.25).

Kişisel verilerin korunmasına ilişkin şirketler ve işletmelerce alınacak idari ve teknik tedbirler kapsamında GDPR ve KVKK düzenlemelerinin yanı sıra Kişisel Verilerin Korunması Kurumu'nun yayınlarından biri olan "*Kişisel Veri Güvenliği Rehberi(İdari ve Teknik Tedbirler)*"⁷⁴⁷ dikkate alınmalıdır. Bu rehberde temin edilmesi istenen veri güvenliği iki ayrı başlık altında incelenmiştir. Bunlar; idari ve teknik tedbirlerdir⁷⁴⁸.

İdari tedbirler kapsamında şirketler ve işletmeler öncelikle organizasyonel bağlamda mevcut risk ve tehditlerin belirlenmesi yapmalıdır. Bu kapsamda öncelikle işlenen kişisel verilerin tespiti yapılır (kişisel veri envanteri hazırlanır) ardından bu verilerin özel nitelikli kişisel veri olup olmadığı değerlendirilerek niteliği itibari ile gereksinim duyduğu gizlilik seviyesi belirlenir. Güvenlik ihlali hallerinde kişinin olası zararı ve risklerin meydana gelme olasılığı hesaplanarak (risk analizinin yapılması) uygun tedbirler belirlenerek uygulanır. Bunun yanı sıra çalışanların kişisel veriler ve yapay zeka alanlarında eğitimlerini gerçekleştirerek; kişisel verilerin korunması ve yapay zeka sistemlerinin anlaşılabilmesi için bu alanlardaki okuryazarlığı sağlamalı ve teşvik etmelidir. Bu eğitim siber saldırılara karşı ilk müdahaleyi de içermelidir. Ayrıca Şirket içi kişisel verilere ilişkin gizlilik sözleşmeleri yapılmalıdır. Kişisel verilerin güvenliği politikalarını insan haklarını temel alan bir yaklaşımla oluşturmalı ve bu sayede risklerin istikrarlı şekilde önlenmesi sağlanmalıdır. Söz konusu politikalara ilişkin şirket içi doğru ve tutarlı prosedürler hayata geçirilmelidir. *Veri minimizasyonu ilkesi* uyarınca amaca hizmet etmeyen kişisel verilerin işlenmesi mümkün olduğunca azaltılmalıdır. Kurum içi düzenli ve rastgele denetimler ile kişisel verilerin korunması mevzuatına uyum denetlenmelidir⁷⁴⁹.

Yapay zeka uygulamaları bağlamında kişisel verilerin korunmasına ilişkin teknik tedbirlerin sağlanması ancak bu alanda uzman kişilerce gerçekleştirilebilir. Teknik tedbirler, idari tedbirlerde olduğu gibi insan haklarını temel alan bir yaklaşımla gerçekleştirilmelidir.

⁷⁴⁶ Dülger, M. V (2021). *Tasarlanmış ve önceden tanımlanmış veri koruma ile zarara karşı risk sorumluluğu: Kişisel Verileri Koruma Kurulu'nun 18 Şubat 2019 tarihli kararları ne anlama geliyor?* SSRN, s.7 <https://doi.org/10.2139/ssrn.3792301>.

⁷⁴⁷ Kişisel Verileri Koruma Kurumu (2018). *Kişisel veri güvenliği rehberi: Teknik ve idari tedbirler*. Kişisel Verileri Koruma Kurumu Yayınları. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (Erişim Tarihi: 26.07.2025) .

⁷⁴⁸ Konunun değerlendirmesi için ayrıca bkz. Yürük, Z (2023). Veri sorumlusunun veri güvenliğine ilişkin idari ve teknik tedbirleri alma yükümlülüğü. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 22 (48), 899–920. <https://doi.org/10.46928/iticusbe.1218693> .

⁷⁴⁹ Kişisel Verileri Koruma Kurumu (2018). *Kişisel veri güvenliği rehberi: Teknik ve idari tedbirler*. Kişisel Verileri Koruma Kurumu Yayınları, s.7-12, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (Erişim Tarihi: 26.07.2025) .

Teknik tedbirler kapsamında verilerin korunması için kişisel verilere ilişkin muhtemel siber saldırılar karşısında iyi yapılandırılmış bir güvenlik duvarı ile siber güvenliğin sağlanması ilk adımdır. Kişisel verileri içeren ortamların güvenliğinin sağlanması, bu verilere erişimin sınırlandırılması (erişim yetkisi tanınarak, yetkili kişilere kullanıcı adı ve şifre tanımlanmalıdır); söz konusu verilerin güvenliğinin sürekli takibinin yapılması şirket ve işletmelerce teknik kapsamda alınacak tedbirler kapsamındadır⁷⁵⁰.

Özel nitelikli kişisel verilere ilişkin Kişisel Verilerin Korunması Kurumu'na belirlenen yeterli önlemlerin alınması (KVKK m.6/4) yükümlülüğü Şirket ve işletmelerin idari ve teknik tedbir yükümlülüğü kapsamında ayrıca gözetilmelidir⁷⁵¹. Nitekim, Kurum 31/01/2018 tarihli ve 2018/10 sayılı kararında yeterli önlemlerin neler olduğunu detaylı şekilde açıklamıştır. Bu karara göre yeterli önlemler; özel nitelikli kişisel verilere ilişkin ayrı bir politika ve prosedür belirlenmesi yükümlülüğü; çalışanlara yönelik konu ile ilgili eğitimlerin yanı sıra gizlilik sözleşmesi, erişimin ve yetki sınırlandırılması; verilerin muhafaza edildiği ortam için kriptografik yöntemlerin kullanılması, işlemlerin güvenli şekilde loglanması, iki aşamalı kimlik doğrulaması gibi teknik tedbirler uygulanmalıdır. Ayrıca fiziksel ortama ilişkin güvenlik tedbirleri ve özel nitelikli verilerin aktarımında şifreleme ve kriptografik yöntemlerin kullanılmalıdır⁷⁵².

25 Eylül 2024'te imzalanan AB Yapay Zeka Paketi, şirketleri üç temel yükümlülük altına sokmaktadır: Yapay Zeka Yasası'na uyum sağlamak ve yönetim stratejisi benimsemek, yüksek riskli sistemleri tespit ederek haritalamak ve çalışanlar arasında yapay zeka farkındalığını artırmak⁷⁵³. Böylece teknolojinin faydalarından yararlanarak ekonomik büyüme hedeflense de kişi hak ve özgürlükleri güvence altına alınmaya çalışılmıştır⁷⁵⁴. Yapay zeka teknolojilerinden optimum verim alınabilmesi sürekli ve güncel veriler ile eğitilmesine bağlıdır⁷⁵⁵.

Yapay zeka teknolojisinin karmaşıklığı ve bu teknolojinin her geçen gün gelişmesi karşısında kişisel verilerin bu sistemlerde nasıl korunacağı meselesi gündeme gelmiştir. Norveç Veri Koruma Otoritesi tarafından bu kapsamda YZ sistemlerine ilişkin öneriler sunan Ocak 2018'de yayımlanan raporda⁷⁵⁶, yapay zeka teknikleri ve teknolojisi kişisel verilerin korunması bağlamında ele alınarak değerlendirilmiştir. Nihayetten kişisel veri mahremiyetine önem veren yapay zeka tabanlı sistemlerin teknik alt yapıları hakkında çözüm önerileri getirilmiş ve YZ

⁷⁵⁰ Kişisel Verileri Koruma Kurumu (2018). *Kişisel veri güvenliği rehberi: Teknik ve idari tedbirler*. Kişisel Verileri Koruma Kurumu Yayınları, s.16-24, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (Erişim Tarihi: 26.07.2025).

⁷⁵¹ Kişisel Verileri Koruma Kurulu (2018, 31 Ocak). "Özel nitelikli kişisel verilerin işlenmesinde veri sorumluları tarafından alınması gereken yeterli önlemler" hakkında Kurul Kararı No. 2018/10. Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/4110/2018-10> (Erişim Tarihi: 26.07.2025).

⁷⁵² Detaylı bilgi için bkz. Kişisel Verileri Koruma Kurulu (2018, 31 Ocak). "Özel nitelikli kişisel verilerin işlenmesinde veri sorumluları tarafından alınması gereken yeterli önlemler" hakkında Kurul Kararı No. 2018/10. Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/4110/2018-10> (Erişim Tarihi: 26.07.2025).

⁷⁵³ European Commission. *What is the AI Pact?* <https://digital-strategy.ec.europa.eu/en/policies/ai-pact#ecl-inpage-What-is-the-AI-Pact?> (Erişim Tarihi: 22.05.2025).

⁷⁵⁴ European Commission (2018, April 25). *Artificial intelligence for Europe* (COM (2018) 237 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Erişim Tarihi: 20.05.2025).

⁷⁵⁵ Demirtaş, 2024, s.17.

⁷⁵⁶ The Norwegian Data Protection Authority Committee (2018). *Artificial intelligence and privacy report*. Norwegian Data Protection Authority.

uygulamalarını geliştiren teknolojinin aynı zamanda bu uygulamaların getirdiği risk ve ihlallerin üstesinden gelmede yardımcı olabileceği belirtilmiştir.

Norveç Veri Koruma Otoritesi 2018 tarihli raporunda, YZ uygulamalarında kişisel veri korunması ihlallerinin azaltılması için temel olarak: eğitim setlerinde kişisel verilere duyulan ihtiyacın azaltılmasına yönelik yöntemler, temel veri setini azaltmadan kişisel verileri korumayı sürdürebilen yöntemler ve kara kutudan kaçınmak için tasarlanmış yöntemler ele alınmıştır. Rapor kapsamında çok sayıda kullanıcı tarafından kullanılabilir riskten uzak bir yaklaşım benimseyen birçok teknik açıklanmıştır⁷⁵⁷. Yeni bir gizlilik koruma makine öğrenme tekniği olan Federe Öğrenme⁷⁵⁸ modeli bugün birçok alanda kullanılmaya başlanmıştır⁷⁵⁹. Örneğin, Firefox URL çubuğunu geliştirmek için, Federe Öğrenme tekniği kullanılmıştır⁷⁶⁰. Nitekim, federe öğrenme modeli, mahremiyet korumalı yapay zeka uygulamaları geliştirmek için kullanılabilir önemli yöntemlerden biridir⁷⁶¹.

Norveç Veri Koruma Otoritesi, yapay zeka tabanlı uygulamaları kullanan şirketlere; kullanmaya başlayacakları YZ tabanlı uygulamayı kullanmadan önce risk değerlendirmesi yapmalarını, söz konusu uygulamanın tasarından itibaren kişisel verilerin korunmasını öncellenmesini talep etmelerini, sistemin ayrımcılık yasağına aykırı sonuçlar doğurmayacağından emin olmak için üzerinde testler yapmalarını, sistemin kişisel verilerin korunması hakkı bağlamında ilgili kişinin haklarını sağlamada güçlük çıkarmadığından emin olmalarını ve veri koruma ekipleri oluşturmalarını önermektedir. Bu güçlü önerilere YZ tabanlı uygulamalar kullanan e-ticaret şirketlerinin de uyum sağlaması önemlidir.

⁷⁵⁷ Bu teknikleri Generative Adversarial Networks, Federated learning, Matrix capsules, Differential privacy, Homomorphic encryption, Transfer learning, RAIRD, Explainable AI ve LIME olarak saymak mümkündür. bkz. The Norwegian Data Protection Authority Committee (2018) . *Artificial intelligence and privacy report*. Norwegian Data Protection Authority, s.26.

⁷⁵⁸ "Federatif öğrenme, merkezi bir modelin en son sürümünü bir istemci birimine (örneğin bir cep telefonuna) indirerek çalışır. Model daha sonra verilere dayalı olarak istemcide lokal olarak geliştirilir. Modeldeki değişiklikler daha sonra sunucuya geri gönderilir ve burada diğer istemcilerdeki modellerden gelen değişiklik bilgileriyle birleştirilir. Değiştirilen bilgilerin ortalaması, merkezi modeli iyileştirmek için kullanılır. Yeni, geliştirilmiş merkezi model artık tüm istemciler tarafından indirilebilir. Bu, kullanıcıların verilerini paylaşmak zorunda kalmadan, çok sayıda kullanıcıya dayalı olarak mevcut bir modeli iyileştirme fırsatı sunar." The Norwegian Data Protection Authority Committee (2018) . *Artificial intelligence and privacy report*. Norwegian Data Protection Authority, s.26.

⁷⁵⁹ Uygulama örnekleri için bkz. Süzen, A. A., ve Kayaalp, K (2019) . Büyük verilerde gizlilik tabanlı yaklaşım: Federe öğrenme. *International Journal of 3D Printing Technologies and Digital Industry*, 3 (3), 302.s. 302.

⁷⁶⁰ Model, Yaklaşık 360.000 kullanıcı dağıtılmış ve bu şekilde model eğitilmiş ve geliştirilmiştir. Firefox. *Federated learning in Firefox*. <https://florian.github.io/federated-learning-firefox/> (Erişim tarihi: 09.06.2025)

⁷⁶¹ Başkaya ve Karacan, 2022, s. 489.

SONUÇ

Kişisel verilerin korunması hakkı bugün insanın kişiliğinin bir parçası olan, başta özel hayatın gizliliği ve kişilerin maddi ve manevi varlığını geliştirme hakkı olmak üzere birçok temel hak ve özgürlükle ilişkili olan ve temelinde self-determinasyon ilkesinin yattığı bağımsız şekilde korunan bir hak haline gelmiştir. Bilişim ve teknoloji çağında vazgeçilmez bir unsur haline gelen kişisel veriler bugün birçok alanda farklı amaçlara hizmet etmekte, ekonomik bir değer ve güç unsuru haline gelmektedir. Bu temel sebeplerle kişisel verilerin korunması düzenlemelerinde dahi kişisel verilerin korunması ile kişisel verilerin serbest akışının sağlanması amaçlandığı ifade edilmektedir.

Yapay zeka teknolojisi ile her ne kadar başlangıçta insan gibi düşünebilen ve görevleri yerine getirebilen yazılımlar ve programlar elde edilmek istenmiştir. Tarihi süreç içerisinde YZ talep edilen görevleri gerçekleştirmede insan yeteneklerinin üstünde performanslar sergilemiş ve birçok müsabakada insana galip gelmiştir. Ne var ki, yapay zeka teknolojileri insana özgü bilinci, kendi kendine karar verme ve uygulama becerisini hala kazanamamıştır. Bugün yaygın olarak kullanılan yapay zeka programları dar kapsamlı yapay zeka sınıfında yer alan ve yalnızca eldeki verilerden hareketle karar alabilen yazılımlardır. Dolayısıyla insana özgü muhakeme yeteneğine sahip olan sistemler bugün hala uzak bir gelecek olarak gözükmektedir. Bugün kullanılan yapay zeka uygulamalarını büyük verinin sağladığı imkandan yararlanarak gelişmiş veri analizi yöntemleri kullanarak üstün başarı gösterebilen sistemler olarak tanımlayabiliriz. YZ sistemlerinin en büyük gelişiminin öğrenme kabiliyeti kazanmaları olduğu konusunda görüş birliği bulunmaktadır. Bu sistemlerin öğrenme kabiliyetinin temel besini ise büyük miktarda veridir. E-ticaret sektöründe kullanılan yapay zeka uygulamalarında ise çoğunlukla kişisel verileri işlenmekte böylece YZ çıkarımlarda bulunmakta ve kararlar almaktadır.

Gelişmiş teknolojinin bir ürünü olan yapay zekâ sistemleri, sunduğu çok sayıda faydanın yanı sıra çeşitli tehlikeleri de beraberinde getirmektedir. Özellikle kişisel verilerin korunması hakkı bakımından, yapay zekâ uygulamalarının mevcut koruma mekanizmalarının yetersiz kaldığı ve bireylerin hak ve özgürlüklerini ciddi biçimde tehdit ettiği gözlemlenmektedir. Nitekim, yapay zekâ sistemleri ayrımcılık, manipülasyon ve güvenilirlik sorunları gibi riskleri de beraberinde getirerek temel hak ve özgürlüklerin ihlaline yol açabilmektedir.

E-ticaret platformları bugünkü büyüme ve satış hacmini yapay zekaya sistemlerine borçludur. Nitekim bu sistemler sayesinde kişiselleştirilmiş hizmet sunarak müşteri deneyimini zenginleştiren ve gelirlerini arttıran e-ticaret şirketleri aynı zamanda ticari stratejilerini de doğruluk yüzdesi çok yüksek olan ve insandan kaynaklı hataları en aza indiren yapay zeka teknolojisi sayesinde doğru şekilde belirleyebilmektedir. E-ticaret platformlarında yaygın olarak kullanılan yapay zeka uygulamaları kısaca chatbot ve sanal asistanlar, kişiselleştirme, öneri sistemleri, akıllı arama sistemleri, dinamik fiyatlandırma ve stok yönetimi uygulamalarıdır. Bu uygulamalarda genellikle makine öğrenmesi, derin öğrenme, yapay sinir ağı ve doğal dil işleme yapay zeka teknikleri uygulanmaktadır.

E-ticarete kullanılan YZ sistemleri kişisel veri eğitim setleri ile kendilerini eğitmekte, doğal dil işleme yöntemi ile kullanıcı ile sağlıklı şekilde iletişim kurarak duygu farkındalığına varan boyutlarda kullanıcıyı anlayabilmekte, talebi ve sorunu tanımlayabilmekte, derin

öğrenme tekniği kullanarak kullanıcı deneyimlerinden öğrenebilmektedir. Ne var ki, tüm bu işlevlerin gerçekleşmesi için yapay zeka sistemleri çok sayıda kişisel veriyi kullanmakta ve depolamaktadır. Kişiselleştirme yaparak müşterilerin profillerini çıkaran, kişisel verileri kullanan ve veri setleri için depolayan yapay zeka sistemleri kişilerin mahremiyetlerini, temel hak ve özgürlüklerinin etkin kullanmalarını tehdit etmektedir. Yapay zeka uygulamalarının topladığı verileri kimlere aktarabileceği ise başka bir risk unsurunu oluşturmaktadır.

Yapay zeka ve kişisel verileri işleme ilkeleri bağlamında yapılan değerlendirmede yapay zeka uygulamalarının bu ilkelere büyük ölçüde uyumlu olmadığı gözlemlenmiştir. Nitekim, kişisel verilerin korunması ilkelerinden, veri minimizasyonu ilkesi ile eğitim setleri ile model oluşturulması ve optimum iyi kararı vermesi için güncel ve yeni verilere ihtiyaç duyması bağlamında yapay zeka uygulamaları uyusmamaktadır. Yapay zeka uygulamalarının işledikleri verileri başka bağlamlarda kullanabilme kolaylığı ve uygulamadaki bu gerçeklik amaçla sınırlılık veri işleme prensibi ile bağdaşmamaktadır. Kullanılan yapay zeka algoritmaları teknik olarak kullanıcılara açıklanmamakta çoğu zaman kullanıcılar yapay zeka algoritması ile çalışan bir sistem içerisinde işlem yaptıklarını dahi bilmemektedir. Bu durum şeffaflık veri işleme prensibi ile bağdaşmamaktadır. Model eğitimlerinde kullanılmak üzere kullanıcılara ilişkin kişisel verilerin saklanması, kişisel verilerin sınırlı süre ile muhafaza edilme prensibi ile çelişmektedir.

Kişisel verilerinin, yapay zeka algoritmaları ile işlendiğini veya müracaat yollarını bilmeyen kullanıcılar, kişisel verilerinin doğru veya güncel olduğu denetimini gerçekleştirememekte böylece düzeltilmesi veya silinmesi haklarını kullanamamaktadır. Bu durum kişisel verilerin doğru ve güncel olması prensibini tehlikeye uğrattığı gibi yapay zeka kararlarının doğruluğuna da gölge düşürmektedir. Nitekim, yanlış veya eksik veriler ile doğru ve isabetli kararlar oluşturulması beklenemez.

Yapay zeka teknikleri kullanan e-ticaret şirketlerinin, kişisel verilerin korunması hukukuna uyum göstermesi önünde bazı güçlükler bulunmaktadır. Bunlardan ilki bu konuda farkındalığın olmamasıdır. Çoğu tüketici gibi e-ticaret şirketleri de kullandıkları sistemin teknik yapısını bilmemektedir. Tüketiciler bu konuda daha dezavantajlı konumdadır çünkü tüketicilerin çoğu zaman kişisel verilerinin toplandığından, yapay zeka algoritmaları ile haklarında çıkarımlar bulunulduğundan bu sebeple kişisel ayrımcılığa maruz kalabileceklerinden haberleri dahi olmamaktadır. Bu noktada veri sorumlularının aydınlatma yükümlülüğü ve tüketicilerin bilgi edinme hakkı önem arz etmektedir.

Düzenleyici hükümler, veri sorumlularını kişisel verilerini işledikleri bireyleri; hangi kişisel verilerin, hangi amaçlarla toplandığı, verilerin toplanması ve işlenmesinde kullanılan teknikler ile kişisel verilerin kimlere ve hangi amaçlarla aktarıldığı konularında bilgilendirmekle yükümlü kılmaktadır. Bu çerçevede, tüketicilerin de kişisel verilerine ilişkin bilgi edinme hakkı bulunmaktadır. Ancak yapay zekâ uygulamalarında kullanılan sistemlerin karmaşık yapısı ve teknik terminoloji, kişisel verilerin nasıl işlendiğinin ilgili kişiler tarafından anlaşılmasını güçleştirmektedir. Bu nedenle veri sorumluları, yapay zekâ tarafından gerçekleştirilen veri işleme faaliyetlerini açık, sade ve anlaşılır bir dille; gerektiğinde ise görsel unsurlar kullanarak ilgili kişilere açıklamalıdır. Her şeyden önce, bireyler kişisel verilerinin işlendiği, bu işlemin yapay zekâ teknikleri kullanılarak gerçekleştirildiği ve bu sürecin muhtemel çıktıları hakkında açıkça bilgilendirilmelidir. Söz konusu bilgilendirme, yapay zekâ karşısında kişisel verilerin etkin bir şekilde korunabilmesi açısından temel bir ön koşuldur. Bu

sayede bireyler, kişisel verileri üzerindeki denetimlerini sürdürebilecek ve veri koruma mevzuatından doğan haklarını bilinçli bir şekilde kullanabileceklerdir.

Kişisel verilerin korunması hukuku araçları güçlü olsa da; yapay zeka bu araçların kullanılmasını etkisizleştirebilmektedir. Yapay zeka teknolojisinden beklenen faydaların elde edilmesi için çoğu zaman şirketler bu hakkı ihlal edilmesi riskini almaktadır. Kimi zaman ise şirketler YZ tekniklerini kullanırken kişisel verileri nasıl koruyacaklarını ve kişisel verilerin korunmasından doğan yükümlülüklerini nasıl yerine getireceklerini bilmemektedir. Son dönemde artan YZ farkındalığı sayesinde yapay zekaya ilişkin düzenlemeler yapılmaya başlanmıştır. Fakat bu düzenlemeler oldukça yenidir. Nitekim, bu alandaki dünyadaki ilk düzenlemelerden olan Avrupa Birliği Yapay Zeka Yasası(AI Act) ve Avrupa Konseyi Çerçeve Sözleşmesi henüz geçen yıl 2024 yılında kabul edilmiştir. Bu alanda düzenleyici metinlerin artması ile farkındalığın oluşması için özellikle disiplinler arası çalışmaların artması ile yapay zeka teknolojisi karşısında kişisel verilerin korunmasına yardımcı olacaktır.

Avrupa Birliği Yapay Zeka Yasası(AI Act), tüm yapay zeka sistemleri için genel bir düzenleme getirmek yerine, yapay zeka sistemleri için risk kategorileri oluşturarak her kategoriye farklı yükümlülükler getirilmiştir. Kişisel verilerin korunması için ihlal niteliği taşıyabilecek uygulamalar, yüksek riskli yapay zeka kategorisi içinde sayılmaktadır. Yüksek riskli yapay zeka uygulamalarının yerine getirmesi gereken yükümlülükler belirleyen düzenleme ayrıca zararlı pek çok yapay zeka uygulamasını yasaklamıştır. Bir diğer düzenleyici metin olan Avrupa Konseyi Çerçeve Yasası, yapay zeka sistemlerinin temel insan haklarına uyumlu kullanılması için genel bir çerçeve sunmaktadır. Bu düzenlemelerin devrim niteliğinde olduğu ve yapay zeka uygulamalarında kişisel verilerin korunması ihtiyacını tam olarak karşıladıkları söylenemese de; bu adımda öncü oldukları ve farkındalık oluşturdıklarından bahsedilebilir. Nitekim, bu düzenlemelerin uygulamada ne kadar etkili oldukları zaman geçtikçe anlaşılacaktır.

AI Act düzenlemesinde, YZ sisteminin tüm yaşam döngüsü boyunca gizlilik hakkının ve kişisel verilerin korunması hakkının garanti altına alınması gerektiği belirtilmektedir(AI Act, *giriş*, para. 69). Bu kapsamda GDPR'ın *data protection by design* ve *protection by default* ilkeleri önem arzetmektedir. Geliştiriciler tarafından alınan önlemler yalnızca anonimleştirme ve şifrelemeyi değil, aynı zamanda algoritmaların verilere getirilmesine izin veren ve taraflar arasında iletim veya ham veya yapılandırılmış verilerin kendilerinin kopyalanması olmadan YZ sistemlerinin eğitilmesine olanak tanıyan teknolojinin kullanımını da içermelidir. Tasarımdan itibaren ve varsayılan ayarla kişisel verilerin korumasını önceleyen sistemler kişisel verilerin korunması ihlallerine karşı bir zırh görevi görecektir. Ayrıca, GDPR düzenlemesinde öngörülen veri koruma görevlisi de şirketlerde kişisel verilerin korunması ihlallerinin azaltılması ve kişisel verilerin korunmasını önceleyen şirket içi politikaların oluşturulmasında önemli bir aktördür.

Yapay zeka teknolojisinin getirdiği risklere karşı panzehir olarak riskleri önleyici algoritmaların geliştirilmesi çok önemlidir. Bu noktada, Norveç Veri Koruma Otoritesi 2018 tarihli raporu büyük bir adım atmıştır. Bu çalışmada oluşturulmaya çalışılan eğitim setlerinde kişisel verilere duyulan ihtiyacın azaltılmasına yönelik yöntemler, temel veri setini azaltmadan kişisel verileri korumayı sürdürebilen yöntemler ve kara kutudan kaçınmak için tasarlanmış yöntemler geliştiriciler açısından yol gösterici olmalıdır. Bu yöntemler kalite standartlarına eklenerek, şirketlerin bu standartları yerine getirip getirmediği veri otoritelerince denetlenmelidir.

Kişisel verilerin korunması hukukuna uyum sağlamak isteyen e-ticaret şirketlerinin, yapay zekâ sistemlerinin kullanımında birtakım temel ilkelere riayet etmesi gerekmektedir. Her şeyden önce, bir yapay zekâ sistemi kullanılmadan önce, bu sistemin kişisel veriler üzerindeki etkileri açısından kapsamlı bir risk değerlendirmesi yapılmalıdır. Bu değerlendirme, olası hak ihlallerini önceden öngörerek gerekli önlemlerin zamanında alınmasını mümkün kılar. Yapay zekâ sistemlerinin tasarım aşamasında veri koruma ilkelerinin gözetilmesi büyük önem taşımaktadır. Bu doğrultuda, sistem geliştiricilerinden tasarımdan itibaren kişisel verilerin korunmasını esas alan, veri minimizasyonunu ve güvenliği önceleyen teknik ve idari düzenlemeleri içeren bir yaklaşım benimsemeleri talep edilmelidir. Kullanılan yapay zekâ sistemleri üzerinde belirli aralıklarla güvenlik açıkları ve ihlal risklerine karşı test ve denetim faaliyetleri yürütülmelidir. Bu tür denetimler, hem sistemin güvenilirliğini artırmakta hem de kişisel veri korumasını güçlendirmektedir. Kişisel verilerin işlenmesinin hukuki dayanağını açık rıza oluşturmaktaysa, bu rızanın gerçekten özgür iradeye dayalı olarak verilip verilmediği titizlikle değerlendirilmelidir. Rıza alma süreçleri, açık, anlaşılır ve yanıltıcı unsurlardan arındırılmış şekilde yapılandırılmalıdır. Ayrıca, yapay zekâ sistemlerinin, veri sahiplerinin kişisel verilerin düzeltilmesi, silinmesi veya işlenmesine itiraz gibi mevzuattan doğan haklarını teknik olarak kullanmalarına imkân tanıyıp tanımadığı analiz edilmelidir. Son olarak, e-ticaret şirketleri bünyesinde kişisel verilerin korunmasına ilişkin etik ilkelere dayalı kurumsal yapılar tesis edilmelidir. Bu çerçevede kurulacak etik kurullar, yapay zekâ uygulamalarının şeffaf, hesap verebilir ve insan haklarına saygılı biçimde işletilmesini temin edecek şekilde faaliyet göstermelidir.

Sonuç olarak belirtmek gerekir ki, yapay zekâ teknolojisinin hak ihlallerine yol açmasının başlıca nedeni, bu teknolojinin bilinçsiz ve denetimsiz biçimde kullanılmasıdır. Bu durum, hem yapay zekâ tabanlı sistemlerin arkasında bu teknolojinin bulunduğu farkında olmayan kullanıcılar hem de yalnızca sağladığı faydaya odaklanarak risk ve sorumluluklarını göz ardı eden şirketler açısından geçerlidir. Bu bağlamda, kişisel verilerin korunması ve yapay zekâ okuryazarlığının artırılması büyük önem taşımaktadır. Bireylerin, kişisel verilerin korunmasına ilişkin hakları ve bu hakların kapsamı hakkında bilinçlendirilmesi; şirket çalışanlarının ve kullanıcıların, yapay zekâ teknolojilerinin işleyişini ve doğurabileceği olası riskleri anlayacak donanıma kavuşturulması, bu alanda atılacak ilk yapısal adımlardandır. Diğer yandan, yapay zekâ uygulamaları çerçevesinde meydana gelebilecek kişisel verilerin korunması hakkı ihlallerinin önlenmesi; ancak bu teknolojinin yasa koyucular ve hukuk uygulayıcıları tarafından derinlemesine kavranmasıyla mümkün olabilecektir. Kişisel verilerin korunmasına ilişkin yasal düzenlemelerin, yapay zekânın teknik ve işlevsel özellikleri dikkate alınarak ihdas edilmesi; uygulayıcı hukukçuların ise bu düzenlemelerin uygulamadaki boşluklarını tespit ederek sürekli güncellenmesini sağlaması, hak ihlallerinin önlenmesi bakımından temel bir zorunluluktur.

KAYNAKÇA

- Akgül, A (2014). *Danıştay ve Avrupa İnsan Hakları Mahkemesi kararları ışığında kişisel verilerin korunması*. Beta Yayınları.
- Akgül, A (2016). Kişisel verilerin korunmasında yeni bir hak: Unutulma hakkı ve AB Adalet Divanı'nın "Google Kararı". *TBB Dergisi*, 116, 11–38.
- Akıntürk, T., & Ateş, D (2024). *Medeni hukuk* (28. baskı). Beta Yayınları.
- Akkurt, S. S (2020). Kişisel veri kavramının hukuki niteliğine ilişkin yaklaşımlara mukayeseli bir bakış. *Kişisel Verileri Koruma Dergisi*, 2(1), 20–32.
- Aksoy, H. C (2010). *Medeni hukuk ve özellikle kişilik hakkı yönünden kişisel verilerin korunması*. Çakmak Yayınları.
- Aksoy, H. C (2022). Kişisel verilerin korunması yönüyle algoritmik karar verme. *Kişisel Verileri Koruma Dergisi*, 4(2), 69–87.
- Altındere, M (2020). *Kişisel verilerin korunması hukuku ve uygulanması*. Adalet Yayınları.
- Antalya, G., & Topuz, M (2024). *Medeni hukuk (Giriş, temel kavramlar, başlangıç hükümleri)* (Cilt 1, Genişletilmiş 5. baskı). Seçkin Yayıncılık.
- Arat, A (2014). Gerçek kişilerde kişiliğin sona ermesi. *Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi*, 9, 257–276.
- Arık, A., & Zeren, D (2023). Tüketicilerin sanal asistanları kullanma niyetinde etkili faktörlerin araştırılması. *Alanya Akademik Bakış*, 7(1), 27–49.
- Aşıkoğlu, İ. Ş (2018). *Avrupa Birliği ve Türk hukukunda kişisel verilerin korunması ve büyük veri*. Onikilevha Yayınları.
- Atalan, S. E (2024). *Uluslararası hukuk bağlamında Avrupa'da yapay zekaya ilişkin düzenlemeler ve kişisel verilerin korunması* (Yayımlanmamış yüksek lisans tezi) İstanbul Üniversitesi.
- Avrupa İnsan Hakları Mahkemesi (2018). *Handbook on European data protection law*. Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (Erişim tarihi: 25.03.2025)
- AYATA, Z., Büyük Yenilik Büyük Değişiklik Gerektirir mi? Avrupa Birliği Rekabet Hukukunun Büyük Veri ile İmtihanı, *Banka ve Ticaret Hukuku Dergisi*, 34(4), s. 203-239.
- Aygün, M (2023). *Milletlerarası usul hukuku ile kanunlar ihtilafı hukuku kuram ve metodolojisi çerçevesinde yapay zeka*. Yetkin Yayınları.
- Ayözger Öngün, Ç (2019). *Kişisel verilerin korunması hukuku: Elektronik haberleşme sektörüne ilişkin özel düzenlemeler dahil* (Genişletilmiş 2. baskı). Beta Yayınları.

- Badur, E (2023). Kişisel verilerin kişiliğin başlangıcı ve sonu ötesinde korunması. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 27(3), 3–32.
- Badur, E (2024). Yapay zeka sistemleri kullanılarak yapılan işleme faaliyetlerinde kişisel verilerin korunması. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 32(4), 2525–2560.
- Balkan, N (2024). Kişisel veri koruma hukuku ile ticaret sicilinin aleniyet fonksiyonu arasındaki menfaat dengesi. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 28, 207–240.
- Başalp, N (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun temel yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21(1), 77–105.
- Başkaya, F., ve Karacan, H (2022). Yapay zeka tabanlı sistemlerin kişisel veri mahremiyeti üzerine etkisi: Sohbet robotları üzerine inceleme. *Bilişim Teknolojileri Dergisi*, 15(4), 481–491.
- Beane, T. P., and Ennis, D. M (1989). La segmentation des marchés: Une revue de la littérature. *Recherche et Applications en Marketing*, 4(3), s.25-52.
- Belhadj, M (2022). *Pazarlama hizmetinde yapay zeka: Netflix öneri sistemi örneği / Artificial intelligence in the service of marketing: Case of Netflix recommendation system* (Yayımlanmamış yüksek lisans tezi). Necmettin Erbakan Üniversitesi.
- Blanke, J. M (2000). "Safe Harbor" and the European Union's directive on data protection. *Albany Law Journal of Science & Technology*, 11, 101–134.
- Büyüközkan Feyzioğlu, G (2021). Dijitalleşen dünyada yapay zeka. İçinde E. Aksoy Retornaz & O. G. Güçlütürk (Ed.), *Gelişen teknolojiler ve hukuk II: Yapay zeka* (ss.1-5). On İki Levha Yayınları.
- Büyüksağış, E (2021). Yapay zeka karşısında kişisel verilerin korunması ve revizyon ihtiyacı. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, 18(2), 529–541.
- Chapdelaine, P (2020). Algorithmic personalized pricing. *New York University Journal of Law & Business*, 17(1), 1–47.
- Chate, P. J (2019). The use of machine learning algorithms in recommender systems: A systematic review. *IJRAR – International Journal of Research and Analytical Reviews*, 6(2), 671–681.
- Çavuşoğlu, G. F (2021). *Kişisel verilerin yapay zekayla işlenmesinden doğan özel hukuk sorunları* (Yayımlanmamış yüksek lisans tezi). Ankara Üniversitesi.
- Darendeli, F (2023). *The protection of biometric data in the era of artificial intelligence technology in EU law*. Yetkin Yayınları.
- Demirtaş, A (2024). ChatGBT gölgesinde kişisel verilerin korunması. *Kişisel Verileri Koruma Dergisi*, 6(1), 14-27.
- Develioğlu, H. M (2017). *6698 sayılı Kişisel Verilerin Korunması Kanunu ile karşılaştırmalı olarak Avrupa Birliği veri koruma tüzüğü uyarınca kişisel verilerin korunması hukuku*, Onikilevha Yayınevi.

Dönmezer, S (1957). Hukuk ve hayat. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 21(1-4), 424–427.

Duch-Brown, N., Martens, B., and Mueller-Langer, F. (2017). *The economics of ownership, access and trade in digital data* (JRC Digital Economy Working Paper 2017-01; JRC104756). European Commission, Joint Research Centre.

Duran, C (2021). Yapay zeka temelli pazarlama: Geleneksel pazarlamanın sonu mu? İçinde N. Ö. İyigün ve M. K. Yılmaz (Ed.), *Yapay zeka: Güncel yaklaşımlar ve uygulamalar*(s. 31-50). Beta Yayınları.

Dülger, M (2015). Sağlıkta kişisel verilerin korunması ve hasta mahremiyeti. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 1(2), 43–80.

Dülger, M. V. (2021). *Tasarlanmış ve önceden tanımlanmış veri koruma ile zarara karşı risk sorumluluğu: Kişisel Verileri Koruma Kurulu’nun 18 Şubat 2019 tarihli kararları ne anlama geliyor?* SSRN. <https://doi.org/10.2139/ssrn.3792301> .

Dülger, M. V., Kahraman, C. C., ve Yalçın, S. (2021). *GDPR ve KVKK bakımından kişisel verilerinin korunması ve konuya ilişkin kurul kararının değerlendirilmesi (Çocukların kişisel verilerinin GDPR ve Kişisel Verilerin Korunması Kanunu açısından korunması ve Yargıtay incelemesi)*. <https://doi.org/10.2139/ssrn.3792410>

Edwards, L., and Veale, M (2019). Slave to the algorithm? Why a “right to an explanation” is probably not the remedy you are looking for. *Duke Law and Technology Review*, 16, 18–84.

Egemen, E. E. (2023). Kişisel verilerin işlenmesinde “doğru ve gerektiğinde güncel olma” ilkesi ve Kişisel Verileri Koruma Kurulunun 2023/78 sayılı kararı. *Trabzon Üniversitesi Hukuk Fakültesi Dergisi*, 1(1), 105–133.

Ergül, E. (2025, Şubat). *Türkiye’nin yapay zeka hukuku: Uluslararası standartlar ve mukayeseli yaklaşımlar* (Sayı 437). SETA. <https://www.setav.org/assets/uploads/2025/02/a437.pdf> Erişim Tarihi: 26.07.2025.

European Court of Human Rights (2025). *Factsheet – Personal data protection*. https://www.echr.coe.int/documents/d/echr/fs_data_eng.

European Parliament (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. Panel for the Future of Science and Technology.

Good, O (2025, July 29). How Google Translate squeezes deep learning onto a phone. *Google AI Blog*. <https://ai.googleblog.com/2015/07/how-google-translatesqueezes-deep.html> Erişim Tarihi: 26.05.2025

Gostin, L. O (1995). Genetic privacy. *Journal of Law, Medicine & Ethics*, 23, 320–330.

Gönen, D (2011). *Tüzel kişilerde kişilik hakkı ve korunması*. XII Levha Yayıncılık.

Greengard, S (2019, May 4). What is artificial intelligence & how does it work? *Datamation*. <https://www.datamation.com/artificial-intelligence/what-is-artificial-intelligence/> (Erişim Tarihi: 25.05.2025).

Gupta, A., Hathwar, D., and Vijayakumar, A (2020). Introduction to AI chatbots. *International Journal of Engineering Research and Technology*, 9(7), 255–258.

- Güçlütürk, O. G (2022). *Yapay zeka ve verinin kullanımı*. On İki Levha Yayınları.
- Güçlütürk, O. G (2023). Üretken yapay zeka, riskler ve mahremiyet üzerine bir değerlendirme. *KVKK Bülten*, 9–11.
- Gülşen, İ (2019). İşletmelerde yapay zeka uygulamaları ve faydaları: Perakende sektöründe bir derleme. *Tüketici ve Tüketim Araştırmaları Dergisi*, 11(2), 407–436.
- Gürsel, İ (2016). Kişisel verilerin korunması hakkının işçi ve işveren ilişkilerine etkileri. *İş Hukuku ve Sosyal Güvenlik Dergisi*, 13(50), 763–848.
- Güven, H., ve Güven, E. T. A (2023). Yapay zeka uygulamalarının e-ticarete kullanımı. *International Journal of Management and Administration*, 7(13), 69–94.
- Hingh, A. de (2018). Some reflections on dignity as an alternative legal concept in data protection regulation. *German Law Journal*, 19(5), 1269–1290.
- Huang, T (2006). Expert systems. In C. Smith (Ed.), *The history of artificial intelligence*. University of Washington (pp. 12–16).
- Irina, I (2016). What is marketing automation and how could it be used for business? *Yearbook of the 'Gheorghe Zane' Institute of Economic Researches, Jassy / Anuarul Institutului de Cercetări Economice 'Gheorghe Zane' Iași*, 25(1), 11–28.
- Isaac, M (2023, 8 Kasım). Mark Zuckerberg taps the strengths of WhatsApp. *The New York Times*. <https://www.nytimes.com/2023/11/08/technology/mark-zuckerberg-whatsapp.html> . Erişim Tarihi: 02.05.2025.
- İnan, O. (2015). *Veri madenciliği uygulamaları için veri indirgeme algoritmalarının geliştirilmesi ve resim madenciliğine uygulanması* (Yayımlanmamış doktora tezi).
- İşeri, İ., Aydın, Ö., ve Tutuk, K (2021). Müşteri hizmetleri yönetiminde yapay zeka temelli chatbot geliştirilmesi. *European Journal of Science and Technology*, (29), 358–365.
- Kahramanlı, H. (2008). *Hibrit bulanık sinir ağını kullanarak bir sınıflandırma ve kural çıkarma sisteminin geliştirilmesi* (Yayımlanmamış doktora tezi). Selçuk Üniversitesi.
- Kaplan, J (2016). *Artificial intelligence: What everyone needs to know*. Oxford University Press.
- Karadeniz, S. (2025). Avrupa Birliği Yapay Zekâ Kanunu'nun risk grupları ve ilgililerin yükümlülükleri bağlamında incelenmesi. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 29(1), 307–366. <https://doi.org/10.34246/ahbvuhfd.1541455> .
- Karaman, Ö (2021). Yapay zeka destekli kişiselleştirme algoritmalarının tüketici zihninde filtre balonu yaratma etkisinin incelenmesi. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 12(32), 1339–1351.
- Kaya, C (2011). Avrupa Birliği veri koruma direktifi ekseninde hassas (kişisel) veriler ve işlenmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 69(1–2), 317–334.
- Kaya, M. B (2010). *Teknik ve hukuki boyutlarıyla internete erişimin engellenmesi: 5651 sayılı kanun ve dünya uygulamaları*. XII Levha Yayınları.

Kaya, M. B (2015). Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 tarihli Google unutulma hakkı kararı çevirisi. <https://dergipark.org.tr/en/download/article-file/1671800> (Erişim Tarihi: 22.03.2025)

Kirazlı, Ş. N (2024). *Chatbot özelinde üretken yapay zeka ve kişisel verilerin hukuka uygun işlenmesi / Processing of personal data in compliance with the law and generative artificial intelligence in the context of chatbots* (Yayımlanmamış yüksek lisans tezi). Sakarya Üniversitesi.

Kişisel Verileri Koruma Kurumu (2025). *Madde ve gerekçesi ile kişisel verilerin korunması kanunu (bilgi notu) ve kişisel verilerin korunmasına ilişkin terimler sözlüğü*. KVKK Yayınları.

Koparan, E., ve Doğan, O (2024). Toplum 5.0 ve e-ticarete yapay zeka odağında bakış: Tanımlar, ilişkiler ve bileşenler. *Yönetim ve Ekonomi Dergisi*, 31(2), 295–324.

Korkmaz, A (2024). Ticaret sicili kapsamındaki faaliyetlerin kişisel verileri koruma hukuku çerçevesinde değerlendirilmesi. *Ticaret ve Fikri Mülkiyet Hukuku Dergisi*, (10), 297–316.

Köksal, D. ve Konukpay, C. (2021). Büyük veri kullanımının temel hak ve özgürlükler üzerindeki etkileri. İçinde O. Güçlütürk & E. Retornaz (Ed.), *Gelişen teknolojiler ve hukuk III: Büyük veri* (1. baskı, s. 15–89). On İki Levha Yayınları.

Küzeci, E (2010). *Kişisel verilerin korunması*. Turhan Kitabevi.

Küzeci, E (2011). Anayasal bir hak: Kişisel verilerin korunması. *Türkiye Bilişim Derneği Bilişim Dergisi*, 142–149.

Küzeci, E (2014). İstatistikî birimler ve bilgilerin geleceğini belirleme hakkı. *İnsan Hakları Yıllığı*, 32, 1–23.

Le, C., Mislove, A. and Wilson, C (2016). An empirical analysis of algorithmic pricing on Amazon Marketplace. In *Proceedings of the 25th International Conference on World Wide Web*, 1339–1349. <https://doi.org/10.1145/2872427.2883089> .

Lemley, M. A (2000). Private property: A comment on Professor Samuelson's contribution. *Stanford Law Review*, 52, 1545–1551.

McCarthy, J (2007). *What is artificial intelligence*. Stanford University. <http://www-formal.stanford.edu/jmc/> (Erişim Tarihi: 20.05.2025)

McGuire, B (2006). The Turing test (pp. 5–9). In C. Smith (Ed.), *The history of artificial intelligence*. University of Washington.

Medeni, İ. T., ve Aktaş, Z (2010). Veri toplumundan bilgi toplumuna dört düzeyli bir toplum modeli. In 3. *Ağ ve Bilgi Güvenliği Ulusal Sempozyumu* (ss. 5–6).

Memiş, T (2017). Veri sorumlusu ve veri işleyen arasındaki ilişkiler ve sorumluluk düzeni. *Beykent Üniversitesi Hukuk Fakültesi Dergisi*, 3(6), 9–23.

Newell, A., and Simon, H. A (1956). The logic theory machine—a complex information processing system. *IRE Transactions on Information Theory*, 2(3), 61–79.

Özcan, A. (2021). *Büyük veri: Fırsatlar ve tehditler*. TRT Akademi, 6(11), s. 10–31. <https://doi.org/10.37679/trta.818569> .

Özgür, N (2023). *Sohbet botları ve yapay zeka etiği* (Yüksek lisans bitirme projesi) İzmir Kâtip Çelebi Üniversitesi. <https://acikerisim.ikcu.edu.tr/yayin/1742489&dil=3&q=> Erişim Tarihi: 30.05.2025

Özparlak, B.O. ve Yılmaz, S.S. (2021). 6G kablosuz teknolojisi ve veri: yeni hukuki tartışmalar. İçinde O. Güçlütürk & E. Retornaz (Ed.), *Gelişen teknolojiler ve hukuk III: Büyük veri* (1. baskı, s. 167-220). On İki Levha Yayınları.

Pap, A. L (2009). Profiling, data mining and law enforcement: Definitions. *Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae: Sectio Iuridica*, 50, 277–302.

Prins, C (2006). When personal data, behavior and virtual identities become commodity: Would property rights approach matter. *SCRIPTed: Journal of Law, Technology and Society*, 3(4), 270–303.

Retornaz, E. A. ve Güçlütürk, O. G (2021). Büyük veri. İçinde E. A. Retornaz & O. G. Güçlütürk (Ed.), *Gelişen teknolojiler ve hukuk III: Büyük veri* (ss. 1–13). On İki Levha Yayınları.

Retornaz, E. A., & Güçlütürk, O. G (2021). Yapay zekanın kişisel veri kavramı ve kişisel verilerin işlenmesinde temel ilkelerle ilişkisi. İçinde E. A. Retornaz & O. G. Güçlütürk (Ed.), *Gelişen teknolojiler ve hukuk II: Yapay zeka* (ss. 275-302). On İki Levha Yayınları.

Rogers, A (1997). European data protection to give unborn children rights? *The Lancet*, 349(9045), s.550. [https://doi.org/10.1016/S0140-6736\(97\)80110-9](https://doi.org/10.1016/S0140-6736(97)80110-9).

Rosenblatt, F (1960). Perceptron simulation experiments. *Proceedings of the IRE*, 48(3), 301–309.

Russell, S., and Norvig, P (2024). *Yapay zeka modern bir yaklaşım* (Çev. Prof. Dr. C. Öz, Çev.; 4). Palme Yayınları (Orijinal yayın tarihi 2023)

Rzepka, C., Berger, B., and Hess, T (2022). Voice assistant vs. chatbot – Examining the fit between conversational agents’ interaction modalities and information search tasks. *Information Systems Frontiers*, 24, 839–856. <https://doi.org/10.1007/s10796-021-10226-5>.

Sağtaş, S (2023). Yapay zeka uygulamalarının e-ticarette kullanımı. İçinde T. Yolcu & K. Özkaynar (Ed.), *Yapay zeka ve pazarlama* (ss. 47–60). Nobel Yayıncılık.

Schwartz, P (1989). The computer in German and American constitutional law: Towards an American right of informational self-determination. *The American Journal of Comparative Law*, 37(4), 675–701.

Schwartz, P. M (2004). Property, privacy, and personal data. *Harvard Law Review*, 114(7), 2055–2128.

Selek, O (2021). *Kişisel verilerin korunması ve verileri yok etmeme suçu (TCK m.138)*. Onikilevha Yayınları.

Selita, F (2019). Genetic data misuse: Risk to fundamental human rights in developed economies. *Legal Issues Journal*, 7(1), 53–95.

Sholtz, P (2001). Transaction costs and the social cost of online privacy. *First Monday*, 6(5). <https://firstmonday.org/ojs/index.php/fm/article/view/885/779> Erişim Tarihi: 23.05.2025

Shortliffe, E. H (1977). Mycin: A knowledge-based computer program applied to infectious diseases. In *Proceedings of the Annual Symposium on Computer Application in Medical Care* (pp. 66–69).

Smith, C (2006). History of AI applied to chess. In C. Smith (Ed.), *The history of artificial intelligence* (pp. 10–11). University of Washington.

Smith, C (Ed.) (2006). *The history of artificial intelligence*. University of Washington. <https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf> Erişim Tarihi: 23.05.2025.

Sterne, J (2017). *Artificial intelligence for marketing: Practical applications*. John Wiley & Sons, Incorporated.

Süzen, A. A., ve Kayaalp, K (2019). Büyük verilerde gizlilik tabanlı yaklaşım: Federe öğrenme. *International Journal of 3D Printing Technologies and Digital Industry*, 3(3), 297–304.

Şen, E (2009). Kişisel verilerin korunması kanunu tasarısı'nın anayasa ve Türk Ceza Kanunu hükümleri çerçevesinde değerlendirilmesi. *İstanbul Barosu Dergisi*, 83(3), 1197–1214.

Şimşek, O (2008). *Anayasa hukukunda kişisel verilerin korunması*. Beta Yayıncılık.

Taştan, F. G (2017). *Türk sözleşme hukukunda kişisel verilerin korunması* (2. basım). Onikilevha Yayınları.

The Norwegian Data Protection Authority Committee (2018). *Artificial intelligence and privacy report*. Norwegian Data Protection Authority.

Turing, A. M (1950). Computing machinery and intelligence. *Mind*, 49, 433–460. <https://courses.cs.umbc.edu/471/papers/turing.pdf> (Erişim Tarihi: 21.05.2025)

Tutsal, E., ve Ventura, K (2022). Müşteri deneyimini iyileştirmede yapay zeka uygulamaları: Çevrimiçi perakende firması örneği. *Journal of Social Research & Behavioral Sciences / Sosyal Araştırmalar ve Davranış Bilimleri Dergisi*, 8(16), 346–368.

Tüzüntürk, S. (2010). Veri madenciliği ve istatistik. *Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 29 (1), 65-90.

Uçak, M (2021). Kişisel verilerin ölümden sonra korunması. *İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi*, 6(10), 97–124.

Xue, Z., Ko, T.-Y., Yunchen, N., Wu, M.-K. D., & Hsieh, C.-C (2018). Isa: Intuit smart agent, a neural-based agent-assist chatbot. In *2018 IEEE International Conference on Data Mining Workshops (ICDMW)* (pp. 1423–1428). IEEE. <https://doi.org/10.1109/ICDMW.2018.00209>.

Yang, G (2006). AI winter and its lessons. In C. Smith (Ed.), *The history of artificial intelligence* (pp. 17–21). University of Washington.

Yetim, S (2009). 5651 sayılı yasa kapsamında tutulan internet trafik bilgilerinin özel hayat ve hayatın gizliliği kapsamında değerlendirilmesi. *Terazi Hukuk Dergisi*, 4(36), 55–63.

Yıldız, A. (2022). Büyük verinin V'leri ve veri analitiği. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (51), 361–378. <https://doi.org/10.30794/pausbed.111>.

Yılmaz, M (2009). Enformasyon ve bilgi kavramları bağlamında enformasyon yönetimi ve bilgi yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49(1), 95–118.

Yürük, Z. (2023). Veri sorumlusunun veri güvenliğine ilişkin idari ve teknik tedbirleri alma yükümlülüğü. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 22(48), 899–920. <https://doi.org/10.46928/iticusbe.1218693> .

Zittrain, J (2000). What the publisher can teach the patient: Intellectual property and privacy in an era of trusted privication. *Stanford Law Review*, 52, 1201–1250.

İNTERNET KAYNAKLARI

6698 Sayılı Kişisel Verilerin Korunması Kanunu. Tam metin için bkz. <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5> Erişim Tarihi: 31.01.2025.

Anadolu Ajansı (2025, 5 Haziran). Elon Musk: Ben olmasaydım Trump seçimi kaybederdi. Anadolu Ajansı. <https://www.aa.com.tr/tr/dunya/elon-musk-ben-olmasaydim-trump-secimi-kaybederdi/3590103>

Anayasa Mahkemesi (AYM) (2015). *E. 2013/84, K. 2014/183, Karar Tarihi: 13.03.2015. Resmî Gazete, 13.03.2015, Sayı: 29294.* <https://www.resmigazete.gov.tr/eskiler/2015/03/20150313-12.pdf> .

Article 29 Data Protection Working Party (2004). *Working document on genetic data (WP91)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf .

Article 29 Data Protection Working Party (2007). *Opinion 4/2007 on the concept of personal data (WP136)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

Article 29 Data Protection Working Party (2011). *Opinion 15/2011 on the definition of consent*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Article 29 Data Protection Working Party (2014). *Opinion 05/2014 on anonymisation techniques*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Article 29 Data Protection Working Party (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Article 29 Data Protection Working Party (2018). *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*. <https://ec.europa.eu/newsroom/article29/items/612053/en>

Article 29 Data Protection Working Party (2018). *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*. <https://ec.europa.eu/newsroom/article29/items/612053/en>

Article 29 Working Party (2006). *Opinion 10/2006 on the processing of personal data by The Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf

Article 29 Working Party (2011). *Opinion 15/2011 on the definition of consent*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Article 29 Working Party (2013). *Opinion 03/2013 on purpose limitation*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Working Party (2014). *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Article 29 Working Party (2014). *Opinion 05/2014 on anonymisation techniques*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Article 29 Working Party (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Eriřim tarihi: 08.06.2025).

Article 29 Working Party (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Avrupa Birlięi Adalet Divanı (2014, Mayıs 13). *Google İspanya kararı (C-131/12)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131>

Avrupa Birlięi Adalet Divanı (2015). *Avrupa Birlięi Adalet Divanı'nın 13 Mayıs 2014 tarihli Google unutulma hakkı kararı (M. B. Kaya, Çev.)*. <https://dergipark.org.tr/en/download/article-file/1671800> Eriřim Tarihi: 22.03.2025.

Avrupa Birlięi Adalet Divanı (ABAD) (2014). *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, ECLI:EU:C:2014:317*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131> Eriřim Tarihi: 22.03.2025.

Avrupa Birlięi Adalet Divanı (ABAD) (2023). *Norra Stockholm Bygg AB v Per Nycander, C-268/21, ECLI:EU:C:2023:325*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0268> Eriřim Tarihi: 12.07.2025.

Avrupa İnsan Hakları Mahkemesi (AİHM) (2023, Mart 9). *L.B. v. Hungary (Grand Chamber)*, Başvuru No: 36345/16. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-222437%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-222437%22]}) Erişim Tarihi: 21.02.2025.

Avrupa Parlamentosu ve Konseyi (2016, 27 Nisan). *Genel Veri Koruma Tüzüğü (EU) 2016/679 (GDPR)*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> . Erişim Tarihi: 25.03.2025.

AXA Sigorta (n.d.). AXA'dan dijital asistan ile hızlı hasar tespiti. <https://www.axasigorta.com.tr/basin-bultenleri/axa-dijital-asistan-ile-hizli-hasar-tespiti> Erişim Tarihi: 31.05.2025

BBC (2021). Whatsapp'ın yeni kullanıcı sözleşmesi gizlilik açısından ne anlama geliyor? <https://www.bbc.com/turkce/haberler-dunya-55610827> Erişim Tarihi: 05.06.2025

BBC. *Business news*. <https://www.bbc.com/news/business-26266689> Erişim Tarihi: 05.06.2025.

Burges, M (2023). ChatGPT has a big privacy problem. *Wired*. <https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/> Erişim Tarihi: 05.06.2025

CBOT. CBOT Chatbot Platformu ve Üretici Yapay Zeka Teknolojisi. CBOT | Türkiye'nin Lider Yapay Zeka Şirketi | Kurumsal Chatbot Projeleri. Erişim Tarihi: 30.05.2025

CBOT. En İyi Chatbot Ödülü Haberi. <https://www.cbot.ai/tr/getir-destek-alfa-awards-2023te-en-iyi-sanal-asistan-chatbot-odulunun-sahibi-oldu/> Erişim Tarihi: 31.05.2025

Coles, C (2023, February 28). 11% of data employees paste into ChatGPT is confidential. *Cyberhaven News*. <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt> Erişim Tarihi: 05.06.2025

Council of Europe (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108)*. <https://rm.coe.int/1680078b37> (Erişim Tarihi: 19.03.2025)

Council of Europe (1981). *Convention for the protection of individuals with regard to automatic processing of personal data (No. 108)*. Strasbourg. <https://rm.coe.int/1680078b37> (Erişim tarihi: 19.03.2025)

Council of Europe (1997). *Convention on Human Rights and Biomedicine (Oviedo Convention)*. <https://rm.coe.int/168007cf98> Erişim Tarihi: 22.05.2025

Council of Europe (1997). *Recommendation No. 97 (7)*, 13.02.1997. <https://rm.coe.int/cmrec-97-5-on-the-protection-of-medical-data/1680a43b64> Erişim Tarihi: 24.02.2024.

Council of Europe (1997). *Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data*. <https://rm.coe.int/16806af967> Erişim Tarihi: 22.02.2025.

Council of Europe (2001). *Additional Protocol to Convention No. 108 regarding supervisory authorities and transborder data flows (Treaty No. 181)*. <https://rm.coe.int/1680080626> Erişim Tarihi: 24.04.2024.

Council of Europe (2001). *Convention No. 181 on the Protection of Individuals with regard to Automatic Processing of Personal Data* (08.11.2001). <https://rm.coe.int/1680080626> Erişim tarihi: 25.03.2025.

Council of Europe (2018). *Handbook on European Data Protection Law* (2018 Edition). https://www.echr.coe.int/documents/d/echr/Handbook_data_protection_ENG Erişim Tarihi: 04.05.2025

Council of Europe (2019). *Guidelines on Artificial Intelligence and Data Protection*. Directorate General of Human Rights and Rule of Law, Strasbourg. <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8> Erişim Tarihi: 02.06.2025

Council of Europe (2023). *Artificial Intelligence*. <https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6> Erişim Tarihi: 20.05.2025

Council of Europe (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CETS No. 225, Vilnius, September 5, 2024. <https://rm.coe.int/1680afae3c> Erişim Tarihi: 21.05.2025

Council of Europe. About us. <https://www.coe.int/en/web/about-us> Erişim Tarihi: 25.05.2025

Council of Europe. *The Framework Convention on Artificial Intelligence*. <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> .

Council of the European Union, & European Parliament. (2023, January 23). *European Declaration on Digital Rights and Principles for the Digital Decade* (2023/C 23/01). Publications Office of the EU. <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> (Erişim tarihi: 20.07.2025) .

Danimarka Kişisel Veri Kurumu. Danish Data Protection Act. <https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf> Erişim Tarihi: 23.02.2025

Estonya Hükümeti. Estonian Personal Data Protection Act. <https://www.riigiteataja.ee/en/eli/523012019001/consolide> Erişim Tarihi: 23.02.2025

Euronews. <https://www.euronews.com/> Erişim Tarihi: 23.02. 2025

European Commission (2010, November 4). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF>

European Commission (2012, January 25). *Press release: Commission proposes new rules to strengthen data protection*. https://ec.europa.eu/commission/presscorner/detail/en/memo_14_186

European Commission (2012, January 25). *Press release: GDPR regulation*. https://ec.europa.eu/commission/presscorner/detail/en/memo_14_186 (Erişim Tarihi: 04.05.2025).

European Commission (2012, January 25). *Why do we need an EU data protection reform?* https://ec.europa.eu/commission/presscorner/detail/en/memo_14_186 Erişim Tarihi: 04.05.2025.

European Commission (2015). Data Protection Reform – Questions and Answers [Press release]. https://ec.europa.eu/commission/presscorner/detail/pt/memo_15_6385 Erişim Tarihi: 06.05.2025.

European Commission (2017). Antitrust: Commission Opens Three Investigations Into Suspected Anticompetitive Practices in E-commerce [Press release]. Brussels. https://ec.europa.eu/commission/presscorner/detail/en/ip_17_201 Erişim Tarihi: 02.06.2025

European Commission (2018) Declaration of Cooperation on AI. <https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence> Erişim Tarihi: 19.05.2025

European Commission (2018). Artificial Intelligence for Europe (Communication No. 237 Final). Brussels. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> Erişim Tarihi: 20.05.2025

European Commission (2025). Approval of the content of the draft Communication from the Commission—Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act). Brussels. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> Erişim Tarihi: 22.05.2025.

European Commission (2025). Communication from The Commission To The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions: AI Continent Action Plan (COM(2025) 165 Final). Brussels. <https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan> Erişim Tarihi: 22.05.2025.

European Commission (2025). *European approach to artificial intelligence*. <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

European Commission. (2014). *Towards a circular economy: A zero waste programme for Europe* (COM(2014) 442 final). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014DC0442> Erişim Tarihi: 15.07.2025.

European Commission. *What does data protection by design and by default mean?* https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. Erişim Tarihi: 16.06.2025.

European Court of Human Rights (2024). *Factsheet – Personal Data Protection*. https://www.echr.coe.int/documents/d/echr/fs_data_eng

European Court of Human Rights. *AIHM kararları*. [https://hudoc.echr.coe.int/#%22documentcollectionid2%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\]}](https://hudoc.echr.coe.int/#%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]})

European Court of Justice. *Case law of the Court of Justice of the European Union*. <https://curia.europa.eu/juris/recherche.jsf?language=fr>

European Data Protection Board (2025, January 30). *Article 29 Working Party*. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en

European Data Protection Supervisor (2012). Opinion of the European Data Protection Supervisor on Data Protection Reform Package. Brüksel.

European Parliament & Council (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending various regulations and directives ('Artificial Intelligence Act')*. Official Journal of the European Union, L Series, 2024/1689.. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

European Parliament (2020, June). *Artificial Intelligence: how Does It Work, Why Does It Matter, and What Can We Do About It?* Panel for the Future of Science and Technology. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU\(2020\)641547_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf) Erişim Tarihi: 20.05.2025

European Parliament and Council (2002). *Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*. <https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng> Erişim Tarihi: 18.04.2025.

European Union (1995). *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

European Union (2002). *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector*. <https://eur-lex.europa.eu/eli/dir/2002/58/oj>

European Union (2012). *Consolidated version of the Treaty on the Functioning of the European Union* (C 326/47). <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF>

European Union (n.d.). *EUR-Lex: Access to European Union law*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT>

European Union Agency for Fundamental Rights (FRA), Council of Europe, & European Data Protection Supervisor (EDPS) (2018). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf Erişim tarihi: 25.03.2025.

European Union Agency for Fundamental Rights (FRA), Council of Europe, & European Data Protection Supervisor (EDPS) (2018). *Handbook on European data protection law* (s. 85). Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf Erişim tarihi: 25.03.2025.

Firefox. *Federated learning in Firefox*. <https://florian.github.io/federated-learning-firefox/> Erişim tarihi: 09.06.2025.

Google. *Arama ipuçlarını ve sonuçların Google'daki aramanızla ne şekilde ilgili olduğunu öğrenin*.

<https://support.google.com/websearch/answer/10563935?hl=tr#zippy=%2Cm%C3%BCstehce n-sonu%C3%A7lar%2Carama-terimleri-ve-ilgili-terimler> Erişim tarihi: 02.06.2025.

Google. Privacy Policy. <https://policies.google.com/privacy> Erişim Tarihi: 10.05.2025.

Grasseger, H., and Krogerus, M (2017, January 28). The Data That Turned the World Upside Down. *VICE*. <https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win> Erişim Tarihi: 05.06.2025

High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019). *A Definition of AI: Main Capabilities and Scientific Disciplines*. European Commission, Brussels. <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> Erişim Tarihi: 20.05.2025

High-Level Expert Group on Artificial Intelligence (AI HLEG). *Ethics Guidelines for Trustworthy AI*. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> Erişim tarihi: 20.05.2025.

IBM. AI in Action 2024. <https://www.ibm.com/think/reports/ai-in-action#AI+roadmap> Erişim Tarihi: 19.05.2025.

IBM. Deep Blue. <https://www.ibm.com/history/deep-blue> Erişim Tarihi: 20.05.2025.

IBM. Unstructured Data. <https://www.ibm.com/think/topics/unstructured-data> Erişim Tarihi: 19.05.2025.

IBM. What is AI? https://www.ibm.com/think/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=what%20is%20ai Erişim Tarihi: 19.05.2025.

IBM. What is Intelligent Search? <https://www.ibm.com/think/topics/intelligent-search> Erişim Tarihi: 02.06.2025.

ICO. Information Commissioner's Office. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-information-a-guide/> Erişim Tarihi: 16.05.2025.

International Organization for Standardization. (2015). *Information technology – Vocabulary* (ISO/IEC 2382:2015). <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:ed-1:v2:en> Erişim Tarihi: 15.07.2025.

Kişisel Verileri Koruma Kurulu. (2018, 26 Temmuz). “Kişisel verilere hukuka aykırı erişilmesini önleme” yükümlülüğünü yerine getiremeyen veri sorumlusu hakkında Kurul Kararı No. 2018/91. Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/5365/2018-91> Erişim Tarihi: 26.07.2025.

Kişisel Verileri Koruma Kurulu. (2018, 31 Ocak). “Özel nitelikli kişisel verilerin işlenmesinde veri sorumluları tarafından alınması gereken yeterli önlemler” hakkında Kurul Kararı No. 2018/10. Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/4110/2018-10> Erişim Tarihi: 26.07.2025.

Kişisel Verileri Koruma Kurulu. (2020, 11 Ağustos). 18 yaşını doldurmamış ilgili kişiye ait sağlık raporunun imha edilmesine yönelik ilgili kişinin babası tarafından veri sorumlusuna başvurulması ve cevap alınamaması üzerine ilgili kişinin kendisi tarafından Kurul’a yapılan

şikayet (Kurul Kararı No. 2020/622). Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/6816/2020-622> Erişim Tarihi: 26.07.2025.

Kişisel Verileri Koruma Kurulu. (2023, 19 Ocak). “İlgili kişinin borç bilgisinin ortağı olduğu şirketin kurumsal numaralarına kısa mesaj olarak gönderilmesi” hakkında Kurul Kararı No. 2023/78. Kişisel Verileri Koruma Kurumu. <https://www.kvkk.gov.tr/Icerik/7596/2023-78> Erişim Tarihi: 26.07.2025 .

Kişisel Verileri Koruma Kurumu (2019). Karar No: 2019/273 - Talep edilen kişisel verilerin ölmüş kişiye ait olması sebebiyle reddi. <https://www.kvkk.gov.tr/Icerik/6710/2019-273> Erişim tarihi: 22.02.2025.

Kişisel Verileri Koruma Kurumu (KVKK) (2025). 100 soruda Kişisel Verilerin Korunması Kanunu. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf> Erişim Tarihi: 18.04.2025.

Kişisel Verileri Koruma Kurumu (KVKK) (2025). 2016–2025 yılları arasındaki veri ihlali halinde öngörülen idari para ceza tablosu. <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/634a65ed-62c3-4570-a53f-d413d8735b6a.pdf> Erişim Tarihi: 26.04.2025.

Kişisel Verileri Koruma Kurumu. (2018). Kişisel veri güvenliği rehberi: Teknik ve idari tedbirler. Kişisel Verileri Koruma Kurumu Yayınları. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf Erişim Tarihi: 26.07.2025.

Kişisel Verileri Koruma Kurumu. (2025). Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler , KVKK Yayınları, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf> . Erişim Tarihi: 01.06.2025.

Kişisel Verileri Koruma Kurumu. Veri Sorumlusu ve Veri İşleyen, KVKK Rehberi. <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen> Erişim Tarihi: 26.04.2025.

Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler. Kişisel Verileri Koruma Kurumu Rehber Yayınları, Ankara. <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Duzenlemeler> Erişim Tarihi: 24.04.2025

Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu (2016, 18 Ocak). Türkiye Büyük Millet Meclisi. <https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d26/c006/tbmm26006040ss0117.pdf> Erişim Tarihi: 22.04.2025.

Kişisel Verilerin Korunması Kanunu’na ilişkin uygulama rehberi (2025). KVKK Yayınları (Yayın No: 58), 16–19. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF> Erişim Tarihi: 25.03.2025.

Kore Mevzuat Araştırma Enstitüsü. Intelligent Robots Development and Distribution Promotion Act. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=17399&type=sogan&key=13 Erişim Tarihi: 19.05.2025

McKinsey (2025, 12 March). *The State of AI: How Organizations are Rewiring to Capture Value*. McKinsey & Company. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai/> Eriřim Tarihi: 24.05.2025.

MCLEAN, G (2019, 25 February). Algorithms are Maximising Profits for Online Retailers by Colluding to Keep Prices High. <https://theconversation.com/algorithms-are-maximising-profits-for-online-retailers-by-colluding-to-keep-prices-high-112179> Eriřim Tarihi: 02.06.2025.

Microsoft. *What is a qubit?* Microsoft Azure. <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit/> . Eriřim Tarihi: 17.07.2025.

OECD (n.d.). *Trust in global cooperation: The vision for the OECD for the next decade*. <https://www.oecd.org/en/about/legal/trust-in-global-cooperation-the-vision-for-the-oecd-for-the-next-decade.html> Eriřim tarihi: 24.03.2025.

OECD. (2012). *OECD Economic Outlook, Volume 2012 Issue 2*. OECD Publishing.

OECD. (2016). *Big Data: Bringing Competition Policy to the Digital Era* (OECD Roundtables on Competition Policy Papers, No. 193). OECD Publishing.

OECD. *The OECD AI Principles*. <https://www.oecd.org/en/topics/ai-principles.html> Eriřim Tarihi: 25.05.2025.

Oksijen (2023, 04 Aralık). RTB House: 2024'te erezlerin yerini Yapay Zeka dolduracak. <https://gazeteoksijen.com/bilim-ve-teknoloji/rtb-house-2024te-cerezlerin-yerini-yapay-zeka-dolduracak-195788> Eriřim Tarihi: 01.06.2025.

SAS Institute. *What is big data?* SAS. https://www.sas.com/tr_tr/insights/big-data/what-is-big-data.html Eriřim Tarihi: 18.07.2025.

SAS. *An executive's guide to cognitive computing*. https://www.sas.com/en_us/insights/articles/big-data/executives-guide-to-cognitive-computing.html Eriřim Tarihi: 22.05.2025.

Swiss Confederation (2022). *Federal Act on Data Protection*. <https://www.fedlex.admin.ch/eli/cc/2022/491/en> . Eriřim tarihi: 21.02.2025.

Swiss Confederation (n.d.). *New federal act on data protection (nFADP): Amendments and comparison with previous law*. <https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html> Eriřim tarihi: 21.02.2025.

T.C. Avrupa Birlięi Bařkanlıęı (2025, Ocak 31). *Genel Veri Koruma Tüzüęü (GDPR) Türke eviri*. <https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf>

T.C. Cumhurbaşkanlıęı Dijital Dönüřüm Ofisi & T.C. Sanayi ve Ticaret Bakanlıęı (2024). *Ulusal Yapay Zeka Stratejisi 2024-2025 Eylem Planı*. <https://cbddo.gov.tr/SharedFolderServer/Genel/File/UlusalYapayZekaStratejisi2024-2025EylemPlanı.pdf> Eriřim Tarihi: 17.05.2025

T.C. Cumhurbaşkanlıęı Dijital Dönüřüm Ofisi/T.C. Sanayi Ve Ticaret Bakanlıęı (2021). *Ulusal Yapay Zeka Stratejisi 2021-2025*. <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf> Eriřim Tarihi: 17.05.2025.

TECHTARGET. *What's the difference between chatbots and virtual assistants?* https://www.techtarget.com/searchcio/answer/Whats-the-difference-between-chatbots-and-virtual-assistants?utm_source=chatgpt.com Erişim Tarihi: 01.06.2025.

The Council of Europe (2024, 17 May). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. <https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6> Erişim Tarihi: 20.05.2025.

Ticaret Bakanlığı. *E-ticaret Bilgi Platformu, E-ticarete Giriş*. <https://www.eticaret.gov.tr/cevrimiciegitim/e-ticarete-giris-egitimi-12> Erişim Tarihi: 16.05.2025.

TÜBİTAK BİLGEM. *Üçüncü Dalga Yapay Zeka Teknolojileri*. https://b3lab.org/sayfalar/yapay_zeka-12/ Erişim Tarihi: 18.05.2025.

Türk Dil Kurumu. *Güncel Türkçe Sözlük*. <https://sozluk.gov.tr/> Erişim Tarihi: 31.01.2025.

Türkiye Cumhuriyeti Ticaret Bakanlığı. *Chatbot Kurgusunun Yapılması*. <https://www.eticaret.gov.tr/cevrimiciegitim/chatbot-kurgusunun-yapilmasi-64> Erişim Tarihi: 02.06.2025.

Türkiye Ticaret Bakanlığı, ETBİS. *İstatistikler*. <https://www.eticaret.gov.tr/istatistikler> Erişim Tarihi: 19.05.2025

UK Government (2018). *Data Protection Act 2018*. <https://www.legislation.gov.uk/ukpga/2018/12/enacted> Erişim tarihi: 23.02.2025.

UNESCO (2021). *Recommendation on the Ethics of Artificial Intelligence*. Fransa. <https://unesdoc.unesco.org/ark:/48223/pf0000381137> Erişim Tarihi: 21.05.2025

UNESCO. *İnsan Genomu ve İnsan Hakları Evrensel Bildirgesi*. <https://www.unesco.org.tr/Pages/459/73/%C4%B0nsan%20Genomu%20ve%20%C4%B0nsan%20Haklar%C4%B1%20Evrensel%20Bildirgesi> Erişim Tarihi: 22.03.2025.

United Nations (1948). *Universal Declaration of Human Rights*. <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (Erişim Tarihi: 25.03.2025). Türkçe çevirisi için bkz. HSK. *İnsan Hakları Evrensel Beyannamesi* [Türkçe çeviri]. <https://www.hsk.gov.tr/eklentiler/dosyalar/9a3bfe74-cdc4-4ae4-b876-8cb1d7eeae05.pdf> (Erişim Tarihi: 25.03.2025).

United Nations General Assembly (1990, December 14). *Guidelines for the regulation of computerized personal data files*. <https://www.refworld.org/policy/legalguidance/unga/1990/en/13761> Erişim Tarihi: 25.03.2025

UPWORK (2024, 22 August) *AI Chatbot vs. AI Virtual Assistant: What's the Difference?* <https://www.upwork.com/resources/ai-chatbot-vs-virtual-assistant> Erişim Tarihi: 31.05.2025.

WhatsApp. About. <https://www.whatsapp.com/about>. Erişim Tarihi: 02.05.2025.

World Economic Forum (2011). *Personal Data: The Emergence of a New Asset Class*. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf Erişim Tarihi: 02.05.2025.

World Economic Forum (2016). *The Fourth Industrial Revolution: What It Means, How to Respond*. <https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> Eriřim Tarihi: 02.05.2025.

YARGI KARARLARI VE MAKALE KAYNAKLARI

AİHM Kararları, [https://hudoc.echr.coe.int/tur#{%22documentcollectionid2%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\]}](https://hudoc.echr.coe.int/tur#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}) Eriřim Tarihi: 21.02.2025.

AYM Kararları, <https://kararlarbilgibankasi.anayasa.gov.tr/> Eriřim Tarihi: 30.01.2025.

Cambridge, <https://www.cambridge.org/core/> . Eriřim Tarihi: 30.01.2025.

Dergipark, <https://dergipark.org.tr/en/> Eriřim Tarihi: 30.01.2025.

Harvard Law Review, <https://harvardlawreview.org/> . Eriřim Tarihi: 30.01.2025.

Heinonline, <https://home.heinonline.org/> . Eriřim Tarihi: 30.01.2025.

KVK Kurulu Kararı, <https://www.kvkk.gov.tr/Icerik/5419/Kurul-Kararlari> Eriřim Tarihi: 22.02.2025.

Lexpera, <https://www.lexpera.com.tr/> . Eriřim Tarihi: 30.01.2025.

Resmi Gazete, <https://www.resmigazete.gov.tr/> Eriřim Tarihi: 30.01.2025.

Stanford Law Review, <https://www.stanfordlawreview.org/> . Eriřim Tarihi: 30.01.2025.