Yayın No : 113

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

ÜRETKEN YAPAY ZEKÂ VE KİŞİSEL VERİLERİN KORUNMASI REHBERİ (15 SORUDA)

Kasım 2025

Kısaltmalar Listesi

Bkz.	: Bakınız
GAN	: Çekişmeli Üretken Ağlar
GPT	: Üretken Önceden Eğitilmiş Dönüştürücü
Kanun/6698 sayılı Kanun	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
Kurul	: Kişisel Verileri Koruma Kurulu
Kurum	: Kişisel Verileri Koruma Kurumu
LLM	: Büyük Dil Modeli
ÜYZ	: Üretken Yapay Zekâ
VAE	: Varyasyonel Otomatik Kodlayıcılar
YZ	: Yapay Zekâ

İçindekiler

Yapay Zekâya İlişkin Bazı Kavramlar ve Tanımlar[1]

Açık veri *(open data)*: Açık bir formatta sunulan, herkes tarafından herhangi bir amaç için serbestçe kullanılabilen, yeniden kullanılabilen ve paylaşılabilen veri. *(2019/1024 sayılı Açık Veri Direktifi)*

Algoritma *(algorithm)*: Belirli bir görevi yerine getirmek, belirli bir problemi çözmek veya bir makine öğrenmesi ya da yapay zekâ modeli oluşturmak için tasarlanmış hesaplama prosedürü veya talimat ve kurallar dizisi. *(International Association of Privacy Professionals (IAPP)-Glossary of Privacy Terms)*

Algoritmik karar sistemleri *(algorithmic decision systems)*: Büyük miktarda kişisel verinin analizine dayanarak korelasyonlar çıkarmak veya daha genel olarak, karar vermede faydalı olduğu düşünülen bilgileri türetmek için kullanılan sistemler. *(European Parliamentary Research Service-Understanding Algorithmic Decision-Making: Opportunities and Challenges)*

Büyük dil modeli *(large language model)*: Metin tabanlı görevleri yerine getirmek için karakterler, kelimeler ve ifadeler arasındaki kalıpları ve ilişkileri analiz etmek ve öğrenmek amacıyla, büyük metin veri setleri üzerinde önceden eğitilmiş modeller oluşturmak için derin öğrenme algoritmalarını kullanan bir yapay zekâ türü. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

Büyük veri *(big data)*: Hacim, çeşitlilik, hız ve değişkenlik gibi özelliklerine bağlı olarak, işlenmesi ve anlamlı bir değer üretilmesi için özel teknolojiler ve teknikler gerektiren kapsamlı veri setleri. *(ISO/IEC 22989:2022)*

Dar/zayıf yapay zekâ *(narrow/weak AI)*: Belirli görevleri yüksek yeterlilikle gerçekleştirmek üzere tasarlanmış yapay zekâ sistemleri. *(ISO/IEC 22989:2022)*

Derin kurgu/derin sahte *(deep fake)*[2]: Yapay zekâ tarafından oluşturulan veya değiştirilen, mevcut kişi, nesne, yer, varlık ya da olayları andıran ve bir kişide hatalı şekilde gerçek ya da doğru izlenimi oluşturabilecek nitelikteki görsel, ses veya video içerikleri. *(2024/1689 sayılı AB Yapay Zekâ Tüzüğü)*

Derin öğrenme *(deep learning)*: Makine öğrenmesinin bir alt alanı olup çok sayıda gizli katmana sahip sinir ağlarının eğitilmesi yoluyla zengin hiyerarşik temsiller oluşturulmasına yönelik bir yaklaşım. *(ISO/IEC 22989:2022)*

Doğal dil işleme *(natural language processing)*: Bilgiyi içeriğe dönüştürerek bilgisayarların insan dilini anlamasına, yorumlamasına ve uygulamasına yardımcı olan bir yapay zekâ alt alanı. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

Gözetimli makine öğrenmesi *(supervised machine learning)*: Eğitim sürecinde etiketlenmiş verilerin kullanıldığı makine öğrenmesi türü. *(ISO/IEC 22989:2022)*

---

1 Bu bölümde yer verilen kavramlar, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuattaki tanımlar ile ulusal çalışmalar başta olmak üzere; Avrupa Birliği düzenlemeleri ile Avrupa Veri Koruma Kurulu (EDPB), Avrupa Veri Koruma Denetçisi (EDPS), *International Association of Privacy Professionals* (IAPP) ve benzeri kuruluşların çalışmalarından seçilen yüz kavrama ilişkin tanımın bir araya getirilmesiyle oluşturulan "Kişisel Verilerin Korunması Terimler Sözlüğü" temel alınarak derlenmiş olmakla birlikte, söz konusu çalışmada bulunmayan ilave kavramları da içermektedir. Kurum tarafından yayımlanmış olan bahse konu sözlük çalışmasını görüntülemek için bkz. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/d1e5b8a6-d244-4ab7-a2e6-f36af317b4c2.pdf.

2 Derin öğrenme *(deep learning)* ve sahte *(fake)* kelimelerinin birleştirilmesiyle oluşturulan *"deep fake"* ifadesi için "derin kurgu" ya da "derin sahte" gibi karşılıklar kullanılmakla birlikte, genel kabul görmüş bir Türkçe karşılığı bulunmadığından, bu Rehber'de *"deep fake"* ifadesi tercih edilmiştir.

Gözetimsiz makine öğrenmesi *(unsupervised machine learning)*: Eğitim sürecinde etiketlenmemiş verilerin kullanıldığı makine öğrenmesi türü. *(ISO/IEC 22989:2022)*

Güçlü/yapay genel zekâ *(strong AI/artificial general intelligence)*: Geniş bir görev yelpazesini tatmin edici bir performans düzeyinde yerine getiren yapay zekâ sistemleri. *(ISO/IEC 22989:2022)*

Halüsinasyon *(hallucination)*: Üretken yapay zekâ modellerinin, gerçek görünümü altında görünüşte makul ancak gerçekte yanlış çıktılar oluşturduğu durumlar. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

İnce ayar *(fine-tuning)*: Bir temel modelin, belirli bir görev için gözetimli öğrenme yoluyla daha fazla eğitilmesi süreci. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

İnsan merkezli yapay zekâ *(human-centric AI)*: Yapay zekânın tasarlanması, geliştirilmesi, yerleştirilmesi *(deployment)* ve kullanılmasında insanın refahını, özerkliğini, değerlerini ve ihtiyaçlarını ön planda tutan bir yaklaşım. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

Kara kutu *(black box)*: Yapay zekâ sistemleri tarafından ulaşılan sonuçların üretildiği sürecin ve algoritmanın neden belirli kararları verdiğinin insanlar tarafından tam olarak anlaşılamadığı durumlar. (*European Parliamentary Research Service-EU Gudelines on Ethics in Artificial Intelligence:Context and Implementation)*

Komut *(prompt)*: Bir çıktı üretmesi için yapay zekâ modeli veya sistemine sağlanan bir girdi veya talimat. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

Mahremiyet artırıcı teknolojiler *(privacy-enhancing technologies)*: Bilgi sisteminin işlevselliğini kaybetmeden, kişisel veri işleme faaliyetini ortadan kaldırarak veya azaltarak ya da gereksiz ve/veya istenmeyen şekilde işlenmesini önleyerek mahremiyeti koruyan uyumlu bir bilgi ve iletişim teknolojisi önlemleri sistemi. *(Avrupa Veri Koruma Denetçisi (EDPS) –Glossary)*

Makine öğrenmesi *(machine learning)*: Sistemlerin verilerden veya deneyimlerden öğrenmesini sağlamak için hesaplama teknikleri kullanan bir süreç. *(ISO/IEC 22989:2022)*

Makine öğrenmesi modeli *(machine learning model)*: Girdi verilerine veya bilgilere dayalı olarak çıkarım ya da tahmin üreten matematiksel yapı. *(ISO/IEC 22989:2022)*

Pekiştirmeli öğrenme *(reinforcement learning)*: Bir ortamla etkileşim yoluyla ödülü en üst düzeye çıkaracak en uygun eylem dizisini öğrenme süreci. *(ISO/IEC 22989:2022)*

Profilleme *(profiling)*: Bir gerçek kişiyle ilgili belirli kişisel yönlerin değerlendirilmesi, özellikle söz konusu gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, bireysel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi amacıyla kişisel verilerin kullanılmasını içeren her türlü otomatik kişisel veri işleme biçimi. *(2016/679 sayılı Genel Veri Koruma Tüzüğü)*

Sentetik veri *(synthetic data)*: Bir sistem veya model tarafından oluşturulan, gerçek verinin yapısı ile istatistiksel özelliklerini taklit edebilen ve genellikle gerçek dünyadaki verilerin sınırlı, erişilemez ya da kullanılamayacak kadar hassas olduğu durumlarda, makine öğrenmesi modellerini test etmek veya eğitmek amacıyla kullanılan veri. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

Tasarımdan itibaren mahremiyet *(privacy by design)*: Veri koruma ilkelerine uyum sağlanması amacıyla, veri işleme faaliyetleri ve bilgi sistemlerinin tasarımına veri koruma ve mahremiyetin entegre edilmesini amaçlayan yaklaşım. *(Avrupa Veri Koruma Denetçisi (EDPS)-Our Work By Topics: Privacy By Design)*

Temel model *(foundation model)*: Dil, görme, robotik, akıl yürütme, arama veya insan etkileşimi gibi geniş yetenekleri mümkün kılmak üzere, kapsamlı ve çeşitli veri kümeleri üzerinde eğitilmiş, kullanıma özgü uygulamalar için temel oluşturabilecek büyük ölçekli bir model. *(International Association of Privacy Professionals (IAPP) AI Governance Center-Key Terms for AI Governance)*

Varsayılan olarak mahremiyet *(privacy by default)*: Veri sorumlusunun, kullanıcı müdahalesi olmaksızın varsayılan olarak, yalnızca her bir veri işleme amacı için kesinlikle gerekli olan verilerin işlenmesinin sağlanmasını öngören yaklaşım. *(Avrupa Veri Koruma Denetçisi (EDPS)-Our Work By Topics: Privacy By Default)*

Yapay sinir ağı *(artificial neural network)*: Ayarlanabilir ağırlıklara sahip bağlantılarla birbirine bağlanmış bir veya daha fazla nöron katmanından oluşan, girdi verilerini alan ve bir çıktı üreten ağ. *(ISO/IEC 22989:2022)*

Yapay süper zekâ *(artificial superintelligence)*: Bilimsel yaratıcılık, genel bilgelik ve sosyal beceriler de dâhil olmak üzere, hemen her alanda en iyi insan zekâsından çok daha üstün olan yapay zekâ sistemleri. *(Nick Bostrom-How Long Before Superintelligence?)*

Yapay zekâ *(artificial intelligence-AI)*: Bir bilgisayarın veya bilgisayar kontrolündeki bir robotun çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyeti; dinamik ve belirsiz ortamlarda akıl yürütme, anlam keşfetme, genelleme veya geçmiş deneyimlerden öğrenme gibi insanlara özgü bilişsel kabiliyetlerle donatılmış sistemler. *(Ulusal Yapay Zekâ Stratejisi 2021-2025)*

Yapay zekâ etmeni *(AI agent)*: Çevresini algılayan, bu çevreye tepki veren ve hedeflerine ulaşmak için eylemlerde bulunan otomatik bir etmen. *(ISO/IEC 22989:2022)*

Yapay zekâ geliştiricisi *(AI developer)*: Yapay zekâ sistemlerine ait her türlü ürün için içerik ve uygulama geliştiren gerçek veya tüzel kişi. *(Kişisel Verileri Koruma Kurumu-Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler)*

Yapay zekâ modeli *(AI model)*: Kendi başına bir yapay zekâ sistemi oluşturmayan, ancak genellikle yapay zekâ sistemlerine entegre edilerek bu sistemlerin temel bileşenlerinden birini teşkil eden yapı. *(Avrupa Komisyonu-AI Act Service Desk-Frequently Asked Questions)*

Yapay zekâ servis sağlayıcısı *(AI service provider)*: Yapay zekâ tabanlı sistemler, veri toplama sistemleri, yazılımlar ve cihazlar kullanarak ürün ve/veya hizmet sunan gerçek veya tüzel kişi. *(Kişisel Verileri Koruma Kurumu-Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler)*

Yapay zekâ sistemi *(AI system)*: Değişken düzeylerde özerklikle çalışacak şekilde tasarlanmış, yerleştirme *(deployment)* sonrasında uyarlanabilirlik gösterebilen ve aldığı girdiler doğrultusunda açık veya örtülü hedeflere uygun olarak tahmin, içerik, tavsiye veya kararlar gibi çıktılar üreten, bu çıktılarla fiziksel veya sanal ortamları etkileyebilen makine tabanlı sistem. *(2024/1689 sayılı AB Yapay Zekâ Tüzüğü)*

Yarı gözetimli makine öğrenmesi *(semi-supervised machine learning)*: Eğitim sürecinde hem etiketlenmiş hem de etiketlenmemiş verilerin kullanıldığı makine öğrenmesi türü. *(ISO/IEC 22989:2022)*

Amaç ve Kapsam

Dijital teknolojiler, yaşamın hemen her alanında köklü ve çok yönlü bir dönüşümü beraberinde getirmiştir. Bu dönüşüm, yalnızca üretim araçları ya da iletişim biçimleriyle sınırlı kalmamış; aynı zamanda toplumsal yapıları, karar alma süreçlerini ve bireylerin gündelik yaşam alışkanlıklarını da etkilemiş ve yeniden şekillendirmiştir. Bu sürecin en dikkat çekici unsurlarından biri ise Yapay Zekâ (YZ) teknolojilerinin hızlı gelişimi ve yaygınlaşmasıdır.

YZ sistemleri, büyük ve karmaşık veri setlerini analiz etme, örüntüleri tanıma ve öngörüde bulunma kapasiteleri sayesinde dijital dönüşümün temel bileşenlerinden biri hâline gelmiştir. Sağlık hizmetlerinden finansa, eğitimden ulaşıma kadar birçok alanda etkili biçimde kullanılan bu sistemler; veri temelli karar alma süreçlerini güçlendirme, kişiselleştirilmiş hizmetler sunma ve çok boyutlu problemlere çözüm üretme potansiyeli ile iş süreçlerini dönüştürmekte ve yenilikçi uygulamalara zemin hazırlamaktadır.

YZ teknolojilerinin sunduğu fırsatların yanı sıra, bu sistemlerin kullanımına bağlı olarak gündeme gelen etik, toplumsal ve hukuki sorular da önemini korumaktadır. Özellikle algoritmaların işleyişine dair şeffaflık eksikliği, karar alma süreçlerinin denetlenebilirliği, ayrımcılık riski, ön yargıların yeniden üretimi ve hesap verebilirliğin sınırları gibi hususlar, YZ sistemlerinin geniş ölçekte benimsenmesi sürecinde dikkatle ele alınması gereken başlıca konular arasında yer almaktadır.

Bu hususlar gündemdeki yerini korurken, son yıllarda YZ alanında yaşanan gelişmeler, teknolojik inovasyon açısından yeni bir dönemin kapılarını aralamıştır. Bu bağlamda öne çıkan en çarpıcı gelişme, doğal dil girdilerine dayalı olarak insan üretimine benzer içerikler oluşturabilme kapasitesiyle dikkat çeken Üretken Yapay Zekâ (ÜYZ) sistemlerinin yükselişidir. ÜYZ sistemleri; mevcut verilerden hareketle metin, görsel, ses, video veya yazılım kodu gibi çeşitli formatlarda içerik üretebilme kapasiteleri ile geleneksel YZ uygulamalarının sınırlarını aşmaktadır.

Bu sistemler, zamanla daha geniş kullanıcı kitleleri tarafından benimsenmekte ve eğitimden sağlığa, yazılım geliştirmeden medya ve eğlence sektörüne kadar pek çok alanda önemli katkılar sağlamaktadır. Bu çerçevede ÜYZ uygulamaları, bireysel ve kurumsal düzeyde yenilikçi fırsatlar sunmakla birlikte etik, hukuki ve toplumsal düzeyde ele alınması gereken çok yönlü riskleri de beraberinde getirmektedir.

Söz konusu fırsatlar ve riskler büyük ölçüde, bu sistemlerin geliştirilmesi ve kullanılmasına ilişkin süreçlerde işlenen veri kümelerinin niteliğine ve bu verilerin nasıl işlendiğine bağlı olarak şekillenmektedir. Bu bağlamda, bahse konu sistemlerin öğrenme süreçleri, çıktı üretme kapasiteleri ve genel işleyişleri, kullanılan verilerin yapısal özellikleri ve içerdiği bilgi türleriyle ilişkilidir. Bu verilerin önemli bir bölümünü ise, geleneksel YZ sistemlerinde olduğu gibi, kişisel veriler oluşturmaktadır.

Bu durum, kişisel verilerin korunmasını ÜYZ sistemlerinin tasarımından uygulanmasına kadar tüm aşamalarda gözetilmesi gereken temel bir unsur hâline getirmektedir. Zira teknolojik gelişmeler ile bireylerin mahremiyetinin korunması arasında kurulacak dengeli bir ilişki, yalnızca bireylerin hak ve özgürlüklerinin güvence altına alınmasına hizmet etmekle kalmayacak, aynı zamanda toplumun söz

konusu teknolojilere duyduğu güveni de pekiştirecektir. Bu bağlamda, ÜYZ sistemlerinin insan haklarına ve temel özgürlüklere saygılı, şeffaf, denetlenebilir ve insan merkezli bir yaklaşımla geliştirilmesi ve uygulanması büyük önem taşımaktadır.

Bu Rehber'de; ÜYZ sistemlerinin kişisel verilerin korunması bağlamında ortaya çıkarabileceği etkilerin değerlendirilmesi ve bu sistemlerin geliştirilmesi ile kullanılmasında bireylerin mahremiyetine saygılı bir yaklaşımın teşvik edilmesi amaçlanmaktadır. Bu doğrultuda, sistemin yaşam döngüsü boyunca gerçekleştirilen kişisel veri işleme faaliyetleri bakımından, veri sorumlusu niteliğini haiz aktörlere yol gösterilmesi hedeflenmektedir.

Bu amaç doğrultusunda öncelikle; ÜYZ sistemlerinin içerik üretim süreci, yaşam döngüsünün hangi aşamalardan oluştuğu, kullanım alanları ve kullanımının ne tür riskler taşıdığı gibi temel hususlara değinilmektedir. Devamında, bu sistemler aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetleri, 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun/Kanun) çerçevesinde ele alınmaktadır. Son olarak, günlük hayatta ÜYZ uygulamalarından yararlanırken kişisel verilerin korunması açısından bireylerin dikkat etmesi gereken hususlara ve bu teknolojileri kullanan çocuklara yönelik olarak ebeveynler tarafından alınabilecek önlemlere ilişkin değerlendirmelere yer verilmektedir.

1. Üretken Yapay Zekâ Nedir?

Genel olarak bakıldığında "üretken/üretici yapay zekâ" *(generative artificial intelligence)*; büyük ölçekli veri kümeleri üzerinde eğitilen ve kullanıcı tarafından girilen istem ya da komuta *(prompt)* yanıt olarak metin, görsel, video, ses veya yazılım kodu gibi farklı formatlarda içerikler üretebilen YZ türünü ifade etmektedir. Bu sistemler, mevcut verilerdeki örüntüleri/kalıpları *(pattern)* tanımlamak amacıyla yapay sinir ağları ve derin öğrenme algoritmalarını kullanan, bu sayede yeni ve bağlama uygun içerikler üretebilen bir yapıya dayanmaktadır[3].

ÜYZ, temelde geleneksel YZ teknolojilerindeki ilerlemeler üzerine inşa edilmiş olmakla birlikte, geleneksel sistemlerden farklı olarak tamamen yeni içerikler üretebilme kapasitesine sahiptir. Bu bağlamda, geleneksel YZ modelleri genellikle belirli görevleri yerine getirmek üzere tasarlanmakta ve görece sınırlı veri kümeleri üzerinde eğitilmekte iken; ÜYZ modelleri, esnek ve çok yönlü bir yapıyla, birden fazla işlevi gerçekleştirebilecek şekilde yapılandırılmaktadır.

Kriterler	**Geleneksel/Klasik YZ** ***(Conventional AI)***	**ÜYZ** ***(Generative AI)***
Amaç nedir?	Önceden tanımlanmış bir veri kümesi kullanılarak belirli problemleri çözmek veya önceden belirlenmiş görevleri yerine getirmektir.	Yeni içerikler (metin, görsel, müzik vb.) üretmek ve girdi olarak kullanılan veri kümesinde yer almayan özgün çıktılar elde etmektir.
YZ modeli nasıl eğitilmektedir?	Eğitim süreci için yapılandırılmış büyük veri kümelerinden örüntüler öğrenir ve bu örüntüleri tahminlerde bulunmak ya da belirli görevleri yerine getirmek için kullanır.	Yapılandırılmamış veri kümeleri aracılığıyla örüntüler öğrenir. Model, belirli iş kullanımlarına yönelik olarak ince ayar *(fine-tuning)* yapılmak üzere sürekli olarak eğitilebilir.
YZ modeli, girdi verilerinden öğrenmek için ne tür bir algoritma kullanır?	Genellikle kural tabanlı sistemler, karar ağaçları ve benzer modeller üzerinde çalışır. Verideki temel örüntüleri öğrenebilir; ancak algoritmanın etkin bir şekilde çalışabilmesi için daha fazla ön işlemeye ihtiyaç duyar.	Farklı türde girdileri işleyebilen ve verideki temel ilişkiler ile örüntüleri öğrenebilen esnek sinir ağı algoritmaları kullanır.
YZ modeli genellikle nasıl kullanılır?	Görüntü tanıma, öneri sistemleri, anomali tespiti, metin sınıflandırma ve risk tahmin sistemleri gibi uygulamalarda kullanılır.	Sanat, müzik, hikâye anlatımı, içerik üretimi, görsel sentezi, metin ve video üretimi ile mantıksal çıkarım gibi görevlerde kullanılır.
YZ modeli nasıl değerlendirilir?	Genellikle doğruluk, kesinlik ve duyarlılık gibi ölçütleri esas alan, göreve özgü performans metrikleriyle değerlendirilir.	ÜYZ'nin çıktıları, daha öznel ve insan yargısına bağlı nitelikte olabilmektedir. Çıktıların güvenilirliğinin değerlendirilmesi önem taşımaktadır.

Tablo 1: Geleneksel YZ ile ÜYZ Teknolojisinin Karşılaştırılması[4]

3 Baum, D.: Generative AI and LLMs, Snowflake Special Edition, New Jersey 2024, s.3.

4 California Government Operations Agency: Benefits and Risks of Generative Artificial Intelligence Report, (https://www.govops.ca.gov/wp-content/uploads/sites/11/2023/11/GenAI-EO-1-Report_FINAL.pdf), s. 4-5.

ÜYZ ile çeşitli alanlarda birçok türde içerik oluşturulabilmekte olup bunlardan bazıları şu şekildedir:

Metin Oluşturma: ÜYZ modellerinin en yaygın kullanım alanlarından biri metin üretimidir. Bu modeller, doğal dil işleme *(natural language processing-NLP)* algoritmalarını kullanarak insan dilini anlamlandırmakta ve kullanıcı girdileri doğrultusunda özetleme, makale yazma, hikâye oluşturma, soru-cevap formatında içerik üretme gibi çeşitli görevleri yerine getirebilmektedir. Bu bağlamda içerik oluşturma, müşteri hizmetleri sohbet botları ve dil tabanlı inovatif uygulamalar gibi alanlarda ÜYZ modellerinden önemli faydalar elde edilmektedir.

Görsel/Video Oluşturma: ÜYZ, kullanıcı girdilerinden yola çıkarak görseller ve videolar oluşturabilen modelleriyle bu alanda önemli bir rol oynamaktadır. Bu modeller, büyük ölçekli görsel veri kümeleri üzerinde eğitilerek sanat eserleri, animasyonlar, illüstrasyonlar, konsept tasarımlar ve video içerikleri gibi çeşitli görsel materyaller üretme kapasitesine sahiptir. Metinsel açıklamalardan görsel çıktılar üretilebilmesi, dijital sanat, grafik tasarım ve reklamcılık gibi alanlarda yenilikçi çözümler sunmaktadır.

Ses/Müzik Oluşturma: ÜYZ, ses ve müzik üretimi alanında da önemli bir kullanım potansiyeline sahiptir. Bu modeller, mevcut ses verileri üzerinde eğitilerek yeni ses efektleri, konuşmalar veya müzik eserleri oluşturabilmektedir. Özellikle eğlence sektörü, oyunlar ve dijital içerik üretimi gibi alanlar, bu teknolojinin sunduğu yenilikçi çözümlerden en çok faydalanılan alanlar arasında yer almaktadır.

ÜYZ'nin görsel, video ve ses üretimindeki bir diğer uygulama alanı, *deep fake* teknolojisidir. *Deep fake;* YZ tarafından oluşturulan veya değiştirilen, mevcut kişi, nesne, yer, varlık ya da olayları andıran ve bir kişide hatalı şekilde gerçek ya da doğru izlenimi oluşturabilecek nitelikteki görsel, ses veya video içeriklerini ifade etmektedir. *(2024/1689 sayılı AB Yapay Zekâ Tüzüğü-AI Act, m.3/60)*

ÜYZ tabanlı bu teknoloji, mevcut görsel, ses ve video verilerinden yola çıkarak bireylerin yüz ifadelerini ve seslerini değiştirebilen ya da bir kişinin gerçekçi bir taklidini oluşturabilen yöntemleri kapsamaktadır. Farklı kullanım alanlarında yenilikçi çözümler sağlayabilen *deep fake,* kötüye kullanıldığında ise mahremiyet, itibar ve güvenlikle ilgili sorunlara yol açma potansiyeline sahiptir. Bu nedenle, *deep fake* teknolojisinin sunduğu imkânların yanı sıra beraberinde getirdiği risklerin de göz önünde bulundurulması önem taşımaktadır.

Yazılım Kodu Oluşturma: ÜYZ, yazılım geliştirme süreçlerini hızlandırmak ve kolaylaştırmak amacıyla da kullanılmaktadır. Bu modeller; yeni kod üretme, programlama dilleri arasında çeviri yapma, kod tamamlama, işlevsel modüller geliştirme, hata ayıklama ve optimizasyon gibi çeşitli görevleri yerine getirebilmektedir.

Sentetik Veri Oluşturma: ÜYZ, sentetik veri oluşturma süreçlerinde de etkin bir şekilde kullanılmaktadır. Sentetik veri, bir sistem veya model tarafından oluşturulan, gerçek verinin yapısı ile istatistiksel özelliklerini taklit edebilen ve genellikle gerçek dünyadaki verilerin sınırlı, erişilemez ya da kullanılamayacak kadar hassas olduğu durumlarda, makine öğrenmesi modellerini test etmek veya eğitmek amacıyla kullanılan verileri ifade etmektedir[5]. ÜYZ, çeşitli formatlarda sentetik veri üreterek, eğitim veri kümelerinin zenginleştirilmesine ve YZ modellerinin performansının artırılmasına katkı sağlayabilmektedir.

5 International Association of Privacy Professionals (IAPP): Key Terms for AI Governance, (https://iapp.org/media/pdf/resource_center/key_terms_for_ai_governance.pdf), s. 10.

2. Üretken Yapay Zekâ Sistemlerinde İçerik Üretimi Nasıl Gerçekleşmektedir?

Çoğu YZ sisteminde olduğu üzere, ÜYZ sistemleri de veri odaklı bir şekilde işleyiş göstermektedir. Ancak içerik üretiminde kullanılan bu modellerin tasarımı, kullanım amacı ve bağlamı, üretilecek içeriğin türüne göre önemli ölçüde farklılık gösterebilmektedir.[6]

Makine Öğrenmesi *(Machine Learning-ML)*		Sistemlerin verilerden öğrenerek, açıkça programlanmaya gerek olmaksızın, belirli görevlerdeki performansını otomatik olarak geliştiren bir YZ türüdür.
Yapay Sinir Ağı *(Artificial Neural Network-ANN)*		İnsan beyninin yapısından ve işleyişinden (örneğin, nöronlar arasındaki sinaptik bağlantılardan) esinlenen bir makine öğrenmesi yapısıdır.
Metin Üreten YZ	Genel Amaçlı Dönüştürücüler *(General-purpose Transformers)*	Verilerin farklı kısımlarına odaklanarak bunların birbiriyle nasıl ilişkili olduğunu belirleyebilen bir yapay sinir ağı türüdür.
	Büyük Dil Modelleri *(Large Language Models-LLM)*	Büyük miktarda metin verisi üzerinde eğitilmiş ve genellikle dönüştürücü mimarisine dayanan modellerdir.
	Üretken Önceden Eğitilmiş Dönüştürücü *(Generative Pre-trained Transformer-GPT)*	Modelin, dilin inceliklerini yakalamasını ve bağlama duyarlı, tutarlı metinler üretmesini sağlayacak şekilde, büyük miktarda veri üzerinde önceden eğitilmiş bir büyük dil modeli türüdür.
Görsel Üreten YZ	Çekişmeli Üretken Ağlar *(Generative Adversarial Networks-GANs)* Varyasyonel Otomatik Kodlayıcılar *(Variational Autoencoders-VAEs)*	Görsel üretmede kullanılan sinir ağı türleridir.

Tablo 2: ÜYZ'de Kullanılan Başlıca Yöntemler[7]

6 Belirtildiği üzere, ÜYZ çeşitli türlerde içerik oluşturabilmekle birlikte, en yaygın kullanım alanlarını temsil etmesi nedeniyle bu Rehber'de metin ve görsel üretim süreçlerine odaklanılmıştır.

7 United Nations Educational, Scientific and Cultural Organization (UNESCO): Guidance for Generative AI in Education and Research, (https://unesdoc.unesco.org/ark:/48223/pf0000386693), s. 8.

Genel olarak bakıldığında, ÜYZ sistemlerinin içerik üretme kapasitesinin temelinde, çok büyük veri kümeleri üzerinde eğitilen ve çeşitli görevleri yerine getirebilecek şekilde tasarlanan "temel modeller" *(foundation models)* yer almaktadır. Bu modeller, belirli görevler için özelleştirilen YZ uygulamalarının inşasında bir yapı taşı işlevi görmektedir. Kamuya açık bilgi kaynaklarını da kapsayacak şekilde geniş veri kümeleriyle eğitilen temel modeller; görsel, ses, video ve dil gibi karmaşık yapıları temsil edebilme kapasitesine sahiptir. Bu modeller, "ince ayar" *(fine-tuning)* süreçleriyle belirli görev ya da uygulamalara uyarlanabilmekte ve farklı türde içeriklerin üretiminde etkili biçimde kullanılabilmektedir.[8]

A. Metin Üretim Süreci

Temel modeller arasında, özellikle dil tabanlı içeriklerin üretiminde kullanılan "büyük dil modelleri" *(Large Language Models-LLM)* önemli bir yer tutmaktadır. LLM'ler, kimi zaman milyarlara varan kelimeden oluşan büyük miktarda metin verisi üzerinde eğitilmiş, kelimeler ve ifadeler arasındaki örüntüler ve ilişkileri temel alarak çok çeşitli girdilere doğal dilde yanıtlar üretebilen belirli bir temel model türüdür[9]. Günümüzde LLM'ler; içerik üretimi, mantıksal çıkarım, dil çevirisi, kod yazımı, özetleme ve bilgi arama gibi pek çok alanda kullanılmaktadır.

Bu modeller, genellikle sinir ağı mimarisindeki düğümler *(nodes)* ve katmanlar *(layers)* arasındaki bağlantıları tanımlamak ve bu bağlantılara ağırlık atamak için kullanılan, sayısal değerlerden oluşan önemli sayıda parametreye sahiptir. Bu parametreler, çeşitli değerlerin ağırlıklarını değiştirmek üzere ayarlanabilir ve bu da modelin, istem ile veri içerisindeki önceliklerini ve çeşitli veri noktalarını, kelimeleri ve bağlantıları nasıl yorumladığını doğrudan etkiler. LLM'ler ayrıca, bir kelime dizisinde bir sonraki kelimeyi tahmin etmek için de bu parametreleri kullanır. Bu süreçte model, istemde yer alan kelimelerden sonra gelme olasılığı en yüksek olan kelimeyi tahmin eder ve ardından, tahmin edilen bu kelimeden sonra gelme olasılığı en yüksek olanı belirler. Bu işlem, model en olası örüntüyü tamamladığına inanana kadar devam eder. Bu bağlamda, bir ÜYZ modelinin çıktısının, modelin verilen girdiye karşılık en olası sonucu tahmin etmesiyle oluştuğunu söylemek mümkündür.[10]

Günümüzde bu mekanizma, "üretken önceden eğitilmiş dönüştürücü" *(Generative Pre-trained Transformer-GPT)* olarak bilinen modellerde yaygın olarak uygulama alanı bulmaktadır. GPT, insan diline benzer metinler üretmek amacıyla derin öğrenme yöntemlerinden yararlanan bir büyük dil modeli türüdür. Bu modellerin gücü, temelde iki bileşene dayanmaktadır.[11] Bunlardan ilki, modele etiketlenmemiş verilerdeki örüntüleri tanımayı ve bu örüntüleri yeni girdilere uygulamayı öğreten üretken ön eğitim *(generative pre-training)* sürecidir. GPT modelleri bazı sürümlerde trilyonlara varan parametreyle eğitilmekte olup bu parametreler, modelin eğitim verilerinden öğrendiği ve yeni veriler üzerinde tahmin yapabilmesini sağlamak üzere eğitim süreci boyunca ayarladığı içsel değişkenlerdir. Diğer bileşen ise modelin bir girdi dizisinin tüm bileşenlerini eş zamanlı olarak işleyebilmesini

8 European Data Protection Supervisor (EDPS): Generative AI and the EUDPR: First EDPS Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems, (https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf), s. 4.
9 EDPS, Generative AI and the EUDPR, s. 4.
10 Baker, P.: Generative AI, 1. Baskı, New Jersey, 2025, s. 7-8.
11 Belcic, I. / Stryker, C.: What is GPT (Generative Pretrained Transformer), (https://www.ibm.com/think/topics/gpt).

sağlayan dönüştürücü *(transformer)* mimarisidir. Dönüştürücü mimari, kelimeler arasındaki mesafeye bakılmaksızın cümlelerin bütünsel olarak analiz edilebilmesini ve bağlamsal ilişkilerin etkili bir şekilde kavranabilmesini sağlamaktadır. Bu yetkinlik, modelin her bir kelimenin bağlam içerisindeki göreli önemini belirlemesine olanak tanıyan "öz-dikkat" *(self-attention)* mekanizmasından kaynaklanmakta olup bu sayede model, insanların bağlam için bir cümlenin farklı kısımlarına odaklanmasını taklit edebilmektedir.[12] Böylelikle yalnızca sözcük sırasına bağlı kalınmaksızın, uzak konumlanmış ifadeler arasında da anlamlı bağlantılar kurularak bağlamsal olarak tutarlı yanıtlar üretilebilmesi mümkün hâle gelmektedir.

Bu çerçevede, GPT'nin eğitim sürecinin ardından bir isteme yanıt olarak metin üretme süreci şu şekilde özetlenebilir:[13]

1) Kullanıcı tarafından girilen istem, *"token"* olarak adlandırılan daha küçük birimlere bölünür.
2) GPT, isteme uygun tutarlı bir yanıt oluşturabilecek olası kelimeleri veya ifadeleri tahmin etmek için istatistiksel örüntülerden yararlanır.

- GPT, önceden oluşturulmuş geniş veri modelinde (internetten ve diğer kaynaklardan toplanan metinlerden oluşan) sıkça birlikte görülen kelimeleri ve ifade örüntülerini tanımlar.
- Bu örüntülere dayanarak GPT, belirli bir bağlamda belirli kelimelerin ya da ifadelerin görünme olasılıklarını tahmin eder.
- Varsa önceki bağlamdan üretilen olasılık dağılımına göre, yoksa da örneklemeye dayalı ve rastgelelik içerebilecek bir başlangıç tahminiyle GPT, bu olasılıkları kullanarak yanıt içerisinde bir sonraki kelime ya da ifadeyi tahmin eder.

3) Tahmin edilen kelimeler ya da ifadeler, okunabilir bir metne dönüştürülür.
4) Oluşturulan metin, rahatsız edici veya zararlı içeriklerin kaldırılması amacıyla "koruma mekanizmaları" *(guardrails)* olarak bilinen filtreleme sisteminden geçirilir.
5) 2 ila 4. adımlar, yanıt tamamlanana kadar tekrarlanır. Yanıt, maksimum *token* sınırına ulaşıldığında ya da önceden tanımlanmış durdurma kriterleri karşılandığında tamamlanmış kabul edilir.
6) Oluşturulan yanıt, okunabilirliği artırmak amacıyla biçimlendirme, noktalama ve diğer iyileştirmelere tabi tutulur. (Örneğin; "Elbette", "Tabii ki" veya "Üzgünüm" gibi insanlara özgü ifadelerle yanıta başlayacak şekilde.)

B. Görsel Üretim Süreci

Metin üretimine odaklanan modellerin yanı sıra, ÜYZ sistemlerinin bir diğer önemli uygulama alanı da görsel üretimidir. Görsel üretimine yönelik geliştirilen yöntemlerin örnekleri arasında, "varyasyonel otomatik kodlayıcılar" *(Variational Autoencoders-VAE)* ile "çekişmeli üretken ağlar" (*Generative Adversarial Networks-GAN*) yer almaktadır. VAE'ler, temel haliyle, eğitim verilerinden anlamlı gizli

12 What is GPT?, (https://cloud.google.com/discover/what-is-gpt).
13 UNESCO, Guidance for Generative AI in Education and Research, s. 9-10.

değişkenleri ayırmayı öğrenen bir "kodlayıcı" *(encoder)* ile bu değişkenleri, daha düşük boyutlu bir temsil alanı olan "gizli uzay"da *(latent space)* temsil eden ve ardından bu değişkenleri kullanarak girdiyi yeniden oluşturan bir "kod çözücü"den *(decoder)* oluşan derin öğrenme modelleridir.[14]

Görsel üretiminde kullanılan diğer bir yöntem olan GAN'lar ise birbirini alt etmeye çalışarak öğrenen bir çift sinir ağından oluşan bir makine öğrenmesi varyasyonudur. Bu ağlardan ilki olan "üretici" *(generator)*, rastgele gürültüden başlayarak insan tarafından programlanan kurallara dayanarak bir çıktı (örneğin, bir görsel) üretmeye çalışır. "Ayırt edici/ayırıcı" *(discriminator)* olarak adlandırılan diğer ağ ise çıktının belirli kriterlere göre (örneğin, görselin nasıl olması gerektiği) doğru olup olmadığını değerlendirecek şekilde programlanmıştır. Ayırt edici ağ, üreticinin oluşturduğu çıktıyı inceler ve temel olarak bunun gerçek veya doğru olup olmadığını belirlemeye çalışır. Döngünün başında üretilen ilk çıktıların hedeflenen nitelikten oldukça uzak olması muhtemeldir. Ancak ayırt edici ağın verdiği geri bildirimler programa entegre edilir ve üretici ağ yeni çıktılar oluşturmaya devam eder. Bu geri bildirim döngüsü, üretici ağın, ayırt edici ağın kalite beklentilerini karşıladığını düşündüğü veriler üretinceye kadar devam eder. Görsel örneğinde bu durum, üretilen görselin gerçek olduğu konusunda üretici ağın ayırt edici ağı "kandırması" anlamına gelir.[15]

Genel olarak *deep fake* teknolojilerinde başlıca yöntemlerden biri olan bu yapı, farklı içerikler oluşturulabilmesine imkân sağlamaktadır. Örneğin, popüler müziklerden veya tek bir sanatçının eserlerinden oluşan bir veri kümesi üzerinde eğitilmiş bir GAN, orijinal müziğin yapısını ve karmaşıklığını takip eden yeni müzik eserleri üretebilmektedir.

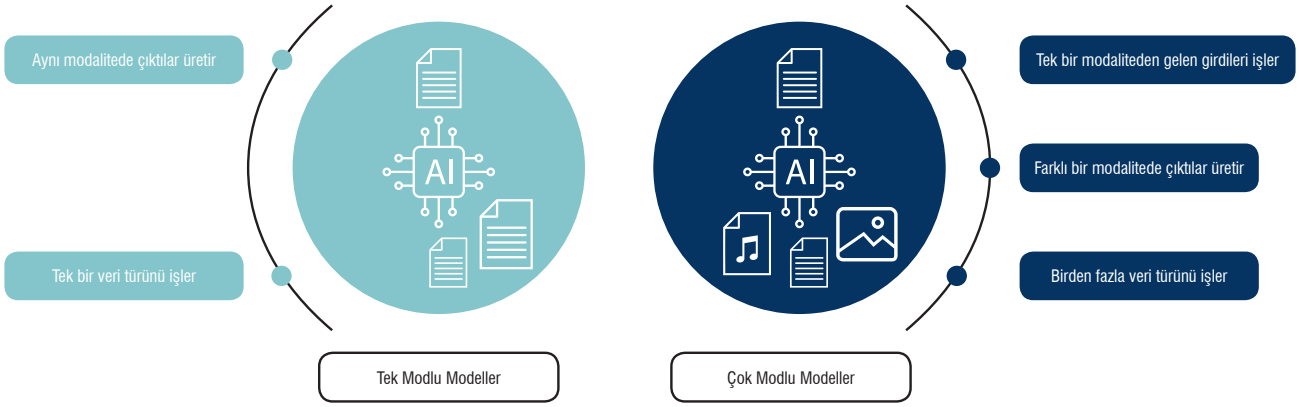
C. ÜYZ Modellerinin Temel Sınıflandırması

Genel olarak ÜYZ modelleri, "tek modlu modeller" *(unimodal models)* ile "çok modlu modeller" *(multimodal models)* olmak üzere iki temel kategori altında sınıflandırılmaktadır. "Modalite" *(modality)* terimi, modelin işlediği veri türünü ifade etmektedir. Bu doğrultuda tek modlu modeller, yalnızca tek bir türde veri işleyen ve yine aynı türde çıktı üreten yapılardır. Örneğin, yalnızca metin girdisi alıp metin çıktısı üreten büyük dil modelleri bu kategori altında değerlendirilmektedir.

Buna karşılık çok modlu modeller, birden fazla veri türünü işleyebilmekte ve bir veri türünden girdiyi alarak farklı bir veri türünde çıktı üretebilmektedir. Bu yönüyle çok modlu modeller; metin, görsel, ses gibi farklı türde verileri işleyebilme kapasitesine sahiptir. Örneğin, çok modlu bir model "uçan bir bisiklet" gibi metinsel bir girdiyi analiz ederek bu betimlemeye uygun bir görsel içerik oluşturabilmektedir. Benzer şekilde metin, ses ve görsel gibi farklı veri türlerinin bir arada işlenmesiyle, örneğin akan bir nehrin sesiyle desteklenen bir şehir manzarası gibi sanatsal çıktılar üretilebilmektedir.

14 Bergmann, D. / Stryker, C.: What is a Variational Autoencoder?, (https://www.ibm.com/think/topics/variational-autoencoder).

15 Future of Privacy Forum (FPF): The Spectrum of Artificial Intelligence-Companion to the FPF AI Infographic, (https://fpf.org/wp-content/uploads/2021/08/FPF-AIEcosystem-Report-FINAL-Digital.pdf), s. 17.



Şekil 1: Tek Modlu Modeller ile Çok Modlu Modeller

"Space Opera Theater" (Théâtre D'opéra Spatial) isimli bu görsel, Jason M. Allen tarafından Midjourney adlı ÜYZ aracı kullanılarak oluşturulmuştur. 2022 yılında ABD'de düzenlenen bir sanat yarışmasında "dijital sanatlar" kategorisinde birincilik ödülüne layık görülen[16] bu görselin üretim sürecinde, 600'ü aşkın metin tabanlı komut dizisinin (prompt) kullanıldığı bilgisine kamuya açık kaynaklardan ulaşılabilmektedir.

16 An A.I.- Generated Picture Won an Art Prize. Artists Aren't Happy, (https://www.nytimes.com/2022/09/02/technology/ai-artificial-intelligence-artists.html).

3. Bir Üretken Yapay Zekâ Modelinin Yaşam Döngüsü Hangi Aşamalardan Oluşmaktadır?

ÜYZ modellerinin tasarımı, geliştirilmesi ve uygulanması; birbirini izleyen ve işlevsel bütünlük taşıyan süreçlerden oluşmakta olup bu süreçler, teknolojinin güvenli ve sürdürülebilir şekilde hayata geçirilmesinde belirleyici bir rol oynamaktadır.

Bu çerçevede, bir ÜYZ modelinin yaşam döngüsünün temel aşamalarının genel olarak şu şekilde belirtilmesi mümkündür:[17]

Şekil 2: Bir ÜYZ Modelinin Yaşam Döngüsünün Temel Aşamaları

- ÜYZ modellerinin yaşam döngüsü, modelin kullanım amacı ve kapsamının belirlenmesiyle başlamaktadır. Bazı durumlarda, sürece uygun bir temel model belirlemek mümkün olabilirken, kimi durumlarda ise modelin sıfırdan geliştirilmesi gerekebilmektedir.[18]

- ÜYZ modellerinin geliştirilmesinde ikinci aşama, modelin eğitimi için gerekli verilerin toplanması ve ön işlemeye tabi tutulmasıdır. Bu modellerin eğitilmesinde genellikle büyük miktarda veriye ihtiyaç duyulması nedeniyle, verilerin toplanmasında çeşitli yöntemlere başvurulmaktadır. Bu süreçte, en yaygın kullanılan yöntemlerden biri "web kazıma" *(web scraping)* teknolojileri aracılığıyla kamuya açık kaynaklardan verilerin elde edilmesidir. Web kazıma; web sayfalarını taramak, bu sayfalardan görsel, video, metin, iletişim bilgileri gibi içerikleri toplamak, kopyalamak ve/veya çıkarmak ve elde edilen bilgileri sonraki kullanım için depolamak (örneğin, bir veri tabanında) amacıyla otomatik yazılımların kullanılmasıdır.[19]

17 Belirtilen adımlar, bir ÜYZ modelinin yaşam döngüsünün genel çerçevesini sunmakta olup bu adımların kapsamı ve sırası; bağlam, uygulama alanı ve ihtiyaçlara göre değişkenlik gösterebilmektedir.

18 EDPS, Generative AI and the EUDPR, s. 4.

19 Information Commissioner's Office (ICO): Generative AI First Call for Evidence: The Lawful Basis for Web Scraping to Train Generative AI Models, (https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/generative-ai-first-call-for-evidence/).

Bunun yanı sıra, ÜYZ modellerinin eğitiminde kullanılan diğer veri kaynakları arasında;

→ ÜYZ araçlarına istem gönderimi gibi yollarla kullanıcılar tarafından sağlanan veriler,
→ Üçüncü taraflarca oluşturulan veri tabanlarından elde edilen veriler,
→ Geliştirici veya operatörlerin kendi bünyelerinde tuttukları veri tabanları üzerinden ulaşılan veriler yer almaktadır. [20]

- Bir sonraki adım, modelin kullanım amacına uygun şekilde eğitilmesi ve "ince ayar"ının *(fine-tuning)* yapılmasıdır. Örneğin LLM'ler, gözetimli öğrenme yöntemleri, insan müdahalesi içeren teknikler ("insan geri bildirimi ile pekiştirmeli öğrenme-*reinforcement learning with human feedback"* gibi) veya parametre ya da komut ayarı gibi yöntemler aracılığıyla optimize edilebilmektedir. Bu tür yöntemler, sistemin bilgiyi ve bağlamı daha iyi tanımasını ve işlemesini, tercih edilen yanıtları belirlemesini, hassas sorulara yanıt verirken çıktıyı sınırlandırmasını ve geliştiricilerin değerleriyle uyumlu hâle getirilmesini (örneğin, zararlı veya toksik içerik üretiminden kaçınılmasını) sağlamak amacıyla kullanılmaktadır. [21]

- Bir sonraki aşamada, modelin değerlendirilmesi ve doğruluğu ile kullanım amacına ne ölçüde uyumlu olduğu gibi faktörlerin düzenli biçimde incelenmesini sağlayacak değerlendirme ölçütlerinin oluşturulması amaçlanmaktadır. [22]

- Bu aşamayı izleyen süreçte, modeller önceki aşamalarda belirlenen ölçütler kullanılarak, sürekli izleme ve düzenli değerlendirme süreçlerini de kapsayacak şekilde yerleştirilmekte *(deploy)* ve uygulanmaktadır.[23] Yerleştirme sonrasında da modelin iyileştirilmesi için düzenli geri bildirimler sağlanmaktadır.

Yukarıda yer verilen aşamalar doğrultusunda, ÜYZ sistemlerinin yaşam döngüsü; modelin geliştirilmesinden operasyonel hâle getirilmesine, kullanımının sürdürülmesinden sonlandırılmasına kadar uzanan bütüncül bir süreci kapsamaktadır. Bu süreçte, teknik gerekliliklerin yanı sıra etik, hukuki ve toplumsal boyutların da dikkate alınması önem taşımaktadır.

Bu bağlamda, yaşam döngüsünün her bir aşamasının titizlikle planlanması ve etkin şekilde yürütülmesi, ÜYZ teknolojilerinin insan merkezli, güvenli, sorumlu ve toplumsal faydayı önceleyen bir yaklaşımla kullanılabilmesi açısından kritik bir gerekliliktir.

20 Confederation of European Data Protection Organisations (CEDPO): Generative AI: The Data Protection Implications, (https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf), s. 7-8.
21 EDPS, Generative AI and the EUDPR, s. 4-5.
22 EDPS, Generative AI and the EUDPR, s. 4.
23 EDPS, Generative AI and the EUDPR, s. 4.

4. Üretken Yapay Zekâ Hangi Alanlarda Kullanılmaktadır?

ÜYZ, birçok alanda dönüşüm sağlayarak yenilikçi çözümler sunan bir teknolojidir. Farklı formatlarda, insan üretimine benzer içerikler oluşturabilme kapasitesi sayesinde iş süreçlerini yeniden şekillendiren bu teknoloji, geleneksel yöntemlerin ötesine geçerek yenilikçi ve işlevsel uygulamalara zemin hazırlamaktadır. Özellikle genel talimatlardan içerik oluşturma, mevcut içeriği yeniden işleme ve veri analizi gibi temel görevleri yerine getirme kapasitesi, ÜYZ'yi hem üretkenliği artıran hem de yeni sistemlerin geliştirilmesine katkı sağlayan bir araç hâline getirmektedir.[24] Bu yönüyle ÜYZ, gerek mevcut iş modellerinin dönüştürülmesine gerek farklı alanlarda yenilikçi yaklaşımlar geliştirilmesine imkân tanımaktadır.

Bu bağlamda, ÜYZ'nin günümüzdeki kullanım alanları şu şekilde örneklendirilebilir:

Müşteri Hizmetleri: ÜYZ, müşteri hizmetlerinde hızlı ve etkili çözümler sunarak, hem müşteri etkileşimlerinin optimize edilmesine hem de işletmelerin operasyonel verimliliğinin artırılmasına katkı sağlayabilmektedir. Bu kapsamda, sohbet botları ve sanal asistanlar; hizmet süreçlerini kolaylaştırma, işletmelerin maliyetlerini azaltma ve müşteri memnuniyetini artırma potansiyeline sahiptir. Ayrıca bu modeller, müşterilere kişiselleştirilmiş öneriler sunulmasını ve kullanıcı deneyimine dayalı hizmetler geliştirilmesini mümkün kılmaktadır.

Sağlık: ÜYZ, hasta kayıtlarının analiz edilmesi yoluyla sağlık hizmeti sağlayıcılarının teşhis süreçlerini destekleyebilmekte ve kişiselleştirilmiş tedavi planları geliştirilmesini mümkün kılabilmektedir. Bunun yanı sıra, hastaların tıbbi durumları ve tedavi süreçleri hakkında bilgilendirilmesi, önleyici sağlık hizmetlerine yönelik öneriler oluşturulması ve kimyasal modelleme aracılığıyla ilaç keşfi ya da geliştirilmesi gibi alanlarda da önemli fırsatlar sunmaktadır.

24 Commission Nationale de l'Informatique et des Libertés (CNIL): CNIL's Q&A on the Use of Generative AI Systems, (https://www.cnil.fr/en/cnils-qa-use-generative-ai-systems).

Eğitim: ÜYZ, öğrencilerin bireysel performansları, ihtiyaçları ve ilgi alanlarına göre kişiselleştirilmiş öğrenme planlarının oluşturulmasına imkân tanımakta ve böylece eğitimde tek tip yaklaşımların yerini, yetkinliğe dayalı öğrenme modellerine bırakmasına katkı sunabilmektedir. Ayrıca, ders planlarının hazırlanması ve eğitim materyallerinin oluşturulması gibi süreçlerde sağladığı destekle öğretim sürecinin verimliliği de artırabilmektedir.

Pazarlama ve Reklamcılık: İçerik üretimi, hedef kitle analizi ve kampanya optimizasyonu gibi süreçlerde, ÜYZ yaygın bir şekilde kullanılmaktadır. Bu teknoloji; özelleştirilmiş kampanyaların tasarlanması, reklam metinlerinin hazırlanması, sosyal medya içerikleri ve uygun görsellerin oluşturulması gibi uygulamalar aracılığıyla, hedef kitle ile daha etkili ve kişiselleştirilmiş bir iletişim kurulmasına katkı sağlayabilmektedir. Ayrıca, müşteri davranışlarının analizine dayalı olarak daha isabetli öngörüler sunulabilmekte ve bu sayede süreçlerde hız ve verimlilik artışı elde edilebilmektedir.

Kültürel Endüstriler ve Sanat: ÜYZ, sanat ve tasarım süreçlerinde yeni araçlar sunarak süreçleri hızlandırabilmekte ve çeşitlendirebilmektedir. Bu kapsamda, metin üretebilen ya da metinsel açıklamalardan hareketle görsel içerikler ve sanat eserleri oluşturabilen modeller; reklamcılık, medya, sinema gibi sektörlere katkı sunabilmektedir. Müzik alanında ise ÜYZ destekli sistemler, yeni melodiler üretme ve mevcut besteleri geliştirme gibi süreçlerde sanatçılara yardımcı olabilmektedir.

Yazılım Geliştirme: ÜYZ, yazılım geliştirme süreçlerinde de giderek artan bir şekilde kullanılmaktadır. Özellikle kod üretme araçları, yeni kod parçalarının yazımını otomatikleştirerek hem süreci hızlandırabilmekte hem de geliştiricilerin operasyonel yükünü azaltabilmektedir. Ayrıca, mevcut kodların yeniden yapılandırılması, hataların tespiti ve açıklayıcı belgeler oluşturulması gibi görevlerde de fayda sağlayarak yazılım geliştirme sürecinin verimliliğini artırabilmektedir.

Arama ve Bilgiye Erişim: ÜYZ, arama motorlarına ve sanal asistanlara entegre edilerek, bu sistemleri daha gelişmiş bilgi asistanlarına dönüştürebilmektedir. Bu doğrultuda, ÜYZ ile entegre edilen arama sistemleri; kullanıcılara yalnızca bağlantı listeleri sunmakla kalmamakta, aynı zamanda arama sonuçlarına ilişkin özetlenmiş ve bağlamsal açıklamalar da sağlayabilmektedir.

Hukuk: Sözleşme hazırlanması, hukuki belgelerin analiz edilmesi ve özetlenmesi ile dava dosyalarının incelenmesi gibi görevlerde ÜYZ kullanımı, meslek profesyonellerinin rutin ve zaman alıcı işlemleri otomatikleştirmelerine imkân tanıyabilmektedir. Ayrıca, mahkeme kararlarının analizinde ve benzer içtihatların tespitinde bu teknolojilerin giderek daha yaygın bir şekilde kullanıldığı görülmektedir.

> ÜYZ birçok alanda yenilikçi fırsatlar sunmakla birlikte bu teknolojilerin kullanımı etik, güvenlik ve hukuki açılardan birtakım riskleri de beraberinde getirmektedir. Bu riskler, Rehber'in bir sonraki bölümünde ele alınmaktadır.

5. Üretken Yapay Zekânın Kullanımı Ne Gibi Riskler Taşımaktadır?

ÜYZ, hızlı ve etkin karar alma, dinamik kişiselleştirme ve sürekli erişilebilirlik gibi önemli avantajlar sunmaktadır. Talebe bağlı olarak içerik ve yanıt üretebilme kapasitesi sayesinde operasyonel verimliliği artırmakta; bu sayede emek-yoğun süreçlerin hızlandırılması veya otomatikleştirilmesi, maliyetlerin azaltılması ve çalışanların daha yüksek katma değerli işlere yönlendirilmesi mümkün hâle gelebilmektedir.

Ancak tüm bu imkânlara karşın, bireylerin haklarının korunması ve toplumsal güvenliğin sağlanabilmesi açısından, ÜYZ sistemlerinin ortaya çıkarabileceği riskler dikkate alınarak, bu sistem ve modellerin sorumlu ve bilinçli bir şekilde tasarlanması, geliştirilmesi ve kullanılması önem arz etmektedir.

Bu çerçevede, ÜYZ'nin gündeme getirdiği risklerden bazıları şu şekildedir:

"Halüsinasyonlar" ve Tutarsız Çıktılar: ÜYZ modellerinin doğasında yer alan en önemli risklerden biri, "halüsinasyon" olarak adlandırılan hatalı çıktılardır. Bu kavram, ÜYZ tarafından üretilen, gerçeklikle örtüşmeyen ancak çoğu zaman oldukça makul ve ikna edici görünen içerikleri ifade etmektedir. Örneğin, bir avukatın içtihat araştırması sırasında ÜYZ aracılığıyla gerçekte var olmayan mahkeme kararları veya alıntılarla karşılaşması, bu riske somut bir örnek teşkil etmektedir. Bu tür hataların temelinde, ÜYZ modellerinin istemleri anlamaktan ziyade, eğitildikleri veriler üzerinden istatistiksel olarak en olası çıktıları üretmeye dayalı bir yapıya sahip olmaları yatmaktadır.[25] Bu nedenle, üretilen yanıtlar dilsel olarak tutarlı görünse dahi, içerik bakımından hatalı ya da gerçek dışı olabileceğinden, doğruluklarının kontrol edilmesi önem taşımaktadır.

Ön Yargı ve Yanlı Çıktılar: ÜYZ modelleri, hem eğitim verilerinde yer alan ön yargıları hem de ince ayar sürecinde etkili olan insan değerlendirmelerindeki yanlılıkları, çıktılarında yansıtma ve pekiştirme riski taşımaktadır. Bu durum, saldırgan ya da ayrımcı içeriklerin üretilmesine neden olabilmekte ve toplumsal eşitsizlikleri derinleştirme potansiyeli barındırmaktadır. Ayrıca, ÜYZ modellerinin önemli bir kısmının "kara kutu" *(black box)* niteliğinde olması, karar alma süreçlerinin anlaşılmasını zorlaştırmakta hatta kimi zaman imkânsız hâle getirebilmektedir. Bu durum, ön yargıların veya saldırgan içeriklerin tespit edilmesini ve giderilmesini karmaşık bir hâle getirmekte ve kontrol edilmesini güçleştirmektedir. Öte yandan, eğitim veri kümelerinde veri noktalarının dengeli bir biçimde temsil edilmemesi, model çıktılarında ön yargılı, hatalı veya saldırgan söylemlerin ortaya çıkması ihtimalini artırmaktadır.

25 CNIL, CNIL's Q&A on the Use of Generative AI Systems, (https://www.cnil.fr/en/cnils-qa-use-generative-ai-systems).

Verilerin Gizliliği ve Güvenliği: ÜYZ modelleri, ikna edici nitelikte oltalama e-postaları, sahte kimlikler veya diğer zararlı içerikler oluşturmak amacıyla kullanılabilmekte olup bu durum, kullanıcıların verilerinin gizliliği ve güvenliği açısından ciddi riskler doğurabilmektedir. Ayrıca, bu modellerin eğitildiği geniş veri kümeleri arasında internetten elde edilen veriler de bulunmakta olup bu veriler, kişisel verileri de içerebilmektedir. Bu veriler, model çıktılarına yansıtılarak veri sızıntısı ve gizlilik ihlallerine yol açabilmektedir. Bunun yanında, kullanıcıların istemlerinde paylaştıkları kişisel verilerin veya kurumsal düzeyde hassas nitelik taşıyan bilgilerin açığa çıkması riski de dikkate alınması gereken önemli bir güvenlik sorunudur.

Fikri Mülkiyet Hakkı İhlalleri: ÜYZ modellerinin kullanımı, fikri mülkiyet haklarının ihlali riskini de beraberinde getirmektedir. Bu modeller, eğitim verilerinden öğrenerek özgün gibi görünen yeni içerikler oluşturabilmektedir. Ancak kullanılan veri kümelerinin telif hakkı ile korunan eserleri içermesi durumunda, model tarafından üretilen içeriklerin fikri mülkiyet haklarını ihlal ettiği yönünde hukuki iddialar gündeme gelebilmektedir.

Deep Fake **ve Manipülatif İçerikler:** ÜYZ sistemleri, son derece gerçekçi görünen sahte görsel, ses ve video içerikleri oluşturmak amacıyla kullanılabilmektedir. Bu tür manipülatif içerikler, yanlış bilginin yayılması, kimlik sahteciliği yapılması ya da bireylerin itibarının zedelenmesi gibi amaçlarla kötüye kullanılma riski taşımaktadır.

ÜYZ önemli avantajlar ve diramik çözümler sunan bir teknoloji olmakla birlikte bu modeller, kavramları ve istemleri anlama yetisine sahip olmayıp eğitildikleri veriler üzerinden istatistiksel olarak en muhtemel sonuçları oluşturmaktadır.

Bu nedenle ÜYZ çıktılarının;

- **Yanlış**
- **Tutarsız**
- **Ön Yargılı**
- **Yanıltıcı/Manipülatif**

olabileceği unutulmamalıdır.

6. Üretken Yapay Zekâ Sistemlerinde Kişisel Veri İşlenmekte midir?

Bir ülkede yürürlükte olan veri koruma mevzuatının uygulanabilmesi için öncelikle, ilgili faaliyet kapsamında bireylere ait "kişisel veri"lerin işlenmiş olması gerekmektedir.

Ülkemizde yürürlükte olan 6698 sayılı Kanun'un 3'üncü maddesinin (1) numaralı fıkrasının (d) bendinde "kişisel veri", *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmakta; anılan maddenin (e) bendinde ise "kişisel verilerin işlenmesi" kavramı, *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* şeklinde ifade edilmektedir.

Çoğu YZ sisteminde olduğu gibi, ÜYZ sistemleri de veri odaklı bir şekilde işlemekte ve öğrenme süreçlerini büyük ölçekli veri kümeleri üzerinden yürütmektedir. Geleneksel YZ eğitimi, geniş veri kümelerinin modellere sunulmasını ve bu modellerin söz konusu verilerdeki örüntüleri ve ilişkileri öğrenmesini içermekte; eğitim süreci tamamlandığında ise model, öğrenmiş olduğu bu kalıplar doğrultusunda çıktılar ortaya koymaktadır. Bu kapsamda, bireylere ait kişisel verilerin eğitim verilerine dahil edilmiş olması hâlinde, söz konusu veriler modelin iç yapısını ve çıktıları etkileyebilmektedir.[26]

Benzer şekilde, ÜYZ sistemlerinin yaşam döngüsünün çeşitli aşamalarında da kişisel veri işleme niteliğinde faaliyetlerle karşılaşılabilmektedir. Bu durum; eğitim veri kümelerinin oluşturulması, eğitim sürecinin yürütülmesi, modelin oluşturulup kullanıma sunulmasının ardından yeni veya ilave bilgilerin çıkarılması ve sistem çalışır durumdayken girilen veriler ile üretilen çıktılar yoluyla gerçekleşebilmektedir.[27] Bu çerçevede, kişisel veri işleme faaliyeti her zaman ilk bakışta açık bir şekilde anlaşılamasa da arka plandaki işleme süreçlerinde kişisel veri niteliği taşıyan bilgilere doğrudan ya da dolaylı şekilde temas edilebilmektedir.
Modelin kişisel veri işlenmesini özellikle hedeflememesi veya söz konusu kişisel verilerin yalnızca rastlantısal ya da dolaylı bir şekilde işlenmiş olması, kişisel veri işleme faaliyetinin varlığını ortadan kaldırmamaktadır. Bu nedenle model, kişisel veri işlemek üzere tasarlanmamış olsa dahi, bu durumun

26 CEDPO, Generative AI: The Data Protection Implications, s. 6.
27 EDPS, Generative AI and the EUDPR, s. 7.

geçerliliğini değerlendirmek amacıyla tüm aşamalarda düzenli kontrollerin gerçekleştirilmesi ve sistemin izlenmesi, uygulanabilecek kontrol mekanizmaları arasında yer almaktadır. Bu durum veri koruma düzenlemelerinin yanında, giderek yaygınlaşmaya başlayan YZ veri yönetişim çerçeve ve standartlarının da bir gereğidir.

Bu kapsamda, ÜYZ sistemlerinin yaşam döngüsü içerisinde herhangi bir şekilde kişisel verilerin işlenmesi söz konusu ise yürürlükteki veri koruma mevzuatı uygulama alanı bulmaktadır. Zira 6698 sayılı Kanun, teknolojiden bağımsız bir şekilde, kişisel verilerin işlendiği her durumda geçerli olan genel bir hukuki çerçeve sunmakta olup YZ/ÜYZ sistemleri de bu kapsamda değerlendirilmektedir.

Örnek 1: Bir teknoloji şirketi, çalışanlarının mesleki gelişimini desteklemek amacıyla, ÜYZ destekli bir içerik oluşturma aracı kullanarak eğitim materyalleri hazırlamaktadır. Söz konusu sistem, daha önce yürütülmüş eğitimlere ilişkin video kayıtlarını ve eğitici notlarını analiz ederek, yeni özetler ve sunum taslakları üretmektedir. Ancak analiz edilen bu kayıt ve belgeler arasında katılımcıların ad ve soyadları, unvanları, görüntüleri ve ses kayıtları gibi kişisel veri niteliği taşıyan bilgileri de yer almaktadır.

Bu durumda, ÜYZ sisteminin içerik oluşturma süreci kapsamında kişisel verilerin işlenmesi söz konusu olmakta; dolayısıyla bu çerçevede gerçekleştirilen veri işleme faaliyetlerinin kural olarak 6698 sayılı Kanun hükümleri çerçevesinde değerlendirilmesi gerekmektedir.

Örnek 2: Bir grafik tasarım ajansı, sosyal medya kampanyalarında kullanılmak üzere reklam görselleri ve kısa tanıtım metinleri üretmek amacıyla, ÜYZ tabanlı bir içerik oluşturma aracından faydalanmaktadır.

Ajans, ÜYZ sistemine yalnızca genel temalar ve kavramsal yönlendirmeler içeren istemler sunmaktadır. Bu istemler arasında "yaz indirimi temalı afiş", "şehir silueti içeren manzara tasarımı" veya "soyut çizgilerle oluşturulmuş modern tasarımlar" gibi, herhangi bir gerçek kişiye ait bilgi içermeyen ifadeler yer almaktadır. ÜYZ tarafından üretilen içerikler de benzer şekilde, kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin herhangi bir bilgi içermemektedir.

Bu çerçevede, ajansın ÜYZ sistemine sağladığı girdiler ile elde ettiği çıktılar –sistemin içerik üretimi kapsamında işlenen veriler açısından- değerlendirildiğinde, kişisel veri niteliği taşıyan herhangi bir bilginin bulunmadığı anlaşılmaktadır. Dolayısıyla söz konusu örnekte kural olarak 6698 sayılı Kanun kapsamında bir kişisel veri işleme faaliyetinin varlığından söz edilememektedir.

Diğer yandan, bazı durumlarda ÜYZ sistemlerine kişisel veri içermeyen girdiler sunulmasına rağmen, modelin eğitim sürecinde yer alan bilgiler doğrultusunda çıktılarda kişisel veri niteliği taşıyan bilgilerin üretilebilmesi mümkündür. Bu kapsamda, modelin doğrudan kişisel verileri hedeflememesi veya kullanıcı tarafından sağlanan girdilerin kişisel veri içermemesi, 6698 sayılı Kanun kapsamında kişisel veri işleme faaliyetinin varlığını ortadan kaldırmamaktadır.

Örnek 3: Bir kullanıcı, ÜYZ tabanlı bir metin üretim aracına "Ünlü bir Türk fizikçinin başarı hikâyesini anlat" şeklinde genel nitelikli bir istem sunmuştur. İstemde herhangi bir gerçek kişiye ait bilgi bulunmamakla birlikte, model çıktısında bir gerçek kişiye ilişkin ad-soyad, çalışma geçmişi ve ödül bilgileri yer almıştır.

Bu durumda, kullanıcı tarafından sağlanan girdide kişisel veri bulunmamasına karşın, modelin eğitim sürecinde öğrendiği bilgiler doğrultusunda bir gerçek kişiye ilişkin verileri yeniden üretmesi söz konusudur. Bu çerçevede, çıktı aşamasında kişisel veri niteliği taşıyan bilgilerin ortaya çıkması nedeniyle, söz konusu faaliyet kişisel veri işleme faaliyeti kapsamında değerlendirilebilecektir.

ÜYZ sistemlerinin işleyişinde yalnızca anonim ya da anonimleştirilmiş verilerin kullanıldığı durumlara da değinilmesi önem taşımaktadır. Kanun'un 3'üncü maddesinin (1) numaralı fıkrasının (b) bendinde "anonim hâle getirme", *"kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi"* şeklinde tanımlanmaktadır. Diğer bir ifadeyle anonim hâle getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılması veya değiştirilmesi yoluyla, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi ya da bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişi ile ilişkilendirilemeyecek şekilde kaybetmesi anlamına gelmektedir.[28] Nitekim başlangıçtan itibaren belirli bir kişiyle ilişkilendirilmesi mümkün olmayan anonim veriler ile sonradan anonim hâle getirilmiş veriler, kişisel veri niteliği taşımadıklarından 6698 sayılı Kanun hükümlerine tabi tutulmamaktadır.

Bu doğrultuda, ÜYZ sistemlerinin tasarımı, geliştirilmesi ve test edilmesi gibi süreçlerde yalnızca anonim ya da anonimleştirilmiş verilerin kullanılması hâlinde, söz konusu faaliyetler kural olarak veri koruma mevzuatının kapsamı dışında kalmaktadır. Bununla birlikte, anonim hâle getirildiği ileri sürülen verilerin gerçekten anonim olup olmadığının teknik yöntemler ve nesnel ölçütlerle ortaya konulması, bu verilerin kişisel veri niteliği taşıyıp taşımadığının belirlenmesi açısından önem taşımaktadır. Öte yandan, veri kümeleri anonim hâle getirilene kadar bu verilerin kişisel veri niteliğini koruduğu dikkate alındığında, bu süreçlerde gerçekleştirilen veri işleme faaliyetlerinin 6698 sayılı Kanun'a uygun şekilde yürütülmesi gerekmektedir.

28 Kişisel Verileri Koruma Kurumu: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Rehberi, (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf),s.25.

7. Üretken Yapay Zekâ Sistemlerinin Yaşam Döngüsü Kapsamında Veri Sorumlusu ile Veri İşleyen Nasıl Belirlenmelidir?

6698 sayılı Kanun'un 3'üncü maddesinin (1) numaralı fıkrasının (ı) bendinde "veri sorumlusu", *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak belirtilmekte; anılan maddenin (ğ) bendinde ise "veri işleyen", *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* şeklinde tanımlanmaktadır.

Veri işleyen; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği, veri sorumlusunun organizasyonu dışındaki ayrı bir gerçek veya tüzel kişidir.

Veri işleyenin faaliyetleri kişisel veri işlemenin daha çok teknik kısımları ile sınırlı iken; veri sorumlusu ise kişisel verilerin işlenmesine ilişkin karar alma yetkisine sahiptir ve kişisel veri işleme faaliyetinin "neden" ve "nasıl" yapılacağı sorularının cevabını verecek olan kişidir.

Bu kapsamda, veri sorumlusunun tespitinde aşağıdaki hususlara kimin karar verdiğinin dikkate alınması önem taşımaktadır:

- Kişisel verilerin toplanması ve toplama yöntemi,
- Toplanacak kişisel veri türleri,
- Toplanan kişisel verilerin hangi amaçlarla kullanılacağı,
- Hangi bireylerin kişisel verilerinin toplanacağı,
- Toplanan kişisel verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı,
- Kişisel verilerin ne kadar süreyle saklanacağı.

Bununla birlikte veri sorumlusu, yapacağı kişisel veri işleme sözleşmesi ile aşağıdaki gibi hususlarda karar verme yetkisini veri işleyene bırakabilmektedir:

- 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 saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot,
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hâle getirilmesi yöntemi.

ÜYZ sistemlerinin karmaşık yapısı ve çok katmanlı işleyiş modeli, bu sistemlerdeki veri sorumlusu/veri sorumluları ile veri işleyen rollerinin tespitini, geleneksel veri işleme faaliyetlerine kıyasla daha güç hâle getirmektedir. Zira bu sistemlerin tasarlanması, eğitilmesi, yerleştirilmesi ve kullanılmasına ilişkin süreçlerde farklı düzeylerde sorumluluk üstlenen çok sayıda gerçek veya tüzel kişi yer alabildiğinden, kişisel veri işleme faaliyetlerine ilişkin kararların hangi aktör tarafından alındığı her zaman açık bir biçimde ortaya konulamamaktadır.

Bunun yanı sıra, ÜYZ sistemlerinde veri işleme faaliyetleri, çoğu zaman yalnızca tek bir aşamada gerçekleşmemekte ve sabit bir işlevle sınırlı kalmamaktadır. Bu sistemlerin, yaşam döngülerinin farklı safhalarında farklı amaç ve yöntemlerle yeniden yapılandırılabilmesine bağlı olarak, veri işleme süreçlerinin niteliği ve kapsamı dinamik bir şekilde değişebilmektedir.

Diğer yandan, taraflar arasında akdedilen sözleşmelerin, bir gerçek veya tüzel kişinin veri sorumlusu ya da veri işleyen olarak nitelendirilip nitelendirilemeyeceğini tek başına belirleyemeyeceği de göz önünde bulundurulmalıdır. Zira kişisel verilerin işlenmesine ilişkin sorumluluğun tespitinde önem taşıyan husus, sözleşmesel ifadelerden ziyade, tarafların bu faaliyetler üzerindeki fiili kontrolü ve kişisel verilerin işlenmesine ilişkin karar alma yetkisidir.

Bu doğrultuda, ÜYZ sistemlerinde "geliştirici" ve "yerleştirici" konumundaki aktörler, her durumda doğrudan veri sorumlusu ya da veri işleyen rolüyle örtüşmeyebilmektedir. Zira aynı gerçek veya tüzel kişi, sistemin farklı aşamalarında üstlendiği işlevlere bağlı olarak değişen düzeylerde kontrol ve karar alma yetkisine sahip olabilmektedir. Bu nedenle, veri sorumlusu ile veri işleyen rollerinin tespitinde, genel bir yaklaşımdan ziyade, her bir işleme faaliyetinin niteliği, bağlamı ve tarafların fiili rolleri esas alınarak somut bir değerlendirme yapılması gerekmektedir.

Örneğin, bir kuruluşun ürün veya hizmet olarak sunmak üzere temel bir ÜYZ modeli geliştirdiği ve bu süreçte kişisel verilerin işlenme amaçları ile vasıtaları üzerinde etki ve kontrol sahibi olduğu durumlarda, geliştirme sürecine ilişkin çeşitli veri işleme faaliyetleri bakımından bu kuruluş veri sorumlusu olarak değerlendirilebilecektir. Buna karşılık, geliştiricinin kişisel verileri üçüncü bir tarafın talimatları doğrultusunda ve bu tarafın veri işlemenin amaç ve vasıtaları üzerinde belirleyici olduğu bir çerçevede işlemesi durumunda ise geliştiricinin veri işleyen olarak nitelendirilmesi söz konusu olabilecektir.

Bu çerçevede, ÜYZ sistemlerinde veri sorumluluğuna ilişkin yapılacak değerlendirmelerde, kişisel verilerin işlenmesine dair temel nitelikteki kararların kim tarafından alındığı göz önünde bulundurulmalıdır. Bu kararlar, veri işleme faaliyetinin niteliği, kapsamı, amacı ve bağlamı gibi unsurlar üzerinde belirleyici olmakta ve örnek olarak şu hususları içermektedir:

- Hangi tür verilerin işleneceği (örneğin, metin, ses, görüntü),
- İşlenecek verilerin hangi kategorilere ait olduğu (örneğin, ad-soyad, sosyal medya gönderileri),
- Bu verilerin hangi kaynaklardan elde edileceği (örneğin, belirli internet siteleri veya sosyal medya platformları).

Örnek 4: Bir şirketin insan kaynakları birimi, işe alım sürecinde adayların başvurularını daha hızlı ve sistematik bir şekilde değerlendirebilmek amacıyla LLM tabanlı bir ÜYZ sistemini kullanıma almıştır. Bu sistem, adaylar tarafından gönderilen özgeçmişler, motivasyon mektupları ve başvuru formlarında yer alan bilgileri analiz ederek her bir aday için kısa özetler üretmekte ve ilan kriterlerine göre ön değerlendirme puanları sunmaktadır.

Sisteme hangi verilerin yükleneceği, bu verilerin hangi amaçlarla analiz edileceği ve elde edilen çıktıların nasıl değerlendirileceği gibi hususlar ilgili şirket tarafından belirlenmektedir. Hâlihazırda geliştirici tarafından oluşturulmuş bir ÜYZ modelini kendi faaliyetlerine entegre ederek kullanan ve bu kapsamda veri işleme faaliyetinin amacı, kapsamı ve yöntemi gibi hususlarda karar alma yetkisine sahip olan şirket, söz konusu işleme faaliyetleri bakımından veri sorumlusu olarak değerlendirilebilecektir.

Bazı durumlarda ise bir kuruluşun veri işleme faaliyetinin niteliği ve kapsamı üzerindeki kontrol ve etki düzeyi açık bir şekilde ortaya konulamamaktadır. Bu durum özellikle, günümüzde yaygın bir kullanım alanı bulan "kapalı erişimli" *(closed-access)* modeller açısından geçerlidir.

Zira bu tür modellerin geliştirilme ve dağıtılma biçimi, bu modelleri yerleştiren kuruluşların, veri işleme faaliyetlerine ilişkin temel kararlar üzerinde gerekli kontrol ve etkiyi sağlayabilmeleri için ihtiyaç duydukları tüm bilgilere erişmelerini her zaman mümkün kılmamaktadır. Ayrıca, ÜYZ geliştiricileri tarafından alınan genel nitelikli kararlar, modelin yerleştirilmesi sürecindeki işleyişini de etkileyebilmektedir. Bu nedenle, kapalı erişimli modelleri yerleştiren aktörlerin, yerleştirme aşamasındaki tüm işleme faaliyetleri üzerinde anlamlı bir kontrol ve etki sahibi olmamaları durumu söz konusu olabilmektedir. Bu gibi durumlarda tarafların veri işleme süreçlerindeki rollerinin belirlenmesinde, yerleştiricinin hangi bilgilere erişebildiğinin ve geliştirici tarafından sağlanan kontrol düzeyinin niteliğinin dikkate alınması önem taşımaktadır.

> Veri sorumlusu ile veri işleyen rollerinin tespitinde, genel bir yaklaşımdan ziyade, her bir veri işleme faaliyetinin niteliği, bağlamı ve tarafların fiili rolleri dikkate alınarak bir değerlendirme yapılmalıdır. Bu kapsamda, kişisel verilerin işlenmesine ilişkin amaç ve vasıtaların kim tarafından belirlendiği dikkatle değerlendirilmeli ve tarafların üstlendikleri roller ile fiili uygulamaların uyumlu olup olmadığı gözden geçirilmelidir.

8. Kişisel Verilerin İşlenmesinde Genel İlkeler Üretken Yapay Zekâ Sistemlerinde Nasıl Uygulanmalıdır?

6698 sayılı Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde kişisel verilerin, ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde;

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

şeklinde sayılan ilkelere uyulmasının zorunlu olduğu düzenlenmektedir.

Anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hâl ve şartta Kanun'un 4'üncü maddesinde sayılan ilkelere uyulması hukuki bir zorunluluk olup ÜYZ sistemleri kapsamında işlenen kişisel veriler de Kanun'un bahse konu maddesinde düzenlenen ilkelere uygun şekilde işlenmelidir.

A. Hukuka ve Dürüstlük Kurallarına Uygun Olma İlkesi

Hukuka ve dürüstlük kurallarına uygun olma ilkesi; kişisel verilerin işlenmesinde kanunlarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade etmektedir. Dürüstlük kuralına uygun olma ilkesi uyarınca veri sorumlusu, kişisel veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate almalıdır. Diğer bir ifadeyle; ilgili kişinin beklemediği ve beklemesinin de gerekmediği sonuçların ortaya çıkmasını önleyici şekilde hareket etmesi gerekmektedir. Anılan ilke uyarınca, ayrıca ilgili kişi için söz konusu kişisel veri işleme faaliyetinin şeffaf olmasının sağlanması ve aydınlatma yükümlülüğüne uygun hareket edilmesi önem taşımaktadır.

ÜYZ sistemlerinin geliştirilmesi, eğitilmesi ve uygulanması süreçlerinde hukuka ve dürüstlük kurallarına uygunluk ilkesinin gözetilmesi; kişisel verilerin hukuka uygun şekilde elde edilmesini, ilgili kişilere açık ve anlaşılır biçimde bilgi verilmesini ve işleme faaliyetlerinin şeffaf bir şekilde yürütülmesini gerektirmektedir. Bu kapsamda, sistemin eğitildiği veri kümelerinin hangi kaynaklardan sağlandığı, bu verilerin işlenmesine yönelik geçerli bir hukuki dayanağın bulunup bulunmadığı ve ilgili kişilere gerekli aydınlatmanın yapılıp yapılmadığı gibi hususların değerlendirilmesi önem taşımaktadır.

Bu bağlamda bireylerin; verilerinin hangi amaçlarla işlendiği, işlemenin kapsamı ve bireyler açısından olası etkileri gibi hususlarda zamanında, yeterli, açık ve erişilebilir bir şekilde bilgilendirilmesi, bu ilkenin önemli bir boyutunu oluşturmaktadır. Bu doğrultuda, ÜYZ sistemlerini geliştiren ve yerleştiren aktörlerin; sistemin hangi veri türleriyle çalıştığı, bu verilerin nasıl işlendiği ve çıktıların hangi kriterlere göre oluşturulduğu gibi hususlarda ilgili kişilere açık ve anlaşılır bilgilendirmeler sunmaları yerinde bir uygulama olacaktır.

Bununla birlikte, hukuka ve dürüstlük kurallarına uygunluk ilkesi, yalnızca 6698 sayılı Kanun ve ikincil düzenlemelerde öngörülen asgari yükümlülüklerin yerine getirilmesiyle sınırlı değildir. Bu ilke aynı zamanda, kişisel veri işleme faaliyetlerinin ilgili kişilerin makul beklentileriyle çelişmeyecek şekilde yürütülmesini, işlemenin potansiyel etkilerinin önceden öngörülmesini ve bireylerin temel hak ve özgürlüklerinin gözetilmesini de içermektedir.

Bu çerçevede, ÜYZ sistemlerinde ortaya çıkabilecek algoritmik ön yargılar, söz konusu ilkenin uygulanabilirliği bakımından dikkatle ele alınması gereken bir husustur. Genellikle kamuya açık kaynaklardan elde edilen büyük veri kümeleriyle eğitilen bu sistemler, toplumda hâlihazırda var olan ön yargıları ve eşitsizlikleri yansıtma veya pekiştirme riski taşımaktadır. Eğitim verilerinde belirli grupların yeterince temsil edilmemesi ya da veri kümelerinin yapısal olarak dengesiz olması gibi etkenler, sistem çıktılarında ayrımcı, adaletsiz veya yanıltıcı sonuçların ortaya çıkmasına neden olabilmekte ve bu da bireylerin beklemediği ve beklemesinin gerekmediği sonuçlarla karşılaşmasına yol açarak söz konusu ilkenin ihlali anlamına gelebilmektedir.

Örnek 5: Bir kurum, tanıtım materyallerinde kullanılacak mesleki görseller oluşturmak için ÜYZ tabanlı bir görsel üretim aracından faydalanmaktadır. Sistem, gerçek kişilere ait fotoğrafların da yer aldığı geniş ölçekli veri kümeleri üzerinde eğitilmiştir. Bu veri kümelerinde belirli cinsiyetlerin belirli mesleklerle orantısız biçimde temsil edilmesi, sistemin çıktılarında da benzer bir dengesizlik ortaya çıkarmıştır. Nitekim sistem, "doktor" ifadesi girildiğinde çoğunlukla erkek, "hemşire" ifadesi girildiğinde ise genellikle kadın figürler üretmektedir.

Bu durum, sistemin eğitiminde kullanılan veri kümelerindeki temsiliyet dengesizliklerinin çıktılara yansıması sonucunda ayrımcı ve ön yargılı çıktılar üretilmesine, buna bağlı olarak da hukuka ve dürüstlük kurallarına aykırı sonuçların ortaya çıkmasına neden olabilecektir.

Örnek 6: Bir çeviri hizmeti sağlayıcısının ÜYZ destekli otomatik konuşma tanıma sisteminde, bazı kullanıcı gruplarında diğer gruplara kıyasla belirgin şekilde daha yüksek kelime hatası oranları tespit edilmiştir. Yapılan teknik analiz sonucunda, eğitim verilerinde belirli İngilizce aksanların yeterince temsil edilmediği ve bu durumun sistemde örnekleme yanlılığına yol açtığı anlaşılmıştır. Ortaya çıkan bu sistematik farklılık, ilgili kişiler açısından öngörülemeyen ve ayrımcılığa yol açabilecek sonuçlara neden olarak hukuka ve dürüstlük kurallarına uygunluk ilkesine aykırılık teşkil edebilecektir.

Bu kapsamda, risklerin azaltılmasını teminen; ÜYZ sistemlerinde kullanılan veri kümelerinin özenle seçilmesi, toplumsal çeşitliliği adil biçimde temsil etmesine dikkat edilmesi ve çeşitlilik ile kapsayıcılık ölçütlerine uygun olarak yapılandırılması önem taşımaktadır. Ayrıca bu ilkenin uygulanabilirliğini güçlendirecek şekilde, sistem çıktılarının düzenli olarak değerlendirilmesini sağlayacak izleme ve denetim mekanizmalarının oluşturulması, ayrımcılık riski içeren durumların tespit edilmesi ve gerekli hâllerde müdahale imkânı sağlanması da önemlidir. Bu doğrultuda, ön yargı barındıran çıktı risklerinin azaltılmasına yönelik olarak ince ayar gibi yöntemlerin dikkate alınması yerinde bir yaklaşım olabilecektir. Bunun yanı sıra, bireylerin hak ve menfaatlerini korumaya yönelik proaktif, önleyici ve destekleyici nitelikte diğer tedbirlerin alınması da bahse konu ilkenin etkin şekilde hayata geçirilmesine katkı sağlayacaktır.

B. Doğru ve Gerektiğinde Güncel Olma İlkesi

Doğru ve gerektiğinde güncel olma ilkesi; kişisel verilerin doğruluğunun ve gereken durumlarda güncelliğinin sağlanmasının önemini ortaya koymaktadır. Bu ilke, 6698 sayılı Kanun'da düzenlenen, ilgili kişinin kişisel verilerinin düzeltilmesini talep etme hakkı ile uyumludur. Kişisel verilerin doğru ve güncel bir şekilde tutulması, veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da gereklidir. Kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması noktasında aktif özen yükümlülüğü; veri sorumlusu eğer bu verilere dayalı olarak ilgili kişiyle alakalı bir sonuç ortaya koyuyor ise geçerlidir. Bunun dışında veri sorumlusu her zaman ilgili kişinin kişisel verilerinin doğru ve güncel olmasını temin edecek kanalları açık tutmalıdır.

ÜYZ sistemleri, özellikle eğitim aşaması başta olmak üzere yaşam döngülerinin tüm evrelerinde büyük miktarda veri kullanmakta ve sıklıkla kişisel verilerden de yararlanmaktadır. Bu durum, "doğru ve gerektiğinde güncel olma" ilkesinin uygulanması bakımından özel dikkat gerektiren bir alan oluşturmaktadır. Zira bu sistemlerin çıktılarının doğruluğu, büyük ölçüde kullanılan veri kümelerinin kalitesi, güvenilirliği ve temsiliyet düzeyi ile ilişkilidir. Bu nedenle doğru, güncel ve bağlam içinde anlamlı verilerin kullanılması, sistemin güvenilirliğinin sağlanması ve üretilecek çıktıların doğruluğu açısından kritik bir öneme sahiptir.

Bu kapsamda, ÜYZ sistemlerini geliştiren, sağlayan ve kullanan aktörlerin, eğitim verilerinde yer alan yanıltıcı ya da doğruluğu teyit edilemeyen bilgilerin ayıklanmasına yönelik gerekli tedbirleri almaları ve sistem çıktılarında kişisel verilerin yer alması durumunda bunlara ilişkin denetim ve filtreleme süreçlerini işletmeleri faydalı olacaktır. Eğitim verilerinin kaynağının kayıt altına alınması, veriler sisteme dahil edilmeden önce içerik bakımından gözden geçirilmesi ve eksik, hatalı ya da güncelliğini yitirmiş bilgilerin ayıklanması gibi uygulamalar, bu ilkenin etkin bir şekilde hayata geçirilmesine katkı sunabilecektir.

Bununla birlikte söz konusu ilkenin, yalnızca sistemin girdileri bakımından değil, aynı zamanda üretilen çıktılar yönünden de dikkate alınması önem taşımaktadır. Zira bu sistemler, yüksek temsiliyet düzeyine sahip kaliteli veri kümeleriyle eğitilmiş olsalar dahi, kişisel veriler de dahil olmak üzere, bağlamdan kopuk veya gerçek dışı içerikler üretebilmektedir. "Halüsinasyon" olarak adlandırılan bu tür çıktılar, sistemin güvenilirliğini zedeleyebilecek riskler doğurabilir. Eğitim verilerinin doğruluğu ve kalitesi, halüsinasyonların tamamen önüne geçemese de bu durumun meydana gelme olasılığını ve hata payını azaltmada etkili olabilecektir. Özellikle kişisel verilerin yer aldığı çıktılarda, yanlış veya yanıltıcı bilgilerin paylaşılması, ilgili kişiler açısından zarara yol açabilecek sonuçlar doğurabileceğinden, sistem çıktılarının düzenli olarak izlenmesi ve gerektiğinde insan gözetimi mekanizmalarıyla desteklenmesi önem taşımaktadır.

ÜYZ sisteminin kullanıma sunulmasının ardından da sistem davranışlarının belirli aralıklarla izlenmesi, doğruluk düzeyinin değerlendirilmesi ve gerektiğinde çıktılar üzerinde düzeltme veya güncelleme yapılmasını mümkün kılacak mekanizmaların oluşturulması, söz konusu ilkenin bütüncül biçimde gözetilmesine katkı sağlayacaktır. Bu süreçte veri sorumlularının, ÜYZ sistemlerinin geliştirilmesinden kullanımına kadar olan tüm aşamalarda, verilerin doğruluğunu ve gerekli durumlarda güncelliğini destekleyecek şekilde mahremiyetin tasarıma entegre edildiği bir yaklaşımı benimsemeleri ve baştan sona izlenebilir, denetlenebilir bir veri yönetişimi anlayışı geliştirmeleri, söz konusu ilkenin uygulanabilirliğini güçlendirecektir.

Örnek 7: Bir müşteri ilişkileri hizmet sağlayıcısı, kullanıcı şikâyetlerini özetlemek amacıyla ÜYZ tabanlı bir model kullanmaktadır. Bu model, kullanıcılar tarafından iletilen şikâyetlerin temel içeriğini anlamlı bir şekilde özetlemeyi hedeflemektedir. Ancak yapılan değerlendirmelerde, modelin bazı durumlarda şikâyet metinlerini bağlamından kopuk biçimde özetlediği, bazı örneklerde ise müşterilere ilişkin kişisel verileri eksik ya da hatalı yansıttığı gözlemlenmiştir.

Bu tür bir durum, hem sistemin işlevsel amacına ulaşmasını engelleyebilecek hem de kişisel verilerin doğruluğunun sağlanması ilkesine aykırılık teşkil edebilecektir. Bu tür risklerin azaltılabilmesi adına geliştiricilerin, model çıktılarının düzenli olarak gözden geçirilmesini sağlayacak denetim mekanizmaları kurmaları; modeli uygulamaya koyanların ise bu sistemleri belirli kriterler çerçevesinde izlemeleri yerinde olacaktır. Ayrıca son kullanıcıların geri bildirimleri aracılığıyla sürece dahil edilmesi, sistemin doğruluk düzeyinin sürekli olarak iyileştirilmesine katkı sunacaktır.

C. Belirli, Açık ve Meşru Amaçlar için İşlenme ile İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkeleri

Belirli, açık ve meşru amaçlar için işlenme ile işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkeleri; 6698 sayılı Kanun'un 4'üncü maddesinde düzenlenen diğer ilkelerdendir. Kişisel verilerin "belirli, açık ve meşru amaçlar için işlenme" ilkesi; kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetlerinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve bu faaliyetin gerçekleştirilme amacının belirliliğini sağlayacak detayda ortaya konulmasını sağlamaktadır. Bu ilke veri sorumlusunun, kişisel veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kılmaktadır. Amacın meşru olması ise veri sorumlusunun işlediği kişisel verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.

"İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine göre ise işlenen kişisel veriler, belirlenen amaçların gerçekleştirilebilmesine elverişli olmalıdır. Amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmalı, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemelidir. Burada önemli olan; amacı gerçekleştirmeye yönelik yeterli kişisel verinin temin edilmesi, bunun dışındaki amaç için gerekli olmayan kişisel veri işlemeden kaçınılmasıdır. Mevcutta olmayan ve sonradan gerçekleşmesi düşünülen amaçlarla kişisel veri işlenmemelidir. Ölçülülük ilkesi ise kişisel veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması anlamına gelmektedir. Diğer bir deyişle, kişisel veri işlemenin amacı gerçekleştirecek ölçüde olmasını ifade etmektedir.

ÜYZ sistemlerinde veri işleme faaliyetleri, sistemin yaşam döngüsü boyunca çeşitli düzeylerde ve karmaşık süreçlerle gerçekleşebilmektedir. Bu nedenle, anılan ilkeler bu sistemlerdeki kişisel veri işleme faaliyetlerinin hukuka uygunluğunun değerlendirilmesinde dikkate alınması gereken temel unsurlar arasındadır.

Bu çerçevede öncelikle veri sorumlularının sistemin her aşamasında kişisel veri işleme faaliyetlerini yalnızca işleme amaçları ile ilgili ve gerekli olanla sınırlamaları ve bu şekilde bir ayrım gözetilmeksizin gerçekleştirilen kişisel veri işleme faaliyetlerinden kaçınmaları gerekmektedir. Örneğin, "ÜYZ sistemlerimizde kullanmak" veya "veri tabanımızı geliştirmek" gibi muğlak ve geniş kapsamlı ifadeler, veri işlemenin amacını açık ve belirli bir şekilde ortaya koymadığından, 6698 sayılı Kanun'un 4'üncü maddesinde düzenlenen "belirli, açık ve meşru amaçlar için işlenme" ilkesine aykırılık teşkil

edebilecektir. Bu doğrultuda, geliştiricilerin "ÜYZ modeli geliştirmek" gibi geniş amaçlar yerine, sistemin yaşam döngüsünün her bir aşaması için spesifik, açık ve gerekçelendirilebilir amaçlar belirlemeleri ve işleme faaliyetlerinin bu amaçları karşılamak için neden gerekli olduğunu ortaya koyabilmeleri önemlidir. Dolayısıyla her bir işleme faaliyeti açısından yalnızca gerekli olan kişisel veriler işlenmeli, belirlenen amacın dışına çıkılmamalı ve veri toplama, saklama ile paylaşım süreçleri bu çerçevede yapılandırılmalıdır. Örneğin, kişisel verilerin belirli bir modelin eğitilmesi amacıyla toplanmasının ardından aynı veri kümesinin daha sonra başka bir modelin eğitimi için yeniden kullanılmak istenmesi durumunda, bu ikincil kullanımın verilerin ilk toplanma amacına uygunluğu değerlendirilmelidir. Bu noktada ilgili kişilerin makul beklentileri dikkate alınmalı ve daha sonraki işlemenin asıl işleme amacıyla uyumlu olmaması durumunda veri sorumlusu tarafından yeni bir veri işleme süreci belirlenmelidir.

ÜYZ modellerinin eğitimi için büyük miktarda veri kullanılmasının, her zaman daha fazla performans veya daha iyi sonuçlar anlamına gelmeyebileceği unutulmamalıdır. Aksine, veri kümelerinin dikkatle yapılandırılması, uygun şekilde denetlenen bir eğitim süreciyle desteklenmesi, düzenli izlemeye tabi tutulması ve amaçla bağlantılı, gereklilik sınırları içinde kalan verilerin işlenmesi, hem veri güvenliği hem de çıktı kalitesi açısından daha işlevsel sonuçlar doğurabilecektir. Bu nedenle, modelin performansını artırmak amacıyla geniş kapsamlı ve belirsiz veri toplamaktan kaçınılması ve veri koruma düzenlemeleriyle uyumlu şekilde hareket edilmesi önem taşımaktadır.

Örnek 8: Bir kuruluş, ÜYZ tabanlı bir dil modeli geliştirmektedir. Eğitim sürecinde çeşitli kaynaklardan elde edilen büyük ölçekli veriler kullanılarak modelin dil anlama ve üretme kapasitesinin artırılması hedeflenmektedir. Bu aşamada işlenen kişisel veriler, doğrudan modelin teknik yeterliliğini geliştirmeye yöneliktir.

Modelin eğitiminin ardından, aynı kuruluş bu modeli temel alarak kullanıcıların metin tabanlı taleplerine yanıt verebilen bir uygulama geliştirmiştir. Bu aşamada işlenen kişisel veriler ise kullanıcı ile doğrudan etkileşim kuran bir sistemin işlevselliği çerçevesinde değerlendirilmektedir.

Bu bağlamda, ÜYZ modeli geliştirilmesi ile bu modele dayalı uygulama geliştirilmesi, veri koruma düzenlemeleri kapsamında farklı amaçlar teşkil etmektedir. Bu kapsamda, veri sorumlularının her bir aşamadaki işleme faaliyetini ayrı ayrı değerlendirerek veri işleme amaçlarını belirli ve açık bir şekilde tanımlayabilmeleri önem taşımaktadır.

Veri minimizasyonu yönünden ise eğitim ve geliştirme aşamalarında ne kadar veriye ihtiyaç duyulduğu, veri işlemenin orantılı olup olmadığı ve bu çerçevede veri minimizasyonu önlemlerinin nasıl uygulanacağı dikkatle değerlendirilmelidir. Bu kapsamda, modelin kalitesini ve kullanıcı deneyimini geliştirmeye yönelik olarak gereken büyüklükte veri kullanımına imkân tanınmakla birlikte, ÜYZ bağlamında veri minimizasyonu ilkesi, kullanılan kişisel verilerin yalnızca gerekli olanla sınırlı tutulması gerektiği şeklinde anlaşılmalıdır. Bu bağlamda, mevcut olmayan veya gelecekte gerçekleşmesi öngörülen amaçlarla kişisel veri işlenmemelidir.

Örnek 9: İşe alım süreçlerinin desteklenmesi amacıyla ÜYZ tabanlı bir sistem geliştirilmesi planlanmaktadır. Bu sistemin, adayların özgeçmişlerini analiz ederek pozisyona uygunluk derecelerini değerlendirebilmesi ve örnek mülakat soruları oluşturması beklenmektedir. Bu kapsamda, geçmiş iş başvurularına ilişkin verilerin kullanılmak istenmesi durumunda, yalnızca sistemin amacına ulaşması için gerekli olan veriler işlenmelidir. Bu gibi durumlarda veri sorumlularının kişisel verilerin "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine uyum sağlama bakımından, kullanılacak verilerin sistemin hedefleriyle orantılı olup olmadığını teknik ve istatistiki yöntemlerle değerlendirmeleri ve işleme faaliyetlerini bu çerçevede düzenli olarak gözden geçirmeleri tavsiye edilmektedir.

D. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Edilme İlkesi

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi uyarınca, kişisel verilerin "amaçla sınırlılık ilkesi"nin de bir gereği olarak, işlendikleri amaç için gerekli olan süreye uygun şekilde muhafaza edilmeleri gerekmektedir. Buna ilişkin olarak veri sorumlusu, Kanun'un 12'nci maddesi kapsamında gerekli teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin saklanmasında amaçla sınırlılık ilkesi uyarınca veri sorumlusu tarafından belirlenen saklama sürelerinin yanı sıra, veri sorumlusunun tabi olduğu ilgili mevzuat kapsamında da belirlenmiş saklama süreleri mevcuttur. Buna göre veri sorumluları, işledikleri kişisel veriler için mevzuatta öngörülmüş bir süre varsa bu süreye uyacak; eğer mevzuatta bir süre öngörülmemişse kişisel verileri ancak işlendikleri amaç için gerekli olan süre kadar saklayabilecektir. Bir kişisel verinin daha fazla saklanması için geçerli bir sebep bulunmaması hâlinde, o veri silinecek, yok edilecek veya anonim hâle getirilecektir. İleride tekrar kullanılabileceği düşünülerek ya da herhangi bir başka gerekçe ile kişisel verilerin muhafaza edilmesi yoluna gidilemeyecektir.

ÜYZ sistemlerinin yaşam döngüsü boyunca kişisel veriler, farklı aşamalarda çeşitli amaçlarla işlenebilmekte olup bu kapsamda belirli sürelerle muhafaza edilmeleri gerekebilmektedir. Bu doğrultuda kişisel verilerin saklama süresinin belirlenmesi, her bir işleme faaliyetinin amacı dikkate alınarak değerlendirilmeli ve verilerin yalnızca ilgili amacın gerektirdiği süre boyunca tutulmasını sağlayacak şekilde saklama ve imha süreçleri yapılandırılmalıdır.

Kişisel verilerin işlenme amacının ortadan kalktığı veya işleme için geçerli hukuki dayanağın sona erdiği durumlarda bu veriler silinmeli, yok edilmeli ya da anonim hâle getirilmelidir. Özellikle ÜYZ sistemlerinin eğitiminde kullanılan kişisel veri içeren veri kümeleri bakımından makul, açık ve

gerekçelendirilebilir saklama sürelerinin belirlenmesi önem taşımaktadır. Zira bu tür verilerin belirsiz sürelerle saklanması, zamanla bireylerin gizliliğinin ihlali riskini artırabileceği gibi veri minimizasyonu ve amaçla sınırlılık ilkeleriyle de çelişebilecek niteliktedir. Bu çerçevede, veri sorumlularının hangi kişisel verilerin ne kadar süreyle muhafaza edileceğini düzenli olarak gözden geçirmeleri ve buna uygun saklama-imha politikaları geliştirmeleri yerinde olacaktır.

Örnek 10: Bir e-ticaret platformu, ÜYZ tabanlı bir otomatik metin analiz ve yanıt öneri sistemi geliştirmiştir. Sistemin temelini oluşturan model, geçmiş müşteri destek yazışmalarında yer alan mesaj kayıtları kullanılarak eğitilmiştir. Kayıtlar, kişisel veri içerebilecek şekilde müşteri mesajları ile müşteri temsilcilerinin yanıtlarından oluşmaktadır. Model, bu verilerden yola çıkarak müşteri mesajlarına daha hızlı, uygun ve kişiselleştirilmiş yanıtlar üretebilecek biçimde eğitilmiştir. Eğitilen model daha sonra sisteme entegre edilerek günlük müşteri hizmeti operasyonlarında kullanılmaya başlanmıştır.

Modelin planlanan sürümü tamamlandıktan sonra, şirketin bu mesaj kayıtlarını "ileride yeni sürümler geliştirilebileceği" gerekçesiyle belirsiz süre ile saklamaya devam etmesi durumunda, "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkesine aykırılık ortaya çıkabilecektir.

9. Üretken Yapay Zekâ Sistemlerinde Kişisel Verilerin İşlenme Şartları (Hukuki Sebep) Nasıl Belirlenmelidir?

ÜYZ sistemleri ile kişisel verilerin işlenmesi arasındaki ilişki, özellikle uygun hukuki sebeplerin belirlenmesi açısından büyük önem taşımaktadır. 6698 sayılı Kanun uyarınca, kişisel verilerin hukuka uygun şekilde işlenebilmesi için Kanun'un 5'inci maddesinde veya özel nitelikli kişisel veriler için ise Kanun'un 6'ncı maddesinde belirtilen işleme şartlarından en az birine dayanılması zorunludur.

Kanun'da yer alan işleme şartları arasında YZ teknolojilerine veya belirli bir teknolojik araca açık bir atıf bulunmamaktadır. Ancak bu durum, söz konusu teknolojiler kullanılarak kişisel veri işlenemeyeceği anlamına gelmemektedir. Zira 6698 sayılı Kanun, kişisel verilerin işlenmesini düzenleyen genel bir çerçeve sunmakta olup işlemede kullanılan araç veya teknolojilerin niteliğinden bağımsız olarak kişisel veri işleme faaliyetlerine uygulanabilmektedir. Bu nedenle, ÜYZ sistemleri aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetlerinde de Kanun'da öngörülen mevcut işleme şartlarından birine dayanılması gerekmektedir.

A. Kanun'un 5'inci Maddesi Kapsamında Uygun İşleme Şartının Belirlenmesi

Kişisel verilerin işlenme şartları 6698 sayılı Kanun'un 5'inci maddesinde sayılmış olup buna göre aşağıdaki hâllerden en az birinin bulunması durumunda kişisel verilerin işlenmesi mümkündür:

- İlgili kişinin açık rızasının varlığı.
- 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.

Kişisel verilerin işlenmesine ilişkin olarak Kanun'un 5'inci maddesinde sayılan işleme şartları sınırlı sayıdadır ve her bir veri işleme faaliyeti bu şartlardan en az birine dayanmak suretiyle gerçekleştirilmelidir. Bu işleme şartları, yeni veri işleme teknikleri ve süreçleri bakımından da bir çerçeve niteliği taşımaktadır. Diğer bir ifadeyle, her ne kadar kişisel verilerin işlenme şartları sınırlı sayıda olsa da, Kanun'da yer alan şartlar, yeni teknik ve süreçlerle gerçekleştirilen kişisel veri işleme faaliyetlerini de kapsayacak özelliğe sahiptir.

ÜYZ ile kişisel verilerin işlenmesinde önem taşıyan hususlardan biri, ÜYZ'nin geliştirilmesi, çalıştırılması ve çıktılarının kullanılması gibi farklı kişisel veri işleme faaliyetlerinin somut olayda bir arada bulunabilmesidir. Bu adımların her biri bağımsız birer veri işleme faaliyeti teşkil edebileceğinden, her biri için ayrı bir işleme şartının belirlenmesi önem arz etmektedir.

Örneğin, bir büyük dil modelinin çalıştırılması sürecinde;

- Kullanıcı tarafından girilen kişisel verilerin modelin çalıştırılması amacıyla işlenmesi,
- Bu verilerin modelin geliştirilmesi amacıyla kullanılması,
- Model tarafından üretilen çıktıların kullanıcıyla etkileşimin kişiselleştirilmesi amacıyla kullanılması,
- Model tarafından üretilen çıktıların modelin geliştirilmesi için kullanılması

gibi işlemler, ayrı birer kişisel veri işleme faaliyeti teşkil edebilmektedir. Bu nedenle, söz konusu faaliyetler için ayrı ayrı işleme şartlarının belirlenmesi gerekebilecektir. ÜYZ sistemleri, verilerin her aşamada yoğun şekilde işlenmesini gerektirebildiğinden, bu süreçlerin her birinin sistemin, modelin veya uygulamanın özelliklerine göre değerlendirilmesi önem taşımaktadır.

ÜYZ uygulamaları bakımından, Kanun'un 5'inci maddesinde yer alan işleme şartlarının her biri somut olaya göre değerlendirilebilmekle birlikte, bunlardan bazılarının nitelikleri gereği diğerlerine kıyasla daha fazla ön plana çıkması mümkündür.

a. İlgili Kişinin Açık Rızasının Varlığı

Kanun'un 5'inci maddesinde; öncelikle kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği belirtilmekte, ardından ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenebileceği sınırlı sayıdaki diğer şartlar sıralanmaktadır. İlgili maddede açık rıza ilk sırada yer almakla birlikte, maddede sayılan işleme şartları arasında herhangi bir hiyerarşi bulunmadığının vurgulanması gerekmektedir. Bu durum, hem Kişisel Verileri Koruma Kurulunun (Kurul) çeşitli kararlarından hem de özel nitelikli kişisel veriler için yeniden düzenlenen Kanun'un 6'ncı maddesinin (3) numaralı fıkrasında tüm işleme şartlarının aynı fıkra altında sayılmasından da açıkça anlaşılmaktadır.

Kişisel veri işleme faaliyetinin 6698 sayılı Kanun'da bulunan açık rıza dışındaki şartlardan birine dayanması hâlinde ilgili kişiden ayrıca açık rıza alınmaması gerekmektedir. Zira kişisel veri işleme faaliyetinin, açık rıza dışında bir işleme şartına istinaden yürütülmesi mümkün iken ilgili kişilerden ayrıca açık rıza alınması, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacaktır. Nitekim böyle bir durumda, ilgili kişi tarafından verilen açık rızanın geri alınması hâlinde kişisel veri işleme faaliyetinin

sona ereceği kanaatiyle hareket edileceğinden ve veri sorumlusunun diğer kişisel veri işleme şartlarından birine istinaden kişisel veri işleme faaliyetini sürdürmesi söz konusu olabileceğinden ilgili kişi yanıltılmış olacak ve böylelikle hukuka ve dürüstlük kurallarına aykırı bir durum ortaya çıkacaktır.

Bu kapsamda, veri sorumlusu tarafından kişisel veri işleme faaliyetinin öncelikli olarak açık rıza dışındaki işleme şartlarından birine dayanıp dayanmadığı değerlendirilmeli; eğer işlemeye temel teşkil eden amaç 6698 sayılı Kanun'da belirtilen açık rıza dışındaki şartlardan en az birini karşılamıyorsa, o zaman kişisel veri işleme faaliyetinin gerçekleştirilebilmesi için kişinin açık rızasının alınması yoluna gidilmelidir.

Kanun'un 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rıza; *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* şeklinde tanımlanmaktadır. ÜYZ ile kişisel verilerin işlenmesine ilişkin alınacak rızanın geçerli bir açık rıza olarak değerlendirilebilmesi için de bu unsurların sağlanması gerekmektedir.

ÜYZ ile gerçekleştirilen veri işleme faaliyetlerinde, ilgili kişilere işlemede YZ kullanıldığının açıkça belirtilmesi, açık rızanın geçerliliği için gerekli olmakla birlikte çoğu durumda tek başına yeterli olmamaktadır. Somut işlemenin niteliğine ve olası etkilerine bağlı olarak, açık rızanın geçerli olabilmesi için ilgili kişiye, ÜYZ kullanıldığının yanı sıra, şu hususlarda da bilgi verilmesinde fayda bulunmaktadır:

- Kullanılan ÜYZ sisteminin türü,
- Verinin ÜYZ'yi geliştirmek için mi yoksa çalıştırmak için mi işleneceği,
- İşleme sonucunda oluşturulacak verinin niteliği, işlevi ve amacı,
- İşlenen kişisel verilerin ÜYZ çıktıları yoluyla üçüncü kişiler tarafından görülme ihtimalinin bulunup bulunmadığı.

ÜYZ'nin kullanımı için alınan açık rızanın, ÜYZ'nin geliştirilmesini kapsamayacağı da vurgulanmalıdır. Ayrıca, ÜYZ çıktılarının da kişisel veri niteliği taşıyabileceği göz önünde bulundurulmalıdır. Bu kapsamda, ÜYZ'nin kullanımı amacıyla alınan açık rıza, doğrudan kişisel veri niteliğindeki çıktıların işlenmesini kapsamayacak olup bu tür verilerin işlenebilmesi için yeniden bir işleme şartının belirlenmesi gerekebilecektir.

Örneğin, kişilerin fotoğraflarını yükleyerek farklı filtrelerle portrelerini oluşturdukları uygulamalarda;

- Uygulamanın kullanılması,
- Yüklenen verilerin ÜYZ'nin geliştirilmesinde kullanılması,
- ÜYZ ile üretilen çıktıların depolanması,
- Çıktıların ÜYZ'nin geliştirilmesi amacıyla kullanılması

işlemlerinden her biri bağımsız birer kişisel veri işleme faaliyeti teşkil etmekte olup açık rızaya dayanılması durumunda her biri için ayrı ayrı açık rıza alınması önem taşımaktadır. Açık rıza alınırken yapılacak bilgilendirmenin açık, anlaşılır ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir. İlgili kişinin anlayamayacağı ölçüde uzun ve teknik terimlerle hazırlanmış bilgilendirmelere dayalı olarak alınan açık rıza, kural olarak geçerli kabul edilmeyecektir.

b. Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgili Olma

Kanun'un 5'inci maddesinin (2) numaralı fıkrasında sayılan işleme şartları arasında, *"bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* hâli de düzenlenmektedir. Bu kapsamda vurgulanması gereken husus, söz konusu şartın bir sözleşmenin metnine dâhil edilen her türlü veri işleme faaliyetine dayanak teşkil etmeyeceğidir. Bu işleme şartına dayanılabilmesi için veri işlemenin doğrudan sözleşmenin kurulması veya ifasıyla ilgili olması ve kişisel verilerin sözleşmenin taraflarına ait olması gerekmektedir. Dolayısıyla, sözleşme ile doğrudan bağlantısı bulunmayan ek veri işleme faaliyetleri bakımından bu şarta dayanılamayacak ve bu tür durumlarda başka bir işleme şartının değerlendirilmesi gerekecektir.

Örneğin;

- Bir sosyal medya uygulamasının kullanım sözleşmesinde, kullanıcı gönderi, fotoğraf veya mesajlarının ÜYZ modelini geliştirmede kullanılabileceğinin belirtildiği çoğu durumda, bu işlem hizmetin sunulması için zorunlu olmadığından, sözleşmenin ifası şartına dayanılması kural olarak mümkün olmayacaktır.
- ÜYZ destekli bir akıllı ev asistanı cihazı tarafından kullanıcının talimatlarına yanıt oluşturulması için verilerin işlenmesi gerekeceğinden, bu faaliyetlerin hizmetin ifası için gerekli olduğu kabul edilerek sözleşmenin ifası şartına dayanılması mümkün olabilecektir.
- Büyük dil modelleri (örneğin, ÜYZ tabanlı sohbet botları) tarafından verilen hizmetin ifası için kullanıcının girdilerinin işlenmesi gerektiğinden, bu faaliyetler de sözleşmenin ifası şartına dayandırılabilecektir.
- Akıllı ev asistanı cihazları aracılığıyla kişiselleştirilmiş reklam sunulmasına yönelik veri işleme faaliyetleri veya büyük dil modellerinin geliştirilmesi amacıyla kullanıcı verilerinin kullanılması, kullanım sözleşmesinin kurulması veya ifasıyla doğrudan ilişkili sayılamayacağından, bu şarta dayanılması mümkün olmayacak ve bu tür işlemler için ayrı bir işleme şartının varlığının değerlendirilmesi gerekebilecektir.

c. Verinin İlgili Kişi Tarafından Alenileştirilmiş Olması

ÜYZ sistemleri kapsamında gerçekleştirilecek kişisel veri işleme faaliyetleri bakımından öne çıkan bir diğer işleme şartı, verinin *"ilgili kişinin kendisi tarafından alenileştirilmiş olması"*dır. Bu kapsamda öncelikle, söz konusu işleme şartının, alenileştirilmiş verilerin herhangi bir amaçla serbestçe işlenebileceği anlamına gelmediği vurgulanmalıdır. Diğer bir ifadeyle, herkes tarafından serbestçe erişilebilen veri, herkes tarafından serbestçe işlenmeye açık veri anlamına gelmemektedir.

Alenileştirme şartına dayanılabilmesi için kişisel veri işleme faaliyetinin, ilgili kişinin alenileştirme iradesiyle uyumlu olması gerekmektedir. Bu doğrultuda, örneğin bir kişinin sosyal medya hesabını açık olarak kullanması, bu hesapta paylaştığı tüm verilerin ÜYZ sistemlerinde doğrudan girdi olarak veya bir ÜYZ modelinin geliştirilmesinde öğrenme seti kapsamında kullanılabileceği anlamına gelmemektedir. Bu tür bir kullanım, ilgili kişinin alenileştirme iradesinin sınırlarını aşacağından, söz konusu işleme şartına dayanılması bu durumda mümkün olmayacaktır.

d. Veri Sorumlusunun Meşru Menfaatleri için Veri İşlenmesinin Zorunlu Olması

ÜYZ bağlamında öne çıkan bir diğer işleme şartı, *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"*dır. Bu şarta ilişkin vurgulanması gereken ilk husus, meşru menfaate dayalı işleme şartının, diğer işleme şartları uygulanamadığında başvurulacak bir "son çare" olmadığı gibi, her şeyi kapsayabilecek ve tüm veri işleme faaliyetlerini hukuka uygun hâle getirecek bir "torba şart" niteliği de taşımadığıdır.

Bu işleme şartına dayanılabilmesi için temelde iki aşamalı bir değerlendirme yapılması gerekmektedir. Buna göre öncelikle, veri sorumlusunun meşru menfaatinin varlığı belirlenmeli; ardından, bu menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar vermediği ortaya konulmalıdır.

Bu doğrultuda Kurulun 25.03.2019 tarih ve 2019/78 sayılı Kararı'nda[29] belirtilen şu hususların da veri sorumluları tarafından dikkate alınması uygun olacaktır:

- Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,
- Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,
- Meşru menfaatin hâlihazırda mevcut, belirli ve açık olması,
- İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi hâlinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,
- Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin, bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,
- Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,
- Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,
- Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,
- Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testi yapılması.

Veri sorumlusunun meşru menfaati, kişisel veri işleme faaliyeti sonucunda elde edilecek faydaya yönelik olup, her somut olay özelinde ayrıca değerlendirilmelidir. Bu noktada önemli olan, veri sorumlusunun menfaati ile ilgili kişinin temel hak ve özgürlükleri üzerindeki etkileri ve buradaki yarışan menfaatler arasında makul bir dengenin kurulabilmesidir.

ÜYZ ile gerçekleştirilen işlemlerde meşru menfaat şartına dayanabilmek için, ilgili ÜYZ sisteminin kullanım amacına, etkisine ve verinin işlenme sürecine göre olay bazında bir değerlendirme yapılarak karar verilmesi gerekmektedir. Bu çerçevede, Kurulun 25.03.2019 tarih ve 2019/78 sayılı Kararı'nda

29 İlgili Karara ilişkin özeti görüntülemek için bkz. https://www.kvkk.gov.tr/Icerik/5434/2019-78.

belirtilen hususların, ÜYZ sistemleri kapsamında gerçekleştirilecek veri işleme faaliyetleri bakımından da dikkate alınması önem taşımaktadır.

Üzerinde durulması gereken bir diğer önemli husus, herkes tarafından serbestçe erişilebilen verilerin, ÜYZ sistemlerinin oluşturulması veya geliştirilmesi amacıyla ve meşru menfaat şartına dayanılarak işlenmesinin mümkün olup olmadığıdır. Zira daha önce de belirtildiği üzere, herkes tarafından serbestçe erişilebilen bir veri, herkes tarafından serbestçe işlenmeye açık veri anlamına gelmemektedir ve bu nedenle, bu tür verilerin alenileştirme şartına dayanılarak işlenmesi mümkün olmayacaktır. Bununla birlikte, ilgili kişinin kişisel verilerinin herkese açık ve kolayca erişilebilir bir platformda yer alması, meşru menfaat şartına ilişkin denge testinde göz önünde bulundurulabilecek bir unsurdur.

Örnek 11: Bir şirket, sosyal medya platformlarında kamuya açık olarak paylaşılan kişisel veri niteliğindeki biyografi, paylaşım ve yorumları toplayarak ("web kazıma" yöntemiyle) kendi dil modelini eğitmek istemektedir.

İlgili kişiler bu verileri alenileştirirken ÜYZ modellerinin geliştirilmesi amacını taşımadıklarından, bu verilerin alenileştirme şartına dayanılarak ÜYZ modelinin eğitimi amacıyla işlenmesi mümkün olmayacaktır.

Ancak, bu verilerin ilgili kişiler tarafından herkese açık hâle getirilmiş olması, denge testinde dikkate alınabilecektir.

Bununla birlikte, söz konusu işleme faaliyeti sonucunda ilgili kişi açısından olumsuz bir sonucun ortaya çıkması ihtimali bulunması durumunda, meşru menfaat şartına dayanılması mümkün olmayacaktır. Örneğin, bir kişinin internet ortamında bulunan fotoğraf veya bilgileri kullanılarak o kişinin yüzünü, sesini veya yazışma tarzını taklit eden modellerin geliştirilmesi durumunda, söz konusu işleme şartına dayanılamayacaktır.

Her ne kadar 6698 sayılı Kanun tarafından zorunlu tutulmamış olsa da meşru menfaate dayalı veri işleme faaliyetlerinde, menfaat çatışmalarının dengelenmesi sürecinde özellikle etkileri itibarıyla ilgili kişilerin hayatları üzerinde önemli sonuçlar doğurabilecek olan ÜYZ sistem ve modelleriyle gerçekleştirilecek işlemeler bakımından veri koruma etki değerlendirmesi yapılması faydalı olacaktır. Bu kapsamda; ÜYZ ile yapılacak işlemenin gerekli olup olmadığı, veri sorumlusuna sağladığı menfaatin ne olduğu, aynı menfaatin ÜYZ ile işleme olmaksızın elde edilmesinin mümkün olup olmadığı, ilgili kişilerin mahremiyetleri kapsamındaki makul beklentileri ve veri işleme sonucunda ortaya çıkabilecek olası olumsuz etkiler gibi hususların önceden değerlendirilmesi önerilmektedir.

B. Özel Nitelikli Kişisel Veriler Açısından Uygun İşleme Şartının Belirlenmesi

Özel nitelikli kişisel verilerin neler olduğu ve bu verilerin işlenme şartları 6698 sayılı Kanun'un 6'ncı maddesinde sayılmaktadır. Buna göre; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olup bu verilerin işlenmesi yasaktır. Ancak, aşağıdaki hâllerden birinin varlığı durumunda bu verilerin işlenmesi mümkündür:

- İlgili kişinin açık rızasının olması.
- 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.
- İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması.
- Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması.
- 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.
- İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması.
- 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.

6698 sayılı Kanun, özel nitelikli olarak sınıflandırılan kişisel verilerin korunmasına özel bir önem atfetmekte ve bu tür verilerin işlenmesini kural olarak yasaklamakta, işlenecekleri hâllerde ise bu verilerin niteliği gereği ortaya çıkabilecek risklerin azaltılmasını teminen özel önlemlerin alınmasını gerektirmektedir.

Özel nitelikli kişisel verilerin ÜYZ sistemleri kapsamında işlenmesi durumunda, bu verilerin niteliğinden kaynaklı olarak ilgili kişinin mağdur olmasına veya ayrımcılığa maruz kalmasına neden olabilecek sonuçların ortaya çıkması ihtimali bulunmaktadır. Bu nedenle, bu tür durumlarda özel nitelikli kişisel verilerin işlenmesinden kaynaklanabilecek risklerin dikkatle değerlendirilmesi ve bu riskleri en aza indirecek uygun önlemlerin alınması önem taşımaktadır.

İşleme şartları bakımından değerlendirildiğinde ise Kanun'un 5'inci ve 6'ncı maddeleri arasında önemli farklar bulunmaktadır. Her iki maddede de ilgili kişinin açık rızasının varlığı ve ilgili kişi tarafından alenileştirilmiş olması hâlleri işleme şartı olarak yer almakla birlikte, sözleşmesel gereklilik ve meşru menfaat sebepleri özel nitelikli kişisel veriler için öngörülmemiştir. Diğer yandan, Kanun'un 5'inci maddesinden farklı olarak 6'ncı maddede, sağlık, istihdam ve vakıflarla derneklere ilişkin bazı alanlarda özel nitelikli kişisel verilerin açık rıza aranmaksızın işlenebileceği düzenlenmiştir.

Kurulun 31.01.2018 tarih ve 2018/10 sayılı Kararı'nda[30], özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler açıklanmakta olup ÜYZ sistemleri kapsamında gerçekleştirilecek kişisel veri işleme faaliyetlerinde de söz konusu önlemlerin dikkate alınması gerekmektedir.

İşlenen verilerin sağlık verisi olması hâlinde ise sağlık verilerinin işlenmesine ilişkin mevzuat hükümlerine uygun hareket edilmesi gerektiğinin de vurgulanması önem taşımaktadır.

> ÜYZ sistemleri kapsamında gerçekleştirilecek kişisel veri işleme faaliyetlerinde de 6698 sayılı Kanun'da yer alan sınırlı sayıdaki işleme şartlarından en az birine dayanılması zorunludur. Kanun'un 5'inci ve 6'ncı maddelerinde her ne kadar doğrudan YZ/ÜYZ'ye ilişkin bir atıf bulunmasa da, bu hükümlerde yer alan işleme şartlarının çerçeve niteliği, YZ/ÜYZ ile ilgili kişisel veri işleme faaliyetlerine de uygulanabilmelerine imkân tanımaktadır.
>
> Bu doğrultuda, ÜYZ sistemleri kapsamında kişisel verilerin işlenmesi gereken durumlarda, ÜYZ'nin geliştirilmesi ve kullanılması süreçlerinde her bir işleme faaliyeti tespit edilmeli ve buna göre uygun işleme şartı belirlenmelidir.

30 İlgili Kararı görüntülemek için bkz. https://www.kvkk.gov.tr/Icerik/4110/2018-10.

10. Üretken Yapay Zekâ Sistemlerinde Kişisel Verilerin Yurt Dışına Aktarımı Nasıl Değerlendirilmelidir?

Kişisel verilerin yurt dışına aktarımı, 6698 sayılı Kanun'un 9'uncu maddesinde hükme bağlanmıştır. Buna göre kişisel veriler, veri sorumlusu ve veri işleyen tarafından:

Kanun'un 5 ve 6'ncı maddelerinde belirtilen şartlardan birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında verilmiş yeterlilik kararı bulunması hâlinde, yurt dışına aktarılabilir. Yeterlilik kararı, Kurul tarafından verilir ve Resmî Gazete'de yayımlanır. Yeterlilik kararı verilirken öncelikle Kanun'un 9'uncu maddesinin (3) numaralı fıkrasında yer alan hususlar dikkate alınır. Yeterlilik kararı, en geç dört yılda bir değerlendirilir. Kurul, değerlendirme sonucunda veya gerekli gördüğü diğer hâllerde, yeterlilik kararını ileriye etkili olmak üzere değiştirebilir, askıya alabilir veya kaldırabilir.

Kurul tarafından verilen yeterlilik kararının bulunmaması durumunda, Kanun'un 5'inci ve 6'ncı maddelerinde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, Kanun'un 9'uncu maddesinin (4) numaralı fıkrasında yer alan uygun güvencelerden birinin taraflarca sağlanması hâlinde yurt dışına aktarılabilir.

Yeterlilik kararının bulunmaması ve 9'uncu maddenin (4) numaralı fıkrasında öngörülen uygun güvencelerden herhangi birinin de sağlanamaması durumunda ise kişisel veriler, arızi olmak kaydıyla sadece Kanun'un 9'uncu maddesinin (6) numaralı fıkrasında yer alan hâllerden birinin varlığı hâlinde yurt dışına aktarabilir. Ancak mezkur (6) numaralı fıkranın (a), (b) ve (c) bentlerinde sayılan arızi haller kamu kurum ve kuruluşlarının kamu hukukuna tâbi faaliyetlerine uygulanmaz.

Veri sorumlusu ve veri işleyenler tarafından, yurt dışına aktarılan kişisel verilerin sonraki aktarımları ve uluslararası kuruluşlara aktarımlar bakımından da bu Kanun'da yer alan güvenceler sağlanır ve 9'uncu madde hükümleri uygulanır.

Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

10.07.2024 tarih ve 32598 sayılı Resmi Gazete'de "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" yayımlanmıştır. Bu yönetmelik ile: i) yeterlilik kararına dayalı

aktarımların, ii) uygun güvencelere dayalı aktarımların, iii) arızi aktarımların uygulanmasına ilişkin usul ve esaslar belirlenmiştir.

Türkiye'de faaliyet gösteren veri sorumlularının, yurt dışında yerleşik birtakım hizmet sağlayıcılar aracılığıyla ÜYZ sistemlerini kullanmaları ve bu sistemler aracılığıyla kişisel verilerin yurt dışına aktarılması durumunda, söz konusu veri aktarım faaliyetinin 6698 sayılı Kanun'un 9'uncu maddesi ile Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'e uygun şekilde gerçekleştirilmesi gerekmektedir.

Bu çerçevede, Kanun'un 9'uncu maddesi kapsamında gerçekleştirilecek aktarımlara ilişkin yol gösterilmesi amacıyla Kurum tarafından hazırlanmış olan *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"*[31] de dikkate alınabilecektir.

31 Söz konusu Rehberi görüntülemek için bkz. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf.

11. Üretken Yapay Zekâ Sistemleri Bağlamında Şeffaflık Nasıl Sağlanabilir?

6698 sayılı Kanun'un "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10'uncu maddesinde, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişinin, ilgili kişilere;

a. Veri sorumlusunun ve varsa temsilcisinin kimliği,
b. Kişisel verilerin hangi amaçla işleneceği,
c. İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
ç. Kişisel veri toplamanın yöntemi ve hukuki sebebi,
d. 11'inci maddede sayılan diğer hakları

konularında bilgi vermekle yükümlü olduğu düzenlenmiştir.

Bu kapsamda, Kanun'un 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğü, 10.03.2018 tarih ve 30356 sayılı Resmî Gazete'de yayımlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" hükümlerine uygun olarak yerine getirilmelidir.

ÜYZ sistemlerinde şeffaflığın sağlanması, ilgili kişilerin veri işleme süreçlerine dair bilgi sahibi olmalarının ve kişisel verileri üzerindeki denetim haklarını etkin bir şekilde kullanabilmelerinin temini açısından önemli bir unsurdur. Bu kapsamda, 6698 sayılı Kanun'un 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğü ile 10.03.2018 tarih ve 30356 sayılı Resmî Gazete'de yayımlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ", ÜYZ sistemleri açısından da geçerli temel çerçeveyi ortaya koymaktadır.

Bu doğrultuda, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi tarafından, ilgili kişilere Kanun'un 10'uncu maddesinde sayılan unsurlar konusunda bilgi verilmesi gerekmektedir. Ayrıca, ilgili kişinin açık rızasına veya Kanun'daki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmeli ve kişisel veri işleme amacında bir değişiklik söz konusu olduğunda, ilgili kişilere bu amaca yönelik olarak yeniden aydınlatma yapılmalıdır. Özellikle bir ÜYZ sistemini ya da bu sisteme ait arayüzü kullanmak için yapılacak işlemeler ile mevcut sistem ve modellerin geliştirilmesi için yapılacak işlemeler için ayrı ve açıkça aydınlatma

yapılması önem arz etmektedir. Bunun yanı sıra açık rızaya dayalı veri işleme süreçlerinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemleri ayrı ayrı yerine getirilmelidir. Bu bağlamda aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılan bildirim anlaşılır, açık ve sade bir dille sunulmalıdır.

ÜYZ sistemlerinin farklı aşamalarında gerçekleştirilen kişisel veri işleme faaliyetlerinin şeffaf bir şekilde yürütülebilmesi adına bu faaliyetlere ilişkin bilgilerin güncel ve erişilebilir şekilde sunulması önem taşımaktadır. Özellikle aydınlatma metinlerinin ve varsa gizlilik politikalarının, mevcut ve potansiyel kullanıcılar tarafından kolaylıkla erişilebilir bir biçimde sistem arayüzlerinde sunulması bilgiye erişimi kolaylaştıracaktır. Ayrıca, kişisel verilerin hizmet sunumunun ötesinde, ÜYZ sistemlerinin eğitimi ve geliştirilmesine yönelik süreçlerde de kullanılması durumunda, bu tür kullanım biçimlerine dair bilgilere aydınlatma metinlerinde yer verilmesi, ilgili kişilerin beklentilerinin yönetilmesi ve veri işleme süreçlerine ilişkin şeffaflık düzeyinin artırılması açısından faydalı olacaktır.

Bunun yanı sıra, sistemlerde yapılan güncellemeler sonucunda veri işleme faaliyetlerinde bir değişiklik meydana gelmesi durumunda, bu değişikliklerin kullanıcılarla paylaşılması da bu sistemlerde şeffaflığın sağlanmasına katkıda bulunacaktır. Kullanıcı arayüzlerinin, varsayılan gizlilik ayarları hakkında bilgi sunacak şekilde tasarlanması ve bu ayarların kullanıcılar tarafından kolayca görüntülenip değiştirilebileceği kontrol mekanizmaları ile desteklenmesi, kullanıcıların bilinçli tercihler yapmalarını kolaylaştıracaktır.

Bu bağlamda, ÜYZ sistemlerinin kullanıcıyla doğrudan etkileşimde bulunduğu (sohbet botları gibi) durumlara da değinilmesinde fayda görülmektedir. Bazı sistemler, kullanıcıyla doğrudan iletişim kurmakta ya da karar destek mekanizmalarında rol oynamaktadır. Bu tür sistemlerle etkileşimde bulunan bireylerin, bir ÜYZ sistemiyle iletişim kurduklarını açıkça bilmeleri önem taşımaktadır. Sistemlerin, ÜYZ temelli olduğunu açıkça belirten bir bilgilendirme mekanizması içermesi, hem şeffaflığın hem de kullanıcı güvenliğinin sağlanması açısından dikkate alınması gereken bir husustur.

Diğer taraftan, ÜYZ sistemlerinin geliştirilmesinde kullanılan veri kümelerine ilişkin olarak yeterli düzeyde şeffaflığın sağlanmaması, kişisel verilerin korunması ve bireylerin mahremiyetinin güvence altına alınmasına ilişkin endişelere yol açabilmektedir. Bu çerçevede, sistemin eğitiminde kullanılan veri setlerinin kaynağı, toplama yöntemi, işleme ölçütleri ve denetim mekanizmaları hakkında makul ölçüde açıklık sağlanmasında fayda bulunmaktadır. Özellikle, doğrudan ilgili kişiden elde edilmeyen ve örneğin, kamuya açık kaynaklardan otomatik yollarla toplanan kişisel verilerin söz konusu olduğu durumlarda, bu tür veri işleme faaliyetlerinin şeffaflığı ve hukuka uygunluğu daha dikkatli bir değerlendirme gerektirmektedir. Bu çerçevede, kişisel verilerin ilgili kişiden elde edilmemesi hâlinde, kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde ilgili kişiye karşı aydınlatma yükümlülüğünün yerine getirilmesi beklenmektedir. Bununla birlikte, ilgili kişilere doğrudan aydınlatma yapılmasının mümkün olmadığı (örneğin, teknik açıdan imkânsızlık bulunması) hâllerde ise kamuya açık aydınlatma metinleri aracılığıyla bu veri işleme faaliyetleri hakkında açık, anlaşılabilir ve erişilebilir bilgiler sunulmasının faydalı olacağı değerlendirilmektedir.

Öte yandan, ÜYZ sistemlerinde şeffaflığın sağlanması yalnızca ilgili kişilere yönelik bilgilendirmelerle sınırlı olmayıp bu sistemlerin kullanımına dahil olan diğer paydaşlara yönelik bilgi akışını da kapsayabilmektedir. Bu çerçevede, ÜYZ sistemlerinin sağlayıcılarının, sistemin kullanımı sırasında ortaya çıkabilecek olası gizlilik ve veri koruma riskleri ile bu risklere karşı geliştirilen politika ve uygulamalar hakkında, sistemleri entegre eden veya yeniden yapılandırarak kullanan yerleştiricileri bilgilendirmeleri önem arz etmektedir. Söz konusu riskler ve ilgili kontrol mekanizmalarına ilişkin bilgilerin, sistemin hem devreye alınmasından önce hem de kullanım sürecinde açık, anlaşılabilir ve erişilebilir şekilde sunulması, sistemlerin güvenli ve sorumlu şekilde işletilmesine katkı sağlayacaktır.

12. Üretken Yapay Zekâ Sistemleri Kapsamında İlgili Kişilerin Hakları Nasıl Kullandırılabilir?

6698 sayılı Kanun'un 11'inci maddesinde ilgili kişinin hakları düzenlenmiş olup buna göre herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a. Kişisel veri işlenip işlenmediğini öğrenme,
b. Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
c. Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
ç. Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
d. Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
e. 7'nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
f. (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
g. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
ğ. Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme

haklarına sahiptir.

ÜYZ sistemlerinin kendine özgü yapısal ve işlevsel özellikleri nedeniyle, 6698 sayılı Kanun'un 11'inci maddesi ile güvence altına alınan ilgili kişi haklarının uygulanmasında birtakım pratik zorluklar ortaya çıkabilmektedir. Bu sistemlerde kişisel verilerin çok katmanlı yapılarda ve farklı teknik süreçler aracılığıyla işlenmesi, bireylerin veri işleme faaliyetlerine ilişkin bilgi edinme, veriye erişim sağlama, verilerin düzeltilmesini, silinmesini veya yok edilmesini talep etme gibi haklarının kullanımını güçleştirebilmektedir.

Bununla birlikte, veri sorumlularının ilgili kişi haklarının etkin biçimde kullanılmasını sağlamaya yönelik yükümlülükleri, ÜYZ sistemleri açısından da geçerliliğini korumaktadır. Söz konusu sistemlerin

işleyiş biçimi, bu hakların kullanımında bazı güçlükler doğursa da, bu durum Kanun'un 11'inci maddesinde düzenlenen ilgili kişi haklarının uygulanamaz hâle gelmesi sonucunu doğurmamaktadır. Bu bağlamda, ÜYZ sistemlerinin kendine özgü nitelikleri göz önünde bulundurularak uygun teknik ve idari mekanizmaların yapılandırılması, ilgili kişi haklarının bu sistemler kapsamında da etkili biçimde kullanılabilmesine katkı sağlayacaktır.

ÜYZ sistemlerinin, karar alma süreçlerinde destekleyici veya belirleyici biçimde kullanılması, ilgili kişi haklarının uygulanması bakımından daha da kritik bir hâl alabilmektedir. Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (g) bendinde düzenlenen *"işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme"* hakkı, bireylerin bu tür sistemler aracılığıyla yürütülen karar süreçlerinde kendileri aleyhine ortaya çıkan bir sonuca karşı değerlendirme talep edebilmelerine imkân sağlayan önemli bir güvence olarak değerlendirilmektedir.

Günümüzde otomatik karar alma mekanizmaları; işe alım, kredi değerlendirmesi ve sigortacılık gibi birçok alanda yaygın olarak kullanılmakta ve ÜYZ sistemleri de bu süreçlerde bireylerle ilgili değerlendirme ve kararların şekillenmesinde rol oynayabilmektedir. Ancak bu sistemlerde kullanılan algoritmaların karmaşıklığı ve karar alma süreçlerine dair şeffaflık düzeyinin düşük olması, bireylerin kendileri hakkında alınan kararların gerekçesini anlayabilmelerini ve bu bağlamda haklarını kullanabilmelerini güçleştirmektedir.

Bu çerçevede, ÜYZ sistemlerinin karar alma süreçlerinde kullanılmasının planlandığı hâllerde, bu kullanımın haksız, ayrımcı veya etik dışı sonuçlara yol açma potansiyeli taşıyıp taşımadığının dikkatle değerlendirilmesi ve ilgili risklerin yeterince öngörülemediği ya da yönetilemediği durumlarda, bu tür sistemlerin devreye alınıp alınmaması konusunda ihtiyatlı bir yaklaşım benimsenmesi uygun olacaktır.

Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (g) bendinde düzenlenen itiraz hakkı, yalnızca alınan kararın sonucuna karşı değil, aynı zamanda kararın dayandığı temellerin yeniden değerlendirilmesini talep etme imkânı sunan bir araç olarak da değerlendirilebilir. Bu düzenleme, bireylerin verileri üzerindeki denetimini ve karar süreçleri hakkında bilgi edinme hakkını esas alan insan merkezli veri işleme anlayışının mevzuata yansıyan bir örneği olarak da düşünülebilir. İnsan odaklı yaklaşım, veri işleme süreçlerinde şeffaflığın artırılması, bireylerin verileri üzerindeki kontrolünün güçlendirilmesi ve adil karar alma mekanizmalarının teşvik edilmesi gibi hedefleri içermektedir. Bu bağlamda itiraz hakkı, bireylere kendileri hakkında verilen kararların gerekçelerini sorgulama imkânı sunmakla kalmayıp, aynı zamanda karar süreçlerinin daha şeffaf, hesap verebilir ve gerektiğinde insan müdahalesine açık bir şekilde yürütülmesini destekleyen bir mekanizma olarak öne çıkmaktadır.

İlgili kişi haklarının gözetilmesi yalnızca karar süreçleriyle sınırlı olmayıp, ÜYZ sistemlerinde kişisel verilerin işlendiği tüm aşamaları kapsayacak biçimde ele alınmalıdır. Bu doğrultuda; eğitim verileri, ince ayar süreçlerinde kullanılan veriler, model çıktılarında yer alan bilgiler ile kullanıcı sorgularına dâhil edilen içerikler de bu kapsama dahildir. Sistemin yaşam döngüsünün her aşamasında bireylerin Kanun'un 11'inci maddesi kapsamında sahip oldukları hakları etkili biçimde kullanabilmelerini sağlayacak açık, erişilebilir ve işlevsel mekanizmaların oluşturulması bu nedenle büyük önem taşımaktadır.

Öte yandan, veri sorumlularının sistemin tüm aşamalarındaki kişisel veri işleme faaliyetlerini tanımlayabilmeleri ve bu faaliyetlere ilişkin izlenebilirlik sağlayacak teknik ve idari süreçleri yapılandırmaları, hem hesap verebilirliğin sağlanması hem de ilgili kişilerin başvurularının zamanında ve etkin biçimde karşılanabilmesi bakımından önem arz etmektedir. Bu kapsamda, veri işleme süreçlerine ilişkin kayıtların sistematik biçimde tutulması ve veri kümelerinin yönetiminde izlenebilirlik sağlayan araçların kullanılması gibi uygulamalar, ilgili kişi başvurularının değerlendirilmesini kolaylaştırabilecektir. Ayrıca, eğitim verilerinin kaynağına ve niteliğine açıklık kazandırabilecek veri eşleştirme *(data mapping)* ve veri etiketleme *(data labeling)* gibi yöntemler de bu süreci destekleyebilecek araçlar arasında yer almaktadır.

Diğer taraftan, ilgili kişilerin haklarını kullanabilmelerine yönelik gerekli tedbirlerin yalnızca sistemin kullanım aşamasına özgülenmemesi ve tasarım ile geliştirme süreçlerinden itibaren bu hususların gözetilmesi, kişisel verilerin korunmasına yönelik yaklaşımın proaktif temeller üzerinde inşa edilmesine imkân tanıyacaktır. Bu kapsamda, "tasarımdan itibaren mahremiyet" *(privacy by design)* ile "varsayılan olarak mahremiyet" *(privacy by default)* yaklaşımlarının benimsenmesi, bireylerin haklarının ÜYZ sistemleri bağlamında sistematik ve sürdürülebilir biçimde gözetilmesine önemli katkılar sunacaktır.

13. Üretken Yapay Zekâ Sistemlerinde Kişisel Verilerin Güvenliği Açısından Nelere Dikkat Edilmelidir?

6698 sayılı Kanun'un 12'nci maddesinde veri güvenliğine ilişkin yükümlülükler düzenlenmektedir. Anılan maddenin (1) numaralı fıkrası uyarınca veri sorumlusu;

a. Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b. Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c. Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Bahse konu maddenin (2) numaralı fıkrasına göre ise veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, maddenin (1) numaralı fıkrasında belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

ÜYZ sistemlerinin gelişimi, kişisel verilerin güvenliği açısından dikkate değer bir dizi yeni riski de beraberinde getirmektedir. Bu riskler, özellikle sistemin veriyle kurduğu ilişki ve işleme süreçlerinin niteliği bakımından, geleneksel sistemlerden farklılaşabilmektedir. Bu çerçevede ÜYZ'ye özgü güvenlik riskleri; eğitim verilerinin güvenilir olmaması, sistemlerin yapısal karmaşıklığı, şeffaflık eksikliği ve yeterli test süreçlerinin yürütülmemesi gibi faktörlerden kaynaklanabilmektedir.

Bu bağlamda, ÜYZ sistemlerinin yaşam döngüsü içerisinde kişisel verilerin işlendiği durumlarda veri sorumlularının, 6698 sayılı Kanun'un 12'nci maddesi uyarınca, kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla, uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almaları gerekmektedir.

Bu çerçevede, ÜYZ sistemlerinde kişisel veri güvenliğini temin etmeye yönelik olarak dikkate alınabilecek bazı teknik ve idari tedbirler aşağıda örnek mahiyetinde sunulmaktadır:

- "Tasarımdan itibaren mahremiyet" *(privacy by design)* ile "varsayılan olarak mahremiyet" *(privacy by default)* yaklaşımları, veri işleme faaliyetinin başlangıç aşamasından itibaren tüm yaşam döngüsü boyunca kişisel verilerin korunmasında destekleyici bir işlev görebilir. Risk temelli bir yaklaşımla bu bakış açısına uygun hareket edilmesi, ÜYZ sistemlerinin ortaya çıkarabileceği tehdit ve risklerin önceden dikkate alınmasını ve zamanında bertaraf edilmesini kolaylaştırabilir. Bu kapsamda, sistemlerin tasarımından itibaren veri korumayı önceleyen tekniklerin benimsenmesi ve ilgili kişilere verilerinin işlenmesinde anlamlı kontrol sağlayabilecek ayar ve mekanizmaların oluşturulması, bireylerin haklarının korunmasının yanı sıra kullanıcıda güven tesis edilmesi açısından da önem taşımaktadır.

- Sistemlerin yaşam döngüsünün her aşamasında karşılaşılabilecek risklerin tanımlanması, değerlendirilmesi ve yönetilmesi amacıyla veri koruma etki değerlendirmesi yapılması, ÜYZ sistemleri açısından iyi uygulama örneklerinden biri olarak değerlendirilebilir. Bu değerlendirmeler, işleme faaliyetinin kapsamı ve bireyler üzerindeki olası etkilerin anlaşılmasını sağlamanın yanı sıra bu risklerin önüne geçilmesine yönelik önlemlerin şekillendirilmesine katkı sunabilir. Ayrıca, uygun veri yönetişimi yaklaşımlarıyla birlikte düşünüldüğünde, veri güvenliğinin bütüncül şekilde ele alınmasına da imkân sağlayabilir.

- Mahremiyet artırıcı teknolojilerin *(privacy-enhancing technologies)* ÜYZ sistemlerine entegre edilmesi, kişisel verilerin işlenmesinde mahremiyetin teknik düzeyde gözetilmesine imkân tanıyacaktır. Bu teknolojilerin, sistemin tasarımına erken aşamada dâhil edilmesi, olası veri ihlallerinin önlenmesine katkı sunabileceği gibi sistem güvenliğinin bütüncül olarak güçlendirilmesine de hizmet edebilecektir. Özellikle geniş bir YZ ekosistemi içerisinde çalışması planlanan sensörlü otonom araç sistemleri ve bunların ses-görüntü bileşenleri, ÜYZ sistemlerine bağlı gözlük ya da kamera sistemleri, artırılmış gerçeklik ekipmanları gibi anlık şekilde çevreden yüksek miktarda veri toplayıp bu verileri işleyen sistemler bakımından, bu teknolojilerin tasarımdan itibaren mahremiyet ilkesi ile birlikte göz önünde bulundurulması ve bu sistemlerdeki veri işleme faaliyetleri ile veri akışlarının mahremiyet artırıcı tekniklerle desteklenmesi önem taşımaktadır.

- Geleneksel bilgi teknolojisi sistemlerinde uygulanan güvenlik önlemlerine ek olarak, ÜYZ sistemlerinin hâlihazırda bilinen zafiyetlerine (modeli ters çevirme saldırıları, istem enjeksiyonu, jailbreak girişimleri ve üyelik çıkarımı saldırıları gibi) karşı teknik kontrollerin entegre edilmesi ve bu kontrollerin düzenli olarak izlenip gözden geçirilmesi, güvenliğin sürekliliği açısından önem taşımaktadır.

- Bilinmeyen risklerin ortaya konulmasına yönelik "kırmızı takım" *(red teaming)* tekniklerinin uygulanması, ÜYZ sistemlerindeki zayıf noktaların ve geliştirilmesi gereken alanların daha erken tespit edilmesine imkân sağlayabilir. Bu tür test süreçlerinin farklı cinsiyet, mesleki geçmiş ve uzmanlık alanlarından katılımcılarla yürütülmesi, değerlendirmelerin kapsam ve derinliğini artıracaktır.

- Veri sorumlularının, yalnızca güvenilir kaynaklardan temin edilen veri kümelerini kullanmaları ve kurum içi veri kümeleri de dâhil olmak üzere düzenli doğrulama ve geçerlilik kontrolleri gerçekleştirmeleri faydalı olacaktır.

- Risklerin dinamik yapısı dikkate alınarak, risk değerlendirmelerinin düzenli olarak gözden geçirilmesinde, gerektiğinde güncellenmesinde ve gelecekteki zararların önlenmesi adına bu risklerin temel nedenleri tespit edilerek azaltılmasına öncelik verilmesinde fayda bulunmaktadır.

- ÜYZ sistemlerinin kullanımına bağlı güvenlik risklerinin tanımlanması ve bu risklerin ele alınması konusunda çalışanlara yönelik bilinçlendirme faaliyetleri ve eğitim süreçlerinin yürütülmesi, kişisel veri güvenliği kültürünün kurumsal düzeyde yerleşmesine katkı sağlayacaktır.

- ÜYZ sistemleriyle ilgili güncel güvenlik açıkları ve tehdit ortamına ilişkin gelişmelerin yakından takip edilmesi ve bu doğrultuda önleyici tedbirlerin sistemli şekilde hayata geçirilmesi, risk yönetiminin proaktif bir zeminde yürütülmesini destekleyecektir.

- Yama yönetimi ve yazılım güncellemelerine ilişkin süreçlerin düzenli olarak işletilmesi, bilinen güvenlik açıklarının hızla giderilmesine ve kötü amaçlı yazılımların sistemlere sızmasının önlenmesine yardımcı olacaktır.

- Yetkisiz erişimlerin önlenmesine yönelik olarak çok faktörlü kimlik doğrulama gibi yöntemlerin benimsenmesi, kullanıcı hesaplarının ve sistem bileşenlerinin daha güvenli ve denetlenebilir biçimde korunmasına katkı sağlayacaktır.

- ÜYZ sistemlerinde kişisel veri işleme faaliyetlerine ilişkin işlem kayıtları ile sistem günlüklerinin güvenli biçimde saklanması, olası ihlallerin tespit edilmesi ve müdahale süreçlerinin etkin şekilde yürütülmesi açısından işlevsel bir araç niteliği taşımaktadır. Bu kayıtların denetlenebilir biçimde tutulması ise sistemin şeffaflığını ve hesap verebilirliği destekleyen bir unsur olarak değerlendirilebilecektir.

6698 sayılı Kanun uyarınca, kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla, veri sorumlularına yol göstermek üzere Kurum tarafından hazırlanmış olan *"Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)"*[32] başlıklı dokümanın da bu süreçte dikkate alınması mümkündür.

32 Söz konusu Rehberi görüntülemek için bkz. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf

14. Günlük Hayatta Üretken Yapay Zekâ Uygulamalarını Kullanırken Kişisel Verilerin Korunması Açısından Bireyler Hangi Hususlara Dikkat Etmelidir?

ÜYZ teknolojileri; metin, görsel, ses ve yazılım kodu gibi farklı içerik türlerinin hızlı ve etkili bir biçimde üretilmesini mümkün kılarak eğitim, iletişim, sağlık, finans, hukuk ve kamu hizmetleri gibi birçok alanda önemli kolaylıklar sunmakta ve verimliliği artırmaktadır. Bununla birlikte, bu sistemlerle kurulan etkileşimler kapsamında ortaya çıkabilecek kişisel verilerin korunmasına ilişkin riskler göz ardı edilemeyecek düzeydedir. Bu çerçevede, bireylerin ÜYZ uygulamalarını kullanırken kişisel veri güvenliğini önceleyen bilinçli bir tutum sergilemeleri bir gereklilik olarak öne çıkmaktadır.

Öncelikle, bireylerin bu sistemler ile kurdukları etkileşimlerde sundukları içeriklerde yer alan bilgilerin mahiyetini dikkatle değerlendirmeleri önem taşımaktadır. Özellikle ad-soyad, adres, telefon numarası ve kimlik bilgileri gibi kişiyi doğrudan ya da dolaylı olarak tanımlamaya elverişli kişisel verilerin paylaşımından kaçınılmalıdır. Bu tür verilerin yetkisiz kişilerce ele geçirilmesi durumunda, gizliliğin ihlali, kimlik hırsızlığı veya diğer kötüye kullanımlar gibi ciddi sonuçlar doğabileceği unutulmamalıdır.

Benzer şekilde, üçüncü kişilere ait kişisel verilerin de bu sistemlerle paylaşılmamasına özen gösterilmelidir. Zira kişilerin bilgisi olmaksızın verilerinin bu sistemlerle paylaşılması, istenmeyen sonuçlar doğurabilir ve kişilerin özel yaşamını olumsuz etkileyebilir. Bu nedenle, bireylerin ÜYZ sistemlerini kullanırken üçüncü kişilere ait bilgilerin ifşasına yol açabilecek içerikleri paylaşmaktan kaçınmalarında fayda bulunmaktadır.

ÜYZ sistemleriyle bilgi paylaşımı yapılırken, mümkün olduğunca anonimleştirilmiş ve genelleştirilmiş ifadelerin tercih edilmesi tavsiye edilmektedir. Örneğin bir olay aktarılırken, kişi isimleri, tarih veya konum gibi belirli ayrıntıların yerine soyut ve genel bir anlatımın benimsenmesi, kişisel veri paylaşımının önlenmesinde etkili bir yöntem olabilir. Bu yaklaşım, hem bireylerin mahremiyetlerinin korunmasına katkı sunacak hem de bu sistemlerle kurulan etkileşimlerde veri temelli risklerin azaltılmasına imkân sağlayabilecektir.

Bunun yanı sıra, bireylerin kullandıkları ÜYZ uygulamalarının veri işleme faaliyetlerine ilişkin yeterli farkındalığa sahip olmaları da bir gereklilik olarak değerlendirilmektedir. Bu bağlamda, söz konusu uygulamaların hangi tür verileri topladığı, bu verileri hangi amaçlarla işlediği, kimlerle paylaştığı ve ne kadar süreyle sakladığı gibi hususlarda kullanıcıların yeterli bilgiye sahip olmaları önem arz etmektedir. Bu doğrultuda, ilgili aydınlatma metinleri ile gizlilik politikalarının dikkatle incelenmesi, bireylerin veri işleme süreçlerine daha bilinçli şekilde katılımını sağlayacaktır. Ayrıca gizlilik ayarlarının gözden

geçirilmesi, yalnızca gerekli bilgilerin sağlanması ve mümkün olan durumlarda veri paylaşımını sınırlayıcı tercihlerin aktif hâle getirilmesi, bireysel gizliliğe katkı sunan adımlar arasında yer almaktadır.

Özellikle sağlık verileri, finansal bilgiler, hukuki süreçlere ilişkin bilgiler ve bunlara benzer hassas nitelikteki konulara ilişkin bilgilerin, ÜYZ sistemleri ile paylaşılmasından kaçınılması gerektiği de unutulmamalıdır. Zira bu tür bilgiler, bireylerin hem fiziksel hem de dijital güvenliğini tehdit edebilecek mahiyettedir ve yetkisiz erişim durumunda ciddi hak ihlallerine veya zararlara neden olabilir. Bu nedenle, bu tür bilgilerin paylaşılmak istenmesi durumunda çok daha bilinçli ve temkinli bir tutum sergilenmesi önem taşımaktadır.

Sonuç olarak, ÜYZ teknolojileri, doğru ve bilinçli kullanıldığında hem bireyler hem de kurumlar açısından önemli fırsatlar sunmaktadır. Ancak bu teknolojilerden güvenli şekilde faydalanılabilmesi; kişisel verilerin korunması, mahremiyetin güvence altına alınması ve veri güvenliğine ilişkin risklerin en aza indirilmesi ile mümkündür. Bu bağlamda, bireylerin bu teknolojileri kullanırken kişisel veri güvenliğini ön planda tutmaları ve haklarını gözeten, sorumlu ve bilinçli bir kullanım anlayışı benimsemeleri önem arz etmektedir. Bireylerin bu farkındalıkla hareket etmesi; teknolojik gelişmelerin insan haklarına saygılı, etik değerlere uygun ve mahremiyet bilinciyle şekillenmesini sağlayacaktır. Bu sayede hem bireysel hak ve özgürlükler korunacak hem de teknolojinin sunduğu imkânlardan güvenli biçimde yararlanmak mümkün olacaktır.

15. Üretken Yapay Zekâ Araçlarını Kullanan Çocuklara Yönelik Olarak Ebeveynler Tarafından Alınabilecek Önlemler Nelerdir?

Günümüzde ÜYZ teknolojileri; eğitimden eğlenceye, günlük yaşam alışkanlıklarından sosyal etkileşim biçimlerine kadar birçok alanda hızla yaygınlaşmaktadır. Bu teknolojilere yönelik erişim imkânlarının artması, özellikle çocukların ÜYZ tabanlı uygulamalara olan ilgisini ve kullanım sıklığını da beraberinde getirmektedir. Sohbet botları, içerik üretim programları ve ÜYZ destekli öğrenme platformları gibi araçlar çocuklar için hem eğlenceli hem de öğretici olabilirken; aynı zamanda mahremiyet, güvenlik, yanıltıcı bilgi ve etik kullanım açısından bazı riskleri de bünyesinde barındırmaktadır. Bu bağlamda, çocukların dijital dünyada karşılaşabileceği olumsuzluklara karşı bilinçli ve yönlendirici bir ebeveynlik anlayışı geliştirilmesi büyük bir öneme sahiptir.

İlk olarak, çocukların kullandığı ÜYZ tabanlı platformların yaşa uygun içerikler sunup sunmadığı kontrol edilmeli ve dikkatle değerlendirilmelidir. Başta metin tabanlı sohbet uygulamaları olmak üzere bazı ÜYZ araçları, çocuklar için uygun olmayan veya yanıltıcı bilgi barındıran içerikler üretebilmektedir. Bu bağlamda, ebeveynlerin ilgili uygulamaların kullanım koşullarını, gizlilik politikalarını ve içerik filtreleme özelliklerini incelemesi, olası risklerin önüne geçilmesi açısından faydalı olacaktır.

Özellikle ÜYZ kullanılarak gerçekçi biçimde oluşturulan sahte video, görsel ve ses içeriklerini ifade eden ve son yıllarda hızla yaygınlaşan *deep fake* teknolojileri, çocuklar açısından önemli riskler barındırmaktadır. Zira hâlen gelişim sürecinde olan bilişsel yetenekleri nedeniyle çocuklar, yetişkinlere kıyasla bu tür içeriklere karşı daha savunmasızdır ve kolaylıkla manipüle edilebilirler. Önceleri ileri düzey dijital beceri ve güçlü yazılımlar gerektiren *deep fake* içeriklerin, günümüzde kullanımı kolay mobil uygulamalar aracılığıyla ve sınırlı teknik bilgiyle üretilebilmesi, bu içeriklerin daha yaygın şekilde erişilebilir hâle gelmesini sağlamakta, içeriklerin gerçeklik düzeyini artırmakta ve tespit edilmelerini giderek zorlaştırmaktadır. *Deep fake* teknolojileri, çocukların bu tür içerikleri ayırt etme kapasitelerinin sınırlı olması nedeniyle, yetişkinlere oranla daha yüksek düzeyde tehdit oluşturmaktadır. Buna bağlı olarak çocuklar, siber zorbalık ve çevrim içi istismar gibi tehditlere daha açık hâle gelmektedir.

Bunun yanı sıra, çevrim içi ortamlarda paylaşılan kişisel fotoğraf ve videoların kötü niyetli kişilerce izinsiz şekilde kullanılarak *deep fake* içeriklere dönüştürülmesi, çocukların dijital ortamda hedef hâline gelmesine yol açabilir. Bu nedenle, ebeveynlerin çocuklarını *deep fake* içeriklerin varlığı ve doğurabileceği olumsuz sonuçlar hakkında bilinçlendirmeleri, sosyal medya hesaplarında gizlilik ayarlarını etkin şekilde düzenlemeleri ve çevrim içi ortamlarda gerçekleştirilen paylaşımlara ilişkin yönlendirici bir tutum sergilemeleri önem taşımaktadır. Bu tür önlemler, çocukların yalnızca teknolojiyle değil, aynı zamanda teknolojinin ortaya çıkarabileceği yanıltıcı içeriklerle baş edebilme becerilerinin desteklenmesi açısından da önemli bir rol oynamaktadır.

Diğer yandan, çocukların ÜYZ araçları üzerinden ad-soyad, okul bilgileri, adres veya telefon numarası gibi kişisel bilgilerini paylaşmaları da ciddi riskleri beraberinde getirebilir. Bu nedenle, kişisel verilerin korunmasının önemine ilişkin olarak çocuklara yaşlarına uygun şekilde bilgilendirme yapılmalı ve bu konuda farkındalık kazandırma yönünde adımlar atılmalıdır.

Teknolojik araçlar ne kadar gelişmiş olursa olsun, çocukların dijital deneyimlerinin anlamlı ve güvenli bir çerçevede şekillenmesi, ebeveyn rehberliğiyle mümkün kılınabilir. Bu bağlamda, dijital ebeveynlik yalnızca kontrol mekanizması kurmakla sınırlı kalmamalı; çocuğun bu teknolojiyle kurduğu ilişkiyi anlamayı ve bu ilişkiyi yönlendirmeyi de kapsamalıdır. Dolayısıyla ebeveynlerin, ÜYZ teknolojilerinin ne olduğu, nasıl çalıştığı, hangi avantajlarının ve sınırlarının bulunduğu konusunda çocukların yaşına uygun açıklamalar yapmaları önemlidir. Aynı zamanda, ÜYZ araçlarının her zaman doğru, tarafsız veya etik içerikler üretmeyebileceğini anlatmaları, çocuğun dijital ortama karşı sorgulayıcı bir bakış açısı geliştirmesine yardımcı olacaktır.

Bu süreçte, erken yaşlardan itibaren çocuklara etik kullanım bilinci kazandırılması da ihmal edilmemelidir. Dijital ortamda başkalarının fikirlerine, içeriklerine ve özel bilgilerine saygı gösterilmesi gerektiği, çocuğun benimsemesi gereken temel bir değer olarak ele alınmalıdır.

Diğer yandan, ÜYZ araçlarının kullanım süresi konusunda sınırlar belirlemek, çocuğun dijital yaşamla gerçek yaşam arasında sağlıklı bir denge kurmasını sağlar. Uzun süreli ekran kullanımı; dikkat dağınıklığı, sosyal etkileşimde azalma ve fiziksel hareketsizlik gibi olumsuz sonuçlara yol açabileceğinden, bu riskleri azaltmaya yönelik olarak günlük kullanım süresi kontrol altında tutulmalıdır.

Son olarak, ÜYZ ile kurulan etkileşimlerin çocuğun duygusal ve psikolojik gelişimi üzerindeki etkileri ebeveynler tarafından dikkatle gözlemlenmelidir. Gerçeklik algısının zayıflaması, yalnızlaşma eğilimi, özgüven kaybı veya teknolojiye bağımlılık gibi belirtiler gözlemlendiğinde, uzman desteği alınması ve müdahale sürecinin geciktirilmemesi önemlidir.

Bunlarla sınırlı olmamak üzere bu gibi önlemlerin, çocukların ÜYZ teknolojilerinden doğru, güvenli ve bilinçli şekilde yararlanmalarını sağlamak amacıyla ebeveynler tarafından hayata geçirilmesinde fayda bulunmaktadır. Teknolojiyle kurulan ilişki, bilinçli ve sorumlu bir yaklaşımla şekillendirildiğinde, ÜYZ uygulamaları çocuklar için yalnızca bir dijital araç olmanın ötesinde gelişimlerini destekleyen fırsatlara dönüşebilir. Ebeveynlerin bu sürece aktif katılımı, dijital çağın sunduğu imkânların çocuklar açısından yapıcı ve güvenli bir şekilde değerlendirilmesinde belirleyici bir role sahiptir.

Rehberin Hazırlanmasında Faydalanılan Kaynaklar[33]

An A.I.- Generated Picture Won an Art Prize. Artists Aren't Happy, https://www.nytimes.com/2022/09/02/technology/ai-artificial-intelligence-artists.html.

Baker, P.: Generative AI, New Jersey: John Wiley&Sons Inc, 1. Baskı, 2025.

Baum, D.: Generative AI and LLMs, New Jersey: John Wiley&Sons Inc., Snowflake Special Edition, 2024.

Belcic, I./Stryker, C.: What is GPT (Generative Pretrained Transformer), 2024, https://www.ibm.com/think/topics/gpt.

Bergmann, D./Stryker, C.: What is a Variational Autoencoder?, 2024, https://www.ibm.com/think/topics/variational-autoencoder.

Bostrom, N.: How Long Before Superintelligence?, https://nickbostrom.com/superintelligence.

California Government Operations Agency: Benefits and Risks of Generative Artificial Intelligence Report, 2023, https://www.govops.ca.gov/wp-content/uploads/sites/11/2023/11/GenAI-EO-1-Report_FINAL.pdf.

Canadian Centre for Cybersecurity: Generative Artificial Intelligence, 2023, https://www.cyber.gc.ca/en/guidance/generative-artificial-intelligence-ai-itsap00041.

Commission Nationale de l'Informatique et des Libertés (CNIL): CNIL's Q&A on the Use of Generative AI Systems, 2024, https://www.cnil.fr/en/cnils-qa-use-generative-ai-systems.

Confederation of European Data Protection Organisations (CEDPO): Generative AI: The Data Protection Implications, 2023, https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf.

European Commission: AI Act Service Desk-Frequently Asked Questions, 2025, https://ai-act-service-desk.ec.europa.eu/en/faq.

European Data Protection Board (EDPB): Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models, 2024, https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

European Data Protection Supervisor (EDPS): Generative AI and the EUDPR: First EDPS Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems, 2024, https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf.

European Data Protection Supervisor (EDPS): Glossary, https://www.edps.europa.eu/data-protection/data-protection/glossary_en.

European Data Protection Supervisor (EDPS): Privacy by Default, https://www.edps.europa.eu/data-protection/our-work/subjects/privacy-default_en.

European Data Protection Supervisor (EDPS): Privacy By Design, https://www.edps.europa.eu/data-protection/our-work/subjects/privacy-design_en.

European Parliamentary Research Service (EPRS): Children and Deepfakes, 2025, https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf.

European Parliamentary Research Service (EPRS): EU Guidelines on Ethics in Artificial Intelligence: Context and Implementation, 2019, https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.

European Parliamentary Research Service (EPRS): Understanding Algorithmic Decision-Making: Opportunities and Challenges, 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf.

33 Bu Rehber'de faydalanılan internet sitesi adreslerinin geçerliliği 29.10.2025 tarihinde teyit edilmiştir.

Future of Privacy Forum (FPF): The Spectrum of Artificial Intelligence-Companion to the FPF AI Infographic, 2021, https://fpf.org/wp-content/uploads/2021/08/FPF-AIEcosystem-Report-FINAL-Digital.pdf.

Information Commissioner's Office (ICO): ICO Consultation Series on Generative AI and Data Protection, 2024, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2024/09/ico-consultation-series-on-generative-ai-and-data-protection/.

Information Commissioner's Office (ICO): Information Commissioner's Office Response to the Consultation Series on Generative AI, 2024, https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/.

International Association of Privacy Professionals (IAPP): Glossary of Privacy Terms, https://iapp.org/resources/glossary/.

International Association of Privacy Professionals (IAPP): Key Terms for AI Governance, 2025, https://iapp.org/resources/article/key-terms-for-ai-governance/.

International Organization for Standardization (ISO): ISO/IEC 22989:2022, https://www.iso.org/standard/74296.html.

Kişisel Verileri Koruma Kurumu (KVKK): Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), 2025, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf.

Kişisel Verileri Koruma Kurumu (KVKK): Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2025, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF.

Kişisel Verileri Koruma Kurumu (KVKK): Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, 2025, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf.

Kişisel Verileri Koruma Kurumu (KVKK): Kişisel Verilerin Yurt Dışına Aktarılması Rehberi, 2025, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf.

Kişisel Verileri Koruma Kurumu (KVKK): "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" – Kişisel Verileri Koruma Kurulunun 31.01.2018 tarih ve 2018/10 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/4110/2018-10.

Kişisel Verileri Koruma Kurumu (KVKK): "Veri Sorumlusunun Kanuni Yükümlülüğünü Yerine Getirmek için İşlediği Kişisel Verileri Meşru Menfaat Çerçevesinde Kullanma Talebiyle Kuruma Yapmış Olduğu Başvuru" – Kişisel Verileri Koruma Kurulunun 25.03.2019 tarih ve 2019/78 sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/5434/2019-78.

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

T.C. Sanayi ve Teknoloji Bakanlığı/Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi: Ulusal Yapay Zekâ Stratejisi 2021-2025, https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf.

United Nations Educational, Scientific and Cultural Organization (UNESCO): Guidance for Generative AI in Education and Research, 2023, https://unesdoc.unesco.org/ark:/48223/pf0000386693.

What is GPT?, https://cloud.google.com/discover/what-is-gpt.

Nasuh Akar Mahallesi 1407. Sok. No:4, 06520 Çankaya/Ankara
Tel: 0312 216 50 00
www.**kvkk**.gov.tr