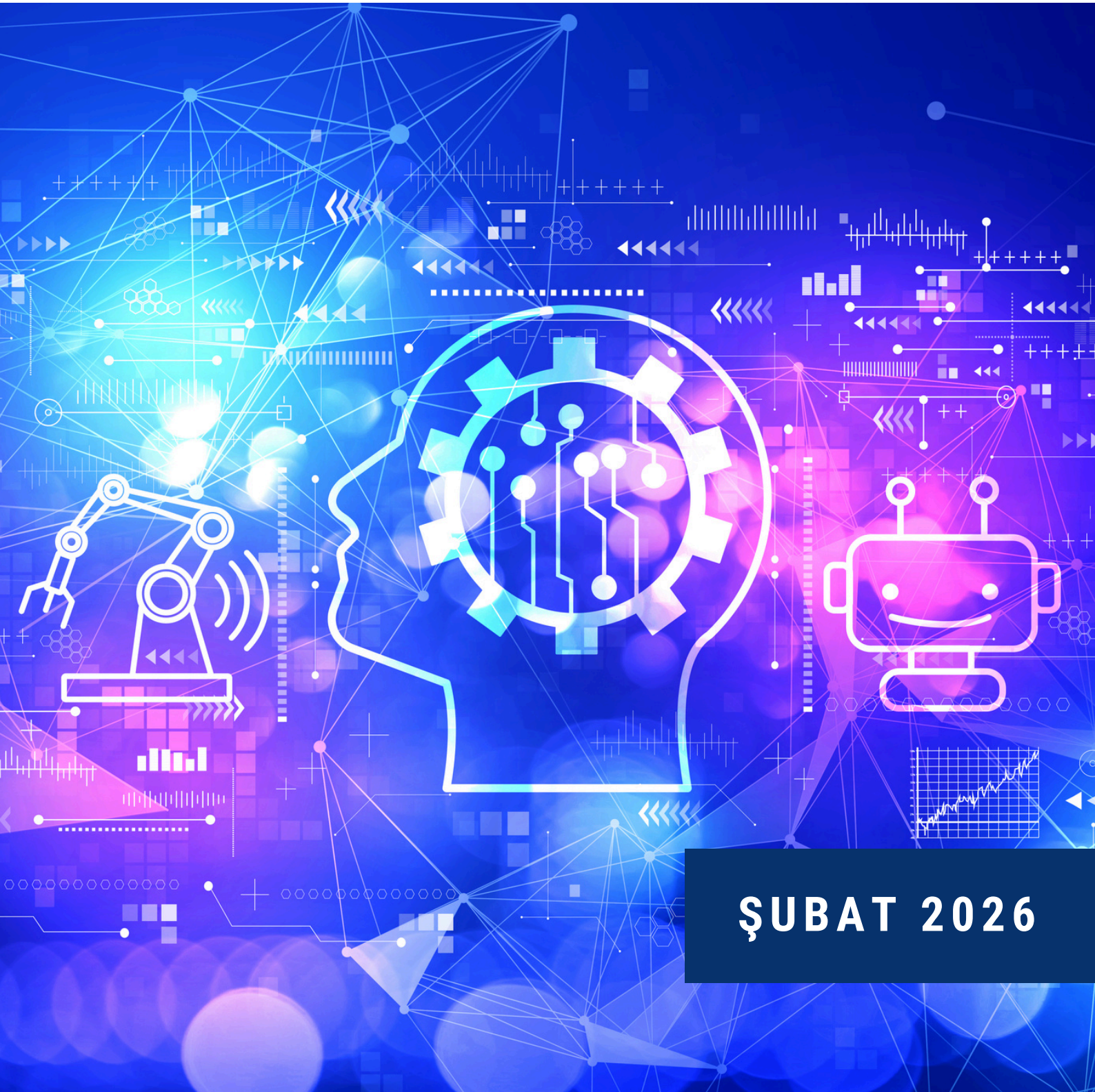
YAPAY ZEKÂ ÇAĞINDA HUKUK

İSTANBUL BAROSU
BİLİŞİM HUKUKU KOMİSYONU
YAPAY ZEKÂ ÇALIŞMA GRUBU



ŞUBAT 2026

BAŞLARKEN

Yapay zekâ teknolojileri, insanların hayatını kolaylaştırma, ekonomik büyümeyi destekleme, sağlık, refah, güvenlik ve mahremiyet konularındaki zorluklarla mücadele etme gibi pek çok hususta büyük bir potansiyele sahiptir. Bununla birlikte, yıkıcı birtakım teknolojiler gibi, yapay zekâ da bazı riskler taşıyabilir ve emek, güvenlik, mahremiyet, etik ve beceriler gibi çeşitli alanlarda karmaşık toplumsal zorluklara neden olabilir. Bu açıdan toplum üzerindeki tüm etkilerini içerir şekilde yapay zekâya kapsamlı ve bütünsel bir yaklaşım çok önemlidir.

İstanbul Barosu Bilişim Hukuku Komisyonu Yapay Zekâ Çalışma Grubu olarak gelişen yapay zekâ teknolojisinin toplumda, hukuk sisteminde ve mesleğimizde yarattığı etkiler konusunda harekete geçmenin bir gereklilik olduğunu düşünüyoruz. Buradan hareketle, diğer çalışmalarımız ve 2020 yılından bu yana her ay yayımladığımız bültenler ile gelişen teknolojilerin hukuki bakış açısıyla ele alınmasına yardımcı olmayı ve bu konuda farkındalığı arttırmayı hedefliyoruz. Çalışmalarımıza İstanbul Barosu internet sitesinden ulaşabilirsiniz.

BU SAYIDA

SİNGAPUR'UN AJAN YAPAY ZEKÂYA İLİŞKİN MODEL ÇERÇEVE YÖNERGESİ

Av. Sena VURAL AÇANAL

Singapur tarafından 22 Ocak 2026 tarihinde yayımlanan Model Yapay Zekâ Çerçeve Yönergesi ("**Yönerge**''), özellikle Ajan Yapay Zekâ ("**Ajan YZ**") sistemlerinin kullanımına ilişkin riskleri ve sorumluluk alanlarını ele almaktadır. Yönerge, yapay zekâ ("**YZ**'') sistemlerinin yalnızca öneri sunan araçlar olmaktan çıkıp doğrudan eylem gerçekleştirebilen yapılara dönüşmesi karşısında mevcut risk analizlerinin yeniden değerlendirilmesi gerektiğini ortaya koymaktadır.

Klasik Üretken **YZ**, özgülendiği alanda çıktılar veren **YZ** sistemidir. Örneğin ChatGPT, kullanıcı tarafından kendisine girilen komut doğrultusunda metinler üretir. **Ajan YZ** sistemleri ise Üretken **YZ** sistemlerinden farklı olarak plan yapmak, çok adımlı işlemler yapmak, ödeme yapmak veya veritabanına yazmak gibi çeşitli fonksiyonları yerine getirebilmektedir. Bunların yanı sıra başka ajan sistemlerle birlikte çalışmak ve kullanıcısının yerine eylem gerçekleştirmek gibi geniş kapsamlı görevleri de yerine getirebilmektedirler.

Bu yönüyle **Ajan YZ** sistemleri Üretken **YZ** sistemlerinden, öneri vermekle sınırlı kalmayıp icra edebilme kabiliyetine sahip olmasıyla ayrılmaktadır.

YZ sistemlerinin artık görüş bildirmenin ötesine geçip eylem alabiliyor olması karşısında klasik **YZ** sistemlerine özgü risk analizleri yetersiz kalmaktadır. Bu aşamadan sonra riziko ölçümleri, sistemlerin yalnızca hatalı çıktı üretme ihtimalinin ötesine geçmekte, doğrudan yapacakları işlemlerin yanlış olması, işlemlerde yetki aşımı problemlerinin meydana gelmesi veya zincirleme hatalara yol açılması ihtimallerini kapsayacak şekilde değerlendirilebilecektir. Bu itibarla **YZ** modellerinin kullanımından doğan risklerin yeniden tasarlanması güncel bir ihtiyaç olmaktadır.

Bir **Ajan YZ** sisteminin hatasının bir başka ajan sistemi tetikleyebilecek olması, küçük bir veri hatasının büyük bir operasyonel soruna dönüşebilecek olması gibi riskler söz konusu olduğundan,

Singapur'un 22 Ocak 2026 tarihinde yayımladığı **Yönerge**'de konunun ilk olarak risk analizi bakımından ele alınması gerektiği vurgulanmaktadır. Yönerge'ye göre kurumların **Ajan YZ** kullanmadan önce sistemin hangi alanda kullanılacağı, hassas veri ile çalışılıp çalışılmayacağı, **YZ** sisteminin bilgileri değiştirme yetkisinin olup olmadığı, eylem üzerinde insan onayı gerekip gerekmediği gibi konularda netlik sağlanması gerekmektedir.

Yönerge, risk sınırlandırmak için en etkin yöntem olarak **YZ** sistemlerinin yetki sınırlarının önceden belirlenmesi yöntemini benimsemiştir. Risk sınırlandırma yaklaşımı, riskin sonradan yönetilmek zorunda kalmadan en baştan daraltılmasını öngörmektedir. Buna göre **Ajan YZ** sistemlerinin hangi araçlara erişebileceği, hangi verileri dokümante edebileceği, hangi sistemlere erişim yetkisi olabileceği gibi sınırları önceden daraltılmış olmalıdır.

Yönerge, risk yönetimi bakımından insan sorumluluğunu da dikkate alan düzenlemeler içermektedir. Buna göre **Ajan YZ** sistemlerinin otonomi kabiliyeti, insanların hukuki ve kurumsal sorumluluğunu ortadan kaldırmamaktadır. **Yönerge**'de **Ajan YZ** kullanan kurumlarda kim veya kimlerin sorumluluk sahibi olacağının tespiti için kurum içerisinde bir görev dağılımı ve hesap verilebilirlik zincirinin kurulması önerilmekte, insan denetiminin her daim sağlanabilmesi mümkün olmasa da, yüksek riskli ve geri döndürülmesi mümkün olmayan işlemlerde onayının onayının zorunlu tutulması gerektiği vurgulanmaktadır. Örneğin veri silme, para transferi, hassas verilerin işlenmesi gibi işlemlerin **YZ** tarafından otomatize edilmememesi tavsiye edilmektedir. Bir kurumda **Ajan YZ** sistemleri kullanılırken, yazılımcı, model sağlayıcı, kurum yöneticisi, güvenlik takımı ve son kullanıcı gibi birçok aktörün sorumluluk zincirindeki yerinin belirlenmiş olması ve sistemin kullanım alanını belirleyen, teknik tasarımını yapan, test eden, onay veren, denetleyen kişilerin en baştan atanması Yönerge'de gereklilik olarak ifade edilmektedir.

YZ modelinin fiilen yürürlüğe konulması, kullanıma sunulması anlamına gelen "*Deploy evresi*" öncesinde teknik ve organizasyonel güvenlik önlemlerinin alınması için sistemin çok adımlı davranışları test edilmelidir. Deploy sonrasında anomali tespitinin yapılması ve gerekli görülmesi halinde sistemin devre dışı bırakılmasını sağlayacak mekanizmanın da kurgulanması gerekmektedir.

Yönerge'nin risk yönetimini ele aldığı son boyut, son kullanıcı sorumluluğudur. Buna göre son kullanıcı, bir **Ajan YZ** ile etkileşime girdiği konusunda açıkça bilgilendirilmelidir. Söz konusu bilgilendirme **Ajan YZ** sisteminin yetkilerinin neler olduğu, verileri nasıl işlediği konularında yeterli bilgi içermelidir ve bir insan muhatap alternatifi sunulmalıdır.

Bu ilkelerin benimsenmesi halinde şeffaflık ve aydınlatma yükümlülüğü dijital ortamda sağlanmış olacaktır.

Günden güne dijitalleşen dünyada **YZ** teknolojilerinin gelişim hızı ve insan yaşantısında ajan sistemlerin kullanımındaki artış karşısında Yönerge, risk noktasında doğrudan sorumluluğun kime ait olacağına dair kesin bir çözüm sunmamakla birlikte, temsil hukuku, kusur nitelendirmesi, illiyet bağı, veri sorumluluğu gibi konularda yeni tartışma alanları açması bakımından önem arzetmektedir.

Detaylı bilgi için:
https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf

AVRUPA KOMİSYONU'NDAN GROK VE X'E YENİ SORUŞTURMA

Av. Sevgi ÖZTÜRK

Avrupa Komisyonu *(European Commission)*, 25 Ocak 2026 tarihinde yayımladığı basın açıklaması ile Dijital Hizmetler Yasası (*Digital Services Act* – "**DSA**") kapsamında X platformu hakkında yeni bir resmî soruşturma başlatıldığını duyurmuştur. Soruşturmanın odağında, platforma entegre edilen Grok adlı üretken yapay zekâ ("**YZ**") sisteminin oluşturabileceği sistemik riskler yer almaktadır. Ayrıca Avrupa Komisyonu X'e karşı Aralık 2023'te başlattığı ve halen devam eden soruşturmasının kapsamını da genişletti.

DSA, 2022 yılında yürürlüğe giren ve Avrupa Birliği ("**AB**") genelinde dijital hizmet sağlayıcılarına kapsamlı yükümlülükler getiren bir düzenlemedir. Özellikle "Çok Büyük Çevrimiçi Platformlar" (*Very Large Online Platforms* – "**VLOP**") bakımından yalnızca içerik kaldırma yükümlülüğü öngörmemekte; aynı zamanda sistemik risklerin değerlendirilmesi ve azaltılmasına yönelik önleyici bir uyum modeli benimsemektedir.

Bu kapsamda **DSA** uyarınca **VLOP** statüsündeki platformlar; yasadışı içeriklerin yayılması, temel haklara yönelik riskler, demokratik süreçlerin manipülasyonu ve çocukların korunmasına ilişkin riskler bakımından risk değerlendirmesi yapmakla yükümlüdür. **DSA** ise, tespit edilen risklere karşı etkili, orantılı ve ölçülebilir azaltma önlemlerinin alınmasını zorunlu kılmaktadır. Bu yönüyle **DSA**, klasik içerik kaldırma modelinden farklı olarak, platformun bütüncül biçimde denetlenmesini amaçlamaktadır.

Komisyon tarafından yeni soruşturma, Grok adlı **YZ** sistemi tarafından üretilen cinsel içerikli görüntüler sonrasında başlatıldı. Soruşturma kapsamında, Grok'un X platformuna entegrasyonu sonrasında ortaya çıkabilecek risklerin yeterli şekilde analiz edilip edilmediği ve gerekli önlemlerin uygulanıp uygulanmadığı incelenmektedir. Özellikle **YZ** tarafından üretilen manipüle edilmiş içerikler, çocukları tasvir eden yasa dışı materyaller ve bu içeriklerin

platformun tavsiye algoritmaları aracılığıyla yayılımı soruşturma kapsamında değerlendirilmektedir. Bu bağlamda özellikle, **YZ** tarafından üretilen ve çocukların cinsel istismarına ilişkin materyal teşkil edebilecek içeriklerin platform aracılığıyla yayılması **DSA** kapsamında öngörülen sistemik risk değerlendirmesinin merkezinde yer almaktadır. Bu durum, üretken **YZ** sistemlerinin yalnızca içerik üretme aracı olarak değil, aynı zamanda platformda risk üretebilen unsurlar olduğunu da göstermektedir.

DSA'nın getirdiği sistemik risk yaklaşımı, reaktif içerik müdahalesinden ziyade önleyici risk yönetişimine dayalı bir uyum modeli ortaya koymaktadır. **DSA**, kullanıcıların çevrimiçi ortamdaki temel haklarını, özellikle ifade özgürlüğü ve mahremiyetini korumayı amaçlarken, aynı zamanda çocukların korunması ve demokratik süreçler bakımından platformlara yükümlülükler yüklemektedir.

Usul bakımından Avrupa Komisyonu, soruşturma kapsamında bilgi talep etme, yerinde inceleme gerçekleştirme ve geçici tedbir uygulama yetkisine sahiptir. İhlal tespiti halinde ise şirketin küresel yıllık cirosunun %6'sına kadar idari para cezası uygulanabilmekte; ayrıca belirli yükümlülüklerin yerine getirilmesine yönelik bağlayıcı kararlar alınabilmektedir.

Avrupa Komisyonu'nun kısa süre önce X şirketine **AB** yasalarını ihlal ettiği gerekçesiyle verdiği 120 milyon avro para cezası da **DSA** kapsamındaki yükümlülüklerin etkin olduğunu ve yaptırıma bağlanabilen bir denetim mekanizmasının işletildiğini göstermektedir.

X platformunun **VLOP** statüsü nedeniyle doğrudan Komisyon denetimine tabi olması, bu süreci daha da önemli kılmaktadır. Nitekim söz konusu soruşturma, **AB**'nin **YZ** entegrasyonlarını yalnızca teknik bir yenilik olarak değil; temel haklar, çocukların korunması ve demokratik düzen bakımından hukuki değerlendirme konusu olarak ele aldığını göstermektedir.

Sonuç olarak bu süreç, dijital platform sorumluluğunun kapsamının genişlediğine işaret etmektedir. **YZ** sistemlerinin de doğrudan hukuki denetim alanına dahil edildiği yeni bir etik platform sorumluluğu anlayışını ortaya koymaktadır.

Detaylı bilgi için:

https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203

https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

KALİFORNİYA EYALETİ'NDE AVUKATLIK VE TAHKİM MEVZUATI'NDA YAPAY ZEKÂ DEĞİŞİKLİKLERİ

Av. Ahmet Sadık HIDIR

Amerika Birleşik Devletleri'nin Kaliforniya Eyaleti Senatosu'ndan Ocak 2026 tarihinde geçen "**Senate Bill 574**" yasası Yapay Zekâ **("YZ")** kullanımına doğrudan standartlar getiren bir yasa niteliği taşımaktadır. Bu değişiklikle avukatlar ve hakemlerin uyması gereken yükümlülükler doğrudan yasal bir zemine oturtulmuştur. Buna göre eyaletteki avukatların, **YZ** kullanılarak üretilen tüm materyallerde birtakım yükümlülüklere uyması zorunlu hale gelmiştir.

Buna göre;

- Gizli, kişisel veya diğer kamuya açık olmayan bilgilerin, kamuya açık bir üretken YZ sistemine girilmemesi,
- Üretken **YZ**'nin herhangi bir sınıflandırma temelinde bireylere veya topluluklara karşı ayrımcılık yapmaması,
- Üretken **YZ** materyalinin doğruluğun teyit edilmesi,
- Önyargılı, saldırgan veya zararlı içeriklerin kullanılmaması,
- Hatalı ve yanıltıcı çıktıların düzeltilmesi,
- Mahkemeye sunulan dilekçenin, sorumlu avukatın doğrulamadığı hiçbir **YZ** alıntısını içermemesi gerektiği,

öngörülmüştür. Yasada üretken **YZ** kavramı, *"yapay zekâ sisteminin eğitim verilerinin yapısını ve özelliklerini taklit eden metin, görüntü, video ve ses dahil olmak üzere sentetik içerik üretebilen bir yapay zekâ sistemi"* şeklinde tanımlanmıştır. Kişisel tanımlayıcı bilgi ise *"sürücü belgesi numaraları, doğum tarihleri, sosyal güvenlik numaraları, ulusal suç bilgileri ve suçlu kimlik ve bilgi numaraları, tarafların, mağdurların, tanıkların ve mahkeme personelinin adresleri ve telefon numaraları, tıbbi veya psikiyatrik bilgiler, mali bilgiler, hesap numaraları veya mahkeme kararı ya da kanunla gizli sayılan diğer herhangi bir içerik"* olarak ifade edilmiştir.

Bunlara ilave olarak Kaliforniya Medeni Usul Kanunu'nda yapılan değişiklikle alternatif uyuşmazlık ve tahkim süreçleri bakımından şu hükümler öngörülmüştür:

- Bir hakemin karar alma sürecinin herhangi bir bölümünü herhangi bir üretken yapay zekâ aracına devredemeyeceği,
- Hakemlerin üretken **YZ** araçlarını kullanmalarının, olguların, hukukun ve delillerin bağımsız analizinin yerini alamayacağı,
- Bir hakemin, taraflara önceden uygun açıklamalar yapmadan **YZ** tarafından kayıt dışı olarak üretilen bilgilere dayanamayacağı,
- Üretken bir **YZ** aracının bağımsız olarak doğrulanabilen kaynakları gösteremediği takdirde bu tür kaynakların var olduğunun varsayılamayacağı,
- Hakemin karar alma sürecine yardımcı olmak için herhangi bir **YZ** aracını kullanmasına bakılmaksızın, kararın tüm yönlerinden hakemin sorumlu olacağı

belirtilmiştir.

Sonuç olarak, hassas müvekkil verilerinin genel kullanıma açık üretken **YZ** sistemlerine girilmesi kesin olarak yasaklanmaktadır. **YZ**'nin gerçekte var olmayan mahkeme kararları veya sahte içtihatlar (halüsinasyon) üretebilme riski nedeniyle bu konudaki doğrulama yükümlülüğü avukatlara yüklenmiştir.

Detaylı bilgi için:
https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB574

IPC VE OHRC YAPAY ZEKÂNIN SORUMLU KULLANIMINA İLİŞKİN PRENSİPLER

Ahmet KALINOĞLU

Kanada Ontario Bilgi ve Gizlilik Komiserliği Ofisi **("IPC")** ve Kanada Ontario İnsan Hakları Komisyonu **("OHRC")**, kamu sektörü tarafından sorumlu ve güvenilir yapay zekâ **("YZ")** benimsenmesinin önemini vurgulamaya devam ederek iki kurumun ortaklaşa birtakım prensipler geliştirmişlerdir. Bu prensipler, kuruluşların **YZ** sistemlerini gizlilik ve insan hakları yükümlülükleriyle tutarlı şekilde benimsemelerini ve değerlendirilmelerini sağlayacak temel unsurları belirlemektedir.

1. İlke: Geçerli ve Güvenilir

Bu ilke kapsamında **YZ** sistemlerinin, tasarlanma, kullanılma veya uygulanma amaçları için geçerli ve güvenilir çıktılar sergilemesi gerektiği vurgulanmaktadır. Bu ilke gereğince **YZ** sistemleri, belirli bir süre boyunca ve kullanılma amaçlarına yönelik tasarlandıkları süreçlerde bağımsız test standartlarını karşılamalı ve tutarlı performans gösterip güvenilir olduklarını objektif kanıtlarla kanıtlamalıdır. Ek olarak da **YZ**'nin yaşam döngüsü boyunca düzenli olarak değerlendirilmesi ve gerektiği gibi çalıştığından emin olunması gerektiği belirtilmiştir.

2. İlke: Güvenli

Bu ilke, **YZ**'nin insan haklarına, ayrımcılığa karşı korunma hakkına ve gizlilik hakkına ihlal teşkil edecek zararlarını veya istenmeyen zarar verici sonuçlarını önleyecek biçimde ve insanın yaşamını, fiziksel ve ruhsal sağlığını, ekonomik güvenliğini ve de çevreyi destekleyici şekilde geliştirilmesi, benimsenmesi, yönetilmesi ve **YZ**'nin tüm yaşam döngüsü boyunca izlenmesi gerektiğini ifade etmektedir. Bu ilke **YZ** sistemlerinin, güvensiz hale geldiklerinde duruma göre geçici veya kalıcı olarak kapatılması veya hizmet dışı bırakılması gerekliliğini de vurgulamaktadır.

3. İlke: Gizliliği Koruyucu

Bu ilke, **YZ** sistemlerinin geliştiricilerine, sağlayıcılarına veya kullanıcılarına proaktif önlem almaları gerektiğini ifade eder; kişisel bilgilerin gizliliğini ile güvenliğini korumanın

ve bilgiye erişme hakkının desteklenmesi gerektiğini vurgulamaktadır. Üçüncü ilke uyarınca gizliliğin daha iyi şekilde korunması amacıyla bireyler, kişisel bilgilerinin hangi amaçla ve ne şekilde işleneceği hakkında bilgilendirilmelidir ve diğer yandan da büyük miktarda kişisel bilgi ihtiyacı azaltılmalıdır. Son olarak da **YZ**'nin yaşam döngüsü boyunca kişisel bilgilerin yetkisiz erişimden veya kötüye kullanımdan korunmasın için güçlü güvenlik önlemlerinin şart olduğu vurgulanmaktadır.

4. İlke: İnsan Hakları ile Uyumluluk

İnsan haklarının devredilemez olduğunu ve **YZ** sistemlerinin/prosedürlerinin tasarımına da koruma mekanizmalarının entegre edilmesi gerektiğini vurgulayan dördüncü ilke, **YZ** sistemlerini kullanan kurumların, ayrımcılığı etkili şekilde önlemesi ve gidermesi ve de YZ'nin kullanılmasıyla elde edilen menfaatlerin evrensel ve ayrımcılıktan uzak olmasını sağlaması gerektiği belirtmektedir. Bu ilkeye göre kurumlar, tespit edilen önyargıları gidermek için eğitim setlerindeki verileri ayarlamalı ve veri kümelerindeki ayrımcı etkileri azaltmak için aktif önlemler almalıdır.

5. İlke: Şeffaf

Beşinci ilke uyarınca **YZ** sistemlerini geliştiren, sağlayan ve kullanan kurumlar, bu sistemlerinin başkaları için görünür, anlaşılabilir, izlenebilir ve açıklanabilir olmasını sağlamalıdır. Şeffaflık kavramının **YZ** sistemleri hakkında açıkça bildirim sağlamayı, nasıl çalıştığını görünür, açıklanabilir ve anlaşılabilir kılan uygulamalar benimsemeyi içerdiği vurgulanmıştır. Ayrıca şeffaflığın şu özelliklerden oluştuğu da belirtilmiştir: **YZ** sistemlerinin görünürlüğü, **YZ** sistemlerinin anlaşılabilirliği, **YZ** sistemlerinin açıklanabilirliği, **YZ** sistemlerinin izlenebilirliği.

6. İlke: Hesap Verebilirlik

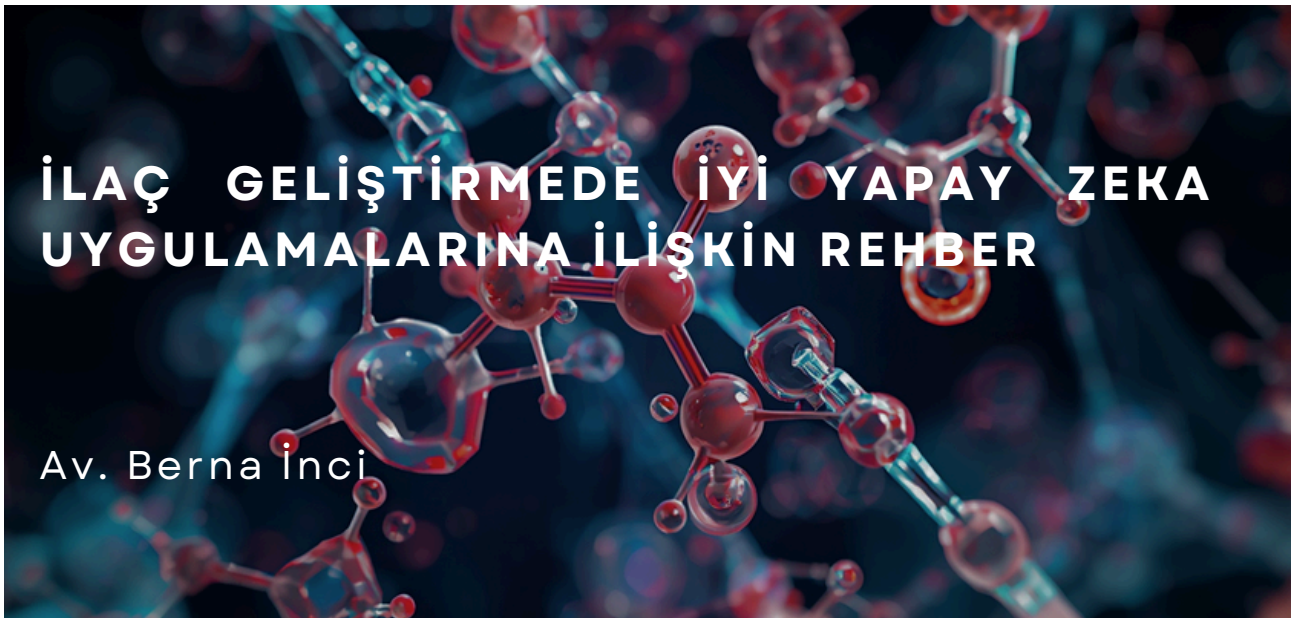
Bu ilke uyarınca kurumlar, **YZ** sistemlerinin tüm yaşam döngüsü boyunca hesap verebilirliğini sağlamak için insan müdahalesi yaklaşımını da içeren, açık bir şekilde tanımlanmış roller, sorumluluklar ve gözetim süreçlerine sahip bir iç yönetim yapısı uygulamalıdır. Aynı zamanda altıncı ilke, **YZ** sistemiyle ilişkili riskleri belirlemek ve değerlendirmek ve bu risklere karşı gerekli önlemleri geliştirmek için önceden risk değerlendirmelerinin yapılması gerektiğini vurgulamaktadır. Ek olarak bu ilke gereğince kurumlar, **YZ** sisteminin çalışma sürecine ilişkin bir belgeyi bağımsız denetim organına ve düzeltici veya iyileştirici eylemlerde bulunmaya hazır olmalıdır. Bunun yanı sıra kurumlar, bilgi edinme taleplerini veya **YZ** sisteminin karar alma sürecine ilişkin itirazları alabilecekleri ve tüm bunlara cevap verebilecekleri bir mekanizma oluşturmalıdır.

Sonuç olarak bu **IPC-OHRC** prensipleriyle, riski değerlendirmek, sistem tasarımını ve o sistemin dağıtımını yönlendirmek ve **YZ** yaşam döngüsü boyunca hesap verebilirliği için açık, güvenilir ve bir çerçeve sunmakta olduğu belirtilmektedir.

Bu ilkelerin uygulanmasının, **YZ** sistemlerinden etkilenen kişilerin haklarını korumasını sağlarken bir yandan da bu sistemlerin geliştirilmesi, sağlanması ve kullanımı boyunca sorumlu yeniliği teşvik ettiği vurgulanarak; kurumların bireyleri ve toplulukları potansiyel zararlardan etkili bir şekilde koruyabileceği, adalete olan bağlılıklarını gösterebileceği ve kamu güvenini artırabileceği söylenmektedir.

Detaylı bilgi için:

https://www3.ohrc.on.ca/en/principles-responsible-use-artificial-intelligence



İLAÇ GELİŞTİRMEDE İYİ YAPAY ZEKA UYGULAMALARINA İLİŞKİN REHBER

Av. Berna İnci

Avrupa İlaç Ajansı (*European Medicines Agency*) (“**EMA**”) ve Amerika Birleşik Devletleri İlaç İdaresi (F*ood and Drug Administration*) (“**FDA**”) tarafından Ocak 2026 ‘da “İlaç Geliştirmede İyi Yapay Zekâ Uygulamalarına İlişkin Rehber” (“**Rehber**”) ile temel ilkeler yayımlanmıştır. Hazırlanan bu **Rehber**’de ilaç ürünlerinin döngülerinin tüm aşamaları da dahil olmak üzere (klinik öncesi, klinik süreci, pazarlama ve üretim) analiz yapma veya kanıt oluşturma amaçlı kullanılan yapay zekâ (“**YZ**”) sistemlerinin geliştirilmesi ve uygulamasına yönelik hukuki ve teknik çerçeve belirlenmiştir. **Rehber** içerisinde kullanılan “ilaç” terimi ilgili yasal düzenlemelerde tanımlanan ilaçlar ile biyolojik ürünleri kapsamakta iken **YZ** ise ilaçların döngüsü boyunca veri işleyen ve üreten sistem düzeyindeki teknolojilerdir. Günümüzde gelişen teknolojiler ile ilaç ürünlerinin döngüsü boyunca **YZ** kullanımı giderek artmıştır. **YZ** de dahil olmak üzere yeni teknolojilerin ortaya çıkması ve gelişmesi ile birlikte ilaçların döngü safhalarında kullanılan bu sistemlerin hasta yararı ve güvenliği gerekliliklerini sağlamasının önemi de artmaktadır. Ayrıca bu teknolojilerin geliştirilmesi ve yaygınlaştırılması ile ilaç geliştirmede inovasyonu teşvik eden, ilacın pazara sunulma süresini kısaltan, farmakovijilansı[1] güçlendiren , insanlardaki toksisite ile ilacın etkililik tahminini iyileştiren ve hayvan deneylerine olan bağımlılığı azaltabilecek çok yönlü yaklaşımların desteklenmesi beklenmektedir.

İlaç geliştirmedeki **YZ** kullanımı arttıkça iyi uygulamaların ve fikir birliği standartlarının geliştirilmesi de daha bir önemli hale gelmiştir. Hazırlanan bu **Rehber** ile uluslararası düzenleyiciler ve standart kuruluşları ile diğer iş birlikçilerin ilaç geliştirmedeki iyi uygulamaları ilerletmek için çalışabilecekleri alanlar tanımlanmıştır. **Rehber**’de tanımlanan iş birliği alanları arasında; araştırma, eğitim araçları ve kaynakları oluşturma ile uluslararası uyumlaştırma yer almaktadır.

Ayrıca bu iş birliği alanları ilgili yasal düzenleyici çerçevelere uygun olarak farklı yargı bölgelerindeki düzenleyici politikaları ve kılavuzları oluşturmaya da yardımcı olabilecektir. Başlangıç niteliğinde olan bu ortak çalışma daha geniş kapsamlı uluslararası etkileşimlere de zemin hazırlayabilecek niteliktedir.

Rehber'de bahsedilen temel ilkeler ise şu şekildedir;

1. *İnsan Odaklı Tasarım*: **YZ** teknolojilerinin geliştirilmesi ve kullanımı etik ve insan odaklı değerler ile uyumlu olmalıdır.
2. *Risk Temelli Yaklaşım*: **YZ** teknolojilerinin geliştirilmesi ve kullanımı; kullanım bağlamına ve belirlenen model riskine dayalı olarak orantılı doğrulama, risk azaltma ve gözetim içeren risk temelli bir yaklaşımı takip etmelidir.
3. *Standarda Bağlılık:* **YZ** teknolojileri; "İyi Uygulamalar, GxP (Good Practice)"[2] de dahil olmak üzere ilgili yasal, teknik, bilimsel, siber güvenlik ve düzenleyici standartlara bağlı kalmalıdır.
4. *Net Kullanım Bağlamı*:**YZ** teknolojilerinin iyi tanımlanmış bir kullanım bağı olmalıdır. İyi tanımlanmış kullanım bağı ise bu sistemlerin neden kullanıldığına dair rolü ve kapsamı tanımlamaktadır.
5. *Multidisipliner Uzmanlık:* Hem **YZ** teknolojisini hem de kullanım bağlamını kapsayan multidisipliner uzmanlık bu teknolojilerin kullanımı boyunca entegre edilmelidir.
6. *Veri Yönetişimi ve Dokümantasyonu:* Veri kaynaklarının kökeni, veri işleme adımları ve analitik kararlarlar "İyi Uygulamalar" gerekliliklerine uygun olarak ayrıntılı, izlenebilir ve doğrulanabilir şekilde belgelenmelidir. Hassas nitelikli veriler için bu teknolojilerin kullanımı boyunca veri gizliliği ve veri koruma da dahil olmak üzere uygun veri yönetişimi sürdürülmelidir.
7. *Model Tasarımı ve Geliştirme Uygulamaları:* **YZ** teknolojilerinin geliştirilmesi, model ve sistem tasarımlarında yazılım mühendisliğindeki en iyi uygulamalar takip edilerek; yorumlanabilir, açıklanabilir ve tahmin performansı kullanıma en uygun verilerinden yararlanılmalıdır. İyi modeller ve sistemlerin geliştirilmesi hasta güvenliğine katkıda bulunan şeffaflığı, güvenilirliği, genellenebilirliği ve dayanıklılığı teşvik etmelidir.
8. *Risk Temelli Performans Değerlendirmesi:* Uygun şekilde tasarlanmış test ve değerlendirme yöntemleri aracılığıyla tahmin performansının doğrulanmasını destekleyen ayrıca hedeflenen kullanım bağlamına uygun veriler ve ölçütler kullanılarak insan ve **YZ** etkileşimleri de dahil olmak üzere tüm sistem değerlendirilmelidir.

9. *Yaşam Döngüsü Yönetimi:* **YZ** teknolojilerinin yeterli performansı sağlayabilmesi için periyodik yeniden değerlendirmelere tabi tutulmalı, kullanılan **YZ** teknolojilerine risk temelli kalite yönetim sistemleri uygulanmalıdır.
10. *Net ve Temel Bilgiler:* Kullanıcılar ve hastalar da dahil olmak üzere kullanılan **YZ** teknolojilerinin kullanım bağlamı, performansı, kısıtlamaları, temel verileri, güncellemeleri açıklanmalıdır. Ek olarak yorumlanabilirlik ve açıklanabilirlik hakkında da net, anlaşılabilir ve erişilebilir bilgiler yalın bir dil ile sunulmalıdır.

Detaylı bilgi için:
https://www.ema.europa.eu/en/documents/other/guiding-principles-good-ai-practice-drug-development_en.pdf

https://www.who.int/teams/regulation-prequalification/regulation-and-safety/pharmacovigilance#:~:text=Farmakovijilans%20(PV)%2C%20ila%C3%A7%20yan%20etkilerinin%20veya%20ila%C3%A7la,%C3%B6nlenmesiyle%20ilgili%20bilim%20ve%20faaliyetler%20olarak%20tan%C4%B1mlan%C4%B1r

https://www.pharmaguideline.com/2017/01/concept-of-gxp-in-pharmaceuticals.html#gsc.tab=0

[1]Farmakovijilans; ilaç ve aşı ile ilgili olumsuz etkilerin veya diğer sorunların tespiti, değerlendirilmesi, anlaşılması ve önlenmesi ile ilgili bilim ve faaliyetlerdir.
[2]Ürün ve hizmetlerin güvenli olmasını sağlamaya yardımcı GCP,GDP vb. kılavuzları ifade etmektedir.

AB VERİ YASASI SSS DOKÜMANINDAKİ GÜNCELLEMELER (OCAK 2026 -VERSIYON 1.4.)

Av. Öykü Dalgıç VOLKAN

Avrupa Komisyonu, 12 Eylül 2025 tarihinde yürürlüğe giren AB Veri Yasası'nın (*Tüzük (EU) 2023/2584*) uygulamasına açıklık getirmek amacıyla hazırladığı "Sıkça Sorulan Sorular" (**"SSS"**) dokümanını 22 Ocak 2026 tarihinde güncellemiştir. Söz konusu güncelleme, özellikle veri paylaşımı, bağlı ürünler ve birlikte işlerlik konularında önemli açıklamalar içermektedir.

Dijital Tek Pazar (**"DTM"**), Avrupa Birliği'nin (**"AB"**) tek pazar programının önemli bir bileşenidir. AB'nin tek pazarı dijital çağa uyarlamaya çalışırken merkeze aldığı en önemli kavramlardan biri 'veri' kavramıdır. AB Veri Yasası ("**Yasa**''), **DTM** düzenlemelerinin bir parçası olarak veri ekonomisi sektöründe üretilen değerin sektör oyuncuları arasında adil şekilde paylaşımını sağlamaktadır. Verilere erişim için standart kurallar ortaya koymakta bu şekilde verinin kullanılabilirliğini artırarak **AB**'nin veri ekonomisini güçlendirmeyi ve bu alanda rekabetçi bir pazar oluşturmayı amaçlamaktadır.

Yasa, temelde **AB** veri ekonomisi içinde kimlerin, hangi veriyi, nasıl koşullarda kullanabileceğine dair net kurallar belirlemektedir. Ancak söz konusu kuralların nasıl yorumlanacağı ve hayata geçirileceği ayrıca açıklığa kavuşturulması gereken hususlardandır. Bu çerçevede, **Yasa**'nın paydaşlar açısından pratikteki uygulamasına yardımcı olmak amacıyla oluşturulan **SSS** dokümanı güncellenmiş, yeni versiyonu yayımlanmıştır. **SSS** dokümanı bir önceki versiyonda olduğu gibi; (i) Yasa'nın diğer AB yasaları ile etkileşimi; (ii) Nesnelerin interneti bağlamında verilere erişim ve verilerin kullanımı; (iii) Yasa kapsamına giren veri türleri; (iv) "Kullanıcı"; (v) "Veri Sahibi" ve (vi) "Üçüncü Taraf"'lara ilişkin açıklamalar; (vii) Adil, makul ve ayrımcı olmayan koşullar, tazminat ve uyuşmazlıkların çözümü; (viii) İşletmeler arası veri paylaşımı sözleşmelerinde adaletsizlik; (ix) İşletmelerden-kamu kurumlarına veri erişimi; (x) Veri işleme servisleri arasında geçiş kuralları;

(xii) Üçüncü ülke makamları tarafından AB'de tutulan kişisel olmayan verilere yasadışı erişim ve aktarım (xiii) Birlikte işlerlik; (xiv) Yaptırım ve (xv) Sonraki adımlar ve Gelecekteki eylemler başlıklarından oluşmaktadır.

Bir önceki versiyon ile yeni versiyon arasındaki farklılıklara değinmek gerekirse; güncellenen **SSS** dokümanında dikkat çeken değişikliklerden biri, ham/önceden işlenmiş veriler ile çıkarılan/türetilen veriler arasındaki ayrıma ilişkindir. Önceki versiyonda yer alan ham/ önceden işlenmiş veriler ile çıkarılan/türetilen verilerin kapsam dışında kalmasına ilişkin gerekçeyi açıklayan ifade yeni versiyonda kaldırılmış, yalnızca ham/önceden işlenmiş veriler ile çıkarılan/türetilen verileri ayırt etmeye dair **Yasa**'nın ilgili gerekçesine atıf yapmakla yetinilmiştir. Bu ayrım, Yasa altında düzenlenen işletmeler (B2B) arası ve işletmeler ile tüketiciler (B2C) arasındaki veri paylaşımı açısından önem taşımaktadır. Zira **Yasa**, bağlı bir ürünün kullanımından elde edilen ve veri sahibinin kolayca erişebileceği tüm ham ve önceden işlenmiş verilere uygulanmaktadır. Bu veriler meta veriler de dahil olmak üzere hem kişisel hem de kişisel olmayan verileri kapsamaktadır. Buna karşılık, çıkarılan veya türetilen veriler açıkça kapsam dışında bırakılmıştır.

Bağlı ürünlere ilişkin açıklamalar da güncellemede önemli yer tutmaktadır. **SSS** dokümanı 'bağlı ürün' tanımına odaklanmakta ve 'bağlı ürünler': akıllı ev aletleri, tüketici elektroniği, endüstriyel makineler, tıbbi cihazlar, akıllı telefonlar ve televizyonlar olarak örneklenmektedir.
Bununla birlikte bağlı ürünlerin **Yasa** kapsamına girmesi noktasında hangi durumların belirleyici olacağı ortaya koyulmaktadır. Buna göre bir bağlı ürünün, 'birlik piyasasına sürülmüş' ise Yasa kapsamına gireceği; 'piyasaya sunmanın' ise üretim aşamasından sonra iki ekonomik aktör arasında gerçekleşen mülkiyet hakkının devri ile ilgili olduğu açıklanmaktadır. Bu noktada **SSS**'in yeni versiyonunda bir ürünün **AB'**de piyasaya sürüldüğünün ne zaman kabul edildiğini açıklığa kavuşturmak için yeni bir örnek eklenmiştir. Bu yeni örnek, **AB**'ye getirilen bir ürünün ancak serbest dolaşıma sunulduğunda piyasaya sürüldüğünün kabul edileceğini belirtmektedir. Avrupa Komisyonu'na göre, bu açıklamanın özellikle deniz taşıtları gibi ürünler açısından önemli olduğu anlaşılmaktadır.

Bir diğer önemli güncelleme, birlikte işlerlik konusuna ilişkindir. **SSS** yeni versiyonda; birlikte işlerlik deposunun çevrimiçi ve sürekli güncellenebilecek bir platform formatında olması ve bu depo aracılığı ile hizmet sağlayıcıların sundukları hizmet türüne hangi uyumlaştırılmış standartların veya ortak şartnamelerin uygulandığını görebilecekleri bir 'tek durak noktası' oluşturulması; bu şekilde bulut bilişim hizmetlerinin birlikte işler/çalışabilir olması ve müşterilerin işlevselliklerini kaybetmeden hizmet geçişlerini gerçekleştirebilmeleri hedeflenmiştir.

Bu bağlamda, yeni versiyonda sağlayıcıların müşterilere erişilebilir hale getirdikleri arayüzlerin, birlikte işlerlik deposunda belirtilen standartlarla uyumlu olmasını sağlamaları gerektiği açıkça belirtilmektedir.

Son olarak Komisyon, veri paylaşımı için Model Sözleşme Şartları (MCT) ile bulut bilişim sözleşmeleri için Standart Sözleşme Maddeleri (SCC) taslaklarını yayımlamıştır. Bu metinlerin bağlayıcı olmadığı ve taraflarca değiştirilebileceği belirtilmektedir. Bu yönüyle söz konusu sözleşme şartları, Genel Veri Koruma Tüzüğü (“**GDPR**”) kapsamındaki standart sözleşme maddelerinden ayrışmaktadır.

Sonuç olarak yapılan bu güncelleme ile **SSS** dokümanının, Avrupa Komisyonu tarafından gerektiğinde güncellenecek bir ‘canlı belge’ olması amaçlanmıştır. Bu bağlamda, Yasa’nın bölgesel kapsamının yalnızca **AB** ile sınırlı olmaması ve kuruldukları yerden bağımsız şekilde **AB**’ye ürün ve servis sunan bağlı ürün üreticileri, ilgili hizmet sağlayıcıları, veri sahipleri ve veri işleme servis sağlayıcıları gibi paydaşların da **Yasa**’nın bölgesel uygulaması kapsamında olmaları sebebiyle **SSS** dokümanına ilişkin güncellemeleri yakından takip etmelerinin önem arz ettiği değerlendirilmektedir.

Detaylı bilgi için:
https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act

https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en

19 Şubat 2026

İstanbul Barosu, Bilişim Hukuku Komisyonu, Yapay Zekâ Çalışma Grubumuz tarafından hazırlanan Yapay Zekâ Çağında Hukuk Bültenimizin Aralık 2025 sayısı İstanbul Barosu internet sitesinde yayımlandı.

Bültene erişim için:

https://www.istanbulbarosu.org.tr/files/komisyonlar/yzcg/2025aralikbulten.pdf

04 Şubat 2026

İstanbul Barosu, Bilişim Hukuku Komisyonu, Yapay Zekâ Çalışma Grubumuz tarafından hazırlanan "Yapay Zeka Yönetişiminde ABD, AB ve Çin Modelleri" adlı blog yazısı İstanbul Barosu internet sitesinde yayımlandı.

Blog yazısına erişim için:

https://istanbulbarosu.org.tr/yayinlar/kamuya-yansiyan-hukuki-surecler-isiginda-buyuk-dil-modeli-sohbet-robotlarinda-guvenilirlik

19 Şubat 2026

İstanbul Barosu, Bilişim Hukuku Komisyonu, Yapay Zekâ Çalışma Grubumuz tarafından hazırlanan "Kamuya Yansıyan Hukuki Süreçler Işığında Büyük Dil Modeli Sohbet Robotlarında Güvenilirlik" adlı blog yazısı İstanbul Barosu internet sitesinde yayımlandı.

Blog yazısına erişim için:

https://istanbulbarosu.org.tr/yayinlar/kamuya-yansiyan-hukuki-surecler-isiginda-buyuk-dil-modeli-sohbet-robotlarinda-guvenilirlik

BİLİŞİM HUKUKU KOMİSYONU

YAPAY ZEKÂ ÇALIŞMA GRUBU

HAZIRLAYAN BÜLTEN EKİBİ

Av. Necati Alp ÇELEBİ
Av. Berke Celil AKTAŞ
Av. Berna İNCİ
Av. Perin Selin BIYIKLIOĞLU ÖZKAZANÇ

BÜLTEN EDİTÖR EKİBİ

Av. Nazlı ÖZKUL
Av. Elif TANYERİ
Av. Tuğberk AYDEMİR