

İSTANBUL GEDİK ÜNİVERSİTESİ
BİLİŞİM HUKUKU VE YAPAY ZEKÂ ATÖLYESİ
ÖĞRENCİ RAPORLARI
4 MAYIS 2026

1.Çalışma Grubu Raporu-

Prof. Dr. Kutluhan Bozkurt'un sorusu: “AB Düzenlemeleri kapsamında YZ bakımından Sorumluluk Sorunsalı”

Katılımcılar:

- 1. Esra İnce (Hukuk Fakültesi)**
- 2. Osman Ezgin (Bilgisayar Mühendisliği)**
- 3. Muhammed Aykan Pişkin (Hukuk Fakültesi)**
- 4. Ege Keser (Bilgisayar Mühendisliği)**
- 5. Melike Çomak (Bilgisayar Mühendisliği)**

Yapay zekâ, bilgisayarların ve makinelerin insan benzeri şekilde öğrenme, mantık yürütme, problem çözme, dili anlama ve karar verme yetenekleri kazanmasını amaçlayan bir teknolojidir. Bu süreçte özellikle Yapay Sinir Ağları, insan beynindeki nöronların çalışma prensibini taklit ederek verilerden öğrenmeyi sağlar. Yazılımlar ve makinelerin veriyi işleyerek düşünme benzeri davranışlar sergilemesini ve görevleri otonom biçimde yerine getirmesini mümkün kılan bu sistemler bütünü; sebep olduğu zararlar bakımından özel hukukun genel hükümlerine, bilhassa Borçlar Kanunu kapsamındaki haksız fiil başta olmak üzere genel hukuki sorumluluk hallerine tabidir ve bu rejim çerçevesinde incelenmelidir.

Bu teknolojik otonomi, beraberinde geleneksel hukuk kuramlarını sarsan yapısal bir dönüşümü getirmektedir. Zira yapay zekânın girdi ile çıktı arasındaki muhakeme sürecinin insan denetimi dışına çıkabilmesi, klasik araç-gereç statüsünü tartışmaya açmaktadır. Algoritmaların kendi kendine kararlar üretebildiği bu yeni ekosistemde, hukukun temelini oluşturan irade ve kusur kavramları dijital bir belirsizliğe evrilmektedir.

Hukuk sistemimiz tarihsel olarak kusur üzerine inşa edilmiştir; bir zarar varsa, bu zarara yol açan bir insan hatası aranır. Ancak yapay zekâ dünyasında, yapay zekanın neden o kararı verdiğini teknik olarak bilsek bile, bu kararın arkasında doğrudan kınanabilir bir insan iradesi bulmak her zaman mümkün olmaz. Yazılımın kendi kendine öğrenme süreci, eylem ile insan arasındaki bağı giderek zayıflatmaktadır.

Avrupa Birliği, bu karmaşayı aşmak için odağını kimin hatalı olduğunda değil, riskin nasıl yönetileceğine çeviriyor. Özellikle Avrupa Parlamentosu ve Konseyinin Yapay Zekâ Kurallarına İlişkin (AB) 2024/1689 Sayılı Tüzüğü (AI Act) çerçevesinde gördüğümüz bu perspektif, teknolojinin ne kadar akıllı olduğuna değil, toplum için ne kadar büyük bir tehlike teşkil ettiğine odaklanmaktadır¹. AI Act, tazminat hukuku anlamında

¹ European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L.

doğrudan bir sorumluluk ihdas etmese de idari yükümlülükler üzerinden sorumluluğun referans normlarını oluşturur.

Ancak AI Act'in getirdiği "yüksek riskli sistemlere" ilişkin şeffaflık, insan gözetimi ve veri kalitesi yükümlülükleri, olası bir uyuşmazlıkta ulusal mahkemelerin "kusur" veya "özen yükümlülüğünün ihlali" tespitini yapmasında temel bir referans standardı oluşturacaktır. Dolayısıyla Tüzük, sorumluluğu doğrudan dağıtmaya da sorumluluğun tespit edileceği hukuki zemini inşa etmektedir. Sorumluluk artık sadece bir ceza aracı değil, zararın adil bir şekilde paylaştırılması sorunudur.

Yapay zekânın kendi kendine karar verme yeteneği arttıkça, üretici ile ürün arasındaki bağ kaçınılmaz olarak incelmektedir. Geleneksel ürün sorumluluğunda üretici, ürünün fabrikadan çıktığı andaki kusurlarından sorumlu tutulurken; öğrenen bir algoritma, piyasaya çıktıktan aylar sonra tasarımcısının bile hayal edemeyeceği bir davranış sergileyebilir. Örneğin otonom bir aracın, eğitim verisindeki hatalı örüntüler nedeniyle yanlış karar vererek bir kazaya sebep olması durumunda, zararın kaynağını belirlemek ve bu zarar ile üretici arasında bir illiyet bağı kurmak son derece karmaşık hale gelmektedir.

Bu noktada öngörülebilirlik ilkesi büyük bir darbe almaktadır. Eğer bir sistemin vereceği zararın en yetkin uzmanlar bile önceden kestiremiyorsa, mağdurun bu zararın tazminini ispatlaması neredeyse imkânsız hale gelir. Avrupa Birliği (AB) tarafından hazırlanan Yapay Zekâ Sorumluluk Direktifi (Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence / AI Liability Directive – AILD)² bu eşitsizliği gidermek için karine ilkeleri ve ispat yükünün hafifletilmesi gibi mekanizmaları önererek bireyi algoritmaların karmaşıklığı karşısında yalnız bırakmamayı hedeflemektedir.

Ancak Avrupa Birliği'nin bu alandaki regülasyon mimarisi, tasarlanan ilk halinde kalmamış ve AILD sürecinin askıya alınması, hukuki manzarayı ciddi şekilde değiştirmiştir. AB'nin stratejisi başlangıçta birbirini tamamlayan iki temel sacayağı üzerine kuruluydu: Önleyici kurallar getiren Yapay Zekâ Yasası (AI Act) ve telafi edici mekanizmalar olan AILD ile revize edilmiş Ürün Sorumluluğu Direktifi. AILD'nin devreden çıkmasıyla birlikte, yapay zekânın neden olduğu zararlarda kusura dayalı sorumluluğun uyumlaştırılması hedefi büyük bir darbe almış; bu alandaki yük, ağırlıklı olarak revize edilmiş Ürün Sorumluluğu Direktifi'ne ve üye ülkelerin birbirinden farklı ulusal haksız fiil hukuklarına kalmıştır.

AILD tasarısının rafa kaldırılması, sorumluluk sorunsalının kalbinde yer alan kara kutu (black box) problemini yeniden alevlendirmiştir. Geleneksel haksız fiil hukukunda mağdurdan, yalnızca zararı değil, aynı zamanda zararı doğuran kusuru ve aradaki nedensellik bağına da kanıtlaması beklenir. AILD, bu kördüğümü spesifik bir illiyet bağı karinesi ile çözmeyi ve ispat yükünü teknoloji şirketlerinin omuzlarına yüklemeyi vadediyordu. Bu direktifin rafa kaldırılması, mağduru milyarlarca parametreyle çalışan bir algoritmanın iç işleyişindeki hatayı ispat etme külfetiyle, yani geleneksel hukukun yetersizlikleriyle büyük ölçüde yeniden baş başa bırakma riskini doğurmuştur.

Bu noktada Avrupa Birliği vatandaşları için geriye kalan en güçlü hukuki sığınak, güncellenen Revize Edilmiş Ürün Sorumluluğu Direktifi (PLD) olmuştur.³ PLD, meselenin ontolojik boyutunu çözerek yazılımları ve yapay zekâ sistemlerini net bir biçimde "ürün" olarak tanımlamıştır. Bu adım, kusursuz sorumluluk rejiminin dijital çağa uyarlanması anlamına gelir. PLD, karmaşık teknolojiler (yapay zekâ dahil) söz konusu olduğunda, mağdurun teknik

² European Commission. (2022). *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)*. COM(2022) 496 final.

³ European Commission. (2022). *Proposal for a Directive of the European Parliament and of the Council on liability for defective products*. COM(2022) 495 final.

zorluklar nedeniyle ispat yapamaması durumunda ürünün kusurlu olduğuna ve zarara bu kusurun yol açtığına dair bazı karineler sunarak AILD'nin bıraktığı boşluğun bir kısmını telafi etmeye çalışmaktadır. Artık bir algoritmanın kendi kendine öğrenme süreci sonucunda, piyasaya sürüldükten aylar sonra geçirdiği evrim nedeniyle ortaya çıkan zararlardan da üretici sorumlu tutulabilecektir.

Avrupa Birliği bahsedilen alanda hızla yol kat ederken; Türkiye, yapay zekanın hukuki statüsünü netleştirme konusundaki çalışmalarına yeni başlamıştır. Yakın zamanda gündeme gelen yasa tasarısı taslakları incelendiğinde AB Yapay Zekâ Yasası'nın (AI Act) temelini oluşturan risk kategorizasyonu ve sorumluluk rejimini esas almadığı; bunun yerine sadece temel bir kavramsal tanımlama düzeyinde kaldığı görülmektedir. Taslakların teknik açıdan yetersiz kalması, otonom sistemlerdeki “kara kutu problemi” ve buna bağlı gelişen “ispat yükü” gibi raporun temelini oluşturan kritik hukuki çıkmazlara çözüm üretilmesini imkânsız kılmaktadır. Yapay zekânın ulaştığı otonomi seviyesi, hukukun asırlardır dayandığı "insan iradesi" ve "kusur" paradigmalarını yetersiz bırakmaktadır. AI Act idari ve önleyici bir zemin sunarken, PLD mağdurları koruyan kusursuz bir güvenlik ağı örmektedir. Türkiye'nin de yapay zekâ mevzuatını şekillendirirken, salt tanımlayıcı metinler yerine; AB'nin dinamik birikiminden faydalanarak ispat kolaylıkları, karine mekanizmaları ve adil bir risk dağılımı öngören, mağdur haklarını önceleyen kapsamlı bir "Yapay Zekâ Sorumluluk Rejimi" inşa etmesi hukuki bir zorunluluktur. Aksi takdirde, gelişen teknoloji karşısında bireyler, ispatı imkânsız zararlarla tek başlarına mücadele etmek zorunda kalacaklardır.

2.Çalışma Grubu Raporu

Prof. Dr. Kutluhan Bozkurt'un sorusu: Mevcut Uluslararası Hukuk ve AB Hukuku Perspektiflerinde Yapay Zekanın Kişiliğini Tartışınız.

Katılımcılar:

1.Muhammet Emre Arıcı (Bilgisayar Mühendisliği)

2. Sude İrem Boylan (Bilgisayar Mühendisliği)

3. Doğuemre Timuçin (Bilgisayar Mühendisliği)

4. Aybüke Işıl Işkın (Hukuk)

5. Hazal Ağgez (Hukuk)

1.GİRİŞ

Yapay zekanın hukuki kişiliği, öncelikle bu sistemlerin nasıl çalıştığının teknik olarak anlaşılmasını gerektirir. Hukuki kavramların doğru konumlandırılabilmesi için mühendislik perspektifi bir ön koşuldur. Bu bölümde yapay zekanın temel prensipleri ele alınmakta; ardından bu teknik özelliklerin hukuki değerlendirmeleri nasıl etkilendiği tartışılmaktadır.

1.1 Yapay Zekanın Teknik Çalışma Prensipleri

Öncelikle yapay zekanın nasıl işlediğine ve elindeki kaynakları nasıl kullandığına dair bir çıkarımla işe başlamalıyız.

Yapay zekâ, verileri algoritmik yapılar aracılığıyla normal şartlarda insan bilişsel yeteneklerinin elverdiği analiz, sentez, karar verme süreçlerini taklit eden bir mühendislik disiplindir. Temel olarak, istatistiksel modelleme ve örüntü tanıma üzerine kuruludur.

Çalışma prensipleri şöyledir:

1.1.1-Veri Girişi ve Ön İzleme

Sistemin ilk aşaması ham verinin sisteme kabulüdür. Yani eldeki ses, metin, görüntü verilerini baz alarak bunları bilgisayar dilinin anlayabileceği vektöre çevirir.

1.1.2-Algoritmik Modelleme

Yapay zekanın karar mekanizması bir matematiksel model üzerinden işlenir ve buna yapay sinir ağları denir. Nöronlar - Katmanlar ve Özellik Çıkarımı prensiplerini kullanır.

1.1.3-Eğitim ve Optimizasyon

Yapay zekanın öğrenme ve yorumlama süreci aslında bir hata payı minimize etmesi şeklindedir. Aslında yapay zekanın sahip olduğu ilk veri büyük oranda hatalıdır ve yapay sinir ağları bu hatayı en aza indirmek için matematiksel ve istatistiksel hesapları kullanır. Aslında ortadaki temel işlem matematiksel prosedürdür.

1.1.4-Çıkarım

Eğitim süreci tamamlanmış ve hata payı kabul edilebilir seviyeye inmiş model, artık çıkarım yapmaya hazırdır. Bu aşamada sistem daha önce hiç karşılaşmadığı veri setiyle artık matematiksel olarak doğru bir veri çıkarımı yapabilir hale gelmiştir.

Özetle,

Yapay zekâ statik bir yazılımın aksine tecrübe ile performansını arttıran dinamik bir sistemdir. Teknik olarak yaptığı şey düşünmekten ziyade; olasılık hesapları, doğrusal cebir ve yüksek performanslı işlem gücünün birleşimiyle ortaya çıkan ileri düzey bir hesaplama metodolojisidir.

1.2 Halüsinasyon (Hallucination) Problemi ve Hukuki Öngörülmezlik

Büyük dil modellerinin en kritik teknik zafiyetlerinden biri halüsinasyon (hallucination) olarak adlandırılan olgudur: model, yüksek güven skoru ile yanlış bilgi üretebilmektedir. Bu durum rastgele değil, modelin istatistiksel örüntülere dayanarak "olası" gördüğü bir çıktıyı üretmesinden kaynaklanır.

Bununla bağlantılı olarak kalibrasyon (calibration) sorunu gündeme gelmektedir: Modelin bir çıktıdan ne ölçüde emin olduğu (confidence score) ile o çıktının gerçekte ne ölçüde doğru olduğu arasında sistematik bir uyumsuzluk mevcuttur. Bu özellikler, yapay zekanın davranışını deterministik değil stokastik kılmaktadır. Hukuki kişilik ise öngörülebilirliği, dolayısıyla yükümlülük doğurabilme kapasitesini gerektirir; mevcut sistemler bu standardı karşılayamamaktadır.

2. Açıklanabilir Yapay Zekâ (XAI) ve Hukuki Şeffaflık

Modern derin öğrenme modellerinin kararları neden açıklanamadığı sorusunun teknik yanıtı, hukuki şeffaflık talepleriyle doğrudan çatışır. Bu bölümde teknik “kara kutu” problemi ile AB hukukunun şeffaflık gereklilikleri arasındaki gerilim incelenmektedir.

2.1 Kara Kutu Problemi: Teknik Açıklama

Transformer tabanlı modellerde (GPT ve türevleri) kararların nasıl üretildiği birkaç teknik nedenden ötürü izlenemez:

Açıklanabilirlik Sorununun Teknik Kökleri

1. Boyutluluk Felaketi: GPT-4’te yaklaşık 1,76 trilyon parametre arasındaki etkileşimler, insan zihninin kavrayabileceği sınırlar ötesindedir. Tek bir çıktı, trilyonlarca parametrenin eş zamanlı etkileşiminin ürünüdür.
2. Doğrusal Olmayan Aktivasyonlar: Sinir ağlarındaki aktivasyon fonksiyonları (ReLU, GELU) doğrusal olmayan ilişkiler yaratır. Bu, basit ‘girdi → çıktı’ açıklamasını imkansız kılar.
3. Dikkat Kafaları (Attention Heads): Transformer modellerinde yüzlerce dikkat kafası birbirinden farklı özelliklere odaklanır. Hangi kafanın hangi kararı etkilediği belirsizdir.
4. Özellik Süperpozisyonu: Aynı nöronlar birden fazla kavramı temsil edebilir. ‘Bu nöron neyi öğrendi?’ sorusunun net yanıtı yoktur.

2.2. Post-Hoc Açıklama Araçları: LIME ve SHAP

XAI alanında geliştirilen post-hoc (sonradan uygulanan) açıklama yöntemleri, modelin gerçek iç mekanizmasını değil, davranışının yaklaşık yorumunu sunar:

Yöntem	Açıklama	Sınırlılık
--------	----------	------------

LIME (Local Interpretable Model-Agnostic Explanations)	Herhangi bir modelin lokal davranışını, o bölgede daha basit (doğrusal) bir yaklaşım modeli kurarak açıklar.	Lokal açıklama küresel davranışı temsil etmez; farklı çalıştırmalarda tutarsız sonuçlar üretebilir.
SHAP (SHapley Additive Explanations)	Oyun teorisinden türetilen Shapley değerleri aracılığıyla her özelliğin karar üzerindeki marjinal katkısını hesaplar.	Hesaplama maliyeti yüksektir; büyük modellerde yaklaşık değerlerle çalışmak zorunda kalınır.
Saliency Maps	Girdi piksellerinin/token'larının karar üzerindeki gradyan etkisini görselleştirir.	Görüntü sınıflandırma için geliştirilmiştir; dil modellerine doğrudan aktarımı sorunludur.

Bu araçların temel kısıtı şudur: Modelin kararını sonradan yorumlamak, o kararın nasıl üretildiğini açıklamakla eşdeğer değildir. Bu teknik sınırlılık, AB AI Act'in öngördüğü şeffaflık standardıyla doğrudan çelişir.

Yapay zekâ teknolojisinin hızlı gelişimi, geleneksel hukuki kategorilerin sınırlarını zorlamaktadır. Otonom kararlar alabilen, öğrenebilen ve karmaşık görevleri yerine getirebilen YZ sistemleri, hukuki sorumluluk, temsil ehliyeti ve haklar gibi temel hukuki kavramların yeniden değerlendirilmesini zorunlu kılmaktadır.

3. YAPAY ZEKÂ İLE AB İLİŞKİSİ

Bu bağlamda AI ACT'ten bahsetmek gerekir:

AB, AI ACT ile yapay zekaya bir kişilik vermekten ziyade onu bir ürün güvenliği ve risk yönetimi nesnesi olarak konumlandırmıştır. 2017'de Avrupa Parlamentosu, otonom robotlar için elektronik kişilik statüsünü önermesine rağmen sorumluluğun gerçek sorumlulardan kaçırılmasına neden olabileceği endişesi ile bu öneri AI ACT'te dahil edilmemiştir. AB yapay zekâ tüzüğü yapay zekaya bir kişilik atfetmekten ziyade risk temelli bir yaklaşım benimsemekte ve yapay zekâ sistemlerini kabul edilemez, yüksek, orta, düşük riskli olarak sınıflandırmaktadır.

Türkiye'de bu konuyla ilgili mevcut kanun tasarısı bulunan ve Avrupa Birliği'ne aday devlet statüsünde olan bir ülkedir. Bu nedenle bu gelişmeleri yakından takip ederek yapay zeka alanında yapacağı mevcut düzenlemeleri buna göre konumlandırmalıdır.

3.1 YAPAY ZEKÂ İLE ULUSLARARASI HUKUK İLİŞKİSİ VE CEZASIZLIK

Uluslararası hukukta ise yapay zekanın kişiliği konusunda henüz küresel bir bağlayıcı antlaşma bulunmamaktadır. Var olan tartışmalar daha çok devletlerin sorumluluğu ve temel insan hakları eksenindedir. Bu konudaki en büyük tartışma, yapay zekâ tamamen otonom bir karar verdiğinde ve bu verdiği karar doğrultusunda bir zarar meydana geldiğinde ortada kast sahibi ve cezalandırılabilir bir hukuk süjesi bulunmamasıdır. Yapay zekaya kişilik verilmemesi, bu boşluğun nasıl doldurulacağı sorusunu da açıkta bırakmaktadır. Bunun için kusursuz sorumluluk, üretici sorumluluğu ve kullanıcı sorumluluğuna gidilmesi konusunda farklı görüşler olmasına rağmen hiçbir kesin sonuç elde edilmemiştir. Bu duruma şu an verilebilecek en güncel ve net örnek, BM Güvenlik Konseyi'nin gündemine taşınan ve uluslararası hukuk çevrelerinde "hesap verebilirlik uçurumu" olarak nitelendirilen Ölümcül Otonom Silah Sistemleri (LAWS) meselesidir. Devletlerin geliştirdiği otonom insansız hava araçları gibi

sistemler, insan müdahalesi olmaksızın hedef tespit edip angaje olabilmektedir. Bu sistemlerin yanlış hedef tespiti nedeniyle sivillere zarar verdiği belgelenmiş vakalar mevcuttur; ne var ki söz konusu vakalarda ne sistemi geliştiren şirket ne onu konuşturduran komutan ne de yazılımın kendisi uluslararası insancıl hukuk kapsamında etkili biçimde yargılanabilmiştir. Bu durum, uluslararası hukuk doktrininde "sorumluluk boşluğu" (responsibility gap) kavramıyla kavramsallaştırılmakta; yapay zekâyâ hukuki kişilik tanınmamasının yarattığı bu boşluğun nasıl doldurulacağı sorusu ise yanıtsız kalmaya devam etmektedir. Eğer yapay zekâ bir kişilik olarak kabul edilip cezai sorumluluk yüklenirse, bu durum savaş suçlarının cezasız kalmasına neden olacak ve bu durum suça teşebbüs eden devletlere açık çek sunacaktır.

Aynı şekilde yapay zekanın yanılma payının olması, yapay zekanın şu anki hali ile bu akli ve hukuki olgunluğa sahip olmadığını göstermektedir. Bir varlığa kişilik tanımak için onun hukuki yükümlülüklerini yerine getirebiliyor olması gerekmektedir. Bu noktada bir çelişki mevcuttur.

Savaş suçları dışında yapay zekânın bireysel kullanımı da ceza hukukunda aykırılıklar teşkil edebilmektedir. Örneğin, yapay zekanın hakaret suçunu oluşturduğu noktada bunu üreticisine atfetmenin mümkün olup olmayacağı tartışılan bir konudur. Bu sorun, kast taksir tartışması yapılarak ilgili kişiler dikkat ve özen yükümlülüğüne uysaydı böyle bir netice öngörebilirler miydi sorusu ekseninde düşünülmelidir. Ancak hakaret suçu TCK'da taksir ile işlenebilecek şekilde düzenlenmediği için cezasızlık ortaya çıkmakta bu durum da bir hukuki boşluk yaratmaktadır. Buna öneri olarak bu suçların taksirli hallerinin ceza kanununda düzenlenerek veya ceza kanununa yeni suçlar eklenerek var olan cezasızlığın önüne geçilebilir.

4.SONUÇ VE DEĞERLENDİRME

Bu tartışma, yapay zekanın hukuki kişiliği meselesinin yalnızca teknik bir sorun değil; aksine, çok daha geniş kapsamlı bir **hukuki tasarım meselesi** olduğunu ortaya koymuştur.

Temel bulgularımız şöyle özetlenebilir:

- **Mühendislik perspektifinden:** Mevcut derin öğrenme modelleri stokastik, açıklanamaz ve öngörülemezdir. Halüsinasyon problemi ve kalibrasyon eksikliği, hukuki sorumluluğun temel koşullarıyla bağdaşmamaktadır. XAI araçları (LIME, SHAP) gerçek şeffaflık sağlamamakta; post-hoc yorumlar nedensellik kurmamaktadır.
- **AB hukuku perspektifinden:** AI Act, yapay zekâyı bir kişilik olarak değil risk nesnesi olarak konumlandırarak pratik bir çözüm sunmaktadır. Ancak yüksek riskli kategorilerde şeffaflık zorunluluğu ile teknik gerçeklik arasındaki gerilim çözüme kavuşturulamamıştır.
- **Uluslararası hukuk perspektifinden:** Bağlayıcı küresel bir çerçeve bulunmamakta; LAWS vakası sorumluluk boşluğunu somut biçimde göstermektedir. Otonom silahlardaki adversarial attack senaryoları gibi teknik zafiyetler hesap verebilirliği imkânsız kılabilmektedir.

Özetle mühendislik perspektifi, kişilik tartışmalarının çoğunlukla hatalı teknik öncüllere dayandığını gösterirken; hukuk perspektifi, mevcut çerçevelerin yeni nesil sorumluluk boşluklarını kapatmakta yetersiz kaldığını vurgulamaktadır.

Bu noktada, YZ sistemlerine hukuki bir kişilik atfedilip atfedilmemesinden bağımsız olarak, özellikle yüksek riskli sistemler için **teknik açıklanabilirlik standartlarının** geliştirilmesi bir zorunluluktur. Tarihsel süreç, teknolojinin her zaman düzenlemenin önünde ilerlediğini göstermiştir. 1990'larda internetin öngörülemez yükselişi karşısında hukuk sistemlerinin geç kalması, günümüz için önemli bir derstir. Yapay zekâ alanında benzer bir gecikmenin yaşanmaması adına aşağıdaki adımlar büyük öneme sahiptir:

1. **Teknik açıklanabilirlik standartları:** Özellikle yüksek riskli sistemler için XAI gerekliliklerinin teknik gerçeklikle uyumlu biçimde tanımlanması.

2. **Sektörel sorumluluk rejimleri:** Üretici, işletici ve kullanıcı sorumluluğunun açık biçimde ayrıştırıldığı katmanlı sorumluluk çerçeveleri.
 3. **LAWS için bağlayıcı uluslararası araçlar:** BM düzeyinde otonom silah sistemlerini düzenleyen bağlayıcı antlaşmalar öncelikli diplomatik gündem maddesi olmalıdır.
 4. **Türkiye'nin proaktif konumlanması:** AB aday ülkesi sıfatıyla AI Act standartlarının erken benimsenmesi, iç hukuktaki boşlukların taksirli eylemler dahil kapatılması.
- Yapay zekanın hukuki kişilik edinmesi, teknolojik gelişimin belirli bir eşiği aşmasına bağlıdır. Bu eşik mevcut paradigmada henüz aşılmamıştır. Asıl ve acil mesele kişilik değil; sorumluluk boşluklarının kapatılmasıdır. Elinizdeki bu rapor, söz konusu eksiklere dikkat çekmeyi ve bunların kapatılmasına ön ayak olmayı hedeflemektedir.

3.Çalışma Grubu Raporu-

Dr. Öğr. Üyesi Aytaç Uğur Yerden’in sorusu:

“Yapay zekâ sistemlerinde enerji verimliliğini sağlamak amacıyla modelin küçültülmesi veya budanması, algoritmanın doğruluk oranında bir miktar düşüşe yol açabilir. Sürdürülebilirlik hedefleri doğrultusunda optimize edilmiş ve daha az enerji harcayan bir modelin (örneğin otonom bir sistem veya siber güvenlik aracının) kritik bir hata yapması durumunda hukuki sorumluluk kime ait olmalıdır?”

Katılımcılar:

1. Gamze Meryem Vural (Hukuk)
2. Arda Ali Sona (Bilgisayar Mühendislik)
3. Fatih Emre Yüce (Bilgisayar Mühendislik)
4. Ramazan Türkyılmaz (Bilgisayar Mühendislik)

1. Giriş: Yapay Zekâ Nedir?

Doktrinde tek ve kesin bir tanımı üzerinde henüz tam bir uzlaşa sağlanamamış olsa da genel hatlarıyla yapay zekâ; insan zekasını devasa veri setleri ve karmaşık matematiksel algoritmalar aracılığıyla istatistiksel olarak taklit eden sofistike bir bilgisayar bilimi dalıdır. Doğası gereği salt istatistiksel temellere dayandığı için bu sistemlerin bilinci, duygusal kapasitesi veya gerçek bir öznenin sahip olduğu kişiliği bulunmamaktadır.

2. Yapay Zekanın İşleyişi ve Temel Özellikleri

Yapay zekâ sistemleri, temel olarak kendisine sunulan verileri en kısa sürede işleyip analiz ederek ve veriler arasındaki örüntüleri tanıyarak kullanıcıya en doğru çıktıyı sunmayı hedefler. Bu işleyiş, yüksek hesaplama gücü ve devasa yapay sinir ağları gerektirir. Ancak modeller büyüdükçe artan donanım maliyetleri ve gecikme süreleri, sistemlerin optimize edilmesini zorunlu kılmıştır.

2.1. Model Optimizasyonu (Model Compression)

Model optimizasyonu (Model Compression), yapay zekâ modellerinin doğruluk oranını mümkün olduğunca koruyarak hesaplama maliyetini, bellek kullanımını ve enerji tüketimini azaltmayı amaçlayan yöntemlerin genel adıdır. Bu kapsamda budama (Pruning) ve kuantizasyon (Quantization) en yaygın kullanılan tekniklerdir.

Budama: Yapay sinir ağındaki matematiksel ağırlıklardan, sonuca etkisi en az olan veya gereksiz görülen bağlantıların tespit edilip sıfırlanarak devreden çıkarılması işlemidir. Bu yöntemle model sadeleşir ve işlem yükü ciddi oranda düşer.

Kuantizasyon: Verinin ve model içi parametrelerin sahip olduğu yüksek hassasiyetli matematiksel değerlerin (örneğin 32-bit sayılar), daha düşük ve hesaplaması kolay makul değerlere (örneğin 8-bit sayılar) dönüştürülerek düşürülmesidir. Bu sayede modelin hafızada kapladığı alan ve enerji tüketimi azaltılır.

3. Yapay Zekanın Sürdürülebilirlik ve Yönetişim İlkeleri

Yapay zekâ ekosisteminin sağlıklı işleyişi için kabul görmüş temel ilkeler aşağıda detaylandırılmıştır:

Eşitlik ve Adalet: Algoritmik süreçlerin herhangi bir grup veya birey aleyhine önyargı içermemesi, fırsat eşitliğini gözetmesi esastır.

Hukukun Üstünlüğü: Tüm yapay zeka faaliyetlerinin ulusal ve uluslararası hukuk normlarına, insan haklarına ve kişisel verilerin korunması kanunlarına tam uyumlu olması zorunludur.

Regülasyon ve Denetim: Yapay zekanın kontrolsüz gelişimini engellemek adına yasal çerçevelerin oluşturulması ve bu sistemlerin bağımsız mekanizmalarca düzenli olarak denetlenmesi gerekir.

Şeffaflık: Sistemlerin hangi verilerle eğitildiği ve hangi süreçlerden geçerek çıktı ürettiği konusunda paydaşlara açık bilgi sağlanmalıdır.

Açıklanabilirlik ve Yorumlanabilirlik: Yapay zekanın verdiği kararların "kara kutu" olmaktan çıkarılıp, teknik olmayan kişilerce de açıklanabilirlik, mantıksal olarak takip edilebilir ve yorumlanabilirlik olması kritik önem taşır.

Kırmızı Yapay Zekâ (Red AI): Günümüzde yapay zekâ yarışını domine eden temel yaklaşımdır. Firmalar, modellerin doğruluk payını sadece birkaç puan artırabilmek için hesaplama gücünü ve parametre sayısını katlanarak artırmaktadır. Bu durum, eğitim aşamasında devasa elektrik tüketimine ve uçak yolculuklarıyla yarışacak seviyede karbon emisyonuna yol açar. Kırmızı yapay zekâ, çevresel olarak sürdürülemez olmasının yanı sıra, teknolojik gelişimi sadece yüksek sermayeli şirketlerin tekeline bırakarak "Yönetişimde Eşitlik" ilkesini de zedeler.

Yeşil Yapay Zekâ (Green AI): Kırmızı yapay zekanın yarattığı tahribata bir tepki ve çözüm olarak doğmuştur. Temel felsefesi, yapay zekâ sistemlerini sadece "ne kadar zeki" olduklarına göre değil, "ne kadar verimli" olduklarına göre değerlendirmektir. Daha az veri ile daha hızlı öğrenebilen, kod tekrarını azaltan, model mimarisini optimize eden ve bulut bilişimde yenilenebilir enerji kullanan sistemleri ifade eder.

Karşılaştırma Kriteri	● Kırmızı Yapay Zeka	● Yeşil Yapay Zeka
Temel Hedef	Maliyetten bağımsız maksimum doğruluk ve en yüksek performans	Enerji verimliliği, düşük karbon salınımı ve çevre dostu sonuçlar
Enerji Tüketimi	Çok yüksek — devasa veri merkezleri ve yoğun GPU/TPU gücü gerektirir	Optimize edilmiş ve düşük — gereken minimum işlem gücünü hedefler
Karbon Ayak İzi	Yüksek ve üstel olarak artan çevresel tahribat	Minimum düzey; yenilenebilir enerji kaynaklarıyla desteklenmesi teşvik edilir
Model Yaklaşımı	Daha fazla veri ve parametre — "daha büyük, daha iyidir" mantığı	Akıllı algoritmalar, veri kalitesi ve model sıkıştırma teknikleri
Geliştirme Maliyeti	Çok yüksek donanım ve elektrik maliyetleri	Ekonomik olarak daha sürdürülebilir ve bütçe dostu
Erişilebilirlik	Yalnızca dev teknoloji şirketleri için erişilebilir; tekelleşmeye yol açar	KOBİ'ler, akademisyenler ve bağımsız araştırmacılar için de erişilebilir

Tablo 1

4. Yapay Zekanın Hukuki Sorumluluğu

4.1. Enerji Verimliliği ve Hukuki Sorumluluk Rejimi Arasındaki Denge

Güncel hukuk düzeninde yapay zekâ sistemleri bağımsız bir hukuki kişiliğe sahip olmadıklarından, doğrudan sorumlu tutulmaları mümkün değildir. Bu nedenle, sistemin ürettiği klasik hataların kime atfedileceğinden ziyade, "tasarım tercihlerinin bilinçli olarak risk üretmesi" halindeki sorumluluğun kime atfedileceği temel hukuki tartışmadır. Burada kritik soru; ihlalin veya zararın "kimin kontrolü ve bilgisi dâhilinde gerçekleştiği" hususudur.

4.1.1. Bilinçli Tasarım Tercihi Olarak Sorumluluğun Ağırlaşması

Yapay zekâ modellerinde uygulanan budama (pruning) veya küçültme işlemleri; sistemin kritik uygulama alanı bilindiği halde, öngörülebilir riskler yeterince test edilmeden salt enerji tasarrufu gerekçesiyle tercih edilmişse hukuki sorumluluk doğar. Bu senaryoda:

Türk Borçlar Kanunu (TBK) m. 49 kapsamında kusura dayalı sorumluluktan (hukuka aykırı fiil, kusur, zarar ve nedensellik bağı) veya

Ürün güvenliği bağlamında ayıplı ürün sorumluluğundan söz edilebilir.

Buradaki kilit nokta; enerji verimliliği gibi bir tasarım gerekçesinin hukuken otomatik bir mazeret sayılmamasıdır. Aksine, güvenlik yerine verimliliğin seçilmesi bilinçli bir tasarım tercihi olduğu için, doğacak zararlarda sorumluluğu ağırlaştıran bir unsur olarak değerlendirilebilir.

4.1.2. Aktörlere Göre Paylaştırılmış Sorumluluk Yaklaşımı

Karmaşık yapay zekâ ekosisteminde en makul ve adil hukuki yaklaşım "paylaştırılmış sorumluluk" modelidir. Bu bağlamda sorumluluklar aktörlere göre şu şekilde şekillenir:

Üretici ve Piyasaya Sürenin Sorumluluğu: Özellikle AB Yapay Zekâ Tüzüğü (ABYZT) ve ürün sorumluluğu direktifleri bağlamında; bir sistem "yeşil" veya "sürdürülebilir" iddiasıyla piyasaya sürülüyor ancak barındırdığı kritik hata potansiyeli kullanıcıya açıkça bildirilmiyorsa, bu durum objektif kusursuz sorumluluk kapsamına girebilir. Hata kaçınılmaz olsa dahi, zarar görenin kusur ispatına gerek kalmaksızın üretici sorumlu tutulabilir.

İşleten ve Kullanıcının Sorumluluğu: Daha düşük doğruluk oranına sahip olduğu bilinen "küçültülmüş" bir sistem, insan denetimi olmaksızın yüksek riskli uygulamalarda kullanılmışsa, işletici açısından açık bir özen yükümlülüğüne aykırılık mevcuttur. Bu ihlal, işletici hakkında idari ve somut olayın niteliğine göre cezai yaptırımların uygulanmasına yol açabilir.

4.1.3. Sürdürülebilirlik İddiasının Normatif Sınırları ve ABYZT Kapsamı

Sürdürülebilirlik, hukuken meşru bir kamu yararı olmakla birlikte bir "üst değer" (mutlak hak) değildir. Hukuki hiyerarşide enerji verimliliği; insan güvenliğinin, yaşam hakkının ve temel hakların önüne geçemez. Sürdürülebilirlik hedefleri, hukuki sorumluluğun niteliğini ve özen yükümlülüğünü hafifletmez.

Bu durum, doğrudan bağlayıcı bir regülasyon olan Avrupa Birliği Yapay Zekâ Tüzüğü (ABYZT) ile de güvence altına alınmıştır. ABYZT uyarınca; yüksek riskli sistemlerde doğruluk, güvenilirlik ve insan denetimi unsurları hiçbir koşulda enerji tasarrufu gerekçesiyle ihlal edilemez. Tüzüğün risk yönetimi (m.9), veri yönetimi (m.10), teknik dokümantasyon (m.11), şeffaflık (m.13), insan gözetimi (m.14) ve doğruluk/siber güvenlik (m.15) maddeleri bu dengeyi katı kurallara bağlamış ve yaptırımlarla (m.83 ve devamı) desteklemiştir. Bu regülasyon, AB içinde faaliyet gösteren veya bu pazara ürün sunan tüm küresel aktörler için doğrudan bağlayıcıdır.

5. Sonuç

Yapay zekâ teknolojilerinin hızlı evrimi, beraberinde getirdiği devasa veri işleme ihtiyacı ve artan enerji tüketimi sebebiyle çevresel sürdürülebilirliği merkeze alan "Yeşil Yapay Zeka" yaklaşımlarını zorunlu kılmıştır. Budama ve kuantizasyon gibi model optimizasyonu teknikleri, enerji verimliliğini artırmak ve teknolojiyi tekelden çıkarıp daha erişilebilir kılmak adına kritik mühendislik adımlarıdır. Ancak bu optimizasyon süreçlerinde doğruluktan ve performanstan verilen tavizler, beraberinde derin hukuki ve etik sorunlar getirmektedir.

Hukuki düzlemde en net gerçek şudur ki; sürdürülebilirlik ve enerji verimliliği meşru bir kamu yararı olsa da, insan güvenliğinin, yaşam hakkının ve temel hakların önüne geçebilecek mutlak bir "üst değer" değildir. Özellikle Avrupa Birliği Yapay Zekâ Tüzüğü (ABYZT) ve mevcut ulusal normlar (TBK ve Ürün Sorumluluğu Direktifleri), enerji tasarrufu sağlamanın yüksek riskli sistemlerde doğabilecek hatalar için geçerli bir hukuki mazeret olamayacağını kesin bir dille ortaya koymaktadır.

Yapay zekâ sistemlerinin bağımsız bir hukuki kişiliği bulunmadığından, ortaya çıkan zararlarda kusur veya ürün sorumluluğu doğrudan sürece dâhil olan insan veya kurumlara aittir. Enerji verimliliği adına güvenlik risklerinin göz ardı edilmesi, hukuken "bilinçli bir tasarım tercihi" olarak kabul edilip sorumluluğu ağırlaştıran bir unsur niteliği taşır. Bu bağlamda, sistemi optimize eden geliştirici, piyasaya süren üretici ve yüksek riskli alanda insan denetimi olmaksızın kullanan işletici arasında "paylaştırılmış sorumluluk" ilkesinin uygulanması en adil ve rasyonel yaklaşımdır.

Ezcümle, güvenli, adil ve sürdürülebilir bir yapay zekâ ekosistemi, ancak teknolojik inovasyonun ve çevre dostu hedeflerin, tavizsiz bir hukuki sorumluluk ve etik yönetim çerçevesiyle dengelenmesiyle inşa edilebilir. Kritik durumlarda hukuki sorumluluk cansız algoritmaların değil; riski öngören, yöneten ve verimlilik ile güvenlik arasında karar verme yetkisine sahip olan gerçek ve tüzel kişilerin omuzlarındadır.

4. Çalışma Grubu Raporu-

Dr. Öğr. Üyesi Aytaç Uğur Yerden’in sorusu: Algoritmaların karbon ayak izi yasal olarak nasıl denetlenmelidir? Sadece şeffaf raporlama yeterli midir, yoksa yüksek enerji tüketen modellere yasal kısıtlamalar veya ekstra vergilendirmeler getirilmeli midir?

Katılımcılar:

1. Ali Alper Ünsal (Bilgisayar Mühendisliği)
2. Yusuf İhsan Gül (Bilgisayar Mühendisliği)
3. Ayça Engindeniz (Bilgisayar Mühendisliği)
4. Ayça Rüyam Çalışkan (Hukuk)

Sorunun tespiti:

Tablo1’de görülebileceği üzere, yapay zekanın toplam karbon ayak izi içerisindeki oranının %0,5 - %1,5 arasında olmasına rağmen 2026 yılı itibarıyla yapay zekâ, emisyon artış hızı bakımından en dikkat çeken sektör konumundadır.

Tablo 1. Sektörlerin Küresel CO2 emisyon payı (Kaynak: IPCC (AR6) / EDGAR (2025) / Climate Watch)

Sektör	Küresel CO2 Emisyon Payı (%)	Durum Özeti
Enerji ve Isınma	~%26 - %30	En büyük kirletici; fosil yakıt bağımlılığı devam ediyor.
Sanayi ve İmalat	~%21	Çimento ve çelik üretimi gibi karbon yoğun süreçler.
Ulaşım (Kara/Hava/Deniz)	~%16	Havacılık tek başına toplam emisyonun yaklaşık %2'sini oluşturur.
Tarım ve Hayvancılık	~%14	Metan gazı ve arazi kullanımı kaynaklı yüksek etki.
Yapay Zeka & Veri Merkezleri	~%0,5 - %1,5	Payı düşük görünse de, 2030'a kadar %3-4 bandına çıkması bekleniyor.

Algoritmaların karbon ayak izi yasal olarak nasıl denetlenmelidir?

Öncelikle devletlerin algoritmaları için çevresel etki değerlendirmesi sistemi kurması gerekir. Büyük ölçekli yapay zekâ modelleri geliştirilmeden önce, tıpkı çevre hukukundaki ÇED raporları gibi, “dijital çevresel etki raporu” hazırlanmalıdır. Bu raporda modelin eğitim sürecinde ne kadar enerji tüketileceği, hangi enerji kaynaklarının kullanılacağı, veri merkezlerinin su tüketimi ve ortaya çıkacak karbon emisyonu açıkça belirtilmelidir. Böylece kamu otoriteleri ve toplum, teknolojik gelişmenin çevresel maliyetini önceden görebilir.

Yapay zeka şirketi faaliyete geçtikten sonra, bu şirketlere ISO/IEC 21031 gibi standartlar çerçevesinde ne kadar karbon ayak izi ürettiklerine dair şeffaf raporlama yapma zorunluluğu getirilmelidir. Böylelikle şirket içerisinde ve şirketin paydaşları arasında bu konu üzerinde farkındalık yaratıldığı gibi bu raporları yasal beyanları olarak kabul edilmiş olacaktır.

Algoritmaların koşturulduğu sunucuların ve veri merkezlerinin PUE (Enerji Kullanım Etkinliği) değerleri, bağlı bulunulan devlet kurumları tarafından IoT (Nesnelerin İnterneti) tabanlı akıllı sayaçlarla anlık izlenmelidir. Şirketlerin tükettiği enerji miktarını "gizli ticari bilgi" statüsünün arkasına saklaması engellenmelidir. Bu şekilde yapılacak şeffaf raporlamanın doğruluğu kontrol edilebilecektir.

Avrupa Birliği'ndeki mevcut mevzuat incelendiğinde; AB Yapay Zeka Yasası (EU AI Act) çevresel etkisini doğrudan bir belgeleme ve şeffaflık zorunluluğu haline getirmiştir. Annex XI kapsamında, büyük dil modelleri (LLM) gibi sistemlerin sağlayıcıları, modellerinin enerji tüketimini teknik dokümantasyonun bir parçası olarak raporlamak zorundadır. Son olarak kritik altyapılarda kullanılan yapay zeka sistemleri, tüm yaşam döngüleri boyunca çevresel etkilerini takip etmek ve raporlamakla yükümlüdür.

Yüksek enerji tüketen modellere yasal kısıtlamalar getirilmeli midir?

Belirli bir doğruluk payına ulaşmak için aşırı enerji tüketen modellerin ticari kullanımına sınırlama getirilebilir. Kısacası modellerin verimliliği ölçülüp verimliliği düşük modellere yasal kısıtlamalar uygulanabilir. Şebekede elektrik tüketiminin en yoğun olduğu saatlerde, hukuki olarak bir önceliklendirme yapılabilir. Tıbbi teşhis veya bilimsel araştırma yapan hayati modellerin tam kapasite çalışmasına izin verilirken; sadece eğlence, oyun veya görsel filtreleme amaçlı çalışan yüksek enerjili algoritmaların işlem kapasitesi, elektrik şebekesini rahatlatmak adına örneğin bant genişliği daraltılarak yasal olarak sınırlandırılabilir.

Verimliliğin yanı sıra yapay zeka şirketlerinin kullandığı donanımlar da denetlenmelidir. Veri merkezlerinin belirli bir yüzdede yenilenebilir enerji kullanma zorunluluğu getirilebilir.

Avrupa Birliği (AB) mevzuatında, yüksek enerji tüketen yapay zeka modellerini doğrudan yasaklayan, çalışmalarını durduran veya onlara kesin bir enerji kotası koyan doğrudan bir yasal kısıtlama şu an için bulunmamaktadır.

Ekstra vergilendirmeler getirilmeli midir?

Ekstra vergilendirmeler şirketleri daha verimli algoritmalar geliştirmeye teşvik etmek için etkili yol olabilir. Örneğin, yapay zeka şirketleri büyük dil modelleri geliştirmek yerine belirli konularda uzmanlaşmış daha verimli çalışan "Small Language Models" – SLM tipinde modeller geliştirmeye teşvik edilebilir.

Vergilendirme süreci modelin eğitim süreci ve kullanım süreci için ayrı ayrı uygulanabilir. Eğitim süreci için gereken işlemci gücü üzerinden bir "karbon vergisi" alınması, geliştiricileri modeli optimize etmeye zorlar. Kullanım sürecinde ise yüksek enerji tüketen modeller geliştiren firmaların, bu zararı telafi etmek için karbon dengeleme projelerine yatırım yapması yasal bir zorunluluk haline getirilebilir. Toplanan bu vergilerin mutlaka yeşil teknoloji fonuna aktarılarak sürdürülebilir enerji yatırımlarına yönlendirilmesi sağlanmalıdır. Böylece sistem sadece cezalandırmak yerine sürdürülebilirliğe katkı sağlayacaktır.

Avrupa Birliği (AB) mevzuatında, şu an için (Mayıs 2026 itibarıyla) sadece yüksek enerji tüketen yapay zeka modellerine yönelik özel bir "Yapay Zeka Karbon Vergisi" veya doğrudan bir "Ekstra Vergi" bulunmamaktadır.

5. Çalışma Grubu Raporu-

Dr. Öğr. Üyesi Gürkan Özocak'ın sorusu:

Soruları: Teknolojik gelişmeler ışığında Türk ceza ve ceza muhakemesi hukuku mevzuatında düzenlenen bilişim suçları ve suçluların tespitine yönelik hükümler ihtiyacı karşılama bakımından yeterli midir? Değilse, nasıl düzenlemeler yapılmalıdır?

Katılımcılar:

1. **Ecegüneş Dağ (Bilgisayar Mühendisliği)**
2. **Gülcan Akşit (Hukuk)**
3. **Kaan Sarı (Bilgisayar Mühendisliği)**
4. **Mohamed Nabih Alluş (Bilgisayar Mühendisliği)**

Teknolojik Gelişmeler Işığında Türk Ceza ve Ceza Muhakemesi Hukukunun Bilişim Suçları Bakımından Yeterliliği

Teknolojik gelişmeler ışığında Türk ceza ve ceza muhakemesi hukuku mevzuatının bilişim suçları ve suçluların tespiti bakımından yeterliliği; mevcut bir temel yapının varlığına rağmen, günümüz ihtiyaçları karşısında yetersiz kalmaktadır.

Mevcut ceza hukukunun temelini oluşturan kusur ilkesi, failin irade ve bilinç sahibi olmasını zorunlu kılar. Bu nedenle yapay zekânın (AI) hukuki anlamda bir "fail" olarak cezalandırılması, mevcut sistem içinde mümkün değildir. Zira yapay zekâ, hukuki kişilikten yoksun; yalnızca algoritmik süreçler üzerinden çıktı üreten bir yazılım sistemidir. Bir yazılım mühendisi açısından yapay zekâ, irade sahibi bir özne değil; kodlama, veri işleme ve olasılıksal modelleme süreçlerinin birleşiminden oluşan teknik bir araçtır. Bu nedenle klasik anlamda "cezalandırma"nın —örneğin hapis cezasının— yapay zekâyı uygulanması, hukuken ve teknik olarak anlamını yitirmektedir.

Bununla birlikte öğretilerde, yapay zekâyı sınırlı da olsa "elektronik kişilik" tanınması yönünde tartışmalar mevcuttur. Bu yaklaşımın kabul edilmesi hâlinde yaptırımların niteliği de değişecektir. Örneğin; yapay zekâ sistemlerinin faaliyetlerinin kısıtlanması, veri setlerinin silinmesi, modelin devre dışı bırakılması veya elde ettiği ekonomik değere el konulması gibi "cezai güvenlik tedbirleri" benzeri mekanizmalar gündeme gelebilir. Böylece klasik ceza hukuku yaptırımlarından ziyade, dijital sistemlere özgü koruyucu ve önleyici yaptırımların uygulanması mümkün hâle gelecektir.

Sorumluluk açısından ise "açıklanabilir yapay zekâ" (explainable AI) ilkesi önem kazanmaktadır. Eğer suç; yazılım içerisinde bilinçli şekilde bırakılmış bir güvenlik açığından (backdoor), hatalı veri setinden veya kasıtlı yönlendirmeden kaynaklanıyorsa sorumluluk yazılımcıya ait olacaktır. Buna karşılık, kullanıcı tarafından gerçekleştirilen "prompt injection" [1] gibi manipülasyonlar sonucunda hukuka aykırı içerik üretilmişse sorumluluğun kullanıcıya yüklenmesi gündeme gelecektir. Bu bağlamda sorumluluğun belirlenmesi, teknik nedensellik zincirinin doğru biçimde analiz edilmesine bağlıdır.

Yapay Zekâ ve Kaynak Tüketimi: Enerji ve Su Kullanımı

Yapay zekâ modellerinin eğitimi ve işletilmesi, yüksek düzeyde enerji tüketimi ve soğutma ihtiyacı doğurarak önemli çevresel etkiler yaratmaktadır. Bu durum doğrudan klasik anlamda bir "suç" teşkil etmese de, çevresel hukuk ve idare hukuku bakımından önemli bir düzenleme alanı oluşturmaktadır.

Yazılım perspektifinden bakıldığında "verimsiz kodlama" doğrudan cezai sorumluluk doğurmazken; hukuki perspektifte, özellikle büyük ölçekli şirketlerin çevresel regülasyonlara —ESG kriterleri [2]

gibi— uymaması idari yaptırımlara konu olabilmektedir. Bu çerçevede, çevresel etkilerin bilinçli şekilde göz ardı edilmesi durumunda şirket yönetiminin sorumluluğu gündeme gelir.

Nitekim Türk Ceza Kanunu'nun 181. maddesinde düzenlenen çevrenin kasten kirletilmesi suçu, gelecekte dijital altyapıların neden olduğu kaynak tüketimi ve karbon ayak izi gibi unsurlar bakımından geniş yorumlanabilir. Bu kapsamda, yüksek enerji tüketen veri merkezleri veya verimsiz yapay zekâ sistemleri işleten şirketler bakımından ağır idari para cezaları, faaliyet durdurma ya da lisans iptali gibi yaptırımlar gündeme gelebilecektir.

Algoritmik Etik ve Davranış Bozuklukları

Farklı yapay zekâ sistemlerinin —örneğin farklı modellerin farklı üslup ve içerik üretmesi— değişken davranışlar sergilemesi, "algoritmik şeffaflık" ve "etik kontrol" sorununu gündeme getirmektedir. Bir yapay zekânın küfür, nefret söylemi veya hukuka aykırı içerik üretmesi durumunda, doğrudan fail olarak yapay zekâ değil; hizmet sağlayıcı şirket sorumlu tutulmaktadır.

Bu kapsamda, kullanıcıların kişilik haklarının ihlali söz konusu olduğunda tazminat sorumluluğu doğabilmektedir. Teknik açıdan ise bu durum, modelin güvenlik bariyerlerinin (safety guardrails) yetersiz olduğunu göstermektedir. Avrupa Birliği Yapay Zekâ Tüzüğü (AI Act) çerçevesinde bu tür sistemler "yüksek riskli sistem" kategorisine alınarak daha sıkı denetime tabi tutulmakta; gerektiğinde piyasadan çekilmeleri dahi mümkün olmaktadır.

Dijital Ödeme Sistemleri ve Veri Sızıntıları

Masterpass gibi dijital ödeme sistemleri, kart bilgilerinin doğrudan saklanması yerine tokenize etme (jetonlaştırma) [3] yöntemini kullanarak güvenlik sağlamaktadır. Buna rağmen veri ihlallerinin tamamen önlenememesi, siber güvenlik risklerinin varlığını sürdürdüğünü ortaya koymaktadır.

Hukuki açıdan; veri tabanına yetkisiz erişim sağlayan kişiler, Türk Ceza Kanunu'nun 243. maddesi (bilgi sistemine girme) ve 245. maddesi (banka veya kredi kartlarının kötüye kullanılması) kapsamında cezalandırılmaktadır. Kurumlar bakımından ise Kişisel Verilerin Korunması Kanunu (KVKK) uyarınca yeterli teknik ve idari tedbirlerin alınmaması, idari para cezasına yol açmaktadır.

Teknik açıdan, bir veri sızıntısının kaynağının "zero-day" (sıfırıncı gün) [4] açığı mı yoksa ihmal sonucu yamalanmamış bir güvenlik zafiyeti mi olduğunun tespiti büyük önem taşımaktadır. İhmalin tespiti hâlinde kurumun kusurlu sorumluluğu gündeme gelmekte ve tazminat yükümlülüğü artmaktadır.

Mevcut TCK Düzenlemelerinin (Md. 243-246) Teknolojik Gelişmeler Karşısındaki Yeterliliği

Yapay zekanın ötesinde, Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" başlıklı bölümünde yer alan 243-246. maddeleri, yazıldığı dönemin "statik internet" mantığına göre tasarlanmış olup, günümüzün dinamik dijital dünyasında ciddi boşluklar barındırmaktadır:

- **TCK md. 243 (Bilişim Sistemine Girme):** Maddede suçun oluşması için sisteme girilmesi veya orada kalınmaya devam edilmesi aranmaktadır. Ancak günümüzde nesnelerin interneti (IoT), giyilebilir teknolojiler ve bulut bilişim (cloud) sistemleri mevcuttur. Verinin sisteme girilmeksizin, havada siber ağlar üzerinden akarken (man-in-the-middle saldırıları [5] ile) ele geçirilmesi durumunda maddenin lafzi sınırı zorlanmaktadır. Ayrıca yapay zekâ

ajanlarının otonom olarak gerçekleştirdiği yetkisiz erişimlerde "hukuka aykırılık bilincinin" kime yükleneceği belirsizdir.

- **TCK md. 244 (Sistemi Engelleme, Bozma, Verileri Yok Etme):** DDOS saldırıları gibi sistemleri kilitleyen modern yöntemler maddede dolaylı karşılık bulsa da, fidye yazılımları (ransomware) yoluyla verilerin silinmeyip sadece güçlü algoritmalarla şifrelenerek erişilmez kılınması eylemi maddede açıkça tanımlanmamıştır. Veri şifreleme, verinin fiziken yok edilmesi veya bozulması olmadığından, suçta ve cezada kanunilik ilkesi gereği madde metninin revize edilerek "verileri erişilmez kılma" ibaresinin eklenmesi bir zorunluluktur.

- **TCK md. 245 (Banka veya Kredi Kartlarının Kötüye Kullanılması):** Bu madde geleneksel plastik kartlar düşünülerek kaleme alınmıştır. Günümüzde ise kripto varlık cüzdanları, merkezizsiz finans (DeFi) hesapları, dijital cüzdanlar (Apple Pay, Papara vb.) ve biyometrik ödeme sistemleri yaygındır. Kripto varlıkların rıza dışı transferi veya soğuk cüzdanların ele geçirilmesi eylemleri TCK 245 kapsamında doğrudan cezalandırılmamakta; nitelikli hırsızlık (md. 142/2-e) veya TCK 244 arasında nitelendirme ihtilafları doğmaktadır. 245. maddenin "Dijital Ödeme Araçları ve Kripto Varlıkları" kapsayacak şekilde genişletilmesi şarttır.

- **TCK md. 245/A (Zararlı Yazılım):** Bir bilişim suçunun işlenmesi amacıyla cihaz, program veya şifre imal edilmesini düzenleyen bu madde, siber güvenlik uzmanlarının ve beyaz şapkalı hackerların sistem test etmek için geliştirdiği çift yönlü (dual-use) yazılımları da suçlama riski taşımaktadır. Maddede "kullanım amacına yönelik kastın" tespiti gri bir alan olarak kalmaktadır.

Ceza Muhakemesinde Suçluların ve Dijital Delillerin Tespiti (CMK md. 134 Sorunu)

Bilişim suçlarında faillerin tespiti ve delil elde edilmesi, Ceza Muhakemesi Kanunu'nun (CMK) sınırlarını en çok zorlayan alandır. Mevcut sistemdeki en temel koruma tedbiri olan CMK md. 134 (Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma) hükmü, bugünün siber gerçekliği karşısında pratik değerini kaybetmektedir:

- **Fiziki El Koyma Çıkmazı:** CMK 134, özü itibarıyla kolluğun suç mahallindeki fiziki bir bilgisayara veya sabit diske el koyması mantığına dayanır. Oysa günümüzde veriler sınır ötesindeki çok uluslu bulut sunucularında (Cloud) tutulmaktadır. Şüpheli yakalandığında elindeki cihaz sadece veriye erişen bir "ara yüzdür". Sunucusu yurt dışında olan veri üzerinde arama yapılması devletlerin egemenlik hakları ve adli yardımlaşma (MLAT) [6] engellerine takılmakta, suçluların tespiti gecikmekte veya imkânsızlaşmaktadır.

- **IP Değişkenliği, VPN ve Tor Ağları:** Siber suçlular kimliklerini gizlemek için dinamik IP'ler, VPN (Sanal Özel Ağ) servisleri ve Tor gibi anonim ağlar kullanmaktadır. Mevcut CMK mevzuatı, adli kolluğun siber alanda sınır ötesi "online sızma" veya "uzaktan arama" (remote search) yapmasına izin vermemektedir.

- **Dijital Delilin Bozulabilirliği ve Hash Değeri:** Dijital deliller çok hızlı değiştirilebilir ve yok edilebilir yapıdadır. Kolluğun arama ve kopyalama esnasında cihazın imajını alırken "Hash (Zaman Damgalı Matematiksel Özet)" değerini doğru saptayamaması, yargılamada delilin sıhhatini sakatlamakta ve zincirleme usul hatalarına yol açmaktadır.

Yasa Dışı Bahis ve Kumarın Bilişim Suçları Kapsamındaki Yeri

Yasa dışı bahis siteleri, bilişim teknolojileri üzerinden işlenen suçların en tipik örneklerinden birini oluşturmaktadır. Bu siteler; hem 7258 sayılı Kanun hem de Türk Ceza Kanunu hükümleri çerçevesinde değerlendirilmektedir.

A. Teknik Altyapı ve Erişim Engelleme: Bu tür siteler, alan adı değiştirerek —örneğin site1.com, site2.com biçiminde— Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından uygulanan erişim engellerini aşmaya çalışmaktadır. 5651 sayılı Kanun kapsamında BTK, katalog suçlar çerçevesinde

mahkeme kararı aranmaksızın erişim engeli getirebilmektedir. Bu durum, bilişim hukukunda hızlı müdahale mekanizmasının en önemli örneklerinden birini teşkil etmektedir.

B. Ödeme Sistemleri ve Manipülasyon: Yasa dışı bahis platformları, finansal işlemleri gizlemek amacıyla başkasına ait banka hesapları, kripto varlıklar veya otomatik transfer botları kullanmaktadır. Bu noktada Türk Ceza Kanunu'nun 245. maddesi (banka/kredi kartlarının kötüye kullanılması) ile yasa dışı bahse imkân sağlama suçları devreye girmektedir. Ayrıca bu sistemlerde görev alan araçlar ve teknik destek sağlayıcılar da doğrudan hukuki sorumluluk altına girebilmektedir.

C. Siber Güvenlik Riskleri ve Veri İhlali: Bu platformların en kritik risk alanı veri güvenliğidir. Kullanıcı bilgilerinin şifrlenmeden saklanması, dark web üzerinde satılması veya kötü amaçlı yazılımlar aracılığıyla cihazlara sızılması ciddi siber güvenlik tehditleri doğurmaktadır. Bu tür sistemler aynı zamanda cihazları **botnet ağlarına** [7] dahil ederek geniş ölçekli siber saldırıların bir parçası hâline getirebilmektedir.

Sonuç ve Öneriler

Tespit edilen bu yapısal yetersizlikler yalnızca bir eleştiri düzeyinde bırakılmamalı; somut yasal düzenlemelerle giderilmelidir. Yapay zekâ, dijital ödeme sistemleri ve yasa dışı çevrimiçi faaliyetler; ceza hukuku ile bilişim hukukunun kesişiminde yeni bir sorumluluk rejimi doğurmaktadır. Mevcut mevzuat bu alanları tam anlamıyla kapsamamakta olup, teknik gelişmelerle uyumlu, daha esnek ve risk temelli bir hukuki düzenleme ihtiyacı giderek artmaktadır.

Bilişim suçlarının artan çeşitliliği ve teknolojik dönüşümün hız kazanması; bu alanda dağınık ve parçalı mevzuat yapısının yerine, bütüncül ve sistematik bir yasal düzenleme ihtiyacını ortaya çıkarmaktadır. Bu kapsamda, yalnızca mevcut Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu hükümlerinin güncellenmesi yeterli olmayıp; bilişim suçlarını doğrudan ve kapsamlı biçimde düzenleyen özel bir "Bilişim Suçları Kanunu"nın hazırlanması gerekmektedir.

Söz konusu kanun, yalnızca mevcut suç tiplerini yineleyen bir yapıdan ziyade; yapay zekâ, büyük veri, algoritmik sistemler, dijital platformlar ve kripto varlıklar gibi yeni teknolojik alanları da kapsayan, dinamik ve teknolojiye uyumlu bir normatif çerçeve içermelidir. Böylece suç tiplerinin yalnızca mevcut teknolojilere göre değil, gelecekte ortaya çıkabilecek dijital risk alanlarına göre de tanımlanması mümkün olacaktır.

Bu doğrultuda oluşturulacak yasal düzenlemenin en önemli unsurlarından biri; teknolojik gelişmeleri sürekli takip edecek ve mevzuatın güncelliğini sağlayacak bağımsız bir "Dijital Hukuk ve Teknoloji Düzenleme Kurulu"nın kurulmasıdır. Bu kurulun üstlenmesi öngörülen görevler şu şekilde sıralanabilir:

- Yapay zekâ, siber güvenlik ve veri teknolojilerindeki gelişmeleri izlemek,
- Yeni ortaya çıkan dijital riskleri analiz etmek,
- Gerekli yasal değişiklik önerilerini hazırlamak,
- Ulusal ve uluslararası düzenlemelerle uyumu sağlamak,
- Kamu kurumları ile özel sektör arasında teknik ve hukuki koordinasyonu yürütmek.

Kurulun bağımsız, uzmanlık temelli ve disiplinler arası bir yapıda oluşturulması; hem hukuki hem de teknik açıdan etkin karar alma süreçlerini destekleyecektir. Özellikle hukukçular, bilişim uzmanları, yapay zekâ mühendisleri ve kriminoloji alanında uzmanlaşmış kişilerin birlikte yer aldığı böyle bir yapı, dijital suçlarla mücadelede bütüncül bir yaklaşımın temelini oluşturacaktır.

Sonuç olarak, bilişim suçlarıyla etkin biçimde mücadele edebilmek için yalnızca mevcut mevzuatın güncellenmesi yeterli olmayıp; aynı zamanda teknolojik gelişmeleri sürekli izleyen, esnek ve proaktif bir düzenleyici mekanizmanın oluşturulması zorunluluk arz etmektedir. Bu sayede hukuk sistemi, dijital dönüşüm karşısında reaktif bir tutum sergilemek yerine önleyici ve yönlendirici bir işlev üstlenebilecektir.

[AKADEMİK DİPNOTLAR]

[1] Prompt Injection: Yapay zekâ ve büyük dil modellerine (LLM) yönelik bir siber manevra/saldırı türüdür. Sistemin önceden tanımlanmış güvenlik filtrelerini, bağlam sınırlarını veya sistem talimatlarını aşmak amacıyla, kötü niyetli kullanıcılar tarafından modele özel tasarlanmış doğal dil girdilerinin (prompt) gönderilmesi eylemidir. Bu yöntemle yapay zekâ manipüle edilerek, normal şartlarda üretmesi engellenmiş olan hukuka aykırı veya telif ihlali barındıran çıktıların üretilmesi sağlanır.

[2] ESG (Environmental, Social, and Governance): Şirketlerin faaliyetlerinin çevresel etkilerini, toplumsal sorumluluklarını ve kurumsal yönetim kalitelerini ölçen uluslararası uyum kriterleridir. Yapay zekâ veri merkezlerinin yüksek karbon ayak izi ve su tüketimi, bu kriterlerin "Çevresel" (Environmental) ayağı kapsamında hukuki denetimlere ve idari yaptırımlara tabi tutulmaktadır.

[3] Tokenize Etme (Jetonlaştırma): Dijital ödeme sistemlerinde veri güvenliğini sağlamak amacıyla; kredi kartı numarası (PAN) gibi hassas bir verinin, sistem dışından ele geçirilse dahi tek başına hiçbir finansal karşılığı olmayan ve "token" (jeton) adı verilen rastgele, şifreli ve benzersiz bir değer dizisiyle değiştirilmesi sürecidir. Bu yöntem sayesinde hassas kart verileri ağ üzerinde açıkça taşınmaz ve saklanmaz.

[4] Zero-Day (Sıfırıncı Gün) Açığı: Bir yazılım veya donanım sisteminde meydana gelen, geliştiriciler tarafından henüz keşfedilmemiş ve dolayısıyla henüz bir yaması (patch) veya güvenlik güncellemesi bulunmayan sistemsal zafiyetlerdir. Saldırganların bu açığı istismar ettiği an ile yazılımcıların durumdan haberdar olduğu an arasında "0 gün" bulunmasından ötürü bu isimle anılır. Bilişim hukukunda kurumların kusur sorumluluğunun sınırlarını tayin etmede kritik bir teknik parametredir.

[5] Man-in-the-Middle (Ortakdaki Adam / MitM) Saldırısı: İki siber sistem arasındaki iletişimin, tarafların haberi olmaksızın üçüncü bir kötü niyetli kişi veya otonom yazılım tarafından gizlice dinlenmesi, kesilmesi veya değiştirilmesi siber saldırı modelidir. Veri, uç noktadaki fiziksel sistemlere/veri tabanlarına henüz girilmeden ağ katmanında havada ele geçirildiği için klasik "bilişim sistemine girme" (TCK md. 243) suçunun lafzi sınırlarını zorlamaktadır.

[6] MLAT (Mutual Legal Assistance Treaty - Karşılıklı Adli Yardımlaşma Antlaşması): İki veya daha fazla devlet arasında, ceza soruşturmalarında ve dijital delil toplama süreçlerinde yasal bilgi ve yardım paylaşımını düzenleyen uluslararası antlaşmalardır. Sunucusu yurt dışında olan bulut (cloud) sistemlerindeki verilere erişim, devletlerin egemenlik hakları gereği bu antlaşma mekanizmalarına tabidir ve siber suç soruşturmalarındaki en büyük bürokratik gecikme nedenlerinden biridir.

[7] Botnet (Zombi Ağları): Siber saldırganlar tarafından zararlı yazılımlarla uzaktan kontrol

altına alınmış, internete baęlı ok sayıda bilgisayar, sunucu veya IoT (Nesnelerin İnterneti) cihazından oluřan aędır. Cihaz sahiplerinin haberi olmaksızın bu sistemler, yasa dıřı bahis siteleri tarafından b y k  lekli siber saldırılarda ( rneęin DDoS) veya finansal trafik gizlemede koordineli bir ara olarak kullanılabilmektedir.

6. Çalışma Grubu Raporu-

Dr. Öğr. Üyesi Gürkan Özocak'ın sorusu: Yapay zekâ bakımından otonom araçların ve daha geniş kapsamda otonom sistemlerin meydana getirdiği zararlı sonuçlar yönünden ceza sorumluluğu nasıl belirlenmelidir?

Katılımcılar:

1. Irmak Altay (Bilgisayar Mühendisliği)
2. Riad Osman (Bilgisayar Mühendisliği)
3. Mehmet Efe Aytaş (Bilgisayar Mühendisliği)
4. Egesu Bayat (Hukuk)
5. Hatice Şimdi (Hukuk)

ÖZET

Yapay zekâ destekli otonom sistemlerin —özellikle otonom araçların— neden olduğu ölüm, yaralanma ve mal varlığı zararları, ceza hukukunun klasik kavramlarını yeniden düşünmeyi zorunlu kılmaktadır. Klasik ceza hukuku, kararlarını veren ve eylemini iradi olarak gerçekleştiren bir insan failini esas alır; oysa otonom sistemler, davranışı önceden tam olarak öngörülemeyen, sürekli öğrenen ve birden fazla aktörün katkısıyla ortaya çıkan kararlar üretir. Bu durum literatürde "sorumluluk boşluğu" olarak adlandırılmaktadır.

Bu rapor, ceza sorumluluğunun tek bir aktöre yüklenmesi yerine; üretici, yazılımcı, işletmeci, kullanıcı ve düzenleyici otorite arasında otonomi seviyesine göre kademeli olarak dağıtıldığı çok katmanlı bir model önermektedir. Ceza hukuku, bu mimaride ancak ağır ve organizasyonel kusur hâllerine müdahale eden ultima ratio olarak konumlandırılmalı; sıradan kazaların telafisi, kusursuz sorumluluk ve zorunlu sigorta mekanizmaları üzerinden gerçekleştirilmelidir.

1. GİRİŞ VE SORUNUN ÇERÇEVESİ

Otonom araçların kara trafiğine, otonom dronların hava sahasına, robotik cerrahi sistemlerinin ameliyathanelere, otonom üretim hatlarının fabrikalara girmesiyle birlikte; bu sistemlerin yol açtığı zararlı sonuçların kime, hangi temelle isnat edileceği sorusu acil bir hukuki gündem hâline gelmiştir. Ceza hukuku açısından mesele yalnızca bir tazminat tartışması değildir; zira ceza hukuku kınama, önleme ve toplumsal güvenliğin yeniden tesisi gibi tazminattan farklı işlevler taşır.

Sorunun özü; modern ceza hukukunun kusur (kast veya taksir), nedensellik ve insan iradesi temelli yapısıyla, kararlarını öğrenme algoritmalarıyla şekillendiren makineler arasındaki uyumsuzluktan kaynaklanır. Bu rapor, söz konusu uyumsuzluğu temel boyutlarıyla ele almakta; karşılaştırmalı hukuk perspektifiyle çözüm önerilerini değerlendirmekte ve Türk ceza hukuku bakımından yapılması gerekenleri tartışmaktadır.^{4 5}

2. SORUNUN HUKUKSAL ÇEKİRDEĞİ

2.1. Tipiklik, Hukuka Aykırılık ve Kusur

⁴ Matthias, Andreas. "The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata", *Ethics and Information Technology*, Vol. 6, No. 3, 2004, s. 175-183.

⁵ Sözüer, Adem. "Yapay Zekâ Çağında Ceza Hukukunun Geleceği", *İstanbul Hukuk Mecmuası*, C. 78, S. 2, 2020, s. 593-625.

Ceza sorumluluğunun klasik unsurları olan tipiklik, hukuka aykırılık ve kusur, otonom sistemler bakımından her üç boyutta da problemliliğe hâle gelmektedir. Tipiklik bakımından, fiilin kim tarafından gerçekleştirildiği belirsizdir: Üretici mi, yazılımcı mı, eğitim verilerini sağlayan mı, aracı satışa sunan mı, sistemin "sürücüsü" konumundaki kullanıcı mı, yoksa sistemin kendisi mi? Hukuka aykırılık bakımından, trafik kurallarına uyumun denetimini insandan makineye devreden bir hukuk düzeni, ihlalin kime atfedileceği konusunda yeni ölçütlere ihtiyaç duyar.

En çetrefilli mesele kusurdur. TCK m. 21 anlamında kast ya da m. 22 anlamında taksir, iradi bir insan davranışına dayanır.⁶ Sinir ağı tabanlı bir sistemin kararını kast veya taksir kalıbına oturtmak doğrudan mümkün değildir. Bu noktada kusurun, sistemi tasarlayan, üreten, eğiten, satışa sunan veya işleten gerçek/tüzel kişilere izafe edilmesi gerekir; ancak bu izafe işleminin hukuki ölçütleri henüz tam anlamıyla belirlenmiş değildir.⁷

2.2. Kara Kutu Sorunu

Derin öğrenme modellerinin kararları çoğu zaman üreticinin kendisi tarafından bile tam olarak açıklanamaz. Bu "kara kutu" (black box) sorunu, hem nedensellik bağının kurulmasını hem de öngörülebilirliğin —ki taksirin temel ölçütüdür— tespitini güçleştirir. Açıklanabilir yapay zekâ (explainable AI) çalışmaları bu güçlüğü kısmen hafifletse de, mevcut teknolojik düzeyde ceza yargılamasının ihtiyaç duyduğu kesinlikten oldukça uzaktır. Bu durum, açıklanabilirlik yükümlülüğünü hukuki bir yükümlülük olarak konumlandırma ihtiyacını doğurmaktadır.⁸

3. CEZA SORUMLULUĞUNUN OLASI ADRESLERİ

3.1. Üretici ve Yazılım Geliştirici Sorumluluğu

İlk akla gelen yol, ürün sorumluluğunun klasik kalıplarını ceza hukukuna uyarlamaktır: tasarım hatası, üretim hatası, talimat ve uyarı eksikliği. Türk hukukunda bu sorumluluk, taksirle öldürme (TCK m. 85) veya taksirle yaralama (TCK m. 89) çerçevesinde değerlendirilebilir. Ancak burada üreticinin objektif özen yükümlülüğüne aykırı davranmış olması ve zararın öngörülebilir olması gerekir. Sistemin makul ölçüde test edilmiş, güncel teknik standartlara uygun olarak piyasaya sürülmüş olması üretici lehine bir dayanak oluşturur. Aksine, bilinen bir riskin göz ardı edilmesi, yetersiz simülasyon, eğitim verilerindeki taraflılığın farkına rağmen düzeltilmemesi ya da güvenlik güncellemelerinin (OTA) ihmali doğrudan kusur teşkil edebilir.⁹

3.2. Operatör ve Kullanıcı Sorumluluğu

Seviye	Tanım	İnsan Rolü
Seviye 0	Sürücüsüz değil	Tam kontrol
Seviye 1	Sürücü asistanı	Sistem destekli, insan kontrolü

⁶ Türk Ceza Kanunu, Kanun No. 5237, R.G. 12.10.2004, S. 25611 (özellikle m. 20, 21, 22, 23, 60, 85, 89, 170, 179).

⁷ Hilgendorf, Eric. "Können Roboter schuldhaft handeln?", Beck/Hilgendorf (Hrsg.), *Jenseits von Mensch und Maschine*, Nomos, Baden-Baden, 2012, s. 119-132.

⁸ European Commission, High-Level Expert Group on AI. *Ethics Guidelines for Trustworthy AI*. Brüksel, 8 Nisan 2019.

⁹ Türk Ceza Kanunu, Kanun No. 5237, R.G. 12.10.2004, S. 25611 (özellikle m. 20, 21, 22, 23, 60, 85, 89, 170, 179).

Seviye	Tanım	İnsan Rolü
Seviye 2	Kısmi otonomi	Sistem kontrolü, insan gözetimi
Seviye 3	Koşullu otonomi	Sistem kontrolü, insan talep edildiğinde müdahale
Seviye 4	Yüksek otonomi	Sistem kontrolü, belirli senaryolarda insan gerekmez
Seviye 5	Tam otonomi	Sistem tam kontrol, insan sürücü gerekmez

Operatör ve kullanıcı sorumluluğu, otonomi seviyesine göre değişen bir tablo çizer. SAE J3016 sınıflandırması burada anahtar rol oynar. Seviye 0–2’de sürücü asıl karar vericidir; klasik trafik suçları doğrudan ona izafe edilir. Seviye 3’te ("koşullu otonomi") sürücünden talep üzerine kontrolü devralması beklenir; bu nedenle "devralma yükümlülüğüne" uymama bağımsız bir kusur kaynağı oluşturur. Seviye 4 ve 5’te ise sürücü kavramı işlevsizleşir; sorumluluk büyük ölçüde üretici/işletici tarafına kayar.

Almanya’nın 2017’de Karayolları Kanunu’nda yaptığı değişiklik ile 2021’deki "otonom sürüş yasası", bu kademeli sorumluluk modelinin somutlaştığı en önemli örneklerdendir. Söz konusu düzenlemede aracın bir "teknik denetçisi öngörülmüş ve sorumluluk kısmen bu kişiye yüklenmiştir.^{10 11 12}

3.3. İşletmecinin ve Filo Sahibinin Sorumluluğu

Özellikle ticari otonom araçlar (robotaksi, otonom kamyon filoları) bakımından işletmecinin sorumluluğu önem kazanır. Bakım yükümlülüğünün ihlali, yazılım güncellemelerinin yapılmaması, sistemin tasarlandığı koşulların dışında —operational design domain dışında— çalıştırılmasına izin verilmesi, organizasyonel kusur olarak somutlaşır.

3.4. Tüzel Kişilerin Ceza Sorumluluğu

Türk hukukunda tüzel kişiler hakkında doğrudan ceza yaptırımını uygulanamaz (TCK m. 20/2); yalnızca güvenlik tedbirleri (TCK m. 60) söz konusu olabilir. Oysa Almanya, Fransa, Hollanda gibi ülkelerde gelişen kurumsal ceza sorumluluğu modelleri, yapay zekâ sistemleri bakımından çok daha elverişli bir çerçeve sunmaktadır. Çünkü tek bir gerçek kişi failine indirgenemeyen "dağıtık kusur" hâllerinde organizasyonun kendisini muhatap almak gerekir. Bu nedenle Türk hukukunda da tüzel kişilere yönelik gerçek anlamda cezai yaptırımların yeniden tartışmaya açılması zorunlu görünmektedir.¹³

¹⁰ SAE International. *J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, revize 2021.

¹¹ Almanya — *Straßenverkehrsgesetz (StVG)*, 2017 (BGBl. I 2017, S. 1648) ve 2021 değişiklikleri (*Gesetz zum autonomen Fahren*, BGBl. I 2021, S. 3108).

¹² Beck, Susanne. "Intelligent Agents and Criminal Law - Negligence, Diffusion of Liability and Electronic Personhood", *Robotics and Autonomous Systems*, Vol. 86, 2016, s. 138-143.

¹³ Türk Ceza Kanunu, Kanun No. 5237, R.G. 12.10.2004, S. 25611 (özellikle m. 20, 21, 22, 23, 60, 85, 89, 170, 179).

4. "YAPAY ZEKÂNIN KENDİSİNİN" FAİL OLABİLİRLİĞİ

Avrupa Parlamentosu'nun 2017 tarihli kararıyla tartışmaya açtığı "elektronik kişilik" önerisi, ceza hukuku açısından oldukça sınırlı kabul gören bir tezdır. Bu tezin reddedilmesinin başlıca nedenleri şunlardır: ceza yaptırımının bir anlam taşıyabilmesi için failin acı çekme, pişmanlık duyma ve davranışını yeniden şekillendirme kapasitesine sahip olması gerekir; mevcut yapay zekâ sistemleri bu kapasitelere sahip değildir. Ayrıca cezanın özel ve genel önleme amaçları makine üzerinde işlevsizdir.

Daha da önemlisi, "elektronik kişilik" tanımak, gerçek sorumluları —üretici ve işleticiyi— sorumluluktan kurtaran bir paravan işlevi görme riski taşır. AB'nin 2024'te kabul ettiği Yapay Zekâ Yasası bu tezi açıkça reddetmiş; yapay zekânın insan denetimi altında kalmasını esas almıştır.^{14 15 16}

5. NEDENSELLİK VE OBJEKTİF İSNADİYET

Otonom sistemlerin neden olduğu zararlarda nedensellik bağının kurulması, klasik *conditio sine qua non* formülüyle çözülemez; çünkü zincirde birden fazla "hipotetik fail" yer alır. Bu nedenle çağdaş Alman doktrininde geliştirilen ve Türk doktrininde de yansımaları bulunan objektif isnadiyet teorisi devreye girer. Bu teoriye göre fail, hukuken izin verilmeyen bir riski yaratmış ve bu risk tipik bir neticede somutlaşmışsa neticeden sorumlu tutulur.

Otonom araç bağlamında şu sorular sorulur: Üretici, izin verilen riskin sınırlarını aşan bir tasarım kararı aldı mı? Risk, sertifikasyon süreçlerinde tespit edilebilir miydi? Kullanıcı, sistemin tasarlandığı kullanım alanı dışında bir kullanım gerçekleştirdi mi? Bu sorulara verilen yanıtlar, sorumluluğun katmanlı biçimde dağıtılmasına izin verir.

Burada güven ilkesi de tartışmalı bir rol oynar. Trafik hukukunda her sürücü, diğerlerinin kurallara uyacağına güvenebilir. Sertifikalı bir otonom sistemin, üreticinin verdiği talimatlara uygun kullanılması hâlinde kullanıcıyı koruyan bir "güven ilkesi uzantısı" doğabilir mi? Doktrindeki eğilim belirli koşullarda olumlu yöndedir; ancak bu, üreticinin sorumluluğunu artıran simetrik bir etki doğurur.^{17 18 19}

6. DÜZENLEYİCİ ÇERÇEVENİN ROLÜ

AB Yapay Zekâ Yasası, yüksek riskli sistemler arasında otonom araç bileşenlerini de saymakta; uygunluk değerlendirmesi, kayıt tutma, açıklanabilirlik, insan denetimi gibi yükümlülükler getirmektedir. Bu yükümlülüklerin ihlali, ceza hukuku bakımından doğrudan suç tipi oluşturmaya da taksirin tespitinde objektif özen yükümlülüğünün somut içeriğini belirler.

İngiltere'nin Automated and Electric Vehicles Act 2018 düzenlemesi farklı bir model sunar: Sigortacı mağduru tazmin eder, rücu hakları üreticiye karşı iletir. Türk hukukunda da Sanayi ve Teknoloji Bakanlığı'nın araç tip onayı mevzuatı, Karayolları Genel Müdürlüğü'nün altyapı düzenlemeleri ve Ulusal Yapay Zekâ Stratejisi çerçevesinde geliştirilmesi öngörülen düzenlemeler bu işlevi görecektir.

Mevzuatın belirlediği teknik standartlara uyum, bir tür "mevzuata uygunluk savunması"

¹⁴ Avrupa Parlamentosu. *Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)), P8_TA(2017)0051.

¹⁵ Hallevy, Gabriel. "The Criminal Liability of Artificial Intelligence Entities", *Akron Intellectual Property Journal*, Vol. 4, 2010, s. 171-201.

¹⁶ Avrupa Birliği — *Regulation (EU) 2024/1689 - Artificial Intelligence Act*, OJ L 1689, 12.7.2024.

¹⁷ Roxin, Claus. *Strafrecht Allgemeiner Teil, Band I*. 4. Auflage, C. H. Beck, München, 2006.

¹⁸ Koca, Mahmut / Üzülmüş, İlhan. *Türk Ceza Hukuku Genel Hükümler*. 15. Baskı, Seçkin Yayıncılık, Ankara, 2022.

¹⁹ Gless, Sabine / Silverman, Emily / Weigend, Thomas. "If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability", *New Criminal Law Review*, Vol. 19, No. 3, 2016, s. 412-436.

sağlayabilir; ancak bu mutlak bir bağımsızlık değildir. Üreticinin, mevzuat üstü bilgi ve kapasiteyle önlenilecek bir riski göz ardı etmesi hâlinde sorumluluk doğmaya devam eder.²⁰

21 22

7. CEZA HUKUKU İLE TAZMİNAT HUKUKUNUN İŞLEVSEL AYRIMI

Çağdaş tartışmada güçlenen bir görüş, otonom sistemlerin yarattığı zararların büyük ölçüde kusursuz sorumluluk ve zorunlu sigorta mekanizmalarıyla, yani hukuki sorumluluk üzerinden çözülmesi gerektiği yönündedir. Bu yaklaşım, ceza hukukunun istisnai niteliğine de uygundur. Ceza hukuku, ancak ağır kusurun, kasten gizlenmiş kusurların, sistemik organizasyonel ihmallerin söz konusu olduğu hâllere saklanmalı; sıradan trafik kazalarında devreye girmemelidir.

Bu anlayışın pratik karşılığı şudur: Otonom araç kazasında mağdurun derhâl tazmini sigorta üzerinden sağlanmalı; üretici veya işleticinin ağır ihmali tespit edildiğinde ise bağımsız bir cezai soruşturma süreci başlatılmalıdır. Böylece ceza hukukunun caydırıcılığı, hukuki sorumluluk hukukunun telafi işleviyle birlikte çalışır.^{23 24}

8. TÜRK HUKUKU BAKIMINDAN DEĞERLENDİRME

Türk hukuku henüz otonom araçlara özgü bir ceza normu öngörmemiştir. Hâlihazırda olası senaryolar mevcut TCK normlarıyla çözülmek zorundadır: taksirle öldürme (m. 85), taksirle yaralama (m. 89), trafik güvenliğini tehlikeye sokma (m. 179), genel güvenliğin kasten tehlikeye sokulması (m. 170) ve özellikle bilinçli taksir (m. 22/3) bağlamında değerlendirilebilecek hâller.

Bu çerçevede önerilebilecek yasama adımları şunlardır: Otonomi seviyelerine göre kademeli sorumluluk modelinin yasalaştırılması; üretici için "denetlenebilirlik ve loglama" yükümlülüğünün getirilmesi; kazadan sonra kara kutu verilerinin korunması ve adli makamlara açılması zorunluluğunun düzenlenmesi; bağımsız bir teknik denetim kurumunun kurulması; zorunlu yapay zekâ sigortasının ihdas edilmesi; ve nihayet tüzel kişiler için sınırlı da olsa cezai yaptırım imkânının tartışmaya açılması.

Bu adımların atılması, hem mağdurların etkin biçimde korunmasını hem de yenilikçi teknolojinin Türkiye'de gelişmesini önündeki hukuki belirsizliğin azaltılmasını sağlayacaktır.²⁵

9. SONUÇ

Otonom sistemlerin yol açtığı zararlarda ceza sorumluluğu, tek bir adresi olan klasik bir kusur sorunu olarak ele alınamaz; çok katmanlı, dağıtık ve kademeli bir model gerektirir. Bu modelin temel taşları üreticinin objektif özen yükümlülüğü, kullanıcının/operatörün otonomi seviyesine göre değişen yükümlülükleri, işleticinin organizasyonel sorumluluğu, düzenleyicinin belirlediği teknik standartlar ve nihayet zararı süratle gideren sigorta mekanizmalarıdır.

Ceza hukuku bu mimarının tamamını taşımak yerine, ağır ve organizasyonel kusurların yaptırımını olarak konumlanmalı; "elektronik kişilik" gibi sorumluluğu buharlaştırma riski taşıyan tezlerden kaçınılmalıdır. Türk ceza hukukunun da orta vadede, mevcut taksir teorisini

²⁰ Avrupa Birliği — *Regulation (EU) 2024/1689 - Artificial Intelligence Act*, OJ L 1689, 12.7.2024.

²¹ Birleşik Krallık — *Automated and Electric Vehicles Act 2018*, c. 18; ve *Automated Vehicles Act 2024*, c. 10.

²² Cumhurbaşkanlığı Dijital Dönüşüm Ofisi & Sanayi ve Teknoloji Bakanlığı. *Ulusal Yapay Zekâ Stratejisi 2021-2025*. Ankara, 2021.

²³ Türk Borçlar Kanunu, Kanun No. 6098, R.G. 04.02.2011, S. 27836 (özellikle m. 49, 65-69).

²⁴ Aksoy, Hüseyin Can. "Otonom Araçlar ve Hukuki Sorumluluk", *Türkiye Adalet Akademisi Dergisi*, S. 41, 2020, s. 1-34.

²⁵ Türk Ceza Kanunu, Kanun No. 5237, R.G. 12.10.2004, S. 25611 (özellikle m. 20, 21, 22, 23, 60, 85, 89, 170, 179).

koruyarak bu çok aktörlü modele özgü düzenlemelere kavuşması kaçınılmaz görünmektedir. Aksi hâlde, hızla yaygınlaşan otonom teknolojiler karşısında hem mağdurların korunmasında hem de hukuki öngörülebilirlikte ciddi açıklar oluşacaktır.^{26 27}

KAYNAKÇA

I. Kitaplar ve Monografiler

Demirbaş, Timur. *Ceza Hukuku Genel Hükümler*. 17. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Hakeri, Hakan. *Ceza Hukuku Genel Hükümler*. 25. Baskı, Adalet Yayınevi, Ankara, 2022.

Koca, Mahmut / Üzülmüş, İlhan. *Türk Ceza Hukuku Genel Hükümler*. 15. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Özgenç, İzzet. *Türk Ceza Hukuku Genel Hükümler*. 18. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Roxin, Claus. *Strafrecht Allgemeiner Teil, Band I*. 4. Auflage, C. H. Beck, München, 2006.

Pagallo, Ugo. *The Laws of Robots: Crimes, Contracts, and Torts*. Springer, Dordrecht, 2013.

Hilgendorf, Eric / Beck, Susanne (Hrsg.). *Robotik im Kontext von Recht und Moral*. Nomos, Baden-Baden, 2014.

Calo, Ryan / Froomkin, Michael / Kerr, Ian (Eds.). *Robot Law*. Edward Elgar Publishing, Cheltenham, 2016.

II. Makaleler ve Kitap Bölümleri

Aksoy, Hüseyin Can. "Otonom Araçlar ve Hukuki Sorumluluk", *Türkiye Adalet Akademisi Dergisi*, S. 41, 2020, s. 1-34.

Beck, Susanne. "Intelligent Agents and Criminal Law - Negligence, Diffusion of Liability and Electronic Personhood", *Robotics and Autonomous Systems*, Vol. 86, 2016, s. 138-143.

Calo, Ryan. "Robotics and the Lessons of Cyberlaw", *California Law Review*, Vol. 103, No. 3, 2015, s. 513-563.

Gless, Sabine / Silverman, Emily / Weigend, Thomas. "If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability", *New Criminal Law Review*, Vol. 19, No. 3, 2016, s. 412-436.

Hallevy, Gabriel. "The Criminal Liability of Artificial Intelligence Entities", *Akron Intellectual Property Journal*, Vol. 4, 2010, s. 171-201.

Hilgendorf, Eric. "Können Roboter schuldhaft handeln?", Beck/Hilgendorf (Hrsg.), *Jenseits von Mensch und Maschine*, Nomos, Baden-Baden, 2012, s. 119-132.

Matthias, Andreas. "The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata", *Ethics and Information Technology*, Vol. 6, No. 3, 2004, s. 175-183.

Sözüer, Adem. "Yapay Zekâ Çağında Ceza Hukukunun Geleceği", *İstanbul Hukuk Mecmuası*, C. 78, S. 2, 2020, s. 593-625.

Ünver, Yener. "Yapay Zekâ ve Ceza Hukuku", *Ceza Hukuku Dergisi*, C. 14, S. 41, 2019, s.

²⁶ Pagallo, Ugo. *The Laws of Robots: Crimes, Contracts, and Torts*. Springer, Dordrecht, 2013.

²⁷ Calo, Ryan. "Robotics and the Lessons of Cyberlaw", *California Law Review*, Vol. 103, No. 3, 2015, s. 513-563.

657-702.

III. Mevzuat

Türk Ceza Kanunu, Kanun No. 5237, R.G. 12.10.2004, S. 25611 (özellikle m. 20, 21, 22, 23, 60, 85, 89, 170, 179).

Türk Borçlar Kanunu, Kanun No. 6098, R.G. 04.02.2011, S. 27836 (özellikle m. 49, 65-69).

Karayolları Trafik Kanunu, Kanun No. 2918, R.G. 18.10.1983, S. 18195.

Avrupa Birliği — *Regulation (EU) 2024/1689 - Artificial Intelligence Act*, OJ L 1689, 12.7.2024.

Avrupa Birliği — *Directive (EU) 2024/2853 on Liability for Defective Products*, OJ L, 18.11.2024.

Almanya — *Straßenverkehrsgesetz (StVG)*, 2017 (BGBl. I 2017, S. 1648) ve 2021 değişiklikleri (*Gesetz zum autonomen Fahren*, BGBl. I 2021, S. 3108).

Birleşik Krallık — *Automated and Electric Vehicles Act 2018*, c. 18; ve *Automated Vehicles Act 2024*, c. 10.

IV. Resmî Belgeler ve Raporlar

Avrupa Parlamentosu. *Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)), P8_TA(2017)0051.

European Commission, High-Level Expert Group on AI. *Ethics Guidelines for Trustworthy AI*. Brüksel, 8 Nisan 2019.

Bundesministerium für Verkehr und digitale Infrastruktur (Almanya). *Ethik-Kommission Automatisiertes und Vernetztes Fahren - Bericht*. Berlin, Haziran 2017.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi & Sanayi ve Teknoloji Bakanlığı. *Ulusal Yapay Zekâ Stratejisi 2021-2025*. Ankara, 2021.

UK Law Commission & Scottish Law Commission. *Automated Vehicles: Joint Report* (Law Com No 404; Scot Law Com No 258), HC 1068, January 2022.

V. Standartlar

SAE International. *J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, revize 2021.

ISO/SAE. *ISO 21448:2022 - Road Vehicles - Safety of the Intended Functionality (SOTIF)*.

ISO. *ISO 26262:2018 - Road Vehicles - Functional Safety* (tüm bölümler).

7. Çalışma Grubu Raporu-

Dr. Öğr. Üyesi Başak Buluz Kömeçoğlu'nun sorusu: Açıklanabilirlik zorunluluğu, yapay zekâ sistemlerinin performansı ile ne ölçüde bir “trade-off” yaratır? Bu durumda düzenlemeler, daha şeffaf ama daha düşük performanslı sistemleri mi önceliklendirmelidir, yoksa yüksek performanslı ancak “kara kutu” modellerin kullanımına belirli koşullar altında izin verilmeli midir? Bu koşullar teknik ve hukuki olarak nasıl tanımlanmalıdır?

Katılımcılar:

1. Ayşe Nur Ünal (Bilgisayar Mühendisliği)
2. Mustafa Hali (Bilgisayar Mühendisliği)
3. Yusuf Ali Gün (Bilgisayar Mühendisliği)
4. Yusuf Mengüç (Hukuk)

Öneri

Yapay zekâ modellerinde şeffaflık sağlamaya yönelik girişimler sistematik olarak öngörü performansını ve kaynak kullanım verimliliğini olumsuz etkileyebilmektedir. Bu bağlamda performansın ve kaynak kullanımının optimize edilmesi için “kara kutu” modellerin açıklanabilirliğini artırmaktansa hiyerarşik bir hukuksal filtreleme sistemi önerilmiştir. Modelin iç yapısına müdahale etmek yerine verebileceği cevapların kapsamın belirlenmesi öngörülmektedir.

Açıklanabilirlik, yapay zekanın ürettiği cevabın gerekçesini temellendirebilme becerisidir.

Literatürde iki temel yaklaşım vardır.

İçkin yorumlanabilir modeller: Karar ağaçları ve lojistik regresyon gibi iç mekanizmaların direkt anlaşılabilir olduğu modellerdir. Yüksek boyutlu verilerde performans kaybına neden olabilmektedir.

Post-hoc açıklama yöntemleri: Geliştirilmiş modelin iç yapısına müdahale etmeksizin matematiksel olarak dışarıdan temsil edilmeye çalışan yöntemler. SHAP ve LIME bu yöntemin önde gelen araçlarıdır. Bu yöntemlerin modelin iç işleyişini değil matematiksel modellemeleri olduğu unutulmamalıdır. Yani bu yöntemlerden elde edilecek sonuçlar olasılıksaldır.

Önerilen yaklaşım: Hiyerarşik Denetim Katmanları

Önerilen modelde “kara kutu” niteliği taşıyan yüksek performanslı yapay zeka sistemleri tarafından türetilmiş çıktılar, kullanıcıya ulaşmadan önce aşağıda belirtilen denetim katmanlarından geçirilmesi gereken bir protokole tabi tutulur.

I. Küresel Etik ve İnsan Hakları Regülasyon Katmanı

Kapsam: Birleşmiş Milletler (BM) İnsan Hakları Evrensel Beyannamesi ve UNESCO AI Etik İlkeleri başta olmak üzere uluslararası normatif çerçeveler.

Fonksiyon: Üretilen çıktıların, temel insan hakları doktrini, ayrımcılıkla mücadele ilkeleri ve evrensel etik standartlara uygunluğunu denetleyerek; sistemin değer temelli bir güvenlik süzgecinden geçirilmesini sağlar.

II. Uluslararası Dijital Güvenlik ve Siber Hukuk Katmanı

Kapsam: Uluslararası siber suç sözleşmeleri, veri iletim protokolleri.

Fonksiyon: Üretilen çıktıların, siber saldırı, zararlı yazılım üretimi veya küresel dijital güvenliği

tehdit edebilecek unsurlar içerip içermediğini kontrol ederek; ilgili riskin oluşmadan önlenmesini sağlar.

III. Ulusal Mevzuat ve Jeopolitik Yasal Yetki Katmanı

Kapsam: Kullanıcının doğrudan etkileşimde bulunduğu coğrafi yetki alanına ilişkin anayasal metinler ile yerel yasal düzenlemeler; Türk Ceza Kanunu ve Hollanda Kamu Sağlığı Yasası gibi spesifik mevzuat örnekleri bu katmanın veri setini oluşturmaktadır.

Fonksiyon: Üretilen sistem çıktılarını ilgili coğrafyanın yasal sınırlarına göre filtreleyerek özelleştirir. Özellikle düşünce ve ifade özgürlüğünün kapsamı veya belirli maddelerin kullanımına dair hukuki rejimin ülkeden ülkeye farklılık gösterdiği durumlarda; sistem, yerel yasalarla çelişen talepler için erişim engeli veya “yanıt kısıtlaması” uyarısı döndürerek yasal güvenliği sağlar.

IV. Sektörel Regülasyon ve Mevzuat Katmanı

Kapsam: İlgili sektöre yön veren düzenleyici otoritelerin yayınladığı yönetmelik ve standartlar.

Fonksiyon: Finansal danışmanlık, tıbbi tanı ve teşhis veya savunma sanayii gibi yüksek riskli alanlarda, üretilen çıktıların sektörel yasal sınırları ihlal etmesini önleyerek uzmanlık alanı dışındaki yetkisiz beyanların engellenmesini sağlar.

V. Kurumsal Strateji ve Fikri Mülkiyet Katmanı

Kapsam: Kurum içi yönetmelikler, gizlilik sözleşmeleri ve fikri mülkiyet haklarını gözeten kurumsal protokoller.

Fonksiyon: Modelin, kuruluşa ait stratejik planları, ticari sırları veya gizli nitelikteki verileri dış ortama sızdırmasını engelleyerek kurumsal veri güvenliğini sağlar.

VI. Sosyokültürel Uyumluluk ve Değerler Katmanı

Kapsam: Bölgesel hassasiyetler, inanç sistemleri ve sosyokültürel normlar.

Fonksiyon: Yasal bir engel bulunmasa dahi, toplumun genel değer yargılarına aykırı veya ofansif algılanabilecek içerikleri filtreler; bu sayede marka itibarının korunmasını ve toplumsal meşruiyetin sürdürülmesini sağlar.

VII. Kullanıcı Yetkilendirme ve Erişim Hiyerarşisi Katmanı

Kapsam: Kullanıcı demografisi, yaş sınırlandırmaları ve kurumsal hiyerarşideki erişim seviyeleri.

Fonksiyon: Sistemin sunduğu bilgi derinliğini kullanıcının yetki profilini baz alarak dinamik olarak yapılandırır; örneğin üst düzey bir yöneticiye sunulan veri kapsamı ile stajyer personel ya da reşit olmayan kullanıcıya sunulan içerik arasındaki erişim sınırlarını belirler.

Yukarıda detaylandırılan katmanlı bir mimarinin sabit bir yapı teşkil etmediği; uygulama alanının gereksinimlerine, operasyonel koşullara ve değişen normatif çevrelere bağlı olarak modüler bir biçimde güncellenebileceği, yeniden yapılandırılabileceği veya genişletilebileceği öngörülmektedir. Bu esneklik, sistemin farklı disiplinlere ve gelişen yasal düzenlemelere dinamik olarak uyum sağlamasına olanak tanır.

Verimlilik ve Doğruluk Analizi

Katmanlı mimarinin “şeffaf model” yaklaşımlarına kıyasla avantajları şunlardır.

Öngörü performansının korunması: Modelin ağırlık parametrelerine müdahale edilmediği için yüksek boyutlu verilerin analizinde oluşabilecek performans kayıplarının önüne geçilir, model en yüksek performansında kalır.

Dinamik adaptasyon: Mevzuat deęişiklikleri ya da yeni yasal düzenlemeler sonrasında modelin en baştan eğitilmesine gerek duyulmaz, sadece sınırları güncellenir. Bu sayede güncellik ve yasaya uygunluk korunmuş olur.

Gelişmiş hata yönetimi ve bilinçli geri bildirim: Sistem sınırlardan geçemeyen cevaplar için tek tip red cevabı yerine ilgili yasanın/mevzuatın kapsamı ile birlikte geri bildirim verilir.

Riskler ve Önlemler

Gecikme: Çok katmanlı denetim mekanizmasının entegre edilmesi cevap yolunun uzaması anlamına gelir. Bu yükün azaltılması ve zaman kaybını aşmak amacıyla GPU veya NPU benzeri paralel işlemcili mimariler üzerinde eş zamanlı taramalar yapılır.

Sonuç: Yüksek Performans, Yüksek Sorumluluk

Yapay zekâ ekosisteminde performans ve etik değerler birbirini dışlayan unsurlar olarak deęil birbirini tamamlayan bir bütün olarak ele alınmalıdır. Önerdiğimiz modelde yapay zekâ modellerinin, performanstan ödün vermeden sorumlulukları yerine getirmek için katmanlı bir denetim mekanizması stratejisi önerilir.

Bu taslaęı teknik ve hukuki boyutlarıyla şu şekilde tanımlayabiliriz:

1. Teknik Tanımlama: "Denetimli Kara Kutu" Modeli

Teknik açıdan bu taslak, en yüksek performansı sunan ancak iç işleyişı şeffaf olmayan "kara kutu" modellerin (derin öğrenme, transformörler vb.) kullanımını tamamen reddetmez. Bunun yerine, bu modellerin çıktılarını bir "post-processing" (işlem sonrası) denetim katmanından geçirir.

Hibrit Denetim Mimarisi: Taslak, yüksek performanslı modeller ile sembolik-mantıksal denetim mekanizmalarını birleştiren bir yapı önerir.

Baęlamsal Performans: Performansın sadece "doęruluk" (accuracy) deęil, aynı zamanda "güvenilirlik" ve "denetlenebilirlik" metrikleriyle ölçüldüğü bir sistem kurgulanmıştır.

Açıklanabilirlik Araçları: Kara kutu modellerin çıktıları, teknik olarak SHAP veya LIME gibi tekniklerle anlamlandırılmalı ve taslaęınızdaki hiyerarşik süzgeçten geçirilmelidir.

2. Hukuki Tanımlama: "Hiyerarşik Normlar Denetimi"

Hukuki açıdan bu taslak, yapay zekâ çıktılarını sadece birer veri sonucu olarak deęil, hukuki birer işlem olarak ele alır ve onları bir "normlar hiyerarşisine" tabi tutar.

Uluslararası Hukuk ve Üst Normlar (Jus Cogens/Erga Omnes): Taslaęımızın en özgün yanı, yapay zekâ çıktısının denetimine en üst hukuk normlarından başlamasıdır. Bu, sistemin temel insan hakları ve evrensel hukuk ilkelerine aykırı bir sonuç üretmesini teknik düzeyde engellemeyi amaçlar.

Avrupa Birlięi Yasası (AI Act) Uyumu: Taslak, yapay zekâ yasası'nın 13. maddesindeki şeffaflık ve 25. maddesindeki deęer zinciri sorumluluęu ile doğrudan örtüşür. Yüksek riskli sistemler için öngörülen "insan gözetimi" ve "yeterli şeffaflık" kriterlerini, önerdiğiniz hiyerarşik denetim mekanizmasıyla somutlaştırır.

Hesap Verebilirlik ve İtiraz Hakkı: Çıktıların yönetmeliklere, sektörel kurallara ve şirket tüzüklerine uygunluk denetimi, GDPR (Madde 22) kapsamındaki "otomatik kararlara itiraz etme" ve "gerekçe isteme" haklarının hukuki altyapısını oluşturur.

Hukuki Testler: Kara kutu kullanımına izin verilmeden önce; zaruriyet, orantılılık, risk azaltma ve şeffaflık testlerinin yapılması gerektiğini savunan bir "uygunluk testi" (compliance test) protokolü sunar.

Bu alıřma, "daha az performanslı ama daha řeffaf" sistemler ile "yksek performanslı ama riskli" sistemler arasındaki sahte ikileminiř yıkarak. Bunun yerine, yksek performansı koruyan ancak hukuki denetim szgeciyle (uluslararası hukuktan řirket tzğne kadar) dizginlenen bir "sorumlu yapay zekâ" modeli tanımlar. Bylelikle bir řirketin kullandığı yapay zeka o řirketin stats kapsamında hareket edecektir bu baėlamda tzk ya da statden doėacak sorumluluklar da bu řirketin sorumluluk alanına girecektir.

8. Çalışma Grubu Raporu-

Dr. Öğr. Üyesi Başak Buluz Kömeçoğlu'nun sorusu: Bir yapay zekâ sisteminin verdiği kararın açıklanabilir olması, hukuki sorumluluğun kime ait olduğunu gerçekten netleştirir mi? Algoritmik karar süreçlerinde geliştirici, sistemi kullanan kurum ve kullanıcı arasında sorumluluk nasıl dağıtılmalıdır? Bu sorumluluk teknik olarak nasıl izlenebilir ve hukuken nasıl kanıtlanabilir?

Katılımcılar:

1. Sudenur ÇAKIR (Bilgisayar Mühendisliği)
2. Kaan GÖKDEMİR (Bilgisayar Mühendisliği)
3. Bedirhan ARI (Bilgisayar Mühendisliği)
4. Oday MOUKKİ (Yazılım Mühendisliği)
5. Yusuf MENGÜTAY (Hukuk)

1. Giriş: Açıklanabilirlik ve İliyet Bağının Kurulması

Mühendislik literatüründeki açıklanabilirlik kavramı, sistemin hangi girdilere (verilere) dayanarak hangi sonucu ürettiğini şeffaflaştırarak, hukuki sorumluluğun ve illiyet bağının tespitinde adeta bir teknik izlenebilirlik ve destekleyici analiz aracı görevi görmektedir. Grup olarak, hukuk ve mühendislik perspektiflerini bir araya getirdiğimizde ilk tespitimiz şu oldu: Yapay zekâ (YZ) sistemlerinin, özellikle derin öğrenme (çok katmanlı öğrenme) algoritmalarının karar alma süreçlerinin "**açıklanabilir**" olması (**ExplainableAI - XAI**), illiyet bağının kurulmasını kolaylaştıran önemli bir araçtır; ancak tek başına yeterli değildir. Çünkü XAI çıktıları yaklaşık (approximate) açıklamalardır, bu sebeple mahkemede kesin nedensellik kanıtı olarak kabul edilmeleri tartışmalıdır. Geleneksel "**kara kutu**" (**blackbox**) (**şeffaf olmayan**) modellerinde algoritmanın o kararı alırken ne düşündüğünün bilinmemesi, hata durumunda kusurun kime atfedileceğini belirsizleştirir. Hukuk sistemimizde birine sorumluluk yükleyebilmek için eylemle zarar arasında bir "**illiyet bağı**" (**nedensellik**) (**neden-sonuç ilişkisi**) kurmamız şarttır.

2. Paydaşlar Arasında Sorumluluk Dağılımı (EU AI Act Perspektifi)

Masadaki tartışmamızda, hukuki sorumluluğun dağılımını Avrupa Birliği Yapay Zekâ Yasası'nın (EU AI Act) aktörleri tanımlayış biçimi üzerinden değerlendirdik. Burada şu ayrımı netleştirmek gerekir: EU AI Act doğrudan sorumluluk hukuku düzenlemez; EU AI Act bir uyum ve yükümlülük çerçevesi sunarken, hukuki sorumluluk ulusal hukuk kurallarına göre belirlenir. Bu bağlamda roller şöyledir:

- **Geliştirici (Provider) (sistem üreticisi):** Algoritmanın tasarımı, eğitim verisinin (öğrenme materyalinin) temizliği ve sistemin şeffaf bir altyapıya sahip olmasından sorumludur. **EU AI Act Madde 12** uyarınca sistemin yaşam döngüsü boyunca kararlarını kaydedecek "**otomatik loglama**" (**kayıt**) (**işlem günlüğü**) mekanizmalarını kurmak ve **Madde 13** gereğince kurumların sistemi nasıl kullanacağına dair şeffaf talimatlar hazırlamak geliştiricinin yasal yükümlülükleri arasındadır.
- **Sistemi Kullanan Kurum (Deployer - Hastane, Banka vb.):** Sistemi kendi amacı doğrultusunda kullanan kurumlar, **EU AI Act Madde 14** kapsamında sistemin denetimini yapacak yetkin bir "**insan gözetimi**" (**humanoversight**) (**uzman kontrolü**) atamak zorundadır. Yapay zekânın ürettiği uyarıları dikkate almamak veya bu insan denetimi mekanizmasını devre dışı bırakmak kurumun sorumluluğunu önemli ölçüde

etkileyebilir.

- **Son Kullanıcı / Etkilenen Kişi:** Yapay zekânın kararına maruz kalan (örneğin kredisi reddedilen veya işe alınmayan) kişidir. **EU AI Act Madde 86 uyarınca**, bu kişilerin kararın nasıl alındığına dair "**açıklama talep etme hakkı**" (**right to an explanation**) bulunmaktadır. Bu hakkın kullanılabilmesi için XAI (Açıklanabilir YZ) teknik bir gereklilik olarak değerlendirilmektedir.

3. Teknik İzlenebilirlik ve Kanıtlama Mekanizmaları

Bir YZ sisteminin aldığı hatalı kararın incelenebilmesi için mühendislerin sunduğu şu teknik altyapılar, mahkemede bilirkişi değerlendirmesine konu olabilecek teknik analiz araçlarıdır:

- **SHAP ve LIME Analizleri (karar açıklayıcılar):** Karar anında YZ'nin hangi girdiye (**feature**) (özellikle/değişkene) ne kadar ağırlık verdiğini matematiksel olarak yorumlayan ve hakimin anlayabileceği insan diline çeviren bu raporlar, mahkemede tek başına kesin delil değil, destekleyici niteliktedir. Buradaki temel sorun şudur: SHAP/LIME model-agnostic approximation dediğimiz yöntemlerdir, yani aynı input (girdi) için farklı çalıştırmalarda farklı sonuçlar verebilir ve manipülasyona açık olabilir.
- **Otomatik Log Kayıtları (işlem günlükleri):** EU AI Act'in de zorunlu kıldığı log kayıtları sayesinde, sistemin aldığı kararlar zaman damgalı (zaman onaylı) ve değiştirilemez şekilde kayıt altına alınarak geriye dönük izlenebilirlik sağlanır.

4. Örnek Olay Analizi: Medikal Tanı Hatası

Hukuki sınırları netleştirmek adına grubumuzla tartıştığımız örnek senaryo şöyledir: Bir hastanede kullanılan yapay zekâ sisteminin radyoloji görüntüsünde bir tümörü atlaması durumunda;

- **Tespit:** XAI araçları (**Isı haritaları/Heatmaps**) (odaklanma analizleri) ile sistemin nereye odaklandığına bakılır.
- **Müşterek Kusur ve Sorumluluk Paylaşımı:** Eğer sistem tümör yerine görüntüdeki alakasız bir cihaz etiketine odaklanmışsa, bu durum kötü bir eğitim verisinden kaynaklanabileceğinden bir geliştirici/üretici kusuruna işaret edebilir.

Diğer yandan, eğer XAI araçları sistemin tümörü doğru tespit ettiğini gösteriyor ancak hastanedeki doktor bu uyarıyı göz ardı edip hastayı eve göndermişse, sorumluluk ağırlıklı olarak kuruma kayabilir. Ancak, gerçek dünya senaryolarında hukuki sorumluluk genellikle ikili (binary) bir ayrım ("**ya geliştirici ya doktor**") üzerinden işlemez. Bu tür vakalarda genellikle taraflar arasında bir "**müşterek kusur (joint liability)**" aranır ve ortaya çıkan hukuki sorumluluk, tarafların "katkı oranına göre sorumluluk paylaşımı" çerçevesinde değerlendirilir.

5. Sonuç ve Hukukî Öneriler

Grubumuzun hukuk ve mühendislik disiplinlerini harmanlayarak ulaştığı sonuca göre; yapay zekâda açıklanabilirlik sorunu sadece teknik bir optimizasyon (iyileştirme) meselesi değil, mahkemelerde "illiyet bağının" (nedensellik) (neden-sonuç ilişkisinin) kurulabilmesi ve adil sorumluluk dağılımı için önemli bir gereklilik olarak değerlendirilmektedir. Bu doğrultuda çözüm önerilerimiz şunlardır:

- **Açıklanabilirlik Paradoksunun (çelişkisinin) Aşılması ve Hibrit Mimari (karma yapı):** Yüksek riskli (işe alım, kredi skorlama vb.) YZ sistemlerinde salt performans odaklanan "kara kutu" (şeffaf olmayan) modelleri yerine, şeffaflığı da barındıran "Hibrit Mimari" tasarımları yasal bir standart hâline getirilmelidir.
- **Sürekli Denetim ve Yapay Zekâ Mimarları (sistem uzmanları):** Sistemi kullanan

kurumlar, yapay zekâyı sadece satın alıp kullanan pasif aktörler olmaktan çıkıp; algoritmaların adil çalışıp çalışmadığını izleyecek "YZ Mimarları" istihdam etmeli ve sistem üzerinde "Sürekli Açıklanabilirlik Denetimi" yapmalıdır.

- **Teknik Analiz ve İzlenebilirlik Standartları:** Karar sonrası çalışan Post-Hoc (karar sonrası) (SHAP/LIME) açıklama araçlarının ürettiği veriler ve EU AI Act Ek-4 (Annex IV) kapsamında geliştiricilerin hazırlamak zorunda olduğu "Teknik Dokümantasyon", olası uyuşmazlıklarda mahkemelerde bilirkişi değerlendirmesine sunulacak son derece önemli ve destekleyici teknik analiz araçlarıdır.
- **Tehlike Sorumluluğuna (kusursuz sorumluluğa) Geçiş:** Türk Borçlar Kanunu (TBK) Madde 49'da yer alan ve insan "kusuru" (kasti/ihmali) arayan klasik sorumluluk anlayışı, kendi kendine öğrenen otonom (**bağımsız**) algoritmalar karşısında yetersiz kalabilmektedir. Bu nedenle YZ faaliyetleri, bizzatı tehlikeli işletme faaliyeti sayılarak **TBK Madde 71 "Tehlike Sorumluluğu"** kapsamında özel bir kusursuz sorumluluk rejimine (düzenine) tabi tutulmalıdır.
- **Sorumluluk ve Zarar Giderme Modelleri:** Elektronik kişilik yaklaşımı literatürde tartışılmış olmakla birlikte, güncel hukuk doktrininde yaygın kabul görmemektedir. Bu nedenle, yapay zekâ kaynaklı zararların çözümünde ürün sorumluluğu, risk temelli sorumluluk ve sigorta temelli modeller gibi alternatif yaklaşımlar daha uygulanabilir seçenekler olarak değerlendirilmektedir. Bu çerçevede, zararların karşılanabilmesi için sigorta temelli yaklaşımlara dayanan, tarafların prim ödediği güvence fonları gibi modeller öne çıkmaktadır.