

Üretken Yapay Zekâ ve Aracı Sorumluluk Rejimi: 5651 Sayılı Kanun'un Yapısal Bağdaşmazlığı ve Reform Seçenekleri^(*)

Generative AI and the Intermediary Liability Regime: The Structural Incompatibility of Turkish Law No 5651 and Reform Options

Muhammed Furkan AKINCI^(**)

Öz:

Bu çalışma, 5651 sayılı Kanun'daki içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcı ayırımının üretken yapay zekâ hizmetlerine hangi ölçüde uygulanabileceğini ve bu uyarlamada sorumluluk standardının Avrupa Birliği'nin aracı hizmet sağlayıcılara ilişkin çerçevesiyle (Dijital Hizmetler Tüzüğü (Digital Services Act, DSA) ve Yapay Zekâ Tüzüğü (Artificial Intelligence Act, AI Act)) nasıl tutarlı biçimde kurulabileceğini inceler. Yöntem olarak karşılaştırmalı doktrinel analiz benimsenmiş; Türk hukuku bakımından 5651 sayılı Kanun ile birlikte TBK, TCK, KVKK ve FSEK, AB hukuku bakımından DSA ve 2024/1689 sayılı Yapay Zekâ Tüzüğü, Amerikan hukuku bakımından ise Communications Decency Act (CDA) § 230 inceleme kapsamına alınmıştır. Analiz, üretken yapay zekâ değer zincirinin model sağlayıcı-konuşlandırıcı-kullanıcı katmanlarına ayrıldığını; çekirdek çıkarımın (inference) ise üçüncü kişi içeriklerinin depolanması ve bildirim üzerine münferit içeriğin kaldırılması varsayımına dayanan güvenli liman kurgusuyla yapısal olarak uyumadığını göstermektedir. Bu nedenle 5651 sayılı Kanun, ancak kullanıcı içeriğinin kalıcı biçimde saklandığı ve üçüncü kişilere açıldığı barındırma ve yayın özelliklerinde işlevsel olabilir; model ağırlıkları düzeyinde ise kaldırma talebi teknik olarak karşılıksız kalmakta ve ölçülülük sorunları ortaya çıkmaktadır. Çalışma, reform gündemi bakımından üç öneri geliştirmektedir: (i) içeriğin çıkarılması ile erişimin engellenmesi ikiliğini tamamlayan sistem davranışı tedbirleri, (ii) haberdar edilme eşliğini üretken çıktılara uygun biçimde somutlaştıran altı unsurlu bir bildirim standardı ve (iii) bilgi-kontrol-müdahale kapasitesi ölçütlerine dayanan rol temelli tahsis matrisi. Ayrıca Anayasa Mahkemesi'nin 5651 sayılı Kanun m. 9'u iptali sonrasında, kişilik haklarına ilişkin başvuru usulünün kademeli müdahale, gerekçeli cevap, karşı bildirim ve şeffaflık güvenceleriyle kanun düzeyinde yeniden kurulması gerektiği savunulmaktadır.

^(*) Araştırma Makalesi / *Research Article*
Yayın Kuruluna Ulaştığı Tarih: 02.02.2026
Yayınlanmasının Kabul Edildiği Tarih: 02.03.2026
DOI: 10.58733/İmhfd.1879761

Bu makaleye atıf için: Muhammed Furkan Akıncı, 'Üretken Yapay Zekâ ve Aracı Sorumluluk Rejimi: 5651 Sayılı Kanun'un Yapısal Bağdaşmazlığı ve Reform Seçenekleri' 2026 11(1) İMHFD 651-708

^(**) *Dr. Öğr. Üyesi*, Boğaziçi Üniversitesi, Hukuk Fakültesi, Bilişim Hukuku Anabilim Dalı, İstanbul - Türkiye
E-posta: mfurkanakinci@gmail.com
Orcid: 0009-0007-5851-1128

Anahtar Kelimeler:

Üretken Yapay Zekâ, Aracı Sorumluluğu, 5651 Sayılı Kanun, Güvenli Liman, Uyar-Kaldır.

Abstract:

This article examines how the actor categories of Turkish Law No 5651 (content provider, hosting provider, and access provider) should be mapped onto generative AI deployments and which liability standard can remain coherent with EU intermediary governance, in particular the Digital Services Act and the AI Act. Methodologically, it relies on doctrinal analysis and a functional comparison matrix that translates legal categories into technical layers of the generative AI pipeline. It argues that generative AI value chains are layered (model provider, deployer, end user) and that core inference is structurally incompatible with safe-harbour models premised on storing third-party items and removing them upon notice. Consequently, Law No 5651 can operate meaningfully only at the storage and publication layers (user uploads, profiles, archives), whereas model weights and training data challenge notice-and-takedown both technically and normatively. Building on a feature-based classification of platform functions, the article proposes a layered hybrid approach: Law No 5651 supplies a procedural and remedial framework (notice, action, access blocking or removal), while substantive liability is allocated through general tort, criminal, data-protection and copyright norms (TBK, TCK, KVKK, FSEK). Finally, in light of the Turkish Constitutional Court's annulment of Article 9, the article sketches a notice-and-action reform that emphasises graded intervention, reason-giving, counter-notice, and transparency safeguards, aligning Turkish practice with the EU's shift from pure liability to duty-of-care governance.

Keywords:

Generative AI, Intermediary Liability, Turkish Law No 5651, Safe Harbour, Notice and Takedown.

Extended Summary:

This article addresses a doctrinal mapping problem that becomes acute once generative AI systems are deployed at scale: traditional intermediary liability regimes presuppose third-party items that can be stored, identified, and removed upon notice, whereas generative AI produces probabilistic outputs from model weights and operational pipelines. The research question is twofold. First, how should the actor categories of Turkish Law No 5651 (content provider, hosting provider, access provider and related categories) map onto the main roles in generative AI deployment (model provider, deployer, end user)? Second, which liability standard can be defended as coherent with EU intermediary governance, given the Digital Services Act's notice-and-action architecture and the AI Act's provider and deployer obligations?

The article begins by locating the mismatch at the level of legal technique. Law No 5651 is built around a hosting centered paradigm: hosting assumes that unlawful content exists as a storable object and that responsibility is largely triggered by knowledge obtained through a notification. Generative AI, by contrast, combines (i) training and fine-tuning on data sets, (ii) inference-time prompting, and (iii) downstream publication and archiving features. In core inference, the system does not merely transmit or store third-party content; it generates new outputs, and those outputs cannot be removed from model weights in the same way as a hosted file or post. This makes a categorical classification of foundation models as hosting providers conceptually unstable, and it also makes notice-and-takedown at the weights level both technically infeasible and normatively overbroad.

Against this background, the article proposes a functional, feature-based classification that separates (a) storage and publication modules (user uploads, profiles, archives, sharing and indexing features) from (b) core inference. Where a generative AI service offers persistent storage and publication to third parties, the deployer may plausibly be analyzed under Law No 5651's

hosting-provider framework, subject to the statute's knowledge and action conditions. By contrast, a model provider's core inference service, especially when provided through an API, does not fit the hosting safe harbor's third-party information premise. The practical implication is that the Turkish debate should not turn on labels (model vs platform) but on which actor controls which function, which stage of the pipeline is at issue, and which actor can take proportionate and effective measures at that stage.

The EU comparison clarifies the direction of travel. Under the Digital Services Act, hosting safe harbors remain, but they are complemented by a layered governance structure that requires notice-and-action mechanisms, transparency and risk management, especially for online platforms and very large online platforms. The DSA also keeps the prohibition of general monitoring while enabling structured procedural obligations. In the AI Act, the main axis is not "hosting" but the provider and deployer distinction, with additional obligations for general-purpose AI models and systemic-risk models. Together, the DSA and AI Act illustrate a shift from a purely liability-triggered model to a duty-of-care governance model: liability questions do not disappear, but they are increasingly mediated through procedural and organizational obligations.

For Turkish law, the article therefore argues for a layered hybrid approach. Law No 5651 provides the procedural tools aimed at ending ongoing violations at the publication layer (access blocking or removal, notice processing, transparency), but it cannot by itself allocate substantive responsibility across a generative AI value chain. Substantive liability must be built through the relevant fields of Turkish private and public law: tort law (TBK) for negligence and organizational fault; criminal law (TCK) for actor-specific attribution within the limits of corporate criminal liability; data protection law (KVKK) for training data, logs, prompts and outputs, including role allocation between controller and processor; and copyright law (FSEK), including the special notice procedures and their tensions with data protection and procedural safeguards.

The analysis of remedies and procedure becomes particularly salient after the Turkish Constitutional Court annulled Article 9 of Law No 5651. The annulment reveals that a workable notice-and-action system must be designed with graded intervention, clear thresholds, reasoning duties and effective counter-notice mechanisms. In the generative AI context, these safeguards are not merely formalities: they are necessary to avoid systematic over-removal, to protect freedom of expression, and to ensure that interventions are targeted at the correct layer (publication and archiving rather than weights).

The article concludes with a reform package that aims to preserve the limited usefulness of Law No 5651 while preventing category errors. First, a feature-based classification should be adopted in legal analysis and, where necessary, in legislation, to distinguish hosting-like functions from core inference. Second, procedural obligations should be rebuilt post-annulment in a way that is compatible with EU notice-and-action standards while respecting the prohibition of general monitoring. Third, substantive liability should be allocated through a role-based matrix across TBK, TCK, KVKK and FSEK, so that each actor is assessed against the measures it can realistically implement at the relevant stage of the pipeline. This layered approach offers a coherent liability standard that reflects both the technical realities of generative AI and the EU's intermediary governance benchmark.

GİRİŞ

Temel modellerin kitlesel ölçekte konuşlandırılması, üretken yapay zekâyı aracı sorumluluğu tartışmasının merkezine yerleştirmiştir. Klasik aracı sorumluluğu rejimleri, üçüncü kişi içeriğinin barındırılması ve bildirim üzerine münferit içeriğin çıkarılması varsayımı üzerine kurulu pasif aracılık modelini esas alır. Buna karşılık üretken yapay zekâ sistemleri, kullanıcı komutlarına (prompt) yanıt olarak yeni içerik üretir. Bu farklılık, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un (5651 sayılı Kanun) içerik sağlayıcı ile yer sağlayıcı ayırımının üretken yapay zekâ değer zincirine doğrudan uygulanmasını güçleştirir; zira model sağlayıcı, konuşlandırıcı ve son kullanıcı arasında dağılan işlevler, sorumluluğu tek bir aktör kategorisinde toplananın sınırlarını daha açık biçimde ortaya koyar¹.

5651 sayılı Kanun, 2007 yılında ağırlıklı Web 2.0 döneminin aracı hizmet sağlayıcılarını esas alarak tasarlanmıştır. Kanun, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, toplu kullanım sağlayıcı ve sosyal ağ sağlayıcı şeklinde beşli bir aktör sınıflandırması öngörür. Bununla birlikte bu sınıflandırma, internet sükülerinin genel tanımlanmasında kavram karmaşası üretebilmekte ve yeni teknolojik gelişmeler karşısında yetersiz kalabilmektedir. Nitekim arama motorlarının bu kategorilerden hangisi kapsamında değerlendirileceği doktrinde hâlen tartışmalıdır².

Kanun'un yer sağlayıcı bakımından öngördüğü güvenli liman, depolama esaslı bir sorumluluk varsayımı üzerine kuruludur. Yer sağlayıcı, hukuka aykırı içerikten haberdar edildiğinde ve teknik olarak imkân bulunduğu ölçüde içeriği yayından çıkarmakla yükümlüdür; buna karşılık kural olarak içerik kontrolü veya hukuka aykırılığı araştırma yükümlülüğü altında değildir³. Bununla birlikte Anayasa Mahkemesi, 11.10.2023 tarihli kararıyla 5651 sayılı Kanun m. 9'u yapısal sorunlar nedeniyle iptal etmiş; özellikle kademeli müdahale yönteminin

¹ David Atkinson ve Jacob Morrison, 'Unsettled Law: Time to Generate New Approaches?' (SSRN 2024) 10; Hasala Ariyaratne, 'ChatGPT and Intermediary Liability: Why Section 230 Does Not and Should Not Protect Generative Algorithms' (SSRN 2023) 8-9; Eugene Volokh, 'Large Libel Models? Liability for AI Output' (2023) 3 Journal of Free Speech Law 489, 495; Peter Henderson, Tatsunori Hashimoto ve Mark Lemley, 'Where's the Liability in Harmful AI Speech?' (2023) 3 Journal of Free Speech Law 622.

² Alper Işık, 'Anayasa Mahkemesi'nin 5651 Sayılı Kanun'un 9. Maddesi Bağlamında İnternete Erişimin Engellenmesine Dair Değişen Yaklaşımının Değerlendirilmesi' (2022) 30 Selçuk Üniversitesi Hukuk Fakültesi Dergisi 967, 973; İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651) 2007, m. 1, m. 2; Yusuf Başlar, 'İnternet Sükeleri ve Cezai Sorumlulukları' (2022) 19 Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 603, 621.

³ 5651 sayılı Kanun, m. 2/m, m. 5/2.

bulunmaması ve yasama organınca yeni bir usul kurulmamış olmasını ölçülülük bakımından sorunlu görmüştür⁴.

Üretken yapay zekânın teknik işleyişi, depolama temelli bu sorumluluk tekniğiyle doğrudan çatışmaktadır. Model ağırlıklarından olasılıksal çıktı üretimine dayanan bu sistemlerde yanıtlar, internette kamuya açık bilgiler, lisanslanan içerikler ve kullanıcılar ile insan eğitmenlerinin sağladığı veriler üzerinden şekillenen bir veri havuzuna dayanır. Olasılıksal çalışma biçimi ve kara kutu niteliği, iç işleyişin ve karar alma süreçlerinin kolayca yorumlanamamasına yol açar. Bu nedenle temel modeller, tasarımları gereği çıktılarının güvenli olacağına dair güçlü teorik garantiler sunamaz; yetersiz güvenlik önlemleriyle konuşlandırıldıklarında zararlı söylem üreten bir çalışma biçimine kayabilmektedir⁵.

Bu risk, somut vakalarda da görünür hâle gelmiştir. Bir uyuşmazlıkta üretken bir sistem, gerçek bir kişi hakkında tamamen uydurma bir zimmete para geçirme anlatısı üretmiş; ilgili kişi hiçbir davada taraf olmamasına rağmen hayalî bir davaya ilişkin kurgusal pasajlar ve sahte bir dosya numarası dahi sunmuştur. Üretken modellerin örüntülerden öğrenerek yeni çıktı üretmesi, bu tür hallüsinasyonların teknik olarak beklenebilir bir yan etki olabileceğine işaret etmektedir⁶.

Bu bağlamda, eğitim verisinin münferit bir parçasının etkisinin model ağırlıkları düzeyinde giderilmesi, makine unutma (machine unlearning) literatürünün hedeflediği türden bir müdahaledir. Bu literatür, bir yandan sistemlerin unutulması problemini erken dönemde kavramsallaştırmış; diğer yandan veri silme ve sertifikalı kaldırma gibi alt yaklaşımlarla kuramsal güvenceler ve uygulanabilirlik sınırları üzerine yoğunlaşmıştır⁷. Bununla birlikte stokastisite, artımlı eğitim ve unutulma talebi arttıkça performansın bozulması gibi nedenlerle, belirli

⁴ Anayasa Mahkemesi, E. 2020/76, K. 2023/172, T. 11.10.2023, para. 101; İsmail Demez, '5651 Sayılı Kanun'un İnternet Adreslerine Erişimin Engellenmesine İlişkin 9. Maddesinin İptali ve Öneriler' (2024) 15 Türkiye Adalet Akademisi Dergisi 177, 185, 191.

⁵ David Atkinson ve Jacob Morrison (n 1) 4; Peter Henderson, Tatsunori Hashimoto ve Mark Lemley (n 1) 595.

⁶ John G. Browning, 'Whose Bot Is It Anyway? Determining Liability for AI-Generated Content' (2025) 45 Northern Illinois University Law Review 340, 18; Nina Brown, 'Bots Behaving Badly: A Products Liability Approach to Chatbot-Generated Defamation' (2023) 3 Journal of Free Speech Law 411.

⁷ Yinzhi Cao ve Junfeng Yang, 'Towards Making Systems Forget with Machine Unlearning' *IEEE Symposium on Security and Privacy (SP)* (2015) 1-2 <<https://www.ieee-security.org/TC/SP2015/papers-archived/6949a463.pdf>>; Antonio A Ginart ve diğerleri, 'Making AI Forget You: Data Deletion in Machine Learning' (arXiv:190705012 2019) 1-2 <<https://arxiv.org/abs/1907.05012>>; Chuan Guo ve diğerleri, 'Certified Data Removal from Machine Learning Models' (arXiv:191103030 2019) 1-2 <<https://arxiv.org/abs/1911.03030>>.

bir veri parçasının etkisini geriye dönük olarak silmek özellikle derin öğrenme modellerinde hâlen güç ve tartışmalıdır⁸. Bu nedenle üretken yapay zekâ sistemleri, veriyi veya parametreyi doğrudan silmekten ziyade RLHF ve filtreleme⁹ gibi yöntemlerle belirli tür çıktıları istatistiksel olarak bastırmaya çalışır. Dolayısıyla tekil içerik kaldırma refleksini esas alan yaklaşımlar, model ağırlıkları düzeyinde sınırlı bir karşılık bulur¹⁰. Dahası üretken sistemler, başkasınca sağlanan bir içeriği yalnızca iletme veya depolamakla kalmaz; kullanıcı komutuna yanıt olarak yeni içerik üretir. Bu durum, başkasınca sağlanan bilgi koşuluna dayanan aracı sorumluluk bağışıklıklarının üretken modeller bakımından otomatik olarak işletilebileceği varsayımını zayıflatmaktadır¹¹.

Bu yapısal fark, barındırma kavramının tanımında da görünür hâle gelir. DSA, barındırma hizmetini hizmet alıcısının talebi üzerine bilginin depolanması olarak tanımlar; 5651 sayılı Kanun ise yer sağlayıcıyı içerikleri barındıran sistemleri sağlayan kişi olarak nitelendirir. Üretken yapay zekâ, üçüncü kişi içeriğini barındırmak yerine içerik ürettiği için bu tanımların hiçbirine tam olarak oturmaz. Güvenli liman korumasının salt teknik, otomatik ve pasif faaliyetleri hedeflemesi karşısında, daha önce üçüncü kişilerce ifade edilmemiş mesajlar üreten yazılımları konuşlandıran aktörleri sorumluluktan bütünüyle muaf tutmak, normatif tercih olarak da tartışmalıdır¹².

Bu çalışma, üretken yapay zekâ sistemlerinin aracı sorumluluk rejimleriyle kesişimini Türk hukuku bakımından sistematik biçimde incelemektedir. Karşı-

⁸ Thanh Tam Nguyen ve diğerleri, 'A Survey of Machine Unlearning' (arXiv:220902299 2022) 5, 9-10 <<https://arxiv.org/abs/2209.02299>>; Lucas Bourtole ve diğerleri, 'Machine Unlearning' *IEEE Symposium on Security and Privacy (SP)* (2021) 2, 5 <<https://arxiv.org/abs/1912.03817>>; Ayush Sekhari ve diğerleri, 'Remember What You Want to Forget: Algorithms for Machine Unlearning' (arXiv:210303279 2021) 1-2 <<https://arxiv.org/abs/2103.03279>>.

⁹ RLHF, insan geri bildirimle pekiştirmeli öğrenme (reinforcement learning from human feedback, RLHF) tekniğidir; model, insan değerlendiricilerin tercihleri üzerinden kurulan bir ödül işlevine göre yeniden ayarlanarak belirli tür yanıtları daha düşük olasılıkla üretmeye yönlendirilir. Filtreleme ise konuşlandırma aşamasında girdiye veya çıktıya uygulanan güvenlik ve uygunluk kontrollerini (filtering; örneğin sınıflandırıcılar, anahtar kelime listeleri ve kural tabanlı engeller) ifade eder; bu katmanlar eğitim verisini veya model parametrelerini ortadan kaldırmadan, belirli tür içeriklerin üretilmesini ya da kullanıcıya sunulmasını azaltmayı amaçlar.

¹⁰ David Atkinson ve Jacob Morrison (n 1) 9.

¹¹ Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 62; Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 63; Hasala Ariyaratne (n 1) 8-9; Peter Henderson, Tatsunori Hashimoto ve Mark Lemley (n 1) 622.

¹² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) 2022 (OJ L 277, 27 October 2022, pp 1-102), m. 6; 5651 sayılı Kanun, m. 2/m; Giancarlo Frosio (ed) (n 11) 62; Eugene Volokh (n 1) 495.

laştırmalı inceleme, üç rejimin (CDA § 230, DSA ve AB Yapay Zekâ Tüzüğü) aracı sorumluluğunu hangi kurucu varsayımlar üzerine kurduğunu belirlemeyi ve bu varsayımların üretken sistemlerde hangi noktalarda karşılık bulmadığını göstermeyi amaçlar. Türk hukuku bakımından temel tez, 5651 sayılı Kanun'un depolama temelli güvenli liman kurgusunun üretim temelli çıkarım süreçleriyle yapısal olarak bağdaşmadığıdır.

Bu doğrultuda çalışma üç öneri geliştirmektedir: (i) içeriğin çıkarılması ve erişimin engellenmesi ikiliğini tamamlayacak biçimde sistem davranışına yönelik aşamalı tedbir kategorileri; (ii) haberdar edilme eşliğini üretken çıktılara uygun biçimde somutlaştıran, girdi-çıktı bağlamını da içeren doğrulanabilir bir bildirim standardı (altı unsur standardı); (iii) sorumluluğu kategorilere göre değil bilgi-kontrol-müdahale kapasitesine göre tahsis eden rol temelli bir matris. Ayrıca Anayasa Mahkemesi'nin m. 9 iptali sonrasında, kişilik haklarına ilişkin başvuru yolunun asgari usul güvenceleriyle birlikte kanun düzeyinde yeniden kurulması gerektiği kabul edilmelidir.

Metin, giriş bölümünü izleyen kısımlarda (i) 5651 sayılı Kanun, DSA, AB Yapay Zekâ Tüzüğü ve CDA § 230'un aracı sorumluluğa ilişkin çerçevelerini karşılaştırmakta; (ii) üretken yapay zekâ değer zincirinde fonksiyonel eşleştirme ve sorumluluk standardını tartışmakta; (iii) Türk hukukunda uygulama ve içtihat sorunlarını incelemekte; (iv) reform seçeneklerini değerlendirmektedir.

I. GENEL BAKIŞ

Bu çalışmada karşılaştırmalı olarak ele alınan üç aracı sorumluluğu çerçevesi, farklı teknolojik dönemlerin ihtiyaçlarına göre şekillenmiştir¹³. Bu çerçeveler, çevrimiçi araçların üçüncü kişi kaynaklı içerikten hangi koşullarda sorumsuz kalacağını ve hangi koşullarda sorumluluk üstleneceğini, farklı tekniklerle sınırlandırmakta ve koşullandırmaktadır. Üretken yapay zekânın yaygınlaşması ise ortak bir gerilimi daha da keskinleştirmektedir: çevrimiçi platformların sorumluluğu tartışması, klasik haksız fiil sorumluluğu ekseninden düzenleyici özen yükümlülükleri eksenine doğru kaymakta; olay sonrası müdahale mantığı tek başına yeterli görülmemektedir¹⁴.

¹³ Miriam C. Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) 12 JIPITEC 361, 361.

¹⁴ Andrea Palumbo, 'The Digital Services Act and the Protection of Fundamental Rights' [2024] European Law Blog 2.

A. Türkiye

5651 sayılı Kanun, internet aktörlerini beş kategoride tanımlamaktadır: (i) içerik sağlayıcı, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler; (ii) yer sağlayıcı, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler; (iii) erişim sağlayıcı, kullanıcılarına internet ortamına erişim imkânı sağlayan gerçek veya tüzel kişiler; (iv) toplu kullanım sağlayıcı, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek veya tüzel kişiler; (v) sosyal ağ sağlayıcı, kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişiler¹⁵.

Üretken yapay zekâ hizmetlerinin bu beşli sınıflandırma içindeki konumu, tek bir etikete indirgenememektedir. Nitelendirme, hizmetin (i) çıktıyı ve kullanıcı içeriklerini üçüncü kişilere hangi ölçüde açtığı, (ii) konuşma/çıktı kayıtlarını kalıcı biçimde saklayıp saklamadığı ve (iii) paylaşım ile görünürlük işlevleri üzerinden kamusalılığı nasıl kurduğu dikkate alınarak yapılmalıdır. Bu nedenle üretken bir hizmet, somut ürün tasarımına göre içerik sağlayıcı, yer sağlayıcı veya sosyal ağ sağlayıcı kategorileriyle kesişebildiği gibi; kapalı devre kullanım senaryolarında “internet ortamı” eşiği gerçekleşmediğinden 5651 sayılı Kanun kapsamı dışında da kalabilir¹⁶. Erişim sağlayıcı ve toplu kullanım sağlayıcı kategorileri ise üretken hizmet sağlayıcıları bakımından kural olarak tali olmakla birlikte, erişimin engellenmesi tedbirlerinin uygulanmasında muhatap sıfatıyla önem taşımaktadır.

Bu sınıflandırma sorunu, özellikle içerik sağlayıcı ile yer sağlayıcı rejimleri arasındaki sorumluluk tekniği farkı nedeniyle önem taşımaktadır. Nitekim içerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur¹⁷. Yer sağlayıcı bakımından güvenli liman ise depolama esaslı bir varsayım üzerine kurulmakta; yer sağlayıcı, yer sağladığı içeriği kural olarak kontrol etmek veya hukuka aykırı faaliyeti araştırmakla yükümlü olmamakta; buna karşılık hukuka aykırı içerikten haberdar edildiğinde içeriği yayından çıkarması beklenmektedir¹⁸. Doktrinde bu tasarımın, yer sağlayıcıya genel bir gözetim yükümlülüğü yüklenmemesi ve sorumluluğun bildirim (haberdar edilme) eşiği üzerinden işletilmesi anlamına geldiği kabul

¹⁵ 5651 sayılı Kanun, m. 2/f, 2/n, 2/d, 2/l, 2/j.

¹⁶ 5651 sayılı Kanun, m. 2/f, m. 2/g, m. 2/j.

¹⁷ 5651 sayılı Kanun, m. 4/1.

¹⁸ 5651 sayılı Kanun, m. 5/1-5/2.

edilmektedir¹⁹. Bu tercih, ihlale müdahalenin de kural olarak olay sonrası işletilecek usuller üzerinden yürütülmesini zorunlu kılmakta; kişilik hakları bakımından bu usulî hattın merkezinde ise m. 9 düzenlemesi yer almaktadır.

Anayasa Mahkemesi, 11.10.2023 tarihli kararıyla 5651 sayılı Kanun'un 9. maddesini kademeli müdahale yönteminin bulunmaması ve usulî güvence eksiklikleri gerekçesiyle tümüyle iptal etmiştir²⁰. İptal hükmü 10.10.2024 itibarıyla yürürlüğe girmiş olup bu çalışma hazırlanırken m. 9'u ikame eden bir kanunî usul bulunmamaktadır²¹. İptal kararının gerekçeleri ve sonuçları aşağıda Bölüm III.B'de ayrıntılı olarak ele alınmaktadır.

Bu arka plan, 5651 sayılı Kanun'un üretken yapay zekâ bakımından iki noktada zorlandığını belirginleştirmektedir. Birincisi, aktör sınıflandırmasının ürün tasarımına göre değişkenlik göstermesidir. İkincisi, risk temelli bir çerçeve bulunmadığından müdahale araçlarının çoğu kez içeriğin çıkarılması veya erişimin engellenmesi ikiliğine sıkışmasıdır. Üstelik yer sağlayıcı güvenli limanının dayandığı depolamaya ilişkin varsayım, kullanıcı komutuna yanıt olarak yeni içerik üreten sistemlerin çekirdek işleviyle örtüşmemektedir²².

B. AB

AB hukukunda aracı sorumluluğu rejimi, 2000/31/AT sayılı Elektronik Ticaret Direktifi (E-Ticaret Direktifi) ile kurulmuş; ABAD içtihadıyla pasif aracılık ile bilgi ve kontrol ölçütleri üzerinden somutlaştırılmış; nihayet 2022/2065 sayılı Dijital Hizmetler Tüzüğü (Digital Services Act, DSA) ile tüzük düzeyinde yeniden yapılandırılmıştır. DSA'nın genel uygulama tarihi 17 Şubat 2024'tür²³. Üretken yapay zekâ bakımından DSA'daki güvenli limanların ve aktif rol ölçütünün uygulanabilirliğini değerlendirmek için, muafiyet tekniğinin dayandığı üçüncü taraf içeriği varsayımını ve bu varsayımın ABAD kararlarında nasıl somutlaştırıldığını dikkate almak gerekir²⁴. DSA, E-Ticaret Direktifi dönemin-

¹⁹ Ahunor Açıkgoz ve Murat Gürel, 'Başkasına Ait İçerikteki Fikrî ve Sınai Hak İhlalleri Nedeniyle Dijital Platformların Hukukî Sorumluluğu' (2024) 82 İstanbul Hukuk Mecmuası 693, 715; Yusuf Başlar (n 2) 611; Mehmet Bedii Kaya, *İnternet Hukuku* (2 Baskı, On İki Levha Yayıncılık 2021) 153.

²⁰ AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 101, 106; İsmail Demez (n 4) 185, 191.

²¹ RG, T. 10.01.2024, S. 32425 194; 5651 sayılı Kanun (mevzuat.gov.tr güncel metin, erişim 24 Ocak 2026) 2007, m. 9.

²² David Atkinson ve Jacob Morrison (n 1) 9.

²³ Digital Services Act, m. 93/2.

²⁴ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) 2000, dibace 42; ABAD, Google France, C-236/08, T. 23.03.2010, para. 112-114; Digital Services Act, dibace 18.

den sonra üye devletlerde giderek farklılaşan ulusal özen yükümlülüklerinin iç pazarda parçalanma ve hukuki belirlilik sorunları doğurduğu tespitinden hareketle, aracı hizmetlere ilişkin ortak kuralları güncellemekte ve yeknesaklaştırmaktadır²⁵. Komisyon, DSA Teklifi'nde (COM(2020) 825 final) güvenli liman kurallarının tüzük düzeyinde yeniden kurulmasını, uyumlaştırmayı güçlendirme ve parçalanmayı önleme gerekçeleriyle ayrıca temellendirmiştir²⁶.

1. E-Ticaret Direktifi ve ABAD İçtihadı

Komisyon'un E-Ticaret Direktifi'ne ilişkin 1998 tarihli teklifinde, çevrimiçi hizmet sağlayıcıların üçüncü kişi bilgisini iletme ve depolama faaliyetleri bakımından sorumluluğuna ilişkin belirsizlik özellikle vurgulanmış; bu nedenle üye devletlerde ortaya çıkan farklı yaklaşımları uyumlaştırmak amacıyla salt iletme (mere conduit) ilişkin muafiyet ile diğer aracı faaliyetler bakımından sorumluluğu sınırlayan bir çerçeve önerilmiştir²⁷.

E-Ticaret Direktifi, bilgi toplumu hizmetleri bakımından (i) salt iletim, (ii) önbellekleme ve (iii) barındırma için ayrı muafiyet şartları getirmiş; ayrıca aracı hizmet sağlayıcılara ilettikleri veya depoladıkları bilgileri genel olarak izleme yahut hukuka aykırı faaliyeti gösteren olguları aktif olarak araştırma yükümlülüğü yüklenemeyeceğini düzenlemiştir²⁸. Muafiyetlerin dayandığı varsayım, sağlayıcının faaliyeti salt teknik, otomatik ve pasif kaldığı sürece üçüncü kişilerce sağlanan bilgi üzerinde bilgi veya kontrol sahibi sayılmamasıdır²⁹.

Bununla birlikte Direktif, içeriğin çıkarılması veya erişimin engellenmesine ilişkin usulü yeknesak bir şekilde kodifiye etmemiş; hızlı ve güvenilir usullerin esasen tarafların gönüllü düzenlemeleri ve ulusal prosedürler üzerinden gelişmesini öngörmüştür³⁰. Ayrıca muafiyet hükümleri, ihlalin sonlandırılmasına

²⁵ Digital Services Act, dibace 1; Digital Services Act, dibace 2; Digital Services Act, dibace 4; European Commission, 'European Commission, Commission Staff Working Document: Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' (2020) SWD(2020) 348 final 90, 117 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0348>>.

²⁶ European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC 2020 3; DSA Proposal 7.

²⁷ European Commission, Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market 1998 27.

²⁸ E-Commerce Directive, m. 12-15; E-Commerce Directive, dibace 47.

²⁹ E-Commerce Directive, dibace 42.

³⁰ E-Commerce Directive, dibace 46.

veya önlenmesine yönelik yargısal veya idari emirleri (injunction) dışlamaz; muafiyet ile giderim yolları arasındaki ayrım özellikle vurgulanmıştır³¹.

ABAD, Direktif'in bu çekirdeğini 2010-2021 arasında bir dizi kararla somutlaştırmıştır. Google France (23.03.2010) kararında aracı rolün salt teknik, otomatik ve pasif niteliğini ve bilgi ve kontrol ölçütünü; L'Oréal v eBay (12.07.2011) kararında ise satış tekliflerinin sunumunu optimize etme ve tanıtma gibi faaliyetlerin aktif role işaret edebileceğini vurgulamıştır³². Scarlet Extended (24.11.2011) kararı, genel filtreleme yükümlülüğünün genel izleme yasağı ve temel haklar çerçevesinde sınırlandırılması gerektiğini ortaya koymuştur³³. Glawischnig-Piesczek (03.10.2019) kararı, özdeş veya eşdeğer içerik emirlerinin genel gözetim yasağıyla ilişkisini tartışmaya açmış; YouTube ve Cyando (22.06.2021) kararı ise otomatik indeksleme ve öneri işlevlerinin tek başına hukuka aykırılık hakkında belirli bir bilgi sonucunu doğurmadığını belirterek bilgi standardını daha da netleştirmiştir³⁴.

2. Dijital Hizmetler Tüzüğü (DSA)

DSA, E-Ticaret Direktifi sonrasında özellikle hukuka aykırı içerik, dezenformasyon ve diğer toplumsal riskler bakımından üye devletlerde ortaya çıkan farklı özen yükümlülüklerinin iç pazarı olumsuz etkilediği tespitinden hareketle, aracı hizmetlere ilişkin kuralları tüzük düzeyinde yeknesaklaştırmaktadır³⁵. Bu kapsamda DSA, salt iletim, önbellekleme ve barındırma muafiyetlerini ve genel gözetim yasağını korumakta; ayrıca muafiyetlerin sınırını aktif rol ölçütü üzerinden açıkça ifade etmektedir³⁶. Nitekim DSA m. 89 ile E-Ticaret Direktifi'nin 12 ila 15. maddeleri yürürlükten çıkarılmıştır³⁷. Buna ek olarak özellikle çevrimiçi platformlar ve çok büyük çevrimiçi platformlar için kademeli özen yükümlülükleri öngörülmektedir³⁸. Barındırma hizmeti, hizmet alıcısının talebi üzerine sağlanan bilginin depolanması olarak tanımlanmaktadır³⁹. Muafiyet koşulları,

³¹ E-Commerce Directive, dibace 45.

³² ABAD, Google France, C-236/08, T. 23.03.2010 (n 24), para. 112-114; ABAD, L'Oréal v eBay, C-324/09, T. 12.07.2011, para. 113-116.

³³ ABAD, Scarlet Extended, C-70/10, T. 24.11.2011, para. 40, 46-48, 51-52.

³⁴ ABAD, Glawischnig-Piesczek, C-18/18, T. 03.10.2019, para. 53; ABAD, YouTube ve Cyando, Birleşik Davalar C-682/18 ve C-683/18, T. 22.06.2021, para. 114-115.

³⁵ Digital Services Act, dibace 2; Digital Services Act, dibace 4.

³⁶ Digital Services Act, m. 4-6, 8, 89; Digital Services Act, dibace 18.

³⁷ Digital Services Act, m. 89.

³⁸ Digital Services Act, dibace 3.

³⁹ Digital Services Act, m. 3/g-(iii).

hukuka aykırı faaliyet veya içeriğe ilişkin fiili bilgiye sahip olmama ya da bu bilgiyi edindiğinde derhal içeriği kaldırma veya erişimi engelleme şeklinde belirlenmektedir⁴⁰. Kritik unsur, muafiyetin kapsamını belirleyen üçüncü taraf içerik şartıdır; muafiyet yalnızca hizmet alıcısının talebi üzerine sağlanan bilgi bakımından geçerli olmaktadır.

DSA'nın üretken yapay zekâ ürünlerine uygulanabilirliği, iki aşamalı bir nitelendirme sorununa işaret etmektedir: öncelikle hizmetin aracı hizmet olarak değerlendirilip değerlendirilemeyeceği; ardından bu kabul hâlinde barındırma hizmeti, çevrimiçi platform veya çevrimiçi arama motoru gibi alt türlerden hangisine daha yakın olduğudur. İlk değerlendirmelerde üç unsur öne çıkmaktadır: (i) sohbet robotlarının (chatbot) çıktı üretiminin, barındırma muafiyetinin dayandığı hizmet alıcısının talebi üzerine depolanan bilgi varsayımıyla ne ölçüde örtüştüğü, (ii) üçüncü taraf kaynaklara erişim, indeksleme veya arama benzeri fonksiyonların bulunup bulunmadığı ve (iii) sürüm ve özellik farklılıklarının (örneğin sabit veri setiyle çalışan bir sürüm ile internet tarama ve indeksleme içeren bir sürüm ayrımı) sınıflandırmayı etkileyip etkilemediği⁴¹.

Bu çerçeve, DSA'nın üretken yapay zekâyı salt çıktıdan doğan bir sorumluluk meselesine indirmek yerine, içerik yönetişimini usulî ve kurumsal özen yükümlülükleri üzerinden ele aldığını göstermektedir. Bu nedenle yanlış bilgi, manipülasyon veya derin sahte gibi çıktı-temelli kötüye kullanım senaryolarında tartışma, muafiyetin varlığı veya yokluğu ikiliğinin ötesinde, risk azaltım, şeffaflık ve bildirim ve işlem mekanizmasının (notice-and-action) hangi ürün katmanında ve hangi süreç güvenceleriyle işletilebileceği sorusuna odaklanmalıdır⁴².

Ampirik bulgular, üretken yapay zekâ araçlarının yanlış bilgi üretimini yalnızca örgütlü aktörler için değil, gelir ve etkileşim motivasyonu ile hareket eden bireysel üreticiler için de ucuzlaştırıp ölçeklenebilir kıldığını göstermektedir. Bu tespit, DSA'daki sistemik risk yaklaşımının salt tekil içeriklerin kaldırılmasına indirgenen bir refleksle sınırlanamayacağını; yanlış bilginin üretim-dağıtım döngüsünü besleyen teşvik yapıları ve pazarlama taktiklerini de hedefleyen kurumsal

⁴⁰ Digital Services Act, m. 6/1.

⁴¹ Laureline Lemoine ve Mathias Vermeulen, 'Assessing the extent to which Generative AI falls within the scope of the Digital Services Act: an initial analysis' (2023) draft 6-8; Beatriz Botero Arcila, 'Is It a Platform? Is It a Search Engine? It's ChatGPT! The European Liability Regime for Large Language Models' (2023) 3 Journal of Free Speech Law 455, 483-485.

⁴² Digital Services Act, m. 16/2; Ioannis Revolidis, 'Generative AI Content Misuse and the DSA' (Universitat Oberta de Catalunya 2024) 8; Forbrukerrådet, 'Ghost in the Machine: Addressing the consumer harms of generative AI' (2023) 21.

ve operasyonel tedbirlerin önem kazandığını desteklemektedir⁴³. Sohbet arayüzlerinin reklamla bütünleşmesi ve etkileşimin ticarileşmesi, üretken sistemlerin yalnızca çıktı üretimi bakımından değil, teşvik ve görünürlük tasarımı bakımından da düzenleyici değerlendirmeyi tetikleyebileceğini göstermektedir⁴⁴.

Bir yaklaşım, üretken yapay zekâyı (i) bağımsız (self-standing) bir hizmet olarak piyasaya sunulan ürün ve (ii) arama motoru veya çevrimiçi platform gibi mevcut bir aracı hizmetin içine gömülü (embedded) bir özellik veya işlev olarak sunulan hizmet şeklinde ikiye ayırmayı önermektedir. İkinci senaryoda sınıflandırma, çoğu kez sohbet robotundan ziyade ona ev sahipliği yapan aracı hizmetin (örneğin arama motoru veya platform) niteliği üzerinden yapılır; bu da üretken yapay zekâ fonksiyonunun çok büyük çevrimiçi platform veya çok büyük çevrimiçi arama motoru yükümlülüklerini tetikleyip tetiklemeyeceğini belirleyen kritik bir eşik oluşturur⁴⁵.

Bu bağlamda sohbet robotunun arama motoru hizmetinin bir parçası sayılması (Bing Chat is Bing), DSA kapsamındaki arama motoru yükümlülüklerinin doğrudan devreye girebileceğini göstermektedir. Buna karşı, sohbet robotunun ayrı bir hizmet olarak nitelendirildiği itirazlarda dahi, arama motoruyla fonksiyonel bütünleşme ve kullanıcıların aynı arayüzde hizmete erişmesi nedeniyle düzenleyici sorumluluğun alternatif bir bağlantı üzerinden yeniden kurulabileceği tartışılmaktadır⁴⁶.

Üretken yapay zekâ çıktılarının kişiselleştirme, sıralama veya yönlendirme mantığıyla sunulduğu ürün tasarımlarında, sohbet robotu fonksiyonunun öneri sistemi benzeri bir kurgu içinde değerlendirilmesi de mümkündür; bu durumda kullanıcılara profilemeye dayanan bir seçenek sunulmasının gündeme gelebileceği ileri sürülmektedir⁴⁷. Kötüye kullanım senaryolarının (yanlış bilgi, manipülasyon, derin sahte) çoğu kez dağıtım ve görünürlük katmanlarında yoğunlaştığı dikkate alındığında, tartışmanın ağırlık merkezinin çıktıyı kimin ürettiği sorusundan çok, risk tespiti ve azaltımının hangi ürün tasarımında hangi süreçlerle sağlanabileceğine kayması gerekir⁴⁸.

⁴³ Amelia Hassoun ve diğerleri, 'The Influencer Next Door: How Misinformation Creators Use GenAI' (arXiv:240513554 2024) 4.

⁴⁴ Fidji Simo, 'Reklamlara yaklaşımımız ve ChatGPT'nin ulaşılabilirliğini artırma hedefimiz' (OpenAI, 16 Ocak 2026) <<https://openai.com/tr-TR/index/our-approach-to-advertising-and-expanding-access/>>, Reklam ilkelerimiz.

⁴⁵ Laureline Lemoine ve Mathias Vermeulen (n 41) 2, 9-10.

⁴⁶ Ibid 10-11.

⁴⁷ Ibid 18.

⁴⁸ Ioannis Revolidis (n 42) 4; Amelia Hassoun ve diğerleri (n 43) 4.

Çok büyük çevrimiçi platformlar (VLOP) için özel yükümlülükler öngörülmektedir. Avrupa Birliği'nde aylık 45 milyon aktif kullanıcı eşliğini aşan platformlar, sistemik risk değerlendirmesi, bağımsız denetim ve veri erişimi gibi ek yükümlülüklerle tabidir⁴⁹. Üretken yapay zekâ fonksiyonlarının bir platform özelliği olarak sunulduğu örneklerde, platform sağlayıcısının tanımlanan riskleri azaltmak için tedbirler alma yükümlülüğü bulunduğu ve Komisyon'un üretken yapay zekâ risklerine ilişkin bilgi taleplerini seçili VLOP ve çok büyük çevrimiçi arama motoru sağlayıcılarına yönelttiği belirtilmektedir⁵⁰. Bu yaklaşım, üretken yapay zekâ işlevinin bağımsız bir hizmet olarak değil, gömülü bir özellik olarak konumlandığı ürün tasarımlarında, yükümlülüklerin sohbet robotundan ziyade ev sahibi aracı hizmet üzerinden işletilebileceğine işaret etmektedir⁵¹.

Genel gözetim yasağı, DSA'da da korunmaktadır: aracı hizmet sağlayıcılara ilettikleri veya depoladıkları bilgileri izlemelerine ya da hukuka aykırı faaliyet gösteren olguları aktif olarak aramalarına yönelik genel bir yükümlülük getirilemez⁵². ABAD, genel filtreleme yükümlülüğünün temel haklarla bağdaşmadığını tespit etmiştir⁵³. Özen yükümlülüklerinin sorumluluk sorusundan bağımsız nitelik taşıdığı vurgulanmaktadır⁵⁴.

Aktif rol ölçütü, DSA'da muafiyetlerin sınırını belirleyen bir ilke olarak açıkça ifade edilmektedir. Aracı hizmet sağlayıcının, hizmet alıcısı tarafından sağlanan bilgi üzerinde bilgi sahibi olmasını veya kontrol etmesini sağlayacak türde aktif bir rol oynaması halinde sorumluluktan muafiyet uygulanmaz⁵⁵. Güvenli liman, salt teknik, otomatik ve pasif nitelikteki davranışları korumaktadır⁵⁶. ABAD içtihadına göre reklam optimizasyonu potansiyel aktif rol teşkil etmekte⁵⁷, satış optimizasyonu ve listeleme düzenleme ise aktif rol oluşturmaktadır⁵⁸. Depolamanın salt teknik, otomatik ve pasif nitelikte olup olmadığı, mua-

⁴⁹ Digital Services Act, m. 33, 34, 37, 40.

⁵⁰ European Parliament, 'European Parliament, Answer P-002793/2025(ASW) Given by Executive Vice-President Virkkunen on Behalf of the European Commission (21 August 2025)' (2025) P-002793/2025(ASW) <https://www.europarl.europa.eu/doceo/document/P-10-2025-002793-ASW_EN.pdf> Erişim Tarihi 03 Şubat 2026, para. 1.

⁵¹ Laureline Lemoine ve Mathias Vermeulen (n 41) 9-10.

⁵² Digital Services Act, m. 8.

⁵³ ABAD, Scarlet Extended, C-70/10, T. 24.11.2011 (n 33), para. 40, 46-48, 51-52.

⁵⁴ Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Technology Law Journal 28.

⁵⁵ Digital Services Act, dibace 18.

⁵⁶ Giancarlo Frosio (ed) (n 11) 62.

⁵⁷ ABAD, Google France, C-236/08, T. 23.03.2010 (n 24), para. 114-116.

⁵⁸ ABAD, L'Oréal v eBay, C-324/09, T. 12.07.2011 (n 32), para. 113-116.

fiyetin işletilip işletilemeyeceği bakımından belirleyici ölçüt olarak öne çıkmaktadır⁵⁹. Bu bağlamda, yapay zekâ ile moderasyon yapılan günümüz çevrimiçi platformlarında pasif ve aktif ayrımının korunmasının yerinde olup olmadığı haklı olarak sorgulanmaktadır⁶⁰. İfade özgürlüğü denetimi bakımından da pasif aracılık varsayımının sınırları tartışmalıdır. Avrupa İnsan Hakları Mahkemesi (AİHM), Delfi AS v Estonya kararında, profesyonelce işletilen büyük ölçekli bir haber portalının anonim yorumlar bakımından yalnızca bildirim üzerine kaldırma mekanizmasına dayanmasını yeterli görmemiş; kullanılan filtreleme araçlarını ve öngörülebilirlik düzeyini sorumluluk değerlendirmesinde dikkate almıştır⁶¹. Buna karşılık Mahkeme, MTE ve Index.hu Zrt v Macaristan kararında, nefret söylemi veya şiddete teşvik içermeyen yorumlar bakımından katı sorumluluk yaklaşımının ölçüsüz sonuçlar doğurabileceğini; etkin usul güven-celeriyle desteklenen bildirim üzerine kaldırma mekanizmasının birçok durumda uygun bir denge aracı işlevi görebileceğini vurgulamıştır⁶². İyi niyetli gönüllü tedbirler tek başına güvenli liman kaybına yol açmamaktadır⁶³.

Yaptırım çerçevesi kapsamında, DSA ihlalleri için küresel yıllık cironun yüzde altısına varan idari para cezası öngörülmektedir⁶⁴. Çok büyük çevrimiçi platformlar (VLOP) ve çok büyük çevrimiçi arama motorları (VLOSE) bakımından Komisyon'un bilgi talebi ve denetim gibi soruşturma araçlarının yanı sıra geçici tedbir, taahhüt ve uyumsuzluk kararları yoluyla müdahalede bulunabileceği; ayrıca para cezası ve dönemsel para cezası mekanizmalarının öngörüldüğü anlaşılmaktadır⁶⁵.

DSA, paradigma dönüşümünü yansıtmaktadır: çevrimiçi platformların sorumluluğu hukuki sorumluluk alanından düzenleyici yükümlülük alanına taşınmaktadır⁶⁶. Sorumluluk muafiyetinin özen yükümlülüklerine uyumla ilişkilendirilmesi önerilmektedir⁶⁷. Sorumluluk çerçevesi başkalarının tüm haksız fiillerine fer'i nitelik taşırken, hesap verebilirlik çerçevesi yalnızca belirli yardımların

⁵⁹ Jaani Riordan (n 11) 30.

⁶⁰ Miriam C. Buiten (n 13), para. 37.

⁶¹ AİHM (Büyük Daire), Delfi AS v Estonia, B. No: 64569/09, T. 16.06.2015, para. 145-156, 157-160.

⁶² AİHM, Magyar Tartalomszolgáltatók Egyesülete (MTE) and Index.hu Zrt v Hungary, B. No: 22947/13, T. 02.02.2016, para. 64, 91.

⁶³ Digital Services Act, m. 7.

⁶⁴ Digital Services Act, m. 52/3.

⁶⁵ Digital Services Act, m. 67, 69-71, 73-74, 76.

⁶⁶ Miriam C. Buiten (n 13) 361.

⁶⁷ Miriam C. Buiten (n 13), para. 40.

sağlanmaması nedeniyle kusur atfetmektedir⁶⁸. Üretken yapay zekâ yönetişimi için hibrit yaklaşım gerektirdiği ve DSA'nın 16. maddesi ve devamındaki hükümlerin üretken yapay zekâ alanına acilen genişletilmesi gerektiği ileri sürülmektedir⁶⁹.

3. AB Yapay Zekâ Tüzüğü

AB Yapay Zekâ Tüzüğü, yapay zekâyâ özgü aktör kategorileri tanımlamaktadır. Sağlayıcı, bir yapay zekâ sistemi veya genel amaçlı yapay zekâ modeli geliştiren veya geliştiren ve bunu kendi adı veya markası altında piyasaya arz eden ya da hizmete sunan gerçek veya tüzel kişi, kamu otoritesi, ajans veya diğer kuruluştur⁷⁰. Kullanıma sunan, mesleki faaliyeti çerçevesinde kendi yetkisi altında bir yapay zekâ sistemini kullanan gerçek veya tüzel kişi, kamu otoritesi, ajans veya diğer kuruluştur⁷¹. Genel amaçlı yapay zekâ modeli, büyük miktarda veri kullanılarak ölçekli öz-denetimli öğrenme ile eğitilmiş, önemli derecede genellik gösteren ve geniş bir yelpazede farklı görevleri yerine getirebilen yapay zekâ modelidir⁷². Bu tanımlar, model geliştiricilere ve uygulama katmanına tekabül eden kategoriler oluşturmaktadır.

Risk temelli katmanlı yapı, AB Yapay Zekâ Tüzüğü'nün temel özelliğidir. Yasaklanmış yapay zekâ uygulamaları arasında sosyal puanlama sistemleri, kolluk amaçlı gerçek zamanlı uzaktan biyometrik tanımlama ve işyeri ile eğitim bağlamında duygu çıkarımı yer almaktadır⁷³. Yüksek riskli yapay zekâ sistemleri için uygunluk değerlendirmesi zorunluluğu, risk yönetim sistemi, veri yönetişimi ve teknik dokümantasyon gereklilikleri öngörülmektedir⁷⁴. Genel amaçlı yapay zekâ sağlayıcıları için teknik dokümantasyon, alt kullanıcı sağlayıcılara bilgi ve dokümantasyon sunma, telif hakkı uyum politikası ve eğitim verisi özeti yükümlülükleri belirlenmektedir⁷⁵. Standart genel amaçlı yapay zekâ sağlayıcılarının her zaman ayrıntılı teknik ve bilgilendirme dokümantasyonu sağlaması

⁶⁸ Martin Husovec (n 54) 28.

⁶⁹ Philipp Hacker, Andreas Engel ve Marco Mauer, 'Regulating ChatGPT and other Large Generative AI Models' (arXiv 2023) 1 <<https://arxiv.org/abs/2302.02337>>.

⁷⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 2024 (OJ L, 2024/1689, 12 July 2024), m. 3/3.

⁷¹ Artificial Intelligence Act, m. 3/4.

⁷² Artificial Intelligence Act, m. 3/63.

⁷³ Artificial Intelligence Act, m. 5/1 (c), (f), (h).

⁷⁴ Artificial Intelligence Act, m. 6, 9-11, 43, Ek III.

⁷⁵ Artificial Intelligence Act, m. 53/1 (a)-(d).

gerekmekte, bu sayede alt kullanıcıların sistemin kapasitelerini ve sınırlılıklarını anlaması mümkün kılınmaktadır⁷⁶. Sistemik risk taşıyan modeller için model değerlendirmesi, hasımca test, ciddi olay takibi ve raporlama ile siber güvenlik koruması gereklilikleri ek olarak öngörülmektedir⁷⁷. Üretken yapay zekâ sistemlerinin kendi başlarına genel risk kategorisi oluşturduğu değerlendirilmektedir⁷⁸. Hatanın konuşlandırma aşamasında bin kez düzeltilmesinin, soruna kaynağında bir kez müdahale edilmesinden daha verimsiz olduğu vurgulanmaktadır⁷⁹. Bu çerçevede, düzenlemenin ağırlık merkezinin piyasaya arz öncesi yükümlülükler ve idari yaptırım mekanizmaları olduğunu göstermektedir⁸⁰.

Rol dönüşümü kuralı, AB Yapay Zekâ Tüzüğü'nün kritik hükümlerinden birini oluşturmaktadır. Kullanıma sunan, belirli koşullarda sağlayıcıya dönüşebilmektedir: kendi adını veya markasını koyma, esaslı değişiklik yapma veya kullanım amacını yüksek riskli hale getirecek şekilde değiştirme hallerinde rol dönüşümü gerçekleşmektedir⁸¹. Esaslı değişiklik, piyasaya arzdan sonra yapılan, ilk uygunluk değerlendirmesinde öngörülmemiş ve uyum durumunu etkileyen değişiklik olarak tanımlanmaktadır⁸². 5651 sayılı Kanun'da benzeri bir rol dönüşümü kuralı bulunmamaktadır. DSA'da ise yükümlülükler hizmetin fiilî niteliğine göre kademeli olarak ağırlaşsa da, AB Yapay Zekâ Tüzüğü m. 25'teki gibi aktör statüsünü otomatik olarak değiştiren bir dönüşüm mekanizması öngörülmemiştir.

C. ABD

ABD'de aracı sorumluluğu tartışması, 1990'ların başında çevrimiçi hizmet sağlayıcıların üçüncü kişi kaynaklı içerikten hangi statüyle sorumlu tutulacağı sorusu etrafında şekillenmiştir. *Cubby v CompuServe* (1991) kararında aracı, daha çok dağıtıcı (distributor) mantığıyla değerlendirilmiş; *Stratton Oakmont v Prodigy* (1995) kararı ise içerik denetimi yapan bir hizmeti yayıncı (publisher) gibi nitelendirerek gönüllü moderasyon üzerinde caydırıcı bir etki doğurmuş-

⁷⁶ Claudio Novelli ve diğerleri, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity' [2024] *Computer Law & Security Review* 3.

⁷⁷ Artificial Intelligence Act, m. 55.

⁷⁸ Natali Helberger ve Nicholas Diakopoulos, 'ChatGPT and the AI Act' (2023) 12 *Internet Policy Review* 3.

⁷⁹ Philipp Hacker, Andreas Engel ve Marco Mauer (n 69) 22.

⁸⁰ Artificial Intelligence Act, m. 99.

⁸¹ Artificial Intelligence Act, m. 25/1.

⁸² Artificial Intelligence Act, m. 3/23.

tur⁸³. Kongre, bu teşvik bozukluğunu gidermek ve iyi niyetli içerik denetimini teşvik etmek amacıyla § 230'u kabul etmiştir⁸⁴. Erken dönem içtihat, özellikle Zeran v AOL (1997) çizgisinde, § 230'u geniş yorumlayarak bildirim sonrası gecikme ve ihmale dayalı taleplerin de çoğu kez kapsam içine alındığını göstermiştir⁸⁵.

Communications Decency Act (CDA) § 230, ABD'de aracılardan üçüncü kişi kaynaklı içerik nedeniyle yayıncı veya konuşmacı (publisher or speaker) sıfatıyla sorumlu tutulmasını kural olarak dışlayan temel normu oluşturmaktadır⁸⁶. Aynı maddede yer alan § 230(c)(2) ise sağlayıcıların iyi niyetli içerik denetimi kararlarına ayrı bir koruma tanıyarak, gönüllü moderasyonu teşvik eden iyi niyetli içerik denetimi güvencesini (Good Samaritan) kurumsallaştırmaktadır⁸⁷. Bu çerçevede, ABD modelinin ağırlık merkezinin kusur ve özen yükümlülüklerinden ziyade geniş kapsamlı bir bağışıklık tasarımıyla bulunduğu göstermektedir⁸⁸.

Uygulamada Section 230 savunması çoğu kez üç unsur etrafında kurulmaktadır: (i) davalının etkileşimli bilgisayar hizmeti (interactive computer service) sağlayıcısı veya kullanıcısı olması⁸⁹, (ii) ileri sürülen talebin davalıyı yayıncı veya konuşmacı gibi muameleye tabi tutması⁹⁰ ve (iii) ihtilaflı bilginin başka bir bilgi içerik sağlayıcısı (another information content provider) tarafından sağlanmış olması⁹¹. Bu çerçevede bilgi içerik sağlayıcısı (information content provider) tanımı, içeriğin oluşturulması veya geliştirilmesinden (creation or deve-

⁸³ Nandor F. R. Kiss, 'The Twenty-Six Words That Created the Internet ... and then Maybe, Kind Of, Destroyed Society: Understanding and Reforming Section 230 of the Communications Decency Act' (2024) 31 Michigan Technology Law Review 131, 139-141; Lucas Dini, 'Redefining Section 230 Immunity' (2024) 49 Seattle University Law Review 211, 213-215; Louis M. Shaheen, 'Section 230's Immunity for Generative Artificial Intelligence' (2024) unpublished manuscript 5-7.

⁸⁴ Nandor F. R. Kiss (n 83) 139-141; Lucas Dini (n 83) 213-215; Louis M. Shaheen (n 83) 5-7.

⁸⁵ Lucas Dini (n 83) 216-218; Dylan Varga, 'Section 230 and Generative AI: How (Not) to Regulate Algorithmic Defamation' (Honors thesis, Oregon State University 2024) 9; Nandor F. R. Kiss (n 83) 144.

⁸⁶ 47 U.S.C. § 230 (Communications Decency Act) s 230(c)(1).

⁸⁷ CDA § 230 s 230(c)(2).

⁸⁸ Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598; Nandor F. R. Kiss (n 83) 131-133; Lucas Dini (n 83) 213-215.

⁸⁹ CDA § 230 s 230(f)(2).

⁹⁰ CDA § 230 s 230(c)(1).

⁹¹ Haley Bernstein, 'Reconciling Section 230 and the First Amendment: Should Social Media Companies be Held Liable for the Consequences of Their Recommendation Algorithms?' (2023) 19 Journal of Business & Technology Law 11; Vincent Dumas, 'Enigma Machines: Deep Learning Algorithms as Information Content Providers under Section 230 of the Communications Decency Act' [2022] Wisconsin Law Review 1581, 1615; Kevin Ofchus, 'Cracking the Shield: CDA Section 230, Algorithms, and Product Liability' (2023) 46 University of Arkansas at Little Rock Law Review 27, 72.

lopment) bütünüyle veya kısmen sorumlu olmayı kapsadığından, tartışma çoğu kez öneri ve sıralama algoritmaları ile üretken modellerin ne ölçüde geliştirme faaliyeti yürüttüğü sorusunda yoğunlaşmaktadır⁹².

Öneri algoritmaları (recommendation) ve sıralama algoritmaları (ranking), Section 230 bağlamında özellikle kişiselleştirme yoluyla içeriğin görünürlüğünü artıran tasarımlarda ihtilaflı hâle gelmektedir. Bir yaklaşım, bu tür faaliyetleri yayıncılık fonksiyonunun teknik uzantısı olarak değerlendirerek bağımsızlığı koruma eğilimindeyken; karşı görüş, algoritmanın seçme ve önceliklendirme parametreleriyle hukuka aykırı sonuca maddi katkı sunması hâlinde sağlayıcının içeriğin geliştirilmesinden sorumlu tutulması ve bilgi içerik sağlayıcısı sayılması gerektiğini savunmaktadır⁹³. Bu tartışma, DSA'daki aktif rol doktrininin fonksiyonel bir karşılığı olarak görülebilse de, Section 230 bağlamında çoğu kez bağımsızlığın varlığı veya yokluğu ikiliği içinde daha keskin bir sınır tartışmasına dönüşmektedir⁹⁴.

Üretken yapay zekâ bakımından ihtilaf, üçüncü unsurun ve geliştirme ölçütünün nasıl işletileceğinde daha da görünür hâle gelmektedir. Bir görüş, sohbet robotlarının kullanıcı girdilerine yanıt olarak özgün metin ürettiğini; bu nedenle ortada başka bir bilgi içerik sağlayıcısından sağlanan bilginin yeniden yayımlanması değil, sağlayıcının bizzat geliştirdiği bir çıktı bulunduğunu ileri sürerek § 230 korumasının uygulanmaması gerektiğini savunur⁹⁵. Buna karşılık, diğer bir yaklaşım, üretken yapay zekâ servislerinin de belirli koşullarda etkileşimli bilgisayar hizmeti olarak nitelendirilebileceğini ve çıktılarının üçüncü taraf bilgi girdileri ile girdi zinciri üzerinden başka bir bilgi içerik sağlayıcısı şartını karşılayabileceğini ileri sürmektedir⁹⁶. Buna paralel biçimde, § 230'un üretken yapay zekâ için toptan dışlanmasının geniş yan etkiler doğurabileceği ve daha hedefli bir müdahale tasarımının tercih edilmesi gerektiği de belirtilmektedir⁹⁷. Bu nedenle ABD hukukunda ayrımın, yalnızca barındırma-üretim ikiliğinde değil, davalının tasarım tercihleriyle çıktının ne ölçüde geliştirildiği değerlendirmesinde toplandığı söylenebilir⁹⁸.

⁹² CDA § 230 s 230(f)(3); Vincent Dumas (n 91) 1615.

⁹³ Haley Bernstein (n 91) 11; Vincent Dumas (n 91) 1615; Kevin Ofchus (n 91) 72.

⁹⁴ Nandor F. R. Kiss (n 83) 131-133; Lucas Dini (n 83) 223-225.

⁹⁵ Hasala Ariyaratne (n 1) 8-9; Peter Henderson, Tatsunori Hashimoto ve Mark Lemley (n 1) 589.

⁹⁶ Louis M. Shaheen (n 83) 29-30.

⁹⁷ Dylan Varga (n 85) 36.

⁹⁸ Ellison Snider, 'Evolving Online Terrain in an Inert Legal Landscape: How Algorithms and AI Necessitate an Amendment of Section 230 of the Communications Decency Act' (2023) 107 Minnesota Law Review 1829, 1859; Vincent Dumas (n 91) 1615.

Son dönemde reform önerileri, algoritmik tavsiye sistemleri ve üretken yapay zekâ bağlamında Section 230 bağışıklığının kapsamını daraltmaya veya koşullandırmaya yönelmiştir. Akademik literatürde, en azından belirli tür algoritmik yükseltme (amplification) faaliyetlerinin veya yapay zekâ tabanlı içerik üretiminin kapsam dışı bırakılması ya da ayrı bir sorumluluk standardına bağlanması gerektiği savunulmaktadır⁹⁹. Bu tartışma, DSA'nın koşullu güvenli liman düzeni ile usulî ve kurumsal özen yükümlülükleri tasarımıyla karşılaştırıldığında, ABD modelinin sorumluluk (liability) yerine bağışıklık (immunity) eksenine yaslandığını ve üretken yapay zekâ yönetişimi bakımından normatif uyum sorunları ürettiğini göstermektedir¹⁰⁰.

II. HUKUKİ DEĞERLENDİRME

Üretken yapay zekâ sistemlerinin aracı sorumluluk rejimlerine entegrasyonu, hem Türk hukukunda hem de karşılaştırmalı hukuk düzleminde yapısal bağdaşmazlık sorunlarını gündeme getirmektedir. Bu bölümde, söz konusu bağdaşmazlığın hukuki temellerini ortaya koymak amacıyla Türk hukuku, Amerikan hukuku ve Avrupa Birliği hukuku çerçevesinde sorumluluk standartları incelenmekte; ardından bu standartların üretken yapay zekâ sistemlerine uygulanabilirliği değerlendirilmektedir.

A. Türk Hukuku Bakımından Değerlendirme

5651 sayılı Kanun, aracı hizmet sağlayıcıların sorumluluğunu düzenleyen temel çerçeveyi oluşturmaktadır. Kanun, internet aktörlerini içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, toplu kullanım sağlayıcı ve sosyal ağ sağlayıcı olarak sınıflandırır; bu tanımlar, sorumluluğun hangi aktör üzerinde hangi koşullarla doğacağını belirleyen başlangıç noktasıdır¹⁰¹.

Üretken yapay zekâ platformlarının bu aktör kategorileri içindeki konumu doktrinde tartışmalıdır. Bir yaklaşım, içerik sağlayıcı tanımındaki her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan unsurundan hareketle üretken yapay zekâ platformlarının içerik sağlayıcı sayılabileceğini; bunun da yer sağlayıcılara özgü güvenli liman korumasının (m. 5) uygulanamayacağı sonucunu doğuracağını ileri sürmektedir¹⁰². Buna karşılık içerik sağlayıcı tanımı, internet ortamı ve

⁹⁹ 'S. 1993 - No Section 230 Immunity for AI Act (2023)' (2023) s 1; Ellison Snider (n 98) 1859; Nandor F. R. Kiss (n 83) 131-133; Lucas Dini (n 83) 221.

¹⁰⁰ Miriam C. Buiten (n 13) 361.

¹⁰¹ 5651 sayılı Kanun, m. 2/f, 2/n, 2/d, 2/l, 2/j.

¹⁰² Yusuf Başlar (n 2) 609; 5651 sayılı Kanun, m. 2/f, 5.

internet ortamında yapılan yayın ölçütleriyle birlikte okunduğunda, kamuya açık internet ortamında gerçekleşmeyen kullanım senaryolarını (örneğin kullanıcının yalnızca kendi cihazında gerçekleştirdiği ve kamuya açık bir platformda yayımlamadığı üretimleri) doğrudan içerik sağlayıcı kategorisine yerleştirmek güçleşmektedir¹⁰³. Bu durum, kamusalılık ve yayına arz ölçütlerinin her üretken yapay zekâ kullanımında içerik sağlayıcı sıfatını kendiliğinden doğuran tek belirleyici olmadığını göstermektedir.

İçerik sağlayıcı ile yer sağlayıcı arasındaki temel ayrım, (i) içeriğin kaynağı ve (ii) içerik üzerindeki fiilî kontrol bakımından belirginleşir. İçerik sağlayıcı, internet ortamında kullanıma sunduğu içerikten kural olarak sorumludur; bağlantı sağladığı başkasına ait içerikten ise ancak sunuş biçimiyle içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça anlaşılıyorsa genel hükümlere göre sorumlu olur. Yer sağlayıcı ise depolama esaslı bir rejime tabidir ve kural olarak içerik kontrolü veya hukuka aykırılığı araştırma yükümlülüğü altında değildir; ancak hukuka aykırı içerikten haberdar edildiğinde ve teknik olarak imkân bulunduğu ölçüde içeriği yayından çıkarma yükümlülüğü doğar¹⁰⁴.

Yargıtay kararlarında da yer sağlayıcının sorumluluğunun, kural olarak hukuka aykırılıktan haberdar edilmesine rağmen içeriği yayından kaldırmama şeklindeki ihmali davranış üzerinden kurulduğu görülmektedir¹⁰⁵.

Üretken yapay zekâ sistemleri açısından bu sorumluluk modeli, yapısal bir uyumsuzluk barındırmaktadır. Üretken yapay zekâ, kullanıcı girdisine dayanarak özgün içerik üreten bir sistemdir ve bu durum, içeriği yalnızca barındıran yer sağlayıcılardan temel olarak farklıdır. 5651 sayılı Kanun'un 5. maddesindeki kontrol etme yükümlülüğü yoktur muafiyeti, içerik sağlayıcılara değil yer sağlayıcılara tanınmıştır¹⁰⁶. Bu nedenle üretken yapay zekâ çıktıları bakımından TBK'nın 66. maddesi kapsamında adam çalıştıranın sorumluluğu ve ürün sorumluluğu çerçevesinde alternatif sorumluluk temelleri değerlendirilmelidir¹⁰⁷.

Çevrimiçi telif ihlalleri bakımından FSEK, Ek m. 4 ile hak sahibinin başvurusu üzerine ihlale konu içeriğin çıkarılmasını ve bazı hâllerde hizmetin durdu-

¹⁰³ 5651 sayılı Kanun, m. 2/g, 2/ğ.

¹⁰⁴ 5651 sayılı Kanun, m. 4, 5/1-5/2.

¹⁰⁵ Ahunur Açıkgöz ve Murat Gürel (n 19) 728.

¹⁰⁶ Semih Yünlü, 'Üretici Yapay Zekâ Kaynaklı Norm ve Kişi Bazlı Hukuki Sorumluluk' (2024) 72 Adalet Dergisi 501, 533.

¹⁰⁷ Ibid 528, 535-536.

rulmasını içeren özel bir usul öngörür¹⁰⁸. Ne var ki doktrinde, (i) içerik sağlayıcının çoğu senaryoda ihlalin varlığını güvenilir biçimde tespit edememesi ve (ii) derhâl kaldırma ile kimlik bilgisi paylaşımı beklentisinin kişisel verilerin korunması ve kişilik hakları bakımından ikincil ihlaller doğurabilmesi nedeniyle bu usulün uygulamada sorun ürettiği vurgulanmaktadır¹⁰⁹.

Yukarıda belirtildiği üzere (bkz. Bölüm I.A), 5651 sayılı Kanun m. 9 Anayasa Mahkemesi tarafından iptal edilmiş ve 10.10.2024 itibarıyla yürürlükten kalkmıştır¹¹⁰. İptal kararının ayrıntılı değerlendirmesi ve yeni usul tasarımı ihtiyacı, aşağıda Bölüm III.B’de ele alınmaktadır. Bu noktada vurgulanması gereken husus, m. 9’un ortadan kalkmasıyla kişilik hakları bakımından 5651 sayılı Kanun’a özgü hızlı ve standartlaştırılmış başvuru hattının sona ermiş olmasıdır; TMK m. 24-25’e dayalı genel koruma talepleri ile ihtiyati tedbir yolu saklı olmakla birlikte¹¹¹, üretken yapay zekâ çıktılarına özgü müdahale ihtiyaçları dikkate alındığında standartlaştırılmış bir usulün yokluğu ayrıca sorun teşkil etmektedir.

Yer sağlayıcının sorumluluğunda bilgi standardının belirlenmesi, üretken yapay zekâ sistemleri bakımından kritik önem taşımaktadır. Türk hukukunda haberdar edilmenin şekli ve içeriği ile özel bir usul aranıp aranmadığı konusunda Yargıtay kararlarının farklılaştığı tespit edilmektedir. Bu belirsizlik, üretken yapay zekâ hizmetlerinde haberdar edilme eşiğinin öngörülebilir biçimde işlenmesini güçleştirmektedir¹¹².

Haksız fiil sorumluluğu, üretken yapay zekâ kaynaklı zararların tazmininde temel hukuki temeli oluşturmaktadır. TBK’nın 49. maddesine göre kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür¹¹³. Haksız fiilin unsurları fiil, hukuka aykırılık, zarar, illiyet bağı ve kusur olarak belirlenmektedir¹¹⁴. Bununla birlikte hukuka aykırılık her zaman haksız fiil formunda ortaya çıkmayabilir: taraflar arasında bir sözleşme ilişkisinin bulunduğu hâllerde, üretken yapay zekâ çıktısı aynı zamanda borca aykırılık (söz-

¹⁰⁸ Fikir ve Sanat Eserleri Kanunu (5846), Ek m. 4/3.

¹⁰⁹ Yusuf Başlar, ‘Fikir ve Sanat Eserleri Kanunu’nun Ek Madde 4 Hükümünün İhlali Suçları’ (2019) 77 Ankara Barosu Dergisi 37, 48.

¹¹⁰ AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 101, 106.

¹¹¹ Türk Medeni Kanunu (TMK), m. 24-25; Hukuk Muhakemeleri Kanunu (HMK), m. 389 vd.

¹¹² Ahunur Açıkgöz ve Murat Gürel (n 19) 731-732.

¹¹³ Türk Borçlar Kanunu (TBK), m. 49.

¹¹⁴ Semih Yünlü (n 106) 512.

leşmeye aykırılık) sorumluluğunu da gündeme getirebilir¹¹⁵. Kişilik hakkını koruyucu davaların kusuru olmayan kimseye yöneltilmesi mümkün olup, bu durum üretken yapay zekâ platformları bakımından önem taşımaktadır¹¹⁶.

TBK m. 66, adam çalıştıranın, çalışanın kendisine verilen işin görülmesi sırasında üçüncü kişilere verdiği zararlardan sorumluluğunu düzenlemektedir. Adam çalıştıran; çalışanı seçerken, işiyle ilgili talimat verirken, gözetim ve denetimde bulunurken zararın doğmasını engellemek için gerekli özeni gösterdiğini ispat ederse sorumlu olmaz; işletmede adam çalıştıran bakımından ise işletmenin çalışma düzeninin zararın doğmasını önlemeye elverişli olduğunu ispat etmedikçe işletmenin faaliyetleri dolayısıyla sebep olunan zararı gidermekle yükümlüdür¹¹⁷. Üretken yapay zekâ hizmetlerinde bu hükmün pratik karşılığı, insan unsurunun devreye girdiği süreçlerde (örneğin moderasyon kararları, şikâyetlerin değerlendirilmesi, müşteri desteği ve insan eğitmenlerin yürüttüğü etiketleme ve değerlendirme faaliyetleri) daha görünür hâle gelir. Çevrimiçi platformlar bakımından doktrinde, platformun bekçi (gatekeeper) konumu ve tüketicide yarattığı güvenin, özen değerlendirmesinde dikkate alınması gerektiği vurgulanmaktadır¹¹⁸.

Haksız fiil ve adam çalıştıranın sorumluluğunun ötesinde, üretken yapay zekâ çıktılarının ceza hukuku boyutu da ayrıca değerlendirilmelidir. Tüzel kişiler bakımından ceza sorumluluğu değil, şartları varsa güvenlik tedbirleri gündeme gelebilmektedir. TCK'nın 20. maddesinin ikinci fıkrasına göre tüzel kişiler hakkında güvenlik tedbirleri dışında cezaya hükmolunamaz¹¹⁹. Şirket bünyesinde kurulan ve faaliyet gösteren internet sùjelerinin çoğu kez tüzel kişiliğe sahip olması nedeniyle, ceza sorumluluğu bakımından şirket yetkililerinin sorumluluğu öne çıkmaktadır¹²⁰. Yapay zekâ ve yapay zekâlı varlıklar, kişilerin hayat, vücut dokunulmazlığı, özel yaşamın gizliliği, kişisel veriler, şeref ve malvarlığı gibi kişisel değerlerinin ihlal edilmesini ve bilişim suçlarının işlenmesini sağlayabilmektedir¹²¹. Ceza hukuku bakımından yapay zekânın belirli bir

¹¹⁵ Ibid 513.

¹¹⁶ Ibid 515.

¹¹⁷ TBK, m. 66.

¹¹⁸ Burcu Gülseren Özcan Büyüktanır, 'Çiçek Sepeti Kararı Özelinde Aracı Hizmet Sağlayıcısının Tüketicie Karşı Sorumluluğunun Değerlendirilmesi' (2025) 16 Türkiye Adalet Akademisi Dergisi 369.

¹¹⁹ Türk Ceza Kanunu (TCK), m. 20/2.

¹²⁰ Yusuf Başlar (n 2) 617.

¹²¹ Berrin Akbulut, 'Yapay Zeka ve Ceza Hukuku Sorumluluğu' (2023) 27 Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 270, 270-271.

amaca yönelik iradi olarak hareket edebildiği, mevcut gelişmeler açısından kabul edilmemekte; ceza hukuku hareket kabiliyeti gerektirdiğinden yapay zekânın hareket edebilme yeteneğinden söz edilememektedir¹²².

Ceza sorumluluğunun bu yapısal sınırları, üretken yapay zekâ kaynaklı zararların gideriminde kişisel verilerin korunması rejiminin ayrı bir önem kazanmasına yol açmaktadır. Kişisel verilerin korunması, üretken yapay zekâ sistemlerinin yarattığı sorumluluk boşluğunu doldurmada önemli bir normatif zemin sunmaktadır. 5651 sayılı Kanun'un depolama ve barındırma merkezli şeması üretken yapay zekâ eğitim ve çıktı yaşam döngüsünü doğrudan yakalamazken, KVKK doğrudan veri işleme faaliyetini hedeflemektedir¹²³. Günümüzde yapay zekâ platformlarının üretimler için ihtiyaç duyduğu verileri elde ederken kişisel verilerin korunması amacıyla konulan kurallara uydukları söylenememektedir¹²⁴. Yapay zekâ platformlarının üretilen içerikler için ham maddeye ihtiyaç duyduğu, bu ham maddenin çoğunlukla gerçek kişilere ilişkin kişisel veri niteliğindeki bilgiler olacağı ve bu durumda kişisel verilerin ihlaline ilişkin meselelerin ortaya çıkabileceği belirtilmektedir¹²⁵. Çevrimiçi platformların veri sorumlusu oldukları aşikârdır¹²⁶.

B. ABD Hukuku Bakımından Değerlendirme

Türk hukukundaki bu çok katmanlı sorumluluk yapısının karşılaştırmalı düzlemde değerlendirilmesi için, ABD hukukundaki muafiyet tartışmasına da bakılmalıdır. Amerikan hukukunda üretken yapay zekânın aracı sorumluluk muafiyetinden yararlanıp yararlanamayacağı, CDA § 230 çerçevesinde tartışmalıdır. § 230(c)(1), etkileşimli bilgisayar hizmeti sağlayıcısının veya kullanıcısının, başka bir bilgi içerik sağlayıcısı tarafından sağlanan bilgi nedeniyle yayıncı veya konuşmacı olarak muamele görmeyeceğini düzenlemektedir¹²⁷. Doktrinde ve uygulamada Section 230 savunmasının (i) davalının etkileşimli bilgisayar hizmeti sağlayıcısı veya kullanıcısı olması¹²⁸, (ii) talebin davalıyı yayıncı veya

¹²² Ibid 296-297.

¹²³ 5651 sayılı Kanun, m. 2/m, m. 5/2; Kişisel Verilerin Korunması Kanunu (6698), m. 3/d, m. 3/e; Semih Yünlü (n 106) 516-518.

¹²⁴ Semih Yünlü (n 106) 517.

¹²⁵ Ibid 518.

¹²⁶ Erman Ekingen ve Miray Özer Deniz, '7392 ve 7416 Sayılı Kanunlarla Yapılan Değişikliklerin Aracı Hizmet Sağlayıcı Olarak Çevrimiçi Çok Taraflı Platformların Sorumluluklarına ve Tüketicilere Etkileri' (2022) 69 Adalet Dergisi 456.

¹²⁷ CDA § 230 s 230(c)(1).

¹²⁸ CDA § 230 s 230(f)(2).

konusmacı gibi muameleye tabi tutması¹²⁹ ve (iii) ihtilaflı bilginin başka bir bilgi içerik sağlayıcısı tarafından sağlanmış olması unsurları etrafında kurulduğu kabul edilmektedir¹³⁰. Üretken yapay zekâ bağlamında gerilim, özellikle üçüncü unsurun ve geliştirme ölçütünün üretken sistemler bakımından nasıl kurulacağı noktasında yoğunlaşmaktadır¹³¹.

Bir görüşe göre sohbet robotları, kullanıcı girdilerine yanıt olarak özgün metin ürettiği için, üçüncü kişi içeriğinin pasif biçimde iletilmesinden söz edilemez; bu durumda sağlayıcının en azından çıktı düzeyinde bilgi içerik sağlayıcısı olarak değerlendirilmesi ve § 230 korumasının uygulanmaması gerekir¹³². Buna karşılık, üretken yapay zekâ servislerinin (en azından belirli kullanım biçimlerinde) etkileşimli bilgisayar hizmeti olarak nitelendirilebileceği ve çıktının üçüncü taraf bilgi girdileri ile girdi zinciri üzerinden başka bir bilgi içerik sağlayıcısından sağlanan bilgi şartını karşılayabileceği savunulmaktadır¹³³.

Doktrinde, arama ve ayıklama (retrieval) ile içerik üretimi (generation) ayırımının, § 230 analizinde hangi aktörün hangi çıktıdan sorumlu tutulacağı tartışması bakımından pratik bir başlangıç noktası sunduğu belirtilmektedir¹³⁴. Bununla birlikte modern platformlarda öneri ve sıralama sistemlerinin görünürlüğü aktif biçimde şekillendirmesi, algoritmaların geliştirme rolünün sınırlarını da tartışmalı hâle getirmektedir¹³⁵.

Başka bilgi içerik sağlayıcısı ibaresinin yorumu bu bağlamda belirleyicidir. Doktrinde, bu ibarenin davalı sağlayıcı dışında üçüncü kişiyi işaret ettiği; yapay zekâ sisteminin kavramsal olarak başka bir aktör gibi konumlandırılamayacağı; üçüncü taraf verilerle eğitilmiş olmanın tek başına çıktıyı üçüncü tarafın konuşması hâline getirmeyeceği vurgulanmaktadır¹³⁶. Bu nedenle değerlendirme, somut girdi-çıkıtı zincirinde davalının tasarım tercihleriyle çıktının ne ölçüde geliştirildiği üzerinden yürütülmelidir¹³⁷.

¹²⁹ CDA § 230 s 230(c)(1).

¹³⁰ Vincent Dumas (n 91) 1599.

¹³¹ CDA § 230 s 230(f)(3); Vincent Dumas (n 91) 1599.

¹³² Eugene Volokh (n 1) 495; Hasala Ariyaratne (n 1) 8-9.

¹³³ Louis M. Shaheen (n 83) 29-30.

¹³⁴ Peter Henderson, Tatsunori Hashimoto ve Mark Lemley (n 1) 622.

¹³⁵ Kevin Ofchus (n 91) 72; Vincent Dumas (n 91) 1615.

¹³⁶ Eugene Volokh (n 1) 495; Hasala Ariyaratne (n 1) 8-9.

¹³⁷ Vincent Dumas (n 91) 1615.

Bilgiye dayalı sorumluluk sistemi, son yirmi yılı aşkın süredir Avrupa Birliği'nin sosyal medya şirketleri, çevrimiçi pazar yerleri, bulut depolama sağlayıcıları ve kullanıcı tarafından üretilen içeriği depolayan ve yayan diğer birçok çevrimiçi hizmet sağlayıcının sorumluluğunu düzenleyen rejiminin omurgasını oluşturmuştur¹³⁸. Bu kural, 2000 yılında kabul edilen E-Ticaret Direktifi'nin 14. maddesinde düzenlenmiş olup, özellikle telif hakkı ihlali içeren kullanıcı içeriğine ilişkin olarak uygulanabilir olan ve 1998 tarihli Digital Millennium Copyright Act (DMCA) § 512(c) hükmünde yer alan Amerikan hukukundaki benzer bir kuraldan esinlenmiştir¹³⁹. Her iki yargı alanında da yasalar, hizmet sağlayıcıların kullanıcıları için depoladıkları içerikle ilgili sorumluluktan muaf tutulmalarını sağlamaktadır; ancak bunun koşulu içeriğin hukuka aykırılığı hakkında bilgiye sahip olmamaları ve bu bilgiye ulaştıklarında içeriği derhal kaldırmak için harekete geçmeleridir¹⁴⁰. Üretken yapay zekâ bağlamında DMCA güvenli limanı, pasif aracılık varsayımı ile model geliştirme ve konuşlandırma zincirinin çok aktörlü ve üretim odaklı niteliği arasındaki gerilim nedeniyle yeniden tartışılmaktadır; bu nedenle bağışıklığın üretken yapay zekâ tedarik zincirine uyarlanması amacıyla rol-temelli yapay zekâ güvenli limanı (AI harbour) tasarımları önerilmektedir¹⁴¹. Öte yandan telif korumasının giderek otomatik izleme ve filtreleme araçları üzerinden yürütülmesi, usulî güvenceler güçlendirilmedikçe aşırı kaldırma ve kötüye kullanım riskini büyütebilmektedir¹⁴².

Bu nedenle üretken yapay zekâ bağlamında mesele, muafiyetin kapsamını soyut olarak genişletmek veya daraltmaktan ziyade, telif şikâyetlerinin nasıl doğrulanacağına ve hatalı veya istismarcı bildirimlere karşı hangi güvencelerin işletileceğine ilişkindir¹⁴³. DSA'nın bildirim üzerine işlem mekanizmasının standartlaştırılmış, kolay erişilebilir ve kullanıcı dostu biçimde tasarlanması, otomatik telif izleme pratiklerinin aşırı yaptırım (over-enforcement) üretmesini

¹³⁸ Folkert Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Service Providers' (2021) 12 JIPITEC 317, 317.

¹³⁹ Ibid 318.

¹⁴⁰ Ibid.

¹⁴¹ Yang Lin ve Taorui Guan, 'From safe harbours to AI harbours: reimagining DMCA immunity for the generative AI era' (2025) 20 Journal of Intellectual Property Law & Practice 3, 605.

¹⁴² Chien-Chih Lu, 'From safe harbours to over-enforcement: the rise of AI and copyright monitoring' (2025) 20 Journal of Intellectual Property Law & Practice 7, 627; Jennifer M. Urban ve Laura Quilter, 'Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act' (2006) 22 Santa Clara Computer & High Technology Law Journal 621, 641; Ben Depoorter ve Robert Kirk Walker, 'Copyright False Positives' (2014) 89 Notre Dame Law Review 319, 341-345; Michael S. Sawyer, 'Filters, Fair Use and Feedback: User-Generated Content Principles and the DMCA' (2009) 24 Berkeley Technology Law Journal 363, 389-390.

¹⁴³ Yang Lin ve Taorui Guan (n 141) 609; Jennifer M. Urban ve Laura Quilter (n 142) 641; Ben Depoorter ve Robert Kirk Walker (n 142) 341-345.

sınırlayabilecek bir usulî dengeleme aracı olarak görülebilir¹⁴⁴. Aksi hâlde rol-temelli yapay zekâ güvenli limanı önerilerinin düşük kanıt standardı altında sansür güvenli limanı (censorship harbour) etkisi üretmesi ve ifade özgürlüğü ile yenilik ve rekabet üzerinde ikincil maliyetler doğurması olasıdır¹⁴⁵.

DMCA bildir-kaldır pratiğine ilişkin ampirik bulgular, süreç tasarımının hatalı veya tartışmalı bildirimlere açık olduğunu; hizmet sağlayıcıların güvenli limanı koruma refleksiyle kaldırma yönünde aşırı tedbirli davranmaya itilebildiğini göstermektedir¹⁴⁶. Benzer biçimde algoritmik telif filtreleri, özellikle adil kullanım (fair use) gibi bağlam-duyarlı istisna ve sınırlamaları sistematik olarak değerlendirmekte zorlandığından, otomatik ön-filtreye dayalı telif denetimi, itiraz, karşı bildirim ve insan gözetimiyle tamamlanmadığı ölçüde yanlış pozitif (false positive) maliyetlerini artırarak ifade özgürlüğü ve kamusal alan üzerinde sistemik bir aşınma doğurabilmektedir¹⁴⁷.

C. Karşılaştırmalı Değerlendirme

Üretken yapay zekâ sistemlerinin aracı sorumluluk muafiyetleriyle ilişkisi, her üç hukuk sisteminde de muafiyetlerin üzerinde yükseldiği kategori varsayımlarının sınırlarına işaret eder. Türk hukukunda yer sağlayıcı rejimi, depolama varsayımına ve haberdar edilme eşiğine dayandığından, çekirdek çıkarım işlevine doğrudan uygulanabilirliği sınırlıdır¹⁴⁸. Amerikan hukukunda ise § 230'un başka bir bilgi içerik sağlayıcısı tarafından sağlanan bilgi koşulu ile geliştirme (creation or development) ölçütü, üretken modeller bakımından bağışıklığın otomatik işlenmesini güçleştirmekte; bu nedenle doktrinde bağışıklığın kapsamına ilişkin farklı okumalara rastlanmaktadır¹⁴⁹. Avrupa Birliği hukukunda da DSA barındırma muafiyetini hizmet alıcısının talebi üzerine sağlanan bilginin depolanması şartına bağladığından, çıkarım yoluyla özgün çıktı üreten sistemleri barındırma tanımına doğrudan oturtmak güçleşmektedir¹⁵⁰.

¹⁴⁴ Digital Services Act, m. 16/1; Sharon Choi, 'Assessing the Efficacy of Third-Party Liability Copyright Doctrines against Platforms That Host AI-Generated Content' (2025) 66 Boston College Law Review 1087, 1123.

¹⁴⁵ Yang Lin ve Taorui Guan (n 141) 615; Chien-Chih Lu (n 142) 627; Jennifer M. Urban ve Laura Quilter (n 142) 641.

¹⁴⁶ Jennifer M. Urban ve Laura Quilter (n 142) 641; Ben Depoorter ve Robert Kirk Walker (n 142) 325.

¹⁴⁷ Ben Depoorter ve Robert Kirk Walker (n 142) 341-345; Michael S. Sawyer (n 142) 389-390.

¹⁴⁸ 5651 sayılı Kanun, m. 2/m, m. 5/1-5/2; Semih Yünlü (n 106) 534; David Atkinson ve Jacob Morrison (n 1) 9.

¹⁴⁹ CDA § 230 ss 230(c)(1), (f)(3); Hasala Ariyaratne (n 1) 8-9; Louis M. Shaheen (n 83) 29-30.

¹⁵⁰ Digital Services Act, m. 6; Laureline Lemoine ve Mathias Vermeulen (n 41) 5; Beatriz Botero Arcila (n 41) 483-485.

Bu nedenle tartışma, muafiyetin uygulanıp uygulanmayacağından önce, muafiyet tekniğinin dayandığı üç temel varsayımın üretken sistemlerde geçerliliğine odaklanmalıdır. Yapısal bağdaşmazlık üç düzlemde görünür hâle gelmektedir. Birincisi, muafiyetlerin üçüncü taraf içeriği varsayan tasarımı, üretken sistemlerde başkasınca sağlanan bilgi koşulunu karşılamaz; bu nedenle hem 5651 sayılı Kanun hem DSA hem de § 230 bakımından muafiyet mantığı çekirdek çıkarım katmanına doğrudan taşınamaz¹⁵¹. İkincisi, ihlal bildirimi üzerine münferit içerik ögesinin çıkarılabileceği varsayımına dayanan yaklaşım, model ağırlıkları düzeyinde teknik bir karşılık bulmaz; zira bu katmanda silme işlemi çoğu kez belirli tür çıktıları istatistiksel olarak bastıran güvenlik teknikleriyle ikame edilmekte ve bu durum veri koruması ve unutulma hakkı bağlamında makine unutmaya tartışmasını da gündeme getirmektedir¹⁵². Üçüncüsü, muafiyetlerin arkasındaki pasif aracılık varsayımı, kişiselleştirme, öneri ve sıralama ile moderasyon gibi tasarım tercihleriyle zayıflamakta; AB hukukunda aktif rol tartışması bu gerilimin klasik örneğini oluşturmaktadır¹⁵³. Temel haklar arasında kurulacak denge, bu üç düzlemde tasarlanacak her türlü politika cevabının merkezinde yer almak zorundadır¹⁵⁴.

Sonuç olarak, üretken yapay zekâ sistemlerinin aracı sorumluluk rejimleriyle bağdaşmazlığı yorumsal değil tanımsal mahiyettedir. Bu sistemler, mevcut düzenleyici çerçevelerin temel varsayımlarını (üçüncü taraf içeriği barındırma, münferit içerik kaldırma imkânı, pasif aracılık) karşılayamamaktadır. Türk hukuku bakımından sonuç şudur: 5651 sayılı Kanun, esasen ihlalin sona erdirilmesine dönük usulî müdahale araçlarını (içeriğin çıkarılması, erişimin engellenmesi) düzenler; buna karşılık zararların tazmini ve yaptırım sorumluluğu, TBK, TCK, KVKK ve FSEK'in maddi hukuk hükümleri üzerinden kurulmalıdır.

¹⁵¹ 5651 sayılı Kanun, m. 5/1-5/2; Digital Services Act, m. 6; CDA § 230 ss 230(c)(1), (f)(3); Hasala Ariyaratne (n 1) 8-9.

¹⁵² Thanh Tam Nguyen ve diğerleri (n 8) 5, 9-10; Yinzhi Cao ve Junfeng Yang (n 7) 1-2; Chuan Guo ve diğerleri (n 7) 1-2; Lucas Bourtole ve diğerleri (n 8) 2, 5, 10; Ayush Sekhari ve diğerleri (n 8) 1-2; David Atkinson ve Jacob Morrison (n 1) 9; Claudio Novelli ve diğerleri, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity' (2024) Working Paper 13; Philipp Hacker, 'AI Regulation in Europe: From the AI Act to Future Regulatory Challenges' (arXiv:231004072 2023) 18.

¹⁵³ Miriam C. Buiten (n 13), para. 34; ABAD, Google France, C-236/08, T. 23.03.2010 (n 24), para. 112-114; ABAD, L'Oréal v eBay, C-324/09, T. 12.07.2011 (n 32), para. 113-116.

¹⁵⁴ Christophe Geiger, Giancarlo Frosio ve Elena Izyumenko, 'Intermediary Liability and Fundamental Rights' [2019] CEIPI Research Paper No. 2019-06 1.

III. TÜRK HUKUKUNDA UYGULAMA

Üretken yapay zekâ hizmetlerinin Türk hukukundaki konumu, 5651 sayılı Kanun'daki internet sùjeleri tasnifinin üretim temelli hizmetlere uygulanmasındaki güçlükler nedeniyle, önceki bölümlerde tartışılan sorumluluk standardının somut normatif rejimlere nasıl tahsis edileceği sorusunu gündeme getirir¹⁵⁵. Bu bölüm, üretken yapay zekâ değer zincirinde 5651 sayılı Kanun, TBK, TCK, KVKK ve FSEK hükümlerinin hangi katmanlarda devreye girdiğini incelemektedir.

A. Katman ve Aktör Haritası

Üretken yapay zekâ hizmetlerinde zarar genellikle model geliştirme ve güncelleme, hizmet konuşlandırma ve arayüz tasarımı ile kullanıcı girdileri ve yayım tercihleri katmanlarının kesişiminde doğar¹⁵⁶. Bu nedenle uyumsuzluğu tek bir aracı sorumluluk rejimine indirgeyip yükü tek bir aktörde yoğunlaştırmak, çoğu senaryoda hukuki durumu yeterince açıklamaz¹⁵⁷. Aşağıdaki tablo, üretken yapay zekâ değer zincirini aktör ve katman düzeyinde betimlemekte ve her katmanda temas eden başlıca norm setlerini göstermektedir.

Aktör	Katman ve işlev	İlgili norm seti
Model sağlayıcı	Eğitim, ağırlık, çıkarım	KVKK, TBK
Konuşlandırıcı	Arayüz, barındırma, moderasyon	5651 sayılı Kanun, TBK, KVKK
Son kullanıcı	Girdi, paylaşım, yayınlama	TCK, TBK

Tablo 3.1: Üretken yapay zekâ değer zinciri (aktör-katman-norm seti)

Bazı konuşlandırma senaryolarında model sağlayıcı ile konuşlandırıcı arasına ince ayar (fine-tuning) yapan ayrı bir aktör girebilir; bu durumda sorumluluk değerlendirmesi, üçlü şemayı daha ayrıntılı bir tahsis mantığıyla okumayı gerektirir¹⁵⁸. İnce ayar veri setinin oluşturulması ve modelin belirli bir kullanım amacına uyarlanması, teknik olarak çoğaltma ve işleme fiilleriyle temas edileceğinden, KVKK ile birlikte FSEK bakımından eğitim verisinin kullanımı ve

¹⁵⁵ Semih Yünlü (n 106) 533.

¹⁵⁶ Jennifer Cobbe ve Jatinder Singh, 'Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges' (2021) 42 Computer Law & Security Review 105573, 5-6.

¹⁵⁷ Semih Yünlü (n 106) 533.

¹⁵⁸ Jennifer Cobbe ve Jatinder Singh (n 156) 5-6; Philipp Hacker (n 152) 11.

çıktı ikamesi tartışmalarını da gündeme getirebilir¹⁵⁹. Sorumluluğun hangi ölçütlerle tahsis edileceği takip eden bölümde ayrıca ele alınacaktır.

Model sağlayıcı bakımından, eğitim veri setlerinin kişisel veri içermesi hâlinde veri sorumlusu ile veri işleyen ayrımı ile işleme şartları KVKK çerçevesinde değerlendirilir¹⁶⁰. Bununla birlikte model parametrelerinin (ağırlıkların) kişisel veri olup olmadığı, veri setini özdeş kabul ederek değil, ağırlıkların kişiyi belirlenebilir kılıp kılmadığı sorusu üzerinden tartışılmalıdır. Nitekim AB düzeyinde Avrupa Veri Koruma Kurulu (European Data Protection Board - EDPB), kişisel verilerle eğitilmiş bir modelin her durumda anonim sayılamayacağını; anonimlik değerlendirmesinin kişisel verinin modelden geri çıkarılabilirliği ve modelin erişime açılma bağlamı dikkate alınarak somut olayda yapılması gerektiğini vurgulamaktadır¹⁶¹. Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor - EDPS) de üretken sistemlerde kişisel verinin yalnızca eğitim aşamasında değil, dağıtım aşamasında girdi-çıktı düzeyinde ve eğitim verisinin model tarafından ezberlenmesi (memorisation) yoluyla da ortaya çıkabileceğine işaret eder¹⁶². Benzer biçimde Kurum'un anonimleştirme rehberi, anonim hâle getirmeyi, verinin veri sorumlusu veya alıcı gruplar tarafından geri döndürülmesi yahut başka veri setleriyle birleştirilmesi ihtimali dâhil olmak üzere, ilgili faaliyet alanında makul yöntemlerle dahi kimliği belirli veya belirlenebilir bir kişiyle ilişkilendirilememesi olarak açıklamakta; ayrıca tersine işlem yoluyla anonimliğin bozulması riskine özellikle işaret etmektedir¹⁶³. Bu değerlendirmeler, KVKK bakımından da model parametrelerinin kişisel veri niteliği tartışmasında belirlenebilirlik ölçütü ile kişisel verinin modelden fiilen

¹⁵⁹ FSEK, m. 6, m. 21; Osman Gazi Güçlütürk, *Yapay Zekâ ve Verinin Kullanımı* (1 Baskı, On İki Levha Yayıncılık 2022) 238-239, 265.

¹⁶⁰ KVKK, m. 3/d, m. 3/e; Kişisel Verileri Koruma Kurumu, *Veri Sorumlusu ve Veri İşleyen* (KVKK Yayınları No: 106, Haziran 2025) 5-14.

¹⁶¹ European Data Protection Board, 'Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models' (2024) Opinion 28/2024 13-14, 16-17 <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf> Erişim Tarihi 25 Ocak 2026.

¹⁶² European Data Protection Supervisor, 'Generative AI and the EUDPR: Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems (Version 2)' (2025) 12 <https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf> Erişim Tarihi 25 Ocak 2026; Isabel Barberá, 'AI Privacy Risks & Mitigations - Large Language Models (LLMs)' (European Data Protection Board (Support Pool of Experts Programme) 2025) 72 <<https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf>> Erişim Tarihi 25 Ocak 2026.

¹⁶³ Kişisel Verileri Koruma Kurumu, 'Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi' (KVKK Yayınları No: 71 2025) 25-26, 48-49 <<https://www.kvkk.gov.tr/Icerik/2038/kisisel-verilerin-silinmesi-yok-edilmesi-veya-anonim-hale-getirilmesi>> Erişim Tarihi 25 Ocak 2026.

geri çıkarılabilme riskinin birlikte ele alınmasının yerinde olacağını göstermektedir¹⁶⁴. Nitekim Kişisel Verileri Koruma Kurumu, yapay zekâ uygulamalarında kişisel veriye ihtiyaç duyulmaksızın aynı sonuca ulaşabiliyorsa kişisel verinin hiç işlenmemesini; işleme zorunlu ise mümkün olan hâllerde anonimleştirme tercih edilmesini ve kullanıcıya kişisel verilerinin silinmesi, yok edilmesi veya anonimleştirilmesi imkânı tanıyan sistem tasarımlarının benimsenmesini tavsiye etmektedir¹⁶⁵.

Bunun yanı sıra, moderasyon ve şikâyet yönetimi gibi insan unsurunun belirgin olduğu işletim süreçlerinin nasıl kurulduğu ve denetlendiği, TBK m. 66 kapsamında adam çalıştıranın sorumluluğu ile işletmenin çalışma düzenine ilişkin ispat yükü bakımından önem kazanabilir¹⁶⁶.

Konuşlandırıcı, kullanıcı içeriğini barındırma ve yayımlama gibi işlevler bakımından, ilke olarak 5651 sayılı Kanun m. 5/2'de düzenlenen yer sağlayıcı yükümlülükleri çerçevesinde değerlendirilebilir¹⁶⁷. Bu rejim, haberdar edilme eşğine ve olay sonrası müdahale mantığına dayanır.

Konuşlandırıcı, girdi-çıkı yönetimi ve moderasyon tercihleri bakımından TBK m. 49'un kusur ve özen standardı altında da sorumluluğa açık hâle gelebilir¹⁶⁸. Ceza hukuku bakımından fail tespiti ise çoğu kez girdiyi kuran, çıktıyı paylaşan veya yayım kararını veren gerçek kişi üzerinde yoğunlaşır; tüzel kişi bakımından TCK m. 20/2 sınırı nedeniyle tartışma çoğu kez güvenlik tedbirleri veya gerçek kişi isnadı üzerinden yürür¹⁶⁹. Bu durum, özellikle çok aktörlü konuşlandırmalarda sorumluluğu tek bir aktöre doğrudan yükleyen yaklaşımların açıklayıcılığını azaltır.

B. 5651'in Uygulanabildiği Alan: Barındırma ve Yayın Özellikleri

5651 sayılı Kanun'da içerik sağlayıcı, internet ortamı üzerinden kullanıcılarla sunulan bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişi

¹⁶⁴ Semih Yünlü (n 106) 533.

¹⁶⁵ Kişisel Verileri Koruma Kurumu, 'Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence' (KVKK Yayınları No: 33 2024) 17, 19 <<https://www.kvkk.gov.tr/Shared-Folder-Server/CMSFiles/58678459-eba4-451a-a2f3-c1baf17b90f5.pdf>> Erişim Tarihi 25 Ocak 2026.

¹⁶⁶ TBK, m. 66; Fikret Eren, *Borçlar Hukuku Genel Hükümler* (21 Baskı, Yetkin Yayınları 2017) 721-732; Semih Yünlü (n 106) 528.

¹⁶⁷ 5651 sayılı Kanun, m. 5/2; Ahunur Açıkgoz ve Murat Gürel (n 19) 728.

¹⁶⁸ TBK, m. 49; Fikret Eren (n 166) 672.

¹⁶⁹ TCK, m. 20/2; Mahmut Koca ve İlhan Üzülmöz, *Türk Ceza Hukuku Genel Hükümler* (9 Baskı, Seçkin Yayıncılık 2016) 641.

olarak tanımlanmıştır¹⁷⁰. m. 2/g'de internet ortamı kamuya açık internet üzerinde oluşturulan ortam olarak tanımlandığından, bu bölümde 5651 sayılı Kanun bakımından tartışma, çıktının veya kullanıcı içeriğinin üçüncü kişilerin erişimine açıldığı kamuya açık servislerle sınırlı tutulmaktadır¹⁷¹. Kapalı devre kurum içi çözümler veya yalnızca belirli bir işletmenin çalışanlarına hizmet veren işletmeden işletmeye (business-to-business, B2B) araçlar, çoğu durumda m. 2/g'de tanımlanan internet ortamı şartını karşılamadığından 5651 sayılı Kanun rejimi kapsamında değerlendirilmez¹⁷².

Kamuya açık üretken yapay zekâ hizmetlerinde de özellik temelli bir ayrım zorunludur; konuşlandırıcının sunduğu barındırma işlevleri ile modelin çekirdek üretim işlevi ayrı değerlendirilmelidir¹⁷³. Kullanıcı paylaşımı, kullanıcı dosyası, profil ve içerik arşivi gibi barındırma özellikleri bakımından 5651 sayılı Kanun'un yer sağlayıcı rejimi tartışılabilir niteliktedir¹⁷⁴. Buna karşılık çekirdek üretim işlevinde sistem, üçüncü kişiye ait sabit bir içerik ögesini depolamaz; kullanıcı komutuna yanıt olarak yeni içerik üretir. Yer sağlayıcı rejimi ise kural olarak içerik üzerinde önceden denetim yükümlülüğü öngörmez ve sorumluluğu haberdar edilme eşiği sonrasında içeriğin kaldırılmaması noktasına bağlar¹⁷⁵. Bu nedenle depolama ve bildirim üzerine münferit içeriğin kaldırılması varsayımına dayanan yer sağlayıcı rejimini çekirdek üretim işlevine doğrudan uygulamak, yapısal bir uyumsuzluk doğurur.

Çevrimiçi telif ihlallerinde ise FSEK, Ek m. 4 ile hak sahibinin başvurusu üzerine içeriğin çıkarılmasını ve bazı hâllerde hizmetin durdurulmasını içeren özel bir usul öngörmektedir¹⁷⁶. Bu nedenle 5651 sayılı Kanun'daki yer sağlayıcı rejimi, telif uyumsuzluklarında tek başına genel nitelikli bir müdahale rejimi olarak görülmemeli; 5651 tartışması daha çok kişilik hakları ve Kanun'da sayılan suç tipleri bakımından anlam kazanmaktadır.

Üretken yapay zekâ hizmetlerinde barındırma niteliği taşıyan fonksiyonların belirlenmesinde dört ölçüt esas alınabilir: (i) kalıcılık (içeriğin zaman içinde

¹⁷⁰ 5651 sayılı Kanun, m. 2/f.

¹⁷¹ 5651 sayılı Kanun, m. 2/g.

¹⁷² 5651 sayılı Kanun, m. 2/g; Semih Yünlü (n 106) 533.

¹⁷³ Semih Yünlü (n 106) 533; 5651 sayılı Kanun, m. 2/m, m. 2/g; Ahunur Açıkgöz ve Murat Gürel (n 19) 698-700; Yusuf Başlar (n 2) 611-612; David Atkinson ve Jacob Morrison (n 1) 9.

¹⁷⁴ 5651 sayılı Kanun, m. 2/m; Yusuf Başlar (n 2) 611; Ahunur Açıkgöz ve Murat Gürel (n 19) 700.

¹⁷⁵ 5651 sayılı Kanun, m. 5/1, m. 5/2; AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 62.

¹⁷⁶ FSEK, Ek m. 4/3.

saklanması ve yeniden erişilebilir olması), (ii) üçüncü kişiye açıklık (başkalarının erişimine açılması), (iii) indekslenebilirlik (arama ile bulunabilirlik) ve (iv) kamusal sunum (örneğin içerik için paylaşım bağlantısı, herkese açık galeri veya akış, öneri-sıralama yüzeyleri ve dış arama motorlarınca taranabilirlik).

Bu ölçütler, kanunda açıkça sayılmış bir test değil; barındırma ve yayın özelliklerini somutlaştırmaya yarayan pratik göstergelerdir.

Bu ölçütlerin birlikte gerçekleştiği hâllerde yer sağlayıcı rejiminin uygulanabilirliği güçlenirken, yalnızca belirli bir anda görüntülenen dinamik içerikler veya tek seferlik çıktı gösterimi gibi geçici sunumlarda barındırma varsayımı zayıflamaktadır¹⁷⁷. Bu ayrım, AB hukukunda önbellekleme (caching) ile barındırma (hosting) muafiyetlerinin, geçici depolama ile hizmet alıcısının talebi üzerine depolama arasında kurduğu kategori ayrımına da paraleldir¹⁷⁸. Bu noktada özellikle üçüncü kişiye açıklık ile indekslenebilirliğin birlikte gerçekleşmesi, içeriğin fiilen kamusal erişime açılması bakımından belirleyicidir. İndekslenbilirlik ölçütü açısından ise, içeriğin arama ve keşif mekanizmaları üzerinden üçüncü kişilere sistematik biçimde yönlendirilmesi ile salt teknik endeksleme faaliyeti arasındaki ayrım, yer sağlayıcı niteliğinin sınırlarını tartışmada yol gösterici olabilir¹⁷⁹.

Bu tür kamusal sunum ve kontrol unsurlarının sorumluluk değerlendirilmesinde önem kazandığı, profesyonelce işletilen bir haber portalını anonim yorumlar bakımından sorumlu tutan AİHM Delfi AS v Estonya kararında da görülebilmek¹⁸⁰. Buna karşılık AİHM, MTE ve Index.hu Zrt v Macaristan kararında, içerik türü ile başvuruların bildirim üzerine kaldırma mekanizması kurmuş olmaları gibi unsurları orantılılık değerlendirmesinde belirleyici görmüş; nefret söylemi eşiğinin aşılmadığı durumlarda katı sorumluluk yaklaşımının ölçüsüz sonuçlar doğurabileceğini belirtmiştir¹⁸¹. Bu içtihat, Türk hukukunda yer sağlayıcı sorumluluğunun sınırlarını tek başına yeniden tanımlamaz; burada, kamusal sunum ve fiilî kontrol unsurlarının orantılılık değerlendirmesinde nasıl anlam kazandığını göstermek bakımından karşılaştırmalı bir ankraj işlevi görür.

¹⁷⁷ 5651 sayılı Kanun, m. 2/m; Ahunur Açıkgoz ve Murat Gürel (n 19) 698.

¹⁷⁸ E-Commerce Directive, m. 13-14; Digital Services Act, m. 5/1, m. 6/1.

¹⁷⁹ 5651 sayılı Kanun, m. 2/m, m. 2/ğ; Alper Işık, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları* (1 Baskı, On İki Levha Yayıncılık 2023) 217; Mehmet Bedii Kaya (n 19) 187; Ahunur Açıkgoz ve Murat Gürel (n 19) 708.

¹⁸⁰ Delfi AS v Estonia, 64569/09, T. 16.06.2015 (n 61), para. 110-117, 145-156.

¹⁸¹ MTE and Index.hu Zrt v Hungary, 22947/13, T. 02.02.2016 (n 62), para. 64, 72-77, 91.

Yer sağlayıcı sorumluluğunun sınırları, Yargıtay içtihadında esasen haberdar edilme eşiği üzerinden çizilmektedir¹⁸². Doktrinde, Yargıtay'ın yer sağlayıcı sorumluluğunu hukuka aykırılıktan haberdar edildikten sonra içeriği yayımından kaldırmama eylemiyle sınırladığı; bu yaklaşımın yer sağlayıcının olumlu fiilinden doğan sorumluluğu büyük ölçüde dışladığı ifade edilmektedir¹⁸³. Yargıtay Hukuk Genel Kurulu'nun GittiGidiyor kararında da platform işletmecisinin üçüncü kişi ilanlarından doğrudan sorumlu tutulamayacağı; sorumluluğun ancak ihlalden haberdar edildikten sonra içeriği kaldırmama hâlinde tartışılabileceği vurgulanmıştır¹⁸⁴. Bununla birlikte doktrinde, haberdar edilmenin özel bir usule bağlanmamış olmasının bildirimin şekli ve içeriği bakımından belirsizlik yarattığı; bu belirsizliğin özellikle fikrî hak uyuşmazlıklarında Yargıtay uygulamasında farklı yorumlara zemin hazırladığı ifade edilmektedir¹⁸⁵.

Üretken yapay zekâ servislerinde haberdar edilme eşiğinin öngörülebilir biçimde işletilebilmesi için, bildirimin yalnızca çıktıyı değil, çıktının hangi bağlamda üretildiğini de gösterecek unsurları içermesi gerekir. Haberdar edilme bakımından özel bir usul öngörülmemesi, bildirimin şekli ve içeriği açısından belirsizlik yaratmaktadır¹⁸⁶. Buna karşılık doktrinde, Yargıtay'ın bazı kararlarında hak sahibinden üstün hak sahipliğini yaklaşık ispata elverişli delillerle ortaya koymasının beklendiği; bunun da bildirim standardını fiilen ağırlaştırabildiği ifade edilmektedir¹⁸⁷. Geleneksel barındırma hizmetlerinden farklı olarak, yalnızca çıktı metninin iletilmesi çoğu kez konuşturıcının komutu, konuşma bağlamını ve çıktının tekrarlanabilirliğini değerlendirmesine imkân vermez. Bu nedenle, haberdar edilme eşiğinin üretken yapay zekâ bakımından işlerlik kazanabilmesi için, bildirimin asgari unsurlarının (en azından çıktı, girdi bağlamı, ihlal türü ve talep edilen müdahale) kanun veya ikincil düzenleme düzeyinde açıkça belirlenmesi gerekir. Karşılaştırma bakımından DMCA § 512(c)(3)(A) ve DSA m. 16/2, bildirimin asgari unsurlarını ayrıntılandıran iki örnek teşkil etmektedir¹⁸⁸.

5651 sayılı Kanun bakımından üretken yapay zekâ hizmetlerinde üç eşik ayrımı yapmak mümkündür. Birincisi, kullanıcı içeriği barındırma ve yayın

¹⁸² Yargıtay Hukuk Genel Kurulu, E. 2013/1138, K. 2014/16, T. 15.01.2014 (GittiGidiyor) 1359, 1359.

¹⁸³ Ahunur Açıköz ve Murat Gürel (n 19) 728.

¹⁸⁴ Yargıtay HGK, E. 2013/1138, K. 2014/16, T. 15.01.2014 (n 182) 1359.

¹⁸⁵ Ahunur Açıköz ve Murat Gürel (n 19) 731.

¹⁸⁶ Ibid 732.

¹⁸⁷ Ibid.

¹⁸⁸ 17 U.S.C. § 512 (Digital Millennium Copyright Act) s 512(c)(3)(A); Digital Services Act, m. 16/2.

işlevleri bakımından 5651 sayılı Kanun'un 5. maddesi kapsamında yer sağlayıcı tartışması yürütülebilir¹⁸⁹. İkincisi, hizmetin ürettiği çıktıyı kullanıcılara sunması bakımından 5651 sayılı Kanun'un 2/f bendindeki içerik sağlayıcı tanımıyla temas eden bir sorumluluk tartışması doğmaktadır¹⁹⁰. Üçüncüsü ve en kritik olanı şudur: başvuru üzerine münferit içerik ögesinin çıkarılmasına dayanan mekanizma, teknik olarak yalnızca barındırılan veya yayımlanan içerik katmanında anlamlıdır. Buna karşılık ağırlık katmanında aynı müdahale yönteminin doğrudan ve genel bir karşılığı bulunmamaktadır. Literatürde makine unutmama (machine unlearning) yaklaşımları geliştirilmiş olmakla birlikte, bu yaklaşımlar dahi çoğu senaryoda yeniden eğitime yaklaşan yinelemeli bir hesaplama maliyeti doğurmakta ve genelleştirilebilir bir silme tekniği sunmamaktadır. Örneğin SISA yaklaşımında, Purchase veri setinde unutmama süresinin yeniden eğitime kıyasla 4.63 kat, SVHN veri setinde ise 2.45 kat hızlanabildiği rapor edilmiştir¹⁹¹. Daha erken bir çalışmada ise PJScan örneğinde, yeniden eğitimin ortalama 42 iterasyon gerektirdiği, tek örnek unutmama işleminin ise ortalama 2.4 iterasyon sürdüğü belirtilmiştir¹⁹². Bu çalışmalar, ağırlık katmanında geçmiş verinin etkisini kaldırmanın belirli varsayımlar altında ve hâlen deneysel yöntemlerle mümkün olabildiğini göstermekte; bu nedenle makine unutmama, mevcut usul hukukunda standart bir giderim aracı olarak görülemez¹⁹³. Bu bulgular, ağırlık katmanında tekil veri veya içerik parçalarının çıkarılabilir olduğu varsayımını zayıflatmaktadır¹⁹⁴. Bu nedenle 5651 sayılı Kanun'un müdahale yöntemini ağırlık katmanına doğrudan taşımak yerine, fiilen uygulanabilir tedbirlere ve somut olayda öngörülebilir risk azaltımına odaklanan bir değerlendirme daha isabetlidir. Nitekim ABD Ulusal Standartlar ve Teknoloji Enstitüsü'nün (National Institute of Standards and Technology - NIST) Yapay Zekâ Risk Yönetimi Çerçevesi (Artificial Intelligence Risk Management Framework, AI RMF), risk yönetimi işlevlerinin sistemin yaşam döngüsü boyunca ve konuşlandırma sonrasında da yinelemeli biçimde işletilmesi gerektiğini vurgulamaktadır¹⁹⁵. Bu nedenle içerik çıkarma yükümlülüğünü ağırlık katmanına taşımaya yönelik önerilerde,

¹⁸⁹ 5651 sayılı Kanun, m. 5/2.

¹⁹⁰ 5651 sayılı Kanun, m. 2/f; Yusuf Başlar (n 2) 609.

¹⁹¹ Lucas Bourtole ve diğerleri (n 8) 1-2.

¹⁹² Yinzhi Cao ve Junfeng Yang (n 7) 7, 15.

¹⁹³ Thanh Tam Nguyen ve diğerleri (n 8) 5, 9-10.

¹⁹⁴ David Atkinson ve Jacob Morrison (n 1) 9; Claudio Novelli ve diğerleri (n 152) 13.

¹⁹⁵ National Institute of Standards and Technology, 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)' (2023) NIST AI 100-1 20-21 <<https://doi.org/10.6028/NIST.AI.100-1>> Erişim Tarihi 25 Ocak 2026.

(i) müdahalenin nesnesi (münferit içerik ögesi mi, yoksa model parametreleri mi) ile (ii) müdahale yöntemi (silme mi, yoksa filtreleme veya indeksten çıkarma gibi dolaylı önlemler mi) ayrıştırılmadan sağlıklı bir normatif değerlendirme yapılması güçtür¹⁹⁶.

Bu tespit, mevcut müdahale araçlarında bir boşluğa işaret eder: yer sağlayıcı bakımından içeriğin çıkarılması ile erişimin engellenmesi arasında, sistemin işleyişine dönük daha hafif ve aşamalı bir tedbir kategorisi kanunda açıkça tanımlanmamıştır. Nitekim Anayasa Mahkemesi, m. 9 kapsamındaki mekanizmanın kişilik haklarına yönelik saldırılara karşı internet içeriğinin sınırlandırılmasında “kademeli bir müdahale yöntemi” sunmadığını; ayrıca erişim engellemenin karar tarihinden itibaren süresiz etki doğurduğunu ve bu yönüyle ağır bir müdahale teşkil ettiğini belirtmiştir¹⁹⁷. Mahkeme, aynı paragrafta, zararlı içerikle diğer usullerle mücadele edilebildiği sürece bu yöntemle başvurulmaması gerektiğine de işaret etmektedir. Bu değerlendirme, müdahalenin tür ve yoğunluğunu kademelendiren ara tedbir kategorilerinin kanun düzeyinde açıkça düzenlenmesi ihtiyacını güçlendirmektedir.

Bu ayrımın, her somut olayda içerik sağlayıcı sıfatının otomatik olarak kazanıldığı şeklinde anlaşılması gerekir. Zira 5651 bakımından içerik sağlayıcı sorumluluğu, içeriğin internet ortamında kullanıma sunulmasına dayanır; dolayısıyla yalnızca kapalı bir kullanıcı arayüzünde sunulan ve üçüncü kişilerle paylaşılmayan çıktılar bakımından içerik sağlayıcı nitelendirmesi, içeriğin kamusal erişime açılması unsuru dikkate alınarak ayrıca tartışılmalıdır¹⁹⁸.

Anayasa Mahkemesi, 11.10.2023 tarihli kararıyla, 5651 sayılı Kanun m. 9 kapsamında kişilik hakları bakımından işletilen içerik çıkarma ve erişimin engellenmesi mekanizmasının, Anayasa m. 13'teki kanunilik ve ölçülülük ilkeleri bakımından özellikle usulî güvenceler ve kademelilik açısından sorunlar doğurduğunu vurgulamıştır. Mahkeme, sulh ceza hâkimlikleri uygulamasında çatışan haklar arasında adil dengenin çelişmeli yargılama ve gerekçelendirme güvenceleri oluşmadan kurulamadığını; kademeli müdahale imkânı sunmayan ve süresiz etki doğuran erişim engelleme tekniğinin ölçülülük sorununu derinleştirdiğini belirtmiştir¹⁹⁹.

¹⁹⁶ David Atkinson ve Jacob Morrison (n 1) 9; Mehmet Bedii Kaya (n 19) 190-192.

¹⁹⁷ AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 106.

¹⁹⁸ 5651 sayılı Kanun, m. 4/1; Yusuf Başlar (n 2) 620; Semih Yünlü (n 106) 533.

¹⁹⁹ AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 104-106.

Karar 10.01.2024 tarihli Resmî Gazete’de yayımlanmış, iptal hükmünün yürürlüğe girişi yayım tarihinden itibaren dokuz ay sonrasına ertelenmiştir²⁰⁰. Bu süre 10.10.2024 itibarıyla dolmuş ve m. 9 yürürlükten kalkmıştır. Bu çalışma hazırlanırken, 5651 sayılı Kanun metninde m. 9’u ikame eden kanunî bir başvuru usulü bulunmamaktadır; bu durum genel hükümlere dayalı yargısal tedbir imkânlarını dışlamasa da, 5651 sayılı Kanun içinde kişilik haklarına ilişkin standartlaştırılmış ve hızlı bir başvuru yolunun bulunmaması anlamına gelmektedir²⁰¹.

İptal öncesinde m. 9’un öngördüğü uyarı yöntemi, muhataplara fiilen ulaşılamaması ve taleplerin çoğu kez yanıtsız kalması gibi nedenlerle uygulamada etkin biçimde işletilememiştir²⁰². Uyarı yöntemi, internet ortamındaki hukuka aykırı içeriğin, hakkı ihlal edilen kişinin başvurusu üzerine içerik veya yer sağlayıcı tarafından yayından çıkarılmasını hedefleyen bir usul olarak tasarlanmıştır²⁰³.

İptal edilen m. 9/1, sulh ceza hâkimliğine başvuru öncesinde içerik sağlayıcıya, ona ulaşılamaması hâlinde yer sağlayıcıya başvurularak içeriğin çıkarılmasının talep edilebileceğini düzenlemekteydi²⁰⁴. Doktrinde, muhataplara fiilen ulaşılamaması ve taleplerin yanıtsız bırakılmasının yöntemin işleyişini zayıflattığı; ayrıca talebi yanıtsız bırakan veya yerine getirmeyen aktörler bakımından açık bir yaptırım öngörülmemesinin de bu sorunu derinleştirdiği ifade edilmektedir²⁰⁵.

Bu görünüm, m. 9’u ikame edecek bir usul tasarımı üç yapısal eşiği ortaya koymaktadır: (i) muhataplık sorununun (başvuru hangi aktöre, hangi kanalla yöneltilecek?) azaltılması, (ii) yanıtsız bırakma veya yerine getirmeme hâllerine bağlanan sonuçların öngörülebilir kılınması ve (iii) içerik çıkarma kararlarının asgari usulî güvencelerle kayıt altına alınması. Doktrinde de, özellikle yaptırım ve temsilci ile irtibat mekanizmalarının bu eşiği aşmak bakımından belirleyici olduğuna işaret edilmektedir²⁰⁶.

Anayasa Mahkemesi’nin belirlilik ve kademelik vurgusu, ikame edilecek usulde hem hız hem de temel hak güvenceleri bakımından kademeli ve denetlenebilir bir yapının kurulması gerektiğini göstermektedir. Bu çerçevede, asgari

²⁰⁰ RG, T. 10.01.2024, S. 32425 194; AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), hüküm.

²⁰¹ Anayasa Mahkemesi, Bulut Duman ve diğerleri [2. B.], B. No: 2021/8675, T. 01.10.2025, para. 29; 5651 sayılı Kanun (Mevzuat Metin), m. 9.

²⁰² İsmail Demez (n 4) 204-205; Mehmet Bedii Kaya (n 19) 97.

²⁰³ 5651 sayılı Kanun, m. 2/r; Alper Işık (n 179) 235; İsmail Demez (n 4) 204-205.

²⁰⁴ 5651 sayılı Kanun, m. 9/1.

²⁰⁵ İsmail Demez (n 4) 204-205; Mehmet Bedii Kaya (n 19) 97.

²⁰⁶ İsmail Demez (n 4) 204-205; 5651 sayılı Kanun, Ek m. 4; Digital Services Act, m. 13.

olarak (i) başvuru ve içerik veya çıktı tespiti, (ii) hızlı ön değerlendirme, (iii) gerekçeli cevap ve karşı bildirim imkânı, (iv) acil hâllerde geçici tedbir, (v) nihai yargısal karar ve (vi) itiraz ile şeffaflık ve denetim adımlarının normatif düzeyde açık biçimde düzenlenmesi tartışılmaktadır²⁰⁷.

Uyuşmazlık tipleri bakımından hakaret ve itibar saldırısı, kişisel veri ifşası ve telif ihlali senaryolarında kural olarak son kullanıcı fail konumunu korurken, konuşturıcının barındırma ve yayın özellikleri ile kaldırma kapasitesi ölçüsünde olay sonrası yükümlülüklerinin yoğunlaştığı görülür.

C. Esasa İlişkin Sorumluluk: TBK, TCK, KVKK ve FSEK

Üretken yapay zekâ çıktılarından doğan uyuşmazlıklarda 5651 sayılı Kanun, çoğu durumda erişimin engellenmesi ve içeriğin çıkarılması yoluyla ihlalin sona erdirilmesine dönük, olay sonrası işletilen bir müdahale çerçevesi sunmaktadır. Buna karşılık zararların tazmini ve yaptırım düzeninin kurulması, haksız fiil, ceza, kişisel veri ve telif hukukunun birlikte işletilmesini gerektirir. Bu nedenle esasa ilişkin sorumluluk standardı, tek bir aracı sorumluluğu rejimi içinde değil; TBK, TCK, KVKK ve FSEK'in rol temelli olarak tahsis edilen maddi hukuk hükümleri üzerinden kurulmalıdır²⁰⁸.

TBK m. 49 uyarınca haksız fiil sorumluluğu, hukuka aykırı fiil, zarar, illiyet bağı ve kusur unsurlarının birlikte gerçekleşmesine dayanır. Kusur, somut olayda öngörülebilir riskler karşısında makul özenin gösterilip gösterilmediği üzerinden değerlendirilir²⁰⁹. Üretken yapay zekâ değer zincirinde bu ölçütün, salt sorunlu çıktı tespitiyle ikame edilmesi isabetli değildir; değerlendirme, sistemin tasarım ve işletim tercihlerinin risk azaltımı üretip üretmediği sorusuna yönelmelidir²¹⁰.

Bu bağlamda model ağırlıklarına doğrudan müdahalenin (örneğin makine unutmaya yaklaşımlarının) sınırlı ve maliyetli olması, kusur değerlendirmesinde çoğu senaryoda konuşturıcının katmanındaki uygulanabilir risk azaltım tedbirlerine daha fazla ağırlık verilmesini gerektirebilir²¹¹.

Üretken yapay zekâ çıktılarında illiyet bağının (özellikle uygun illiyet bağının) kurulması, klasik haksız fiil kurgusuna göre daha fazla teknik açıklama

²⁰⁷ AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 101, 106; Digital Services Act, m. 16, 20.

²⁰⁸ Semih Yünlü (n 106) 532.

²⁰⁹ TBK, m. 49; Fikret Eren (n 166) 538, 600.

²¹⁰ National Institute of Standards and Technology (n 195) 20-21; David Atkinson ve Jacob Morrison (n 1) 9.

²¹¹ Thanh Tam Nguyen ve diğerleri (n 8) 5, 9-10; Lucas Bourtole ve diğerleri (n 8) 2, 5.

gerektirebilir. Zira aynı komut farklı zamanlarda farklı çıktılar doğurabilir; model sürümü değişebilir; sistem komutu ve filtreleme katmanı devrede olabilir; ayrıca somut uyuşmazlıkta çıktının tekrarlanabilirliği çoğu kez erişim kayıtlarıyla (log) sınılanır. Bu nedenle ispat bakımından, hangi sürümün hangi ayarlarla kullanıldığı, hangi konuşma bağlamında hangi müdahalenin teknik olarak mümkün olduğu ve risk azaltımının hangi aşamada beklenebilir olduğu, özen değerlendirmesinde belirleyici hâle gelebilir²¹².

Doktrinde konuşlandırıcı bakımından (i) teknik dokümantasyon ve şeffaflık çıktıları, (ii) sistem komutu (system prompt) ve çıktı yönetimi, (iii) risk değerlendirmesi ve güvenlik testi (safety testing), (iv) şikâyet ve itiraz hattı ile hızlı müdahale kapasitesi ve (v) erişim kaydı (log) yönetimi ile izlenebilirlik tedbirlerinin özen standardının somut göstergeleri olarak değerlendirilebileceği ileri sürülmektedir. Model sağlayıcı bakımından da eğitim verisinin seçimi ve temizliği, değerlendirme yöntemleri ve güvenlik güncellemeleri benzer biçimde tartışılmaktadır²¹³. Ancak bu unsurların hangi aktöre hangi ölçüde yükleneceği, mevcut normlar çerçevesinde doğrudan belirlenememekte; bu durum, çok aktörlü zincirde maddi sorumluluğun tahsisine ilişkin daha açık bir mantık ihtiyacını ortaya koymaktadır.

Hizmet organizasyonu ve insan unsurunun devreye girdiği safhalar bakımından, özellikle moderasyon ve şikâyet süreçleri TBK m. 66 kapsamında adam çalıştırmanın sorumluluğu ile işletmenin çalışma düzeninin zararın doğmasını önlemeye elverişli olup olmadığı tartışmasını gündeme getirir²¹⁴. TBK m. 66, üretken sistemin bir çalışan gibi kabul edilmesine dayanmaz; sorumluluk, hizmeti yürüten kuruluşun insan gözetim ekipleri ve teknik personeline ilişkin seçim, talimat ve denetim özeni ile işletme düzeni üzerinden tartışılabilir. Burada belirleyici olan, içerik veya çıktı yönetimi, kimlik doğrulama, erişim kaydı yönetimi ve benzeri risk azaltım mekanizmaları üzerinde fiilî kontrolün hangi aktörde toplandığıdır.

Bu çerçevede TBK m. 66'nın üretken yapay zekâ değer zincirine uygulanmasında şu normatif ayrımın benimsenmesi önerilmektedir: Model sağlayıcı bakımından adam çalıştırmanın sorumluluğu, modelin kendisinin bir çalışan gibi

²¹² Artificial Intelligence Act, m. 12; KVKK, m. 12.

²¹³ Artificial Intelligence Act, m. 9, m. 11, m. 12; Digital Services Act, m. 16; Hans Graux ve diğerleri, 'Interplay between the AI Act and the EU digital legislative framework' (European Parliament (Policy Department for Transformation, Innovation and Health) 2025) 42.

²¹⁴ TBK, m. 66; Fikret Eren (n 166) 721-732.

nitelendirilmesi üzerinden değil; model sağlayıcının bünyesinde çalışan güvenlik ekipleri, veri etiketleme personeli ve ince ayar sürecini yürüten teknik kadronun seçimi, talimatlandırılması ve denetimi üzerinden kurulmalıdır. Model sağlayıcının bu personele ilişkin seçim, talimat ve denetim özenini gösterdiğini ispat etmesi (TBK m. 66/2) hâlinde sorumluluktan kurtulması mümkündür. Konuşlandırıcı bakımından ise TBK m. 66 tartışması daha somut bir zemine oturur: Moderasyon ekiplerinin yeterliliği, şikâyet süreçlerinde müdahale hızı, içerik filtreleme talimatlarının güncelliği ve gözetim personelinin eğitimi gibi unsurlar, işletme düzeninin zararı önlemeye elverişli olup olmadığının doğrudan göstergeleridir. Dolayısıyla TBK m. 66'nın üretken yapay zekâ bakımından asıl işlev alanı, modelin üretim faaliyetinde değil; hizmet organizasyonunun insan unsuruna dayanan katmanlarında aranmalıdır²¹⁵.

Ürün sorumluluğu bakımından Avrupa Birliği'nde ayıplılık ölçütü, güvenlik beklentisi üzerinden tanımlanmıştır. Bu ölçüt 85/374/AET sayılı Ürün Sorumluluğu Direktifi'nde m. 6'da düzenlenmiş; 2024/2853 sayılı Direktif'te m. 7'de yeniden düzenlenmiştir²¹⁶. Bu bağlamda (i) dijital içerik ve buna bağlı hizmetlerin ürün sorumluluğu rejimiyle ilişkilendirilmesi, (ii) açık kaynak dâhil çok aktörlü tedarik zincirlerinde sorumluluğun hangi noktada yoğunlaşacağı ve (iii) çevrimiçi aracı hizmet sağlayıcıların hangi şartlarla bu zincirde sorumluluktan ayrışabileceği başlıkları, üretken yapay zekâ sistemleri bakımından özellikle tartışmalıdır²¹⁷.

Haksız fiil ve ürün sorumluluğunun ötesinde, üretken yapay zekâ çıktıları'nın ceza hukuku boyutu da değerlendirilmelidir. Ceza hukuku bakımından tüzel kişi sorumluluğu sınırlıdır. TCK m. 20/2 uyarınca tüzel kişiler hakkında ceza yaptırımına hükmolunamaz; ancak suç dolayısıyla kanunda öngörülen güvenlik tedbirleri saklıdır²¹⁸. Bu nedenle üretken yapay zekâ hizmetlerinde ceza sorumluluğu, kural olarak kusurlu eylemi bulunan gerçek kişilere yönelir²¹⁹.

Fail tespiti bakımından, üretken yapay zekâ değer zincirinde tek bir aktörü peşinen çıktı üreticisi konumuna yerleştirmek yerine rol temelli bir ayrıştırma

²¹⁵ TBK, m. 66/2, m. 66/3; Fikret Eren (n 166) 730-732.

²¹⁶ Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products 1985, m. 6; Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Text with EEA relevance) 2024, m. 7.

²¹⁷ Semih Yünlü (n 106) 535-538; İpek Çevik, 'Avrupa Birliği Dijital Hizmetler Yasası'nın Değerlendirmesi' (2023) 8 YBHD 387, 408-414; Forbrukerrådet (n 42) 54-55.

²¹⁸ TCK, m. 20/2; Mahmut Koca ve İlhan Üzülmöz (n 169) 641.

²¹⁹ Yusuf Başlar (n 2) 617.

yapılmalıdır. Bu ayrıştırmada (i) hukuka aykırı içeriğe vücut veren girdinin sağlanması veya çıktının yayımlanması kararının kimin iradesiyle alındığı, (ii) ihlalin gerçekleştiği katmanın hangi aktörün fiili kontrol alanında bulunduğu ve (iii) ihlali önlemek veya sonlandırmak bakımından kimin makul ve etkili müdahale kapasitesine sahip olduğu birlikte değerlendirilmelidir. İhmali davranışın tartışıldığı hâllerde ise neticeyi önleme yükümlülüğünün (garantörlük) hangi kaynaklardan doğduğu ve somut olayda hangi aktöre yüklenebileceği ayrıca gösterilmelidir. Konuşlandırıcının paylaşım, indeksleme veya arşivleme gibi yayın işlevlerini kurumsal tasarımıyla işletmesi ve bildirim üzerine müdahale imkânına sahip olması hâlinde, iştirakin yahut ihmali davranışın sınırında sorumluluk tartışması gündeme gelebilir. Buna karşılık model sağlayıcı bakımından, belirli bir çıktıyı olay sonrası kontrol imkânının sınırlılığı nedeniyle tartışmanın ağırlık merkezinin çoğu kez TBK ve KVKK katmanına kaydığı söylenebilir²²⁰.

Kişisel verilerin korunması, üretken yapay zekâ bakımından sorumluluk yapısının en belirgin katmanlarından biridir. Zira eğitim verisi, kullanıcı girdileri, sohbet geçmişi, çıktı kayıtları ve güvenlik amaçlı kayıt (log) verisi gibi süreçler doğrudan veri işleme faaliyetleridir.

KVKK'da veri sorumlusu (data controller) ve veri işleyen (data processor) ayrımı, amaç ve vasıtaları belirleme ölçütü üzerinden kurulduğundan, model sağlayıcı-konuşlandırıcı ayrımında rol temelli tahsis bakımından işlevsel bir test sunar. Model sağlayıcı, eğitim verisinin temini ve temizlenmesi ile modelin eğitimi gibi aşamalarda amaç ve vasıtaları belirlediği ölçüde veri sorumlusu olarak; konuşlandırıcı ise kullanıcı hesap verileri, girdiler, sohbet geçmişi ve çıktı kayıtları bakımından veri sorumlusu olarak konumlanabilir. Konuşlandırıcının kendi kullanıcı verilerini bir model sağlayıcının API'si üzerinden işlediği senaryolarda ise rol tahsisi, verinin hangi amaçlarla tutulduğu (servis sunumu, güvenlik, model iyileştirme) temelinde ayrıca netleştirilmelidir. Avrupa Birliği'nde Yapay Zekâ Tüzüğü ile Genel Veri Koruma Tüzüğü etkileşiminde dahi veri işleme yükümlülüklerinin ortadan kalkmadığı, hatta bazı senaryolarda değerlendirmelerin yenilenmesini gerektirebileceği vurgulanmaktadır²²¹.

Uygulamada, rol tahsisi netleştirildikten sonra en azından (i) veri envanteri ve saklama sürelerinin amaçla sınırlı kurulması, (ii) kayıt (log) yönetiminde

²²⁰ Ibid 630; Mahmut Koca ve İlhan Üzülmöz (n 169) 372-375, 379-381, 385-395; Ahunur Açıkgoz ve Murat Gürel (n 19) 724; Yusuf Başlar (n 109) 61-64.

²²¹ KVKK, m. 3/ğ, m. 3/ı; Kişisel Verileri Koruma Kurumu (n 160) 5-14; Erman Ekingen ve Miray Özer Deniz (n 126) 456; Hans Graux ve diğerleri (n 213) 36.

otomatik silme veya anonimleştirme, erişim kontrolü ve denetim izlerinin ayrıştırılması, (iii) denetim ve kötüye kullanım tespiti ihtiyaçlarının veri minimizasyonu ilkesiyle dengelenmesi, (iv) ilgili kişi başvurularında girdi, çıktı ve kayıt katmanlarında geri döndürülebilirliğin sağlanması ve (v) üçüncü taraf entegrasyonlarında alt işleyen zincirinin sözleşmesel ve teknik tedbirlerle güvence altına alınması gibi başlıklar öne çıkmaktadır²²².

Kişisel verilerin korunmasının yanı sıra, üretken yapay zekâ çıktıların telif hukuku boyutu da ayrı bir sorumluluk katmanı oluşturmaktadır. Çevrimiçi telif ihlalleri bakımından FSEK Ek m. 4/3 hükmü, hak sahibinin başvurusu üzerine ihlale konu eserin içerikten çıkarılmasını ve bazı hâllerde bilgi paylaşımını öngören özel bir usul kurmaktadır²²³. Ancak doktrinde, içerik sağlayıcının çoğu senaryoda ihlalin varlığını güvenilir biçimde tespit edememesi ve başvuru üzerine derhâl içerik çıkarma ile kimlik bilgisi paylaşımı beklentisinin, kişisel verilerin korunması ve kişilik hakları bakımından ikincil ihlaller doğurabilmesi nedeniyle bu usulün uygulamada sorun ürettiği belirtilmektedir. Bu sorunlar ışığında doktrinde, çevrimiçi fikrî hak ihlallerine ilişkin müdahale çerçevesinin, FSEK'in parçalı ve ceza ağırlıklı sistematiği yerine, aracı sorumluluğuna dayalı ve bildirim standartlarını usule bağlayan genel nitelikli bir çerçeve içinde yeniden ele alınması önerilmektedir²²⁴.

Üretken yapay zekâ senaryolarında telif ihlali riski iki noktada belirginleşmektedir: (i) ihlalin çoğu kez barındırılan bir kopyadan değil, kullanıcı girdisine yanıt olarak üretilen çıktının yayılması veya ikamesi üzerinden ortaya çıkması ve (ii) ihlal bildirimi üzerine içeriğin çıkarılmasına dayanan usullerin bazı ürün tasarımlarında kişisel veri ifşasını tetikleyebilmesidir. Bu tablo, hızlı müdahale ihtiyacı ile karşı bildirim ve delil standardı gibi usulî güvencelerin birlikte tasarlanması gereken bir gerilime işaret eder. DSA'nın m. 16'daki bildirim üzerine işlem usulü, bu gerilimin usul düzeyinde nasıl yönetilebileceğine ve ihlalin sona erdirilmesine dönük mekanizmalar ile maddi hukuk sorumluluğu arasındaki ayrımın telif alanında nasıl kurulabileceğine ilişkin karşılaştırmalı bir örnek sunmaktadır²²⁵.

²²² KVKK, m. 4, m. 7, m. 12; Kişisel Verileri Koruma Kurumu (n 160) 5-14; Yunus Emre İlalan, *İnternet Ortamında Kişilik Haklarının İhlali, Korunması ve Başvuru Yolları* (Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi 2022) 133-134.

²²³ FSEK, Ek m. 4/3.

²²⁴ Yusuf Başlar (n 109) 48, 51, 65; Yusuf Başlar (n 2) 627-628.

²²⁵ Sharon Choi (n 144) 1113, 1125; Digital Services Act, m. 16.

FSEK Ek m. 4'ün üretken yapay zekâ bakımından uygulanmasında, ihlalin gerçekleştiği katmana göre normatif bir ayırım yapılması gerekmektedir. Birinci katmanda, eğitim verisi düzeyinde telif ihlali iddiası söz konusudur: Model sağlayıcının eğitim sürecinde telif koruması altındaki eserleri hak sahibinin izni olmaksızın kullanması hâlinde, ihlal modelin ağırlıklarına gömülüdür ve FSEK Ek m. 4/3'ün öngördüğü içerik çıkarma usulü yapısal olarak işlevsizdir; zira barındırılan bir kopyadan değil, istatistiksel bir temsil sürecinden söz edilmektedir. Bu katmanda uyumsuzluk, FSEK Ek m. 4 değil; doğrudan FSEK m. 68 ve devamı ile TBK m. 49 çerçevesinde hak sahibi-model sağlayıcı arasındaki maddi hukuk ilişkisi üzerinden çözülmelidir. İkinci katmanda ise çıktı düzeyinde telif ihlali söz konusudur: Üretken yapay zekânın belirli bir eseri büyük ölçüde benzer veya ikame edecek biçimde yeniden üretmesi ve bu çıktının konuşlandırıcı aracılığıyla kamuya sunulması hâlinde, FSEK Ek m. 4'ün bildirim ve çıkarma usulü kural olarak işletilebilir. Ancak bu durumda bildirimin, yalnızca eserin adını değil; ihlale konu çıktıyı somutlaştıran girdi örneğini, çıktının ihlali oluşturan unsurlarını ve mümkünse zaman damgasını içermesi gerekir. Bu unsurlar, aşağıda Bölüm IV.B'de önerilen altı unsurlu bildirim standardının telif alanındaki somutlaşması olarak değerlendirilebilir. Böylece FSEK Ek m. 4, çıktı katmanında işlevsel kalırken; eğitim verisi katmanındaki yapısal bağdaşmazlık, maddi hukuk sorumluluğu çerçevesine yönlendirilmiş olur²²⁶.

Sonuç olarak üretken yapay zekâ sistemlerinin Türk hukukundaki konumu, tek bir normatif çerçeve içinde açıklanamayacak ölçüde çok katmanlıdır. Barındırma ve yayın özellikleri bakımından 5651 sayılı Kanun'un olay sonrası müdahale araçları işletilebilse de, esasa ilişkin sorumluluk standardı TBK, TCK, KVKK ve FSEK çerçevesinde rol temelli olarak kurulmalıdır. Anayasa Mahkemesi'nin 9. maddeyi iptal eden kararı, bu çok katmanlı yapıda özellikle uyarı yöntemine dayalı başvuru yolunun asgari usulî güvencelerle kanun düzeyinde yeniden kurulmasını zorunlu kılmıştır²²⁷.

Bu inceleme, üretken yapay zekâ bakımından üç sorun alanını öne çıkarmaktadır. Birincisi, 5651 sayılı Kanun'un müdahale araçları münferit içerik çıkarma ile erişimin engellenmesi ikiliğiyle sınırlıdır; sistemin işleyişine yönelik aşamalı bir tedbir kategorisi bulunmamaktadır. İkincisi, haberdar edilme eşiği üretken yapay zekânın girdi-çıkı dinamiğine uyarlanmamıştır; bildirimin

²²⁶ FSEK, Ek m. 4/3; FSEK, m. 68; Yusuf Başlar (n 109) 48; Ahunur Açıkgöz ve Murat Gürel (n 19) 730-732.

²²⁷ 5651 sayılı Kanun, m. 2/m, m. 2/ğ, m. 5/2; AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 106; RG, T. 10.01.2024, S. 32425 194.

hangi asgari unsurları içermesi gerektiği belirsizdir. Üçüncüsü, çok aktörlü zarar zincirlerinde maddi sorumluluğun hangi aktöre hangi ölçütle yükleneceği her zaman tartışmalıdır; üretken yapay zekâda ise katmanlaşma ve bilgi asimetrisi bu tartışmayı daha da keskinleştirmektedir. Takip eden bölümde bu üç başlık, sırasıyla sistem davranış yükümlülüğü, altı unsur standardı ve rol temelli tahsis matrisi önerileri altında somutlaştırılmaktadır.

IV. REFORM ÖNERİLERİ

Bu bölüm, Bölüm III sonunda tespit edilen yapısal boşluklara karşılık üç reform önerisi geliştirmektedir. Karşılaştırmalı inceleme, benzer normları yan yana dizmek amacıyla değil; her rejimin aracı sorumluluğunu dayandığı varsayımları açığa çıkarmak ve bu varsayımların üretken yapay zekâ değer zincirinde hangi noktalarda karşılanmadığını sınamak için kullanılmıştır. Bölüm II-IV'te ulaşılan bulgular, üç rejimde de belirli bir varsayımın üretken sistemlerde tam karşılık bulmadığını ve bunun Türkiye bakımından doğrudan kopyalama yerine hedefli bir tasarım gerektirdiğini göstermektedir.

ABD hukukunda CDA § 230, aracılardan üçüncü kişi kaynaklı içerik nedeniyle yayıncı veya konuşmacı sıfatıyla sorumlu tutulmasını kural olarak dışlayan bir muafiyet düzenlemesidir²²⁸. Üretken yapay zekâ bakımından sorun, içeriğin çoğu senaryoda üçüncü kişiden iletilen veya depolanan bir içerik olarak değil, sistemin üretim faaliyeti olarak ortaya çıkmasıdır. Bu nedenle sorumluluğu yaratmama-yalnızca barındırma ayrımı üzerine kuran bir muafiyetin üretken yapay zekâ sağlayıcılarına genişletilmesi, yapısal bağdaşmazlık riskini büyütmektedir²²⁹.

AB hukukunda DSA, bildirim üzerine işlem mekanizmasını korurken, platform tasarımına ilişkin özen yükümlülüklerini de kademeli biçimde yoğunlaştırır²³⁰. Bununla birlikte DSA'nın bildirim sistemi, belirli bir bilgi ögesinin tespit edilebilir ve kaldırılabilir olduğu varsayımına dayanır²³¹. Üretken yapay zekâ çıktılarında ise (i) aynı komutun aynı sonucu vermesi her zaman beklenemez, (ii) çıktı bildirimi anında değil talep anında ortaya çıkar ve (iii) tekil bir çıktının kaldırılması benzer çıktıları tek başına engellemez. Dolayısıyla bildirim standartları, içerik ögesi mantığı korunmakla birlikte üretken sistemlere özgü bağlam unsurları eklenerek işlevsel hâle getirilebilir.

²²⁸ CDA § 230 ss 230(c)(1), (f)(3).

²²⁹ Hasala Ariyaratne (n 1) 8-9; Dylan Varga (n 85) 9-10.

²³⁰ Digital Services Act, m. 16; Digital Services Act, m. 34, m. 35.

²³¹ Digital Services Act, m. 16/2.

AB Yapay Zekâ Tüzüğü ise risk temelli yükümlülükleri sağlayıcı ile konuşturucu ayrımı üzerinden tahsis eder²³². Ne var ki üretken yapay zekâda temel model-ince ayar-ürün arayüzü-son kullanıcı katmanları iç içe geçtiğinden, hangi riskin hangi aktöre hangi ölçüde izafe edileceği uygulamada tartışmalıdır. Nitekim genel amaçlı model hükümlerinin yasama sürecinde görece geç belirginleşmesi ve kurumlar arası müzakerelerde biçim değiştirmesi, rol ve yükümlülük sınırlarının tartışmalı olduğunu göstermektedir²³³.

Bu çerçevede üç öneri öne çıkmaktadır: (i) 5651 sayılı Kanun'un müdahale araçlarına, münferit içerik çıkarma ile erişimin engellenmesi ikiliğiyle sınırlı kalmayan ve sistem davranışına yönelik bir tedbir kategorisi eklenmesi; (ii) haberdar edilme eşliğinin, üretken yapay zekâyâ uygun, doğrulanabilir ve karşı bildirimle dengelenebilir bir bildirim standardı ile somutlaştırılması; (iii) maddi sorumluluğun (TBK, TCK, KVKK ve FSEK) tahsisinde kategorilere değil, işlev ve fiilî müdahale kapasitesine dayanan rol temelli bir matris benimsenmesi.

Bu bölümde bu üç öneri, gerekçeleri ve uygulanış mantığıyla sırasıyla açıklanmakta, bölümün sonunda ise karşılaştırmalı bulgular ile öneriler arasındaki ilişki bir sentez tablosu ile özetlenmektedir.

A. Sistem Davranış Yükümlülüğü

Bu çalışmada sistem davranış yükümlülüğü, içeriğin çıkarılması veya erişimin engellenmesi gibi son çare müdahalelere başvurulmadan önce, belirli bir hukuka aykırılık riskini azaltmaya elverişli sistem tasarımı ve işletimine ilişkin tedbirleri alma ve uygulama yükümlülüğü olarak kullanılmaktadır.

5651 sayılı Kanun'un klasik müdahale yöntemi, hukuka aykırılığın belirli bir içerik ögesinde somutlaştığı ve bu öge çıkarıldığında ihlalin sona ereceği varsa-

²³² Artificial Intelligence Act, m. 25/1; Artificial Intelligence Act, m. 53.

²³³ Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts - General Approach' (2022) ST 14954/22 1 <<https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>>; European Parliament, 'Amendments Adopted by the European Parliament on the Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (2023) P9_TA(2023)0236 74-77, 199 <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf>; Council of the European Union, 'Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World' (09 Aralık 2023) <<https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/>> Erişim Tarihi 24 Ocak 2026, giriş; Michael Veale ve João Pedro Quintais, 'The Obligations of Providers of General-Purpose AI Models' (2025) 3 <<https://files.michaelveale.eu/papers/VealeQuintaisObligationsofGPAIProvidersNov2025.pdf>>; Camille Schyns, *The Lobbying Ghost in the Machine: Big Tech's covert defanging of Europe's AI Act* (Corporate Europe Observatory, February 2023) 5; Philipp Hacker (n 152) 9.

yımına dayanır. Üretken yapay zekâda ise sorun, tekil bir çıktının kaldırılmasından ziyade sistemin belirli tür çıktıları üretme olasılığını artıran tasarım ve işletim tercihlerinde yoğunlaşır. Bu nedenle ilk öneri, 5651 sayılı Kanun'daki müdahale araçlarının kapsamını, belirli bir hukuka aykırılık riskini azaltmaya yönelik sistem davranışına yönelik tedbirleri de içerecek biçimde genişletmektir.

Bu çerçeveye, mevcut hukuktan kendiliğinden çıkarılacak bir yorum kuralı olarak değil; m. 9 iptali sonrasında yeniden kurulacak başvuru usulünün bir parçası olarak, kanun koyucunun açık bir yasal dayanakla tasarlayacağı yeni bir tedbir kategorisi olarak düşünülmelidir. Tedbirlerin kademeli, süreli ve gerekçeli olması; karşı bildirim ve itiraz imkânları ile yargısal denetim güvenceleriyle tamamlanması, hukuk devleti ilkesi bakımından zorunludur.

Sistem davranışına yönelik tedbirler, içeriğin çıkarılması veya erişimin engellenmesi gibi ağır müdahalelere başvurmadan önce daha ölçülü ve aşamalı bir müdahale imkânı sağlar. Anayasa Mahkemesi'nin 5651 sayılı Kanun'un 9. maddesini iptal eden kararında vurguladığı kademelilik, münferit içerik çıkarma ile erişimin engellenmesi arasında ara tedbir kategorilerinin bulunmasını gerektirir; sistem davranış yükümlülüğü de üretken yapay zekâ bakımından bu ara alanı doldurmayı amaçlar²³⁴. Bu kapsamda 5651 sayılı Kanun'da, örneğin (i) belirli ihlal kategorileri bakımından çıktı üretimini azaltmaya dönük teknik yapılandırmalar, (ii) şikâyet ve itiraz süreçlerinin hızlandırılması ve kayıt altına alınması, (iii) tekrarlayan ihlallerde kullanıcı bazlı tedbirler ve (iv) şeffaflık ile raporlama yükümlülükleri, aşamalı biçimde işletilebilecek tedbirler olarak düzenlenebilir.

Örneğin belirli bir sanatçının üslubunu sistematik biçimde taklit etmeye dönük komut kalıplarının yaygınlaştığı ve şikâyetlerin aynı komut türlerinde kümелendiği bir senaryoda, tekil çıktıları tek tek yayından çıkarmak çoğu kez tekrar üretimi engellemez. Buna karşılık (i) belirli komut türleri için hız ve tekrar sınırı, (ii) riskli kategorilerde ek doğrulama veya görünür uyarı, (iii) tekrarlayan ihlallerde hesap bazlı kısıtlama ve (iv) alınan kararların gerekçeli biçimde kayıt altına alınması gibi sistem davranışına yönelik tedbirler, erişimin engellenmesine kıyasla daha ölçülü ve hedefli bir müdahale seti oluşturabilir.

Bu tedbirlerin uygulanmasında idari araçlar daha elverişlidir. Zira sistemin işleyişine yönelik risk azaltım yükümlülükleri, belirli bir içerik ögesine ilişkin yargısal karar mantığından ziyade düzenleyici gözetim ve denetim mantığına

²³⁴ AYM, E. 2020/76, K. 2023/172, T. 11.10.2023 (n 4), para. 104-106; RG, T. 10.01.2024, S. 32425 194.

yakındır²³⁵. Bu nedenle öneri, idari bir merci (örneğin BTK) tarafından uygulanacak, ölçülülük ve yargısal denetim güvenceleriyle çerçevelenmiş aşamalı bir tedbir seti kurulmasını hedefler²³⁶. Tedbirlerin tasarımı kanunilik ve ölçülülük (Anayasa m. 13) ile etkili başvuru hakkı (Anayasa m. 40) güvenceleri birlikte gözetilmelidir. 5651 sayılı Kanun kapsamındaki düzenleme yetkisinin bu tedbirlerin bir kısmını öngörmeye elverişli olduğu ileri sürülebilirse de, hukuki güvenlik ve öngörülebilirlik bakımından açık bir yasal dayanak kurulması tercih edilmelidir. Bu nedenle tedbir kategorileri ve asgari usulî güvenceler, ikincil düzenleme ile değil kanun düzeyinde çerçevelenmelidir.

B. Haberdar Edilme: Altı Unsur Standardı

5651 sayılı Kanun m. 5/2'de yer sağlayıcının sorumluluğu, hukuka aykırı içerikten haberdar edilme ve buna rağmen içeriğin kaldırılmaması eşiği üzerinden kurulur²³⁷. Üretken yapay zekâ uyumsuzluklarında bu eşik, bildirimin yalnızca çıktıyı değil, çıktının hangi bağlamda üretildiğini ve hangi müdahalenin talep edildiğini gösterecek ölçüde somut olmasına bağlıdır. DSA m. 16/2(a)-(d), bildirimin (a) hukuka aykırılık gerekçesini, (b) içeriğin konumunu, (c) bildirim yapanın iletişim bilgilerini ve (d) iyi niyet beyanını içermesini şart koşar²³⁸. DMCA § 512(c)(3)(A)(i)-(vi) da imza, eser ve ihlal konusu materyalin tespiti, konum bilgisi, iletişim bilgileri ve iyi niyet/doğruluk beyanları gibi asgari unsurları arar²³⁹. Türk hukukunda haberdar edilme eşiğinin üretken yapay zekâ bakımından işlevsel kılınması için, bu iki çerçeveden esinlenen altı unsurlu bir bildirim standardı önerilebilir. Bu standart, (i) ihlal iddiasının türü ve hukuki dayanağı; (ii) şikâyet konusu çıktının tespiti ve mümkünse yayındaki konumu (bağlantı, ekran görüntüsü, zaman damgası); (iii) çıktıyı doğuran girdi bağlamı (erişilebilir olduğu ölçüde komut ve varsa ilgili ekler) ile gerekli ise önceki konuşma kesiti; (iv) hukuka aykırılık gerekçesinin açık açıklaması ve delil seti; (v) talep edilen müdahale türü (çıktının yayından çıkarılması, erişimin engellenmesi, düzeltme, belirli komut türlerinin kısıtlanması vb.); (vi) karşı bildirim ve itirazı mümkün kılacak iletişim bilgileri ile beyanlar unsurlarını içermelidir. Bu standartlaştırmaya, telif alanında FSEK Ek m. 4/3'teki başvuru mantığıyla da uyumlu biçimde, bildirimin içeriğini asgari unsurlara bağlamayı mümkün kı-

²³⁵ Miriam C. Buiten (n 13) 377; Martin Husovec (n 54) 28.

²³⁶ 5651 sayılı Kanun, m. 10/1.

²³⁷ 5651 sayılı Kanun, m. 5/2.

²³⁸ Digital Services Act, m. 16/2(a)-(d).

²³⁹ DMCA § 512 ss 512(c)(3)(A)(i)-(vi).

lar²⁴⁰. Bu yaklaşım, Ek m. 4/3'teki özel usulü ortadan kaldırmaz; yalnızca bildirim içeriğinin asgarî düzeyde standartlaştırılmasına hizmet eder.

Girdi bağlamına erişim, her zaman bildirimde bulunan kişide olmayabilir. Bu hâllerde bildirim, erişilebilir veriyle sınırlı tutulmalı; konuşlandırıcı ise elindeki erişim kayıtları üzerinden (KVKK bakımından veri minimizasyonu ve maskeleme ilkeleriyle uyumlu şekilde) bağlamı yeniden kurarak değerlendirmeyi tamamlamalıdır.

Örneğin bir kişi hakkında suç isnadı içeren haber özeti niteliğindeki bir çıktının, bir konuşlandırıcının arayüzünde üretilip üçüncü kişilere aktarılması hâlinde, yalnızca çıktı metninin gönderilmesi çoğu kez konuşlandırıcının komutu, konuşma bağlamını ve çıktının tekrarlanabilirliğini değerlendirmesine imkân vermez. Altı unsur standardı, çıktı ile birlikte komut ve konuşma kesitini ve talep edilen müdahaleyi de içerecek biçimde bildirim somutlaştırarak, konuşlandırıcının gerekçeli bir değerlendirme yapmasını ve karşı bildirim ve itiraz adımlarını işletmesini kolaylaştırır.

Bu standardın amacı yer sağlayıcı güvenli limanını üretken yapay zekâyâ genişletmek değildir; haberdar edilme eşliğini hem müdahale seçeneklerini belirlemeyi mümkün kılan hem de haksız veya ölçüsüz taleplere karşı denetlenebilirlik üreten bir usul ölçütüne dönüştürmektir. Bu yaklaşım aynı zamanda Anayasa Mahkemesi'nin işaret ettiği usul güvenceleri bakımından gerekçeli cevap ve karşı bildirim adımlarını somutlaştırır. Ayrıca otomatik sansür ve bildirim mekanizmasının kötüye kullanılması riskini azaltmak için, açıkça dayanaksız ve kötünietli bildirimlere karşı yaptırımların ve usulî kötüye kullanımı mekanizmalarının da düzenlenmesi gerekir²⁴¹. Bu yükümlülüklerin kapsamı ise konuşlandırıcının ölçeği ve risk profili dikkate alınarak kademelendirilmelidir.

C. Rol Temelli Tahsis Matrisi

Üretken yapay zekâ değer zincirinde maddi sorumluluğun kurulması, tek bir aracı sorumluluğu kategorisine indirgenemez. Zira zarar doğuran süreç, çoğu kez modelin geliştirilmesi, ürünleştirilmesi, arayüz tasarımı, komut yönetimi ve kullanım bağlamı kararlarının birleşik sonucudur. Bu nedenle TBK, KVKK, FSEK ve ilgili ceza normlarının uygulanmasında, hangi aktörün hangi risk hak-

²⁴⁰ FSEK, Ek m. 4/3.

²⁴¹ Digital Services Act, m. 23; HMK, m. 29; TCK, m. 271.

kında bilgi sahibi olduğu, hangi unsurları fiilen kontrol ettiği ve hangi tedbirlere müdahale edebildiği belirleyicidir²⁴².

Rol temelli tahsis matrisi, (i) bilgi, (ii) kontrol ve (iii) müdahale imkânı ölçütlerini birlikte değerlendirir. Bilgi ölçütü, aktörün riskin kaynağına ilişkin anlamlı bir öngörü üretip üretemeyeceğini gösterir. Kontrol ölçütü, riskin doğmasına yol açan tasarım ve işletim tercihlerinin hangi aktörde toplandığını gösterir. Müdahale imkânı ise somut uyumsuzlukta makul ve etkili tedbirin kim tarafından uygulanabileceğine odaklanır. Ekonomik teşvik, bu üç ölçütü ikame eden bağımsız bir sorumluluk unsuru olarak değil; sorumluluk rejimlerinin arkasındaki teşvik yapısını ve riskin hangi noktada sistematikleştiğini anlamaya yarayan yardımcı bir bağlam unsuru olarak dikkate alınabilir²⁴³. Ölçütler, model sağlayıcı-ince ayar yapan-konuşlandırıcı-son kullanıcı hattında ayrı ayrı uygulanır.

Aktör	Bilgi	Kontrol	Müdahale imkânı	Birincil sorumluluk bağlantısı
Model sağlayıcı	Yüksek: eğitim verisi, mimari, bilinen sınırlar	Yüksek: temel model davranışı	Sınırlı: konuşlandırmaya erişim yok; güncelleme veya önlem önerisi	Tasarım kusurları, sistemik risk, eğitim verisi ve KVKK
İnce ayar yapan	Orta-yüksek: alan verisi, hedef kullanım	Orta: ince ayar, veri seçimi	Orta: model türevini değiştirme	İnce ayar kaynaklı riskler, veri işleme, özen
Konuşlandırıcı	Orta-yüksek: kullanım bağlamı, şikâyet verisi	Yüksek: arayüz, sistem komutu, filtreler, barındırma ve yayın	Yüksek: yayından kaldırma, erişim engeli, filtre güncelleme	5651 muhataplığı, KVKK veri sorumluluğu, TBK m. 49 ve 66
Son kullanıcı	Değişken: niyet ve girdi bağlamı	Düşük: girdi ve paylaşım	Düşük: kendi paylaşımını kaldırma	Kasıtlı kötüye kullanım, TCK ve TBK

Tablo 4.1: Rol temelli tahsis matrisi (bilgi-kontrol-müdahale imkânı)

²⁴² TBK, m. 49; Artificial Intelligence Act, m. 25/1.

²⁴³ Jaani Riordan (n 11) 65.

Tablo, ölçütlerin tipik görünümünü göstermektedir. Somut olayda ağırlıklar, risk türüne ve müdahalenin fiilen hangi katmanda mümkün olduğuna göre değişebilir.

Bu yaklaşımın ilk sonucu, tahsis değerlendirmesinin AB Yapay Zekâ Tüzüğü'ndeki rol etiketlerini aynen devralmadan, buna işlevsel olarak yaklaşan bir ölçüt seti (bilgi-kontrol-müdahale imkânı) üzerinden kurulabilmesidir²⁴⁴. Başka bir ifadeyle, AB'de sağlayıcı ile kullanıma sunan ayrımı üzerinden yürüyen tartışmalar, Türk hukukunda doğrudan kopyalanmak zorunda değildir; ancak benzer işlevlerin hangi aktörde toplandığı her somut olayda açıkça gösterilmelidir. İkinci olarak 5651 sayılı Kanun'un usulî müdahale araçları ile TBK, KVKK ve FSEK'in maddi sorumluluk hükümleri, aynı olayda farklı katmanlara uygulanabilir hâle gelir. Barındırma ve yayın katmanında ihlalin sona erdirilmesi, sistem davranışına yönelik tedbirler ve şeffaflık ön plana çıkarken, maddi hukukta kusur ve özen standardı ile tazmin gündeme gelir.

Örneğin bir konuşlandırıcının, müşteri hizmetleri amacıyla temel bir model üzerine ince ayar yaparak sohbet robotu kurduğu ve robotun belirli konuşmalar da sohbet geçmişini veya kişisel verileri yanlış kullanıcıya ifşa ettiği bir senaryoda KVKK bakımından, veriyi işleme amaç ve vasıtalarını belirleyen konuşlandırıcının veri sorumlusu sıfatıyla birincil yükümlülük üstlenmesi beklenir²⁴⁵. İnce ayar yapan aktörün, ince ayar veri setini belirleyerek bu sızıntıyı öngörülebilir kılan bir tasarım tercihi yaptığı gösterilebiliyorsa, bilgi ve kontrol ölçütleri üzerinden onun da sorumluluğu gündeme gelebilir. Model sağlayıcı açısından sorumluluk ise çoğu senaryoda, konuşlandırma üzerindeki fiilî müdahale imkânının sınırlı olması nedeniyle tasarım düzeyindeki bilinen risklerin yönetilmesine (örneğin güvenlik güncellemesiyle giderilebilir bir zafiyetin varlığına) bağlanacaktır. Model sağlayıcının yurt dışında bulunması hâlinde tasarım kusuruna ilişkin taleplerin fiilen takibi güçleşebilir. Bu durum, uygulamada konuşlandırıcıyı birincil muhatap konumuna getirmekte ve rücu ilişkisini çoğu senaryoda sözleşme hukukuna terk etmektedir.

Sonuç olarak reform paketi, 5651 sayılı Kanun'un iptal sonrası dönemde (m. 9) yeniden kurulacak başvuru usulünü yalnızca eski düzeni ikame eden bir metin olmaktan çıkarıp, üretken yapay zekâ bakımından müdahale edilebilirliği artıran, haberdar edilme eşliğini denetlenebilir bir bildirim standardı üzerinden işler kılan ve maddi sorumluluğu işlevsel ölçütlerle tahsis eden bir çerçeveye

²⁴⁴ Camille Schyns (n 233) 5; Philipp Hacker (n 152) 9.

²⁴⁵ KVKK, m. 3/1; Kişisel Verileri Koruma Kurumu (n 160) 5-14.

dönüştürmelidir. Bu çerçeve, karşılaştırmalı rejimlerin üretken yapay zekâ karşısında sınırlarına ulaşan varsayımlarını doğrudan ithal etmeksizin, Türk hukukunun kendi normatif araçlarıyla tutarlı, uygulanabilir ve ölçülü bir çözüm üretmeyi amaçlamaktadır.

Aşağıdaki tablo, karşılaştırmalı bulgular ile (A) sistem davranış yükümlülüğü, (B) altı unsur standardı ve (C) rol temelli tahsis matrisi önerileri arasındaki ilişkiyi özetlemektedir.

Karşılaştırmalı bulgu	Üretken yapay zekâda karşılanmayan varsayım	Türkiye için sonuç	Öneri
CDA § 230	Üçüncü kişi içeriği-altyapı ayrımı	Bağışıklığı genişletmek yerine özen yükümlülüklerini somutlaştıran araçlar gerekir	A
DSA m. 16	Münferit içerik ögesi kaldırılabilirliği	Bildirim standardı, girdi-çıktı bağlamını da içerecek şekilde yeniden kurulmalıdır	B
AB Yapay Zekâ Tüzüğü	Sabit rol sınırları	Rol tanımları ithal edilmeden, bilgi-kontrol-müdahale ölçütleriyle tahsis yapılmalıdır	C

Tablo 4.2: Karşılaştırmalı bulgular ile reform önerileri arasındaki ilişki

SONUÇ

Üretken yapay zekâ, üçüncü kişi kaynaklı içeriğin depolanmasına ve bildirim üzerine münferit içeriğin çıkarılmasına dayanan aracı sorumluluğu kurgusunu, çekirdek çıkarım katmanında fiilen işletilemez hâle getirmektedir. Bu nedenle tartışma, bir aktörü hangi kategori altında nitelendirmekten önce, hangi katmanda hangi müdahalenin hem etkili hem de ölçülü biçimde kurulabileceğini belirlemeye yönelmelidir. 5651 sayılı Kanun m. 9'un iptali sonrasında yeniden kurulacak başvuru usulünde de düzenlemenin odak noktası, müdahalenin etkiliği ile Anayasa m. 13 anlamında ölçülülük ve hukuki belirlilik ilkelerinin birlikte sağlanmasında toplanmaktadır.

Bu çalışma, karşılaştırmalı rejimlerin kurucu varsayımlarını (üçüncü taraf içeriği, münferit içerik nesnesi, sabit rol sınırları) üretken sistemlerin çok aktörlü değer zinciri karşısında sınamakta ve buradan üç tamamlayıcı öneri üretmektedir. Sistem davranış yükümlülüğü, içeriğin çıkarılması ile erişimin engellen-

mesi ikiliği arasında, ihlali üreten davranış kalıplarını hedefleyen kademeli tedbir kategorilerinin kanun düzeyinde öngörülmesini gerektirir. Bu tedbirler, klasik filtre yükümlülüğünden her durumda daha hafif değildir; ancak belirli ihlal kategorileriyle sınırlı, süreli ve gerekçeli biçimde tasarlandığında ve karşı bildirim ile yargısal denetim güvenceleriyle tamamlandığında, ölçülülük bakımından daha elverişli bir müdahale seti sunar. Altı unsur standardı, haberdar edilme eşliğini girdi-çıkı bağlamını görünür kılacak şekilde somutlaştırır; böylece konuşlandırıcının tekrar üretilebilirlik ve teknik müdahale seçeneklerini değerlendirmesine, karşı bildirimin ise denetlenebilir bir usul içinde işletilmesine olanak tanır. Bu unsurların önemli bir kısmı, platformların şikâyet süreçlerinde fiilen kullanılan bilgiler olduğundan, standart yeni bir yük icat etmekten ziyade mevcut pratikleri hukuki güvenceye kavuşturur. Rol temelli tahsis matrisi ise maddi sorumluluğu ithal edilmiş kategori adlandırmalarına değil, somut bilgi-kontrol-müdahale kapasitesi ölçütlerine bağlar; böylece hem muhatabın belirlenmesini hem de kusur/özen değerlendirmesinin görünür ölçütlerle yapılmasını mümkün kılar.

Bu çalışma aracı sorumluluğunun usulî boyutuna odaklanmaktadır. KVKK bakımından veri sorumlusu/veri işleyen ayrımı ile FSEK bakımından eğitim verisi ve çıktı ikamesi sorunları, devam araştırmasında bu tahsis mantığı çerçevesinde ayrıntılandırılmalıdır.

Hakem Değerlendirmesi : Dış bağımsız.

Çıkar Çatışması : Yazar çıkar çatışması bildirmemiştir.

Finansal Destek : Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review : *Externally peer-reviewed.*

Conflict of Interest : *The author has no conflict of interest to declare.*

Grant Support : *The author declared that this study has received no financial support.*

KAYNAKÇA

‘S. 1993 - No Section 230 Immunity for AI Act (2023)’ (2023)

Açıkgöz A ve Gürel M, ‘Başkasına Ait İçerikteki Fikrî ve Sınai Hak İhlalleri Nedeniyle Dijital Platformların Hukuki Sorumluluğu’ (2024) 82 İstanbul Hukuk Mecmuası 693

Akbulut B, ‘Yapay Zeka ve Ceza Hukuku Sorumluluğu’ (2023) 27 Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 270

Ariyaratne H, ‘ChatGPT and Intermediary Liability: Why Section 230 Does Not and Should Not Protect Generative Algorithms’ (SSRN 2023)

Atkinson D ve Morrison J, ‘Unsettled Law: Time to Generate New Approaches?’ (SSRN 2024)

Barberá I, ‘AI Privacy Risks & Mitigations - Large Language Models (LLMs)’ (European Data Protection Board (Support Pool of Experts Programme) 2025) <<https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf>> erişim 25 Ocak 2026

Başlar Y, ‘Fikir ve Sanat Eserleri Kanunu’nun Ek Madde 4 Hükmünün İhlali Suçları’ (2019) 77 Ankara Barosu Dergisi 37

Başlar Y, ‘İnternet Süjeleri ve Cezai Sorumlulukları’ (2022) 19 Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 603

Bernstein H, ‘Reconciling Section 230 and the First Amendment: Should Social Media Companies be Held Liable for the Consequences of Their Recommendation Algorithms?’ (2023) 19 Journal of Business & Technology Law

Botero Arcila B, ‘Is It a Platform? Is It a Search Engine? It’s ChatGPT! The European Liability Regime for Large Language Models’ (2023) 3 Journal of Free Speech Law 455

Bourtole L ve diğerleri, ‘Machine Unlearning’ *IEEE Symposium on Security and Privacy (SP)* (2021) <<https://arxiv.org/abs/1912.03817>>

Brown N, ‘Bots Behaving Badly: A Products Liability Approach to Chatbot-Generated Defamation’ (2023) 3 Journal of Free Speech Law

Browning JG, ‘Whose Bot Is It Anyway? Determining Liability for AI-Generated Content’ (2025) 45 Northern Illinois University Law Review 340

- Buiten MC, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) 12 JIPITEC 361
- Büyüktanır BGÖ, 'Çiçek Sepeti Kararı Özelinde Aracı Hizmet Sağlayıcısının Tüketicilere Karşı Sorumluluğunun Değerlendirilmesi' (2025) 16 Türkiye Adalet Akademisi Dergisi
- Cao Y ve Yang J, 'Towards Making Systems Forget with Machine Unlearning' *IEEE Symposium on Security and Privacy (SP)* (2015) <<https://www.ieee-security.org/TC/SP2015/papers-archived/6949a463.pdf>>
- Choi S, 'Assessing the Efficacy of Third-Party Liability Copyright Doctrines against Platforms That Host AI-Generated Content' (2025) 66 Boston College Law Review 1087
- Cobbe J ve Singh J, 'Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges' (2021) 42 Computer Law & Security Review 105573
- Council of the European Union, 'Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World' (09 Aralık 2023) <<https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/>> erişim 24 Ocak 2026
- Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts - General Approach' (2022) ST 14954/22 <<https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>>
- Çevik İ, 'Avrupa Birliği Dijital Hizmetler Yasası'nın Değerlendirmesi' (2023) 8 YBHD 387
- Demez İ, '5651 Sayılı Kanun'un İnternet Adreslerine Erişimin Engellenmesine İlişkin 9. Maddesinin İptali ve Öneriler' (2024) 15 Türkiye Adalet Akademisi Dergisi 177
- Depoorter B ve Walker RK, 'Copyright False Positives' (2014) 89 Notre Dame Law Review 319
- Dini L, 'Redefining Section 230 Immunity' (2024) 49 Seattle University Law Review 211
- Dumas V, 'Enigma Machines: Deep Learning Algorithms as Information Content Providers under Section 230 of the Communications Decency Act' [2022] Wisconsin Law Review 1581
- Ekingen E ve Deniz MÖ, '7392 ve 7416 Sayılı Kanunlarla Yapılan Değişikliklerin Aracı Hizmet Sağlayıcı Olarak Çevrimiçi Çok Taraflı Platformların Sorumluluklarına ve Tüketicilere Etkileri' (2022) 69 Adalet Dergisi
- Eren F, *Borçlar Hukuku Genel Hükümler* (21 Baskı, Yetkin Yayınları 2017)

- European Commission, 'European Commission, Commission Staff Working Document: Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' (2020) SWD(2020) 348 final <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0348>>
- European Data Protection Board, 'Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models' (2024) Opinion 28/2024 <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf> erişim 25 Ocak 2026
- European Data Protection Supervisor, 'Generative AI and the EUDPR: Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems (Version 2)' (2025) <https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf> erişim 25 Ocak 2026
- European Parliament, 'Amendments Adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (2023) P9_TA(2023)0236 <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf>
- European Parliament, Answer P-002793/2025(ASW) given by Executive Vice-President Virkkunen on behalf of the European Commission (21 August 2025)
- Forbrukerrådet, *Ghost in the Machine: Addressing the consumer harms of generative AI* (June 2023)
- Frosio G (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020)
- Geiger C, Frosio G ve Izyumenko E, 'Intermediary Liability and Fundamental Rights' [2019] CEIPI Research Paper No. 2019-06
- Ginart AA ve diğerleri, 'Making AI Forget You: Data Deletion in Machine Learning' (arXiv:190705012 2019) <<https://arxiv.org/abs/1907.05012>>
- Graux H ve diğerleri, 'Interplay between the AI Act and the EU digital legislative framework' (European Parliament (Policy Department for Transformation, Innovation and Health) 2025)
- Guo C ve diğerleri, 'Certified Data Removal from Machine Learning Models' (arXiv:191103030 2019) <<https://arxiv.org/abs/1911.03030>>
- Güçlütürk OG, *Yapay Zekâ ve Verinin Kullanımı* (1 Baskı, On İki Levha Yayıncılık 2022)
- Hacker P, 'AI Regulation in Europe: From the AI Act to Future Regulatory Challenges' (arXiv:231004072 2023)
- Hacker P, Engel A ve Mauer M, 'Regulating ChatGPT and other Large Generative AI Models' (arXiv 2023) <<https://arxiv.org/abs/2302.02337>>

- Hassoun A ve diğerleri, 'The Influencer Next Door: How Misinformation Creators Use GenAI' (arXiv:240513554 2024)
- Helberger N ve Diakopoulos N, 'ChatGPT and the AI Act' (2023) 12 Internet Policy Review
- Henderson P, Hashimoto T ve Lemley M, 'Where's the Liability in Harmful AI Speech?' (2023) 3 Journal of Free Speech Law
- Henderson P, Hashimoto T ve Lemley M, 'Challenges for Foundation Model Liability and Regulatory Regimes: An Analysis of US Law' in *The Cambridge Handbook of Generative AI and the Law* (Cambridge University Press 2025)
- Husovec M, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Technology Law Journal
- Işık A, 'Anayasa Mahkemesi'nin 5651 Sayılı Kanun'un 9. Maddesi Bağlamında İnternete Erişimin Engellenmesine Dair Değişen Yaklaşımının Değerlendirilmesi' (2022) 30 Selçuk Üniversitesi Hukuk Fakültesi Dergisi 967
- Işık A, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları* (1 Baskı, On İki Levha Yayıncılık 2023)
- İlalan YE, *İnternet Ortamında Kişilik Haklarının İhlali, Korunması ve Başvuru Yolları* (Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi 2022)
- Kaya MB, *İnternet Hukuku* (2 Baskı, On İki Levha Yayıncılık 2021)
- Kiss NFR, 'The Twenty-Six Words That Created the Internet... and then Maybe, Kind Of, Destroyed Society: Understanding and Reforming Section 230 of the Communications Decency Act' (2024) 31 Michigan Technology Law Review 131
- Kişisel Verileri Koruma Kurumu, 'Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi' (KVKK Yayınları No: 71 2025) <<https://www.kvkk.gov.tr/Icerik/2038/kisisel-verilerin-silinmesi-yok-edilmesi-veya-anonim-hale-getirilmesi>> erişim 25 Ocak 2026
- Kişisel Verileri Koruma Kurumu, 'Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence' (KVKK Yayınları No: 33 2024) <<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/58678459-eba4-451a-a2f3-c1baf17b90f5.pdf>> erişim 25 Ocak 2026
- Kişisel Verileri Koruma Kurumu, *Veri Sorumlusu ve Veri İşleyen* (KVKK Yayınları No: 106, Haziran 2025)
- Klonick K, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review
- Koca M ve Üzülmöz İ, *Türk Ceza Hukuku Genel Hükümler* (9 Baskı, Seçkin Yayıncılık 2016)

- Lemoine L ve Vermeulen M, 'Assessing the extent to which Generative AI falls within the scope of the Digital Services Act: an initial analysis' (2023) draft
- Lin Y ve Guan T, 'From safe harbours to AI harbours: reimagining DMCA immunity for the generative AI era' (2025) 20 Journal of Intellectual Property Law & Practice 3
- Lu C-C, 'From safe harbours to over-enforcement: the rise of AI and copyright monitoring' (2025) 20 Journal of Intellectual Property Law & Practice 7
- National Institute of Standards and Technology, 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)' (2023) NIST AI 100-1 <<https://doi.org/10.6028/NIST.AI.100-1>> erişim 25 Ocak 2026
- Nguyen TT ve diğerleri, 'A Survey of Machine Unlearning' (arXiv:220902299 2022) <<https://arxiv.org/abs/2209.02299>>
- Novelli C ve diğerleri, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity' [2024] Computer Law & Security Review
- Ofchus K, 'Cracking the Shield: CDA Section 230, Algorithms, and Product Liability' (2023) 46 University of Arkansas at Little Rock Law Review 27
- Palumbo A, 'The Digital Services Act and the Protection of Fundamental Rights' [2024] European Law Blog
- Revolidis I, 'Generative AI Content Misuse and the DSA' (Universitat Oberta de Catalunya 2024)
- Riordan J, *The Liability of Internet Intermediaries* (Oxford University Press 2016)
- Sawyer MS, 'Filters, Fair Use and Feedback: User-Generated Content Principles and the DMCA' (2009) 24 Berkeley Technology Law Journal 363
- Schyns C, *The Lobbying Ghost in the Machine: Big Tech's covert defanging of Europe's AI Act* (Corporate Europe Observatory, February 2023)
- Sekhri A ve diğerleri, 'Remember What You Want to Forget: Algorithms for Machine Unlearning' (arXiv:210303279 2021) <<https://arxiv.org/abs/2103.03279>>
- Shaheen LM, 'Section 230's Immunity for Generative Artificial Intelligence' (2024) 15 Seattle Journal of Technology, Environmental & Innovation Law 1
- Simo F, 'Reklamlara yaklaşımımız ve ChatGPT'nin ulaşılabilirliğini artırma hedefimiz' (*OpenAI*, 16 Ocak 2026) <<https://openai.com/tr-TR/index/our-approach-to-advertising-and-expanding-access/>>
- Snider E, 'Evolving Online Terrain in an Inert Legal Landscape: How Algorithms and AI Necessitate an Amendment of Section 230 of the Communications Decency Act' (2023) 107 Minnesota Law Review 1829
- Urban JM ve Quilter L, 'Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act' (2006) 22 Santa Clara Computer & High Technology Law Journal 621

- Varga D, ‘Section 230 and Generative AI: How (Not) to Regulate Algorithmic Defamation’ (Honors thesis, Oregon State University 2024)
- Veale M ve Quintais JP, ‘The Obligations of Providers of General-Purpose AI Models’ (2025) <<https://files.michael.v/papers/VealeQuintaisObligationsofGPAIProvidersNov2025.pdf>>
- Volokh E, ‘Large Libel Models? Liability for AI Output’ (2023) 3 Journal of Free Speech Law 489
- Wilman F, ‘The EU’s System of Knowledge-Based Liability for Hosting Service Providers’ (2021) 12 JIPITEC 317
- Yünlü S, ‘Üretici Yapay Zekâ Kaynaklı Norm ve Kişi Bazlı Hukuki Sorumluluk’ (2024) 72 Adalet Dergisi 501