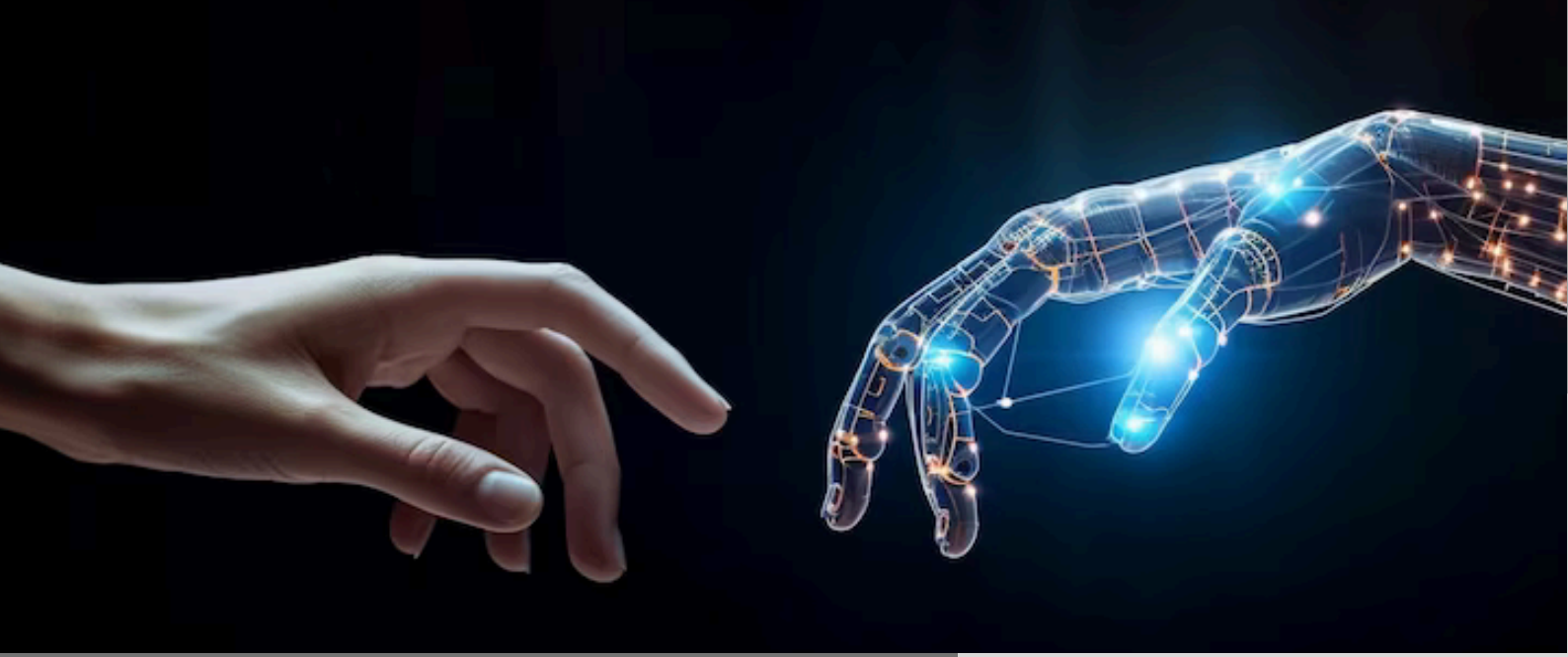




BİLİŞİM HUKUKU KOMİSYONU BÜLTENİ



BU SAYIMIZDA

- 1 **YAPAY ZEKA YASASI KANUN TASLAĞIMIZIN OECD VE AB DÜZENLEMELERİ BAĞLAMINDA İNCELEMESİ**
AV. İREM NALBANT
- 4 **YENİ AB YZ REGÜLASYONUNDA ŞİRKETLERİN KARŞILAŞABİLECEĞİ SINIRLAMALAR**
AV. OĞUZHAN SEYMEN
- 6 **TÜRKİYE'NİN ARTIK BİR KRİPTO YASASI VAR**
AV. AHMET KALKAN
- 8 **YAPAY ZEKA İLE İŞLENEN SUÇLAR**
AV. GÖKÇEN YÜCEL

BÜLTENİMİZDE



Teknoloji, bizlerin takip edemeyeceği hızda gelişmekte ve hayatımızın ayrılmaz bir parçası haline gelmektedir. Her gün gelişen teknolojiye ayak uydurmak biz hukukçular için zorunlu hale gelmiştir. Yapay zeka, blockchain, fintech, NFT, fikri ve sınai mülkiyet, internet, e-ticaret, kişisel verilerin korunması gibi kavramların insan hakları, ceza hukuku, sözleşmeler hukuku gibi hukukun temel alanlarında incelemek ve bunlar hakkında bilgi sahibi olmak biz hukukçuların bakış açısını geleceğe yönlendirecektir.

Aynı zamanda bu kazanımlar ile hukukçular, bilişim dünyasında yoğun zaman geçiren milyarlarca insanın işlem güvenliğini sağlamak ve dijital anlamda da geleceğe temiz bir dünya bırakmak görevi de üstlenmektedir .

Bu düşünceler ile bizler de bilişim ve hukukun kesiştiği alanlardaki gelişmeleri takip ederek siz değerli okuyucularımıza aktarabilmek, yeni çıkan yasal düzenlemeleri sizlerle buluşturabilmek adına Bursa Barosu Bilişim Hukuku Komisyonu olarak sizlere her ay bülten hazırlıyoruz.

Bilişim hukuku alanında meslektaşlarımızın sizler için hazırladığı makaleleri, haberleri, dizi, film ve kitap önerilerini ve daha birçok içeriği her ay bültenimizden takip edebilirsiniz.

Bültenimizin siz okuyucularımız için bilgi verici olmasını ve okurken keyifli zaman geçirmenizi temenni ediyoruz.

Saygılarımızla.

24 Haziran 2024 tarihinde Türkiye'nin ilk yapay zeka yasasına ilişkin kanun taslağı TBMM'ye sunuldu. Teklif ile, yapay zeka teknolojilerinin güvenli, etik ve adil bir şekilde kullanılmasının sağlanması, kişisel verilerin korunmasının temin edilmesi, gizlilik haklarının ihlal edilmesinin önlenmesi ile yapay zeka sistemlerinin geliştirilmesi ve kullanımına yönelik düzenleyici bir çerçevenin oluşturulmasının amaçlandığı belirtilmiştir.

Yasa tasarısında, yapay zeka *"insan benzeri bilişsel işlevleri yerine getirebilen ve öğrenme, mantık yürütme, problem çözme, algılama ve dil anlama gibi yeteneklere sahip bilgisayar tabanlı sistemler"* olarak tanımlanmış olup yapay zeka sistemlerine ilişkin sağlayıcılar, dağıtıcılar, kullanıcılar, ithalatçılar ve distribütörler ise *"yapay zeka operatörleri"* olarak tanımlanmıştır.

OECD'nin yapay zekaya ilişkin -bağlayıcı olmayan- tanım ve görüşleri ise 2019 yılında yayınlanmış, ardından Mayıs 2024'te güncellenmiştir. OECD'nin yaptığı tanımda ise şöyle denmiştir: *"Bir yapay zeka sistemi, farklı düzeylerde özerklikle çalışmak üzere tasarlanmış ve 'dağıtımdan sonra uyarlanabilirlik' gösterebilen makine tabanlı bir sistemdir. Bu sistem, açık veya örtük hedefler doğrultusunda aldığı girdilerden, fiziksel veya sanal ortamları etkileyebilecek tahminler, içerikler, öneriler veya kararlar gibi çıktılar üretmek için çıkarımlar yapar."*

"Dağıtımdan sonra uyarlanabilirlik" ifadesi, yapay zekanın eğitildikten sonra başlangıçta programlandığı haliyle sınırlı kalmaması; aksine, zamanla öğrenmesi, gelişerek performansını iyileştirmesini ifade etmektedir.

Her iki tanımda da, belirli bilişsel işlevleri yerine getiren ve belirli görevlerde uzmanlaşmış sistemler nazara alınmış ve dar yapay zeka modelleri tanımlanmıştır. Her ne kadar henüz bir uygulaması mevcut olmasa da, tanımlarda *"yapay zeka"* olarak verilen bilgilerin *"dar yapay zeka"*ya yönelik olduğunu belirtmek gerekir.

Yasa tasarısında ayrıca yapay zeka teknolojilerinin kullanıcılar ve kamu düzeni açısından güvenli bir şekilde kullanılabilmesi için gerekli olan temel prensiplere değinilmiş,

yapay zeka sistemlerinin toplum yararına hizmet etmesi ve bireylerin haklarının korunmasını sağlamak amacıyla bazı ilkeler belirlenmiştir.

Bu ilkeler güvenlik, şeffaflık, adillik, hesap verebilirlik ve gizlilik olarak sıralanmıştır.

OECD tarafından altı çizilen ilkeler ise insan hakları ve demokratik değerler, adillik, gizlilik, şeffaflık, açıklanabilirlik, sağlamlık, güvenlik ve sorumluluk şeklinde olmuştur. Bu ilkeler, yapay zekayı güvenilir bir şekilde geliştirmek için yapay zeka aktörlerine rehberlik etmesi ve etkili yapay zeka politikaları için öneri olarak belirlenmiştir.

Yasa tasarısındaki *"güvenlik"* ilkesi altında incelenebilecek olan *"sağlamlık"* (robustness) ilkesi, algoritmaların ve kararların doğru ve adil olduğundan emin olunmasıdır. Robust bir sistem, yanlış anlamaları veya hatalı sonuçları önleyerek, kullanıcının yapay zekanın işlemlerine duyduğu güveni karşılamaktadır.

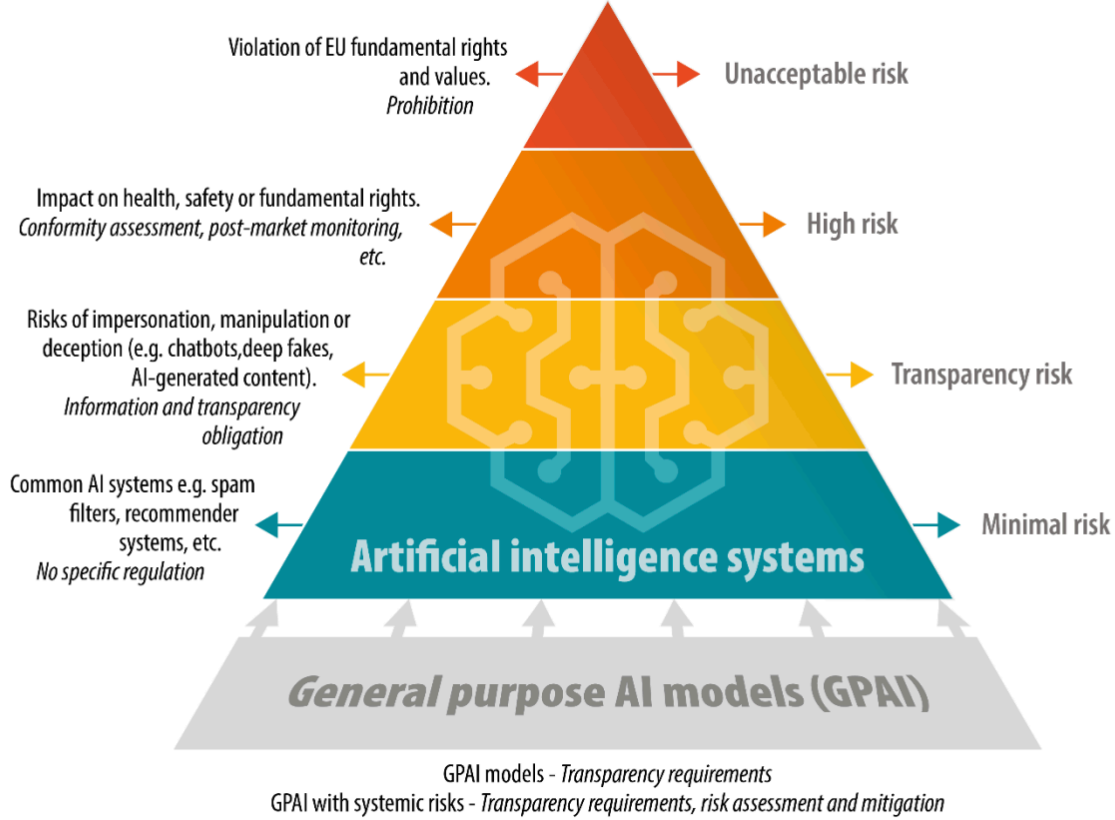
Yapay zekanın en büyük sorunlarından olan ön yargılı yapay zeka (ai bias) konusu göz önüne alındığında, sağlamlık başlığının ayrı bir ilke olarak ele alınması ve kanunda detaylıca düzenlenmesi yerinde olacaktır.

Yasa tasarısının devamında yapay zeka sistemlerinin geliştirilmesi ve kullanımı sırasında ortaya çıkabilecek risklerin belirlenmesi, bu risklere yönelik önlemlerin alınması ve yüksek risk taşıyan sistemlerin uygunluk değerlendirmesine tabi tutulması gerekliliği vurgulanmıştır. Denetim makamlarına bu konuda denetleme ve ihlalleri tespit etme yetkisi verilmiştir.

Risk temelli yaklaşım Avrupa Birliği Yapay Zeka Kodu'nda (EU AI Act) benimsenmiş olup yapay zeka uygulamalarının risk seviyeleri ve hangi risklerin kabul edilemez olduğu incelenmiştir. Bu kapsamda aşağıdaki gibi dört kategori belirlenmiştir:

Risk-based approach

EU AI act risk-based approach



Data source: [European Commission](https://europeancommission.europa.eu)

Açıkça Yasaklanması Gereken Sistemler: Bu uygulamalar, bireylerin güvenliği, geçim kaynakları ve hakları için kabul edilemez bir risk oluşturduğu düşünülen uygulamalar olarak nitelenmiştir. Aşağıdaki şekilde gruplandırılmışlardır:

- Zararlı manipülatif 'üstbilinç teknikleri' kullanan yapay zeka sistemleri.
- Belirli savunmasız grupları (fiziksel veya zihinsel engelli bireyler) hedef alan yapay zeka sistemleri.
- Kamu otoriteleri tarafından veya adlarına sosyal puanlama amaçlarıyla kullanılan yapay zeka sistemleri.
- Hukuki sınırlı durumlarda dışında, kolluk kuvvetlerinin kullanması için kamuya açık alanlarda canlı biyometrik tanımlama sistemleri.

Düzenlemeye (Sınırlamaya) Tabi Tutulması Gereken Sistemler: Bu sistemler, bireylerin güvenliği veya temel haklarını olumsuz etkileyebilecek potansiyele sahip olarak belirlenmiştir ve iki kategori arasında ayırım yapmaktadır:

- Ürünlerin güvenlik bileşeni olarak kullanılan veya AB sağlık ve güvenlik uyumlaştırma mevzuatı kapsamında olan sistemler (örneğin oyuncaklar, havacılık, otomobiller, tıbbi cihazlar, asansörler).
- Komisyon'un yetki verilen eylemler aracılığıyla gerektiğinde güncelleyebileceği eklerde belirtilen sekiz özel alanda kullanılan sistemler.

Bu tür yüksek riskli yapay zeka sistemleri piyasaya sürülmeden veya hizmete konulmadan önce risk yönetimi, teknik dayanıklılık, veri eğitimi ve yönetimi, şeffaflık, siber güvenlik gibi bir dizi gereksinimi karşılamak zorunda olduğu belirtilmiştir.

Sınırlı Risk Taşıyan Yapay Zeka Sistemleri: Bu kategori, insanlarla etkileşim halinde olan (örneğin, sohbet botları), duygu tanıma sistemleri, biyometrik sınıflandırma sistemleri ve görüntü, ses veya video içeriği oluşturan veya manipüle eden yapay zeka sistemlerini içermektedir. Bu sistemler, sınırlı bir şeffaflık yükümlülüğüne tabi olmalıdır, denmiştir.

Düşük veya Minimum Risk Taşıyan Diğer Yapay Zeka Sistemleri: AB içinde geliştirilebilecek ve kullanılabilecek diğer tüm yapay zeka sistemleri, ek hukuki yükümlülüklerle gerek duyulmaksızın kullanılabilir. Ancak yine de, yüksek riskli olmayan yapay zeka sistemleri sağlayıcılarını, yüksek riskli yapay zeka sistemleri için zorunlu gereksinimleri gönüllü olarak uygulamaya teşvik etmek için davranış kuralları oluşturulması öngörülmüştür.

Görüldüğü üzere AB, yapay zeka sistemlerinin minimum risk taşıyanlarının dahi yüksek risk taşıyanlar kadar korunaklı standartlara sahip olması gerektiğini öngörmektedir. Bu bağlamda yapay zeka uygulamalarının oluşturulması, geliştirilmesi ve kullanımına istisnai bir bakış açısıyla bakıldığı söylenebilir.

TBMM'ye sunulan yasa taslağının gerekçesinde de, "Risk değerlendirmesi ve uygunluk değerlendirmesi mekanizmaları, yapay zeka sistemlerinin topluma fayda sağlamasını ve olası zararların en aza indirilmesini hedeflemektedir. Yüksek risk içeren yapay zeka sistemleri için özel güvenlik önlemleri ve sürekli izleme mekanizmaları oluşturularak, bu sistemlerin güvenilirliği ve doğruluğu sağlanmalıdır." denerek benzer bir risk bazlı yaklaşım vurgusu yapılmıştır.

Tasarıda ayrıca, yasak yapay zeka uygulamalarının kullanılması, kurallara riayet etmeyen operatörler ve denetim makamlarına yanlış bilgi sağlanması gibi ihlaller açısından "para cezası" uygulanacağı düzenlenmiştir.

Neticede mevcut yasa tasarısının gerek OECD gerek AB öneri veya düzenlemelerine yabancı olmadığını, yapay zeka kullanımının kullanıcı dostu hale getirilebileceğini söylemek mümkün. Yasanın son halinin ülkemize yararlı olmasını diliyoruz.

KAYNAKÇA:

1. <https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y2/T2/WebOnergeMetni/e50ccc8a-ab90-45fa-a553-76b880c78fb8.pdf>
2. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)
3. <https://oecd.ai/en/ai-principles>

YENİ AB YZ REGÜLASYONUNDA ŞİRKETLERİN KARŞILAŞABİLECEĞİ SINIRLAMALAR

AV. OĞUZHAN SEYMEN

1- Yapay Zeka(YZ) kullanıcısı şirketler, AB Regülasyonu ile neden sınırlamalara tabi tutulabilir?

İlgili regülasyonun; sadece YZ kullanıcısı şirketler nezdinde değil, artık günlük hayatın ve iş hayatının ayrılmaz bir parçası haline geldiğini söylemek mümkündür. Bu da demektir ki günlük hayatta bir yıkıcı teknoloji devrimi yaşanmakta. Bu devrim de haliyle "etik ve güvenlik" tartışmalarını beraberine getiriyor. Dolayısıyla bu tartışmalar, YZ kullanıcısı şirketlerin adeta kulaklarını sınırlamalar ile çınlatacaktır.



2- Regülasyonun getireceği sınırlamalar, riskler açısından hangi kapsamdadır ve sınırlama ne amaçladır?

İlk soruda belirtilene ek olarak, sınırlamanın amacı, yapay zekanın "güvenli, şeffaf ve etik kurallara uygun şekilde" kullanılmasıdır. Risklerin sınırlama kapsamı ise "yüksek riskli YZ, sınırlı riskli YZ, minimal riskli YZ" şeklindedir.

3- Riske göre sınırlandırmalara ne gibi örnekler verilebilir?

İkinci soruda bahsedilen 3 gruba bakıldığında;

Yüksek riskli YZ sisteminden anlaşılması gereken; "sağlık, güvenlik, kritik altyapı, eğitim, iş ve yönetim" gibi önemli riskleri taşıyan alanlardır. Bunlara örnek olarak da "otonom araçlar, tıbbi cihazlar, işçi işe alım yazılımları" gösterilebilir.

Sınırlı risk yapay zeka sisteminden anlaşılması gereken de daha düşük risk taşıyıp kullanıcıların yine de bilgilendirilmesi

zorunluluğu bulunan sistemlerdir mesela chat botlar yüz tanıma sistemleri ve müşteri hizmetleri bu sisteme örnek verilebilir

Minimal riskli yapay zeka sistemleri de düşük riskli uygulamalar olup öncekinden farklı olarak özel bir regülasyona tabi değildir

Mesela oyunların yapay zekaları ve e-posta filtre sistemleri minimal riskteki yapay zeka sistemi kapsamındadır.

4- yapay zeka sistemini kullanan şirketler üç farklı grup bakımından nasıl bir sınırlamaya tabi tutuluyor?

Yukarıdaki tanımlamalardan sonra yine üç grubu ayrı ayrı değerlendirelim.

A]Yüksek riskli yapay zeka sistemlerinde 3 kayda değer sınırlama var ilki kapsamlı test ve sertifikasyon, 2.'si gözetim ve raporlama, 3.'sü de güvenlik ve şeffaflıktır.

Mesela bu sınırlamalara; otonom araçların güvenlik performansının sürekli izlenmesine raporlanması ve işe alım yazılımı noktasında adayların değerlendirme kriterlerin açıkça belirtilmesi örnek gösterilebilir.

B] sınırlı riskli yapay zeka sistemlerine de sınırlama bakımından kullanıcı bilgilendirmek ve verileri korumak önemlidir. Söz gelimi müşteri hizmetlerinin chat kodları kullanıcılara bir yapay zeka ile iletişim kurulduğunu bilgilendirmelidir.

C] minimal riskli sistemler bakımından da belirtildiği üzere özel bir regülasyon sahibi olmayıp etik kuralları uyulması ve genel veri korunmanın sağlanması olmazsa olmazdır.

5- örneklerde belirtilen tıbbi cihazlar, işe alım yazılımları ve otonom araçlardaki sınırlamalar; şirketlere örnek oluşturması için biraz daha nasıl detaylandırılabilir?

Tıbbi cihazlar bakımından; medikal teknoloji şirketi, teşhis cihazını piyasaya sürmeden önce klinik denemeler yapması

gerekir ve denemelerin sonuçlarını idareye, düzenleyici kurumlara rapor etmesi gerekir.

Otonom araçlar açısından da mesela bir otomobil üretilirken, ilgili otomobili piyasayı sürülmeden önce güvenlik testinden geçmesi gerekmekte olup sonuçlara göre düzenleyici otoritelere sunulması gerekir.

İşe alım yazılımı noktasında da aynı şekilde, adayların nasıl değerlendirildiği açık açık belirtilmeli.

6- Her yazıdaki o klasik temenni :)

Günümüz dünyası Avrupa Birliği'nin yeni yapay zeka regülasyonu ile birlikte mükemmel bir dönüşümden ve devrimden geçmektedir.

Bu dönüşümün ortaya çıkardığı sınırlamalar ile de pekala yapay zeka sistemlerinden, güvenli, şeffaf ve etik kurallara uygun süreçler beklenmektedir .

Regülasyon yüksek ve kutsal amaçlar içermektedir. çünkü şayet yapay zekanın, dünyanın geri kalan ömründe hayatımızın olmazsa olmaz bir parçası haline gelecek ise bu sınırlamalara konu prensiplere, ömür verilesi prensipler diyebiliriz.

Yukarıda belirtilen her bir sınırlama elbette kişisel verilerin korunmasına ve uygulamaların etik olmasına hizmet etmektedir.

Temennimiz Avrupa Birliği yapay zeka regülasyonunun uygulayıcısı ülkeler ve AB regülasyonuna ilişkin çerçeve Sözleşmenin taraflarının yanı sıra, Türkiye'nin de yapay zeka bakımından yakın zamanda muhatap olacağı bu düzenlemelerden; sanayi, enerji, tıp ve daha birçok hizmet sektöründe adil, etik ve kişisel verilerin korunduğu bir dünya inşası ile hizmet sağlayıcı ve kullanıcıların temel hak ve hürriyetlerini koruyabilmesidir.

KAYNAKÇA:

1. Avrupa Komisyonu. [Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)]
2. Kişisel Verileri Koruma Kurumu (KVKK) resmi web sitesi
3. AB Dijital Strateji Belgesi

TÜRKİYE'NİN ARTIK BİR KRIPTO YASASI VAR

AV. AHMET KALKAN

Kripto piyasasına ilişkin yeni düzenleme Meclis Genel Kurulu'nda kabul edildi. Düzenlemeyle mağduriyetlere neden olan yasal boşlukların giderilmesi amaçlanıyor.

Yeni kanunla, hizmet sağlayıcılar için sermaye şartı getirildi. Böylece hem yatırımcı korunacak hem de hizmet veren firmalara bir dizi yaptırım uygulanacak. Kripto para kullanıcıları ile ilişkilerin nasıl kurulacağı ve kimlik tespitinin nasıl yapılacağı da yasa ile düzenlendi.

Düzenlemeye göre hizmet sağlayıcı kuruluş ve faaliyetler için Sermaye Piyasası Kurulu'ndan izin alınacak. Kripto varlıkların ihracı, satışı ve dağıtımı için de SPK'ya yetki verildi. Tüm transfer işlemleri kayıt altına alınacak.

Yasaya göre izin almaksızın kripto varlık hizmet sağlayıcısı olarak faaliyet yürüttüğü tespit edilen gerçek kişiler ve tüzel kişilerin yetkililerine 3 yıldan 5 yıla kadar hapis ve 5 bin günden 10 bin güne kadar adli para cezası verilecek.

Kripto varlık hizmet sağlayıcı görevi nedeniyle kendisine tevdi edilen veya koruma, saklama ve gözetimiyle yükümlü olduğu para veya para yerine geçen evrak veya senetleri, diğer malları veya kripto varlıkları kendisinin ya da başkasının zimmetine geçiren kripto varlık hizmet sağlayıcı yönetim kurulu başkan ve üyeleri ile diğer mensupları, 8 yıldan 14 yıla kadar hapis ve 5 bin güne kadar adli para cezası ile cezalandırılacak; kripto varlık hizmet sağlayıcının zararını tazmin edecek.

Suçun, zimmetin açığa çıkmamasını sağlamaya yönelik hileli davranışlarla işlenmesi halinde faile 14 yıldan 20 yıla kadar hapis ve 20 bin güne kadar adli

para cezası verilecek. Ancak, adli para cezasının miktarı kripto varlık hizmet sağlayıcının ve müşterilerinin uğradığı zararın 3 katından az olamayacak.

İzni kaldırılan kripto varlık hizmet sağlayıcının; hukuken veya fiilen yönetim veya kontrolünü elinde bulundurmuş olan gerçek kişi ortaklarının, kripto varlık hizmet sağlayıcının ya da müşterilerinin kaynaklarını kendi veya başkalarının menfaatine kullanırmak fiillerini işleyenlere 12 yıldan 22 yıla kadar hapis ve 20 bin güne kadar adli para cezasına hükmolunacak.



Kanunda "cüzdan" kripto varlıkların transfer edilebilmesini ve bu varlıkların ya da bu varlıklara ilişkin özel ve açık anahtarların çevrim içi veya çevrim dışı olarak depolanmasını sağlayan yazılım, donanım, sistem ya da uygulamalar olarak tanımlandı. Kanuna göre, "kripto varlık" da dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan, değer veya hak ifade edebilen gayri maddi varlıklar olarak tanımlanıyor.

"Kripto varlık hizmet sağlayıcı", platformları, kripto varlık saklama hizmeti sağlayan kuruluşları ve bu Kanuna dayanılarak yapılacak düzenlemelerde

kripto varlıkların ilk satış ya da dağıtımı dahil olmak üzere kripto varlıklarla ilgili olarak hizmet sağlamak üzere belirlenmiş diğer kuruluşlar olarak yer alırken, "kripto varlık saklama hizmeti" platform müşterilerinin kripto varlıklarının veya bu varlıklara ilişkin cüzdandan transfer hakkı sağlayan özel anahtarların saklanması, yönetimini veya Sermaye Piyasası Kurulunca (SPK) belirlenecek diğer saklama hizmetlerini tanımlayacak.

"Platform" kripto varlık alım-satım, ilk satış ya da dağıtım, takas, transfer, bunların gerektirdiği saklama ve belirlenebilecek diğer işlemlerin bir veya daha fazlasının gerçekleştirildiği kuruluşlar olarak tanımlanıyor.

Kanunla, izinsiz sermaye piyasası faaliyetlerinin internet aracılığıyla yürütüldüğünün tespit edilmesi halinde uygulanacak tedbirler hüküm altına alınıyor. Buna göre, gelişen teknolojiyle birlikte internet ortamında işlenen suça konu yayınların içerik veya yer sağlayıcısının belirlenmesinde yaşanan sorunlar nedeniyle içeriğin çıkarılması veya erişimin engellenmesi kararı verilebilecek suçlarda yurt içi-yurt dışı ayrımının kaldırılmış olmasına uygun olarak izinsiz sermaye piyasası faaliyetlerinin internet aracılığıyla yürütülmesinde de yurt içi-yurt dışı ayrımı kaldırılıyor. Uygulanacak tedbirlere, içeriğin çıkarılması tedbiri de ekleniyor.

İzinsiz sermaye piyasası faaliyetlerinin internet aracılığıyla yürütüldüğü tespit edildiğinde, internet aracılığıyla yapılan yayınlarla ilgili olarak içeriğin çıkarılmasına veya erişimin engellenmesine Kurul tarafından karar verilecek ve uygulanmak üzere Erişim Sağlayıcıları Birliğine gönderilecek.

YAPAY ZEKA İLE İŞLENEN SUÇLAR

Av. GÖKÇEN YÜCEL

Giriş

Yapay zeka (YZ) teknolojisinin hızlı gelişimi, birçok alanda büyük fırsatlar sunarken, suç dünyasında da yeni kapılar açmıştır. YZ, özellikle siber suçlar, dolandırıcılık, kimlik hırsızlığı ve çeşitli yasa dışı faaliyetlerde kullanılarak suçlulara avantaj sağlamaktadır. Bu makalede, YZ teknolojisinin suç işlemek amacıyla nasıl kullanıldığını, bu tür suçların etkilerini ve önleyici tedbirlerin neler olabileceğini ele alacağız.

Yapay Zeka ile İşlenen Suçların Türleri

Siber Suçlar: Yapay zeka, siber saldırılar düzenlemek için güçlü bir araç haline gelmiştir. Özellikle makine öğrenmesi ve derin öğrenme teknikleri kullanılarak, siber saldırılar daha sofistike ve etkili hale getirilmektedir. Örneğin, YZ destekli zararlı yazılımlar (malware) ve fidye yazılımları (ransomware), sistemleri tespit edilmeden ele geçirebilmektedir.

Dolandırıcılık ve Kimlik Hırsızlığı: YZ, dolandırıcılık ve kimlik hırsızlığı gibi finansal suçlarda da kullanılmaktadır. Yapay zeka algoritmaları, büyük veri setlerini analiz ederek sahtecilik aktivitelerini tespit etmekte ve bu aktiviteleri gerçekleştirenlerin izini sürmekte kullanılmaktadır. Ancak, aynı teknolojiler suçlular tarafından da kimlik bilgilerini çalmak ve sahte hesaplar oluşturmak için kullanılabilmektedir.



Deepfake Teknolojisi: Deepfake, yüz tanıma ve video manipülasyonu teknolojilerini kullanarak sahte video ve ses kayıtları oluşturma yöntemidir. Bu teknoloji, sahte haberler yaymak, dolandırıcılık yapmak veya itibar suikastı düzenlemek için kullanılabilir. Örneğin, deepfake videoları kullanılarak ünlü kişilerin itibarları zedelenebilir veya sahte kimliklerle yasa dışı işlemler yapılabilir.

Yapay Zeka Suçlarının Etkileri

YZ ile işlenen suçlar, bireyler, kurumlar ve toplum üzerinde derin ve geniş kapsamlı etkilere sahiptir. Kimlik hırsızlığı ve dolandırıcılık, mağdurların mali kayıplar yaşamasına neden olabilirken, deepfake teknolojisi, bireylerin ve kurumların itibarlarını zedeleyebilir. Ayrıca, bu tür suçlar güven kaybına neden olmakta ve dijital dünyada daha fazla güvenlik önlemi alınmasını zorunlu kılmaktadır.

Bireysel Etkiler: YZ destekli kimlik hırsızlığı ve dolandırıcılık, bireylerin mali güvenliğini tehdit etmektedir. Kimlik bilgileri çalınan kişiler, bu bilgilerin kötüye kullanılması sonucu ciddi mali kayıplar yaşayabilir ve uzun süreli hukuki sorunlarla uğraşmak zorunda kalabilirler.



Kurumsal Etkiler: Şirketler, YZ destekli siber saldırılar nedeniyle büyük mali kayıplar yaşayabilirler. Bu tür saldırılar, veri ihlallerine yol açarak şirketlerin müşteri bilgilerini tehlikeye atabilir ve marka itibarlarını zedeleyebilir.

Toplumsal Etkiler: Deepfake videoları ve diğer YZ destekli manipölasyon teknikleri, toplumsal güveni zayıflatabilir ve yanlış bilgilendirme kampanyalarına zemin hazırlayabilir. Bu tür teknolojiler, seçimler ve diğer demokratik süreçler üzerinde olumsuz etkilere sahip olabilir.

Önleyici Tedbirler

YZ ile işlenen suçlarla mücadele etmek için çeşitli stratejiler ve teknolojiler geliştirilmektedir. Bu tedbirler arasında yasal düzenlemeler, teknolojik çözümler ve bilinçlendirme kampanyaları bulunmaktadır.

Yasal Düzenlemeler: YZ teknolojilerinin kötüye kullanımını önlemek için güçlü yasal çerçeveler gereklidir. Yasal düzenlemeler, YZ'nin etik kullanımını teşvik ederken, kötüye kullanım durumlarında caydırıcı cezalar öngörmelidir.

Teknolojik Çözümler: Yapay zekanın suç amaçlı kullanımını tespit etmek ve önlemek için geliştirilen teknolojik çözümler önemlidir. Örneğin, YZ destekli güvenlik sistemleri, siber saldırıları tespit

etmek ve engellemek için kullanılabilir. Ayrıca, deepfake videolarının tespitine yönelik algoritmalar geliştirilerek bu tür sahte içeriklerin yayılması önlenabilir.

Bilinçlendirme Kampanyaları: Bireylerin ve kurumların YZ ile işlenen suçlara karşı bilinçlendirilmesi önemlidir. Bu tür kampanyalar, potansiyel tehditler hakkında bilgi verirken, güvenli internet kullanımı ve veri koruma konusunda da farkındalık yaratabilir.

Sonuç

Yapay zeka teknolojileri, suç dünyasında yeni ve karmaşık tehditler oluştururken, aynı zamanda bu tehditlerle başa çıkmak için yeni çözümler de sunmaktadır. YZ ile işlenen suçlarla etkili bir şekilde mücadele edebilmek için, yasal düzenlemeler, teknolojik yenilikler ve bilinçlendirme kampanyaları gibi çok yönlü yaklaşımlar gereklidir. Bu şekilde, YZ'nin potansiyelinden yararlanırken, kötüye kullanımı da engellenebilir.