

Yapay Zeka ve Kişisel Veriler

25 May 2023

Genel Veri Koruma Yönetmeliği, Kişisel Verileri Yapay Zekaya Karşı Korur mu?

Yapay Zeka ("YZ"), kişisel verilerin analiz edilmesi, insan davranışlarının tahmin edilmesi ve insana ihtiyaç olmaksızın saptamalar ya da hesaplamalar yapılması amacıyla kullanılan çerçevesinde devrim yaratmış ve verinin günümüzdeki önemini perçinlemiştir. YZ, duygulara yer vermeden karmaşık durumlarda karar verme süreçlerini otomatikleştirme yeteneğine ile donatılmış olup; insanlara nazaran çoğu zaman daha doğru ve tarafsız kararlar verme imkanına sahiptir. Diğer taraftan algoritmik kararlar yine de YZ'nin beslendiği data gerekçesi ile hata veya önyargı içerebilmekte bu nedenle de sürekli gözetim ve denetim altındaki bireyler üzerinde olumsuz etkilere yol açabilmektedir. Tüm bunlara karşın, YZ'nin artan kullanımı ve ekonomiye katkısı yadsınamaz bir gerçektir. Son yıllarda, hükümetler YZ'ye yatırım yapmakta ve kullanımı teşvik etmek için politikalar oluşturmaktadır.

YZ kullanımı ile ilgili endişeler, öncelikle kişisel verilerin kullanımdan kaynaklanan temel hak ve özgürlüklerin potansiyel ihlallerine odaklanmıştır. Bu doğrultuda, YZ kullanımıyla kişisel verilerin korunması ve gizlilik konuları, veri koruma yetkilileri tarafından mercek altına alınmıştır. Özellikle ChatGPT olarak bilinen gelişmiş sohbet robotunun güncellenmesi versiyonunun piyasaya sürülmesiyle birlikte, YZ ve kişisel verilerle ilgili tartışmalar ivme kazanmıştır. Nitekim örneğin, ChatGPT'nin kullanımıyla tepki göstermiş ve İtalyan Veri Koruma Otoritesi'nin ("Garante") kararıyla ChatGPT'yi 13 yaşın altındaki çocuklar için engelleyen ilk ülke olmuştur. ChatGPT'den önce, Clearview AI gibi farklı YZ tabanlı yazılımlar için veri koruma otoriteleri tarafından verilen kararlara rastlamak da mümkündür. Clearview AI için Birleşik Krallık Veri Koruma Otoritesi ("ICO") bir soruşturma başlatmış ve küresel çapta yüz tanıma veritabanı oluşturmak için çevrimiçi kaynaklardan görüntü toplaması sebebiyle 7.552.800 £ idari para cezası uygulamıştır. ICO'nun yanı sıra, Garante ve Yunan Veri Koruma Otoritesi de idari para cezaları uygulamaya karar vermiş ve Clearview AI'nın AB'de biyometrik veri işlemlerini yasaklamıştır. Yine aynı konuda, Fransız Veri Otoritesi tarafından alınan kararda da benzer yaptırımlara hükmedilmiştir.

Bu makale kapsamında, özellikle Türkiye ve Avrupa Birliği ("AB") çerçevesinde YZ düzenlemeleri bağlamında kişisel veri ve gizlilik konularına odaklanılmıştır.

YZ nedir? Makine Öğrenmesi ve Derin Öğrenme arasındaki farklar nelerdir?

YZ, bilgisayar sistemlerinin öğrenme, akıl yürütme ve kendi kendini düzeltme gibi insan bilişsel yeteneklerini taklit etme özelliklerini ifade etmektedir. YZ sayesinde bilgisayarlar artık konu tanıma, doğal dil işleme, bilgisayar görüşü, makine öğrenimi ve robotik gibi insan zekası gerektiren görevleri yerine getirebilmektedir. Sadece hizmetlerinin iyileştirilmesinden üretim ve lojistikte verimliliğin artırılması ve daha kişiselleştirilmiş ve verimli hizmetler sunulması kadar potansiyel YZ uygulamaları mevcuttur. YZ, bilgisayarların verilerden öğrenmesini, kalıpları tanıması ve bu verilere dayanarak tahminler veya kararlar alması sağlayan gelişmiş algoritmalar, makine öğrenimi ve sinir ağıları kullanmaktadır. Makine öğrenimi ("MÖ") ve derin öğrenme ("DÖ") YZ'nin iki temel alt alanı olarak kabul edilmekte ve her ikisi de verilere dayalı olarak tahminde bulunma ve karar alma mekanizmalarıyla daha doğru çalışması amacıyla algoritmaların eğitilmesini sağlamaktadır. MÖ algoritmaları açıkça programlanmadan verilerdeki örüntüleri öğrenirken, DÖ çok katmanlı derin sinir ağıları ile eğitimi içeren daha karmaşık bir alt alandır. MÖ ve DÖ arasındaki temel farklar, öğrenilebilecek modellerin karmaşıklığı ve ölçeğidir. MÖ algoritmaları genellikle daha basittir ve derin öğrenme algoritmalarına göre daha az hesaplama yeteneği gerektirir; fakat karmaşık görevlerin üstesinden gelmede o kadar etkili olmayabilir.

YZ, gerçe?e yak?n sonuçlar elde etmek için do?ru, güncel ve eksiksiz verilere ihtiyaç duymakta ve verilerin miktar? ve kalitesi YZ'nin etkinli?inde çok önemli bir rol oynamaktadır. Bununla birlikte, çe?itli kaynaklardan verinin beslenmesi ve veri miktar?ndaki art??, bireyler için öngörüleemeyen sonuçlara yol açabilecektir. Öte yandan, eksik veya yanlış veriler de bireyler için istenmeyen sonuçlar doğurabilecektir. Sonuç olarak, veri koruma düzenlemeleri YZ geli?iminde giderek artan bir endi?e haline gelmi?; ve veri koruma düzenlemelerine uyum, hem gündemi hem de idari makamlar? oldukça me?gul etmeye başlamış?tır.

Dünya'da YZ Düzenlemeleri

Dünya çap?nda hükümetler, YZ'nin risklerini ve zorluklar?n? ele almanın yanı sıra geli?imini ve kullan?m?n? teşvik etmek için YZ ile ilgili mevzuat ve düzenlemeler üzerinde yoğun bir ?ekilde çalış?maktadı?r. Birçok ülkede görüldü?ü üzere, YZ ara?t?rmas? ve geli?tirmesi için fon sağlamay?, endüstri standartlar?n? geli?tirmeyi ve YZ'nin özellikle kamusal alanda kullan?lması da dahil olmak üzere tüm alanlarda kullan?m?n? teşvik etmeyi içeren kapsamlı YZ stratejileri geli?tirilmektedir. YZ alan?nda düzenlemeler ve yat?r?mlar olu?turan ve Türkiye'nin de kendi stratejilerine yön verirken yak?ndan takip etti?i ülkelerden bazıları? aşağıdaki tabloda yer almaktadır.

Ülke	YZ Mevzuatına Yönelik Atılan Önemli Adımlar
Amerika Birleşik Devletleri ("ABD")	ABD, henüz YZ ile ilgili kapsamlı bir federal düzenlemeyi y koymamakla birlikte; ABD Kongresi'nde YZ ile ilgili birkaç yasa sunulmuştur. Buna ek olarak, birçok eyalet, YZ'nin kamu uygulamalarda kullanımıyla ilgili yasalar çıkarmıştır (bkz. Algoritmik Veribilirlik Yasası, Ulusal YZ Girişimi Yasası, Otomatik Karar Sistemleri Hesap Veribilirlik Yasası, Tüketici Gizliliği Yasası, Adil Kredi Raporlama Yasası).
Çin	Çin, 2017 yılında, 2030 yılına kadar YZ alanında küresel bir liderliğini hedefini belirlemiştir. O zamandan bu yana, araştırma ve geliştirme yatırım yapmayı, endüstri standartları oluşturmayı ve YZ'nin kamu sektörlerinde kullanımını teşvik etmeyi içeren kapsamlı bir YZ strateji geliştirmiştir.
Güney Kore	Güney Kore, 2020 yılında, 2025 yılına kadar sağlık hizmetleri, akıllı şehirler ve diğer ilgili uygulamalara odaklanarak YZ araştırılması ve geliştirilmesi için 1 milyar \$ yatırım yapma planını açıklamıştır.
Japonya	Japonya, insan ihtiyaçlarına daha fazla odaklanan bir toplum olarak, amaçlarıyla YZ ve diğer gelişmekte olan teknolojilerin büyümesini teşvik etmeyi hedeflediği Toplum 5.0 girişimini başlatmıştır.
Kanada	Kanada hükümeti tarafından duyurulan Pan-Kanada YZ Strateji, araştırma ve geliştirme fonlarını içermekte olup, YZ uzmanları geliştirmesine ve YZ için etik ve yasal yapıların oluşturulmasına odaklanmıştır.

Avrupa Birliği YZ Mevzuatı

AB, son yıllarda YZ için yasal düzenlemeler ve kılavuzlar geliştirme ve çalışmalar yürütme konusunda oldukça ön planda yer almaktadır. Uzun bir süre önce taslak olarak Avrupa Komisyonu'na ("**Komisyon**") önerilen YZ Yasası, kişisel veri ve gizlilik konularını düzenleyen Genel Veri Koruma Tüzüğü ("**GDPR**") ile uyumlu olmadıkları için bazı

tartışmalara neden olsa da 11 Mayıs 2023 tarihinde Komisyon tarafından onaylanmıştır. AB'deki YZ kapsamında gelişmeleri gösteren zaman çizelgesi aşağıda yer almaktadır.



YZ Yasası ile GDPR arasındaki Çelişkiler

Komisyon, Nisan 2021'de AB'de YZ'nin geliştirilmesi ve kullanılmasıyla ilgili kapsamlı yasal çerçeve oluşturmayı amaçlayan YZ Yasası'nı önermiştir. YZ Yasası'nın ana odak noktası, YZ teknolojisinin etik ve sorumlu bir şekilde kullanılması ve düzenleme, kullanıcının veya geliştiricinin nerede

bulundu?una bak?lmaks?z?n, AB'de geli?tirilen, konu?land?r?lan veya kullan?lan tüm YZ sistemleri için uygulanmaktadır. Chatbotlar ve ki?isel asistanlar gibi gerçek ki?ilerle etkile?ime giren YZ sistemlerinin yan? s?ra kritik altyap?da kullan?lanlar di?er YZ sistemlerini de kapsamaktadır. GDPR, YZ teknolojisinin henüz bugünkü geli?im seviyesinde olmad??? bir zamanda haz?rlanm???tır. O zamanki teknolojiyle uyumlu olacak ?ekilde tasarlanan GDPR kar??s?nda; giderek büyüyen ve geli?en YZ'ye ili?kin olarak haz?rlanan YZ Yasas?'n?n uyumlulu?u noktas?nda endi?eler ortaya ç?km???tır. GDPR, YZ sistemlerini içerenler de dahil olmak üzere AB'deki her türlü veri i?leme faaliyetini kapsayan kapsamlı bir veri koruma düzenlemesi olarak uygulanmaktadır. Bu do?rultuda, her iki düzenleme birbirini tamamlay?c? nitelikte olup; AB'deki YZ sistemleri için geçerli olacaktır.

Yüksek Riskli YZ Sistemleri: YZ Yasas?, yüksek riskli YZ sistemlerini tanımlamakta ve sistem geli?tiricilerin risk de?erlendirmeleri yapmalar?n?, güvenlik önlemlerini uygulamalar?n? ve kullan?c?lara aç?klay?c? belgeler sa?lamalar?n? öngörmektedir. Temel hak ve özgürlükleri tehdit eden belirli YZ kullan?mlar? yasaklanm???tır. ??bu düzenlemeler, ki?isel verileri i?leyen yüksek riskli YZ sistemleri için GDPR uyumlulu?unu etkilemektedir. Yüksek riskli YZ uygulamalar? kullan?ma sunulmadan önce ?effaflık, izlenebilirlik ve insan gözetimi için titiz bir de?erlendirme yapılması?n? gerektirmektedir. Bununla birlikte, GDPR kapsam?nda, YZ Yasas? taraf?ndan yüksek riskli YZ kullan?m? ve bunlar?n uygulanması?na ili?kin öngörülen s?n?rlamalar konusunda belirsizlikler bulunmaktadır. Bu sebeple, YZ Yasas? taraf?ndan getirilen düzenlemelerin GDPR çerçevesinde nasıl uygulanabilece?ine ili?kin soru i?aretleri olu?muştur. Örne?in;

- YZ Yasas? madde 12 uyar?nca, yüksek riskli YZ sistemlerinin olaylar?n otomatik olarak kaydedilmesini ('loglar') sa?layacak ?ekilde tasarlanması? ve geli?tirilmesini düzenlemektedir; ancak bu, GDPR uyar?nca bilgilendirme yükümlülü?ü yerine getirilmeden ki?isel verilerin muhafaza edilmesine neden olabilecektir.
- YZ Yasas? madde 61'de düzenlenen pazar sonrası izleme için getirilen uyum kuralları, GDPR'nin veri minimizasyonu ve aktar?m gerekliliklerinin ihlal edilmesi ve söz konusu bu durumda da GDPR'ye uygun bir ?ekilde ilgili ki?idenden r?za alma ve silme hakk?n?n kullan?lması? hususlarında endi?elere yol açmaktadır.^[1]
- AI Yasas?, özellikle gerçek zamanlı biyometrik verilerin i?lenmesi ve sosyal puanlama ile ilgili olarak, GDPR'nin yakla??m?ndan farklı olarak, kamu ve özel kuruluşlar için farklı gereklilikler belirlemektedir. GDPR, aralar?nda herhangi bir ayrı?m yapmaks?z?n ki?isel verileri i?leyen hem kamu hem özel sektör tüm veri sorumluları? için geçerlidir.^[2]
- Veri sorumluları?, ilgili ki?ilerin hakları?n? korumak ve veri minimizasyonu gibi veri koruma ilkelerini uygulamak amacıyla teknik ve organizasyonel önlemleri almakla yükümlüdür. Bununla birlikte, AI Yasas? madde 10 uyar?nca, yüksek riskli AI sistemleri için yüksek kaliteli, temsili, hata içermeyen ve tam e?itim veri kümelerinin kullan?lması?n? zorunlu kıl?nm???tır. AI do?as? gere?i, mümkün olan en eksiksiz ve do?ru veri kümeleriyle çal??arak en isabetli sonuçlar? üretebilecektir. Her iki maddenin aynı anda nasıl uygulanacağına dair belirsizlikler vardır. AI Yasas?'n?n, GDPR'nin varsayılan koruma gereksinimine uygun gizlilik arttır?c? teknikleri göz önünde bulundurması? oldukça elzemdir.^[3]

?zleme: YZ'nin sorumlu kullan?m?n? sa?lamak için, YZ Yasas?, YZ sistemlerinin geli?tiricilerinin ve operatörlerinin, yüksek riskli YZ davran?? örneklerini tespit etmek ve önlemek için izleme mekanizmaları olu?turması?n? gerektirmektedir. Bu mekanizmalar, YZ sisteminin olu?turdu?u risklerle orantılı olmalı ve temel haklar ve kamu yarar? üzerindeki potansiyel etkiyi dikkate almalıdır. Bununla birlikte, YZ davran???n?n izlenmesinin GDPR kapsam?nda ki?isel verilerin korunması? ve gizlilik üzerinde etkileri olabilecektir. YZ sistemlerinin genellikle büyük miktarda ki?isel veri i?ledi?i göz önüne al?nd???nda, davran??lar?n?n izlenmesi, izleme mekanizmaları?n?n uygun ?ekilde tasarlanmaması? ve uygulanmaması? durumunda veri koruma ve gizlilik için risk olu?turabilecek ek verilerin toplanması?n? ve analiz edilmesini içerebilecektir.

GDPR, verilerin izlenmesi ve i?lenmesi için YZ sistemlerinin kullan?m?n? ele alırken, yalnızca bireysel profil olu?turma biçimleri için geçerlidir ve toplumun kesimlerini toplu olarak etkileyebilecek YZ güdümlü manipölasyon için bir bo?luk bırakılmaktadır. GDPR, YZ Yasas?'ndan farklı olarak, izleme sistemleri konusunda bireysel düzeyde ele al?nm???tır. Ancak YZ Yasas? ise bu bo?lu?u kapsamamaktadır. Söz konusu bu durum ise manipölasyona izin veren belirli tekniklere daha geni? bir yasak getirmekle sonuçlanabilecektir.

YZ Yasas?'n?n ?effaflık ve aç?klanabilirlik gerekliliklerinin, GDPR'nin silme hakk? ve itiraz hakk? ile ilgili hükümleriyle de çeli?ti?i görülmektedir. YZ sistemleri, büyük miktarda ki?isel veriyi i?lemek üzere tasarlanabilmekte

ve bu da bireysel haklara saygı gösterirken ?effaflık ve açıklanabilirliği sağlamayı zorlaştırmaktadır.

YZ Yasası ve GDPR'nin her ikisi de AB'deki YZ sistemleri için geçerli olacak tamamlamayı düzenlemeler olmasına rağmen, YZ Yasası'nın yüksek riskli YZ sistemleri ve ?effaflık gereklilikleri, özellikle kişisel verilerin YZ sistemleri tarafından ?lendiği durumlarda GDPR uyumluluğu üzerinde etkilere sahip olacaktır. Bununla birlikte, YZ Yasası'nın GDPR uyumluluğu üzerindeki etkisi, düzenlemelerin belirli hükümlerine ve bunların pratikte nasıl uygulandığına bağlı olacaktır. YZ Yasası kapsamında yukarıda belirtilen düzenlemeler, GDPR tarafından ortaya konan yükümlülükler ile karışık olarak değerlendirilmelidir. Söz konusu bu yükümlülüklerin yerine getirilmesinde öncelikli odak noktası "veri yönetimi ve yönetimi" olmalıdır. ?lgili kişinin kişisel verilerinin diğer bireylerin verileriyle ?kilendirilebildiği veya farklı amaçlar için ?lenebildiği YZ sistemlerinde, YZ tarafından üretilen veriler, ilgili kişinin hakkında paylaşmadığı veya paylaşmak istemediği bilgileri ortaya çıkabilir. Bu durumun özellikle MÖ veya DÖ yöntemlerini kullanan YZ sistemlerinde ortaya çıkması muhtemeldir. Sistem geliştirmesi tarafından öngörülemeyen veriler için varsayım bilgileri iletilmesi yapılmaması mümkün olmadıktan ve YZ sistemi tarafından üretilen veriler bir veri sorumlusu tarafından tamamen öngörülemediğinden, açıklık ve net veri ?leme koşulları gerektiren aydınlatma yükümlülüğünün yerine getirilmesi GDPR ile uyumlu olmayabilir. Ayrıca yukarıda açıklandığı üzere YZ, mevcut verileri analiz ederek yeni sonuçlar yaratan, mantıksal neden-sonuç ilişkileri kurmaktan ziyade veriler üzerinde korelasyonlar üreten bir sistemdir. Bu nedenle, YZ tarafından üretilen sonuçlar her zaman doğru olmayabilir. Bu durum, GDPR kapsamındaki genel ilkelere uyum ve veri ?leme koşulları gibi birçok yükümlülüğün ihlal edilmesine neden olabilir.

GDPR ve AI Yasası hükümleri, özellikle AI sistemlerinin kişisel verileri ?lediği durumlarda, uygulamada nasıl bir yol izleneceği konusunda da tereddütler doğurmaktadır. Söz konusu bu durum, her iki düzenlemeye de uymaya çalışmanın ?letmeler ve kuruluşlar için kafa karışıklığına ve belirsizliğe yol açabilecektir. YZ kullanımı tarafından kaynaklanan GDPR hükümlerine olası uyumsuzlukları önlemek için, uygun bir veri yönetimi ve yönetimi modelinin benimsenmesi zorunludur. Bu çerçevede, ilgili kişilerin kişisel verilerinin bağlamlarına ait verilerle karıştırmaması ve farklı amaçlarla oluşturulan diğer veri setlerinin bu verilerle birlikte kullanılmaması sağlamaya önem arz etmektedir.

AB Veri Koruma Otoritesi tarafından kılavuzlar ve görüşler yayınlanmasına rağmen, YZ'deki güncel gelişmeler dikkate alınarak GDPR düzenlemelerinin yasal bir temelde netleştirilmesi gerekmektedir. GDPR'nin kapsamı ve YZ Yasası gibi ilgili düzenlemeler önemli ölçüde yoruma tabidir. Bu durum, kişisel verileri kullanan YZ sistemlerinin kullanımıyla engellenmesine veya gizliliğin ihlal edilmesine yol açabilir. Bu nedenle, YZ Yasası ile uyumluluğu sağlamak için ikincil düzenlemelerin yürürlüğe girmesi veya GDPR'de gerekli değişikliklerin yapılması beklenmektedir. Ayrıca, YZ Kanunu'nun GDPR ile uyumlu olmayan hükümlerinin gözden geçirilmesi de elzemdir.

Türkiye'de YZ Mevzuatı ve Kişisel Verilerin Korunması

Türkiye, teknolojiye öncü olması ve YZ ve benzeri sohbet robotları geliştirmesine rağmen, yalnızca YZ özelinde hazırlanmış bir mevzuata sahip değildir, ancak belirli sektörlerde YZ'yi düzenlemek için bazı adımlar atmıştır. Bu alandaki en önemli gelişmelerden biri, YZ sistemleri tarafından ?lenen veriler de dahil olmak üzere Türkiye'de kişisel verilerin ?lenmesini düzenleyen Kişisel Verilerin Korunması Kanunu'nun ("KVKK") 2016 yılında kabul edilmesidir. KVKK kapsamında, Türkiye Veri Koruma Kurumu 2021 yılında [Yapay Zeka Alanında Kişisel Verilerin Korunması Dair Tavsiyeler](#) rehberini yayınlamıştır. Bu rehber yüksek riskli YZ kullanımlarında gizlilik etki değerlendirmelerinin yapılması, özel nitelikli kişisel veri kategorileri için ek önlemlerin alınması ve veri sorumlusu ve veri ?leyeninin belirlenmesi de dahil olmak üzere veri korumada YZ kullanımlarına yönelik bazı öneriler içermektedir. KVKK'ye ek olarak, YZ ile ilgili konulara ele alan sektöre özgü düzenlemeler de bulunmaktadır. Örneğin, Türkiye Sağlık Bakanlığı, sağlık hizmetlerinde YZ kullanımı için veri koruma, ?effaflık ve bilgilendirilme onam gerekliliklerini içeren kılavuzlar yayınlamıştır.

Ayrıca, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ("Dijital Dönüşüm Ofisi"), 30474 sayılı Resmi Gazete'de yayınlanan 10 Temmuz 2018 tarihli Cumhurbaşkanlığı Kararnamesi No. 1 kapsamında kurulmuştur. Dijital Dönüşüm Ofisi, Büyük Veri ve Yapay Zeka Departmanı dahil olmak üzere çeşitli teknolojik

gelişme ve projelere odaklanan birçok departman bünyesinde bulunmaktadır. Dijital Dönüşüm Ofisi, Büyük Veri ve Yapay Zeka Departmanı, Türkiye'de YZ ve büyük verinin uygulanması ve tevik etmeyi, ilgili politika ve düzenlemelerin geliştirilmesini desteklemeyi amaçlamaktadır. Dijital Dönüşüm Ofisi'nin katkılarıyla 20 Ağustos 2021 tarihli ve 31574 sayılı Resmi Gazete'de Cumhurbaşkanlığı Kararnamesi No. 2021/18 ile [Ulusal Yapay Zeka Stratejisi 2021-2025](#) yayınlanmıştır. Ulusal Yapay Zeka Stratejisi 2021-2025, güçlü bir YZ ekosistemi geliştirme, insan gücünü artırma, YZ teknolojilerinin geliştirilmesini ve benimsenmesini destekleme, YZ'nin etik ve sorumlu kullanımı, sağlama, destekleyici ve düzenleyici bir yasal çerçeve oluşturma gibi önemli konuları vurgulamaktadır. Ayrıca, strateji, YZ uygulamalarındaki veri gizliliği, güvenliğini ve etik değerlerin öneminin altını çizmektedir.

Türkiye Cumhuriyeti Cumhurbaşkanlığı tarafından 2019-2023 yılları için hazırlanan [11. Kalkınma Planı](#) ("11. Kalkınma Planı") 18 Temmuz 2019 tarihinde yayınlanmıştır. Burada endüstriyel bulut platformlarında sunulabilecek YZ, gelişmiş veri analitiği, simülasyon ve optimizasyon, ürün döngüsü ve üretim yönetim sistemleri gibi uygulama ve hizmetlerin geliştirilmesini tevik etmek için, 11. Kalkınma Planı teknoloji sağlayıcılar için bir çerçeve belirlenmiştir. Ek olarak, Ulusal Teknoloji Girişimi'nin bir parçası olarak, YZ ve büyük veri teknolojileri için geliştirme yolları belirlenmiştir. Bu yollar, YZ'nin kullanımları için gerekli altyapının kurulması ve nitelikli insan kaynağı geliştirilmesini amaçlamaktadır.



Sonuç olarak,

Türk yasa koyucusunun YZ Yasası'ndan ilham alması ve bunu Türkiye'de gelecekteki YZ ile ilgili düzenlemeler için bir model olarak kullanması mümkündür. Ancak, YZ Yasası'nın GDPR gibi KVKK'yi özel olarak nasıl etkileyeceği henüz belli değildir. Türk yasa koyucusunun, YZ ile ilgili faaliyetlerin hem KVKK hem de AB'de gelecekte yürürlüğe girebilecek YZ ile ilgili düzenlemelerle uyumlu olması sağlamak için KVKK'de değişiklikler veya ek düzenlemeler yapması gerekebilir. 11. Kalkınma Planı'na göre, KVKK'nin GDPR temelinde güncellenmesinin beklendiği açıklandığından, [KVKK'nin çeşitli hükümlerinin GDPR'ye göre değiştirilmesi beklendiğinden](#), GDPR ile ilgili olarak yukarıda Avrupa Birliği YZ Mevzuatı bağlamında belirtilen konular aynı şekilde Türkiye için de dikkate alınacaktır.

Kaynakça:

- Bogucki, A., Engler, A., Perarnaud, C., & Renda, A. (2022). *The AI Act and Emerging EU Digital Acquis, Overlaps, Gaps and Inconsistencies* (CEPS-IAI-EUI Report No. 49). Centre for European Policy Studies. Eriřim https://www.ceps.eu/wp-content/uploads/2022/09/CEPS-IAI-EUI_AI-Act-EU-Digital-Acquis-2022.pdf
- Avrupa Komisyonu. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Eriřim <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0205&from=EN>
- Avrupa Parlementosu. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. Eriřim [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)
- Future of Privacy Forum. (2021, April 20). *GDPR and the AI Act interplay: Lessons from FPF's ADM case-law report*. Eriřim <https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/>
- Türkiye Cumhuriyeti Kalkınma Bakanlığı. (2019). *On Birinci Kalkınma Planı (2019-2023)* Eriřim https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf
- Türkiye Cumhuriyeti Cumhurbaşkanlığı. (2021) *Ulusal Yapay Zeka Stratejisi 2021-2025*. Eriřim <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>
- Kişisel Verileri Koruma Kurumu. (2016) *Kişisel Verilerin Korunması Kanunu*. Eriřim <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5>
- Kişisel Verileri Koruma Kurumu. (2021). *Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler*. Eriřim <https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler>

[1] Bogucki, A., Engler, A., Perarnaud, C., & Renda, A. (2022). *The AI Act and Emerging EU Digital Acquis, Overlaps, Gaps and Inconsistencies*. Centre for European Policy Studies.sf.7.

[2] Bogucki, Engler, Perarnaud, Renda (2022), sf.9.

[3] Bogucki, Engler, Perarnaud, Renda (2022), sf.9.

Related Attorneys

- [DR. E. SEYFİ MOROĞLU, LL.M.](#)
- [BURCU TUZCU ERSİN, LL.M.](#)
- [CEYLAN NECİPOĞLU, PH.D, LL.M.](#)