Etken Yapay Zekâ (Agentic AI) Kullanımına İlişkin Doküman Yayımlandı

13 Nisan 2026

12 Mart 2026 tarihinde Kişisel Verileri Koruma Kurumu ("**Kurum**") tarafından, Etken Yapay Zekâ ("**Etken YZ**") sistemleri, bu sistemlerde Yapay Zekâ Aracıları'nın (AI Agents) işlevleri ile potansiyel kullanım alanları ve risklerine ilişkin genel bir değerlendirme sunan Etken Yapay Zekâ (Agentic AI) isimli doküman ("**Doküman**") yayımlandı. Doküman'da öne çıkan başlıkları aşağıda özetledik.

➢ Etken YZ Sistemleri

Başlangıçta, yapay zekâ sistemleri genellikle önceden tanımlanmış ve tekrarlayan görevleri yerine getirebilecek şekilde tasarlanmışken, zamanla bu sistemlerin kullanım alanları genişledi ve daha karmaşık görevlerde de kullanılmaya başlandı. Bu değişimle birlikte, yapay zekâ sistemleri belirli hedeflere ulaşmaya yönelik eylem seçeneklerini değerlendirebilen ve farklı bağlamlarda işlev görebilen yapılar haline geldi.

Bu gelişimin sonucunda, bugün, "Etken YZ" (Agentic AI) kavramı öne çıkmaktadır. Doküman'da Etken YZ sistemleri "***belirli hedeflere ulaşmak amacıyla çevresel koşulları değerlendirebilen, değişen durumlara uyum sağlayabilen ve farklı düzeylerde otonom biçimde eylem başlatabilen bütünleşik yapılar***" olarak ifade edilmektedir.

Doküman'da, **Etken YZ sistemlerine** birtakım örnekler verilmiştir. Bu örnekler arasında;

- Trafik ve hava koşullarına göre teslimat rotalarını yeniden planlayan lojistik sistemleri,
- Olağan dışı ağ etkinliklerini tespit edip önlem alan siber güvenlik sistemleri ve
- Kullanıcı etkileşimlerine göre destek taleplerini yöneten ve ilk müdahaleyi yapan müşteri destek sistemleri

yer almaktadır.

Buna karşılık; Doküman'da etken olmayan yapay zekâ sistemlerine verilen örnekler de şunlardır:

- İstenmeyen e-postaları sınıflandırmaya yönelik bir spam filtresi,
- Çalışanların sorularına şirket el kitabına dayanarak cevap veren bir sohbet botu ve
- Geçmiş işe alım verilerini kullanarak adayları sıralayan özgeçmiş tarama aracı.

➢ Etken YZ Sistemlerinde Yapay Zekâ Aracıları

Etken YZ sistemleri, karar alma ve eylem süreçlerini "Yapay Zekâ Aracıları" (YZ Aracısı/AI Agents) aracılığıyla yürütmektedir. Doküman'da, YZ Aracısı, "***çevresini algılayan, bu çevreye tepki veren ve belirlenen hedefler doğrultusunda eylemlerde bulunan otomatik bir etmen***" olarak tanımlanmaktadır.

YZ Aracıları, çevresindeki verileri işleyerek hedeflerine ulaşmayı amaçlar ve bunun için çeşitli araçlardan yararlanabilir. Örneğin bir konferans organizasyonu görevi verilen YZ Aracısı, ihtiyaçları belirler, uygun mekanları araştırır ve gerekli adımları planlayıp uygulamaya geçirir.

Etken YZ sistemleri ise birden fazla YZ Aracısı'nı belirli hedeflere ulaşacak şekilde konumlandırır, bu aracıların görevlerini, etkileşim biçimlerini ve karar alma ile eylem süreçlerini daha geniş bir sistem mantığı içinde ele alır.

Doküman'da, bu ilişki bir restoranın baş şefiyle aşçıları arasındaki ilişkiye benzetilmektedir. Baş şef (Etken YZ sistemi); menüyü belirler, hazırlık ve servis süreçlerini planlar ve mutfağın işleyişini koordine ederken, aşçılar (YZ Aracıları) bir sürecin belirli bir aşamasının yürütülmesi gibi görece dar kapsamlı görevleri yerine getirir.

Çoklu YZ Aracısı Sistemleri: Karmaşık hedeflerin yönetildiği durumlarda, **birden fazla YZ Aracısı'nın koordineli şekilde çalıştığı Çoklu YZ Aracısı sistemleri devreye girer**. Bu sistemler, görevleri daha küçük parçalara bölerek daha verimli ve esnek bir yapı sağlar.

Bu kapsamda, Çoklu YZ Aracısı sistemleri, Etken YZ sistemlerinin bir alt türü veya uygulama biçimi olarak değerlendirilebilir. Etken YZ sistemleri genel olarak otonom eylem gerçekleştiren yapıları ifade ederken, Çoklu YZ Aracısı sistemleri, bu yapının birden fazla YZ Aracısı'nın koordinasyonuna dayandığı bir mimariyi ifade eder.

➢ Etken YZ Sistemleri Bağlamında Kişisel Verilerin Korunması Bakımından Potansiyel Riskler

Kurum, Doküman'da Etken YZ sistemleri kapsamında kişisel verilerin korunmasına ilişkin potansiyel risklere örnekler vermektedir. Bu örnekleri sizler için aşağıdaki şekilde özetledik:

- **Veri Kullanımının Büyümesi ve Değişkenliği:** Etken YZ sistemleri, görevlerini yerine getirirken veri kullanımını zamanla değiştirebilir ve başlangıçta öngörülemeyen veri kümelerini sürece dahil edebilir. Bu durum, veri işleme faaliyetlerinin kapsamını genişleterek, amaçla sınırlılık ve veri minimizasyonu ilkelerine uyumu zorlaştırabilir. Ayrıca, veri işleme ile hukuki sebep arasındaki bağın zayıflaması riskini doğurabilir.

Dolayısıyla, belirlenen veri işleme amaçları ile veri işleme faaliyetleri arasındaki ilişkinin ve hukuki sebep bağının sistemin işleyişi boyunca dikkate alınması önemlidir.

- **Özel Nitelikli Kişisel Verilere İlişkin Riskler:** Etken YZ sistemlerinde özel nitelikli kişisel verilerin işlenmesi, bireylerin mağduriyet yaşaması veya ayrımcılığa maruz kalması riskini artırabilir.

- **Önyargı ve Ayrımcılık Riski:** Etken YZ sistemlerinin geniş ve yapılandırılmamış veri kümeleri üzerinden eğitilmesi, mevcut toplumsal veya kültürel önyargıların sistem çıktılarında yansımasına neden olabilir; bu durum, bireyler bakımından ayrımcılık riskini artırabilir.

- **Otonomi ve Kontrol Riski:** Etken YZ sistemlerinin artan otonomi düzeyi, sistemlerin insan müdahalesi olmaksızın eylem başlatabilmesine yol açabilir; bu durum, sistem çıktılarının öngörülebilirliğini ve kontrol edilebilirliğini zorlaştırarak istenmeyen sonuçların ortaya çıkmasına neden olabilir.

- **Teknik Tasarım ve Operasyonel Riskler:** Etken YZ sistemlerinin karmaşık yapısı, YZ aracıları kaynaklı işleyiş aksaklıkları, sistemlerin kötüye kullanıma açık olması ve teknik doğrulama süreçlerindeki zorluklar, sistemlerin güvenilirliği ve etkinliği açısından riskler doğurabilir.

- **Çıkarıma Dayalı Veri Kullanımı ve Veri Anonimleştirmenin Zorlaşması:** Etken YZ sistemlerinin farklı veri kaynaklarını ilişkilendirme kapasitesi, sınırlı veya kişisel veri niteliği taşımayan verilerden bireyler hakkında daha hassas bilgilerin çıkarılmasına neden olabilir ve anonimleştirilmiş verilerin yeniden kişisel verilerle ilişkilendirilmesine yol açarak anonimleştirme süreçlerini zorlaştırabilir.

- **Şeffaflık, Açıklanabilirlik ve Hesap Verebilirlik Eksiklikleri:** Etken YZ sistemlerinde karar alma süreçlerinin çok adımlı ve dağıtık yapısı, hangi eylemin hangi aşamada ve hangi veri ile gerçekleştirildiğinin izlenmesini zorlaştırarak kişisel veri işleme süreçlerinin şeffaflığını ve açıklanabilirliğini olumsuz etkileyebilir. Ayrıca, birden fazla YZ Aracısı'nın ve farklı aktörlerin sürece dâhil olması, sorumluluk ve hesap verebilirlik çerçevesinin net şekilde belirlenmesini güçleştirebilir ve olası ihlal veya zararlardan hangi tarafın sorumlu olduğunun tespitini zorlaştırabilir.

- **Kişisel Verilerin Doğruluğu ve Halüsinasyon Riski:** Etken YZ sistemlerinde, özellikle ÜYZ modellerinin kullanımıyla, "halüsinasyon" olarak bilinen hatalı ancak ikna edici çıktılar üretilebilir. Bu çıktılar, sonraki aşamalarda yanlış bilgilere dayalı kararlar alınmasına yol açabilir ve kişisel verilerin doğruluğunu tehlikeye atabilir.

- **Güvenlik ve Sistem Dayanıklılığı Riski:** Etken YZ sistemlerinin birden fazla veri kaynağı, araç ve dijital ortamla entegre şekilde çalışması, saldırı yüzeyinin genişlemesine ve yeni güvenlik zafiyetlerinin ortaya çıkmasına neden olabilir.

Sonuç olarak, Etken YZ sistemlerinin kullanımında kişisel verilerin korunmasına yönelik risklerin etkili bir şekilde yönetilmesi için sistemin tasarımında, veri kullanımı sürecinde ve idari tedbirlerde dikkatli planlama yapılması kritik bir öneme sahiptir. Bu riskler, veri koruma düzenlemelerinin etkin bir şekilde uygulanmasını gerektirir.

➢ Peki Ne Yapmak Gerek?

Kurum, Doküman'da, Etken YZ sistemlerinde kişisel verilerin korunması bakımından, sistemlerin otonomi düzeyi, kullanım amacı ve mimari özellikleri dikkate alınarak **risk temelli bir yaklaşım** benimsenmesinin önemini vurgulamaktadır. Bu kapsamda alınabilecek başlıca önlemler aşağıda gibidir:

- **İnsan gözetimi:** Artan otonomi düzeyi dikkate alınarak, sistemlerin belirlenen hedefler, etik ilkeler ve toplumsal beklentilerle uyumlu çalışmasını sağlayacak anlamlı insan katılımı ve gözetim mekanizmalarının oluşturulması önemlidir.

- **Şeffaflık ve açıklanabilirlik:** Sistemlerin işleyişinin, kullanılan verilerin ve karar alma gerekçelerinin anlaşılabilir olması için uygun açıklanabilirlik ve izlenebilirlik mekanizmalarının tasarım aşamasından itibaren gözetilmesi gerekmektedir.

- **Veri doğruluğunun sağlanması:** Sistem çıktılarının güvenilirliğini korumak amacıyla kullanılan verilerin güncelliğinin ve doğruluğunun süreç boyunca izlenmesi, özellikle çıktının başka süreçlerde girdi olarak kullanıldığı durumlarda önem taşımaktadır.

- **Rol ve sorumlulukların netleştirilmesi:** Geliştiriciler, yerleştiriciler (deployers) ve diğer ilgili aktörler arasında görev, yetki ve sorumlulukların açık şekilde tanımlanması, sistem kaynaklı risklerin etkin şekilde yönetilmesini destekleyebilir.

- **Tasarımdan itibaren mahremiyet ve varsayılan olarak mahremiyet yaklaşımı:** "Privacy by design" ve "privacy by default" ilkelerinin benimsenmesi ve mahremiyet artırıcı teknolojilerin kullanılması, kişisel verilerin korunmasına yönelik risklerin erken aşamada ele alınmasına katkı sağlayabilir.

- **Risk değerlendirme mekanizmaları:** Sistemlerin yaşam döngüsü boyunca ortaya çıkabilecek veri koruma risklerinin değerlendirilmesi ve gerekli durumlarda veri koruma etki değerlendirmesi (DPIA) gibi araçlardan yararlanılması faydalı olabilir.

- **Yönetişim ve farkındalık:** Kurum içi veri yönetişimi süreçlerinin Etken YZ sistemlerine uyumlu hale getirilmesi ve bu sistemleri kullanan veya yöneten kişiler için eğitim ve farkındalık faaliyetlerinin yürütülmesi de veri güvenliğinin güçlendirilmesine katkı sağlayabilir.

Bora Yazıcıoğlu
bora@yazicioglulegal.com

Nafiye Yücedağ
nafiye@yazicioglulegal.com

Ece Oğur
eceogur@yazicioglulegal.com

Bu not hukuki görüş niteliğinde değildir. Sadece bilgi amaçlı hazırlanmış ve gönderilmiştir. Konuyla ilgili hukuki görüş almak isterseniz bizimle bağlantıya geçmenizi rica ederiz.