

Yapay Zekâ Sistemlerinin Avrupa Birliği Yapay Zekâ Yasası Kapsamında Sınıflandırılması



AB YZ Yasası'nda Öngörülen Risk Kategorizasyonu

AB YZ Yasası'na göre, YZ sistemlerini belirli bir kategoriye entegre etmek için öncelikle sistemin potansiyel kullanım alanları ve bu alanlardaki risk seviyeleri değerlendirilmelidir.



KABUL EDİLEMEZ RİSK KATEGORİSİNDE YER ALAN SİSTEMLERİN BELİRLENMESİ

Bir YZ sisteminin risk seviyesini değerlendirirken ilk adım, sistemin AB YZ Yasası'nın 5. maddesinde belirtilen yasaklanmış kategorilerden birinin kapsamına girip girmediğini belirlemektir. Bu madde, hem kesin yasakları hem de belirli istisnaları belirtir. Madde kapsamında sınırlı şekilde sayılan YZ sistemlerinin kullanımı yasaklanmıştır. Temel hakları ihlal eden ve bu sebeple AB değerlerine aykırı olan yasaklı YZ sistemleri şu şekilde örneklendirilebilir:

- İnsanların karar verme yeteneğini ciddi şekilde manipüle edebilecek aldatıcı tekniklerin kullanıldığı YZ sistemleri.
- Yaş, fiziksel veya zihinsel engel veya sosyoekonomik durum gibi bireysel zayıflıkları hedef alan YZ uygulamaları.
- Hassas karakteristik özellikleri hedef alan biyometrik kategorizasyon sistemleri.
- Kamu otoriteleri tarafından uygulanan, toplumsal davranış veya algılanan kişilik özelliklerine dayanarak olumsuz sonuçlar doğurabilecek sosyal puanlama.
- Acil tehdit durumları veya ciddi suçlardan şüphelenilen kişilerin tespiti dışında, kolluk kuvvetleri tarafından gerçek zamanlı biyometrik tanımlama sistemlerinin kamusal alanda kullanımı.
- Yüz tanıma faaliyetleri için yüz görüntülerinin hedeflenmemiş şekilde kazanması.

SINIRLI RİSKLİ VEYA MİNİMUM RİSKLİ/RİSKSİZ YZ SİSTEMLERİ

- Sohbet botları ve deepfake gibi uygulamalar, AB YZ Yasası kapsamında sınırlı riskli olarak kabul edilmektedir. Görece daha hafif şeffaflık yükümlülüklerine tabi olan sınırlı riskli YZ sistemlerinde geliştiriciler ve dağıtıcılar, son kullanıcıların YZ ile etkileşime girdiklerinin farkında olmalarını sağlamalıdır.
- AB YZ Yasası, minimum riskli/risksiz YZ sistemleri için herhangi bir ek yasal yükümlülük getirmemektedir. Davranış kuralları ve şeffaflık gereklilikleri gibi uygulamalar, bu sistemler için gönüllülük esasına dayalı olarak benimsenebilecektir.

YÜKSEK RİSK KATEGORİSİNDE YER ALAN SİSTEMLERİN BELİRLENMESİ

Yüksek riskli YZ sistemleri şunlardır:

- AB YZ Yasası Ek I'deki AB yasaları kapsamında bir ürünün güvenlik bileşeni olarak kullanılan veya kendileri bir ürün olan ve ilgili AB sektörel ürün güvenliği yasaları tarafından düzenlenen YZ sistemleri.
- AB YZ Yasası Ek III'te listelenen YZ sistemleri.

Ek III'te listelenen YZ sistemleri şu şekilde örneklendirilebilir:

- Kritik altyapılarda kullanılan sistemler (Ulaşım, enerji, su, gıda, telekomünikasyon vb.)
- Eğitim ve mesleki eğitimde kullanılan sistemler (Sınav ve değerlendirme sistemleri, öğrenci davranışı izleme vb.)
- Biyometrik tanımlama ve kategorileendirme sistemleri (Biyometrik doğrulama hariç uzaktan biyometrik tanıma sistemleri, hassas veya korunan nitelikleri veya özellikleri hedef almayan biyometrik kategorizasyon yöntemleri, duygu tanıma sistemleri vb.)
- İstihdam, işçi yönetimi ve serbest mesleğe erişimde kullanılan sistemler (İşe alma, terfi, görev atama vb.)
- Temel özel ve kamu hizmetlerine erişim ve bunlardan yararlanmaya ilişkin sistemler (Kredi puanlama, sosyal güvenlik, acil durum müdahaleleri vb.)
- Kolluk kuvvetleri tarafından kullanılan sistemler (Suç tespitleri, soruşturmaları veya kovuşturmaları sırasında profillemeye, cezai soruşturmalar veya kovuşturmalar sırasında kanıt güvenilirliğini değerlendirme, bireyin suç mağduru olma riskini değerlendirme, poligraflar vb.)
- Göç, iltica ve sınır kontrolüne ilişkin sistemler (Belge doğrulama, risk değerlendirme, vize veya oturma izni başvurularının incelenmesi vb.)
- Adalet ve demokratik süreçlerin yönetiminde kullanılan sistemler (Gerçekleri araştırmak ve yorumlamak ve hukuku somut gerçeklere uygulamak veya alternatif uyuşmazlık çözümü, seçimleri ve referandum sonuçlarını veya oy verme davranışlarını etkilemek vb.)

AB YZ YASASI KAPSAMINDA YÜKSEK RİSKLİ SİSTEMLER İÇİN YÜKÜMLÜLÜKLER NELERDİR?

Yükümlülüklerin çoğu, yüksek riskli AI sistemlerinin sağlayıcıları için öngörülmüştür. AB'de veya üçüncü bir ülkede bulunmalarına bakılmaksızın, yüksek riskli AI sistemlerini AB'de piyasaya sürmeyi veya hizmete sokmayı amaçlayanlar ve yüksek riskli AI sisteminin çıktısının AB'de kullanıldığı üçüncü ülke sağlayıcıları aşağıda sayılan yükümlülüklerle tabidir:

- Yüksek riskli AI sisteminin yaşam döngüsü boyunca bir risk yönetim sistemi kurmak.
- Veri yönetimini yürütmek, eğitim, doğrulama ve test veri kümelerinin ilgili, yeterince temsili ve mümkün olan en iyi ölçüde hatasız ve amaçlanan amaca uygun şekilde eksiksiz olmasını sağlamak.
- Uyumluluğu göstermek için teknik dokümantasyon hazırlamak ve yetkililere bu uyumu değerlendirmek için bilgi sağlamak.
- Yüksek riskli AI sistemlerini, ulusal düzeydeki riskleri ve sistemin yaşam döngüsü boyunca önemli değişiklikleri belirlemek için ilgili olayları otomatik olarak kaydetmesini sağlayacak şekilde kayıt tutma amacıyla tasarlamak.
- Sistemleri, uygun insan denetimini sağlayacak şekilde tasarlamak.
- Yeterli düzeyde doğruluk, sağlamlık ve siber güvenliğin sağlamak.
- Sonraki dağıtıcıların uyumluluğunu sağlamak için kullanım talimatları sağlamak.
- Uyumluluğu sağlamak için bir kalite yönetim sistemi kurmak.
- Uygunluk değerlendirmeleri yoluyla uyumluluğu ispat etmek.
- Sistemin kamu otoriteleri tarafından dağıtıldığı hallerde, kolluk kuvvetleri veya göç için kullanılmadığı sürece kamuya açık bir AB veritabanına kayıt.

Dağıtımdan önce, kamu hukuku tüzel kişiliği dağıtıcıları, bir kamu hizmeti sağlayan özel operatörler ve kredi itibarını, acil durum çağrılarını veya hayat ve sağlık sigortası için risk ve fiyatlandırmayı değerlendirmek için YZ sistemleri kullanan özel operatörler, sistemlerin temel haklar üzerindeki etkisini değerlendirmelidir. Veri koruma etki değerlendirmesi gerekiyorsa, temel haklar etki değerlendirmesi, veri koruma etki değerlendirmesi ile birlikte yürütülmelidir.

Genel Amaçlı YZ Modelleri

Belirgin bir genellik sergileyen, piyasaya nasıl sunulduklarına bakılmaksızın çok çeşitli farklı görevleri yetkin bir şekilde yerine getirebilen ve çeşitli alt sistemlere veya uygulamalara entegre edilebilen YZ modelleri, AB YZ Yasası kapsamında **genel amaçlı YZ modeli** olarak tanımlanmaktadır. Bu tanım, araştırma, geliştirme ve prototipleme faaliyetleri için piyasaya sürülmeden önce kullanılan YZ modellerini kapsamaz.

Genel amaçlı YZ sistemi ise, genel amaçlı bir YZ modeline dayanan, hem doğrudan kullanım hem de diğer YZ sistemlerine entegrasyon için çeşitli amaçlara hizmet etme yeteneğine sahip YZ sistemi anlamına gelir. Genel amaçlı YZ modelleri bir sisteme entegre edildikten sonra, bu sistem yüksek riskli olarak kabul edilirse, sağlayıcılar hem genel amaçlı YZ modelleri hem de yüksek riskli sistemler için öngörülen yükümlülüklerle uymalıdır.

Genel amaçlı YZ modelleri, eğitimi için kullanılan kümülatif hesaplama miktarı 10^{25} kayan nokta işleminden (floating point operations - FLOPs) fazla olduğunda **sistemik riskler** arz eder. Sağlayıcılar, modellerinin bu kriteri karşılayıp karşılamadığını 2 hafta içinde Komisyona bildirmelidir. Sağlayıcı, kriterleri karşılamasına rağmen modelinin sistemik risk oluşturmadığına dair argümanlar sunabilir. Komisyon kendi başına veya bağımsız uzmanlardan oluşan bilimsel panelden gelen nitelikli bir uyarı yoluyla bir modelin yüksek etki kapasitesine sahip olduğuna ve sistemik olduğuna karar verebilir.

Bir YZ modelinin “genel amaçlı” olarak sınıflandırılması için aşağıdaki kriterler dikkate alınmaktadır:

1

Çok Yönlülük: Sistem, çeşitli alanlarda ve farklı görevlerde kullanılabilir.



2

Bağlamsal Uyumluluk: Sistem, bağlam ve ortam değişikliklerine uyum sağlayabilir.



3

Yeniden Eğitim ve Adaptasyon: Sistem, yeni verilerle yeniden eğitilebilir veya modifiye edilebilir olmalıdır.



Modellerin ve sistemlerin tanım ve sınıflandırmaları, kullanılacağı bağlama göre belirlenmeli ve ilgili düzenlemeler yapılmalıdır.

GENEL AMAÇLI YZ MODELLERİ İÇİN YÜKÜMLÜLÜKLER

Genel amaçlı YZ modelleri, AB YZ Yasası kapsamında YZ sistemlerinden ayrı olarak ele alınmaktadır ve öncelikle sağlayıcıları hedef alan kendi özel yükümlülüklerine sahiptir. Genel amaçlı YZ modellerinin tüm sağlayıcıları şunları yükümlülüklerle tabidir:

- Eğitim, test süreci ve değerlendirme sonuçları da dahil olmak üzere teknik dokümantasyonun hazırlanması ve güncel tutulması.
- Genel amaçlı YZ modelini kendi YZ sistemlerine entegre etmek isteyen alt tedarikçilerin, yetenekleri ve sınırlamaları anlamaları ve uyum sağlama için bilgi ve dokümantasyonun hazırlanması ve kullanıma sunulması.
- AB Telif Hakkı Direktifine uyumun sağlanması için politikaların oluşturulması.
- Genel amaçlı YZ modelinin eğitimi için kullanılan içerik hakkında ayrıntılı bir özet hazırlanması ve kamuya açık hale getirilmesi.

Tüm genel amaçlı YZ model sağlayıcıları, Avrupa uyumlaştırılmış standartları yayınlanana kadar gönüllü olarak bir uygulama kuralına (*code of practice*) uymaları halinde yükümlülüklerine uyduklarını gösterebilirler; bu kurallara uyulması bir uygunluk karanesi sağlayacaktır. Uygulama kurallarına uymayan sağlayıcılar, Komisyon onayı için alternatif yeterli uyum araçları göstermelidir.

SİSTEMATİK RİSKE SAHİP GENEL AMAÇLI YZ MODELLERİ İÇİN YÜKÜMLÜLÜKLER

Tüm genel amaçlı YZ modelleri için öngörülen yükümlülüklerle ek olarak, sistemik riske sahip genel amaçlı modellerinin sağlayıcılarının yükümlülükleri:

- Sistemik riski tanımlamak ve azaltmak için çeşitli testler yapmak ve belgelemek de dahil olmak üzere model değerlendirmeleri yapmak.
- Kaynakları da dahil olmak üzere olası sistemik riskleri değerlendirmek ve azaltmak.
- Ciddi olayları ve olası düzeltici önlemleri gecikmeksizin takip etmek, belgelemek, YZ Ofisine (*AI Office*) ve ilgili ulusal yetkili makamlara rapor etmek.
- Yeterli düzeyde siber güvenlik koruması sağlamak.

UYGULAMA KURALLARI

- Uluslararası yaklaşımları dikkate alacaktır.
- Yukarıda sayılan yükümlülükleri kapsayacak ancak bunlarla sınırlı kalmayacaktır. Özellikle de yetkili makamlar ve alt tedarikçiler için teknik dokümantasyona dahil edilecek ilgili bilgiler, sistemik risklerin türünün, niteliğinin ve kaynaklarının tanımlanması ve değer zinciri boyunca ortaya çıkma ve gerçekleşme biçimleri nedeniyle risklerin ele alınmasındaki belirli zorlukları hesaba katan risk yönetimi yöntemleri sürece dahil edilecektir.
- YZ Ofisi, genel amaçlı model sağlayıcılarını ve ilgili ulusal yetkili makamları uygulama kurallarının hazırlanmasına katılmaya davet edebilirken, sivil toplum, endüstri, akademi, alt tedarikçiler ve bağımsız uzmanlar süreci destekleyebilir.

ŞEFFAFLIK GEREKLİLİKLERİ

Belirli YZ sistemlerinin sağlayıcılarına ve dağıtıcılarına özel şeffaflık yükümlülükleri getirilmiştir. Bir YZ sistemi, hem şeffaflık gerekliliklerine hem de yüksek riskli YZ sistemleri veya genel amaçlı YZ modelleri için gerekliliklere tabi olabilir.

- Gerçek kişilerle doğrudan etkileşime giren YZ sistemleri sağlayıcıları, bireysel kullanıcıların bir YZ sistemi ile etkileşime girdiklerinin farkında olmalarını sağlayacak şekilde YZ sistemleri tasarlamalı ve geliştirmelidir.
- Sentetik ses, görüntü, video veya metin içeriği üreten YZ sistemleri ve genel amaçlı YZ sistemleri sağlayıcıları, çıktılarının makine tarafından okunabilir bir formatta işaretlendiğinden ve YZ tarafından üretildiği veya manipüle edildiğinin tespit edilebildiğinden emin olmalıdır.
- Duygu tanıma veya biyometrik kategorizasyon sistemlerinin dağıtıcıları, gerçek kişileri sistemlerin operasyonları hakkında bilgilendirmelidir.
- Kamu yararını ilgilendiren konularda halkı bilgilendirmek amacıyla deepfake üreten veya metni manipüle eden YZ sistemlerinin dağıtıcıları, açıklama gerekliliklerine uymalıdır.

UYGULAMA VE YAPTIRIMLAR

Avrupa Komisyonu bünyesinde yer alan YZ Ofisi, Üye Devletler arasında yönetişimi koordine etmek ve genel amaçlı YZ ile ilgili kuralların uygulanmasını denetlemek için çalışmaktadır. Model ve sistem aynı sağlayıcı tarafından sağlandığında, genel amaçlı modellere dayalı YZ sistemlerini denetleyecektir. Bir piyasa gözetim otoritesinin yetkilerine sahiptir. Ulusal piyasa gözetim otoriteleri, diğer tüm YZ sistemlerinin denetiminden sorumludur. İkincil sağlayıcılar, birincil sağlayıcıların ihlalleri ile ilgili olarak YZ Ofisi'ne şikayette bulunabilir.

Genel amaçlı YZ modellerini denetlemek, standartların ve test uygulamalarının geliştirilmesine katkıda bulunmak ve üye devletler arasında kuralları uygulamak için YZ Ofisi; Avrupa Komisyonu ve üye devlet yetkili makamlarına tavsiyelerde bulunmak ve yardımcı olmak için YZ Kurulu (AI Board); kurula ve Komisyona tavsiyelerde bulunmak ve teknik uzmanlık sağlamak için Danışma Forumu ve yasanın uygulanmasını ve uygulanmasını desteklemek için bağımsız uzmanlardan oluşan Bilimsel Panel (Scientific Panel) kurar.

Üye Devlet otoriteleri, cezalar ve diğer uygulama önlemleri dahil olmak üzere uygulama kurallarını belirlemektedir. Bireyler, ihlal durumlarında ulusal yetkili bir otoriteye şikâyetle bulunabilir ve bu otorite, pazar denetim faaliyetlerini başlatabilir.

- Yasaklanan YZ sistemlerinin kullanımı halinde, global yıllık cironun %7'sine veya 35 milyon Avroya kadar idari para cezası (hangisi daha yüksek ise).
- Diğer ihlaller için, global yıllık cironun %3'üne veya 15 milyon Avroya kadar idari para cezası (hangisi daha yüksek ise).
- Yetkililere yanlış bilgi verilmesi durumunda, global yıllık cironun %1'ine veya 7,5 milyon Avroya kadar idari para cezası (hangisi daha yüksek ise).

YZ Kurulu, yasanın uygulanması konusunda tavsiyelerde bulunacak, ulusal makamlar arasında koordinasyon sağlayacak ve tavsiye ve görüşler yayınlayacaktır.



Hazırlayan:

İrem Aslan

Av. Özden Serinay Öz

Av. Necati Alp Çelebi

İnfografik Ekibi:

Av. Özden Serinay Öz

Stj. Av. İlayda Karaaslan

Tasarım:

Av. Zeynep Öğretmen Kotil