Üretken Yapay Zekâ ve Kişisel Verilerin Korunması: Hukuki Çerçeve ve Uygulama Rehberi

Giriş: Üretken Yapay Zekâ Paradigması

Üretken Yapay Zekâ ve Kişisel Verilerin Korunması adlı bu çalışma, **Üretken Yapay Zekânın (ÜYZ) stratejik tanımını ve hukuki çerçevesini** ele almaktadır. Kaynak, geleneksel yapay zekâ ile ÜYZ arasındaki temel farkları, ÜYZ'nin metin, görsel ve kod oluşturma gibi **çok yönlü yeteneklerini ve Deep Fake teknolojisinin tanımını** detaylandırır. Makale, bu teknolojilerin sunduğu **fırsatları (sağlık, eğitim, pazarlama)** listelerken, aynı zamanda **"halüsinasyonlar," ön yargı ve fikri mülkiyet ihlalleri** gibi temel riskleri analiz etmektedir. Hukuki kısım ise, ÜYZ sistemlerinin tüm yaşam döngüsünde (veri toplama, model eğitimi) 6698 sayılı **Kişisel Verilerin Korunması Kanunu (KVKK) kapsamındaki yükümlülüklerini** incelemekte, özellikle veri sorumlusu/veri işleyen rollerinin tespiti ile hukuka uygunluk ilkelerini açıklamaktadır. Son olarak, kaynak bireysel kullanıcılar ve ebeveynler için **sorumlu ve güvenli kullanım önerileri** sunarak pratik bir rehber niteliği taşımaktadır.

Bu makaleyi Spotify'da sesli olarak dinlemek için podcast'ine bu linkten ulaşabilirsiniz.

1.1.1 Stratejik Bağlam ve Tanım

Dijital teknolojiler, toplumsal yapıları, karar alma süreçlerini ve gündelik yaşam alışkanlıklarını kökten değiştiren çok yönlü bir dönüşüme öncülük etmektedir. Bu dönüşümün en dikkat çekici unsurlarından biri, Yapay Zekâ (YZ) teknolojilerinin hızlı gelişimi ve yaygınlaşmasıdır. Son yıllarda YZ alanında yaşanan en çarpıcı ilerleme ise, mevcut verilerden hareketle tamamen yeni ve özgün içerikler üretebilme kapasitesine sahip **Üretken Yapay Zekâ (ÜYZ)** sistemlerinin yükselişi olmuştur. Eğitimden sağlığa, yazılım geliştirmeden medya sektörüne kadar geniş bir yelpazede endüstrileri yeniden şekillendirme potansiyeli taşıyan bu teknolojiyi stratejik olarak anlamak, günümüz profesyonelleri için bir zorunluluk hâline gelmiştir.

Bu makaleyi Youtube'da görüntülü olarak izlemek için videosuna bu linkten ulaşabilirsiniz.

Genel tanımıyla Üretken Yapay Zekâ, büyük ölçekli veri kümeleri üzerinde eğitilen ve kullanıcı tarafından girilen komutlara (prompt) yanıt olarak metin, görsel, video, ses veya yazılım kodu gibi farklı formatlarda yeni içerikler üretebilen bir YZ türüdür. Geleneksel YZ sistemleri genellikle mevcut verileri analiz etmeye veya sınıflandırmaya odaklanırken, ÜYZ'nin temel işlevi *yaratımdır*. Bu sistemler, yapay sinir ağları ve derin öğrenme algoritmalarını kullanarak mevcut verilerdeki kalıpları tanımlar ve bu kalıplardan yola çıkarak yeni ve bağlama uygun içerikler üretir.

Geleneksel YZ ile ÜYZ arasındaki temel farklar aşağıdaki tabloda özetlenmektedir.

Tablo 1: Geleneksel YZ ile ÜYZ Karşılaştırması

Kriterler	**Geleneksel/Klasik YZ *(Conventional AI)***	**ÜYZ *(Generative AI)***
Amaç	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.
Eğitim	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.
Algoritma Türü	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.
Kullanım Alanları	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.
Değerlendirme	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.

Bu temel farklar, ÜYZ'nin salt analizden yaratıma nasıl geçtiğini ortaya koymakta ve metin, görsel, ses gibi çeşitli formatlarda içerik üretme yeteneklerinin temelini oluşturmaktadır.

1.1.2 Üretken Yapay Zekânın Temel Yetenekleri

Üretken Yapay Zekânın yetenekleri, metinden görsele, sesten koda kadar birden çok içerik formatını kapsayarak geniş bir uygulama alanı sunmaktadır. Başlıca yetenekleri şunlardır:

- **Metin Oluşturma:** Doğal Dil İşleme (Natural Language Processing – NLP) algoritmaları kullanarak insan dilini anlar ve kullanıcı girdileri doğrultusunda makale, özet, hikâye veya sohbet botu yanıtları gibi çeşitli metin tabanlı içerikler üretir.

- **Görsel/Video Oluşturma:** Metinsel açıklamalardan yola çıkarak sanat eserleri, animasyonlar, illüstrasyonlar ve video içerikleri oluşturur. Bu yeteneği, dijital sanat, grafik tasarım ve reklamcılık gibi alanlarda yenilikçi çözümler sunar.
- **Ses/Müzik Oluşturma:** Mevcut ses verileri üzerinde eğitilerek yeni ses efektleri, konuşmalar veya özgün müzik eserleri oluşturabilir. Bu potansiyeli, özellikle eğlence ve oyun endüstrileri için değerlidir.
- **Yazılım Kodu Oluşturma:** Yeni kod üretme, programlama dilleri arasında çeviri yapma, kod tamamlama ve hata ayıklama gibi görevleri yerine getirerek yazılım geliştirme süreçlerini hızlandırır ve kolaylaştırır.
- **Sentetik Veri Oluşturma:** Gerçek verinin yapısını ve istatistiksel özelliklerini taklit eden yapay veriler üretir. Bu sentetik veriler, gerçek dünya verilerinin sınırlı, erişilemez veya hassas olduğu durumlarda makine öğrenmesi modellerini test etmek ve eğitmek için kullanılır.

1.1.3 Deep Fake Teknolojisi

2024/1689 sayılı AB Yapay Zekâ Tüzüğü'ne göre deep fake, "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" olarak tanımlanmaktadır. 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 ciddi sorunlara yol açma potansiyeline sahiptir.

ÜYZ'nin bu çok yönlü yetenekleri, altında yatan karmaşık teknik süreçler ve modellerin yaşam döngüsü sayesinde mümkün olmaktadır.

1.2 Üretken Yapay Zekânın Mekanizması ve Yaşam Döngüsü

1.2.1 İçerik Üretim Süreçleri

Üretken Yapay Zekâ modellerinin 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 özelleştirilmiş YZ uygulamalarının inşasında birer yapı taşı işlevi görür. **"İnce ayar" (fine-tuning)** olarak bilinen süreçlerle belirli uygulamalara uyarlanarak farklı türde içeriklerin üretiminde etkili bir şekilde kullanılırlar.

Metin Üretim Süreci: Metin üretiminde kullanılan en yaygın temel model türü, **"Büyük Dil Modelleri"dir (Large Language Models – LLM)**. Milyarlarca kelimeden oluşan veri setleriyle eğitilen LLM'ler, kelimeler arasındaki istatistiksel ilişkilere dayanarak doğal dilde yanıtlar üretir. Bu alandaki en bilinen mimari, **"Üretken Önceden Eğitilmiş**

Dönüştürücü"dür (Generative Pre-trained Transformer – GPT). GPT modelleri, bir metin dizisindeki bir sonraki kelimeyi olasılıksal olarak tahmin ederek çalışır. Bu süreç, genel hatlarıyla şu adımları izler:

1. Kullanıcı tarafından girilen istem (prompt), "token" adı verilen daha küçük birimlere bölünür.
2. Model, eğitim verilerinden öğrendiği istatistiksel örüntülere dayanarak bir sonraki en olası kelimeyi tahmin eder.
3. Tahmin edilen kelimeler okunabilir bir metne dönüştürülür.
4. Oluşturulan metin, zararlı içerikleri filtrelemek için "koruma mekanizmaları" *(guardrails)* olarak bilinen filtreleme sisteminden geçirilir.
5. Yanıt tamamlanana kadar tahmin ve üretim süreci tekrarlanır.
6. Son yanıt, okunabilirliği artırmak amacıyla biçimlendirilir.

Görsel Üretim Süreci: Görsel üretiminde öne çıkan iki temel yöntem bulunmaktadır:

- **Varyasyonel Otomatik Kodlayıcılar (Variational Autoencoders – VAEs):** Bu modeller, eğitim verilerinden anlamlı özellikleri ayıklayan bir "kodlayıcı" ve bu özellikleri kullanarak yeni görseller oluşturan bir "kod çözücü"den oluşur.
- **Çekişmeli Üretken Ağlar (Generative Adversarial Networks – GANs):** Bu yapıda iki sinir ağı birbiriyle rekabet eder. **"Üretici" (generator)** ağ, yeni görseller oluşturmaya çalışırken, **"ayırt edici" (discriminator)** ağ, bu görsellerin gerçek olup olmadığını değerlendirir. Ayırt edicinin geri bildirimleri sayesinde üretici, zamanla daha gerçekçi çıktılar üretmeyi öğrenir. Bu döngü, üretici ağın ayırt edici ağı "kandırmayı" başardığı, yani ürettiği görselin gerçek olarak kabul edildiği noktaya kadar devam eder.

Model Sınıflandırması: Tek Modlu ve Çok Modlu ÜYZ modelleri, işledikleri veri türüne göre iki temel kategoriye ayrılır:

- **Tek modlu (unimodal) modeller:** Yalnızca tek bir türde veri işler ve yine aynı türde çıktı üretir (örneğin, metin girdisi alıp metin çıktısı veren bir LLM).
- **Çok modlu (multimodal) modeller:** Birden fazla veri türünü işleyebilir ve bir veri türündeki girdiyi farklı bir veri türünde çıktıya dönüştürebilir. Örneğin, "uçan bir bisiklet" gibi metinsel bir girdiyi analiz ederek bu betimlemeye uygun bir görsel içerik oluşturabilir.

Bu teknik mekanizmalar, modellerin geliştirilmesi ve uygulanmasını kapsayan yapılandırılmış bir yaşam döngüsü içinde hayat bulur.

1.2.2 Model Yaşam Döngüsü

Bir ÜYZ modelinin tasarımı, geliştirilmesi ve uygulanması, teknolojinin güvenli ve sürdürülebilir bir şekilde hayata geçirilmesinde belirleyici rol oynayan yapılandırılmış bir yaşam döngüsünü takip eder. Bu döngünün temel aşamaları şunlardır:

1. **Modelin kullanım amacının ve kapsamının belirlenmesi**
2. **Verilerin toplanması ve ön işlemeye tabi tutulması**
3. **Modelin eğitilmesi ve ince ayarının yapılması**
4. **Modelin değerlendirilmesi ve izlenmesi**
5. **Modelin yerleştirilmesi ve devamında düzenli geri bildirimler sağlanması**

Bu aşamalar arasında özellikle **verilerin toplanması** kritik bir öneme sahiptir. Modellerin eğitimi için gerekli olan büyük miktardaki veri, çeşitli yöntemlerle elde edilir. En yaygın yöntemlerden biri, kamuya açık web sayfalarından otomatik yazılımlar aracılığıyla veri toplayan **web kazıma (web scraping)** teknolojisidir. Diğer başlıca veri kaynakları arasında kullanıcılar tarafından sağlanan veriler, üçüncü taraflarca oluşturulan veri tabanları ve geliştiricilerin kendi bünyelerinde tuttukları veri tabanları yer almaktadır.

Bu yaşam döngüsü, yalnızca teknik bir süreç olmakla kalmaz; aynı zamanda önemli etik, hukuki ve toplumsal boyutlar taşır ve bu boyutların dikkatle yönetilmesi gerekir.

1.3 Üretken Yapay Zekâ: Fırsatlar ve Riskler

1.3.1 Başlıca Kullanım Alanları

Üretken Yapay Zekâ, farklı formatlarda insan üretimine benzer içerikler oluşturma kapasitesi sayesinde, modern işletmeler için üretkenliği artıran ve inovasyonu teşvik eden dönüştürücü bir araç olarak konumlanmaktadır. Bu teknoloji, iş süreçlerini yeniden şekillendirerek çeşitli sektörlerde stratejik bir değer yaratmaktadır.

- **Müşteri Hizmetleri:** Sohbet botları ve sanal asistanlar aracılığıyla müşteri etkileşimlerini optimize ederek hizmet süreçlerini kolaylaştırır, maliyetleri düşürür ve kişiselleştirilmiş öneriler sunar.
- **Sağlık:** Hasta kayıtlarını analiz ederek teşhis süreçlerini destekler, kişiselleştirilmiş tedavi planları oluşturur ve kimyasal modelleme aracılığıyla ilaç keşfi gibi alanlarda önemli fırsatlar sunar.
- **Eğitim:** Öğrencilerin bireysel ihtiyaçlarına göre kişiselleştirilmiş öğrenme planları oluşturulmasına imkân tanır ve eğitim materyallerinin hazırlanmasında öğretim sürecinin verimliliğini artırır.
- **Pazarlama ve Reklamcılık:** Hedef kitle analizinden yola çıkarak özelleştirilmiş kampanyalar tasarlar, reklam metinleri hazırlar ve yaratıcı görsel içerikler oluşturarak pazarlama süreçlerinde hız ve verimlilik sağlar.
- **Kültürel Endüstriler ve Sanat:** Metinsel açıklamalardan hareketle görsel sanat eserleri ve müzik kompozisyonları oluşturarak sanat ve tasarım süreçlerini çeşitlendirir.
- **Yazılım Geliştirme:** Kod üretme, mevcut kodları yeniden yapılandırma (refactoring) ve hataları tespit etme gibi görevleri otomatikleştirerek yazılım geliştirme sürecinin verimliliğini artırır.
- **Arama ve Bilgiye Erişim:** Geleneksel arama motorlarını, kullanıcılara özetlenmiş ve bağlamsal yanıtlar sunan gelişmiş bilgi asistanlarına dönüştürür.

- **Hukuk:** Sözleşme hazırlama, hukuki belgeleri analiz etme ve dava dosyalarını inceleme gibi rutin ve zaman alıcı işlemleri otomatikleştirerek meslek profesyonellerine destek olur.

Bu önemli fırsatlar, beraberinde dikkatle yönetilmesi gereken kritik etik, güvenlik ve hukuki riskleri de getirmektedir.

1.3.2 Temel Risklerin Analizi

Üretken Yapay Zekânın sunduğu faydalara rağmen, bireysel hakları korumak ve toplumsal güvenliği sağlamak için dikkatli bir yönetim gerektiren çeşitli riskler de mevcuttur.

- **"Halüsinasyonlar" ve Tutarsız Çıktılar:** ÜYZ modellerinin, gerçeklikle örtüşmeyen ancak makul ve ikna edici görünen, olgusal olarak yanlış çıktılar üretmesi durumudur. Örneğin, bir avukatın içtihat araştırması yaparken sistemin gerçekte var olmayan mahkeme kararları üretmesi bu riske somut bir örnektir.
- **Ön Yargı ve Yanlı Çıktılar:** Modeller, eğitildikleri verilerde bulunan toplumsal ön yargıları ve eşitsizlikleri yansıtma ve pekiştirme riski taşır. Bu durum ayrımcı veya saldırgan içeriklerin üretilmesine neden olabilir. Modellerin **"kara kutu" (black box)** niteliği, bu yanlılıkların tespit edilmesini ve giderilmesini zorlaştırmaktadır.
- **Verilerin Gizliliği ve Güvenliği:** ÜYZ, ikna edici oltalama (phishing) e-postaları veya sahte kimlikler oluşturmak için kullanılabilir. Ayrıca, kullanıcıların istemlerinde (prompt) paylaştıkları kişisel verilerin veya kurumsal sırların açığa çıkması ve veri sızıntılarına yol açması da önemli bir güvenlik sorunudur.
- **Fikri Mülkiyet Hakkı İhlalleri:** Modellerin telif hakkı ile korunan materyaller içeren veri kümeleri üzerinde eğitilmesi durumunda, üretilen içeriklerin fikri mülkiyet haklarını ihlal etmesi yönünde hukuki iddialar gündeme gelebilir.
- **Deep Fake ve Manipülatif İçerikler:** ÜYZ sistemleri, yanlış bilginin yayılması, kimlik sahteciliği veya bireylerin itibarının zedelenmesi gibi amaçlarla son derece gerçekçi sahte görsel, ses ve video içerikleri oluşturmak için kötüye kullanılabilir.

Bu riskler, özellikle veri gizliliği ve güvenliği ile ilgili olanlar, kişisel verilerin korunmasına yönelik yasal düzenlemelerin titizlikle uygulanmasını zorunlu kılmaktadır.

1.4 Üretken Yapay Zekâ ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)

1.4.1 KVKK Kapsamında Değerlendirme

Üretken Yapay Zekâ sistemleri, doğaları gereği veri odaklıdır ve yaşam döngülerinin hemen her aşamasında kişisel verileri işleyebilirler. Bu nedenle, bu sistemler 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) gibi veri koruma mevzuatlarının uygulama alanına girmektedir.

KVKK uyarınca:

- **Kişisel veri**, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanır.
- **Kişisel verilerin işlenmesi** ise “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem” şeklinde ifade edilir.

Kişisel veri işleme faaliyeti; eğitim veri kümelerinin oluşturulması, modelin ince ayarının yapılması veya kullanıcıların sisteme girdiği veriler (girdiler) ve sistemin ürettiği veriler (çıktılar) gibi çeşitli aşamalarda gerçekleşebilir. Modelin kişisel veri işlemeyi özellikle hedeflememesi veya bu işlemenin yalnızca rastlantısal olması, kişisel veri işleme faaliyetinin varlığını ortadan kaldırmaz.

- **Örnek 1 (KVKK Kapsamında):** Bir şirket, çalışanlarının mesleki gelişimi için ÜYZ destekli bir araçla eğitim materyali hazırlamaktadır. Analiz edilen video kayıtları ve notlar, katılımcıların adı, soyadı, görüntüsü ve ses kaydı gibi kişisel verileri içermektedir. Bu durumda, içerik oluşturma süreci KVKK kapsamında bir kişisel veri işleme faaliyetidir.
- **Örnek 2 (KVKK Kapsamında Değil):** Bir grafik tasarım ajansı, ÜYZ aracına “yaz indirimi temalı afiş” gibi genel ve kişisel veri içermeyen komutlar vermektedir. Üretilen çıktılar da kimliği belirli bir kişiye ilişkin bilgi içermemektedir. Bu durumda, ajansın faaliyeti KVKK kapsamında bir kişisel veri işleme faaliyeti olarak değerlendirilmez.
- **Örnek 3 (KVKK Kapsamında):** Bir kullanıcı, ÜYZ’ye “Ünlü bir Türk fizikçinin başarı hikâyesini anlat” şeklinde genel bir komut girmiştir. Modelin çıktısında, belirli bir gerçek kişinin adı, soyadı ve kariyer bilgileri yer almıştır. Girdi kişisel veri içermese de çıktı içerdiği için, bu faaliyet kişisel veri işleme kapsamında değerlendirilebilir.

Anonim hâle getirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir. Yalnızca anonim verilerin kullanıldığı faaliyetler KVKK kapsamı dışında kalsa da verileri anonimleştirme sürecinin kendisi bir veri işleme faaliyetidir.

ÜYZ sistemlerinin sıklıkla kişisel veri işlemesi, bu süreçteki aktörlerin rollerinin ve sorumluluklarının net bir şekilde belirlenmesini zorunlu kılar.

1.4.2 Veri Sorumlusu ve Veri İşleyen Rollerinin Tespiti

ÜYZ ekosisteminin çok aktörlü ve karmaşık yapısı, **Veri Sorumlusu** ve **Veri İşleyen** rollerinin tespitini güçleştirmektedir. Bu rollerin belirlenmesinde sözleşmesel ifadelerden ziyade, veri işleme faaliyetinin “neden” ve “nasıl” yapılacağı üzerindeki fiili kontrol ve karar

alma yetkisi esastır.

KVKK uyarınca:

- **Veri sorumlusu**, “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi”dir.
- **Veri işleyen**, “veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi”dir.

Veri Sorumlusu, aşağıdaki gibi temel konularda karar verir:

- Hangi kişisel verilerin toplanacağı ve nasıl toplanacağı.
- Verilerin hangi amaçlarla kullanılacağı.
- Verilerin kimlerle paylaşılacağı.
- Verilerin ne kadar süreyle saklanacağı.

Veri İşleyen ise genellikle aşağıdaki gibi teknik konularda karar yetkisine sahip olabilir:

- Veri toplama ve saklama için kullanılacak teknoloji ve yöntemler.
- Alınacak güvenlik önlemlerinin detayları.
- Veri aktarım ve imha yöntemleri.

ÜYZ bağlamında “geliştirici” ve “yerleştirici” gibi roller statik değildir ve yürütülen faaliyete göre değişebilir. Örneğin, kendi modelini geliştiren bir kuruluş **veri sorumlusu** iken, üçüncü bir tarafın talimatları doğrultusunda bir model geliştiren aynı kuruluş **veri işleyen** konumunda olabilir.

Özellikle **“kapalı erişimli” (closed-access)** modeller, bu modelleri kendi sistemlerine entegre eden “yerleştiricilerin” veri işleme faaliyetleri üzerindeki kontrolünü sınırlayabilir ve bu durum rol tespitini daha da karmaşık hâle getirebilir.

Bu nedenle, veri koruma sorumluluğunun doğru bir şekilde tesis edilmesi için roller genel bir yaklaşımla değil, her bir veri işleme faaliyetinin niteliği, bağlamı ve tarafların fiili kontrolü analiz edilerek somut olaya özgü bir değerlendirmeyle belirlenmelidir.

1.5 KVKK’nın Genel İlkelerinin Üretken Yapay Zekâ Sistemlerine Uygulanması

KVKK’nın 4. maddesinde düzenlenen genel ilkeler, tüm kişisel veri işleme faaliyetlerinin temelini oluşturur ve hukuka uygunluğun mihenk taşıdır. Bu ilkeler, ÜYZ sistemlerinin yaşam döngüsünün her aşamasında—eğitim verilerinin toplanmasından modelin çıktı üretmesine kadar—titizlikle gözetilmelidir. Aşağıdaki alt bölümlerde, her bir ilkenin ÜYZ bağlamında nasıl uygulanacağı analiz edilmektedir.

6698 sayılı Kanun'un 4. maddesi uyarınca, kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

1. 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.

1.5.1 Hukuka ve Dürüstlük Kurallarına Uygun Olma

Bu ilke, veri işleme faaliyetlerinin şeffaf, hukuka uygun ve veri sahiplerinin makul beklentileriyle uyumlu olmasını gerektirir. ÜYZ sistemlerindeki algoritmik ön yargılar, bu ilkenin ihlaline yol açabilir.

- **Örnek 5:** Bir ÜYZ aracının "doktor" komutu girildiğinde çoğunlukla erkek, "hemşire" komutu girildiğinde ise genellikle kadın figürler üretmesi, eğitim verilerindeki cinsiyetçi temsiliyet dengesizliklerinin bir yansımasıdır ve ayrımcı sonuçlar doğurarak dürüstlük kuralını ihlal edebilir.
- **Örnek 6:** Otomatik konuşma tanıma sisteminin, eğitim verilerinde yeterince temsil edilmeyen belirli aksanlara sahip kullanıcılarda daha yüksek hata oranı göstermesi, ayrımcılığa yol açarak bu ilkeye aykırılık teşkil edebilir.

Bu tür riskleri azaltmak için eğitim veri kümelerinin toplumsal çeşitliliği adil bir şekilde temsil etmesi sağlanmalı ve sistem çıktılarını düzenli olarak denetleyecek izleme mekanizmaları oluşturulmalıdır.

1.5.2 Doğru ve Gerektiğinde Güncel Olma

Bu ilke, ÜYZ sistemlerinin çıktılarının doğruluğunun büyük ölçüde girdi verilerinin kalitesine bağlı olması nedeniyle kritik bir öneme sahiptir. "Halüsinasyon" olarak adlandırılan, modelin olgusal olarak yanlış kişisel veriler üretmesi, bu ilke açısından önemli bir zorluk teşkil eder. Yüksek kaliteli veri kullanımı bu riski azaltsa da tamamen ortadan kaldıramaz.

- **Örnek 7:** Müşteri şikayetlerini özetleyen bir ÜYZ modelinin, bazı durumlarda metinleri bağlamından kopuk özetlemesi veya müşterilere ait kişisel verileri hatalı yansıtması, bu ilkeye aykırılık teşkil eder.

Veri sorumluları, eğitim setleri için veri doğrulama süreçleri uygulamalı, çıktıları gözden geçirmek için insan gözetimi mekanizmaları kurmalı ve kullanıcıların yanlışlıkları bildirip düzeltebilecekleri kanallar oluşturmalıdır.

1.5.3 Belirli, Açık, Meşru Amaçlar İçin İşlenme ve Ölçülülük

Bu ilkeler, veri işleme faaliyetlerinin amacının net bir şekilde tanımlanmasını (amaç sınırlılığı) ve yalnızca bu amaç için gerekli olan verilerin işlenmesini (veri minimizasyonu)

zorunlu kılar. “YZ sistemlerimizi geliştirmek” gibi genel ve muğlak ifadeler, bu ilkelere aykırıdır. Veri sorumluları, ÜYZ yaşam döngüsünün her bir aşaması (eğitim, ince ayar, operasyonel kullanım vb.) için spesifik, açık ve meşru amaçlar belirlemelidir.

- **Örnek 8:** Bir ÜYZ modelinin geliştirilmesi (teknik yeterliliği artırma amacı) ile bu modele dayalı bir uygulamanın işletilmesi (kullanıcıya hizmet sunma amacı), farklı amaçlar teşkil eder ve her biri için ayrı gerekçelendirme gerekir.
- **Örnek 9:** İşe alım süreçleri için geliştirilen bir ÜYZ sisteminin, aday değerlendirmesi için yalnızca pozisyonla ilgili ve orantılı verileri işlemesi gerekir. Amaçla ilgisi olmayan verilerin işlenmesi ölçülülük ilkesini ihlal eder.

1.5.4 İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

Bu ilke (saklama sınırlaması), kişisel verilerin işlenme amacı ortadan kalktığında silinmesini, yok edilmesini veya anonim hâle getirilmesini gerektirir. Özellikle ÜYZ modellerinin eğitiminde kullanılan kişisel verilerin belirsiz sürelerle saklanması, bu ilkeyle çelişir. İşlenme amacı gerçekleştiğinde (örneğin, bir model sürümünün eğitimi tamamlandığında), kullanılan kişisel veriler imha edilmelidir.

- **Örnek 10:** Bir e-ticaret platformunun, müşteri hizmetleri modelini eğittikten sonra eğitimde kullandığı mesaj kayıtlarını “ileride yeni sürümler geliştirilebileceği” gerekçesiyle belirsiz bir süreyle saklamaya devam etmesi, saklama sınırlaması ilkesine aykırılık teşkil edebilir.

Bu temel ilkeler, verilerin *nasıl* işleneceğini düzenlerken, bir sonraki bölüm verilerin *neden* işlenebileceğine dair hukuki dayanakları ele almaktadır.

1.6 Üretken Yapay Zekâ Sistemlerinde Veri İşlemenin Hukuki Sebepleri

KVKK uyarınca, her kişisel veri işleme faaliyeti, Kanun’un 5. ve 6. maddelerinde belirtilen geçerli bir hukuki sebebe dayanmak zorundadır. KVKK, teknoloji-nötr bir çerçeve sunduğundan bu gereklilik ÜYZ sistemleri için de tam olarak geçerlidir. ÜYZ yaşam döngüsünün model eğitimi ve operasyonel kullanım gibi farklı aşamaları, ayrı hukuki sebepler gerektirebilir.

Genel Nitelikli Kişisel Veriler (KVKK Madde 5)

- **Açık Rıza (Explicit Consent):** Geçerli bir açık rıza, belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanmalıdır. Veri sorumlusu, kullanıcılara kullanılan ÜYZ sisteminin türü, verilerin model geliştirme veya operasyonel kullanım amacıyla mı işleneceği ve verilerin çıktılarda görünme potansiyeli gibi konularda net bilgi vermelidir. Örneğin, bir uygulamayı kullanmak için alınan rıza, kullanıcının verilerinin yeni modeller geliştirmek için kullanılmasına izin

vermez; bu amaç için ayrı bir rıza alınması gerekir. Bu ayrım, KVKK'nın 4. maddesinde düzenlenen "belirli, açık ve meşru amaçlar için işlenme" ilkesinin doğrudan bir yansımasıdır.

- **Sözleşmenin Kurulması veya İfası (Contract Performance):** Bu hukuki sebep, yalnızca veri işlemenin sözleşme kapsamındaki hizmeti sunmak için *kesinlikle gerekli* olduğu durumlarda kullanılabilir. Örneğin, bir sohbet botunun kullanıcının komutlarını işlemesi bu kapsama girerken, aynı verilerin yeni modeller geliştirmek amacıyla kullanılması hizmetin ifası için gerekli olmadığından bu hukuki sebebe dayandırılamaz.
- **İlgili Kişi Tarafından Alenileştirilmiş Olma (Data Made Public by the Data Subject):** Verilerin kamuya açık olması (örneğin sosyal medyada paylaşılması), bu verilerin her amaçla serbestçe kullanılabileceği anlamına gelmez. Veri işleme faaliyeti, veri sahibinin veriyi alenileştirirken taşıdığı ilk irade ve amaçla uyumlu olmalıdır.
- **Meşru Menfaat (Legitimate Interest):** Bu hukuki sebep, veri sorumlusunun menfaatleri ile veri sahibinin temel hak ve özgürlükleri arasında bir denge kurulmasını gerektirir. Kurul'un 2019/78 sayılı kararında belirtilen kriterler doğrultusunda bir **"denge testi"** yapılması zorunludur.
  - **Örnek 11:** Bir şirketin, sosyal medyadan web kazıma yöntemiyle topladığı kamuya açık verilerle dil modelini eğitmek istemesi durumunda, "alenileştirme" şartı uygulanamayacağından, bu faaliyet için titiz bir meşru menfaat değerlendirmesi yapılması gerekir.

1.6.1 Özel Nitelikli Kişisel Veriler (KVKK Madde 6)

Özel nitelikli kişisel verilerin işlenmesi, bireylerin mağduriyetine veya ayrımcılığa maruz kalmasına yol açabilecek yüksek riskler taşıdığından çok daha sıkı kurallara tabidir. Kanun'a 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 veridir.

Bu tür veriler için **sözleşmenin ifası** ve **meşru menfaat** gibi hukuki sebepler kullanılamaz. Ayrıca, Kurul'un 31.01.2018 tarih ve 2018/10 sayılı kararında belirtilen yeterli teknik ve idari güvenlik önlemlerinin ÜYZ bağlamında da titizlikle alınması zorunludur.

Geçerli bir hukuki sebebin belirlenmesinin yanı sıra, veri sorumluları diğer temel uygunluk yükümlülüklerini de yerine getirmelidir.

1.7 Üretken Yapay Zekâ Sistemleri için Temel Uygunluk Yükümlülükleri

Geçerli bir hukuki sebep oluşturmanın ötesinde, veri sorumluları ÜYZ sistemlerini kullanırken KVKK kapsamında birçok kritik yükümlülüğü yerine getirmelidir.

1.7.1 Şeffaflık ve Aydınlatma Yükümlülüğü (KVKK Madde 10)

Veri sorumluları, kişisel verilerin elde edilmesi sırasında veri sahiplerini KVKK Madde 10 uyarınca bilgilendirmekle yükümlüdür. ÜYZ bağlamında bu, aşağıdaki hususları içerir:

- Hizmetin kullanımı ve model geliştirme gibi farklı veri işleme faaliyetleri için ayrı ve açık aydınlatma metinleri sunulmalıdır.
- Gizlilik politikaları, sistem arayüzleri içinde kolayca erişilebilir olmalıdır.
- Kullanıcıların bir sohbet botu gibi ÜYZ sistemiyle etkileşimde bulundukları açıkça belirtilmelidir. Bu, şeffaflık için temel bir gerekliliktir.

1.7.2 İlgili Kişi Haklarının Sağlanması (KVKK Madde 11)

Veri sahipleri; verilerine erişme, verilerinin düzeltilmesini veya silinmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme gibi KVKK Madde 11'de sayılan haklara sahiptir. Bu hakların karmaşık ÜYZ sistemlerinde sağlanması teknik zorluklar içerse de bu durum veri sorumlusunu yasal yükümlülüklerinden kurtarmaz. Özellikle işe alım veya kredi değerlendirmesi gibi kritik süreçlerde ÜYZ kullanıldığında, kişinin kendisi aleyhine bir sonucun ortaya çıkmasına **itiraz etme hakkı** (Madde 11(1)(g)) büyük önem taşır ve insan merkezli YZ yaklaşımının temel bir parçasını oluşturur. Veri sorumluları, bu hakların etkin kullanımını sağlamak için **"tasarımdan itibaren mahremiyet" (privacy by design)** ve **"varsayılan olarak mahremiyet" (privacy by default)** yaklaşımlarını benimsemelidir.

1.7.3 Veri Güvenliği Tedbirleri (KVKK Madde 12)

Veri sorumluları, KVKK Madde 12 uyarınca veri güvenliğini sağlamak için uygun teknik ve idari tedbirleri almak zorundadır. ÜYZ sistemleri için önerilen bazı tedbirler şunlardır:

- Privacy by Design ve Privacy by Default ilkelerini benimsemek.
- Veri koruma etki değerlendirmeleri yapmak.
- Mahremiyet Artırıcı Teknolojileri (Privacy-Enhancing Technologies) entegre etmek.
- Prompt injection gibi ÜYZ'ye özgü saldırılara karşı teknik kontroller uygulamak.
- Sistemdeki zayıf noktaları tespit etmek için "kırmızı takım" (red teaming) teknikleri kullanmak.
- Çalışanlar için sağlam farkındalık ve eğitim programları yürütmek.

1.7.4 Kişisel Verilerin Yurt Dışına Aktarımı (KVKK Madde 9)

Kişisel verilerin yurt dışına aktarımı, KVKK Madde 9 ve ilgili ikincil mevzuatta belirtilen sıkı kurallara tabidir. Türkiye'de yerleşik bir veri sorumlusunun, sunucuları yurt dışında bulunan bir ÜYZ hizmetini kullanması, uluslararası veri aktarımı olarak kabul edilir ve bu kurallara uygun şekilde gerçekleştirilmelidir.

Bu yasal yükümlülüklerin yerine getirilmesi, ÜYZ ekosisteminin güvenli bir temel üzerinde işlemesini sağlarken, teknolojinin sorumlu kullanımı bireysel kullanıcılar ve ebeveynler için

de pratik adımlar gerektirmektedir.

1.8 Sorumlu Kullanım için Pratik Rehber

ÜYZ teknolojilerinin güvenli ve etik kullanımı, yalnızca geliştiricilerin değil, aynı zamanda son kullanıcıların ve ebeveynlerin de sorumluluğundadır. Bu rehber, güvenli kullanım için pratik öneriler sunmaktadır.

1.8.1 Bireysel Kullanıcılar için Öneriler

- **Kişisel Veri Paylaşımından Kaçınma:** Kendinize veya üçüncü kişilere ait ad, soyad, T.C. kimlik numarası, adres gibi doğrudan tanımlayıcı bilgileri istemlere (prompt) girmekten kaçının.
- **Hassas Bilgilerin Korunması:** Sağlık, finans veya hukuki süreçlere ilişkin hassas nitelikteki bilgileri ÜYZ sistemleriyle paylaşmayın.
- **Genelleştirilmiş İfadeler Kullanma:** Kişi isimleri, belirli tarihler veya konumlar yerine soyut ve genel bir anlatım benimseyerek istemlerinizi anonimleştirin.
- **Gizlilik Politikalarını İnceleme:** Kullandığınız uygulamanın aydınlatma metnini ve gizlilik politikasını okuyarak verilerinizin nasıl işlendiğini, kimlerle paylaşıldığını ve ne kadar süreyle saklandığını öğrenin.
- **Gizlilik Ayarlarını Yapılandırma:** Uygulamaların gizlilik ayarlarını gözden geçirin ve mümkün olan durumlarda veri paylaşımını sınırlayıcı tercihleri aktif hâle getirin.

1.8.2 Çocukların Korunması: Ebeveynlere Yönelik Tavsiyeler

Çocuklar, ÜYZ teknolojilerini kullanırken uygunsuz içeriklere maruz kalma, yanlış bilgiyle karşılaşma ve deep fake gibi teknolojilerle manipüle edilme gibi özel risklerle karşı karşıyadır.

- **Yaşa Uygunluk Kontrolü:** Çocuklarınızın kullandığı platformların yaşlarına uygun içerikler sunduğundan emin olun.
- **Deep Fake Riskleri Hakkında Bilinçlendirme:** Çocuklarınıza deep fake teknolojisinin varlığını ve dijital içerikleri sorgulamanın önemini anlatarak eleştirel düşünme becerileri kazandırın.
- **Kişisel Bilgi Paylaşımı Konusunda Eğitim:** Ad, okul veya adres gibi kişisel bilgilerini çevrim içi ortamlarda paylaşmamaları gerektiğini öğretin.
- **Açık İletişim ve Rehberlik:** ÜYZ teknolojilerinin ne olduğu, nasıl çalıştığı ve her zaman doğru bilgi üretmeyebileceği konusunda çocuklarınızla açık bir diyalog kurun.
- **Ekran Süresi Sınırları Belirleme:** Dijital yaşam ile gerçek yaşam arasında sağlıklı bir denge kurmaları için ÜYZ araçlarının kullanım süresine sınırlar koyun.
- **Duygusal ve Psikolojik Etkileri Gözlemleme:** Teknoloji kullanımının çocuklarınızın gerçeklik algısı, özgüveni veya sosyal etkileşimleri üzerindeki olası olumsuz etkilerine karşı dikkatli olun ve gerekirse uzman desteği alın.

Üretken Yapay Zekâ hem bireyler hem de kurumlar için önemli fırsatlar sunarken,

beraberinde veri koruma ve mahremiyet açısından yönetilmesi gereken ciddi zorluklar getirmektedir. Ancak sorumlu, şeffaf, insan merkezli ve mahremiyet bilincine sahip bir yaklaşımla, bu teknolojinin sunduğu imkânlardan temel hak ve özgürlükleri koruyarak güvenli bir şekilde yararlanmak mümkündür.