

— Kişisel Verileri Koruma Kurumu —

BÜLTEN

Mart - Mayıs 2025 Sayı:8

**YAPAY ZEKÂYA
GENEL BAKIŞ**

Giriş 5

Röportaj 6

Köşe Yazısı 8

Yapay Zekâya İlişkin Bazı Kavramlar ve Tanımlar 12

Yapay Zekâ ve Kişisel Verilerin Korunması 14

Ulusal Yapay Zekâ Stratejisi
2024-2025 Eylem Planı 16Kişisel Verileri Koruma Kurumunun Yapay Zekâ
Konusundaki Çalışmaları 18“Yapay Zekâ Teknolojilerine Akademik Bakış”
Kitabı Üzerine Kısa Bir İnceleme 20

Genel Olarak Üretken Yapay Zekâ 22

Avrupa Birliği ve Yapay Zekâ Regülasyonu:
Yapay Zekâ Tüzüğü Merceğinden Temel Bilgiler 24

Öne Çıkan Gelişmeler 28

Bizden Haberler 34

Kişisel Verileri Koruma Kurumu

KVKK Bülten

www.kvkk.gov.tr

Sayı:8

Kişisel Verileri Koruma Kurumu

Adına İmtiyaz Sahibi

Prof. Dr. Faruk BİLİR

Yönetim Yeri

Nasuh Akar Mahallesi 1407. Sokak

No:4 Balgat Çankaya/ANKARA

Tel: [312] 216 50 00

© Bütün hakları, Kişisel Verileri Koruma Kurumu'na aittir. Kaynak gösterilmek kaydıyla, tanıtım amaçlı kısa alıntı dışında yayımcının yazılı izni olmadan hiçbir yolla çoğaltılamaz. Yayımlanan yazıların ve fotoğrafların sorumluluğu yazarlarına ve sanatçısına aittir.

GİRİŞ

Yapay zekâ, çağımızın en dikkat çekici teknolojik gelişmelerinden biri olarak insanlık için büyük fırsatlar sunmaktadır. Eğitimden sağlığa, üretimden kamu hizmetlerine kadar pek çok alanda dönüşüm potansiyeli taşıyan bu teknoloji, hayatımızı kolaylaştırmakta ve verimliliği artırmaktadır. Ancak, yapay zekâ teknolojileri sunduğu geniş imkanların yanı sıra, bireyin hak ve özgürlüklerini etkileyebilecek bazı riskleri de beraberinde getirmektedir. Bu nedenle yapay zekâya dair gelişmeleri yalnızca teknik bir ilerleme olarak değil, aynı zamanda hukuki, etik ve toplumsal boyutlarıyla birlikte ele almak önem taşımaktadır.

Bu sayımızda; yapay zekâya ilişkin temel kavramlardan başlayarak kurumumuzun bu alandaki faaliyetlerini genel hatlarıyla ele almak; ayrıca üretken yapay zekâ kullanımı sırasında kişisel verilerin korunmasına yönelik dikkat edilmesi gereken hususlara ve Avrupa Birliği’nin yapay zekâya ilişkin düzenlemelerinin getirdiği yeniliklere de değinmek istedik.

KVKK Bülten’in “Yapay Zekâya Genel Bakış” konulu sekizinci sayısının bu alandaki farkındalığın artmasına ve bilinçli yaklaşımların gelişmesine katkı sağlamasını temenni eder, tüm okuyuculara faydalı olmasını dileriz.



Yapay zekâ, yalnızca teknolojik bir dönüşümün değil, aynı zamanda toplumsal, hukuki ve etik bir dönüşümün de habercisi. Günlük yaşamdan kamu politikalarına, eğitimden özel sektöre kadar pek çok alanda etkisini hissettiren bu teknoloji, beraberinde yeni sorular ve sorumluluklar da getiriyor. Kurum Başkanımız Prof. Dr. Faruk BİLİR ile bir röportaj gerçekleştirerek yapay zekânın toplumsal etkilerini ve veri koruma perspektifinden değerlendirmelerini kendisinden dinledik.

Yapay zekâ teknolojileri artık hayatımızın birçok alanında yer alıyor. Sizce bu teknolojinin toplum üzerindeki etkilerini nasıl değerlendirmeliyiz?

Yapay zekâ teknolojileri, her geçen gün daha fazla alanda kullanılmakta ve günlük yaşamın ayrılmaz bir parçası haline gelmektedir. Bu süreç, yapay zekâya yönelik yaklaşımların da farklılaşmasına neden olmaktadır. Bu teknolojiye ilişkin değerlendirmeler, çoğu zaman iki uç yaklaşım arasında gidip gelmektedir. Bir yanda insan yaşamını dönüştürecek büyük beklentiler, diğer yanda ise endişe verici senaryolar öne çıkmaktadır.

Bu bağlamda, yapay zekânın toplumsal etkilerini anlayabilmek ve bu teknolojiyi doğru biçimde değerlendirebilmek için gerçekçi ve insan merkezli bir yaklaşıma ihtiyaç duyulmaktadır. Bu doğrultuda, yapay zekâ sistemlerinin gelişiminin, toplumsal yararı gözetilen bir anlayışla yönlendirilmesi önem taşımaktadır.

Yapay zekâ bilinçli, denetlenebilir ve sorumlu bir şekilde kullanıldığında, toplumsal faydaya yönelik çözümler geliştirme ve karar alma süreçlerinde bireyleri destekleme yönüyle

önemli katkılar sunabilmektedir. Ancak bu süreçte, mahremiyetin korunması, şeffaflığın sağlanması ve hesap verebilirlik gibi etik ilkeler göz ardı edilmemelidir.

Yapay zekâ teknolojilerinde, teknoloji ile mahremiyet arasındaki dengenin esas alınması neden önemlidir?

Yapay zekâ uygulamalarının gelişimiyle birlikte kişisel verilerin korunması, yapay zekâ sistemlerinin her aşamasında gözetilmesi gereken temel bir unsur hâline gelmiştir. Teknoloji ile mahremiyet arasında kurulacak dengeli bir ilişki, yalnızca bireylerin hak ve özgürlüklerinin korunmasına katkı sunmakla kalmayacak; aynı zamanda teknolojiye duyulan toplumsal güvenin güçlenmesini de sağlayacaktır.

Bu bağlamda, yapay zekâ sistemlerinin temel hak ve özgürlüklere saygılı, şeffaf, denetlenebilir, insan odaklı ve kişisel verilerin korunmasını gözetilen bir yaklaşımla geliştirilmesi ve kullanılması büyük önem taşımaktadır.

Yapay zekâ teknolojilerinde otomatik karar verme süreçleri sıkça kullanılıyor. Sizce bu tür sistemler, bireylerin haklarını kullanmalarını nasıl etkiliyor?

Otomatik karar verme süreçleri günümüzde giderek daha yaygın hale gelmektedir. Özellikle işe alım, kredi başvuruları ve sigortacılık işlemleri gibi birçok alanda bu tür sistemlerle karşılaşırız. Ancak, yapay zekâ sistemlerindeki şeffaflık eksikliği ve algoritmik süreçlerin karmaşıklığı, bu sistemler vasıtasıyla alınan kararların anlaşılmasını zorlaştırabilmektedir.

Bu noktada Kanun'un 11. maddesi, kişisel verisi işlenen bireylere bilgi edinme ve işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı tanıyarak, temel hakların korunmasına yönelik önemli bir çerçeve sunmaktadır. Bu düzenlemeyi, insan odaklı yaklaşımın mevzuatımıza yansıyan somut bir örneği olarak düşünebiliriz.

İnsan odaklı yaklaşım, teknolojik süreçlerin şeffaflığını artırmayı, bireylerin kendi verileri üzerindeki kontrolünü güçlendirmeyi ve adil karar alma süreçlerini teşvik etmeyi amaçlar. Bu bağlamda itiraz hakkı sayesinde bireyler, yalnızca alınan kararları sorgulama fırsatı bulmakla kalmaz, aynı zamanda insan müdahalesinin sürece dahil edilmesini talep ederek daha adil sonuçların ortaya çıkmasına katkı sağlayabilir.

Kişisel Verileri Koruma Kurumu, yapay zekâ modelleri geliştiren ve kullanan şirketlere rehberlik sağlayan bir çerçeve sunuyor mu?

Hem yapay zekâ geliştiren hem de kullanan şirketler için, kişisel verilerin işlenmesiyle ilgili yol gösterici rehberler hazırlanması önemlidir. Kurumumuz, yapay zekâ teknolojileri geliştiren ve kullanan şirketlere rehberlik sağlayabilecek bir doküman yayınlamıştır.

Bu çalışmada, yapay zekâ alanında kişisel verilerin korunmasına ilişkin tavsiyelerde bulunulmuştur. Şirketlerin yapay zekâ sistemlerini geliştirirken, ilgili kişilerin temel hak ve özgürlüklerini korumaya yönelik bir yaklaşım benimsemesi teşvik edilmektedir. Özellikle, sistemlerin tasarım aşamasından itibaren kişisel verilerin korunmasını sağlayacak şekilde yapılandırılması, bu bağlamda tasarımda mahremiyet ve varsayılan olarak mahremiyet ilkelerinin hayata geçirilmesi önerilmektedir. Kurumumuz, bu alandaki rehberlik çalışmalarını uluslararası standartlar ve en iyi uygulamalar doğrultusunda güncellemektedir.

Kurumun yeni çalışması olan “Yapay Zekâ Teknolojilerine Akademik Bakış” isimli kitap, kamuoyuna duyuruldu. Bu çalışmanın yapılmasındaki amacı ve neden bu çalışmaya ihtiyaç duyulduğunu anlatabilir misiniz?

Yapay zekâ; hukuk, bilişim ve etik disiplinlerinin kesişim noktasında yer alan, akademik dünyanın da yoğun ilgi gösterdiği ve katkı sunduğu dinamik bir çalışma alanıdır. Yapay zekâ sistemlerinin beraberinde getirdiği yeni hukuki, teknik ve etik sorular, bu alandaki akademik çalışmalara duyulan ihtiyacı artırmaktadır.

Akademik araştırmalar ve bilimsel yayınlar; yapay zekâya ilişkin düzenlemelerin daha iyi anlaşılmasına, ulusal ve uluslararası uygulamaların karşılaştırmalı olarak değerlendirilmesine ve gelişen teknolojilere uyumlu politika önerilerinin geliştirilmesine önemli katkılar sunmaktadır. Aynı zamanda bu çalışmalar, kişisel verilerin korunmasına ilişkin farkındalığın artmasına ve veri koruma politikalarının uzun vadede sürdürülebilirliğine hizmet etmektedir. Biz de Kurum olarak buradan hareketle, böyle bir çalışmayı yaparak bu alana katkı sunmak istedik.

Son olarak yapay zekâ teknolojilerinin çocukların kişisel verileri üzerindeki etkilerini nasıl değerlendiriyorsunuz?

Yapay zekâ teknolojileri, çocuklara yönelik dijital platformlar, oyunlar ve eğitim uygulamaları gibi alanlarda giderek daha fazla kullanılmaktadır. Bu sistemler, çocukların davranışlarını, ilgi alanlarını ve kimi zaman fiziksel özelliklerini dahi analiz ederek kişiselleştirilmiş içerikler sunabilmektedir. Ancak bu tür veri işleme faaliyetleri, çocukların mahremiyetini ve kişisel verilerinin korunmasını sağlama konusunda özel önlemler alınmasını gerektirmektedir. Örneğin, açık rıza süreçlerinin ebeveyn onayını içerecek şekilde tasarlanması ve çocukların verilerinin ticari amaçlarla kullanılmasının sınırlandırılması önemlidir. Ayrıca, yapay zekâ destekli sistemlerde çocukların yaş gruplarına uygun ayarların varsayılan olarak sunulması, bu konudaki riskleri azaltmak için etkili bir yöntem olabilir.

Bunun yanı sıra, dijital dünyada karşılaşabilecekleri riskler konusunda çocuklara farkındalık kazandırılması da büyük önem taşımaktadır. Çocukların, hangi bilgilerin paylaşılmasının güvenli olduğu ve hangi durumlarda dikkatli olmaları gerektiği gibi konularda bilgilendirilmesi, buna ilişkin risklerin azaltılmasına katkı sağlayacaktır. Bu çerçevede, çeşitli yaş gruplarından çocukların veri koruma bilincini artırmak için farkındalık ve bilgilendirme programları düzenliyor, ayrıca çeşitli dokümanlar yayımlıyoruz. Bunlara ilişkin detaylar için Kurumumuz internet sayfasının takip edilmesini tavsiye ederim.

Prof. Dr. E. Eylem AKSOY RETORNAZ*Galatasaray Üniversitesi Hukuk Fakültesi
Bilişim ve Teknoloji Hukuku Anabilim Dalı

YAPAY ZEKÂ, ALGORİTMİK KARAR VERME VE KİŞİSEL VERİLERİN KORUNMASI

Yapay zekâ teknolojilerinin son dönemdeki yükselişi, toplumlarımızı ve ekonomilerimizi derinden dönüştüren bir değişimi temsil etmektedir. Yapay zekâ alanında dünyanın önde gelen uzmanlarından biri olan Çinli Kai Fu Lee, Türkçe'ye "Yapay Zekâ Yeni Bir Dünya Düzeni" başlığıyla çevrilen kitabında, yapay zekâyı tarihin en büyük dönüşümü olarak tanımlamaktadır. Yazar, yapay zekâyı geleceğin elektriğine benzeterek söz konusu sistemlerin tıpkı elektrik gibi vazgeçilmez ve her yerde var olacağının altını çizmektedir.

Tüm teknolojik gelişmelerde olduğu gibi, yapay zekâ teknolojilerindeki gelişmeler de bir yandan insanlığa büyük kolaylıklar sunarken diğer yandan temel hak ve özgürlükler bakımından bazı riskleri de beraberinde getirmektedir.

Öğrenen algoritmalar, yapay zekâ sistemlerin temelini oluşturur. Algoritma: "İyi tanımlanmış kuralların ve işlemlerin adım adım uygulanmasıyla bir sorunun giderilmesi veya sonuca en hızlı biçimde ulaşılması işlemi [TDK, 2025] olarak adlandırılmaktadır. Öğrenen algoritmalar makine öğrenmesi veya derin öğrenmeyle çalışmaktadır.

Makine öğrenmesinde algoritma ilgili bilgilerin, genellikle bir sonucu tahmin etme veya kestirme amacıyla, bir dizi eğitim verisinden çıkarıldığı bir süreçle çalışmaktadır. Bu süreç insan müdahalesi yalnızca algoritmaya sağlanabilen eğitim verilerinden nasıl bir sonuç elde etmesi gerektiğini belirtmekle sınırlıdır. Daha sonra program, istenen sonucu elde etmeyi sağlayacak işlemleri kendisi üretir.

Derin öğrenme, makine öğrenmesi altında yer alan ve çok sayıda nöron katmanından oluşan yapay sinir ağlarını kullanan bir süreçtir. Çok sayıda parametreden oluşan bu algoritmaların eğitilebilmeleri başka bir ifadeyle verilerden bir model oluşturabilmeleri için büyük miktarda veriye ihtiyaç duyulmaktadır.

Makine öğrenmesi ve derin öğrenmede kullanılan veriler, kişisel veriler de olabilir. Makine öğrenmesi ve derin öğrenme algoritmalarıyla kişisel verilerin üzerinde farklı işlemler yapılması mümkün olduğundan bu algoritmalarla, kişisel verilerin otomatik olarak işlenmesi mümkündür.

Algoritmik Karar Verme Nedir?

Derin öğrenme ve makine öğrenmesiyle çalışan algoritmalar aracılığıyla yapay zekâ sistemleri kullanılarak işlenen kişisel veriler aracılığıyla kurulan bağıntılar sayesinde kararlar verilebilmektedir. Algoritmik karar verme olarak adlandırılan bu süreçlerde kimi zaman hiçbir insan müdahalesi olmadan, kimi zaman ise bu algoritmaların yardımıyla kararlar verilmektedir. Bir karar sürecine insan müdahalesi bulunmadığında otomatik karar verme söz konusudur. Vergi beyannamelerinde veya sosyal yardım başvurularında suistimal olup olmadığını veya tekerrür riskini tespit etmeye çalışan algoritmalar bu karar alma mekanizmalarının birer örneğidir. Algoritmik karar verme süreçleri yalnızca suç riskini saptamak için değil bazı hallerde kamu hizmetlerinin sunumunda da rol oynamaktadır. Örneğin, Belçika'da öğrencilerin hangi semtteki okullara gideceğini saptamak için yapay zekâ sistemlerine başvurulmaktadır.

Ayrımcılık Riski

Büyük veri setleriyle beslenen yapay zekâ sistemlerinin kullanılmasıyla alınan kararlar insanların topluma temel hak ve hürriyetlerini kısıtlayan veya kamu hizmetlerinden yararlanmalarını engelleyen bir etkiye sahip olabilirler. Bir algoritma önyargılı verilerle eğitildiğinde, bu önyargıları yeniden üreterek onları daha da güçlendirebilir.

Hollanda'da yaşanan bir olay, algoritmik karar vermenin bireyler üzerinde nasıl olumsuz sonuçlar doğurabileceğinin çarpıcı bir örneğidir. 2013 yılından itibaren Hollanda hükümeti, çocuk yardım başvurusunun gerçeğe aykırı olma ihtimaline karşı her vatandaşa bir risk puanı atayan bir algoritma kullanarak çocuk yardımından hukuka aykırı bir biçimde yararlananlarla mücadele etmeye karar vermiştir. Bu algoritma, yabancı isimler veya çifte vatandaşlık gibi kriterleri kullanan bir algoritmadır. Hukuka aykırı başvurularla mücadelede algoritmalarının tavsiyelerini takip eden idare, çocuk yardımdan faydalanan ve

çoğunlukla yabancı kökenli olan veya dezavantajlı mahallelerde yaşayan kişilerden giderek artan bir şekilde yardıma ihtiyaçları olduğunu kanıtlayan belgeleri talep etmeye başlamıştır. Yetkililerin talep ettikleri belgeleri sağlayamayan binlerce düşük ve orta gelirli aile, aldıkları yardımları geri ödemeye zorlanmış, bazıları evlerini veya işlerini kaybetmiştir. Bu kişilere yöneltilen suçlamalar nedeniyle sayıları bini aşan çocuk devlet korumasına alınmıştır. Bu algoritmalar nedeniyle pek çok kişi ayrımcı bir profilemeye maruz bırakılmıştır.

Algoritmik Karar Verme ve Kişisel Verilerin Korunması

Algoritmik karar verme sistemlerine başvurulduğunda, bu sistemlerin bireylerin temel hak ve hürriyetlerini ihlal etmediklerinden, ilgili kişilerin özerkliğinin korunduğundan ve eşitlik ve adalet ilkelerine saygı duyulduğundan emin olmak gerekir. Başlıca zorluklardan biri algoritmik sistemlerin genellikle çok şeffaf olmamasıdır. Şeffaflık sağlanmadığı takdirde bu algoritmalar erişilemez "kara kutular" olarak kalacaktır. Bu nedenle şeffaflık, algoritmik sistemlerin etkisini değerlendirmede gerekli bir ilk adımdır ancak tek başına yeterli değildir. Ayrıca bu sistemlerinin hesap verilebilirlik ilkesine uygun olması başka bir ifadeyle yaşam döngülerinin denetlenebilir, belgelenebilir ve sorumluların saptanabilir olması da gerekir.

Şeffaflık ve hesap verilebilirliğin yanı sıra, temel hak ve hürriyetlerin ve kişisel verilerin korunması bakımından algoritmik karar verme sistemlerinden etkilenenlerin bireysel ve demokratik denetimini güvence altına alan hukuki düzenlemeler de gereklidir. Özellikle ilgili kişilerin algoritmik bir karar verme söz konusu olduğunda bu algoritmik karar verme sisteminin kullanımına itiraz edebilmeleri ve ilgili bilgilere erişebilmeleri önem arz etmektedir.

Bireyler kişisel veriler işlenmek suretiyle insan müdahalesi olmadan algoritmik bir karar verildiğinde bu kararlara tabi olmama hakkına da sahiptir. Bu hak, Avrupa Birliği Genel Veri Koruma Tüzüğü [GVKT] m. 22'de, veri öznesinin

kendisiyle ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen, profillemeye de dâhil olmak üzere yalnızca otomatik işlemeye dayalı bir karara tabi olmama hakkına ilişkin düzenlemeyle yasal bir çerçeveye kavuşmuştur. Benzer bir biçimde, 6698 sayılı Kanunun ilgili kişinin haklarının düzenlendiği 11/g. maddesinde, ilgili kişinin “işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,” hakkı düzenlenmiştir.

AB Adalet Divanı’nın, bekletici meseleyle önüne gelen bir olayda kredi değerlendirme yazılımı [banka puanlaması] yapan bir kuruluş ile puanlama sonucunun yetersiz mali ödeme gücünü gösterdiği gerekçesiyle cep telefonu sözleşmesi imzalaması reddedilen bir kişi arasında çıkan uyuşmazlıkta, profil oluşturmaya dayalı otomatik kararlara ilişkin bilgilere GVKT m. 15 uyarınca ilgili kişinin erişim hakkının kapsamını açıklığa kavuşturmuştur. Mahkeme, bu hakkın, karar almanın altında yatan mantığın anlaşılır ve geçerli bir şekilde açıklanmasını gerektirdiğini, böylece ilgili kişinin hangi kişisel verilerinin kullanıldığını ve yapılan değerlendirmeyi nasıl etkilediğini anlayabilmesini sağladığını ileri sürmüştür.

AB Yapay Zekâ Tüzüğü’nde de algoritmik karar vermeye ilişkin bazı düzenlemeler yer almaktadır. Tüzükte özellikle algoritmik ayrımcılık riskini en aza indirmek için özel gereklilikler öngörülmekte ve insan denetimine olan ihtiyaç vurgulanmaktadır. Risk odaklı bir yaklaşım benimseyen AB Yapay Zekâ Tüzüğü’nde yapay zekâ sistemleri bakımından dört risk seviyesi [kabul edilemez, yüksek risk, yüksek risk, minimum risk] yer almaktadır. Tüzükte, bireylerin sosyal davranışlarına veya kişisel özelliklerine göre güvenilirliklerini değerlendirmeyi veya sıralamayı amaçlayan yapay zekâ sistemlerinin ayrımcılığa yol açabileceği özellikle belirtilmektedir.

Kabul edilemez risk ve yüksek riskli yapay zekâda insan denetimine ilişkin düzenlemelerin yanı sıra AB Yapay Zekâ Tüzüğü’nün 86. maddesinde algoritmik bir karara tabi olanlara

bu kararın açıklanması hakkı tanınmıştır. Bu düzenlemeye göre, yüksek riskli bir yapay zekâ sisteminin çıktısına dayalı olarak bir *deployer* [dağıtıcı] tarafından verilen bir karara tabi olan herhangi bir etkilenen kişi, dağıtıcıdan [*deployer*]dan açık ve anlaşılır açıklamalar alma hakkına sahip olacaktır.

AB Yapay Zekâ Tüzüğü’nde yer alan algoritmik karar verme hakkında açıklama isteme hakkı algoritmik şeffaflık ve kişisel verilerin korunması açısından önemli bir adım olsa da yalnızca belirli sektörlerdeki bazı yüksek riskli yapay zekâ sistemlerinin çıktılarına dayalı kararlar için geçerli olduğundan sınırlı bir koruma sağlamaktadır. Açıklama hakkı yalnızca bir kararın yasal etkiler yaratması veya bir kişiyi sağlık, güvenlik ve temel haklarını olumsuz yönde etkileyeceğini önemli ölçüde etkilemesi durumunda söz konusudur. Ayrıca açıklama isteme hakkı yapay zekâ sistemleri sağlayıcılarına değil dağıtıcılarına karşı kullanılan bir haktır.

Yapay zekâ sistemleri ile algoritmik karar verme söz konusu olduğunda kişisel verilerin korunmasının sağlanması bakımından veri koruma etki değerlendirilmesinin yanı sıra şeffaflık ve hesap verilebilirliğin sağlanması için algoritmik etki değerlendirilmesi de uygulanması önem taşımaktadır. Algoritmik etki değerlendirmesi ve veri koruma etki değerlendirmesi birlikte gerçekleştirilerek hem veri işleme faaliyetinin hem de algoritmik karar vermenin hukuka uygunluğunun sağlanması mümkün olacaktır.

YAPAY ZEKÂYA İLİŞKİN BAZI KAVRAMLAR VE TANIMLAR

Algoritma: Belirli bir görevi yerine getirmek, belirli bir problemi çözmek veya bir makine öğrenmesi ya da yapay zekâ modeli oluşturmak için tasarlanmış hesaplama prosedürü veya talimat ve kurallar dizisi. *[International Association of Privacy Professionals (IAPP)-Glossary of Privacy Terms]*

Büyük veri: Hacim, çeşitlilik, hız ve değişkenlik gibi özelliklerine bağlı olarak, işlenmesi ve anlamlı bir değer üretilmesi için özel teknolojiler ve teknikler gerektiren kapsamlı veri setleri. *[ISO/IEC 22989:2022]*

Yapay zekâ: Bir bilgisayarın veya bilgisayar kontrolündeki bir robotun çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyeti; dinamik ve belirsiz ortamlarda akıl yürütme, anlam keşfetme, genelleme veya geçmiş deneyimlerden öğrenme gibi insanlara özgü bilişsel kabiliyetlerle donatılmış sistemler. *[Ulusal Yapay Zekâ Stratejisi 2021-2025]*

Yapay zekâ sistemi: Değişken düzeylerde özerklikle çalışacak şekilde tasarlanmış, yerleştirme [deployment] sonrasında uyarlanabilirlik gösterebilen ve aldığı girdiler doğrultusunda açık veya örtülü hedeflere uygun olarak tahmin, içerik, tavsiye veya kararlar gibi çıktılar üreten, bu çıktılarla fiziksel veya sanal ortamları etkileyebilen makine tabanlı bir sistem. *[2024/1689 sayılı AB Yapay Zekâ Tüzüğü]*

Dar/zayıf yapay zekâ: Belirli görevleri yüksek yeterlilikle gerçekleştirmek üzere tasarlanmış yapay zekâ sistemleri.

Güçlü/yapay genel zekâ: Geniş bir görev yelpazesini tatmin edici bir performans düzeyinde yerine getiren yapay zekâ sistemleri. *[ISO/IEC 22989:2022]*

Yapay süper zekâ: Bilimsel yaratıcılık, genel bilgelik ve sosyal beceriler de dâhil olmak üzere, hemen her alanda en iyi insan zekâsından çok daha üstün olan yapay zekâ sistemleri. *[Nick Bostrom-How Long Before Superintelligence?]*

Makine öğrenmesi: Sistemlerin verilerden veya deneyimlerden öğrenmesini sağlamak için hesaplama teknikleri kullanan bir süreç. *[ISO/IEC 22989:2022]*

Gözetimli makine öğrenmesi: Eğitim sırasında etiketlenmiş verilerin kullanıldığı makine öğrenmesi türü. *[ISO/IEC 22989:2022]*

Gözetimsiz makine öğrenmesi: Eğitim sırasında etiketlenmemiş verilerin kullanıldığı makine öğrenmesi türü. *[ISO/IEC 22989:2022]*

Pekiştirmeli öğrenme: Bir ortamla etkileşim yoluyla ödüllü en üst düzeye çıkaracak en uygun eylem dizisini öğrenme süreci. *[ISO/IEC 22989:2022]*

Derin öğrenme: Makine öğrenmesinin bir alt alanı olup çok sayıda gizli katmana sahip sinir ağlarının eğitilmesi yoluyla zengin hiyerarşik temsiller oluşturulmasına yönelik bir yaklaşım. *[ISO/IEC 22989:2022]*

Yapay zekâ geliştiricisi: Yapay zekâ sistemlerine ait her türlü ürün için içerik ve uygulama geliştiren gerçek veya tüzel kişi. *[KVKK-Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler]*

Yapay zekâ üreticisi: Yapay zekâ sistemlerini oluşturan yazılım, donanım gibi her türlü ürünü üreten gerçek veya tüzel kişi. *[KVKK-Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler]*

Yapay zekâ servis sağlayıcısı: Yapay zekâ tabanlı sistemler, veri toplama sistemleri, yazılımlar ve cihazlar kullanarak ürün ve/veya hizmet sunan gerçek veya tüzel kişi. *[KVKK-Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler]*

Üretken Yapay Zekâ: Metin, görüntü veya ses oluşturma gibi çeşitli görev ve uygulamaları gerçekleştirebilen, geniş çeşitlilikte çıktılar üretmek üzere tasarlanmış özel makine öğrenmesi modellerini kullanan bir yapay zekâ alt dalı. *[Avrupa Veri Koruma Denetçisi (EDPS)-Generative AI and the EUDPR: First EDPS Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems]*

Büyük dil modeli: Metin tabanlı görevleri yerine getirmek için karakterler, kelimeler ve ifadeler arasındaki kalıpları ve ilişkileri analiz etmek ve öğrenmek amacıyla, büyük metin veri setleri üzerinde önceden eğitilmiş modeller oluşturmak için derin öğrenme algoritmalarını kullanan bir yapay zekâ türü. *[IAPP AI Governance Center-Key Terms for AI Governance]*

Doğal dil işleme: Bilgiyi içeriğe dönüştürerek bilgisayarların insan dilini anlamasına, yorumlamasına ve uygulamasına yardımcı olan bir yapay zekâ alt alanı. *[IAPP AI Governance Center-Key Terms for AI Governance]*

Prompt: Bir çıktı üretmek için yapay zekâ modeli veya sistemine sağlanan bir girdi veya talimat. *[IAPP AI Governance Center-Key Terms for AI Governance]*

Halüsinasyon: Üretken yapay zekâ modellerinin, gerçek görünümü altında görünüşte makul ancak gerçekte yanlış çıktılar oluşturduğu durumlar. *[IAPP AI Governance Center-Key Terms for AI Governance]*

Deepfake: Yapay zekâ tarafından oluşturulan veya manipüle edilen, mevcut kişi, nesne, yer, varlık ya da olayları andıran ve bir kişiye gerçek ya da doğru izlenimi verebilecek nitelikteki görüntü, ses veya video içerikleri. *[2024/1689 sayılı AB Yapay Zekâ Tüzüğü]*

İnsan merkezli yapay zekâ: Yapay zekânın tasarlanması, geliştirilmesi, yerleştirilmesi ve kullanılmasında insanın refahını, özerkliğini, değerlerini ve ihtiyaçlarını ön planda tutan bir yaklaşım. *[IAPP AI Governance Center-Key Terms for AI Governance]*

YAPAY ZEKÂ VE KİŞİSEL VERİLERİN KORUNMASI

Yapay zekâ sistemlerinin öğrenme süreçleri ve karar alma kabiliyetleri, büyük ölçüde kullanılan verilere bağlıdır. Bu verilerin önemli bir kısmını ise kişisel veriler oluşturmaktadır. Ayrıca, bu sistemler kişisel veri niteliği taşıyabilecek sonuçlar da üretebilmektedir. Dolayısıyla, bu sistemlerle ilgili süreçlerin farklı aşamalarında doğrudan veya dolaylı şekilde kişisel verilere temas edilebilmektedir.

Ülkemizde 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu, her ne kadar yapay zekâ teknolojilerine özgü hükümler içermese de, bu sistemler kapsamında gerçekleştirilen veri işleme faaliyetlerine uygulanabilecek genel bir hukuki çerçeve sağlamaktadır.

Bu doğrultuda, yapay zekâ tabanlı sistemlerde gerçekleştirilen kişisel veri işleme faaliyetlerinin, 6698 sayılı Kanun'daki düzenlemelere uygun olarak yürütülmesi gerekmektedir. Bu çerçevede, Kanun'un 4'üncü maddesinde, kişisel veri işleme süreçlerinde uyulması gereken temel ilkeler ortaya konulmaktadır. Bu ilkeler, yapay zekâ sistemleri de dahil olmak üzere, tüm veri işleme faaliyetlerinin merkezinde yer almalı ve sürecin her aşamasında gözetilmelidir.

Öte yandan, yapay zekâ uygulamaları kapsamında gerçekleştirilen veri işleme faaliyetleri, Kanun'da belirtilen işleme şartlarına uygun bir şekilde gerçekleştirilmelidir. Bu çerçevede; ilgili kişinin açık rızasına veya Kanun'daki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda Kanun'un 10'uncu maddesi kapsamında aydınlatma yükümlülüğü yerine getirilmelidir.

Diğer taraftan, yapay zekâ uygulamalarında kişisel veri güvenliğinin sağlanması, hukuki bir yükümlülük olmasının yanında, bireylerin bu sistemlere güven duyabilmesi açısından da önem taşımaktadır. Veri sorumlularının, Kanun'un 12'nci maddesi uyarınca gerekli teknik ve idari tedbirleri etkili biçimde hayata geçirmesi bu bakımdan önemlidir. Kurumumuz tarafından yayımlanan "Kişisel Veri Güvenliği Rehberi", bu tedbirlerin uygulanmasına yönelik yol gösterici bir kaynak niteliğindedir.

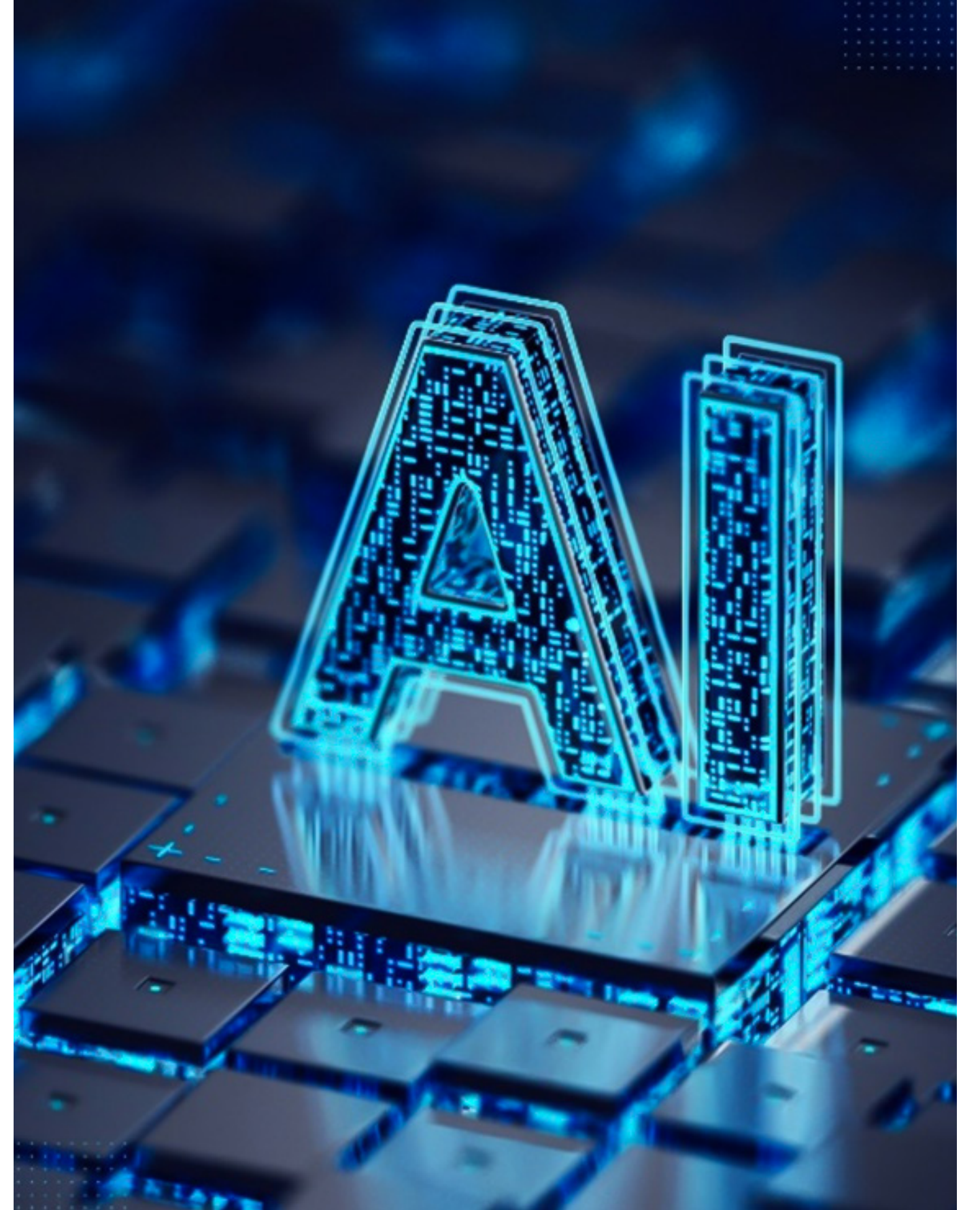
Ayrıca, Kanun'un 11'inci maddesi ile bireylere tanınan itiraz hakkı da yapay zekâ sistemleri bağlamında özel bir öneme sahiptir. Kişiler, verilerinin yalnızca otomatik sistemlerle analiz edilmesi sonucunda kendileri aleyhine bir sonucun ortaya çıkması hâlinde bu karara itiraz edebilmektedir.

İtiraz hakkı, insan müdahalesini mümkün kılması ve karar süreçlerinin denetlenebilirliğini artırması bakımından, insan odaklı yaklaşımın mevzuata yansıyan önemli bir örneğidir. İnsan odaklı yaklaşım, teknolojik süreçlerin şeffaflığını artırmayı, bireylerin kendi verileri üzerindeki kontrolünü güçlendirmeyi ve adil karar alma süreçlerini desteklemeyi amaçlamaktadır.

Bu çerçevede, itiraz hakkı bireylere yalnızca alınan kararları sorgulama imkânı tanımamakta; aynı zamanda insan müdahalesinin sürece dahil edilmesini talep etme olanağı sunarak daha adil, açıklanabilir ve bireyin haklarına saygılı sonuçların ortaya çıkmasına katkı sağlamaktadır.

Bununla birlikte, yapay zekâ gibi dinamik ve hızla gelişen teknolojiler karşısında, Kanun'un sunduğu genel çerçevenin yanı sıra, bu alana özgü daha spesifik düzenlemelere duyulan ihtiyaç giderek daha fazla gündeme gelmektedir. Bu tür düzenlemeler, yapay zekâyâ özgü risklerin, denetim mekanizmalarının ve etik ilkelerin daha açık bir şekilde ele alınmasına katkı sunabilir.

Ancak mevcut durumda, 6698 sayılı Kanun yapay zekâ sistemleri kapsamında gerçekleştirilen kişisel veri işleme faaliyetlerine uygulanmakta olup, bu süreçlere yönelik genel bir hukuki koruma sağlamaktadır. Bu teknolojilere özgü yeni düzenlemelerin hayata geçirilmesi hâlinde ise bu adımların mevcut veri koruma rejimiyle uyumlu ve tamamlayıcı nitelikte olması önem taşımaktadır.



ULUSAL YAPAY ZEKÂ STRATEJİSİ 2024-2025 EYLEM PLANI

Bilindiği üzere yapay zekâ alanında yaşanan güncel gelişmeler doğrultusunda, ülkemizin yapay zekâ alanında daha etkili adımlar atmasını sağlamak üzere Ulusal Yapay Zekâ Stratejisi 2024-2025 Eylem Planı ¹ devreye alınmıştır.

T.C. Sanayi ve Teknoloji Bakanlığı ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan söz konusu eylem planı kapsamında;

- Yapay Zekâ Uzmanlarını Yetiştirmek ve Alanda İstihdamı Artırmak
- Araştırma, Girişimcilik ve Yenilikçiliği Desteklemek
- Kaliteli Veriye ve Teknik Altyapıya Erişim İmkânlarını Genişletmek
- Sosyoekonomik Uyum Hızlandıracak Düzenlemeleri Yapmak
- Uluslararası Düzeyde İş Birliklerini Güçlendirmek
- Yapısal ve İş Gücü Dönüşümünü Hızlandırmak

stratejik öncelikler olarak belirlenmiştir.

Bu çerçevede;

- Kamu kurum ve kuruluşlarının sahip olduğu verilere ilişkin envanter çıkarılarak “Merkezi Kamu Veri Alanı” kurulması ve bu verilerin araştırmacıların ve teknoloji geliştiricilerin kullanımına sunulmasına yönelik mekanizmaların geliştirilmesi,
- Yapay zekâ ekosisteminde veri yönetişimine yönelik düzenlemelerin iyileştirilmesi,
- Yapay zekâ alanındaki uluslararası çalışmaların takip edilmesi, bu konudaki çalışmalara ülkemizce etkin katılım sağlanması ve katkı verilmesi amacıyla “Uluslararası Yapay Zekâ Çalışmaları Takip ve Koordinasyon Komitesi”nin kurulması,
- Verinin güven içerisinde serbest dolaşımına ilişkin çalışmaların takip edilmesi,

gibi pek çok eylemin gerçekleştirilmesi hedeflenmektedir.

Ayrıca eylem planında, üretken yapay zekâ teknolojilerinin geliştirilmesi; Türkçe büyük dil modellerinin ve büyük dil modellerinden yararlanılarak katma değerli ürün ve servislerin geliştirilmesi; Ar-Ge, yenilikçilik ve girişim ekosisteminin güçlendirilmesi; yüksek başarımlı hesaplama altyapılarına ve veriye erişim imkanlarının çoğaltılması; işgücünün dönüşümü ile ülkemizin uzman insan kaynağının artırılması konularına odaklanılmıştır².

¹ <https://cbddo.gov.tr/SharedFolderServer/Genel/File/UlusalYapayZekaStratejisi2024-2025EylemPlanı.pdf>

² <https://cbddo.gov.tr/duyurular/6846/ulusal-yapay-zeka-stratejisi-2024-2025-eylem-planı-yayimlandi>



KİŞİSEL VERİLERİ KORUMA KURUMUNUN YAPAY ZEKÂ KONUSUNDAKİ ÇALIŞMALARI



Kurumumuz yapay zekâ teknolojilerinin gelişimini yakından takip etmekte; bu alandaki fırsatları ve riskleri çok boyutlu bir yaklaşımla değerlendirmektedir. Önceliğimiz, teknolojik yeniliklerin kişisel verilerin korunması hakkını zedelemekten ilerlemesini sağlamak ve bu çerçevede toplumsal farkındalığı artırmaktır.

Bu kapsamda, 2021 yılında **“Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler”** dokümanı yayımlanmıştır. Bu çalışmada, yapay zekâ sistemlerinin tasarımından kullanımına kadar olan süreçlerde şeffaflık, hesap verebilirlik ve etik ilkelere bağlılık gibi temel değerlerin altı çizilmiştir.

Ayrıca insan müdahalesi, veri minimizasyonu, ayrımcılığın önlenmesi ve veri güvenliği gibi hususlara dikkat çekilerek, bireylerin mahremiyetini merkeze alan, bütüncül bir yaklaşımın hayata geçirilmesi gerektiği vurgulanmıştır.

Bunun yanında, Kurumumuz öncülüğünde hazırlanan **“Yapay Zekâ Teknolojilerine Akademik Bakış”** isimli kitap, bu alandaki çok yönlü yaklaşımımızın bir diğer göstergesidir. Farklı disiplinlerden 21 akademisyenin katkısıyla hazırlanan bu çalışmada; yapay zekânın hukuki, etik, teknik ve sektörel boyutları 5 ana başlık altında ele alınmıştır.

Bu bölümler altında; yapay zekâ teknolojilerine etik yaklaşım, yapay zekânın regülasyonu, yapay zekâ algoritmalarıyla profillemeye, yapay zekâda temel veri koruma yöntemleri ve yapay zekâda yönetim gibi çeşitli konulara yer verilmiştir.

Ayrıca, **konu ile bağlantılı olarak sohbet botları ve deepfake teknolojileri ile ilgili yayımladığımız bilgi notları da** Kurumumuzun internet sitesinde yer almaktadır.

Öte yandan, **üretken yapay zekâ sistemlerini kişisel verilerin korunması mevzuatı açısından ele alan Rehberin de** önümüzdeki süreçte kamuoyu ile paylaşılması planlanmaktadır. Bu Rehber ile bireylerin mahremiyetine saygı duyulmasını esas alan bir yaklaşımla, üretken yapay zekâ teknolojilerinin kullanımına yönelik olarak veri sorumlularına yol gösterilmesi ve bu sistemlerden faydalanan bireylere çeşitli tavsiyelerde bulunulması amaçlanmaktadır.

Farkındalık ve bilgilendirme faaliyetlerimiz de bu yaklaşımı destekleyecek şekilde sürdürülmektedir. Bugüne kadar Kurumumuz tarafından yapay zekâ temalı seminerler ve etkinlikler düzenlenmiştir.

Söz konusu seminer ve etkinliklerden başlıcaları şu şekildedir:

Kategori	Etkinlik Adı
SEMİNERLER	Yapay Zekâ Çağında Kişisel Verilerin Korunması
	Yapay Zekâ Geleceği Nasıl Şekillendirecek?
	Otonom Araçlar İçin Yapay Zekâ Teknolojilerinde Kişisel Verilerin Korunması ve Veri Mahremiyeti
	Yapay Zekâ Sistemlerinde Veri Koruma Yaklaşımları
	Yapay Zekâ Sistemleri ve Hukuki Etkileri
	Kişisel Verilerin Korunması ve Yapay Zekâ: Riskler ve Çözümler
ETKİNLİKLER	Üretken Yapay Zekânın Hukuki Boyutu: Güncel Gelişmeler ve Riskler
	Mahremiyet ve Etik İlkeler Işığında Yapay Zekâ Paneli
	Veri Korumanın 44 Yılı: Mahremiyet Perspektifinden Yapay Zekâ Çağı Konferansı
	Yapay Zekâ Teknolojilerine Akademik Bakış Kitabı Tanıtım Toplantısı
	Yapay Zekâ Çağında Kişisel Verilerin Korunması Konferansı
ULUSLARARASI ETKİNLİKLER	Yapay Zekâ Teknolojileri ve Kişisel Veriler Sempozyumu

Kurumumuz, görev alanını ilgilendiren konularda, yapay zekâ konusundaki uluslararası gelişmeleri takip etmekte ve uluslararası nitelikteki toplantılara da katılım sağlamaktadır. Katılım sağlanan uluslararası etkinliklerden bazıları şunlardır:

ULUSLARARASI ETKİNLİKLER	Yapay Zekâ Dünya Zirvesi
	CPDP Veri Koruma ve Yapay Zekâ 13. Konferansı
	İş, Yenilik, Verimlilik ve Becerilerde Yapay Zekâ Uluslararası Konferansı
	ENISA Yapay Zekâ Siber Güvenlik Konferansı
	GPA Yapay Zekâ Çalışma Grubu Toplantısı
	GPA Drafting Team Çalışma Grubu Üretici Yapay Zekâya (Generative AI) İlişkin GPA Rezolüsyonu Taslağı Toplantısı

Kurumumuz, yapay zekâ sistemlerinin insan haklarına ve temel özgürlüklere saygılı, şeffaf, denetlenebilir ve insan odaklı bir yaklaşımla geliştirilmesini ve kullanılmasını önemsemektedir. Bu doğrultuda Kurumumuz, hem mevzuatın uygulanmasına ilişkin yol göstermekte hem de kamuoyunu bilinçlendirme görevini yerine getirmektedir.

“YAPAY ZEKÂ TEKNOLOJİLERİNE AKADEMİK BAKIŞ” KİTABI ÜZERİNE KISA BİR İNCELEME



Günümüzde yapay zekâ teknolojileri başta olmak üzere dijital dönüşüm süreçleri büyük bir hızla ilerlemekte; bu gelişmelerin toplumsal yapılar, normatif sistemler ve bireylerin yaşamları üzerindeki etkisi her geçen gün daha belirgin hâle gelmektedir. Bu bağlamda, yapay zekânın teknik boyutunu ele alan çalışmaların yanı sıra toplumsal, etik ve hukuki etkilerini merkeze alan disiplinler arası akademik çalışmalara duyulan ihtiyaç da giderek artmaktadır.

Bu doğrultuda, Kurumumuz öncülüğünde hazırlanan “Yapay Zekâ Teknolojilerine Akademik Bakış” isimli çalışma, farklı disiplinlerden akademisyenlerin katkıları ile konuyu çok yönlü biçimde ele alarak literatüre katkı sunmayı hedeflemektedir.

Çalışmada amaçlanan temel hususlar arasında şunlar yer almaktadır:

- » Yapay zekânın kavramsal ve tarihsel temellerinin açıklanması,
- » Yapay zekâyâ ilişkin düzenleme eğilimlerinin değerlendirilmesi,
- » Yapay zekânın etik ve sosyal boyutlarının değerlendirilmesi suretiyle teknolojinin sorumlu kullanımına yönelik yol gösterilmesi,
- » Yapay zekâ alanındaki gelişmelerin veri koruma hukuku düzenlemeleri ile uyumlu bir şekilde nasıl ele alınabileceğinin incelenmesi,
- » Çeşitli sektörler özelinde yapay zekâ kullanımlarının ele alınması.

Bu kapsamda çalışma 5 ana bölümden oluşmaktadır:

- Yapay Zekâ ve Makine Öğrenmesine Giriş
- Yapay Zekâ ve Hukuk: Etik İlkeler, Hukuki Çerçeve ve Sorumluluk
- Yapay Zekâ Sistemlerinde Kişisel Verilerin İşlenmesi
- Yapay Zekânın Sektörel Uygulamaları
- Yapay Zekâda Yönetişim ve Metodoloji

İlgili bölümler kapsamında, alanında uzman 21 akademisyen tarafından kaleme alınan toplam 15 makale yer almaktadır.

Çalışmada Yer Alan Makaleler

- Yapay Zekâ ve Makine Öğrenmesine Giriş
- Yapay Zekâ Teknolojilerine Etik Yaklaşım
- Kodlar ve Kanunlar: Yapay Zekânın Regülasyon Rotası ve AB Yapay Zekâ Tüzüğü
- Yapay Zekânın Yol Açtığı Zararlardan Hukuki Sorumluluk
- Veri Koruma Hukukunun Temel Prensipleri ve Yapay Zekâ Uygulamaları Açısından Değerlendirilmesi
- Yapay Zekâ Algoritmalarıyla Profillemeye ve Kişisel Verilerin Korunması
- Yapay Zekâ ve Temel Veri Koruma Yöntemleri
- Hassas Gruplar [Çocuklar, Yaşlılar, Engelli Bireyler] için Geliştirilen Yapay Zekâ Uygulamalarında Dikkat Edilmesi Gereken Etmenler
- Sağlık Alanında Yapay Zekâ ve Kişisel Veriler
- İstihdamda Yapay Zekâ
- Öneri Modellerinin KVKK ile Uyumu
- Ulaşım Sektöründe Yapay Zekâ
- Finans Sektöründe Yapay Zekâ Kullanımı: Kişisel Verilerin Korunması Odağında Bir Değerlendirme
- Eğitimde Yapay Zekâ
- Yapay Zekâda Yönetişim ve Metodoloji

GENEL OLARAK ÜRETKEN YAPAY ZEKÂ

Son yıllarda hızla gelişen üretken yapay zekâ teknolojileri, hayatımızın birçok alanında hız ve verimlilik sağlayarak bilgiye erişimi kolaylaştırmakta ve yeni imkânlar sunmaktadır.

Genel olarak bakıldığında, “üretken/üretici yapay zekâ” [*generative artificial intelligence*]; büyük ölçekli veri kümeleri üzerinde eğitilen ve kullanıcının girdiği bir istem ya da komuta [*prompt*] yanıt olarak farklı formatlarda içerikler oluşturabilen yapay zekâ türünü ifade etmektedir.

Üretken yapay zekâ, birçok alanda dönüşüm sağlayarak yenilikçi çözümler sunan bir teknolojidir. Farklı formatlarda zengin içerikler oluşturma yeteneği sayesinde iş süreçlerini yeniden şekillendiren bu sistemler, geleneksel yöntemlerin ötesine geçerek inovatif ve işlevsel uygulamalara zemin hazırlamaktadır. Özellikle genel talimatlardan içerik üretme, mevcut içerikleri yeniden işleme ve veri analizi gibi temel görevleri yerine getirme kapasitesi; üretken yapay zekâyı hem kullanıcıların üretkenlik potansiyelini artıran hem de yeni sistemler geliştirilmesine katkı sağlayan bir araç hâline getirmektedir. Bu yönüyle üretken yapay zekâ, gerek mevcut iş modellerinin dönüştürülmesine gerekse farklı alanlarda alternatif yaklaşımlar geliştirilmesine olanak tanımaktadır.

Üretken yapay zekâ ile çeşitli alanlarda birçok türde içerik oluşturulabilmekte olup bu kullanım alanlarından bazıları şu şekilde özetlenebilir:

- » **Metin Oluşturma:** Doğal dil işleme tekniklerine dayanan bu sistemler; kullanıcı girdileri doğrultusunda özet çıkarma, makale yazma, soru-cevap formatında metin üretme gibi görevleri yerine getirebilmektedir. Bu bağlamda içerik üretimi, müşteri hizmetleri sohbet botları ve dil temelli uygulamalarda önemli işlevler üstlenmektedir.
- » **Görüntü ve Video Oluşturma:** Kullanıcıdan alınan metinsel açıklamalara dayalı olarak görsel ve video içerikleri üretebilen modeller aracılığıyla sanat eserleri, illüstrasyonlar, animasyonlar, konsept tasarımlar ve video içerikleri oluşturulabilmektedir. Dijital sanat, grafik tasarım ve reklamcılık gibi alanlarda yenilikçi çözümler sunmaktadır.
- » **Ses ve Müzik Üretimi:** Mevcut ses verileri üzerinde eğitilen bu modeller; yeni ses efektleri, konuşmalar veya müzik eserleri oluşturabilmektedir. Bu bağlamda eğlence sektörü, dijital içerik üretimi ve oyun endüstrisi gibi alanlar, bu teknolojiyen en çok yararlanan alanlar arasında yer almaktadır.
- » **Yazılım Kodu Oluşturma:** Yazılım geliştirme süreçlerini desteklemek amacıyla kullanılan üretken yapay zekâ modelleri; kod üretme, programlama dilleri arasında çeviri yapma, kod tamamlama, işlevsel modül geliştirme, hata ayıklama ve optimizasyon gibi çeşitli görevleri yerine getirebilmektedir. Bu yönüyle yazılım geliştiricilere zaman kazandırmakta ve üretkenliği artırmaktadır.



Üretken yapay zekâ sistemlerinden elde edilen çıktıların her durumda doğru, tarafsız veya tutarlı olmayabileceği göz önünde bulundurulmalıdır. Bu sistemler, gerçeklikle örtüşmeyen ancak çoğu zaman oldukça makul ve ikna edici görünen bilgiler üretebilmekte olduğundan üretilen içeriklerin doğruluğunun kontrol edilmesi önem taşımaktadır.

ÜRETKEN YAPAY ZEKÂDAN YARARLANIRKEN KİŞİSEL VERİLERİN KORUNMASI BAKIMINDAN BİREYLERİN DİKKAT ETMESİ GEREKEN BAZI HUSUSLAR

Üretken yapay zekâ teknolojileri, farklı içerik türlerinin hızlı ve kolay bir şekilde üretilmesine olanak tanıyarak çeşitli alanlarda önemli avantajlar sağlamakla birlikte, bu sistemlerden yararlanırken veri güvenliği, gizlilik ve kişisel verilerin korunması gibi hususlara dikkat edilmesi önem taşımaktadır.

ÜRETKEN YAPAY ZEKÂDAN GÜVENLİ BİR ŞEKİLDE YARARLANMAK İÇİN HANGİ ÖNLEMLERİ ALABİLİRSİNİZ?

KİŞİSEL VERİLERİN PAYLAŞIMI KONUSUNDA DİKKATLİ OLUNUZ

Üretken yapay zekâ sistemlerine bilgi sağlarken; ad-soyad, adres, telefon numarası, kimlik bilgileri gibi kişisel verilerinizi paylaşmaktan kaçınınız. Özel hayatınıza ilişkin bilgilerin bu sistemlerle paylaşılması, veri güvenliğinizi açısından önemli bir adımdır.

ANONİM VE GENEL İFADELER KULLANMAYI TERCİH EDİNİZ

Paylaşacağınız bilgileri mümkün olduğunca anonim ve genel ifadelerle aktarmaya özen gösteriniz. Örneğin, belirli bir olaya dair bilgi paylaşırken, kişiye veya zamana özgü detaylar yerine genel bir çerçeve sunulması daha güvenli bir yöntem olacaktır. Bu yaklaşım, kişisel verilerin doğrudan paylaşılmasını önlemede etkili bir yöntemdir.

KİŞİSEL VERİ PAYLAŞIM İZİNLERİNİ KONTROL EDİNİZ

Üretken yapay zekâ sistemlerinin veri toplama ve saklama politikalarını dikkatli bir şekilde inceleyiniz. Mümkün olduğunca, veri paylaşımını en aza indirecek gizlilik ayarlarını tercih ediniz.

HASSAS KONULARDA YAPAY ZEKÂ KULLANIMINA DİKKAT EDİNİZ

Sağlık bilgileri, finansal veriler veya hukuki süreçlerle ilgili verilerinizi paylaşmadan önce dikkatli olunuz. Bu tür bilgilerin gizliliğinin ihlal edilmesi, ciddi güvenlik risklerine yol açabilir.

Üretken yapay zekâ teknolojileri, doğru ve bilinçli kullanıldığında önemli avantajlar sunmaktadır. Ancak, kişisel verilerin korunması, mahremiyetin güvence altına alınması ve veri güvenliğine yönelik risklerin en aza indirilmesi, bu sistemlerin güvenli bir şekilde kullanılması açısından temel gerekliliklerdendir.

Unutulmamalıdır ki; teknolojik gelişmelerin insan odaklı, etik değerlere uygun ve mahremiyet bilinciyle şekillendirilmesi, bireylerin hak ve özgürlüklerinin korunarak teknolojinin faydalarından en iyi şekilde yararlanılmasını sağlayacaktır.

AVRUPA BİRLİĞİ VE YAPAY ZEKÂ REGÜLASYONU: YAPAY ZEKÂ TÜZÜĞÜ MERCEĞİNDEN TEMEL BİLGİLER

Yapay zekânın her gün gelişmesi ve kullanımının yaygınlaşmasıyla birlikte yapay zekânın tabi olduğu hukuki çerçevenin tartışılması yanında özellikle yapay zekâyı hedef alan düzenlemelerin de yapılması gündeme gelmektedir. Bu alanda en öne çıkan düzenleme ise bir Avrupa Birliği (AB) düzenlemesi olan [EU] 2024/1689 sayılı ve 13 Haziran 2024 tarihli yapay zekâya ilişkin yeknesak kuralları belirleyen Avrupa Parlamentosu ve Konseyi tüzüğüdür. Bu düzenleme her ne kadar kısaltılmış ismi [İng. Artificial Intelligence Act] sebebiyle “Yapay Zekâ Yasası” olarak anılsa da esasen bir ulus devlet yasası değil Avrupa Birliği tüzüğü niteliğindedir. Bu sebeple çalışmada kısaca Yapay Zekâ Tüzüğü (YZT) olarak anılacaktır.

Yapay Zekâ Tüzüğü nedir?

YZT, AB seviyesinde yapay zekâ sistemi ve genel amaçlı yapay zekâ modeli olarak adlandırılan yapay zekâ uygulamalarının piyasaya sürülmesi ya da hizmete sunulması için belirli kurallar öngören, bazı uygulamaları ise yasaklayan ve temelinde ürün güvenliği yaklaşımını benimseyen bir düzenlemedir. YZT yapay zekânın her alanını düzenleyen genel bir düzenleme değildir. YZT içerisinde yapay zekâ kaynaklı sorumluluk veya fikir ve sanat eserlerinin yapay zekâ ile kullanılması gibi önemli ve tartışmalı birçok alanda düzenleme bulunmamaktadır.

Yapay Zekâ Tüzüğü ne zaman uygulanacak?

YZT 12.07.2024’te Avrupa Birliği Resmî Gazetesi’nde yayımlanmış ve 01.08.2024’te tamamen yürürlüğe girmiştir. Ancak getirdiği düzenlemelerin gerektirdiği hazırlıkların yapılması için aynı Avrupa Birliği Genel Veri Koruma Tüzüğü’nde [GVKT] olduğu gibi kademeli bir uygulama çerçevesi öngörülmüş olup istisnai bazı düzenlemeler haricinde YZT’nin büyük kısmı 02.08.2026’dan itibaren uygulanmaya başlayacaktır. Bu çalışmanın yazım tarihi itibarıyla ise sadece ilk beş madde uygulanmaya başlamıştır.

Yapay Zekâ Tüzüğü’nün kapsamı nedir?

YZT yapay zekâ olarak adlandırılan tüm sistem ya da uygulamaları da kapsamamaktadır. YZT’nin hem sistem bakımından hem aktör bakımından hem de coğrafi kapsam kriterleri mevcuttur. YZT’nin uygulanabilmesi için kural olarak üç olumlu bir olumsuz şart aranmaktadır: [i] Ortada bir yapay zekâ sistemi ya da genel amaçlı yapay zekâ modeli bulunmalıdır. Bir yapay zekâ uygulamasının bunlardan biri kapsamında olup olmadığı her somut olayda ayrıca incelenmelidir. [ii] YZT kapsamında kalan bir aktör bulunmalıdır. YZT başta sağlayıcı [İng. provider] ve yerleştirici [İng. deployer] olmak üzere yapay zekânın tedarik zincirindeki sınırlı sayıda aktöre uygulanmaktadır. Kural olarak son kullanıcıya yönelik bir düzenleme ise içermemektedir. [iii] YZT’nin coğrafi uygulama alanı değerlendirilmelidir.

Sağlayıcılar için önemli olan sağlayıcının konumundan bağımsız olarak sistemin AB içerisinde sunulması iken yerleştiricilerin AB içerisinde olması aranmıştır. Dahası YZT, sistem ve aktör dışında olsa bile sistem çıktısının AB içerisinde kullanılacak olması durumunda da uygulanacaktır. Bu itibarla YZT Türkiye’de yer alan operatörlere de uygulanabilecektir. [iv] Olumsuz şart olarak ise YZT kapsamında yer alan istisnalardan birinin mevcut olmaması gerekmektedir. YZT m. 2’de AR-GE ya da açık ve ücretsiz lisans gibi durumlar için bazı istisnalar öngörmüştür.

Yapay Zekâ Tüzüğü neler getirmektedir?

YZT, kapsamda kalan yapay zekâ sistemleri ve genel amaçlı modelleri için risk temelli bir yaklaşım benimsemektedir. Buna göre yapay zekâ sistemleri üç temel risk grubuna ayrılmaktadır: [i] Bazı uygulamalar YZT m. 5 uyarınca yasaklanmıştır. Bunlar sınırlı sayıda ancak yoruma açık uygulamalar olup bunlara örnek olarak kamusal alanlarda kolluk faaliyeti icrası amacıyla gerçek zamanlı biyometrik tanıma veya kişileri normalde vermeyecekleri kararlar vermeye iterek zarara sebep olabilecek manipülatif uygulamalar verilebilir. [ii] Yapay zekâ sistemleri için öngörülen ikinci risk grubu ise yüksek riskli sistemlerdir. Bu sistemler YZT’nin Ek-I’inde yer alan AB ürün güvenliği düzenlemelerine ve Ek-III’ünde yer alan sekiz adet temel kullanım alanına göre belirlenmektedir. Bu kullanım alanlarına örnek olarak yasaklanmamış biyometrik kullanımlar, işe alım ve istihdam ya da eğitim ve mesleki eğitim alanında kullanımlar gösterilebilir. Bu itibarla işe alınacak kişilerin seçiminde ya da öğretim faaliyetlerinin değerlendirilmesinde yapay zekânın kullanımı yüksek riskli olarak kabul edilecektir. [iii] Sistemleri için öngörülen üçüncü ve son risk grubu ise yasaklanmış ve yüksek riskli olanlar dışında kalan ve YZT’de bu şekilde anılmasa da genel olarak düşük riskli sistemler olarak adlandırılan diğer sistemlerdir.

YZT, ilk grup sistemlerin AB içerisinde piyasaya sürülmesini ya da hizmete sunulmasını yasaklamakta, son gruptaki sistemler için ise YZT m. 4’te yer alan yapay zekâ okuryazarlığı haricinde sağlayıcı yükümlülük getirmemektedir. YZT’nin odağında yüksek riskli sistemler bulunmaktadır. YZT yüksek riskli yapay zekâ sistemlerinin tedarik zincirindeki aktörlere birtakım yükümlülükler yüklemektedir. Burada en öne çıkan aktör sağlayıcıdır. Sağlayıcı bir yapay zekâ sistemini, kendi geliştirmiş olsun ya da olmasın, kendi adıyla ya da markası altında piyasaya süren kişidir. Yüksek riskli yapay zekâ sistem sağlayıcısı hem YZT m. 16’da sayılan kalite yönetim sistemi kurma gibi yükümlülüklerle uygun davranmalı hem de bunun parçası olarak sağladığı sistemin YZT m. 8-15 arasında düzenlenen ve veri yönetimi, risk yönetim sistemi, siber güvenlik gibi teknik gereksinimlere uygunluğunu temin etmelidir. Yerleştiricilerin yükümlülükleri daha az katı olmakla birlikte en öne çıkan bazı yerleştiriciler için öngörülen temel haklar etki değerlendirmesi yapma yükümlülüğüdür. Bu, söz konusu sistemin veri ile kısıtlı olmaksızın etkilerine yönelik bir değerlendirme olup aynı zamanda kişisel veri işleniyorsa GVKT uyarınca yapılması gerekli olabilecek veri koruma etki değerlendirmesi ile karıştırılmaması gerekir.

YZT bazı sistemlerin işleyişi itibarıyla de ek şeffaflık yükümlülükleri getirmektedir. Bu sistemler YZT m. 50’de düzenlenmekte olup genelde doğrudan insanlarla etkileşime geçen ya da geçecek şekilde içerik üreten sistemlerdir. Bunlar YZT’nin ifadesi olmamakla birlikte “sınırlı risk” ya da “şeffaflık riski” taşıyan sistemler olarak da adlandırılmaktadır. Önemli olan husus bu yükümlülüklerin diğer risk gruplarını dışlayıcı olmamasıdır. Bir yapay zekâ sistemi üç temel risk grubundan sadece bir tanesine girebilir. Ancak YZT m. 50’de yer alan yükümlülükler sistemin işleyişine göre yasaklanmış olmayan tüm sistemlerin sağlayıcılarına uygulanabilir.

YZT genel amaçlı modeller için de ikili bir sınıflandırma öngörmekte ve sağlayıcılara buna göre yükümlülükler yüklemektedir. Tüm genel amaçlı sistem sağlayıcıları için YZT m. 53'te aralarında teknik dokümantasyon ve sistemi entegre edecek olanlar için bilgilendirme oluşturmak da dahil olmak üzere dört temel yükümlülük düzenlenmiştir. Buna ek olarak, yüksek etki doğurabilecek sistemler YZT altında sistemik risk taşıyan genel amaçlı modeller olarak sınıflandırılmış ve bunların sağlayıcıları için YZT m. 55'te dört adet ek yükümlülük getirilmiştir. Sistemik risk taşımanın tespiti ise modelin geliştirilmesinde kullanılan toplam işlem gücü gibi unsurlara bağlanmıştır.

Yapay Zekâ Tüzüğü'nün ihlali durumunda yaptırım nedir?

YZT'nin ihlali idari para cezası yaptırımına bağlanmıştır. İdari para cezalarının tutarının Üye Devletler tarafından belirleneceği öngörülmüş, ancak ilgili yükümlülüklerin tabi olduğu risk gruplarına ve ilgili operatörlere göre YZT m. 99'da belirli alt ve üst sınırlar belirlenmiştir. Ayrıca Üye Devletlerin YZT'nin etkin şekilde uygulanabilmesi uyarı ve parasal olmayan diğer yaptırımlar da öngörebileceği düzenleme altına alınmıştır.

Yapay Zekâ Tüzüğü'nün kişisel verilerin korunması ve Avrupa Genel Veri Koruma Tüzüğü ile ilişkisi nedir?

YZT kişisel verilerin korunmasına ilişkin de detaylı düzenlemeler içermemekte, açıkça YZT kapsamında kalan uygulamalarda kişisel veri işlenmesi halinde GVKT'nin uygulanacağını belirtmektedir. YZT, kişisel veri ve biyometrik veri gibi kavramların tanımı için de GVKT'ye ve ilgili olan diğer bazı noktalarda 2016/680 sayılı kolluk yönergesine atıf yapmaktadır. Diğer yandan YZT'nin kişisel verilerin işlenmesiyle ilişkisinde üç temel noktaya dikkat edilmesi faydalı olacaktır.

İlk olarak YZT kapsamında bazı sistemler için öngörülen veri yönetim yükümlülükleri hem kişisel hem de kişisel olmayan veriler için uygulanacaktır. Bu itibarla kişisel veri işleyerek yapay zekâ geliştiriliyorsa aslında hem GVKT hem de YZT'nin veri yükümlülüklerine dikkat edilmelidir.

İkinci olarak, yapay zekâ ile kişisel verilerin işlenmesi GVKT kapsamında yüksek riskli işleme olarak sınıflandırılabilenlerinden buna özel GVKT kapsamında veri koruma etki değerlendirmesi yapılabilecektir. Bu değerlendirme bazı yerleştiriciler için öngörülen temel haklar etki değerlendirmesi ile karıştırılmamalıdır. Ancak YZT m. 27'de açıkça belirtildiği üzere kesişme olan noktalarda temel haklar etki değerlendirmesi GVKT kapsamında yapılacak veri koruma etki değerlendirmesini tamamlayıcı nitelikte olacaktır.

Üçüncü ve son olarak, YZT sadece iki özel alanda GVKT'ye ek kişisel veri işleme şartı getirmektedir. Bunlardan ilki YZT m. 10[5] uyarınca önyargıların tespiti ve giderilmesi için katı surette gerekli olduğu ölçüde ve yine aynı madde altında sayılan şartlara uygun olarak özel nitelikli kişisel verilerin işlenmesine ilişkindir. İkinci veri işleme dayanağı ise başka amaçlar için işlenmek üzere hukuka uygun şekilde elde edilmiş olan verilerin YZT m. 59'da sayılan koşullarda bir düzenleme deneme alanı (İng. regulatory sandbox) içerisinde münhasıran bazı sistemlerin geliştirilmesi ve test edilmesi amacıyla işlenebilmesine ilişkindir. Bu haller dışında yapay zekâ ile veya yapay zekâ için kişisel veri işlenmesinde ise kural olarak GVKT'de yer alan hukuki sebeplerden birine dayanılması gerekecektir.



KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ

ÖNE ÇIKAN
GELİŞMELER

- * Ülkemizde, 7545 sayılı Siber Güvenlik Kanunu 19.03.2025 tarih ve 32846 sayılı Resmî Gazete’de yayımlandı¹.
- * Avrupa Veri Koruma Kurulu [EDPB], bağlayıcı şirket kurallarının onaylanmasına ilişkin prosedürün ortaya konulduğu dokümanı yayımladı².
- * İspanya Veri Koruma Otoritesi [AEPD], yapay zekâya ilişkin hatalı algıların ele alındığı bir içerik yayımladı³. Ağırlıklı olarak üretken yapay zekâ kapsamında değerlendirmelere yer verilen içerikte, özellikle Birleşik Krallık Veri Koruma Otoritesi’nin [ICO] üretken yapay zekâya ilişkin gerçekleştirdiği danışma sürecinin devamında açıklanan hususlara odaklanılmaktadır.
- * Bağımsız uzmanlar tarafından hazırlanan genel amaçlı yapay zekâ uygulama kurallarının üçüncü taslağı yayımlandı⁴. Taslak, AB Yapay Zekâ Tüzüğü ile uyumlu olarak genel amaçlı yapay zekâ modellerinin sağlayıcıları için şeffaflık ve telif hakkı yükümlülüklerini detaylandırmakta; sistemik risk taşıyan genel amaçlı yapay zekâ modellerinin sağlayıcıları için ise güvenlik ve emniyet önlemlerini içermektedir. Üçüncü taslağın, önceki versiyonlara kıyasla daha sade bir yapı sunduğu ve somut önlemler barındırdığı belirtilmektedir.

1 <https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm>, 19.03.2025.

2 https://www.edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-setting-forth-co-operation-procedure-approval_en, 19.03.2025.

3 <https://www.aepd.es/en/press-and-communication/blog/addressing-misconceptions-%20of-artificial-intelligence>, 11.03.2025.

4 <https://digital-strategy.ec.europa.eu/en/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts>, 11.03.2025.

- * AB Yapay Zekâ Ofisi, AB Yapay Zekâ Tüzüğü’nün belirli hükümlerinin yorumlanmasını kolaylaştırmak amacıyla, genel amaçlı yapay zekâ modellerine ilişkin bağlayıcı olmayan bir soru-cevap dokümanı yayımladı⁵.

- * Avrupa Komisyonu, “*AI Continent Action Plan*” adını verdiği kapsamlı bir eylem planının hayata geçirildiğini açıkladı⁶. Bahse konu eylem planının temel girişimleri arasında;

- » Büyük ölçekli bir yapay zekâ veri ve bilgi işlem altyapısı oluşturulması,
- » Büyük ve yüksek kaliteli verilere erişimin artırılması,
- » Stratejik sektörlerde algoritmalar geliştirilmesi ve yapay zekânın benimsenmesinin teşvik edilmesi,
- » Yapay zekâyâ ilişkin becerilerin ve yeteneklerin güçlendirilmesi,
- » Düzenlemelerin sadeleştirilmesi yer almaktadır.

Konuya ilişkin olarak Komisyon tarafından yapılan açıklamada, AB’nin yapay zekâ politikaları ve mevcut uygulamalara ilişkin olarak iki farklı konuda kamuoyunun görüşüne başvurulduğu belirtilmektedir.

- * Avrupa Veri Koruma Kurulu [EDPB], Hırvatistan Veri Koruma Otoritesi’nin talebi üzerine, “Uzman Destek Havuzu” [*Support Pool of Experts*] programı kapsamında, büyük dil modellerine [LLM] ilişkin gizlilik risklerinin belirlenmesi, değerlendirilmesi ve bunların azaltılmasına yönelik kapsamlı bir risk yönetimi metodolojisinin ortaya konulduğu bir rapor yayımladı⁷.

- * Hong Kong Veri Koruma Otoritesi [PCPD], çalışanlar tarafından iş yerinde üretken yapay zekâ kullanımına ilişkin yönergeler konusunda bir kontrol listesi yayımladı⁸.

- * Kolombiya, yapay zekânın etik ilkelere ve insan haklarına riayet edilerek yargı sistemlerine entegre edilmesini hedefleyen bir çerçeve olan UNESCO’nun Yargı Sistemlerinde Yapay Zekâ Kullanımına İlişkin Yönergelerini benimseyen ilk ülke oldu⁹.

- * Avrupa Komisyonu, AB Yapay Zekâ Tüzüğü’nün 4. maddesi kapsamında düzenlenen yapay zekâ okuryazarlığına ilişkin bir soru-cevap dokümanı yayımladı¹⁰. Söz konusu madde uyarınca; yapay zekâ sistemlerinin sağlayıcıları ile bu sistemleri -kişisel amaçlı ve mesleki niteliği bulunmayan faaliyetler dışında- kendi yetki alanları dahilinde kullanan kişi/kuruluşlar [*deployers*], çalışanlarının ve kendi adlarına bu sistemlerin kullanımıyla ilgilenen diğer kişilerin yeterli düzeyde yapay zekâ okuryazarlığına sahip olmalarını temin etmekle yükümlüdür.

5 <https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers>, 14.03.2025.

6 https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1013, 09.04.2025.

7 https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-privacy-risks-mitigations-large_en, 10.04.2025.

8 https://www.pcpd.org.hk/english/news_events/media_statements/press_20250331.html, 31.03.2025.

9 <https://www.unesco.org/en/articles/justice-meets-innovation-colombias-groundbreaking-ai-guidelines-courts>, 01.04.2025.

10 <https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers>, 07.05.2025.

* ABD Ulusal Güvenlik Ajansı; Avustralya, Yeni Zelanda ve Birleşik Krallık'ın siber güvenlik kurumlarıyla birlikte hazırlanan "Yapay Zekâda Veri Güvenliği: Yapay Zekâ Sistemlerinin Eğitimi ve İşletilmesinde Kullanılan Verilerin Güvenliğini Sağlamaya Yönelik En İyi Uygulamalar" başlıklı belgeyi yayımladı¹¹. Bahse konu belgede, yapay zekâ sistemlerinin yaşam döngüsü ile bu çerçevede karşılaşılabilecek riskler ele alınmakta ve NIST Yapay Zekâ Risk Yönetimi Çerçevesi ile uyumlu bir şekilde yapay zekâ geliştirme, test etme ve işletme süreçlerinde verilerin güvenliğini sağlamak için öneriler sunulmaktadır.

Bu çerçevede başlıca öneriler arasında; güvenilir veri kaynaklarının kullanılması, veri bütünlüğünün korunması, dijital imzaların uygulamaya alınması, erişim kontrollerinin kullanılması, verilerin şifrelenmesi ve devamlı şekilde risk değerlendirmeleri yapılması yer almaktadır.

* Avrupa Veri Koruma Kurulu (EDPB), blokzinciri teknolojileri aracılığıyla kişisel verilerin işlenmesine ilişkin hazırlanan rehberin kamuoyu görüşüne açıldığını duyurdu¹². Bahse konu rehberde; blokzinciri teknolojisinin işleyişi, bu teknoloji kapsamında gerçekleştirilen veri işleme faaliyetlerinin hukuka uygunluğu ile ilgili kişilerin haklarını kullanmalarının sağlanması gibi başlıklara yer verilmekte ve veri işleme faaliyetinde rol alan aktörlere yönelik çeşitli tavsiyelerde bulunmaktadır.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), kişisel verilerin güvenli bir şekilde işlenmesini sağlamaya yönelik teknik bir önlem olarak "şifreleme" yöntemine ilişkin güncellenmiş taslak rehberin kamuoyu görüşüne açıldığını duyurdu¹³.

* Avrupa Birliği Adalet Divanı, "Önemli Kararlar Seçkisi"nin 2024 yılına ait versiyonunu yayımladı¹⁴. Geçtiğimiz yıl içerisinde verilen önemli kararların özetlerini içeren bu seçkide, kişisel verilerin korunmasına ilişkin seçilmiş kararlara da yer verilmektedir. Bu çerçevede; elektronik haberleşme verilerinin işlenmesi, biyometrik ve genetik veriler, AB Genel Veri Koruma Tüzüğü'nün kapsamı, veri sorumlusu kavramı ile Tüzük'ün ihlali durumunda başvurulabilecek hukuki yollara ilişkin seçilmiş kararlar açıklanmaktadır.

* Avrupa Birliği Adalet Divanı, kişisel verilerin korunmasına ilişkin olarak çeşitli ana başlıklar altında sınıflandırılan çok sayıda kararın özetini içeren bir doküman yayımladı¹⁵. Bu kapsamda bahse konu dokümanda;

- » Avrupa Birliği Temel Haklar Şartı ile tanınan kişisel verilerin korunması hakkı,
- » Genel düzenlemeler çerçevesinde kişisel verilerin işlenmesi,
- » Sektöre özgü düzenlemeler çerçevesinde kişisel verilerin işlenmesi,
- » Kişisel verilerin üçüncü ülkelere aktarılması,
- » İnternet ortamında kişisel verilerin korunması
- » Ulusal denetim otoriteleri

başlıkları altında, kişisel verilerin korunması alanında Avrupa Birliği hukukunun gelişimine yön veren çok sayıda karar özetlenmektedir.

- 11 <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4192332/nsas-aisc-releases-joint-guidance-on-the-risks-and-best-practices-in-ai-data-se/>, 22.05.2025.
- 12 https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en, 14.04.2025.
- 13 <https://ico.org.uk/media2/bv1hbcra/encryption-all-2-0-4.pdf>, 13.05.2025.
- 14 https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-04/en_grand_arrets_2024.pdf.
- 15 https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf.

* Avrupa Veri Koruma Kurulu (EDPB) ve Avrupa Veri Koruma Denetçisi (EDPS), AB Genel Veri Koruma Tüzüğü kapsamında kayıt tutma yükümlülüklerinin basitleştirilmesi önerisine ilişkin olarak Avrupa Komisyonuna hitaben yazılan mektubu yayımladı¹⁶.

* Avrupa Veri Koruma Kurulu (EDPB) ile Avrupa Veri Koruma Denetçisi (EDPS), 2024 yılına ilişkin faaliyet raporlarını yayımladı¹⁷.

* İrlanda Veri Koruma Otoritesi (DPC), AB Genel Veri Koruma Tüzüğü'nün (GDPR) 15'inci maddesi uyarınca ilgili kişilerin erişim hakkı taleplerinin ele alınmasına ilişkin yaklaşımın detaylandırıldığı bir içerik yayımladı¹⁸.

* Avrupa Veri Koruma Denetçisi (EDPS), Avrupa Veri Koruma Kurulu (EDPB) tarafından başlatılan 2025 yılı Koordineli Uygulama Çerçevesi (Coordinated Enforcement Framework) eylemine katılacağını duyurdu¹⁹.

Hatırlanacak olursa EDPB tarafından geçtiğimiz Mart ayı içerisinde yapılan duyuruda; bu yıl AB Genel Veri Koruma Tüzüğü'nün (GDPR) 17'nci maddesi kapsamında "silme hakkı (unutulma hakkı)"nın uygulanmasının ele alınacağı, bu çerçevede yıl içerisinde 30 veri koruma otoritesinin çeşitli sektörlerdeki veri sorumlularını inceleyeceği, verilerin silinmesi yönündeki taleplerin veri sorumlularınca nasıl ele alındığının ve bu hakkın kullanılmasına ilişkin koşullar ile istisnaların nasıl uygulandığının değerlendirileceği, süreç boyunca veri koruma otoritelerinin bulgularını paylaşacakları ve gerekli analizlerin gerçekleştirileceği ifade edilmişti²⁰.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), finansal hizmetler kapsamında çocukların kişisel verilerinin işlenmesine ilişkin olarak 40'tan fazla finansal kuruluş üzerinde gerçekleştirdiği incelemenin bulgularını yayımladı²¹. Bulgular arasında; katılımcıların %49'u çocuklara yaşlarına uygun bilgilendirme sağladığını belirtmesine rağmen, dörtte birinden daha azının bu bilgilendirmenin çocuklar tarafından ne derece anlaşılabilir olduğunu test ettiği, "çocuk dostu" olarak nitelendirilen bilgilendirmelerin dahi mesleki dil içerdiği veya yetişkinlere yönelik metinlerin yalnızca sadeleştirilmiş versiyonları olduğu, ayrıca katılımcıların %66'sının bilgilendirmenin çocuk tarafından anlaşılmasının ebeveynin sorumluluğunda olduğunu ifade ettiği gibi hususlar yer almaktadır.

Bu çerçevede; çocuklara yönelik yapılacak bilgilendirmede açık ve sade bir dil kullanılması, mesleki jargondan kaçınılması, yalnızca o anda ihtiyaç duyabilecekleri bilgilerin paylaşılması, farklı yaş grupları için farklı sürümler hazırlanması, doğru uygulamaların tek seferlikten ziyade sürekli bir yaklaşım olarak benimsenmesi, temel bilgilerin daha ilgi çekici biçimlerde sunulması (örneğin görseller, çizgi filmler, diyagramlar, videolar aracılığıyla) ve bilgilendirmelerin anlaşılabilirliğini değerlendirmek amacıyla gerektiğinde çocuklarla test edilmesi yönünde önerilerde bulunmaktadır.

* Avrupa Komisyonu Ortak Araştırma Merkezi (JRC), disiplinler arası bir bakış açısıyla çocukların sağlığı ve sosyal medya kullanımı arasındaki ilişkinin ele alındığı bir çalışma yayımladı²². Sosyal medya kullanımının çocukların zihinsel ve fiziksel sağlığı üzerindeki etkilerinin incelendiği çalışmada ebeveynler, eğitimciler ve çevrim içi platformlar da dahil olmak üzere farklı gruplara yönelik önerilere yer verilmektedir. Bu öneriler arasında; genel olarak farkındalığın artırılması, içerik denetimi sağlanması, yaş doğrulama süreçlerinin etkin bir şekilde hayata geçirilmesi ve hizmet sağlayıcılar ile araştırmacılar arasındaki iş birliklerinin güçlendirilmesi gibi hususlar bulunmaktadır.

* Avrupa Parlamentosu Araştırma Servisi (EPRS), çocukların çevrim içi ortamda korunmasına yönelik seçilmiş AB stratejileri ve bildirgeleri, ilgili AB mevzuatı, ulusal ve bölgesel düzeydeki düzenleme ve girişimler ile farkındalık artırmaya yönelik faaliyetlerin ele alındığı bir çalışma yayımladı²³.

16 https://www.edpb.europa.eu/news/news/2025/simplification-record-keeping-obligation-edpb-and-edps-adopt-letter-eu-commission_en, 08.05.2025.

17 Avrupa Veri Koruma Kurulu tarafından yayımlanan rapor için bkz. https://www.edpb.europa.eu/system/files/2025-04/edpb-annual-report-2024_en.pdf; Avrupa Veri Koruma Denetçisi tarafından yayımlanan rapor için bkz. https://www.edps.europa.eu/system/files/2025-04/edps_annual_report-2024_en.pdf.

18 <https://www.dataprotection.ie/en/dpc-guidance/blogs/DPC-handling-of-Subject-Access-Requests>, 07.03.2025.

19 https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/edps-participates-fourth-coordinated-enforcement-action-focus-right-erasure-personal-data_en, 07.04.2025.

20 https://www.edpb.europa.eu/news/news/2025/cef-2025-launch-coordinated-enforcement-right-erasure_en, 05.03.2025.

21 <https://ico.org.uk/action-weve-taken/audits-and-overview-reports/2025/04/children-s-data-in-financial-services/>, 01.04.2025.

22 <https://publications.jrc.ec.europa.eu/repository/handle/JRC141090>, 08.04.2025.

23 [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)769570](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)769570), 07.04.2025.

* Avrupa Komisyonu, Dijital Hizmetler Tüzüğü (DSA) kapsamında küçüklerin çevrim içi ortamda korunmasına yönelik olarak hazırlanan taslak rehber hakkında kamuoyunun görüşüne başvurulduğunu duyurdu²⁴. Taslak rehber; çocukların dijital ortamda karşı karşıya kalabilecekleri risklerin önlenmesine yönelik olarak profillemeye dayalı reklamların yasaklanması, kullanıcı mahremiyeti ve güvenliğin tasarım aşamasında gözetilmesi, yaşa uygun hizmet sunumu ve ölçülülük ilkesi çerçevesinde açıklamalar içermektedir.

Bunun yanında, çevrim içi platformların risk temelli bir değerlendirme yaklaşımı benimsemeleri, hizmetlerinde meydana gelen önemli değişiklikler sonrasında risk analizlerini güncellemeleri ve sürekli izleme mekanizmaları ile şeffaf bir yönetim yapısı tesis etmeleri yönünde tavsiyelerde bulunmaktadır.

* Avrupa Komisyonu ve OECD'nin ortak girişimi olarak "İlköğretim ve Ortaöğretim için Yapay Zekâ Okuryazarlığı Çerçevesi" geliştirilmektedir²⁵. Eğitimciler ve paydaşlardan geri bildirim almak üzere hazırlanan taslak çerçeve ile yapay zekâ okuryazarlığının ne anlama geldiği ve eğitim süreçlerinin bu çağda nasıl dönüşmesi gerektiği konularında bir diyalog geliştirilmesi amaçlanmaktadır.

* Fransa Veri Koruma Otoritesi (CNIL); mobil uygulamaların mahremiyetin korunmasını temin edecek şekilde tasarlanmasına yardımcı olmak amacıyla, mobil uygulama ekosistemindeki paydaşlara yönelik tavsiyeler içeren ve geçtiğimiz yılın Eylül ayı içerisinde paylaşılan dokümanın güncellenmiş versiyonunun yayımlandığını duyurdu²⁶. Konuya ilişkin olarak Otorite tarafından yapılan açıklamada, rehberin özü değiştirilmeksizin birtakım küçük çaplı düzeltmeler gerçekleştirildiği ifade edildi.

* Kanada Veri Koruma Otoritesi (OPC), bir veri ihlali meydana gelmesi durumunda, söz konusu ihlalin bir birey açısından "önemli zarar riski" oluşturup oluşturmadığının değerlendirilmesine yardımcı olmak amacıyla çevrim içi bir değerlendirme aracı yayımladı²⁷.

* Fransa Veri Koruma Otoritesi (CNIL), çok faktörlü kimlik doğrulama çözümlerinin kullanımına ilişkin tavsiyeler yayımladı²⁸.

* Yunanistan 5 Mart, Monako ise 6 Mart tarihinde, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme'yi Değiştiren Protokolü" (CETS No.223), bilinen adıyla "108+ Konvansiyonu", onaylayan 32. ve 33. devlet oldu²⁹.

* 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuattaki tanımlar ile ulusal çalışmalar başta olmak üzere; Avrupa Birliği düzenlemeleri ile Avrupa Veri Koruma Kurulu (EDPB), Avrupa Veri Koruma Denetçisi (EDPS), IAPP ve benzeri kuruluşların çalışmaları arasından seçilen yüz kavrama ilişkin tanımın bir araya getirilmesiyle oluşturulan "Kişisel Verilerin Korunması Terimler Sözlüğü" paylaşıldı³⁰. Kişisel verilerin korunması ile ilişkili olan seçilmiş kavramları bir araya getirerek ilgililere erişim kolaylığı sağlamayı amaçlayan çalışmaya, Kurumumuzun internet sitesi üzerinden ulaşılabilmektedir.

* İtalyan gazetesi Il Foglio, tamamı yapay zekâ tarafından üretilmiş özel bir baskı yayımlayarak

dünyada bir ilke imza attığını duyurdu³¹. Gazetenin editörü tarafından aktarıldığı üzere, bu özel sayının tüm içerikleri- makaleler, başlıklar, alıntılar ve köşe yazılarındaki ironi dahil – herhangi bir insan müdahalesi olmaksızın yapay zekâ araçları kullanılarak hazırlandı. Deneysel nitelikteki bu çalışmanın, yapay zekânın gazetecilik alanına olan etkilerini ve potansiyel sınırlarını ortaya koymayı amaçladığı belirtilmektedir.

* Çin'de, dünyanın ilk yapay zekâ hastanesi olan Agent Hospital kamuoyuna tanıtıldı³². Tsinghua Üniversitesi Yapay Zekâ Endüstrisi Araştırma Enstitüsü (AIR) tarafından geliştirilen sistemde, 21 farklı tıbbi branşta görev yapan 42 yapay zekâ destekli "doktor" yer alıyor. Büyük dil modeli (LLM) tabanlı akıllı ajanlar tarafından yönlendirilen bu doktorlar, hastalığın başlangıcından tedavi sonrası izleme süreçlerine kadar tüm klinik döngüyü otonom biçimde simüle edebiliyor. Bu süreç; ön değerlendirme, kayıt, muayene, teşhis, tedavi, reçeteleme, rehabilitasyon ve takip aşamalarını kapsıyor.

Sistemin yalnızca birkaç gün içerisinde 10.000'den fazla sanal hastayı değerlendirdiği, insan doktorların haftada ortalama 100 hasta ile ilgilendiği dikkate alındığında, bu performansın yaklaşık iki yıllık bir hasta sayısına karşılık geldiği ve %93.06 oranında doğruluk sağlandığı ifade ediliyor. AIR araştırmacıları, bu teknolojinin yakın gelecekte pratik sağlık uygulamalarında kullanılabilecek olgunluğa ulaştığını belirtmekle beraber, insan hekim ile yapay zekâ iş birliğinin sınırlarının belirlenmesi ve bu sistemin mevcut düzenlemelerle tam uyum içerisinde geliştirilmesi temel bir öncelik olarak öne çıkıyor.

* Siber güvenlik uzmanlarına göre, bir çocuğun yalnızca 20 fotoğrafı, yapay zekâ destekli deepfake teknolojileri aracılığıyla dijital olarak taklit edilmesi için yeterli³³. Birleşik Krallık'ta 16 yaşından küçük çocukları olan 2.000 ebeveynle yapılan bir araştırma, ebeveynlerin her ay çocuklarına ilişkin ortalama 63 fotoğrafı sosyal medya platformlarında paylaştığını ortaya koymaktadır. Bu durum, çocukları yalnızca kimlik hırsızlığı ve dolandırıcılık gibi tehditlerle değil; aynı zamanda psikolojik sömürü, çevrim içi şantaj ve istismar gibi önemli risklerle de karşı karşıya bırakmaktadır.

Bu bağlamda, çevrim içi ortamda çocukların kişisel verilerinin korunması adına ebeveynlerin;

» Kişisel veri, mahremiyet, istenmeyen e-posta ve çevrim içi güvenlik gibi konulara ilişkin olarak çocuklarını bilgilendirmeleri,

» Çocuklara yönelik kişisel veri işleyen ürün ve hizmetlerin bilgilendirici metinlerini dikkatle okumaları,

» Çocuklarının kişisel verilerini çevrim içi ortamlarda herkese açık bir şekilde paylaşmaktan kaçınmaları,

» Güçlü parolalar kullanmaları ve çocuklarını da güçlü parola oluşturma konusunda bilgilendirmeleri,

» Çocuklarının kullandığı bilgisayar, cep telefonu veya oyun konsollarında internet filtreleme gibi koruyucu teknolojilerden yararlanabileceklerinin farkında olmaları

önem taşımaktadır.

24 <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>, 13.05.2025.

25 https://ailiteracyframework.org/wp-content/uploads/2025/05/AiLitFramework_ReviewDraft.pdf, Mayıs 2025.

26 <https://www.cnil.fr/fr/recommandations-applications-mobiles-modifiee>, 08.04.2025.

27 <https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/rrosh-tool/>, 26.03.2025.

28 <https://www.cnil.fr/fr/recommandation-mfa>, 01.04.2025.

29 <https://coe.int/en/web/data-protection/-/greece-becomes-the-32nd-and-monaco-the-33rd-state-to-ratify-convention-108->, 06.03.2025.

30 <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/d1e5b8a6-d244-4ab7-a2e6-f36af317b4c2.pdf>, Mayıs 2025.

31 <https://www.theguardian.com/technology/2025/mar/18/italian-newspaper-says-it-has-published-worlds-first-ai-generated-edition>, 18.03.2025.

32 <https://www.indy100.com/science-tech/china-first-ai-hospital-42-ai-doctors-2672029016>, 16.05.2025.

33 <https://www.independent.ie/irish-news/criminals-need-just-20-images-of-one-child-to-produce-deep-fake-cyber-experts-say/a42584428.html>, 14.05.2025.

7 NİSAN KİŞİSEL VERİLERİ KORUMA GÜNÜ PROGRAMI

7 Nisan Kişisel Verileri Koruma Günü programı kapsamında Kurumumuz, İbn Haldun Üniversitesi ve İstanbul 2 No'lu Barosu iş birliğinde, "Kişisel Veriler ve Hukuki Güncellemeler: 2025 Perspektifi" etkinliği gerçekleştirildi. Adalet Bakanımız Sayın Yılmaz TUNÇ'un teşrifleriyle düzenlenen etkinlik, alanında uzman isimleri bir araya getirdi.

Bakan TUNÇ: "Kişisel verilerin korunması; insanın onuruna, mahremiyetine ve özgürlüğüne duyulan saygının gereğidir."

Etkinliğin açılış konuşmasını Adalet Bakanımız Sayın Yılmaz TUNÇ gerçekleştirdi. Bakan TUNÇ, kişisel verilerin korunmasının; insanın onuruna, mahremiyetine ve özgürlüğüne duyulan saygının gereği olduğunu ifade etti.

Kişisel verilerin korunması amacıyla güçlü, güvenilir ve sürdürülebilir sistemler inşa etmek için bugüne kadar anayasal, yasal ve uluslararası anlaşmalar boyutuyla birçok düzenlemenin hayata geçirildiğini belirten Bakan TUNÇ, bundan sonra da kararlılıkla çalışmaya devam edeceklerini söyledi.

Kurum Başkanımız Faruk BİLİR ise, Kişisel Verileri Koruma Kurumu olarak kişisel veriler konusunda ulusal ve uluslararası gelişmeleri takip ettiklerini ve bu doğrultuda, veri korumanın etkili bir hak arama yolu olarak varlığını sürdürmesi için çalışmalara devam ettiklerini belirtti.



DİJİTAL OYUNLAR VE KİŞİSEL VERİLERİN KORUNMASI SEMPOZYUMU

Kurumumuz ve Fatih Sultan Mehmet Vakıf Üniversitesi Hukuk Fakültesi iş birliğinde “Dijital Oyunlar ve Kişisel Verilerin Korunması Sempozyumu”, Fatih Sultan Mehmet Vakıf Üniversitesi Haliç Yerleşkesi’nde gerçekleştirildi.

Etkinlikte; dijital oyunların tarihsel gelişimi, yapay zekâ ve dijital oyunlar, dijital oyunlar ve çocukların kişisel verilerinin korunması, açık rıza ve aydınlatma yükümlülüğünün hukuka uygun şekilde yerine getirilmesi gibi toplamda 22 konu çeşitli yönleriyle ele alındı.

Etkinliğin açılış konuşmasını Fatih Sultan Mehmet Vakıf Üniversitesi Rektörü Prof. Dr. Nevzat ŞİMŞEK ile Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptı. BİLİR konuşmasında genel olarak; dijital oyunların günümüzdeki yeri ve kişisel verilerin korunmasına etkisi, dijital oyunlarda kişisel verilerin işlenmesi ile çocukların ve gençlerin kişisel verilerinin korunması konularına değindi.



KVKK GÜNCEL GELİŞMELER SEMPOZYUMU

Kurumumuz ve Eskişehir Barosu iş birliği ile Kişisel Verilerin Korunması Kanunu’nda yapılan değişikliklerin ele alındığı “KVKK Güncel Gelişmeler Sempozyumu” düzenlendi. Sempozyumun açılış konuşmalarını Eskişehir Barosu Başkanı Barış GÜNAYDIN ile Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptılar. İki oturum olarak düzenlenen sempozyumda “Veri İhlalleri ve Bilişim Suçları İlişkisi”, “Kişisel Verilerin Yurt Dışına Aktarılması”, “Değişen Veri İşleme Şartları İle Özel Nitelikli Kişisel Verilerin İşlenmesi” ve “Kanun Değişikliğinin Uygulamaya Yansımaları” konuları ele alındı.



KİŞİSEL VERİLERİN KORUNMASI: HUKUKUN DİJİTAL DÜNYADAKİ ROLÜ ETKİNLİĞİ

İstanbul Sabahattin Zaim Üniversitesi (İZÜ) tarafından, dijital dünyadaki hukuki süreçleri ele almak amacıyla, “Kişisel Verilerin Korunması: Hukukun Dijital Dünyadaki Rolü” başlıklı bir etkinlik düzenlendi.

Nizamülmülk Konferans Salonunda gerçekleşen programa, Kurum Başkanımız Prof. Dr. Faruk BİLİR konuşmacı olarak katıldı. Etkinlikte, İZÜ Rektörü Prof. Dr. Ahmet Cevat ACAR, İZÜ Genel Sekterleri Dr. Fatih HASDEMİR, İZÜ Hukuk Fakültesi Dekanı Prof. Dr. Mustafa ATEŞ, akademisyenler ve idari personelin yanı sıra çok sayıda öğrenci yer aldı. Programın açılış konuşmasını yapan Kurum Başkanımız Prof. Dr. Faruk BİLİR, kişisel verilerin korunmasının küresel ölçekte önem taşıyan bir konu olduğunu dile getirdi. BİLİR, “Bilişim teknolojilerinin gelişimi ve yaygınlaşması, veri güvenliğini ön plana çıkarmaktadır. Ülkemizde kişisel verilerin korunmasıyla ilgili yapılan düzenlemeler, bireylerin mahremiyet haklarını güvence altına almayı amaçlamaktadır” dedi.



KİŞİSEL VERİLERİN KORUNMASI KANUNU VE UYGULAMALARI KONFERANSI

Kişisel Verilerin Korunması Kanunu ve Uygulamaları Konferansı, Aksaray Üniversitesi Konferans Salonu'nda gerçekleştirildi. Kurum Başkanımız Prof. Dr. Faruk BİLİR'in konuşmacı olarak davet edildiği etkinliğe öğrenciler katılım sağladı. Kişisel Verilerin Korunması Kanunu hakkında bilgiler paylaşan BİLİR, bu kapsamda Kanun'da yer alan kavramlar, temel ilkeler ve veri işleme şartları başta olmak üzere Kanun ve ikincil mevzuatla ilgili çeşitli konulara değindi.



YAPAY ZEKÂ TEKNOLOJİLERİNE AKADEMİK BAKIŞ KİTABI



Kurumumuz tarafından, yapay zekâ teknolojilerinde kişisel verilerin korunmasına yönelik hukuki, teknik ve etik hususların alanında uzman akademisyenler tarafından çeşitli boyutlarıyla değerlendirildiği "Yapay Zekâ Teknolojilerine Akademik Bakış" isimli kitap yayımlandı.

YAPAY ZEKÂ TEKNOLOJİLERİNE AKADEMİK BAKIŞ KİTABI TANITIM TOPLANTISI

"Yapay Zekâ Teknolojilerine Akademik Bakış" kitabı tanıtım toplantısı KVKK Konferans Salonunda gerçekleştirildi. Toplantının açılış konuşmasını Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptı.

Tanıtım toplantısı kapsamında düzenlenen programda; Samsun Üniversitesi'nden Dr. Öğr. Üyesi Ebru PEKEL ÖZMEN "Yapay Zekâ ve Makine Öğrenmesine Giriş", Bilkent Üniversitesi'nden Doç. Dr. Elif KÜZECİ "Yapay Zekâ Teknolojilerine Etik Yaklaşım", Galatasaray Üniversitesi'nden Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK "Kodlar ve Kanunlar: Yapay Zekânın Regülasyon Rotası ve AB Yapay Zekâ Tüzüğü", İstanbul Teknik Üniversitesi'nden Dr. Öğr. Üyesi Çiçek ERSOY "Veri Koruma Hukukunun Temel Prensipleri ve Yapay Zekâ Uygulamaları Açısından Değerlendirilmesi", TOBB Ekonomi ve Teknoloji Üniversitesi'nden Prof. Dr. Perihan Elif EKMEKÇİ "Sağlık Alanında Yapay Zekâ ve Kişisel Veriler", Gazi Üniversitesi'nden Doç. Dr. Nursel YALÇIN ise "Eğitimde Yapay Zekâ" konularını anlattılar.



"ÖDEME VE ELEKTRONİK PARA SEKTÖRÜNDE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İYİ UYGULAMALAR REHBERİ" ÇALIŞTAYI

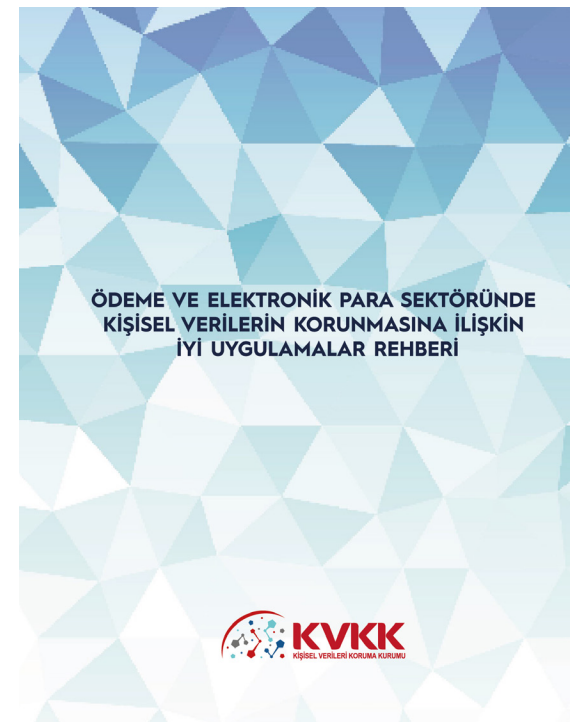
Kurumumuz ile Türkiye Ödeme ve Elektronik Para Kuruluşları Birliği (TÖDEB) iş birliğiyle, ödeme ve elektronik para sektöründe kişisel verilerin korunmasına ilişkin iyi uygulamaları kapsayan "Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi" Çalıştayı İstanbul'da gerçekleştirildi. Çalıştay'ın açılış konuşmalarını TÖDEB Yönetim Kurulu Başkanı Serhat DOLAZ ve Kurum Başkanımız Prof. Dr. Faruk BİLİR gerçekleştirdi.

BİLİR, sektörel bazda ilk olarak bankacılık sektörüne ilişkin iyi uygulamalar rehberinin yayımlandığını, şimdi ise "Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi"nin bu alanda faaliyet gösteren veri sorumlularına yol gösterici nitelikte bir çalışma olduğunu belirtti. BİLİR, Rehber'de; rehberin amacı ve kapsamı, sektörde işlenen kişisel verilerin neler olduğu, bu veriler bakımından veri sorumlusu, veri işleyen, ilgili kişilerin kimler olduğu, genel ilkeler, işleme şartları, kişisel verilerin aktarılması, veri sorumlusunun yükümlülükleri ve veri güvenliği başlıkları altında ilgili hususlara sektörden iyi uygulama örnekleri ve önerileri içerecek şekilde yer verildiğini ifade etti. Ayrıca BİLİR, rehberin hazırlanması sürecinde Kurum olarak TÖDEB ile etkin bir iş birliği içerisinde çalıştıklarını söyleyerek çalışmada emeği bulunanlara teşekkür etti.



ÖDEME VE ELEKTRONİK PARA SEKTÖRÜNDE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İYİ UYGULAMALAR REHBERİ

Kurumumuz ve Türkiye Ödeme ve Elektronik Para Kuruluşları Birliği ile yapılan ortak çalışmalar neticesinde, Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi yayımlandı.



YAPAY ZEKÂ ÇAĞINDA KİŞİSEL VERİLERİN KORUNMASI KONFERANSI

Kurumumuz ve Yapay Zekâ Politikaları Derneği [AIPA Türkiye] iş birliğinde “Yapay Zekâ Çağında Kişisel Verilerin Korunması Konferansı” düzenlendi. KVKK Konferans Salonunda gerçekleştirilen etkinlikte, alanında uzman isimler yapay zekâ konusunu kişisel verilerin korunması çerçevesinde ele aldılar. Konferansın açılış konuşmalarını AIPA Başkanı Zafer KÜÇÜKŞABANOĞLU ve Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptılar.

“Mahremiyet, güvenli bir dijital dünyanın temel unsurlarından biridir.”

Yapay zekânın insanlık tarihindeki en büyük dönüşümlerden biri olduğunu, bu büyük dönüşümü anlamının ve ona uyum sağlamanın geleceği şekillendirme fırsatı sunduğunu söyleyen BİLİR, yapay zekânın iş süreçlerini iyileştirmek ve günümüz dünyasının sorunlarına pratik çözümler geliştirmek için büyük bir potansiyel barındırdığını, bunun ise kişisel verilerin etkin ve güvenli kullanımına bağlı olduğunu ifade etti. BİLİR, yapay zekânın gelişimini kişisel verilerin korunması ve mahremiyet gibi değerler çerçevesinde yönlendirmenin, yapay zekânın insanlığın hizmetinde bir güç olarak kalmasını sağlamak açısından büyük önem taşıdığını belirterek, mahremiyetin yalnızca bir hak değil, aynı zamanda güvenli bir dijital dünyanın temel unsurlarından biri olarak görülmesi gerektiğini dile getirdi.

“Bireyin mahremiyetinin korunmasını teşvik eden yaklaşımların benimsenmesi önemlidir.”

Yapay zekâ tabanlı sistemlerle gerçekleştirilen kişisel veri işleme faaliyetlerinin, Kişisel Verilerin Korunması Kanunu’nda belirtilen temel veri koruma ilkelerine ve veri işleme şartlarına uygun olması gerektiğini hatırlatan BİLİR, veri güvenliğine önem veren ve bireyin mahremiyetinin korunmasını teşvik eden yaklaşımların benimsenmesinin, toplumun yapay zekâya güven duyması bakımından önem taşıdığını söyledi. Kişisel Verilerin Korunması Kanunu ile bireylere itiraz hakkı tanındığını, buna göre kişisel verilerin yalnızca otomatik sistemlerle analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması halinde buna itiraz edebildiğini aktaran BİLİR, “İtiraz hakkı, teknolojik süreçlerin şeffaflığını ve bireylerin verileri üzerindeki kontrolünü artırarak adil kararlar alınmasını amaçlamaktadır. İtiraz hakkı sayesinde bireyler, otomatik veri işlemeye karşı insan müdahalesinin sürece dahil edilmesini talep edebilmektedir” dedi.

“Yapay zekâ insanın rakibi değil, destekçisi olmalıdır.”

“İnsanı merkeze almayan ve insana hizmet etme gayesi taşımayan gelişmenin kıymetli ve kalıcı olması mümkün değildir” diyen BİLİR, etik ilkelerin dikkate alındığı ve mahremiyet temelli yaklaşımların standart hale geldiği bir yapay zekâ ekosisteminin oluşturulması gerektiğini kaydetti. Yapay zekâ hakkındaki endişelerin, teknolojik ilerlemenin önünde duvar değil, yapay zekâ sistemlerini daha güvenli ve faydalı hale getirmek için rehber olması gerektiğinin altını çizen BİLİR, “Yapay zekâ insanın rakibi değil, destekçisi olmalıdır” dedi.

Öte yandan üç oturum olarak planlanan etkinliğin ilk oturumunu, Kişisel Verileri Koruma Kurulu Üyelerimizden Muhammed Serdar CAFOĞLU yönetti. “Güncel Yapay Zekâ Sistemleri ve Kişisel Verilerin Yeri” konusunun ele alındığı oturumda; Kurumumuz Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanı Ersin CAN, AIPA Başkan Yardımcısı Volkan KILIÇ ve AIPA Eğitim Komisyonu Başkan Yardımcısı Dr. Mehmet ADA konuşmacı olarak yer aldılar.

Etkinliğin “Yapay Zekâ Sistemlerinde Kişisel Verilerin Korunmasında Güncel Sorunlar” başlıklı ikinci oturumunun moderatörlüğünü Kurumumuz Başkan Yardımcısı Dr. Cihan KANLIGÖZ yaptı. Oturum kapsamında; AIPA Yönetim Kurulu Üyesi ve AIPA Hukuk ve İnsan Hakları Komisyonu Başkanı Av. Elif Selin YILMAZ ALTAY, AIPA Sağlık Komisyonu Üyesi ve Çankaya Üniversitesi Endüstri Mühendisliği Bölümü Öğretim Elemanı Mehmet Nadir ERHAN, Galatasaray Üniversitesi Hukuk Fakültesi Kamu Hukuku Bilişim ve Teknoloji Hukuku Öğretim Üyesi Dr. Osman Gazi GÜÇLÜTÜRK ve Kurumumuz Kişisel Verileri Koruma Uzmanı Beste EKİN konuşmacı olarak yer aldılar.

Etkinliğin son oturumu ise AIPA Yönetim Kurulu Üyesi Av. Ata GÜMÜŞ’ün başkanlığında gerçekleştirildi. “Yapay Zekâ Sistemlerinde Kişisel Verilerin Korunması Konusunda Dünyadan Örnekler” başlığıyla gerçekleştirilen son oturumun konuşmacıları ise; AIPA Danışma Kurulu Üyesi ve Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü AB Proje Uygulamaları Daire Başkanı Doç. Dr. Tamer SOYSAL, AIPA Hukuk ve İnsan Hakları Komisyonu Üyesi ve Bilkent Üniversitesi Hukuk Fakültesi Öğretim Üyesi Doç. Dr. Barış ÖZÇELİK, Kurumumuz Kişisel Verileri Koruma Uzmanı Ezgi TURGUT BİLGİÇ ve Avrupa Birliği Başkanlığı AB Hukuku ve Çeviri Daire Başkanlığı AB İşleri Uzmanı Çiğdem AKIN oldular.



II. ULUSAL KİŞİSEL VERİLERİN KORUNMASI SEMPOZYUMU

Kurumumuz ve İstanbul Teknik Üniversitesi iş birliğinde düzenlenen “Yapay Zekâ Teknolojileri ve Kişisel Veriler” temalı II. Ulusal Kişisel Verilerin Korunması Sempozyumu İstanbul’da gerçekleştirildi. İTÜ Süleyman Demirel Kültür Merkezi Ayazağa Kampüsü’nde düzenlenen sempozyumun açılış konuşmalarını İTÜ Rektör Yardımcısı Prof. Dr. Lütfiye DURAK ATA ve Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptılar.

Yapay zekânın insan hayatına etkilerinin derinleştiği bir dönemde kişisel verilerin korunmasının önemine dikkat çeken BİLİR, konuşmasında şu ifadelere yer verdi:

“Yapay zekâ insanlık tarihindeki en büyük dönüşümlerden biridir. Bu teknolojiyi mahremiyet gibi değerler çerçevesinde yönlendirmek, yapay zekânın insanlığın hizmetinde kalmasını sağlamak açısından büyük önem taşımaktadır.” Teknolojik gelişmelerin temel hak ve özgürlükler çerçevesinde dengelenmesi gerektiğini vurgulayarak bu hususta hukuki düzenlemelerin önemine işaret eden BİLİR, “Hukuki düzenlemelerin amacı, teknolojiyi durdurmak değildir. Teknolojik gelişmeleri temel insan haklarına ve bireyin mahremiyetine saygılı bir zeminde yönlendirmektir.” dedi.

İki oturum olarak planlanan sempozyumun “Ulusal ve Uluslararası Düzlemde Yapay Zekâ” konulu ilk oturumunu Kişisel Verileri Koruma Kurulu Üyelerimizden Recep KESKİN yönetti.



Oturum kapsamında; Galatasaray Üniversitesi’nden Prof. Dr. E. Eylem AKSOY RETORNAZ “Yapay Zekâ Algoritmalarıyla Profillemeye ve Kişisel Verilerin Korunması”, Galatasaray Üniversitesi’nden Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK “Kodlar ve Kanunlar: Yapay Zekânın Regülasyon Rotası ve AB Yapay Zekâ Tüzüğü”, İstanbul Teknik Üniversitesi’nden Dr. Öğr. Üyesi Çiçek ERSOY “Veri Koruma Hukukunun Temel Prensipleri ve Yapay Zekâ Uygulamaları Açısından Değerlendirilmesi” konularını anlattılar.

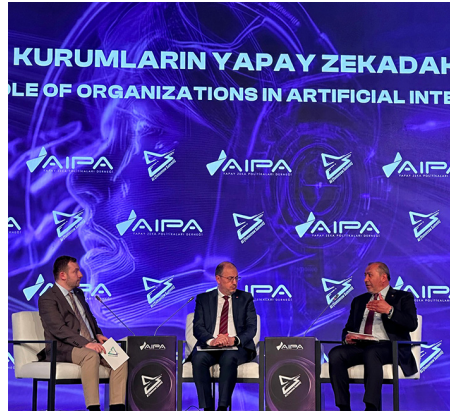
Galatasaray Üniversitesi’nden Prof. Dr. E. Eylem AKSOY RETORNAZ’ın moderatörlüğünü üstlendiği “Yapay Zekâ ve Mahremiyet Dengesi” konulu ikinci oturumda ise; İstanbul Teknik Üniversitesi’nden Prof. Dr. Şule GÜNDÜZ ÖĞÜDÜCÜ “Öneri Modellerinin KVKK ile Uyumu”, Özyeğin Üniversitesi’nden Dr. Öğr. Üyesi Başak OZAN ÖZPARLAK, “İstihdamda Yapay Zekâ” ve Kurumumuz Kişisel Verileri Koruma Uzmanlarından Ezgi TURGUT BİLGİÇ ise “Yapay Zekâ Teknolojilerinde Kişisel Verilerin Otomatik İşleme Tâbi Tutulması ve İtiraz Hakkı” konularını anlattılar.

Ayrıca sempozyum programı kapsamında, Kurumumuz Kişisel Verileri Koruma Uzmanlarından Beste EKİN, Kurumumuz tarafından yayımlanan “Yapay Zekâ Teknolojilerine Akademik Bakış” kitabı ile ilgili genel değerlendirmelerde bulunarak söz konusu çalışma hakkında bilgiler paylaştı.



AI [TOMORROW SUMMIT] 2025 YAPAY ZEKÂ ZİRVESİ

Kurum Başkanımız Prof. Dr. Faruk BİLİR, AI [Tomorrow Summit] 2025 Yapay Zekâ Zirvesi'ne konuşmacı olarak katılım sağladı. BİLİR, yapay zekâ teknolojileri ile kişisel verilerin korunmasının kesişim noktalarına değinerek Kurumumuzun bu kapsamda yapmış olduğu çalışmalar hakkında bilgiler paylaştı.



8. E-SAFE KİŞİSEL VERİLERİ KORUMA ZİRVESİ

Kurumumuz ev sahipliğinde bu yıl 8'inci kez düzenlenen e-Safe Kişisel Verileri Koruma Zirvesi, 30 Nisan Çarşamba günü KVKK Konferans Salonunda gerçekleştirildi.

Alanında uzman konuşmacıların yer aldığı etkinlikte, kişisel verilerin korunması alanındaki gelişmeler hukuki ve teknik açılarından ele alındı. Zirveyi, aralarında hukukçuların ve bilişim uzmanlarının bulunduğu sektör temsilcileri de takip etti.



KİŞİSEL VERİLERİN KORUNMASI MEVZUATI DEĞİŞİKLİKLERİ: YENİ DİNAMİKLER VE MEVZUAT UYUM ÇALIŞTAYI



Kurumumuz ve Mevzuat Uyum Derneği iş birliği ile Kişisel Verilerin Korunması Kanunu'nda yapılan değişiklikleri ele alan çalıştay düzenlendi.

33. AVRUPA VERİ KORUMA OTORİTELERİ KONFERANSI

Avrupa çapındaki veri koruma otoritelerinin katılım sağladığı, kişisel verilerin korunmasına dair önemli gelişmelerin ele alındığı 33. Avrupa Veri Koruma Otoriteleri Konferansı Gürcistan'ın Batum kentinde gerçekleştirildi.

Konferansa, Kurumumuzu temsilen, Kurum Başkanımız Prof. Dr. Faruk BİLİR ve Kurul Üyelerimizden Tamer AKSOY katılım sağladı.

Gürcistan Veri Koruma Otoritesi'nin ev sahipliği yaptığı Konferans'ta başta yapay zekâ olmak üzere; güncel teknolojilerin kişisel verilerin korunmasına etkileri, veri koruma alanında uluslararası iş birliğinin önemi ve çocukların kişisel verilerinin korunması gibi konular hakkında paneller düzenlendi.



MAHREMİYET FARKINDALIK HAFTASI 2025

Kurum Başkanımız Prof. Dr. Faruk BİLİR ve Kişisel Verileri Koruma Kurulu Üyelerimizden Bayram ARSLAN, Filipinler Cumhuriyeti Ulusal Mahremiyet Komisyonu [NPC] tarafından, Metro Manila'da 27-29 Mayıs tarihleri arasında düzenlenen "Küresel Mahremiyet Meseleleri: Sınırların Ortadan Kalktığı Dijital Dünyada Gezinmek ve Yeni Profesyonel Ufukları Genişletmek" temalı "Mahremiyet Farkındalık Haftası"na [PAW 2025] katıldı.

Bu yıl 8'inci düzenlenen organizasyonda, günümüzde ortaya çıkan yeni mahremiyet sorunları tartışılarak iyi uygulama örneklerinin paylaşıldığı paneller düzenlendi.



ÇARŞAMBA SEMİNERLERİ

Kurumumuz tarafından düzenlenen Çarşamba Seminerleri kapsamında;

- Kurumumuz Kişisel Verileri Koruma Uzmanlarından Hazal Deniz ÖZKAN, "Kişisel Verilerin Korunması Hukukunda İdari Para Cezaları"
- Kurumumuz Kişisel Verileri Koruma Uzmanlarından Ahmet Can ESER, "KVKK ve GVKT Kapsamında Veri Sorumlusunun Meşru Menfaati Hakkında Değerlendirme"
- Başkomiser Dr. Enver KAŞLI, "Kolluk Kuvvetlerinde Kişisel Verilerin Korunması"

konularında bilgi paylaşımında bulundular.



ÜNİVERSİTE ÖĞRENCİLERİ ARASINDA KİŞİSEL VERİLERİ KORUMA GÖNÜLLÜSÜ YETİŞTİRME PROJESİ



"Üniversite Öğrencileri Arasında Kişisel Verileri Koruma Gönüllüsü Yetiştirme Projesi"nin beşinci aşamasının ikinci bölümü Ankara'da Kurumumuz Konferans Salonunda yapılan etkinlikle gerçekleştirildi.

Etkinlik kapsamında öğrenciler, proje çerçevesinde gerçekleştirdikleri faaliyetleri ve farkındalık çalışmalarını hazırladıkları sunumlar eşliğinde anlattılar.



MAKALE, SLOGAN VE KARİKATÜR YARIŞMALARI ÖDÜL TÖRENİ

Kurumumuz tarafından düzenlenen makale, slogan ve karikatür yarışmalarının ödül töreni gerçekleştirilerek dereceye giren katılımcılara ödülleri takdim edildi.

Makale yarışmasında; birincilik ödülünü “Kişisel Verilerin Korunması Hukuku Çerçevesinde Hedefli Reklamcılık Uygulamaları”, ikincilik ödülünü “Dijital Çağda Güvenlik Stratejileri: Kişisel Verilerin Korunması ve Siber Güvenlik Perspektifi”, üçüncülük ödülünü ise “Sharenting Ebeveynliği: Çocukların Dijital Gizliliği ve Hukuki Riskler” isimli makaleler kazandı.

Slogan yarışmasında; birincilik ödülünü Çanakkale Tacettin Aslan Mesleki Teknik ve Anadolu Lisesi’nden Sim** Ke**, ikincilik ödülünü Kırıkkale Yıldırım Beyazıt Anadolu Lisesi’nden Ze** Nu** Es**, üçüncülük ödülünü ise Kocaeli Alaettin Kurt Anadolu Lisesi’nden Asm** Ak** kazandı.

Karikatür yarışmasında; birincilik ödülünü İstanbul Pendik Nuh Kuşçulu Seramik ve Cam Teknolojisi Mesleki ve Teknik Anadolu Lisesi’nden Su** Yıl**, ikincilik ödülünü İstanbul Bağcılar Fatih Mesleki ve Teknik Anadolu Lisesi’nden Şev** Bo**, üçüncülük ödülünü ise Balıkesir Ülkü Muharrem Ertaş Anadolu Lisesi’nden Ja** N** Kız** kazandı.



İLKOKUL ÖĞRENCİLERİNE KİŞİSEL VERİ FARKINDALIĞINA YÖNELİK ETKİNLİK

Okul çağındaki çocukların kişisel verilerle tanışması, veri koruma bilinciyle yetişmesi ve buna yönelik farkındalık oluşması amacıyla birçok çalışma ve etkinliği hayata geçiren Kurumumuz, bu çerçevede Edirne Şükrüpaşa İlkokulu'nda kişisel veri farkındalığına yönelik bir etkinlik gerçekleştirdi. Etkinlik kapsamında, öğretmenleri eşliğinde olmak üzere; öğrencilere kişisel verilerin korunması ve kişisel veri farkındalığı ile ilgili konularda yaş gruplarına uygun olacak şekilde sunum yapıldı. Kişisel veri mahremiyetine yönelik bilgiler paylaşıldı.

Ayrıca kişisel verilerin korunmasıyla ilgili hazırlanan farkındalık ve bilgilendirme videoları izletildi. Karşılıklı soru-cevap etkinliğiyle ise öğrencilerin edindikleri bilgileri eğlenceli bir şekilde pekiştirmeleri sağlandı.



SAYIŞTAY'IN 163'ÜNCÜ KURULUŞ YIL DÖNÜMÜ SEMPOZYUMU

Kurum Başkanımız Prof. Dr. Faruk BİLİR, Sayıştay'ın 163'üncü kuruluş yıl dönümü vesilesiyle düzenlenen sempozyuma katılım sağladı.

BİLİR, "Büyük Verinin ve Algoritmaların Dönüştürücü Gücü", "Kamuda Yürütülen Büyük Veri Analitiği Projeleri ve Kamu Hizmetlerine Etkisi", "Büyük Veri Analitiğinin Küresel Rekabetteki Rolü ve Dünya Gündemindeki Yeri", "Büyük Veri Analitiğinin Denetimde Kullanılması ve Denetimin Etkinliğine Katkısı" konularının ele alındığı "Büyük Veri Analitiği ve Denetim" temalı ikinci oturumda, oturum başkanlığını üstlendi.



PODCAST

"Bir Küçük Farkındalık Yeter" isimli podcast kanalımızda; kişisel verilerin korunmasına ilişkin gelişmeler konusunda bilgi paylaşımını amaçlayan podcast serimizin yeni bölümleri yayınlandı.





kvvkkurumu



Kişisel Verileri Koruma Kurumu

Nasuh Akar Mahallesi 1407. Sokak

No.4 06520 Çankaya | ANKARA

T. 0312 216 50 00

www.kvkk.gov.tr