

KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ SEÇİLMİŞ GÜNCEL GELİŞMELER-35

- * AB Konseyi; ev kameraları, buzdolapları, televizyonlar ve oyuncaklar gibi internete bağlı ürünlerin piyasaya sürülmeden önce güvenli olmasını sağlamak amacıyla, dijital bileşenlere sahip ürünler için güvenlik gereksinimlerini düzenleyen "Siber Dayanıklılık Yasası"nı kabul etti¹.

Yeni düzenlemenin temel unsurları arasında;

- Donanım ve yazılım ürünlerinin tasarım, üretim ve piyasaya sunulma süreçlerinde AB genelinde siber güvenlik gereklilikleri getirilmesi, (örneğin, düzenlemenin gerekliliklerine uygun olduğunu göstermek üzere ürünlerde CE işareti bulunması)
- Doğrudan veya dolaylı olarak başka bir cihaza veya ağa bağlı olan tüm ürünler için bu düzenlemenin geçerli olması,
- Tüketicilerin, uygun siber güvenlik özelliklerine sahip donanım ve yazılım ürünleri seçebilmelerinin sağlanması gibi hususlar yer almaktadır.

Düzenleme, AB Resmî Gazetesi'nde yayımlanmasını takip eden yirminci günde yürürlüğe girecek ve 36 ay içerisinde tüm hükümleriyle uygulanacaktır.

- * Birleşik Krallık Veri Koruma Otoritesi (ICO), kuantum teknolojilerinin veri koruma üzerindeki olası etkilerinin ele alındığı bir rapor yayımladı². Raporda; kuantum bilgisayarlar, iletişim, sensör, zamanlama ve görüntüleme teknolojilerinin gizlilik ve veri koruma üzerindeki etkileri incelenmektedir.

Bu kapsamda, kuantum bilgisayarların mevcut kriptografik algoritmaları kırma potansiyeline sahip olabileceği belirtilmekte ve bu nedenle kuruluşların şimdiden kuantum dirençli kriptografiye hazırlanmaları gerektiği vurgulanmaktadır. Diğer yandan, mahremiyetle ilgili mevcut riskleri artırabilecek olmakla birlikte, bu teknolojilerin kişisel verilerin korunmasına yönelik yeni fırsatlar sunabileceği de ifade edilmektedir.

- * Fransa Veri Koruma Otoritesi (CNIL); mobil uygulamaların, mahremiyetin korunmasını temin edecek şekilde tasarlanmasına yardımcı olmak üzere, mobil uygulama ekosistemindeki paydaşlara yönelik bir dizi tavsiye yayımladı³.
- * Avrupa Veri Koruma Kurulu (EDPB), Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) 6(1)(f) düzenlemesi kapsamında, bir veri işleme şartı olarak "meşru menfaat"e ilişkin değerlendirmelerin yer aldığı rehberini yayımladı⁴. Rehber'e ilişkin geri dönüşlerin 20.11.2024 tarihine kadar iletebileceği belirtildi.
- * Avrupa Komisyonu, Veri Yasası'na (*Data Act*) ilişkin sık sorulan soruların açıklandığı bir doküman yayımladı⁵. Hatırlanacak olursa; gönüllü veri paylaşım mekanizmalarına olan güveni artıran Veri Yönetişimi Yasası'nı (*Data Governance Act*) tamamlayıcı nitelikte olan Veri Yasası, verilere erişilmesi ve bunların kullanımı konusunda hukuki açıklık sağlamaktadır. Bu kapsamda Veri Yasası; endüstriyel veriler başta olmak üzere, verilerin kullanılabilirliğini artıran ve veri ekonomisinde yer alan aktörler arasında verinin değerinin dağıtımında adaleti sağlarken veri odaklı inovasyonu teşvik eden bir düzenleme olup 12.09.2025 tarihinde uygulanmaya başlanacaktır.
- * Avrupa Parlamentosu Araştırma Servisi (EPRS); AB Yapay Zekâ Yasası'nın hazırlanma ve yasalaşma süreci, düzenlemenin temel noktaları ve gündeme getirdiği birtakım hususlara ilişkin açıklamalarda bulunulan bir çalışma yayımladı⁶.
- * OECD, finans alanında yapay zekâ kullanımına yönelik farklı düzenleyici yaklaşımların analiz edildiği bir çalışma yayımladı⁷.
- * Avrupa Komisyonu, güvenilir ve güvenli yapay zekânın gelişimini teşvik etmek adına AB Yapay Zekâ Paktını ve gönüllü taahhütlerini imzalayan yüzlerce şirketin ismini duyurdu⁸. İmzacılar arasında; bilgi teknolojileri, telekomünikasyon, sağlık, bankacılık, otomotiv ve havacılık gibi çeşitli sektörlerden çok uluslu şirketler ile Avrupa'daki küçük ve orta ölçekli işletmeler yer almaktadır.

AB Yapay Zekâ Paktı'nda yer alan taahhütler, katılımcı şirketleri en az üç temel eyleme bağlı kalmaya çağırmaktadır:

- Yapay zekânın kuruluş aşamasında benimsenmesini teşvik etmek ve AB Yapay Zekâ Yasası'na gelecekte uyum sağlamak için yapay zekâ yönetim stratejisi
- Yüksek riskli yapay zekâ sistemlerinin haritalandırılması ve AB Yapay Zekâ Yasası kapsamında yüksek riskli olarak sınıflandırılması muhtemel yapay zekâ sistemlerinin belirlenmesi
- Çalışanlar arasında yapay zekâ okuryazarlığını ve farkındalığını teşvik etmek, etik ve sorumlu yapay zekâ geliştirilmesini sağlamak

Bu temel taahhütlere ek olarak, imzacıların yarısından fazlasının insan gözetimi sağlama, riskleri azaltma ve deepfake gibi içerik türlerini şeffaf bir şekilde etiketleme gibi ek taahhütlerde bulunacaklarını bildirdikleri de açıklandı.

- * Avrupa Komisyonu, güvenilir yapay zekâyâ ilişkin Avrupa liderliğini güçlendirmek için yapay zekâ fabrikaları kurulması yönünde çağrıda bulundu⁹. Avrupa Yüksek Performanslı Hesaplama ağı etrafında oluşturulacak ve yeni kurulan şirketler, endüstri ve araştırmacılar gibi çeşitli Avrupa kullanıcılarına sunulacak olan yapay zekâ fabrikalarının; hesaplama gücü, veri ve yetenek olmak üzere yapay zekânın başarıya ulaşması için gerekli temel bileşenleri bir araya getireceği belirtilmektedir.
- * Avustralya'da, kuruluşların güvenli, güvenilir ve sorumlu bir şekilde yapay zekâ sistemleri geliştirmelerine ve kullanmalarına rehberlik etmesi amacıyla hazırlanan "Gönüllü Yapay Zekâ Güvenlik Standardı" yayımlandı¹⁰. Bahse konu dokümanda; on temel koruyucu önlem, bunların nasıl kullanılacağı ve ne zaman uygulanacağına dair örnekler, standardın nasıl geliştirildiği, standarda yönelik temel kavramlar ve hukuki bağlamı gibi hususlara yer verilmekte olup on temel koruyucu önlem ise şu şekilde belirtilmektedir:
 - (1) Yönetişim, dahili kapasite ve düzenleyici uyumluluk için bir strateji dahil olmak üzere hesap verebilirlik süreci oluşturulması, uygulanması ve yayımlanması,
 - (2) Riskleri belirlemek ve azaltmak için bir risk yönetimi süreci oluşturulması ve uygulanması,
 - (3) Yapay zekâ sistemlerinin korunması, veri kalitesini ve kaynağını yönetmek için veri yönetimi önlemleri uygulanması,
 - (4) Modelin performansını değerlendirmek ve kullanım aşamasında sistemi izlemek için yapay zekâ modellerinin ve sistemlerinin test edilmesi,

- (5) Yaşam döngüsü boyunca anlamlı insan gözetimi elde etmek için bir yapay zekâ sisteminde insan kontrolünün veya müdahalesinin etkinleştirilmesi,
- (6) Yapay zekâ destekli kararlar, yapay zekâ ile etkileşimler ve yapay zekâ tarafından oluşturulan içerik hakkında son kullanıcıların bilgilendirilmesi,
- (7) Yapay zekâ sistemlerinden etkilenen kişilerin kullanım veya sonuçlara itiraz edebilmesi için süreçler oluşturulması,
- (8) Yapay zekâ tedarik zincirindeki diğer kuruluşların, riskleri etkili bir şekilde ele almalarına yardımcı olmak üzere veriler, modeller ve sistemler hakkında şeffaf olunması,
- (9) Üçüncü tarafların bu koruyucu önlemlere uyumu değerlendirmelerine olanak sağlamak amacıyla kayıt tutulması ve tutulan bu kayıtların saklanması,
- (10) Paydaşların sürece dahil edilmesi ve güvenlik, çeşitlilik, kapsayıcılık ve adillik konularına odaklanarak paydaşların ihtiyaçların ve koşulların değerlendirilmesi.

* Dünya Ekonomik Forumu, üretici yapay zekâ alanındaki hızlı gelişmelere yanıt olarak Accenture ile iş birliği içerisinde bir rapor yayımladı¹¹. Raporda, üretici yapay zekâ için dayanıklı bir yönetim çerçevesi sunulmakta olup bu kapsamda, kamu-özel sektör iş birliklerinin teşvik edilmesi ve uluslararası iş birliğiyle öngörülü yönetim modelleri geliştirilmesi hedeflenmektedir. Raporda öne çıkan hususlar arasında; düzenleyici boşlukların doldurulması, paydaşların karşılaştıkları yönetsel zorlukların ele alınması ve önümüzdeki süreçte karşılaşılabilecek teknolojik gelişmelere hazırlıklı olunmasına yönelik öneriler yer almaktadır.

* Fransız Siber Güvenlik Ajansı ve Alman Federal Bilgi Güvenliği Ofisi tarafından hazırlanan bir raporda, yapay zekâ kodlama araçlarının güvenli kullanımına yönelik öneriler sunulmaktadır¹². Raporda, bu araçların yazılım geliştirme sürecinde sunduğu fırsatlar ile beraberinde getirdiği riskler ele alınmakta ve bu risklerin nasıl azaltılabileceğine dair somut örnekler paylaşılmaktadır.

Fırsatlar:

- Verimlilik: Kod oluşturma, test senaryoları ve kod biçimlendirme gibi görevleri otomatikleştirerek geliştiricilerin iş yükünü hafifletir.
- Kodu Anlama: Yeni projelerde kodu açıklamak suretiyle geliştiricilerin projelere hızlı bir şekilde adapte olmasına yardımcı olur.
- Programlama Dilleri Arasında Çeviri: Eski kodları, modern programlama dillerine çevirerek bakım süreçlerini kolaylaştırır.

Riskler:

- Veri Güvenliği: Kullanıcı girdileri hassas bilgiler içerebilir ve bu bilgiler sızabilir.
- Kod Kalitesi: Oluşturulan kodun kalitesi ve güvenliği garanti edilemez, güvenlik açıkları bulunabilir.
- Saldırı Riski: Yazılım geliştirme sırasında büyük dil modelleri tabanlı yapay zekâ sistemlerinin kullanılması, kötü niyetli aktörler tarafından istismar edilebilecek yeni saldırı türlerinin ortaya çıkmasına olanak tanıyabilir.

Öneriler:

- Tecrübeli Geliştiriciler: Yapay zekâ, deneyimli geliştiricilerin yerini almamalı ve destekleyici olarak kullanılmalı.
- Risk Analizi: Yapay zekâ araçlarını kullanmadan önce güvenlik riskleri değerlendirilmelidir.
- Kod Kontrolü: Yapay zekâ tarafından oluşturulan kod, geliştiriciler tarafından gözden geçirilmeli ve doğrulanmalıdır.

* Avustralya'da bir avukatın, yapay zekâ yazılımı kullanarak mahkemeye yanlış bilgi sunduğu ortaya çıktı¹³. Melbourne'da bir avukat, aile mahkemesinde görülen bir davada yapay zekâ tarafından hazırlanan ve gerçekte var olmayan davaları içeren bir liste sunduğu gerekçesiyle şikâyet edildi. Hâkimin, listede yer alan davaların var olmadığını fark etmesinin ardından avukat, yapay zekâ destekli bir yazılım kullandığını ve oluşturulan listeyi doğrulamadan mahkemeye sunduğunu kabul etti.

- * TBMM Genel Kurulunda, yapay zekâyla ilgili Meclis Araştırma Komisyonu kurulması kabul edildi¹⁴.
- * T.C. İletişim Başkanlığı, sosyal medya kullanımında kamu kurumlarına yol göstermesi amacıyla “Kurumsal Sosyal Medya Kullanım Rehberi” hazırlandığını duyurdu¹⁵. Toplam on bölümden oluşan bu Rehber’de, kamu kurumlarının sosyal medyayı bilinçli, etkili ve sorumlu bir şekilde kullanmalarının sağlanması amaçlanmaktadır. Rehber’de; kurumsal sosyal medya kullanımında genel ilkeler, kurumsal sosyal medya hesabının güvenliğine ilişkin öneriler, kurumsal sosyal medya hesap yönetimi, etik kurallar ve hukuki sorumluluklar, sosyal medyada kriz iletişimi, dezenformasyonla mücadele ve sosyal medyada teyit, sosyal medya hesapları için önerilen örnek uygulamalar gibi konular ele alınmaktadır.

Bahse konu Rehber’de kişisel verilerin korunmasına ilişkin belirlemeler de yer almakta olup bu çerçevede;

- Sosyal medyada yüzde yüz güvenliğin söz konusu olmadığı, bu nedenle nüfus cüzdanının fotoğrafı, kimlik numarası, annenin evlenmeden önceki soyadı gibi kişisel bilgilerin mesajlaşma ve sosyal medya uygulamaları aracılığıyla paylaşılmaması,
- Kurumsal sosyal medya kullanımında genel ilkeler kapsamında, kişisel verilerin korunması ve gizliliğine özen gösterilmesi ve ilgili mevzuata uygun hareket edilmesi,
- Sosyal medya hesaplarının kullanımı, etkileşimi ve paylaşımları hususlarında 6698 sayılı Kişisel Verilerin Korunması Kanunu da dâhil olmak üzere bir dizi kanun ve diğer mevzuat hükümlerine uyulması,
- Etik kurallar ve hukuki sorumluluklar bağlamında, kişisel verilere ilişkin mevzuata uygun hareket edilmesi ve özel hayatın gizliliğinin korunması gerektiği belirtilmektedir.

İLGİLİ LİNKLER

¹<https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/>, 10.10.2024.

²<https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-quantum-technologies/>, 09.10.2024.

³<https://www.cnil.fr/en/mobile-applications-cnill-publishes-its-recommendations-better-privacy-protection>, 24.09.2024.

⁴https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en, 09.10.2024.

⁵<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>, 06.09.2024.

⁶[https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)698792](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792), 02.09.2024.

⁷https://www.oecd.org/en/publications/regulatory-approaches-to-artificial-intelligence-in-finance_f1498c02-en.html, 05.09.2024.

⁸https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4864, 25.09.2024.

⁹<https://digital-strategy.ec.europa.eu/en/news/eu-boosts-european-ai-developers-ai-factories-call-proposals>, 10.09.2024.

¹⁰<https://www.industry.gov.au/publications/voluntary-ai-safety-standard#read-the-voluntary-ai-safety-standard-2>, 05.09.2024.

¹¹<https://www.weforum.org/publications/governance-in-the-age-of-generative-ai/>, 08.10.2024.

¹²https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/ANSSI_BSI_AI_Coding_Assistants.html, 04.10.2024.

¹³<https://www.theguardian.com/law/2024/oct/10/melbourne-lawyer-referred-to-complaints-body-after-ai-generated-made-up-case-citations-in-family-court-ntwnfb>, 10.10.2024.

¹⁴<https://www.tbmm.gov.tr/Haber/Detay?Id=b6c9a6c7-d544-42f1-8b16-01924ea8ae5f>, 02.10.2024.

¹⁵<https://www.iletisim.gov.tr/turkce/duyurular/detay/iletisim-baskanligindan-kurumsal-sosyal-medya-kullanim-rehberi>, 10.10.2024.