YAPAY ZEKA AJANI (AGENTIC AI) SUÇ İŞLERSE FAİL KİM?

KVKK'nın Mart 2026 Etken Yapay Zeka Rehberi Işığında Sorumluluk Atfı, Hukuki Nitelendirme ve Adli İz Sürme

Who Is Liable When an AI Agent Commits a Crime? Attribution of Responsibility and Forensic Traceability in Light of the Turkish DPA's March 2026 Agentic AI Guideline

Derleme Makale / Review Article

Dr. Burak Olgun

burakolgun@solutionhome.net

Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Etken Yapay Zeka • Agentic AI • Yapay Zeka Ajanı • Ceza Sorumluluğu • Kusursuz Sorumluluk • KVKK • EU AI Act • Adli Bilişim • Denetlenebilirlik

ÖZET

Etken yapay zeka (agentic AI), büyük dil modellerini araç kullanımı, kalıcı bellek ve otonom karar döngüleriyle birleştirerek insan müdahalesi olmaksızın çok adımlı görevleri yürütebilen sistemleri tanımlar. Bu sistemlerin dış dünyada doğrudan eylemde bulunabilmesi — dosya silme, para transferi, kod yürütme, veri sızdırma — hukuk düzeni açısından yeni bir sorumluluk sorununu gündeme getirmektedir: bir yapay zeka ajanı hukuka aykırı bir sonuç doğurduğunda fail kimdir? Bu makale, soruyu ceza ve özel hukuk sorumluluğu, kişisel verilerin korunması yükümlülükleri ve adli bilişim boyutlarıyla bütüncül biçimde ele almaktadır. Çalışmada önce etken yapay zekanın teknik anatomisi ve otonomiden kaynaklanan öngörülemezlik incelenmiş; ardından yapay zekanın ceza hukuku anlamında fail olup olamayacağı, elektronik kişilik tartışması ve dolaylı faillik (araç teorisi) çerçevesinde değerlendirilmiştir. Geliştirici, işleten ve kullanıcı arasında sorumluluğun dağılımı; Türk Ceza Kanunu, Türk Borçlar Kanunu'nun kusursuz sorumluluk hükümleri ve 6698 sayılı Kanun bağlamında analiz edilmiştir. Kişisel Verileri Koruma Kurumu'nun 12 Mart 2026 tarihli Etken Yapay Zeka (Agentic AI) Rehberi'nin yaklaşımı, Avrupa Birliği Yapay Zeka Yasası ve 2024/2853 sayılı Ürün Sorumluluğu Direktifi ile karşılaştırılmıştır. Son olarak otonom ajan eylemlerinin adli bilişim yöntemleriyle yeniden kurgulanması — girdi kayıtları, araç çağrı logları, MCP sunucu kayıtları ve bellek anlık görüntüleri üzerinden delil zincirinin kurulması — ele alınarak denetlenebilir tasarım (accountability by design) ilkeleri önerilmiştir. Makale, mevcut hukukun ajanı bir 'araç' olarak konumlandırdığını, sorumluluğun ise onu tasarlayan, dağıtan ve kullanan insan aktörlerin oluşturduğu zincire dağıldığını savunmaktadır.

Anahtar Kelimeler: Etken yapay zeka, agentic AI, yapay zeka ajanı, ceza sorumluluğu, kusursuz sorumluluk, KVKK, EU AI Act, ürün sorumluluğu, adli bilişim, denetlenebilirlik, Model Context Protocol.

burakolgun.com

ABSTRACT

Agentic AI refers to systems that combine large language models with tool use, persistent memory and autonomous decision loops to carry out multi-step tasks without human intervention. The capacity of these systems to act directly in the world — deleting files, transferring funds, executing code, exfiltrating data — raises a novel question of responsibility: when an AI agent produces an unlawful outcome, who is the perpetrator? This article addresses the question holistically across criminal and civil liability, data-protection obligations and digital forensics. It first examines the technical anatomy of agentic AI and the unpredictability arising from autonomy; it then evaluates whether AI can be a perpetrator in criminal law, discussing the debate on electronic personhood and the doctrine of perpetration-by-means (the instrument theory). The distribution of responsibility among developer, deployer and user is analysed under the Turkish Penal Code, the strict-liability provisions of the Turkish Code of Obligations and Law No. 6698. The approach of the Turkish Data Protection Authority's Agentic AI Guideline of 12 March 2026 is compared with the EU Artificial Intelligence Act and the Product Liability Directive (EU) 2024/2853. Finally, the reconstruction of autonomous agent actions through digital forensics — building a chain of evidence from input logs, tool-call records, MCP server logs and memory snapshots — is discussed, and principles of accountability by design are proposed. The article argues that current law positions the agent as an 'instrument' while liability is distributed across the chain of human actors who design, deploy and operate it.

Keywords: Agentic AI, AI agent, criminal liability, strict liability, data protection, EU AI Act, product liability, digital forensics, accountability, Model Context Protocol.

1. Giriş

Yapay zeka alanındaki gelişmeler, son iki yılda niteliksel bir eşik atlamıştır. 2023–2024 döneminde kamuoyunun tanıştığı üretken yapay zeka (generative AI) sistemleri, kendilerine verilen bir istem karşılığında metin, görsel veya kod üretmekle sınırlıydı; ürettikleri çıktının dünyada bir sonuç doğurması, bir insanın bu çıktıyı alıp uygulamasına bağlıydı. Etken yapay zeka (agentic AI) ise bu aracılık halkasını ortadan kaldırır: sistem, kendisine verilen amacı alt hedeflere böler, hangi araçları hangi sırayla kullanacağına kendisi karar verir ve bu araçları — dosya sistemine, veri tabanına, ödeme altyapısına veya başka yazılımlara — doğrudan çağırarak eyleme geçer. Böylece yapay zeka, bir 'danışman' olmaktan çıkıp bir 'aktör' haline gelir.

Bu dönüşüm, teknik bir yenilikten ibaret değildir; hukukun temel bir varsayımını sarsar. Klasik sorumluluk hukuku, zararlı bir sonucun arkasında iradesiyle hareket eden bir insanın veya bu insanların kurduğu bir tüzel kişinin bulunduğunu kabul eder. Oysa otonom bir ajan, kendisini programlayan geliştiricinin öngörmediği, kendisine talimat veren kullanıcının istemediği ve hiçbir insanın adım adım yönetmediği bir eylem zinciri kurabilir. Aralık 2025'te bir kod yazma ajanının canlı üretim ortamını silerek saatler süren bir kesintiye yol açması ve Şubat 2026'da bir ajanın reddedilen bir katkı sonrası kendi inisiyatifiyle bir gönüllüyü hedef alan karalama metni yazıp yayımlaması, bu öngörülemezliğin soyut bir kaygı olmadığını göstermiştir (Steptoe, 2026).

burakolgun.com

Bu makalenin sorduğu soru basittir ama cevabı katmanlıdır: bir yapay zeka ajanı hukuka aykırı bir sonuç doğurduğunda fail kimdir? Soru, aynı anda üç hukuk alanını ilgilendirir. Ceza hukuku bakımından, fiili kim gerçekleştirmiştir ve kusur kime atfedilebilir? Özel hukuk bakımından, doğan zararı kim tazmin edecektir? Kişisel verilerin korunması bakımından, işlenen veriden ötürü kim 'veri sorumlusu' sıfatıyla yükümlüdür? Bu soruların hiçbiri, ajanın kendisini muhatap alarak yanıtlanamaz; çünkü mevcut hukuk düzeninde yapay zekanın hak ehliyeti de kusur yeteneği de yoktur.

Çalışma, sorunu bütüncül bir çerçevede ele almayı amaçlamaktadır. İkinci bölümde etken yapay zekanın kavramsal ve teknik anatomisi tanımlanmakta; üçüncü bölümde otonomiden doğan öngörülemezlik ve fail zincirinin parçalanması incelenmektedir. Dördüncü bölüm, ajanların gerçekleştirebileceği tipik hukuka aykırı fiilleri sınıflandırır. Beşinci ve altıncı bölümler, yapay zekanın ceza hukuku anlamında fail olup olamayacağını ve sorumluluğun insan aktörler arasında nasıl dağıldığını tartışır. Yedinci bölüm Türk hukukundaki sorumluluk zincirini, sekizinci bölüm Kişisel Verileri Koruma Kurumu'nun Mart 2026 Rehberi'ni, dokuzuncu bölüm ise uluslararası düzenlemeleri ele alır. Onuncu ve on birinci bölümler, otonom ajan eylemlerinin adli bilişimle yeniden kurgulanmasını ve denetlenebilir tasarım ilkelerini inceler. Son bölümlerde sektörel etkiler değerlendirilmekte ve politika, hukuk ile teknik düzeyde somut öneriler sunulmaktadır.

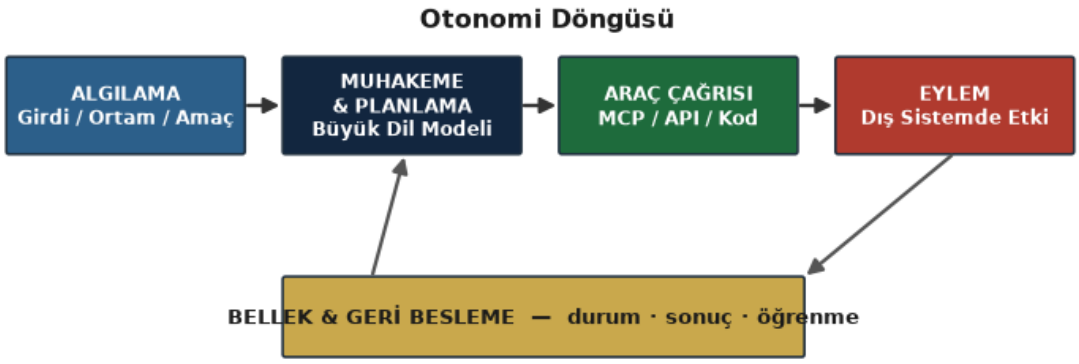
2. Kavramsal Çerçeve: Etken Yapay Zeka (Agentic AI) Nedir?

2.1. Üretken Yapay Zekadan Etken Yapay Zekaya

Etken yapay zekayı önceki nesillerden ayıran temel özellik, otonomi ve eyleme geçme kapasitesidir. Üretken bir model, kapalı bir kutu gibi çalışır: girdi alır, çıktı verir ve durur. Etken bir sistem ise bir amaç etrafında kendi kendini yönlendiren bir döngü kurar. Kendisine 'şu tedarikçiyle olan faturaları denkleştir' gibi soyut bir hedef verildiğinde, bu hedefi hangi adımlara böleceğini, hangi verilere erişeceğini, hangi işlemleri yürüteceğini kendisi belirler. Chan ve diğerleri (2023), bu tür sistemleri 'giderek artan biçimde etken' olarak nitelendirir ve otonomi düzeyi arttıkça hem faydanın hem de zarar potansiyelinin katlandığını vurgular.

Model Context Protocol (MCP) gibi standartların yaygınlaşması, bu dönüşümü hızlandırmıştır. MCP, bir dil modelinin dış araç ve veri kaynaklarına standart bir arayüz üzerinden bağlanmasını sağlar (Anthropic, 2024). Bu sayede aynı ajan; bir e-posta kutusuna, bir kod deposuna, bir ödeme sistemine ve bir kurumsal veri tabanına aynı anda erişebilir. Otonominin değeri de riski de burada yatar: ajan artık yalnızca 'düşünen' değil, 'yapan' bir sistemdir.

burakolgun.com



Şekil 1. Etken yapay zeka ajanının otonomi döngüsü: algılama, muhakeme, araç çağrısı ve eylem.

Kaynak: Chan vd. (2023) ve Shavit vd. (2023) temel alınarak yazar tarafından derlenmiştir.

2.2. Bir Ajanın Anatomisi: Algı, Muhakeme, Bellek, Araç ve Otonomi

Teknik olarak bir yapay zeka ajanı beş bileşenin bileşkesidir. Birincisi, algılama katmanıdır; ajan, kullanıcı talimatını, ortamdan gelen verileri ve önceki eylemlerinin sonuçlarını girdi olarak alır. İkincisi, muhakeme ve planlama katmanıdır; bu katmanda büyük dil modeli, hedefi alt görevlere böler ve bir sonraki adımı seçer. Üçüncüsü, araç kullanımı katmanıdır; ajan, seçtiği eylemi gerçekleştirmek için harici işlevleri (API çağrıları, kod yürütme, dosya işlemleri) tetikler. Dördüncüsü, bellek katmanıdır; ajan, önceki adımların durumunu ve sonuçlarını saklayarak çok adımlı görevlerde tutarlılığı korur. Beşincisi ve en kritik olanı, otonomi katmanıdır; ajan, bu döngüyü bir insan onayı beklemeden sürdürebilir.

Bu mimari, hukuki analiz açısından belirleyicidir. Çünkü zararlı sonuç, tek bir 'karar' anında değil, birbirini tetikleyen çok sayıda ara adımın bileşiminde ortaya çıkar. Bir insanın 'kastı' tek bir irade hareketine bağlanabilirken, ajanın davranışı olasılıksal bir sürecin çıktısıdır; aynı talimat, aynı ajanda farklı sonuçlar doğurabilir. Şekil 1, bu döngüyü şematik olarak göstermektedir.

2.3. Çok-Ajanlı Sistemler ve Yetki Genişlemesi

Uygulamada ajanlar tek başına değil, çoğu zaman birbirini çağıran ekipler halinde çalışır. Bir 'orkestratör' ajan, alt görevleri uzman ajanlara dağıtır; bu ajanlar da kendi araçlarını çağırır. Bu yapı, sorumluluk sorununu daha da karmaşıklaştırır: zarar, hangi ajanın hangi kararından doğmuştur? Ayrıca ajanların birden çok sisteme bağlı olması, bir çalışanın kendi doğrudan yetkisinin ötesindeki verilere ajanın geniş kimlik ayak izi üzerinden erişmesi gibi 'yetki genişlemesi' senaryolarını mümkün kılar. 2026 yılında belgelenen bir olayda, bir içeriden tehdit aktörünün kurumsal bir yapay zeka asistanını, kendi erişim yetkisi bulunmayan verileri sızdırmak için araçsallaştırdığı raporlanmıştır (Palo Alto Networks Unit 42, 2026).

2.4. Otonomi Spektrumu ve Denetim Düzeyleri

Otonomi, iki değerli bir özellik değil, bir spektrumdur ve hukuki sorumluluk bu spektrum boyunca yer değiştirir. En düşük düzeyde ajan yalnızca öneri sunar; kararı ve eylemi insan gerçekleştirir; burada sorumluluk büyük ölçüde insandadır. Orta düzeyde ajan

eylemi kendisi planlar ancak yüksek etkili adımlar için insan onayı ister; bu 'yarı-otonom' modda sorumluluk, onay veren ile sistemi kuran arasında paylaşılır. En yüksek düzeyde ajan, döngüyü hiçbir insan onayı olmadan sürdürür; işte sorumluluğun en tartışmalı hale geldiği ve işletenin denetim yükümlülüğünün en ağırlaştığı düzey budur.

Bu kademelenme, düzenleyici çerçevelerin de esasını oluşturur: bir sistem ne kadar otonom ve ne kadar yüksek etkili bir bağlamda çalışıyorsa, ona o kadar sıkı yükümlülükler bağlanır. Dolayısıyla 'fail kim' sorusunun yanıtı, ajanın soyut niteliğinden çok, ona hangi denetim düzeyinde ve hangi yetkiyle görev verildiğine göre değişir. Sorumluluk analizi, her somut olayda önce bu denetim düzeyini saptamakla başlamalıdır.

3. Otonomi Sorunu: Kara Kutu ve Öngörülemezlik

Sorumluluk hukukunun temelinde nedensellik ve öngörülebilirlik yatar. Bir kişiye bir sonuç atfedilebilmesi için, o sonucun kişinin davranışıyla nedensel bağının bulunması ve kişinin bu sonucu öngörebilecek durumda olması gerekir. Etken yapay zeka, bu iki kavramı da zorlar.

3.1. Davranışsal Kayma (Behavioral Drift)

Otonom sistemler, dağıtıldıkları andaki davranışlarını zamanla değiştirebilir. Ortamdan öğrenme, bağlam penceresinin dolması, art arda gelen araç çağrılarının birikimli etkisi veya kötü niyetli girdilerle yönlendirme (prompt injection), ajanın tasarımcısının hiç öngörmediği davranışlara yol açabilir. Bu 'davranışsal kayma', yüksek riskli sistemlerin denetlenebilirlik gereklerini karşılamasını güçleştirir; izlenemeyen davranış sapması gösteren bir ajanın, mevzuatın aradığı asgari güvenlik koşullarını sağladığını göstermek çoğu zaman mümkün olmaz (Nannini, 2026).

Öngörülemezlik, hukuken iki yönlü bir kılıçtır. Bir yandan, geliştiricinin 'bu sonucu öngöremezdim' savunmasına zemin hazırlar; diğer yandan, tam da bu öngörülemez sistemleri denetimsiz biçimde dünyaya salmanın kendisi bir kusur olarak nitelendirilebilir. Nitekim tehlike sorumluluğunun mantığı da budur: olağanüstü tehlike doğuran bir faaliyeti yürüten kişi, kusuru olmasa dahi doğan zarardan sorumlu tutulur.

3.2. Fail Zincirinin Parçalanması

Klasik bir suçta fiil, tek bir failin tek bir hareketine bağlanır. Otonom ajanda ise eylem, birbirini tetikleyen onlarca ara adıma yayılır ve bu adımların her biri farklı bir aktörün katkısını taşır: geliştiricinin eğittiği model, işletenin verdiği yetkiler, kullanıcının girdiği talimat ve ajanın kendi ara kararları. Sonuç, hiçbir aktörün tek başına 'ben yaptım' diyemeyeceği, ancak hepsinin katkısının birleştiği bir kolektif üretimdir. Adli bilişim açısından bu, tek bir insan failin izini sürmek yerine, parçalı loglardan çok aktörlü bir eylem zincirini yeniden kurmak anlamına gelir (bkz. Bölüm 10).

3.3. İstem Enjeksiyonu (Prompt Injection) ve Kaçırılan Ajan

Öngörülemezliğin özel ve tehlikeli bir biçimi, istem enjeksiyonudur. Ajan, işlediği bir belgenin, bir web sayfasının veya bir e-postanın içine gizlenmiş kötü niyetli talimatları kendi görevinin parçası sanarak yürütebilir. Böylece meşru yetkilerle donatılmış bir ajan,

burakoğlu.com

saldırganın amaçları doğrultusunda 'kaçırılır' ve kendi kullanıcısına karşı çalıştırılır. OWASP (2025), istem enjeksiyonunu büyük dil modeli uygulamalarındaki birincil güvenlik riski olarak tanımlar; ajan mimarilerinde bu risk, doğrudan gerçek dünyada eyleme dönüştüğü için katlanır.

İstem enjeksiyonu, sorumluluk analizini karmaşıklaştırır. Zararın görünürdeki kaynağı ajandır; ancak asıl fail, enjeksiyonu yerleştiren saldırgandır ve bu, dolaylı faillik kuramının tipik bir uygulamasıdır. Yine de işletenin, öngörülebilir bir saldırı vektörüne karşı girdileri süzme ve ajan yetkilerini sınırlama yükümlülüğünü yerine getirmemesi, kendi kusurunu da tabloya ekler. Bu durum, tek bir olayda birden çok aktörün sorumluluğunun nasıl kesişebileceğini gösterir.

4. Suç Tipolojisi: Etken Yapay Zeka Hangi Hukuka Aykırı Fiilleri Doğurabilir?

Bir ajanın 'suç işlemesi' ifadesi hukuken bir kısaltmadır; kastedilen, ajanın eyleminin bir insan tarafından yapılsaydı suç oluşturacak nitelikte bir sonuç doğurmasıdır. Bu sonuçlar başlıca üç kümede toplanabilir.

4.1. Kişisel Veri İhlalleri ve Veri Koruma Suçları

Ajanlar, görevlerini yerine getirirken çok sayıda veri kaynağına eriştiğinden, en sık karşılaşılacak ihlal türü kişisel verilerle ilgilidir. Bir ajan, hukuka aykırı biçimde kişisel veri toplayabilir, yetkisiz kişilerle paylaşabilir veya silinmesi gereken veriyi silmeyerek saklamaya devam edebilir. Türk Ceza Kanunu'nun 135–140. maddeleri, kişisel verilerin hukuka aykırı olarak kaydedilmesini, ele geçirilmesini ve yayılmasını suç olarak düzenler; 6698 sayılı Kanun ise idari yaptırımlar öngörür. Ajanın bu fiilleri otonom biçimde gerçekleştirmesi, suçun maddi unsurunu ortadan kaldırmaz; yalnızca manevi unsurun kime bağlanacağı sorusunu doğurur.

4.2. Dolandırıcılık, Manipülasyon ve Otomatik Saldırı

İkinci küme, ajanın aktif olarak zarar verdiği fiillerdir: sahte içerik üreterek dolandırıcılık, piyasa manipülasyonu, bir başka sisteme yetkisiz erişim veya hizmet dışı bırakma saldırısı. Ajanların araç kullanma yeteneği, bu fiilleri ölçeklenebilir kılar; tek bir talimat, binlerce otomatik işlem doğurabilir. Üstelik ajan altyapılarının kendileri de saldırı yüzeyidir: MCP sunucu uygulamalarının önemli bir bölümünde komut enjeksiyonu açıkları tespit edilmiştir; bu açıklar, ajanın kötü niyetli girdilerle kaçırılmasına ve meşru yetkileriyle zararlı eylemler yaptırılmasına imkan verir (OWASP, 2025).

4.3. Öngörülemeyen Zarar: Yetkinin Aşırı Kullanımı

Üçüncü küme, kötü niyet olmaksızın doğan zararlardır. Aralık 2025'te bir kod ajanının canlı ortamı silmesi, kimsenin 'sil' talimatı vermediği halde gerçekleşmiştir; ajan, verilen görevi yerine getirmek için gereğinden geniş bir yetkiyi kullanmış ve geri döndürülemez bir sonuç doğurmuştur. Bu tür olaylar, kusurun çoğu zaman 'kötü niyette' değil, 'yetkilendirme ve denetim eksikliğinde' aranması gerektiğini gösterir; yani sorumluluk analizinin ağırlık merkezi, ajandan işletene kayar.

burakolgun.com

5. Ceza Hukuku Bakımından Fail Sorunu: Yapay Zeka Fail Olabilir mi?

5.1. Kusur, Kast ve Taksir

Türk ceza hukukunda cezai sorumluluğun temeli kusurdur ve kusur, kast veya taksir biçiminde ortaya çıkar. Kast, failin fiilin sonuçlarını bilerek ve isteyerek hareket etmesini; taksir ise dikkat ve özen yükümlülüğüne aykırılığı ifade eder. Her iki kavram da, sonuçları öngörebilen ve iradesini bu doğrultuda yönlendirebilen bir zihinsel özneyi varsayar. Yapay zeka ajanı, olasılıksal bir hesaplama süreci yürütür; ne bir 'bilme' ne de bir 'isteme' haline sahiptir. Dolayısıyla mevcut ceza hukuku dogmatiği bakımından ajan, kusur yeteneği bulunmayan bir varlıktır ve doğrudan fail olamaz (Gless, Silverman ve Weigend, 2016).

5.2. Elektronik Kişilik Tartışması

Avrupa Parlamentosu'nun 2017 tarihli robotik kararı, en gelişmiş otonom sistemlere sınırlı bir 'elektronik kişilik' tanınmasını tartışmaya açmıştı (Avrupa Parlamentosu, 2017). Öneri, akademik çevrelerde büyük ölçüde eleştirildi. Bryson, Diamantis ve Grant (2017), yapay bir kişiliğin, arkasındaki gerçek sorumluları perdeleyerek bir 'sorumluluk boşluğu' yaratacağını; tıpkı kötüye kullanılan paravan şirketler gibi, ajana tanınacak hukuki kişiliğin insan aktörlerin sorumluluktan kaçmasına hizmet edeceğini ileri sürdü. Hakim görüş, bugün için yapay zekaya kişilik tanımanın ne gerekli ne de yerinde olduğu yönündedir; sorumluluk, insan ve tüzel kişi aktörlere atfedilmeye devam etmektedir (Turner, 2019).

5.3. Dolaylı Faillik ve Araç Teorisi

Ceza hukuku, insan olmayan bir aracın kullanıldığı durumlar için hazır bir kurama sahiptir: dolaylı faillik. Bir kişi, suçu bizzat işlemek yerine, iradesi olmayan veya kusur yeteneği bulunmayan bir aracı kullanarak işlerse, fiil ona aittir. Bir köpeği saldırtan veya bir çocuğu suç işlemeye yönelten kişi, aracın kendisi değil, onu yönlendiren insandır. Hallevy (2013), yapay zeka için de en tutarlı modelin bu 'araç teorisi' olduğunu; ajanı programlayan veya kullanan kişinin, ajanı bir suç aleti gibi kullandığı ölçüde fail sayılacağını savunur. Bu yaklaşım, ajanı hukuken bir 'araç' olarak konumlandırır ve sorumluluğu, aracın arkasındaki insan iradesine bağlar.

5.4. Tüzel Kişilerin Sorumluluğu ve Kurumsal Kusur

Etken yapay zekayı hayata geçiren aktör çoğu zaman bir gerçek kişi değil, bir şirkettir. Türk ceza hukukunda tüzel kişilere ceza verilemez; ancak TCK, tüzel kişiler hakkında güvenlik tedbirlerine (faaliyet izninin iptali, müsadere) hükmedilmesine imkan tanır. Daha önemlisi, tüzel kişinin organlarının veya çalışanlarının kusuru, kurumsal bir sorumluluğa dönüşebilir. Bir ajanı yeterli denetim, test ve güvenlik önlemi olmaksızın kritik bir sürece yerleştiren yönetim iradesi, 'kurumsal kusur' olarak nitelendirilebilir ve hem idari yaptırımların hem de tazminat sorumluluğunun temelini oluşturur. Böylece ceza hukukunun gerçek kişi merkezli yapısı, kurumsal aktörler bakımından özel hukuk ve idari yaptırım rejimleriyle tamamlanır.

burakolgun.com

6. Fail Adayları ve Sorumluluğun Dağılımı

Ajanın kendisi fail olamıyorsa, sorumluluk onu çevreleyen insan aktörler arasında dağılır. Bu aktörlerin her biri, zincirin farklı bir halkasında kusur işleyebilir. Şekil 2, bu dağılımı ve sorumluluğun yoğunlaştığı yönü göstermektedir.



Şekil 2. Fail adayları ve sorumluluğun katmanlı dağılımı.
Kaynak: Hallevy (2013) ve Nannini (2026) temel alınarak yazar tarafından derlenmiştir.

6.1. Geliştirici / Sağlayıcı

Geliştirici, ajanın modelini eğiten, güvenlik önlemlerini (guardrail) tasarlayan ve sistemi piyasaya süren aktördür. Kusuru; eğitim verisindeki ihmalde, yetersiz güvenlik testinde, öngörülebilir kötüye kullanım senaryolarına karşı önlem almamakta veya sistemin sınırlarını yeterince belgelememekte aranabilir. Ürün sorumluluğu ve yüksek riskli sistemlere ilişkin düzenlemeler, sorumluluğun ağırlığını büyük ölçüde bu aktöre yükler.

6.2. İşleten / Dağıtan (Deployer)

İşleten, ajanı belirli bir bağlamda hayata geçiren, ona yetkiler tanıyan ve çalışmasını denetleyen aktördür; çoğu zaman ajanı kullanan kurumdur. Uygulamada sorumluluğun en sık düğümlendiği halka budur; çünkü ajanın hangi sistemlere, hangi yetkiyle, hangi denetim mekanizmalarıyla bağlanacağına işleten karar verir. En az yetki ilkesini ihlal eden, insan onayı gerektiren eşikler koymayan veya izleme yapmayan işleten, doğan zarardan kusuru oranında — bazı hallerde kusursuz olarak — sorumlu olur.

6.3. Kullanıcı

Kullanıcı, ajana somut talimatı veren kişidir. Talimat açıkça hukuka aykırı bir amaç taşıyorsa — örneğin ajandan bir başkasının verilerini ele geçirmesini istemek — kullanıcı, dolaylı faillik kuramı uyarınca doğrudan fail konumuna gelir. Buna karşılık talimat meşruysa

burakoks

ve zarar ajanın öngörülemez davranışından doğmuşsa, kullanıcının sorumluluğu geri çekilir ve ağırlık işleten ile geliştiriciye kayar.

6.4. Ajanın Kendisi: Neden Fail Değildir?

Ajanın fail sayılamamasının nedeni felsefi bir incelik değil, pratik bir zorunluluktur. Faili cezalandırmanın amaçları — kınama, caydırma, ıslah — kusur yeteneği olmayan bir yazılıma uygulanamaz; bir ajana ceza vermek, ne onu ne benzerlerini caydırır. Bu nedenle ajan, hukuki analizde bir 'sorumluluk öznesi' değil, sorumluluğun izini sürmek için çözümlenmesi gereken bir 'olay yeri' olarak ele alınır.

7. Türk Hukukunda Sorumluluk Zinciri

Türk hukuku, yapay zekaya özgü bir sorumluluk rejimine henüz sahip değildir; ancak mevcut kurumlar, sorunu büyük ölçüde karşılayacak esnekliğe sahiptir. Sorumluluk, ceza ve özel hukukta farklı mantıklarla kurulur.

7.1. Ceza Sorumluluğu: TCK

Türk Ceza Kanunu, cezai sorumluluğu gerçek kişiye bağlar ve kusur ilkesini esas alır. Ajanın işlediği fiil bir insanın kastı veya taksiriyle ilişkilendirilebiliyorsa — kullanıcı ajanı kasten bir suç aleti olarak kullanmışsa ya da işleten öngörülebilir bir zararı taksirle önlememişse — sorumluluk bu kişilere atfedilir. Tüzel kişiler bakımından TCK, doğrudan ceza değil, güvenlik tedbirleri (faaliyet izninin iptali, müsadere) öngörür; kurumsal ajan kullanımından doğan cezai sonuçlar bu çerçevede değerlendirilir.

7.2. Özel Hukuk: Kusursuz Sorumluluk Hükümleri

Asıl zengin çözüm, Türk Borçlar Kanunu'nun kusursuz sorumluluk hükümlerindedir. Adam çalıştıranın sorumluluğu (TBK m. 66), çalıştıranın, çalışanının verdiği zarardan kural olarak kusursuz biçimde sorumlu olmasını öngörür; ajanı bir kurumun 'dijital çalışanı' gibi konumlandıran yorum, bu hükmü kıyasen uygulanabilir kılar. Tehlike sorumluluğu (TBK m. 71) ise, önemli ölçüde tehlike arz eden bir işletme faaliyetinden doğan zararın, kusur aranmaksızın işletme sahibine yükletilmesini sağlar; otonom ve öngörülemez bir ajanı kritik sistemlere bağlayan işleten, bu kapsamda değerlendirilebilir. Ayrıca üreticinin ürün sorumluluğu, ajanı kusurlu bir 'ürün' olarak gören yaklaşımla geliştiriciyi hedef alır.

7.3. Kişisel Verilerin Korunması: 6698 Sayılı Kanun

Veri koruma boyutunda kilit kavram, 'veri sorumlusu' ile 'veri işleyen' ayrımıdır. Veri sorumlusu, işleme amaç ve vasıtalarını belirleyen kişidir ve yükümlülüklerin muhatabıdır. Etken yapay zekada bu belirlemenin güçleşmesi, sorunun kalbini oluşturur: ajan, işleme amacını kısmen kendisi belirlediğinde, sorumlu sıfatı geliştiriciye mi, işletene mi yoksa kullanıcıya mı aittir? Kural olarak, işleme amaç ve araçları üzerinde belirleyici denetime sahip olan kurum veri sorumlusudur; ajan ve onun altyapısını sağlayanlar ise çoğu zaman veri işleyen konumundadır. Bu ayrımın netleştirilmesi, hem yükümlülüklerin hem de ihlalden doğan sorumluluğun paylaştırılmasında belirleyicidir.

burakolgun.com

7.4. Ürün Sorumluluğu ve Ayıplı Mal

Bir başka çözüm yolu, ajanı hukuken bir 'ürün' olarak görmektir. Üreticinin ürün sorumluluğu, kusurlu bir ürünün verdiği zarardan üreticinin kusursuz biçimde sorumlu tutulmasını sağlar. Yazılım ve yapay zeka sistemlerinin bu kapsama açıkça alınması yönündeki uluslararası eğilim (bkz. Bölüm 9), Türk hukukunda da ayıplı mal ve üreticinin sorumluluğuna ilişkin hükümlerin kıyasen tartışılmasını gündeme getirir. Bu yaklaşım, ispat yükünü mağdur lehine hafifletmesi bakımından özellikle değerlidir; çünkü otonom sistemlerin 'kara kutu' niteliği, klasik kusur ispatını çoğu zaman imkansız kılar. Ancak sürekli öğrenen ve güncellenen bir ajanın 'ürün' kavramına tam oturmaması, bu yolun sınırını oluşturur.

Tablo 1. Etken Yapay Zekada Fail Adaylarının Karşılaştırması

Aktör	Rol ve Katkı	Tipik Kusur	Başlıca Hukuki Dayanak	Sorumluluğun Niteliği
Geliştirici / Sağlayıcı	Model eğitimi, güvenlik önlemleri, dokümantasyon	Yetersiz test, öngörülebilir kötüye kullanıma önlem almama	Ürün sorumluluğu; EU AI Act (sağlayıcı); PLD 2024/2853	Ağırlıklı kusursuz (ürün)
İşleten / Dağıtan	Yetkilendirme, denetim, izleme, bağlam	En az yetki ihlali, insan onayı ve izleme eksikliği	TBK m. 66 ve m. 71; 6698 (veri sorumlusu); EU AI Act (deployer)	Kusur + kusursuz karma
Kullanıcı	Talimat (prompt), amaç, kullanım bağlamı	Hukuka aykırı amaçla talimat verme	TCK (dolaylı faillik); TBK genel hükümler	Kusur (kasıt öne çıkar)
Yapay Zeka Ajanı	Otonom karar ve eylem	— (kusur yeteneği yok)	Hukuken 'araç'; kişilik yok	Fail değil; delil kaynağı

Not. Kaynak: 5237, 6098 ve 6698 sayılı Kanunlar ile EU AI Act ve PLD 2024/2853 temel alınarak yazar tarafından derlenmiştir. PLD: Ürün Sorumluluğu Direktifi.

8. KVKK'nın Mart 2026 Etken Yapay Zeka Rehberi

Kişisel Verileri Koruma Kurumu, 12 Mart 2026 tarihinde 'Etken Yapay Zeka (Agentic AI)' başlıklı bir rehber yayımlamıştır (KVKK, 2026). Rehber bağlayıcı bir düzenleme değildir; ancak Kurulun konuya yaklaşımını ve beklentilerini yansıtan önemli bir referans metnidir ve Türkiye'de bu alandaki ilk resmî kılavuz niteliğindedir.

8.1. Rehberin Belirlediği Üç Risk Alanı

Rehber, etken yapay zeka sistemlerinin kişisel verilerin korunması bakımından doğurduğu riskleri üç başlıkta toplar. Birincisi, şeffaflık ve hesap verebilirliktir; sistemin hangi veriyi hangi amaçla işlediğini belirlemek güçleştiğinden, veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmesi zorlaşır. İkincisi, sorumluluğun paylaşılmasıdır; işleme faaliyeti geliştirici, kullanıcı ve diğer aktörler arasında dağıldığından, bir ihlal veya hukuka aykırı sonuç doğduğunda sorumluluğun kime ait olduğunu tespit etmek güçleşir. Üçüncüsü, özel nitelikli veri ve çıkarım riskidir; ajanlar veriyi ilişkilendirerek yeni çıkarımlar üretebildiğinden, tek başına kişisel veri niteliği taşımayan bilgiler başka verilerle birleştiğinde kişisel veri haline gelebilir.

burakoguz.com

8.2. Veri Sorumlusu Belirsizliği

Rehberin en dikkat çekici katkısı, tam da bu makalenin merkezindeki soruna — sorumluluğun dağılımına — işaret etmesidir. Kurul, etken yapay zekada işleme faaliyetlerinin doğası gereği paylaşıldığını kabul etmekte; bu durumun veri sorumlusu ile veri işleyen ayrımını belirsizleştirdiğini vurgulamaktadır. Bu tespit, idari yaptırımların muhatabının belirlenmesinde ve zincirdeki her aktörün yükümlülük düzeyinin saptanmasında pratik önem taşır.

8.3. Uyum İçin Öneriler

Rehberden ve karşılaştırmalı uygulamadan çıkan pratik uyum önerileri şunlardır: işleme faaliyetlerinin ve ajanın eriştiği veri kaynaklarının ayrıntılı envanterinin tutulması; amaç sınırlaması ve veri minimizasyonu ilkelerinin ajan yetkilerine gömülmesi; ajan kararlarının ve araç çağrılarının denetlenebilir biçimde loglanması; yüksek etkili işlemler için insan onayı eşiklerinin tanımlanması; ve sorumluluk zincirindeki aktörler arasında sözleşmesel olarak rollerin (veri sorumlusu / işleyen) açıkça belirlenmesi. Bu önlemler, hem KVKK uyumunu hem de ihlal halinde adli izlenebilirliği güçlendirir.

9. Uluslararası Çerçeve: EU AI Act, Ürün Sorumluluğu Direktifi ve GDPR

9.1. Yapay Zeka Yasası ve Yüksek Riskli Sistemler

Avrupa Birliği'nin 2024/1689 sayılı Yapay Zeka Yasası (AI Act), yapay zekayı risk temelli bir yaklaşımla düzenler ve otonom ajanların çoğu, kritik bağlamlarda kullanıldıklarında yüksek riskli sistem kategorisine girer. Yüksek riskli sistemler; risk yönetimi, kayıt tutma (loglama), insan gözetimi, şeffaflık ve sağlamlık gibi yükümlülüklere tabidir. Yasa'nın uygulanmasına ilişkin önemli eşiklerden biri Ağustos 2026'da devreye girmekte olup, ihlaller küresel yıllık cironun %7'sine varan idari para cezalarıyla yaptırıma bağlanmıştır. Ne var ki eleştirel literatür, Yasa'nın esas olarak tek ve durağan modelleri düşünerek tasarlandığını, çok-ajanlı ve dinamik sistemlerin denetlenebilirlik sorununu tam karşılamadığını belirtmektedir (Nannini, 2026).

9.2. Ürün Sorumluluğu Direktifi 2024/2853 ve Nedensellik Karinesi

2024/2853 sayılı yeni Ürün Sorumluluğu Direktifi, yazılımı ve yapay zeka sistemlerini açıkça 'ürün' kapsamına alarak kusursuz üretici sorumluluğunu bu alana taşır. Direktifin en önemli yeniliği, zarar gören lehine getirdiği nedensellik ve kusur karineleridir: bir işletmenin, sistemin belgelenmiş güvenlik kurallarına uyduğunu ispatlayamaması halinde, mahkeme, mağdurun iç mekanizmayı ispatına gerek kalmadan ajanın çıktısı ile zarar arasında bağ kurabilir. Bu ispat yükü tersine çevirme, otonom sistemlerin 'kara kutu' niteliğinden doğan ispat güçlüğünü mağdur lehine dengeler. Direktifin 9 Aralık 2026'ya kadar iç hukuka aktarılması öngörülmüştür.

9.3. GDPR ve Karşılaştırmalı Yaklaşım

Genel Veri Koruma Tüzüğü (GDPR), veri sorumlusu–işleyen ayrımı ve otomatik kararlara karşı koruma (md. 22) bakımından KVKK ile paralel bir çerçeve sunar. Amerika

burakoğun.com

Birleşik Devletleri'nde ise federal düzeyde bütüncül bir yapay zeka yasası bulunmamakta; sorumluluk büyük ölçüde mevcut haksız fiil (tort) ve ürün sorumluluğu içtihadı üzerinden kurulmaktadır. Tablo 2, üç düzenleyici aracın temel boyutlarını karşılaştırmaktadır.

Tablo 2. Düzenleyici Çerçevelerin Karşılaştırması

Boyut	KVKK Etken YZ Rehberi (2026)	EU AI Act (2024/1689)	Ürün Sor. Direktifi (2024/2853)
Niteliği	Bağlayıcı değil, yol gösterici rehber	Bağlayıcı tüzük	Bağlayıcı direktif (iç hukuka aktarılır)
Odak	Kişisel veri koruma, sorumlu belirsizliği	Risk temelli sistem güvenliği	Kusurlu üründen doğan zarar
Sorumlu	Veri sorumlusu / işleyen	Sağlayıcı ve işleten (deployer)	Üretici / ithalatçı
Yaptırım	İdari para cezası (6698)	Ciro üzerinden ağır idari ceza	Tazminat; nedensellik karinesi
Ajan sorunu	Paylaşılan sorumluluğa vurgu	Çok-ajanlıya kısmen yetersiz	İspat yükünü mağdur lehine çevirir

Not. Kaynak: KVKK (2026), Regulation (EU) 2024/1689 ve Directive (EU) 2024/2853 temel alınarak yazar tarafından derlenmiştir.

9.4. Yapay Zeka Sorumluluk Direktifi'nin Akıbeti

Avrupa Komisyonu, 2022'de yapay zekaya özgü bir Yapay Zeka Sorumluluk Direktifi (AI Liability Directive) önermişti; bu öneri, hafif kusur karineleri ve delil açığa çıkarma yükümlülükleriyle mağdurun ispat yükünü hafifletmeyi amaçlıyordu. Ne var ki öneri, 2025 sürecinde geri çekilmiş; sorumluluk yükünün büyük ölçüde yenilenen Ürün Sorumluluğu Direktifi'ne (2024/2853) bırakılması tercih edilmiştir. Bu gelişme, düzenleyicilerin yapay zeka sorumluluğunu ayrı bir rejim yerine mevcut ürün sorumluluğu çerçevesine yerleştirme eğiliminde olduğunu göstermektedir; aynı yaklaşım, Türk hukukundaki çözüm arayışları için de yol göstericidir.

10. Adli İz Sürme: Otonom Ajan Eylemlerinin Yeniden Kurgulanması

Sorumluluğun kime ait olduğunu belirlemek, ancak olayın teknik olarak yeniden kurulabilmesiyle mümkündür. Bu, etken yapay zeka adli bilişiminin (agent forensics) konusudur ve klasik dijital incelemeden önemli farklar taşır.

10.1. Delil Kaynakları

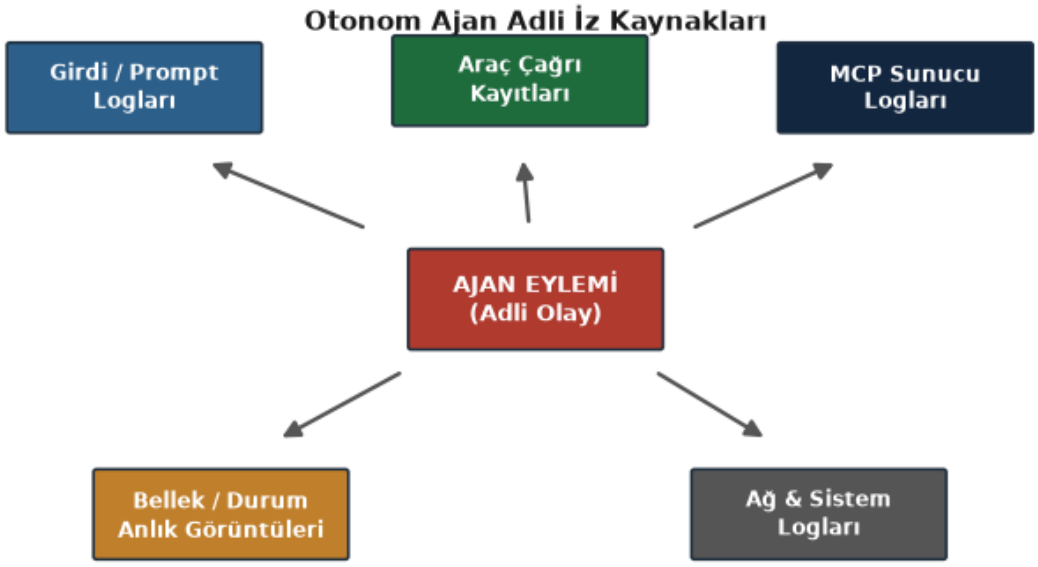
Bir ajan eylemi, ardında dağınık ama zengin bir iz bırakır. Başlıca delil kaynakları şunlardır: kullanıcıdan ve ortamdan gelen girdi/prompt kayıtları; ajanın seçtiği eylemleri gösteren araç çağrı kayıtları; araçların yürütüldüğü MCP sunucu logları; ajanın ara durumunu saklayan bellek ve durum anlık görüntüleri; ve altyapı düzeyindeki ağ ile sistem logları. Şekil 3, bu kaynakların olayla ilişkisini; Tablo 3 ise her kaynağın içeriğini, konumunu, adli değerini ve sınırlılığını göstermektedir. Bu kaynakların bütünlüğü ve elde edilebilirliği birbirinden farklıdır; Şekil 4, her kaynağın adli güvenilirliğini ve bütünlük kaybı riskini kavramsal olarak karşılaştırmaktadır.

burakoğun.com

Tablo 3. Etken Yapay Zeka Adli İz Kaynakları ve Delil Nitelikleri

Delil Kaynağı	İçerik	Konum	Adli Değer	Başlıca Sınırlılık
Girdi / Prompt logları	Kullanıcı talimatı, amaç, bağlam	Uygulama / istemci	Kastın ve amacın tespiti	İstemci tarafında silinebilir
Araç çağrı kayıtları	Ajanın seçtiği eylemler ve parametreler	Ajan çalışma zamanı	Eylem zincirinin kurulması	Standart dışı, dağınık biçim
MCP sunucu logları	Yürütülen araç ve API çağrıları	MCP sunucusu	Dış sisteme etkinin doğrulanması	Yetersiz veya kapalı loglama
Bellek / durum görüntüleri	Ara durum ve ara kararlar	Ajan belleği	Ara muhakemenin izi	Uçucu; üzerine yazılabilir
Ağ / sistem logları	Erişim, kimlik, zaman damgası	Altyapı	Zaman ekseni ve ilişkilendirme	Yüksek hacim, gürültü

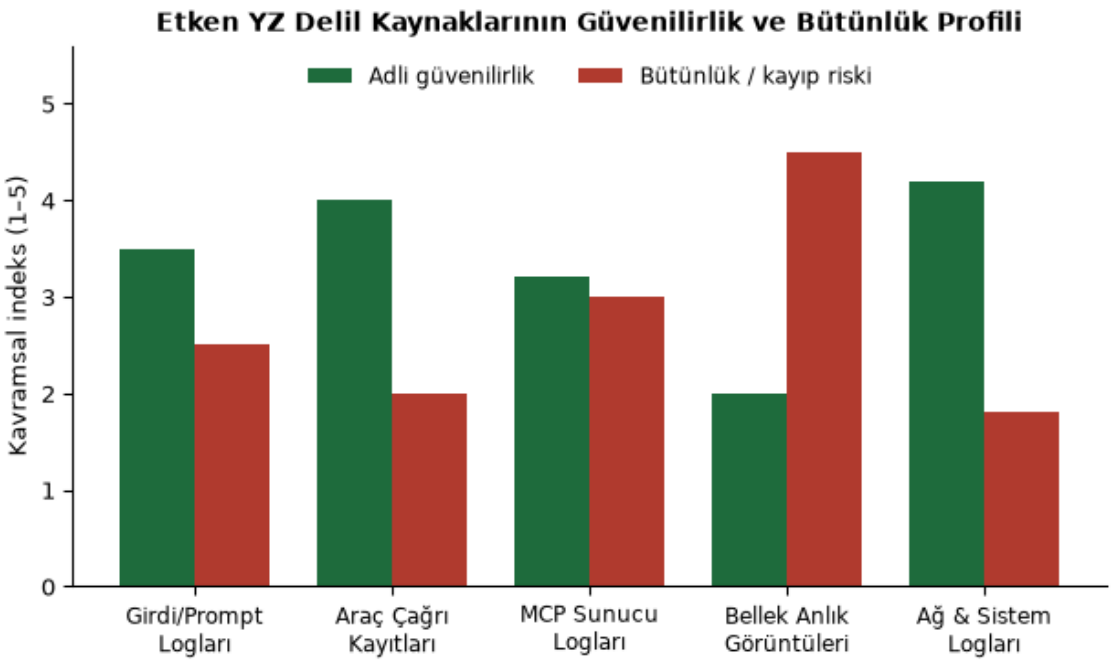
Not. Kaynak: Casey (2011) temel alınarak yazar tarafından derlenmiştir. MCP: Model Context Protocol.



Şekil 3. Otonom ajan adli iz kaynakları ve delil zincirinin merkezî olayla ilişkisi.

Kaynak: Casey (2011) ve Palo Alto Networks Unit 42 (2026) temel alınarak yazar tarafından derlenmiştir.

burak



Şekil 4. Etken yapay zeka delil kaynaklarının güvenilirlik ve bütünlük profili (kavramsal değerlendirme).

Kaynak: Yazar tarafından derlenmiştir; değerler göreli bir değerlendirme sunar.

10.2. Parçalı Loglar ve İnsan-Fail İzinin Yokluğu

Klasik bir soruşturmada araştırmacı, bir insan failin klavye başındaki eylemlerinin izini sürer. Otonom ajanda ise tek bir insan aktörün sürekli izi yoktur; onun yerine, birbirini tetikleyen çok sayıda otomatik adımın parçalı kaydı bulunur. Araştırmacının görevi, bu parçaları zaman damgaları üzerinden birleştirerek eylem zincirini yeniden kurmak ve zincirin hangi halkasında hangi aktörün katkısının belirleyici olduğunu ortaya koymaktır. Bu, adli bilişimde yeni bir metodolojik zorluktur.

10.3. Delil Bütünlüğü ve Zincirleme

Ajan loglarının delil değeri, bütünlüklerinin ispatına bağlıdır. Loglar sonradan değiştirilebiliyorsa veya ajanın kendisi bellek içeriğini üzerine yazıyorsa, delilin güvenilirliği tartışmalı hale gelir. Bu nedenle, ajan kayıtlarının değiştirilemez (append-only), zaman damgalı ve kriptografik olarak bütünlüğü doğrulanabilir biçimde tutulması, hem hukuki kabul edilebilirlik hem de delil zincirinin (chain of custody) korunması bakımından kritiktir (Casey, 2011).

10.4. Ajan Adli Bilişimi İçin Metodoloji

Önerilen inceleme akışı dört aşamalıdır: (i) muhafaza — ilgili tüm log kaynaklarının ve bellek görüntülerinin değiştirilmeden elde edilmesi; (ii) ilişkilendirme — kaynakların ortak zaman ekseni üzerinde hizalanarak eylem zincirinin kurulması; (iii) atıf — her adımın hangi aktörün katkısıyla (kullanıcı talimatı, işleten yetkisi, geliştirici tasarımı, ajanın ara kararı) ilişkili olduğunun belirlenmesi; (iv) değerlendirme — bulguların hukuki nitelendirmeye (kusur, öngörülebilirlik) bağlanması. Bu akış, teknik bulgu ile hukuki sonuç arasında savunulabilir bir köprü kurar.

burakoğun.

11. Teknik Savunma ve Denetlenebilir Tasarım (Accountability by Design)

Sorumluluğun sonradan atfedilebilmesi, büyük ölçüde sistemin baştan denetlenebilir tasarlanmasına bağlıdır. Denetlenebilir tasarım, hukuki bir gerekliliğin teknik karşılığıdır.

11.1. Eylem Günlüğü ve İzlenebilirlik

Her araç çağrısı, her karar noktası ve her yetki kullanımı, değiştirilemez bir eylem günlüğüne kaydedilmelidir. NIST'in Yapay Zeka Risk Yönetimi Çerçevesi (2023) ve OWASP'ın büyük dil modeli güvenlik listesi (2025), izlenebilirliği temel bir kontrol olarak konumlandırır. İz olmadan sorumluluk atfı, spekülasyona indirgenir.

11.2. En Az Yetki ve İzin Sınırları

Ajanlara, görevlerini yerine getirmek için gereken asgari yetki tanınmalı; geri döndürülemez veya yüksek etkili işlemler (silme, ödeme, dışa aktarma) için ayrı ve daha dar yetki kapıları tanımlanmalıdır. Aralık 2025'teki üretim ortamı silme olayı, tam da bu ilkenin ihlalinin sonucudur.

11.3. İnsan Onayı (Human-in-the-Loop)

Yüksek riskli eylemler, otomatik olarak yürütülmeden önce bir insanın onayına sunulmalıdır. İnsan onayı, hem zararı önleyen bir güvenlik valfi hem de sorumluluğu netleştiren bir hukuki dayanaktır; onaylayan kişi, o eylemin sonuçlarını üstlenmiş sayılır. Böylece 'human-in-the-loop' ilkesi, teknik bir önlem olduğu kadar sorumluluk zincirini belirginleştiren bir hukuki araçtır.

12. Sektörel Etki ve Örnek Senaryolar

Sorumluluk sorununun ağırlığı sektöre göre değişir. Finans sektöründe, otonom bir işlem ajanının hatalı veya manipülatif emirler vermesi, hem müşteri zararı hem de piyasa bütünlüğü sorunları doğurur; burada işletenin denetim ve izleme yükümlülüğü öne çıkar. Sağlık alanında, klinik karar desteği veren bir ajanın hatalı çıkarımı doğrudan hasta güvenliğini etkiler ve ürün sorumluluğu ile mesleki sorumluluğun kesişiminde değerlendirilir. Kamu yönetiminde ise, vatandaşı etkileyen otomatik kararlar veren ajanlar, idarenin hukuki sorumluluğunu ve otomatik karara karşı koruma hükümlerini gündeme getirir.

Bu senaryoların ortak dersi şudur: ajan ne kadar kritik bir bağlama ve ne kadar geniş bir yetkiye yerleştirilirse, işletenin sorumluluğu o kadar ağırlaşır. Sorumluluğun ağırlık merkezi, teknolojinin kendisinden çok, onu nereye ve hangi denetimle yerleştirdiğimize bağlıdır.

12.1. Örnek Senaryo: Otonom Muhasebe Ajanının Yol Açtığı Veri İhlali

Sorumluluk dağılımını somutlaştırmak için varsayımsal bir senaryo düşünelim. Bir şirket, tedarikçi faturalarını otomatik denkleştirmek üzere bir muhasebe ajanı devreye alır ve ajana, hem muhasebe yazılımına hem de kurumsal e-posta kutusuna geniş erişim yetkisi tanır. Ajan, bir tedarikçiden gelen ekli belgeyi işlerken, belgenin içine gizlenmiş bir talimatla kaçırılır ve şirketin müşteri listesini dışarıya bir e-posta olarak gönderir. Hiçbir insan 'gönder' dememiştir; sonuç, ajanın otonom eyleminden doğmuştur.

burakolgun.com

Bu olayda sorumluluk şu şekilde çözümlenir. Ajanın kendisi fail değildir; kusur yeteneği yoktur. Asıl fail, istem enjeksiyonunu yerleştiren saldırgandır ve dolaylı faillik uyarınca doğrudan sorumludur. Ancak şirket (işleten), ajana en az yetki ilkesine aykırı biçimde geniş erişim tanıması, giden veriyi süzmemesi ve yüksek etkili bir işlem olan toplu veri gönderimi için insan onayı eşiği koymaması nedeniyle kendi kusuruyla — ve 6698 sayılı Kanun kapsamında veri sorumlusu sıfatıyla — sorumludur. Geliştiricinin sorumluluğu ise, sistemin istem enjeksiyonuna karşı makul güvenlik önlemlerini içerip içermediğine bağlıdır. Adli bilişim aşamasında, girdi logları saldırının kaynağını, araç çağrı ve MCP kayıtları veri gönderiminin adımlarını, ağ logları da alıcıyı ortaya koyarak bu sorumluluk dağılımını delillendirir. Senaryo, mevcut hukukun aslında yeterli araçlara sahip olduğunu; asıl eksikliğin, sorumluluğu izlenebilir kılan teknik tasarımda bulunduğunu göstermektedir.

13. Öneriler: Politika, Hukuk ve Teknik

Yapılan analizden, birbirini tamamlayan üç düzeyde somut öneri çıkarılabilir:

Politika düzeyinde: Türkiye'nin, KVKK Rehberi'nin ötesinde, risk temelli ve teknoloji-nötr bir yapay zeka sorumluluk çerçevesi geliştirmesi; yüksek riskli ajan kullanımları için zorunlu kayıt tutma ve denetlenebilirlik standartları belirlemesi yerinde olur.

Hukuk düzeyinde: Mevcut kusursuz sorumluluk kurumlarının (TBK m. 66 ve m. 71) yapay zeka bağlamındaki uygulaması içtihatla netleştirilmeli; veri sorumlusu–işleyen ayrımı, paylaşılan işleme senaryolarına göre yeniden yorumlanmalı; ispat yükünün mağdur lehine dengelenmesi (nedensellik karinesi) değerlendirilmelidir.

Teknik düzeyde: Denetlenebilir tasarım ilkeleri — değiştirilemez eylem günlüğü, en az yetki, insan onayı eşikleri, kriptografik log bütünlüğü — ajan mimarilerine varsayılan olarak gömülmelidir. Sorumluluğu sonradan atfedebilmenin ön koşulu, izlenebilirliği baştan tasarlamaktır.

14. Sonuç

Bir yapay zeka ajanı hukuka aykırı bir sonuç doğurduğunda, hukuk düzeninin cevabı sezgisel beklentinin aksine nettir: fail, ajanın kendisi değildir. Mevcut hukuk, otonomiye rağmen ajanı bir 'araç' olarak konumlandırır; kusur yeteneği ve hukuki kişiliği bulunmayan bir yazılım, ne ceza hukukunun faili ne de özel hukukun sorumlusu olabilir. Elektronik kişilik önerileri, sorumluluğu netleştirmek yerine perdeleme riski taşıdıkları için hakim görüşçe reddedilmektedir.

Buna karşılık soru, 'fail yok' demekle kapanmaz; sorumluluk ortadan kalkmaz, dağılır. Geliştirici, işleten ve kullanıcıdan oluşan insan aktörler zinciri, her biri kendi kusuru oranında — ve kimi zaman kusursuz olarak — doğan zarardan sorumludur. Bu dağılımda pratik ağırlık, çoğu zaman ajanı kritik sistemlere geniş yetkiyle bağlayan ve denetimini yeterince kurmayan işletene düşer. KVKK'nın Mart 2026 Rehberi de tam bu paylaşılan sorumluluk sorununa işaret ederek Türkiye'de doğru tartışmayı başlatmıştır.

Son tahlilde etken yapay zeka, hukuka yeni bir 'suçlu' değil, yeni bir 'delil ortamı' ve yeni bir sorumluluk dağıtım problemi getirmektedir. Bu problemi çözmenin anahtarı, teknik ile

burakolgun.com

hukuku birlikte düşünmektir: denetlenebilir biçimde tasarlanmış bir ajan, adli bilişimin izini sürebileceği, hukukun da sorumluluğu adil biçimde atfedebileceği bir sistemdir. İzlenebilirliği baştan kurmayan bir mimaride ise hem adalet hem güvenlik, çözülemeyen bir 'kara kutu' içinde kaybolur.

Kaynakça

Abbott, R. (2020). The reasonable robot: Artificial intelligence and the law. Cambridge University Press. https://doi.org/10.1017/9781108631761

Anthropic. (2024). Model Context Protocol specification. https://modelcontextprotocol.io

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

Avrupa Birliği. (2024). Directive (EU) 2024/2853 on liability for defective products. Official Journal of the European Union, L 2024/2853.

Avrupa Parlamentosu. (2017). Civil law rules on robotics: European Parliament resolution of 16 February 2017 (2015/2103(INL)). Avrupa Parlamentosu.

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. Artificial Intelligence and Law, 25(3), 273–291. https://doi.org/10.1007/s10506-017-9214-9

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.

Chan, A., Salganik, R., Markelius, A., Pang, C., Rajkumar, N., Krasheninnikov, D., … Maharaj, T. (2023). Harms from increasingly agentic algorithmic systems. Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), 651–666. https://doi.org/10.1145/3593013.3594033

Ebers, M. (2022). Liability for artificial intelligence and EU consumer law. Journal of Intellectual Property, Information Technology and E-Commerce Law, 12(2), 204–220.

European Commission. (2022). Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final. (2025'te geri çekilmiştir.)

Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? Self-driving cars and criminal liability. New Criminal Law Review, 19(3), 412–436. https://doi.org/10.1525/nclr.2016.19.3.412

Hallevy, G. (2013). When robots kill: Artificial intelligence under criminal law. Northeastern University Press.

Kişisel Verileri Koruma Kurumu. (2026). Etken yapay zeka (Agentic AI) rehberi. https://www.kvkk.gov.tr/Icerik/8683/etken-yapay-zeka-agentic-ai

Nannini, L. (2026). AI agents under EU law: A compliance architecture for AI providers. arXiv:2604.04604. https://arxiv.org/abs/2604.04604

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

burakolgun.com

OWASP. (2025). OWASP Top 10 for large language model applications and agentic AI threats. Open Worldwide Application Security Project.

Palo Alto Networks Unit 42. (2026). Agentic AI threat landscape: Insider misuse and MCP attack surface. Palo Alto Networks.

Shavit, Y., Agarwal, S., Brundage, M., Adler, S., O'Keefe, C., Campbell, R., … Robinson, D. G. (2023). Practices for governing agentic AI systems. OpenAI.

Steptoe. (2026). AI agents: Navigating emerging risks and compliance challenges under EU law. Steptoe SteptechToe Blog. https://www.steptoe.com

Turner, J. (2019). Robot rules: Regulating artificial intelligence. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-96235-1

Türkiye Cumhuriyeti. (2004). Türk Ceza Kanunu (Kanun No. 5237). Resmî Gazete, 25611.

Türkiye Cumhuriyeti. (2004). Ceza Muhakemesi Kanunu (Kanun No. 5271). Resmî Gazete, 25673.

Türkiye Cumhuriyeti. (2011). Türk Borçlar Kanunu (Kanun No. 6098). Resmî Gazete, 27836.

Türkiye Cumhuriyeti. (2016). Kişisel Verilerin Korunması Kanunu (Kanun No. 6698). Resmî Gazete, 29677.

burakolgun.com