KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

YAPAY ZEKÂ ALANINDA KİŞİSEL VERİLERİN KORUNMASINA DAİR TAVSİYELER

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

YAPAY ZEKÂ ALANINDA KİŞİSEL VERİLERİN KORUNMASINA DAİR TAVSİYELER

İÇİNDEKİLER

ÖZET

Bu doküman; yapay zekâ alanında faaliyet gösteren, geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcılar için 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel verilerin korunması amacına yönelik önerileri içermektedir.

ABSTRACT

“This guide includes recommendations for the protection of personal data within the scope of the Law No. 6698 on the Protection of Personal Data for developers, manufacturers, service providers and decision makers operating in the field of artificial intelligence.”

GİRİŞ

Amaç ve Dayanak

Türk Dil Kurumu Sözlüğünde Zekâ, "insanın düşünme, akıl yürütme, objektif gerçekleri algılama, yargılama ve sonuç çıkarma yeteneklerinin tamamı" olarak tanımlamıştır. İnsan, duyuları vasıtasıyla çevreden topladığı verileri beyninde işler ve zekâsı vasıtasıyla bu verilerden faydalı bilgiler üretir. Bu bakımdan insan bir nevi veri toplama ve işleme sistemi gibi düşünülebilir.

Yapay zekâ ise; insana özgü bu özelliklerin analiz edilerek makinelere kazandırılması olup, insan gibi düşünebilen, yorumlayabilen ve kararlar verebilen algoritmaların ve bilgisayar yazılımlarının geliştirilmesi ile ilgilenmektedir[1].

Günümüzde yapay zekâ teknikleri ve uygulamalarında büyük ilerleme kaydedilmiş ve yapay zekâ tabanlı sistemler birçok alanda yaşamı doğrudan etkilemeye başlamıştır.

Yapay zekâ, bireyler ve toplum için önemli faydalar üretmekle birlikte, bireyin temel hak ve özgürlükleri kapsamında kişisel verilerin korunmasını isteme hakkı bakımından doğru biçimde yönetilmelidir. Kişisel veri işlemeyi temel alan yapay zekâ çalışmaları ve uygulamaları 6698 Sayılı Kişisel Verilerin Korunması Kanununa ve ikincil mevzuata uygun olmalıdır.

Bu doküman, yapay zekâ alanında yapılan/yapılacak çalışmalara yönelik tavsiyeleri içermekte ve söz konusu çalışmalar kapsamında kişisel verilerin korunması hususunda açıklık sağlanmasını hedeflemektedir.

---

1 Balaban Erdal M., Kartal E. 2018. Veri Madenciliği ve Makine Öğrenmesi Temel Algoritmaları ve R Dili ile Uygulamaları (İkinci Baskı), İstanbul: Çağlayan Kitabevi ve Eğitim Çözümleri Ticaret AŞ

Doküman hazırlanırken, Avrupa Konseyi İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü tarafından yayınlanmış olan “Yapay Zekâ ve Kişisel Verilerin Korunması Rehber İlkeleri”, OECD tarafından hazırlanan “OECD Yapay Zekâ Konseyi Önerileri” ve Avrupa Konseyi’nin “Güvenilir Yapay Zekâ için Taslak Etik Kuralları” çalışmalarından faydalanılmıştır.

Kapsam

Yapay zekâ alanındaki geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcıları kapsayan bu dokümanda yapay zekâ uygulamalarında kişisel verilerin korunmasına dair tavsiyeler bulunmaktadır.

Tanımlar

Dokümanda yer alan;

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

Kanun: 6698 sayılı Kişisel Verilerin Korunması Kanununu,

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

Geliştirici: Yapay zekâ sistemlerine ait her türlü ürün için içerik ve uygulama geliştiren gerçek veya tüzel kişileri,

Üretici: Yapay zekâ sistemlerini oluşturan yazılım, donanım gibi her türlü ürünü üreten gerçek veya tüzel kişiyi,

Servis sağlayıcı: Yapay zekâ tabanlı sistemler, veri toplama sistemleri, yazılımlar ve cihazlar kullanarak ürün ve/veya hizmet sunan gerçek veya tüzel kişiyi

ifade eder.

Tavsiyeler

Genel Tavsiyeler

- Yapay zekâ uygulamalarının geliştirilmesi ve uygulanması sürecinde ilgili kişilerin temel hak ve özgürlüklerine saygı gösterilmeli, hak ihlaline meydan verilmemelidir.

- İnsan hakları ve temel özgürlüklerin himayesi ile insan onurunun korunması hakkı gözetilmelidir.

- Kişisel veri işleme temelli yapay zekâ ve veri toplama çalışmaları; kişilerin temel hak ve özgürlüklerini koruyan bir yaklaşım içerisinde hukuka uygunluk, dürüstlük, ölçülülük, hesap verebilirlik, şeffaflık, kişisel verilerin doğru ve güncel olması, kişisel veri kullanım amacının belirli ve sınırlı olması ilkeleri ile veri güvenliği yaklaşımına dayalı olmalıdır.

- Kişisel verilerin işlenmesinde; potansiyel risklerin önlenmesi ve azaltılması üzerine odaklanan, insan haklarını, demokrasinin işleyişini, sosyal ve etik değerleri de göz önünde bulunduran bir bakış açısı benimsenmelidir.

- Veri işleme faaliyetinin bireyler ve toplum üzerine etkileri değerlendirildiğinde ilgili kişi açısından kontrolü mümkün olmalıdır.

- Kişisel veri işleme temelli yapay zekâ çalışmalarında, kişisel verilerin korunması açısından yüksek risk öngörülüyorsa, mahremiyet etki değerlendirmesi uygulanmalı ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmelidir.

- Kişisel veri işleme esaslı yapay zekâ çalışmalarında ilk aşamadan itibaren kişisel verilerin korunması mevzuatına uyum sağlanmalı ve tüm sistemler tasarımdan itibaren veri koruma ilkesine göre geliştirilmeli ve yönetilmelidir. Bu kapsamda her projeye özel bir veri koruma uyum programı oluşturulmalı ve uygulanmalıdır.

- Kişisel veri işleme esaslı yapay zekâ teknolojileri geliştirilirken ve uygulanırken özel nitelikli kişisel veri işleniyorsa özel veri koruma kuralları olduğu göz önüne alınarak teknik ve idari tedbirler daha sıkı şekilde uygulanmalıdır.

- Yapay zekâ teknolojilerinin geliştirilmesi ve uygulanmasında aynı sonuca kişisel veri işlenmeksizin ulaşılabiliyorsa, verilerin anonim hale getirilerek işlenmesi yöntemleri tercih edilmelidir.

- Kişisel veri işleme esaslı yapay zekâ çalışmalarının farklı paydaşlarının veri sorumlusu veya veri işleyen olma statüleri projenin başında belirlenerek aralarındaki hukuki ilişki veri koruma mevzuatı ile uyumlu hale getirilmelidir.

Geliştiriciler, Üreticiler ve Servis Sağlayıcılar İçin Tavsiyeler

- Tasarımda, ulusal ve uluslararası düzenleme ve/veya belgelerle tutarlı olarak kişisel veri mahremiyetini esas alan bir yaklaşım gözetilmelidir.

- Temel hak ve özgürlükler üzerindeki muhtemel olumsuz sonuçlar gözetilerek, uygun risk önleme ve azaltma tedbirlerine dayalı ihtiyatlı bir yaklaşım benimsenmelidir.

- Veri toplama da dâhil olmak üzere veri işlemenin her aşamasında, temel hak ve özgürlükler gözetilerek, ilgili kişiler üzerinde meydana gelebilecek ayrımcılık riski veya diğer olumsuz etkiler ve önyargılar önlenmelidir.

- Kullanılan kişisel verilerin kalitesi, niteliği, kaynağı, miktarı, kategori ve içeriği değerlendirilerek asgari veri kullanımına gidilmeli; geliştirilen modelin doğruluğu sürekli izlenmelidir.

- Bağlamından koparılmış algoritma[2] modelleri, bireyler ve toplum üzerinde olumsuz etkilere sebep olma riski açısından dikkatle değerlendirilmelidir.

- İnsan hakları temelli, etik ve sosyal yönelimli yapay zekâ uygulamalarının tasarlanmasına ve potansiyel önyargıların tespit edilmesine katkıda bulunabilecek akademik kurumlarla irtibata geçilmeli; şeffaflık ve paydaş katılımının zor olabileceği alanlarda tarafsız uzman kişi ve kuruluşların görüşü alınmalıdır.

- Bireylere, görüşlerini ve kişisel gelişimlerini etkileyen teknolojilere dayalı işlemelerle ilgili itiraz hakkı tanınmalıdır.

---

2 Bağlamından koparılmış algoritma, Başlangıçta belirli bir yapay zekâ modeli için tasarlanmış algoritmaların amacı dışında farklı bir amaç yada yapay zekâ modelinde kullanılmasını ifade eder.

- Yapay zekâ sistemlerinin kişisel verileri analiz etme ve kullanma gücü göz önüne alındığında, kişisel verilerin işlenmesinde, ilgili kişilerin ulusal ve uluslararası mevzuattan doğan hakları korunmalıdır.

- Uygulamalardan özellikle etkilenmesi muhtemel olan bireylerin ve grupların aktif katılımına dayalı risk değerlendirmesi teşvik edilmelidir.

- Bireylerin münhasıran kendi görüşleri dikkate alınmaksızın otomatik işlemeye dayalı olarak kendilerini etkileyecek bir karara maruz kalmamalarını sağlayacak ürün ve hizmetler tasarlanmalıdır.

- Üretimde kişilik haklarına daha az müdahale eden alternatifler de sunulmalı, kullanıcıların seçim yapma özgürlüğü güvence altına alınmalıdır.

- Ürün ve hizmetlerin tasarımından başlayarak yaşam döngüsü boyunca kişisel verilerin korunması hukukuna uygunluk açısından tüm paydaşlar için hesap verebilirliği sağlayacak algoritmalar benimsenmelidir.

- Kullanıcının veri işleme faaliyetini durdurabilme hakkı tanınmalı ve kullanıcılara ait verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi imkânı tasarlanmalıdır.

- Uygulama ile etkileşime giren kişiler, kişisel veri işleme faaliyetinin gerekçeleri, kişisel verilerin işlenmesinde kullanılan yöntemlerin detayları ile muhtemel sonuçları hakkında aydınlatılmalı ve gerekli haller için etkili bir veri işleme onay mekanizması tasarlanmalıdır.

Karar Alıcılar İçin Tavsiyeler

- Hesap verebilirlik ilkesi tüm aşamalarda gözetilmelidir.
- Kişisel verilerin korunmasına yönelik risk değerlendirme prosedürleri benimsenmeli ve sektör/uygulama/donanım/yazılım temelinde bir uygulama matrisi oluşturulmalıdır.
- Davranış kuralları ve sertifikasyon mekanizmaları gibi uygun önlemler alınmalıdır.
- Yapay zekâ modellerinin farklı bir bağlam veya amaç için kullanılıp kullanılmadığını izlemek üzere karar alıcılar tarafından yeterli kaynak ayrılmalıdır.
- Karar alma süreçlerinde insan müdahalesinin rolü tesis edilmelidir. Bireylerin, yapay zekâ uygulamaları ile sunulan önerilerin sonucuna güvenmeme özgürlüğü korunmalıdır.
- İlgili kişilerin temel hak ve özgürlüklerini önemli ölçüde etkileme ihtimali ortaya çıktığında denetim otoritelerine[3] mutlaka başvurulmalıdır.
- Denetim otoriteleri ve yetkili diğer kuruluşlar arasında, veri mahremiyeti, tüketicinin korunması, rekabetin geliştirilmesi ve ayrımcılıkla mücadele konularında işbirliği teşvik edilmelidir.

3 Denetim Otoriteleri, Yapay zekâ alanında düzenleme ve/veya denetleme yapmaya yetkili kurum ve kuruluşları ifade eder.

- Yapay zekâ uygulamalarının insan hakları, etik, sosyolojik ve psikolojik etkilerini ölçme temelli uygulama araştırmaları desteklenmelidir.

- Bireyler, gruplar ve paydaşlar bilgilendirilerek yapay zekânın büyük veri sistemleri ile birlikte, sosyal dinamikleri şekillendirmede ve onları etkileyen karar verme süreçlerinde oynayacağı rolün tartışılması konusunda aktif olarak yer almaları sağlanmalıdır.

- Verilerin güvenli, adil, yasal ve etik paylaşımını destekleyen dijital ekosistemin oluşturulabilmesi için açık yazılım tabanlı uygun mekanizmalar teşvik edilmelidir.

- İlgili kişiler bakımından yapay zekâ uygulamalarını ve etkilerini anlama konusunda farkındalığı artırmak için dijital okuryazarlık ve eğitim kaynaklarına yatırım yapılmalıdır.

- Uygulama geliştiriciler için kişisel verilerin korunması farkındalığı oluşturmak bağlamında veri mahremiyeti çerçevesinde eğitimler teşvik edilmelidir.

Kaynaklar

Aşağıdaki dokümanların da okunup değerlendirilmesi önerilmektedir:

- 6698 Kişisel Verilerin Korunması Kanunu

- 108 sayılı Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

- Avrupa Konseyi İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü tarafından yayınlanmış olan "Yapay Zekâ Ve Kişisel Verilerin Korunması Rehber İlkeleri" (https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8)

- OECD Yapay Zekâ Konseyi Önerileri (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449)

- Avrupa Konseyi'nin "Güvenilir Yapay Zekâ için Taslak Etik Kuralları" (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419)

- Avrupa Komisyonu Yapay Zekâya İlişkin Beyaz Kitabı (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf)

- Avrupa Komisyonu Yapay Zekâya İlişkin Beyaz Kitabı'na İlişkin 4/2020 sayılı EDPS (Avrupa Veri Koruma Denetçisi) Görüşü (https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf)