ARTIFICIAL INTELLIGENCE REGULATION IN TÜRKİYE: CURRENT POSITION AND FUTURE TRAJECTORY

Asst. Prof. Dr. Osman Gazi Güçlütürk
Galatasaray University

Attribution: Güçlütürk, O. G. (2026). Artificial intelligence regulation in Türkiye: Current position and future trajectory. In H. Arslan, A. Taşdelen, E. Kuzucu Hıdır, & O. A. Çetin (Eds.), *Artificial intelligence and national technology reflections* (pp. 277–302). Turkish Academy of Sciences. https://doi.org/10.53478/TUBA.978-625-6110-86-1.ch12

10.53478/TUBA.978-625-6110-86-1.ch12

ARTIFICIAL INTELLIGENCE REGULATION IN TÜRKİYE: CURRENT POSITION AND FUTURE TRAJECTORY

Asst. Prof. Dr. Osman Gazi Güçlütürk
Galatasaray University

Abstract

The penetration of artificial intelligence systems as general-purpose technologies into every aspect of social and economic life tests the adaptation capacity of legal systems to this dynamic process. This study analyses Türkiye's current position in AI governance and its future regulatory trajectory across three fundamental layers. First, although Türkiye does not yet have a stand-alone AI-specific statute, it evaluates how existing legal norms, such as the Law on the Protection of Personal Data, the Turkish Code of Obligations, and the Turkish Criminal Code, are applied to AI applications. Second, it posits that harmonisation with the EU AI Act (AIA) is not a mere policy choice but a commercial and technical necessity due to the Customs Union relationship between Türkiye and the EU. In this context, the nature of the AIA as a product safety instrument and its direct implications for Türkiye are examined. Third, the institutional transformation and the future AI governance landscape in Türkiye is addressed through the allocation of mandates between the newly established cybersecurity authority (SGB) and the Directorate General for National Technology and Artificial Intelligence (MTYZGM) under the Ministry of Industry and Technology. By providing a critical analysis of the recent legislative proposals submitted to the Turkish Grand National Assembly, the text emphasises the importance of Türkiye developing a unique regulatory strategy that fosters innovation while protecting fundamental rights. The study concludes that AI is not a transient hype but becoming a permanent and horizontal element of the Turkish legal framework.

Keywords

AI Law, AI Act, AI Governance, AI Standardisation, Digital Transformation

Introduction

The rapid advancement of artificial intelligence has generated significant concern as such systems increasingly function as a general-purpose technology capable of deployment across a wide range of social and economic domains (Brandao, 2025; Sabherwal & Grover, 2024). Artificial intelligence is no longer confined to experimental or marginal applications but is now routinely used in contexts where its outputs may directly affect fundamental aspects of individual lives. These include, for example, medical settings in which algorithmic systems assist in the diagnosis of disease or the prioritisation of patients (Al-Antari, 2023), labour markets in which automated tools are used to screen job applicants or evaluate worker performance (Broecke, 2023), and financial services where artificial intelligence informs decisions on creditworthiness (Langenbucher, 2025), insurance pricing (Nowak, 2024), or fraud detection (Singh et al., 2025). As artificial intelligence becomes more deeply embedded in these decision-making processes, its influence on individual rights, opportunities, and welfare becomes correspondingly more significant.

This growing entanglement of artificial intelligence with everyday life raises a range of ethical, social, and regulatory questions. It is increasingly unclear where appropriate boundaries should be drawn in the use of large language model-based systems and other generative tools. Questions arise as to whether such systems should be relied upon for a broad spectrum of tasks, including the provision of information, advice, or creative output, and under what conditions such reliance may be justified (Leslie, 2019). Further concerns relate to the permissibility of using personal data (Retornaz & Güçlütürk, 2023) or copyrighted materials (Güçlütürk, 2022a) in the training of increasingly powerful models, particularly where such practices may conflict with established data protection principles or intellectual property rights. The use of artificial intelligence by children for information retrieval and learning purposes also raises issues regarding developmental impacts, exposure to misinformation, and the erosion of critical thinking skills (Zhai et al., 2024; Anderson, 2024). More broadly, the existing regulatory framework must confront how the society can be protected from the adverse effects of advanced generative systems, especially those capable of convincingly imitating human conversation, voice, images, or video, thereby facilitating deception, manipulation, or the large-scale dissemination of false or harmful content.

What is beyond dispute is that artificial intelligence is not a transient phenomenon. Its continued development and diffusion are inevitable, and the challenges it presents therefore demand sustained and systematic responses. Determining the appropriate form of such responses is, however, far from straightforward. Artificial intelligence is a dynamic and rapidly evolving technology, the capabilities and applications of which

change continuously and often unpredictably (Hirsch-Kreinsen, 2024). Traditional mechanisms for addressing technological risk, such as public education initiatives, awareness raising efforts, voluntary or soft law instruments, and reliance on already-existing legal frameworks, were largely developed without modern artificial intelligence in mind. In regulatory studies, despite the recent emergence of certain common references in major regulatory instruments, there is no uniformly agreed-upon definition of what AI is (Güçlütürk, 2022b). Although this does not imply that existing tools are entirely ineffective, it does indicate that their adequacy cannot be assumed (Güçlütürk, 2025). There is a clear need for careful examination of whether current regulatory and governance mechanisms are capable of addressing the distinctive risks posed by contemporary artificial intelligence systems, or whether new or adapted approaches are required.

Going further, even if the analysis confirms a genuine need for amendment, one should be wary of concluding too readily that such a need must be addressed through new legislation. Whether regulatory intervention is warranted, which approach ought to be adopted, and which regulatory instrument should be deployed are closely related yet analytically distinct questions. Ongoing regulatory developments demonstrate that a wide array of tools and approaches is available, each of which warrants careful examination in light of the underlying objectives of the proposed amendments

With respect to the overarching approach, the relative strengths and vulnerabilities of individual jurisdictions inevitably shape the regulatory posture they adopt. As the world's foremost exporter of AI, the United States tends to favour a comparatively liberal regulatory stance. Although restrictive measures have emerged at the state level, federal authorities have even attempted to impose a ten-year moratorium on state-level AI legislation. Although this proposal did not succeed, a comparable outcome has been pursued indirectly through amendments to the allocation of federal funding that disadvantage states with more restrictive AI laws. While the United States remains broadly freedom-oriented, it simultaneously imposes targeted restrictions on China, its principal competitor in the AI race, in order to limit Chinese access to critical hardware and to constrain the market penetration of Chinese-origin products and services. The European Union (EU) by contrast, is not a leading developer of AI and therefore relies on its regulatory authority and the so-called Brussels effect to assert influence in the field. Accordingly, no single regulatory approach can claim universal applicability.

A comparable divergence is observable at the level of regulatory instruments. Statutory law is authoritative and powerful, yet also rigid, and may prove ill-suited to addressing the dynamic challenges posed by AI. Legislation must be sufficiently broad to withstand the passage of time, while remaining sufficiently precise to ensure legal

certainty. Principles, in turn, are typically enforceable only when reinforced by secondary legislation, official guidance, and technical standards. The design of an effective regulatory framework for AI therefore requires careful consideration not only of the chosen approach but also of the full spectrum of available regulatory instruments.

1. Existing Legal Framework Applicable to AI under Turkish Law

At the time of writing this chapter, there is no AI specific legislation under Turkish law. It is nevertheless essential to emphasise that AI, like any other novel technological application, irrespective of how advanced it becomes, does not operate in a legal vacuum (Güçlütürk, 2025). Legal frameworks are generally designed with varying scopes of application and, in every jurisdiction, contain rules that are intended to apply irrespective of the novelty or dynamic character of the subject matter they regulate. Constitutional provisions on freedom of expression provide a clear illustration of this approach. Although such provisions typically make no explicit reference to the internet or cyberspace, it is now almost universally accepted that freedom of expression, despite significantly predating the invention of the internet, applies equally to expression and interaction taking place online (Murray, 2023). In a similar manner, the absence of AI-specific legislation does not preclude the applicability of existing rules within the Turkish legal framework to AI-related activities and systems.

It is neither possible nor necessary to identify exhaustively every legal provision that may potentially apply to AI. Given the increasingly horizontal and cross-sectoral nature of AI, almost every area of law is likely to intersect with AI-driven processes or outcomes at some point. Nevertheless, certain legal frameworks are particularly closely connected to the development and operation of AI systems and may, in practice, function as quasi-regulation of AI in specific respects. Data protection law is the most prominent example in this regard. Owing to the data-intensive nature of AI, data protection regimes are not only directly applicable to many AI use cases but also exert a shaping influence on the design, training, and deployment of AI systems (Yanamala et al., 2023).

Data protection authorities worldwide have actively monitored the evolution of AI, examined its interaction with data protection principles, and issued guidance and, in some jurisdictions, specific regulatory instruments (Information Commissioner's Office [ICO], 2023; European Data Protection Board [EDPB], 2024). The Turkish Data Protection Authority is no exception. It has addressed various aspects of data processing and AI through events and webinars and has issued two guidelines in this field, one providing general recommendations (Kişisel Verileri Koruma Kurumu [KVKK], 2021) and another analysing the applicability of the Turkish Data Protection

Law No. 6698 in the context of generative AI (Kişisel Verileri Koruma Kurumu [KVKK], 2025). Accordingly, the fact that the Turkish Data Protection Law does not explicitly refer to AI does not prevent its application to AI-driven data processing activities. On the contrary, its broadly drafted provisions are capable of applying to such activities and may, where necessary, require interpretation in light of the specific dynamics introduced by the use of AI (Güçlütürk, 2022b). A comparable approach is evident in the EU. The Artificial Intelligence Act ("AIA") expressly provides that it applies without prejudice to the General Data Protection Regulation ("GDPR"). As a result, where personal data are processed for or by AI systems, the data governance requirements introduced by the Artificial Intelligence Act must be complied with in addition to, rather than as a substitute for, obligations arising under data protection law.

Beyond data protection, several other fields of law are highly relevant to the regulation of AI systems and applications. When copyrighted material is processed for the purpose of training AI models, the applicable copyright regime, including Law No. 5846 on Intellectual and Artistic Works in Türkiye, must be considered (Güçlütürk, 2022a). Questions of liability arising from AI-related harm are to be addressed within the framework of tort and contractual liability, notably under the general provisions of the Turkish Code of Obligations Law No. 6098 (Aksoy, 2025). Similarly, where an AI-powered system or tool is used in the commission of a criminal offence, the relevant provisions of the Turkish Criminal Code Law No. 5237 apply (Altunç, 2021). These examples are illustrative rather than exhaustive, and it would be impractical to attempt to identify every potentially relevant rule. The underlying principle is, however, clear. The absence of an explicit AI-specific provision does not entail the absence of applicable legal rules (Güçlütürk, 2025).

A further and more complex question is whether the mere existence of applicable rules is sufficient to ensure fair and effective governance of AI. The application of pre-existing legal provisions to AI may, in certain cases, produce inadequate or even unjust outcomes. Such situations may indicate the need for regulatory intervention, potentially in the form of legislative amendment or the adoption of new, more targeted rules. In summary, although there is currently no AI-specific legislation in Turkish law, a range of existing legal rules are applicable to AI. Some of these rules apply directly and, in a manner, broadly consistent with approaches adopted in other jurisdictions, particularly in the field of data protection. Others apply in a more tentative manner and require further assessment to determine their adequacy or the necessity for reform. This evaluative process has already begun in Türkiye and will be examined in detail in the following chapter.

2. Ongoing Regulatory Works and the Future

Having examined the existing legal framework, this section turns to the ongoing regulatory work on AI in Türkiye and offers a forward-looking assessment of likely developments. The regulatory trajectory may be analysed across three interrelated layers. First, there are ongoing initiatives that evaluate the capacity of the current legislative framework to respond to AI-related challenges, which may ultimately lead to the adoption of AI-specific legislation or targeted legislative amendments. Second, there is the continuing and expected harmonisation of Turkish law with the EU Acquis Communautaire and relevant international frameworks, a process that will inevitably shape the legal regime applicable to AI. Third, there is the anticipated proliferation of secondary legislation, administrative guidance, and technical standards, which are likely to constitute the practical backbone of AI governance.

Before examining each layer in detail, a general tendency attesting to the enduring presence of AI in legislative agendas can be identified. Notwithstanding the diversity of regulatory instruments available, as outlined above, there is a discernible inclination across jurisdictions towards the adoption of statutes and other legislative texts specifically directed at AI. This development is hardly surprising. Regardless of the overarching approach selected and the breadth of alternative regulatory tools at one's disposal, AI regulation will inevitably entail legislative components for several reasons. First, AI regulations have the potential to affect fundamental rights, including the right to privacy, the freedom to conduct business, and the right to employment. In numerous jurisdictions including Türkiye, as set forth under Article 13 of the Turkish Constitution, provisions bearing on fundamental rights must be enacted through primary legislation rather than secondary instruments. In Germany, the *Wesentlichkeitstheorie* developed by the Federal Constitutional Court holds that all decisions of essential importance for the realisation of fundamental rights must be taken by the legislature itself and cannot be delegated to the executive (Federal Constitutional Court of Germany, 2021), a principle reinforced by Article 19(1) of the Basic Law, which requires that any statute restricting a fundamental right must do so generally and expressly identify the right concerned. In France, Article 34 of the Constitution reserves to *la loi* the determination of rules concerning civic rights and the fundamental guarantees afforded to citizens for the exercise of public liberties, thereby precluding the regulation of such matters by executive decree alone. In Spain, Article 53(1) of the Constitution provides that the rights and freedoms recognised in Chapter II of Title I bind all public authorities and that the exercise of such rights may be regulated only by statute, with Article 81 further requiring that the development of fundamental rights and public liberties be effected through an *ley orgánica*. A comparable logic underpins the European Convention on Human Rights, where the requirement that any interference with protected rights be "prescribed by law" or "in

accordance with the law" has been interpreted by the European Court of Human Rights as demanding not merely a formal legal basis but also adequate accessibility, foreseeability, and protection against arbitrariness. Taken together, these traditions reflect a shared conviction that interferences with fundamental rights must be effected through primary legislation rather than through secondary legislation or executive action, a conviction that necessarily shapes the legislative architecture of AI regulation.

Second, given the dynamic character of the field, the formulation of general principles at the legislative level, with technical and operational details left to secondary legislation, administrative guidance, or technical standards, constitutes a more prudent course than the enactment of detailed provisions liable to become obsolete or impracticable within a short period. Türkiye is no exception in this regard, and developments are accordingly observable across all three regulatory layers.

2.1. Policy Frameworks

Returning to the examination of the regulatory framework in Türkiye, although Türkiye does not currently have an AI-specific statute, as discussed above, several national policy documents are intended to guide future regulatory developments, alongside legislative proposals that have already been submitted to Parliament. The most significant policy document in this context is the National Artificial Intelligence Strategy, which spans the period from 2021 to 2025 (Presidency of the Republic of Türkiye Digital Transformation Office [DTO] & Ministry of Industry and Technology, 2021). The Strategy was adopted as Türkiye's first comprehensive national policy framework on AI and was explicitly designed as an exploratory instrument, reflecting both the novelty of the field and the rapid pace of technological change. It articulates a vision of creating global value through an agile and sustainable AI ecosystem, structured around six strategic priorities, one of which is explicitly devoted to regulation and socioeconomic adaptation. Within this priority, the Strategy recognises the need to review existing legal and administrative frameworks, to identify ethical and legal risks associated with AI deployment, and to develop regulatory approaches that balance innovation with the protection of fundamental rights and public interests. In this respect, the Strategy does not propose immediate binding regulatory obligations but rather envisages preparatory work, including impact assessments, regulatory sandboxes, and alignment with international principles on trustworthy and responsible AI. It also foresees the development of governance mechanisms and coordination structures to support future regulatory action, thereby laying the groundwork for more concrete legal intervention at a later stage. The Strategy is supplemented by an action plan in 2024 (Presidency of the Republic of Türkiye Digital Transformation Office [DTO] & Ministry of Industry and Technology, 2024).

The implementation period of the current Strategy has ended, and preparatory work on a successor strategy has been ongoing. Although no official information has yet been published regarding the content of the next Strategy, it is expected that lessons learned during the initial implementation phase, combined with the accelerating evolution of AI technologies, will influence its design. In this regard, a shorter strategic cycle with more concrete and measurable objectives, rather than broadly framed and ambitious targets, may offer greater regulatory responsiveness and adaptability.

Another development of particular significance is the establishment of the first technology-specific parliamentary research commission in Türkiye. The commission, officially entitled the Parliamentary Research Commission Established to Determine the Steps to Be Taken Regarding the Benefits of Artificial Intelligence, to Establish the Legal Infrastructure in This Field, and to Identify Measures Aimed at Preventing the Risks Arising from the Use of Artificial Intelligence, was created by parliamentary decision in October 2024 and commenced its work in February 2025 (Türkiye Büyük Millet Meclisi, 2024). Through regular meetings and field visits, the commission has examined the impact of AI on both the public sector and industry, with a view to assessing whether the existing legislative framework is capable of addressing AI-driven risks and challenges. The outcome of this process has been published as a 900-page-long report, which contains detailed examination of both the existing legislative framework as well as the need for further amendments (Türkiye Büyük Millet Meclisi, 2026). Although the reports of such commissions are not legally binding *per se* and do not automatically lead to legislative change, they have traditionally played an influential role in shaping subsequent regulatory initiatives and legislative agendas.

2.2. Legislative Proposals

The existence of a parliamentary commission does not limit the legislative initiative of individual members of Parliament. Under the Turkish Constitution, members of Parliament are entitled to submit independent legislative proposals. To date, three AI-related proposals have been submitted by individual members, each signed by a single member, a factor that, while not legally determinative, suggests a limited degree of political consensus and stakeholder support.

The first proposal, submitted in June 2024, was explicitly titled "Artificial Intelligence Law" and consisted of eight articles (Gergerlioğlu, 2024). Although it purported to establish a framework for the secure, ethical, and fair use of AI, as well as for the protection of personal data and privacy, it suffers from significant conceptual and structural shortcomings. In particular, it adopts an excessively broad and outdated definition of AI based on human-like cognitive tasks, an approach that risks conceptual confusion given that contemporary AI systems do not replicate human cognition but merely produce functionally comparable outputs through fundamentally different technical processes. The proposal also attempts to transpose

elements of the AIA into Turkish law in a highly compressed and abstract manner, imposing obligations on so-called high-risk systems without defining these systems, specifying the applicable measures, or clarifying the criteria for risk classification. As a result, it fails to meet basic standards of legal certainty.

The second proposal, submitted in November 2025, adopts a more limited and use-case-specific approach, focusing primarily on AI-powered chatbots used to disseminate illegal, indecent, or misleading content (Öztürk, 2025). Its definition of an AI system is more technically grounded than that of the first proposal, but it relies heavily on enumerating specific techniques, such as machine learning or neural networks, which may render the definition vulnerable to rapid obsolescence. The proposal introduces regulatory obligations for AI service providers, including requirements relating to transparency and auditability of training data, content verification mechanisms to mitigate misinformation, controls aimed at reducing hallucinations, human oversight for high-risk applications, and periodic cybersecurity testing, with administrative fines for non-compliance. While these obligations broadly resemble those found in other jurisdictions, particularly in the EU, the proposal provides little detail regarding their scope and implementation. Moreover, the decision to introduce these obligations through amendments to the existing Cybersecurity Law No. 7545 raises concerns regarding both conceptual coherence and regulatory overreach.

The third proposal, submitted in December 2025, is even narrower in scope and does not seek to establish a general AI regulatory framework (Özdemir, 2025). Instead, it proposes an amendment to Law No. 5651 on the Regulation of Publications on the Internet by introducing an obligation for content providers to clearly label audio, visual, or written content generated by AI. While the underlying objective of enhancing transparency and managing the risks associated with AI-generated content is legitimate, the proposal raises several concerns. Its scope is effectively limited to publicly accessible internet content, leaving closed networks and private communications outside its reach. The proposal also fails to define what constitutes a visible label or marker, leaving considerable uncertainty for content providers. Most critically, it links non-compliance with criminal liability under the offence of publicly disseminating misleading information, despite the fact that the proposed obligation relates to the source of content rather than its truthfulness. This creates a risk of disproportionate and unintended consequences, including the criminalisation of objectively accurate content merely because its AI-generated origin was not disclosed.

Taken together, these developments illustrate both the growing awareness of AI-related risks within the Turkish legal and political system and the difficulties inherent in translating that awareness into coherent and effective regulation. While existing initiatives demonstrate an emerging regulatory momentum, they also reveal the need

for greater conceptual clarity, technical precision, and institutional coordination. The future regulatory framework for AI in Türkiye is therefore likely to depend not only on the adoption of new legislative instruments but also on the careful calibration of existing laws, informed by empirical evidence, comparative experience, and the strategic guidance provided by national policy instruments such as the National Artificial Intelligence Strategy.

2.3. Harmonisation Efforts with the EU AI Act

Turning to another layer, harmonisation with EU law constitutes a central element of Türkiye's prospective AI regulatory roadmap. Although the first legislative proposal discussed above cannot be regarded as a sound attempt at harmonisation with the AIA, the AIA is nonetheless frequently referenced in regulatory debates in Türkiye, and it is widely expected that Turkish law will eventually be aligned with the AIA at least to a certain extent (Güçlütürk, 2025). This expectation is not based on the assumption that the AIA represents a flawless or universally transferable regulatory model. Rather, it reflects the structural and legal realities governing the relationship between Türkiye and the EU.

Türkiye is not a Member State of the EU but remains a candidate country. The legal and political complexities of Türkiye's accession process fall outside the scope of this analysis. For present purposes, it is sufficient to note that the prospect of eventual membership and the general obligation to harmonise domestic legislation with the EU Acquis Communautaire constitute only a secondary factor in Türkiye's engagement with the AIA.

A more decisive factor is Türkiye's functioning customs union with the EU. The EU-Türkiye customs union represents a distinctive arrangement within the EU enlargement framework. Unlike the EU internal market, which is based on the four fundamental freedoms, the customs union is limited in scope and primarily concerns the free movement of certain categories of goods. Under the customs union regime, products covered by the relevant agreements are deemed to circulate freely between the EU and Türkiye, such that a product lawfully placed on the market in one territory is treated as having entered the market of the other (Güçlütürk, 2025).

At first glance, the connection between an older, product-oriented customs union framework and a recent piece of EU legislation addressing a frontier technology such as AI may appear tenuous. Understanding this connection requires closer examination of the legal nature of the AIA. Despite its short name, "Artificial Intelligence Act", the AIA is not a comprehensive or horizontal AI regulation. Rather, it is primarily a product safety instrument adopted within the logic of the EU new legislative framework, supplemented by additional provisions addressing the protection of fundamental rights and European values (Güçlütürk, 2025). The AIA

deliberately refrains from regulating several highly contentious areas of AI governance, including personal data protection, intellectual property issues related to AI training and outputs, and civil liability for AI-related harm. Instead, it conceptualises AI systems and general-purpose AI models as products and imposes obligations that must be fulfilled before such products are placed on the EU market or put into service.

In line with this approach, the AIA does not generally regulate AI systems or models that are developed or used exclusively outside the scope of market placement or service provision within the EU. This product safety orientation is particularly evident in the regime governing prohibited practices. Article 5 of the AIA sets out an exhaustive list of prohibited AI practices, commonly referred to as systems posing unacceptable risk, reflecting concerns rooted in the protection of fundamental rights and values enshrined in the Charter of Fundamental Rights of the EU. Although certain concepts used in these provisions, such as manipulation, remain open to interpretation, the legal consequence is clear. Practices falling within this category may neither be placed on the market nor used within the EU and must be withdrawn if already deployed. Notably, despite extensive debate during the legislative process, the final text of the AIA does not prohibit the development of such systems within the EU or their export to third countries. While the AIA contains stronger and more explicit references to safety and fundamental rights than traditional product safety legislation, such as that governing toys or personal protective equipment, these elements do not alter its core character as a product safety regime. Comparable rights-oriented considerations have long existed in other product safety fields, notably medical device regulation, without transforming their fundamental regulatory nature.

Once the AIA is understood primarily as product safety legislation, its relevance for Türkiye under the customs union framework becomes clearer. Product safety legislation constitutes a central pillar of the customs union relationship. Placing a product on the market is the decisive triggering event for the application of product safety rules. As a general principle, products covered by the customs union must comply with the applicable technical requirements and conformity assessment procedures. Because products placed on the Turkish market are, for customs union purposes, deemed to have entered the EU market, they must satisfy equivalent technical standards. This obligation does not stem directly from EU law, as Türkiye is not a Member State, but from bilateral commitments, most notably the 2006 agreement under which Türkiye undertook to harmonise its conformity assessment procedures with EU rules, while both parties agreed to mutually recognise conformity assessments conducted within their respective systems.

The practical implication is that an AI system falling within the scope of the AIA and placed on the Turkish market, insofar as it is covered by the customs union, would be treated as having entered the EU market and would therefore need to comply with the applicable technical requirements and operator obligations under the AIA. These obligations include, for example, the conduct of conformity assessments and the preparation of an EU declaration of conformity by providers. Although Türkiye has already harmonised a substantial body of EU product safety legislation within the customs union framework, no equivalent regime reflecting the AIA has yet been adopted, which is unsurprising given the recency of the AIA itself. Nevertheless, in order to avoid disruptions to the circulation of AI-related products between the EU and Türkiye, it is necessary for Türkiye to establish an equivalent regulatory regime before the relevant obligations under the AIA become applicable. Under the current text of the AIA, obligations for certain high-risk AI systems are scheduled to apply from 2 August 2026 or 2 August 2027, depending on the classification method, although the Commission's most recent omnibus proposal envisages postponement to later dates, subject to the establishment of adequate safeguards (European Commission [EC], 2025). An agreement has been reached between two European co-legislators, the Council of the EU and the European Parliament regarding the omnibus (Council of the European Union, 2026).

This structural interdependence explains why it is not merely reasonable but effectively inevitable that Türkiye will adopt a regulatory framework broadly aligned with the AIA (Güçlütürk, 2025). The motivation lies not in an idealised perception of the AIA as the optimal AI governance model, but in the functional requirements of the customs union. Nevertheless, three significant issues must be considered before such alignment can operate seamlessly. First, the list of products covered by the customs union is set out in an annex to the relevant decision, and the AIA is not explicitly included in that list. This omission does not, however, preclude harmonisation. Türkiye's alignment with EU law is governed by a complex and evolving process involving multiple institutions and negotiation channels, and regulatory areas not expressly listed in customs union instruments have previously been incorporated into Turkish law through broader harmonisation efforts. A similar approach is likely in the case of the AIA.

Second, the customs union agreement reflects the realities of an earlier technological era and does not address the cross-border movement of intangible assets, particularly data. This omission is increasingly problematic in a context where products are no longer purely physical but incorporate essential digital components and rely on continuous data flows. The absence of an equivalent framework for EU Türkiye data transfers represents a significant regulatory and practical challenge. At the time of writing, no mutual adequacy decision exists between the EU and Türkiye, meaning

that personal data transfers must rely on alternative mechanisms designed to provide appropriate safeguards. This unresolved issue underscores the limits of the existing customs union framework when applied to contemporary, data-driven technologies such as AI and highlights the need for more comprehensive legal coordination beyond traditional product regulation.

Third, it is important to recognise that as a non-EU member, Türkiye is not required to adopt EU legislation verbatim. Any harmonisation efforts must be undertaken only after a comprehensive evaluation of Türkiye's existing relationships with the EU and its international obligations. Crucially, such efforts must also account for national dynamics to ensure that legislative steps do not stifle AI innovation. The objective should be to establish a framework that fosters AI development and aligns with Türkiye's specific national goals without imposing prohibitive or harmful restrictions.

Finally, addressing the third layer, despite the current absence of specific primary and secondary legislation governing AI under Turkish law, a lacuna inherently linked to the lack of a comprehensive legislative framework, it is reasonable to anticipate the proliferation of secondary regulations, guidelines, and soft law instruments in the near future. In fact, this regulatory evolution is already underway in Türkiye; as previously noted, independent bodies such as KVKK have already issued specific guidelines. A pivotal development in this stage is the definitive identification of the administrative bodies vested with regulatory powers, including the competence to enact secondary legislation. In this regard, a recent Presidential Decree (PD) has strategically allocated AI governance mandates between two primary authorities.

The amendments introduced to PDs No. 1 and No. 177 via PDs No. 191 and 192, published in the Official Gazette dated 26.12.2025, have effectively resolved the lingering ambiguities surrounding Türkiye's institutional framework for AI governance. Most notably, the supplementary provisions added to PD No. 177 confirm that the recently established cybersecurity authority, titled *Siber Güvenlik Başkanlığı* (SGB) in Turkish, has formally succeeded the Digital Transformation Office. Despite the titular emphasis on cybersecurity, the SGB's mandate has been solidified to encompass the broader digital government and AI landscape. Its newly defined powers include conducting legislative studies for public-sector AI applications, harmonising national legislation with international standards, and determining data governance processes. Furthermore, the establishment of the "Directorate General for Public Artificial Intelligence" as a service unit under the SGB underscores the institutionalisation of AI within public administration.

This structural shift in the public sector is mirrored in the broader ecosystem by the reorganisation within the Ministry of Industry and Technology. The former Directorate General for National Technology has been renamed the Directorate

General for National Technology and Artificial Intelligence (MTYZGM). This redesignation serves as a significant policy manoeuvre, reflecting the strategic priority assigned to AI technologies rather than considering it as an ordinary branch of the national technology movement. The MTYZGM's expanded jurisdiction now covers the development of AI in line with ethical principles, the formulation of policy proposals, and the enhancement of data, infrastructure, and human capital. By empowering this directorate to support R&D activities and manage cloud infrastructure, the state has clearly designated the Ministry as the primary authority for the technological and commercial AI ecosystem.

From a governance perspective, these changes re-establish the functional distinction between public-sector digital transformation and ecosystem development-a boundary that had become obscured during the transition from the DTO to the SGB. Under this bifurcated model, the SGB acts as the lead actor for internal public-sector AI integration, while the MTYZGM focuses on external ecosystem growth. However, the legal framework necessitates a high degree of inter-institutional synergy. While the MTYZGM holds the primary mandate for international regulatory harmonisation, the SGB is legally required to contribute to these efforts. Conversely, the MTYZGM must support the SGB's public-sector initiatives. This collaborative necessity suggests that the successor to the current National AI Strategy will likely be a joint endeavour between these two pillars of governance.

Ultimately, this regulatory recalibration provides a clear distribution of competencies among existing institutions. By refining the roles of the SGB and the MTYZGM, the government has addressed the "institutional vacuum" that often plagues emerging technology regulation. This settled hierarchy suggests that the Turkish administrative landscape is opting for a multi-layered governance approach using established bodies. Consequently, policy proposals advocating for the creation of a completely new, independent, and centralised AI authority are likely to diminish, as the current framework now provides the necessary legal and administrative infrastructure to manage the field.

3. The Problem of Wishful Thinking and the Role of AI Standardisation

The preceding analysis reveals an emerging consensus across jurisdictions that AI governance frameworks must be formalised through legislative or quasi-legislative instruments. Yet a structural tension persists between the regulatory ambition of these frameworks and the operational reality of their implementation. AI is, by its nature, an extremely dynamic field. Detailed rules are liable to become obsolete within a short period, while broad rules risk undermining the legal certainty that operators require in order to design, deploy, and audit their systems. As a result,

regulatory texts that appear comprehensive on paper may, in practice, resemble aspirational declarations whose substantive content remains underspecified at the moment of application. To a certain extent, even mature frameworks may give the impression of wishful thinking until they are paired with mechanisms capable of translating abstract obligations into concrete and verifiable conduct.

This gap is observable even in instruments that contain seemingly precise requirements. The AIA provides a clear illustration. Although the AIA imposes obligations on providers of high-risk AI systems to ensure certain technical requirements such as risk management, data governance, transparency, human oversight, accuracy, and cybersecurity, the manner in which these requirements should be operationalised in practice remains largely undefined within the text of the AIA itself. Operators are therefore left without a clear methodology for demonstrating compliance, and supervisory authorities lack a uniform benchmark against which to assess it. This indeterminacy is not a drafting oversight but a structural feature of any framework that seeks to govern a rapidly evolving technology through primary legislation.

It is at this juncture that technical standards have come to play a central role. Standards do not formulate principles or general requirements but instead set out concrete actions, processes, and methodological steps that operators may follow in order to address a given regulatory objective. They are a well-established mechanism across numerous technical fields, including information security (ISO/IEC 27001:2022), medical devices (Regulation (EU) 2017/745), and electrical safety (Directive 2014/35/EU), and have long served as the practical interface between legal obligations and engineering practice (Schepel, 2005). Standards are not, in themselves, legally binding instruments. They may, however, be granted legal authority through reference in primary or secondary legislation, or acquire de facto authority through widespread adoption by industry, supervisory authorities, and contracting parties. ISO/IEC 27001, which specifies the requirements for an information security management system, is frequently described as a de facto global benchmark for information security and is commonly invoked in commercial contracts, public procurement, and regulatory assessments, despite its formally voluntary character (Mirtsch et al., 2021). In the field of AI, ISO/IEC 42001:2023, published in December 2023, introduces a certifiable management system standard for AI and is increasingly referenced as an emerging baseline for organisational AI governance (Deloitte, 2024; KPMG, 2025).

A second model is exemplified by the United States National Institute of Standards and Technology (NIST). The NIST AI Risk Management Framework (AI RMF), released in January 2023, is expressly designed as a voluntary, rights-preserving, non-sector-specific and use case agnostic framework (National Institute of Standards and

Technology, 2023). It does not create binding obligations and contains no enforcement mechanism. Its function is rather to provide a structured set of approaches organised around the four functions of govern, map, measure, and manage, which organisations may adapt to their own contexts. The NIST AI RMF has nonetheless gained considerable traction as a reference point in both public and private governance, illustrating that influential standardisation can occur outside both binding regulation and formal conformity assessment regimes. The framework is also evolving through sector-specific profiles that translate its generic functions into more targeted guidance for particular deployment contexts. In April 2026, NIST launched the development of an AI RMF Profile on Trustworthy AI in Critical Infrastructure, intended to guide operators of critical infrastructure sectors towards specific risk management practices when engaging AI-enabled capabilities across information technology, operational technology, and industrial control systems (National Institute of Standards and Technology, 2026). This trajectory illustrates how standards as voluntary frameworks can mature into more granular, sector-tailored governance instruments without acquiring the rigidity of statutory rules.

The EU approaches standards differently in the context of enforcement of product safety rules. Standards, technically called "harmonised standards" are formally integrated into the regulatory architecture, to which the AIA framework is not an exception. Under the AIA, high-risk AI systems that conform to harmonised standards published in the Official Journal of the EU benefit from a presumption of conformity with the corresponding technical requirements. To this end, the European Commission issued a standardisation request in May 2023 to the European standardisation organisations CEN and CENELEC, which was subsequently amended in June 2025 to reflect the final text of the AIA (European Commission, 2023; European Commission, 2025b). The development of these harmonised standards is, however, significantly delayed. The original deadline for delivery was missed, and CEN-CENELEC is now targeting publication during 2026 (CEN-CENELEC, 2025; European Commission, 2026). This delay is one of the principal reasons underlying the postponement proposed in the Commission's recent omnibus initiative, since the absence of harmonised standards undermines both the ability of providers to demonstrate compliance and the ability of market surveillance authorities to enforce the high-risk regime in a consistent manner (Kilian et al., 2025).

Standardisation as a regulatory tool presents a number of advantages. It permits the operationalisation of broadly drafted legal requirements without locking such requirements into rigid statutory language, thereby preserving the capacity of the legal framework to remain stable while the underlying technical content evolves. It allows technical expertise to be channelled into the regulatory process through participation of industry, academia, civil society, and public authorities in

standardisation bodies, producing a level of granularity that primary legislation could not feasibly achieve. It enables a degree of international convergence, since standards developed by ISO, IEC, and other international bodies can serve as common reference points across jurisdictions with otherwise divergent regulatory approaches. From a compliance perspective, it offers operators a degree of legal certainty, particularly where conformity with a standard triggers a presumption of compliance with statutory obligations. It also reduces enforcement costs, since both operators and supervisory authorities can rely on a shared technical methodology.

These advantages are accompanied, however, by significant limitations. Standardisation processes are typically slow, consensus based, and resource intensive, which sits uneasily with the pace of AI development (Veale & Zuiderveen Borgesius, 2021; Kilian et al., 2025). The CEN-CENELEC experience under the AIA illustrates that even where there is clear political pressure and a defined legislative deadline, the production of usable harmonised standards may extend well beyond the originally planned timeframe. Furthermore, the participation of stakeholders in standardisation bodies is not evenly distributed. Industry actors with sufficient resources are generally better represented than civil society organisations, small and medium sized enterprises, or affected communities (Galvagna, 2023; Gornet & Herman, 2024), which raises legitimate concerns regarding the democratic credentials of standards that effectively shape the scope of fundamental rights protections (Veale & Zuiderveen Borgesius, 2021). There is also a substantive concern that certain requirements of the AIA, particularly those addressing fairness, non discrimination, and the protection of fundamental rights, may not be readily reducible to the kind of quantifiable technical specifications that standardisation bodies are accustomed to producing (Laux et al., 2024). The translation of normative concepts into measurable parameters risks either oversimplification, which undermines the protective intent of the legal requirement, or excessive abstraction, which deprives the standard of operational value (Laux et al., 2024). Finally, granting de facto or de jure regulatory authority to non-public standardisation bodies raises broader questions of legitimacy, transparency, and judicial reviewability, particularly where compliance with a standard determines the lawful placement of a product on the market (Leyden, 2025).

These considerations are directly relevant to Türkiye. As discussed in the preceding section, harmonisation with the AIA is structurally required by the functioning of the customs union, and Türkiye has historically aligned its conformity assessment system with that of the EU. Where the AIA is operationalised through harmonised European standards, Türkiye will need to ensure that an equivalent technical infrastructure exists domestically, whether through the adoption of Turkish standards mirroring the corresponding European standards through the Turkish Standards Institution (TSE),

or through direct reference to the European standards within Turkish secondary legislation. The Turkish regulatory framework is therefore already accustomed to integrating standardisation in other technical fields, and may extend the same approach to AI, treating standardisation not as an ancillary element but as a constitutive component of AI governance. This integration must, however, be informed by an awareness of the limitations identified above, in particular the risks associated with delays in standard development, the uneven representation of stakeholders, and the difficulty of reducing rights based requirements to technical metrics. A reflexive approach, in which standards are systematically reviewed against their regulatory objectives and updated as the technology and its societal implications evolve, will be essential if standardisation is to fulfil its function as the practical backbone of AI governance rather than as a further layer of formal compliance disconnected from substantive outcomes.

Conclusion

In light of the preceding analysis, it is evident that the Turkish legal landscape is navigating a critical transition from a period of normative adaptation-where existing general rules were stretched to encompass autonomous systems-to a structured era of technological institutionalisation. While the absence of a primary artificial intelligence statute has not resulted in a legal vacuum, the rapid proliferation of generative systems has exposed the inherent limitations of relying solely on classical legal doctrines designed for a pre-algorithmic age. The future of AI governance in Türkiye is now shaped by a multi-layered regulatory trajectory that moves beyond exploratory policy toward a concrete legal infrastructure.

The functional necessity of the Customs Union renders alignment with the EU AIA a pragmatic inevitability rather than a discretionary policy choice. However, this alignment remains structurally incomplete without a comprehensive resolution to the data transfer impasse. For the Customs Union to function effectively in the age of intelligence, the legal framework must evolve beyond the movement of tangible goods to address the seamless and secure flow of the data that fuels these systems, necessitating a more robust synchronisation with international data protection benchmarks.

It is equally important to recognise that Türkiye is not required to adopt EU legislation verbatim and any harmonisation efforts must be undertaken in a manner that does not stifle AI innovation. The objective should be to establish a framework that fosters AI development and aligns with Türkiye's existing regulatory engagements as well as national goals without imposing prohibitive or harmful restrictions.

Simultaneously, the recent administrative restructuring via Presidential Decrees has effectively resolved the institutional vacuum that previously slowed coherent policymaking down. By strategically bifurcating mandates, the amended framework has established a specialised hierarchy where the SGB acts as the lead architect for public-sector digital transformation and internal administrative integration, while the MTYZGM serves as the primary engine for the commercial ecosystem and technical harmonisation. This settled distribution of powers suggests that the practical backbone of Turkish AI law will be formed not only by parliamentary statutes but by a dense layer of secondary legislation and technical standards issued by these competent bodies.

Ultimately, the emerging legislative proposals in TBMM, despite their current conceptual and structural shortcomings, signal a political drive that soft law and voluntary guidelines may no longer sufficient to manage the risks of AI. The challenge for the Turkish regulator lies in ensuring that forthcoming interventions move beyond abstract imitations of foreign frameworks to provide genuine legal certainty. This requires a regulatory environment that balances the need for innovation with the robust protection of fundamental rights, particularly in the contexts of data privacy, intellectual property, and civil liability. As the National AI Strategy enters its next cycle, the focus may shift from broadly framed ambitions to a precise, technically grounded framework that recognises artificial intelligence not as a transient phenomenon, but as a permanent, horizontal, and foundational pillar of the modern Turkish legal order.

References

Aksoy, H. C. (2025). Yapay zekânın yol açtığı zararlardan hukuki sorumluluk [Civil liability for damages caused by artificial intelligence]. In F. Bilir (Ed.), *Yapay zekâ teknolojilerine akademik bakış* (pp. 179–197). Adalet Yayınevi.

Altunç, S. (2021). Yapay zekâ ve ceza hukuku sorumluluğu [Artificial intelligence and criminal law liability]. In E. E. Aksoy Retornaz & O. G. Güçlütürk (Eds.), *Yapay zekâ ve hukuk* (pp. 347–348). On İki Levha Yayıncılık.

Al-Antari M. A. (2023). Artificial Intelligence for Medical Diagnostics-Existing and Future AI Technology!. *Diagnostics, 13*(4), 688. https://doi.org/10.3390/diagnostics13040688

Anderson, J. (Host). (2024, October 2). The impact of AI on children's development [Audio podcast episode]. In *The Harvard EdCast. Harvard Graduate School of Education.* https://www.gse.harvard.edu/ideas/edcast/24/10/impact-ai-childrens-development

Brandao, P. R. (2025). The Impact of Artificial Intelligence on Modern Society. *AI*, *6*(8), 190. https://doi.org/10.3390/ai6080190

Broecke, S. (2023). Artificial intelligence and labour market matching (OECD Social, Employment and Migration Working Papers No. 284). OECD Publishing. https://doi.org/10.1787/2b440821-en

CEN-CENELEC. (2025, October 23). Update on CEN and CENELEC's decision to accelerate the development of standards for artificial intelligence. https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/

Council of the European Union. (2026, May 7). Artificial intelligence: Council and Parliament agree to simplify and streamline rules [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/

Deloitte. (2024). ISO 42001 standard for AI governance and risk management. Deloitte Insights. https://www.deloitte.com/us/en/services/consulting/articles/iso-42001-standard-ai-governance-risk-management.html

European Commission. (2026). *Understanding the standardisation of the AI Act.* https://digital-strategy.ec.europa.eu/en/faqs/understanding-standardisation-ai-act

European Commission. (2025a, November 19). *Proposal for a Regulation of the European Parliament and of the Council as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, COM(2025) 836 final. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

European Commission. (2025b). *Amendment to the standardisation request C(2023) 3215 in support of Union policy on artificial intelligence* (M/613). https://ec.europa.eu/docsroom/documents/64114

European Commission. (2023). Commission Implementing Decision of 22.5.2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, C(2023) 3215 final. https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

European Commission. (n.d.). Turkey: Customs Unions and preferential arrangements. Directorate-General for Taxation and Customs Union. https://taxation-customs.ec.europa.eu/turkey-customs-unions-and-preferential-arrangements_en

European Data Protection Board. (2024, December 17). Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

Federal Constitutional Court of Germany. (2021, March 24). *Order of the First Senate, 1 BvR 2656/18 et al.* (Climate Protection Act). https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2021/03/rs20210324_1bvr265618en.html

Gergerlioğlu, Ö. F. (2024, June 24). Yapay zekâ kanunu teklifi [Proposal for Artificial Intelligence Law] (2/2223). Grand National Assembly of Türkiye. https://www.tbmm.gov.tr/Yasama/KanunTeklifi/e21539a0-888a-4500-81be-01904a918c53

Güçlütürk, O. G. (2025). Kodlar ve kanunlar: Yapay zekânın regülasyon rotası ve AB Yapay Zekâ Tüzüğü [Codes and laws: The regulatory path of artificial intelligence and the EU AI Regulation]. In F. Bilir (Ed.), *Yapay zekâ teknolojilerine akademik bakış* (pp. 109–178). Adalet Yayınevi.

Güçlütürk, O. G. (2022a). ChatGPT ile üretilen içeriklerin eser niteliğinin 5846 sayılı Fikir ve Sanat Eserleri Kanunu bakımından değerlendirilmesi [The Evaluation of The Legal Status of Content Generated Via ChatGPT as Copyrighted Work under Law No. 5846,]. Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2022(2), 701–730.

Güçlütürk, O. G. (2022b). *Yapay zeka ve verinin kullanımı* [Artificial intelligence and the use of data]. On İki Levha Yayıncılık.

Hirsch-Kreinsen, H. (2024). Artificial intelligence: A "promising technology". *AI & Society,* 39, 1641–1652. https://doi.org/10.1007/s00146-023-01629-w

Information Commissioner's Office. (2023, March 15). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Kilian, S., Jäck, R., & Ebel, F. (2025). *European AI standards: Technical standardisation and implementation challenges under the EU AI Act*. European Journal of Risk Regulation, 16(3), 1038–1062

Kişisel Verileri Koruma Kurumu. (2025). Üretken yapay zekâ ve kişisel verilerin korunması rehberi (15 soruda) [Guideline on generative artificial intelligence and protection of personal data (in 15 questions)] (Publication No. 113). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/MTY5MjNmNmIwZWY3YTE.pdf

Kişisel Verileri Koruma Kurumu. (2021). Recommendations on the protection of personal data in the field of artificial intelligence (Publication No. 33). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/58678459-eba4-451a-a2f3-c1baf17b90f5.pdf

KPMG. (2025). ISO/IEC 42001: AI management system for governance. KPMG Switzerland. https://kpmg.com/ch/en/insights/artificial-intelligence/iso-iec-42001.html

Langenbucher, K. (2025). Artificial Intelligence and Financial Services. In N. A. Smuha (Ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (pp. 322–338). chapter, Cambridge: Cambridge University Press

Laux, J., Wachter, S., & Mittelstadt, B. (2024). Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance, 18*(1), 3–32.

Leslie, D. (2019). *Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector.* The Alan Turing Institute.

Leyden, A. (2025). Standards and the EU AI act: Legitimacy, state of play, and future challenges. *Information & Communications Technology Law*. Advance online publication.

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the adoption of the International Information Security Management System Standard ISO/IEC 27001: A web mining-based analysis. IEEE Transactions on Engineering Management, 68(1), 87–100.

Murray, A. (2023). *Cyber-speech. In Information technology law: The law and society* (5th ed., pp. 95–124). Oxford University Press.

National Institute of Standards and Technology. (2026, April). Concept note: AI RMF profile on trustworthy AI in critical infrastructure. U.S. Department of Commerce. https://www.nist.gov/programs-projects/concept-note-ai-rmf-profile-trustworthy-ai-critical-infrastructure

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Nowak, M. (2024, 29 Eylül). How AI is redefining insurance pricing strategies. Insurance Thought Leadership. https://www.insurancethoughtleadership.com/underwriting/how-ai-redefining-insurance-pricing-strategies

Özdemir, İ. (2025, December 3). 4/5/2007 tarih ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi [Proposal for the amendment of the Law No. 5651 of 4/5/2007 on the regulation of publications on the internet and combating crimes committed through such publications] (2/3133). Grand National Assembly of Türkiye. https://www.tbmm.gov.tr/Yasama/KanunTeklifi/c6d96014-55f7-45fe-a014-019ae46fb0f0

Özdemir Tosun, H. (2025, November 30). TBMM Yapay Zeka Araştırma Komisyonu raporunu tamamladı [TGNA Artificial Intelligence Research Commission has completed its report]. Anadolu Agency. https://www.aa.com.tr/tr/gundem/tbmm-yapay-zeka-arastirma-komisyonu-raporunu-tamamladi/3758009

Öztürk, H. (2025, November 7). *Bazı kanunlarda değişiklik yapılmasına ilişkin kanun teklifi* [Proposal for the amendment of certain laws] (2/3037). Grand National Assembly of Türkiye. https://www.tbmm.gov.tr/Yasama/KanunTeklifi/12d348f9-77ee-4f09-8b78-019a5e27521f

Presidency of the Republic of Türkiye Digital Transformation Office & Ministry of Industry and Technology. (2024). *Ulusal yapay zekâ stratejisi 2024-2025 eylem planı* [National artificial intelligence strategy 2024-2025 action plan]. https://www.sanayi.gov.tr/assets/pdf/UlusalYapayZekaStratejisi2024-2025EylemPlani.pdf

Presidency of the Republic of Türkiye Digital Transformation Office & Ministry of Industry and Technology. (2021). *National artificial intelligence strategy 2021-2025.* https://cdn-assets.inwink.com/b0269dea-af7b-4460-b29a-c40b9941c4c5/d32fa511-ac43-49ef-b5b2-d90034d2af03

Retornaz, E. E. A., & Güçlütürk, O. G. (2023). *Yapay zekada Kişisel Verilerin Korunması Kanunu'nun uygulanmasındaki sorunlara ilişkin değerlendirmeler* [Evaluations on the problems in the enforcement of the Turkish Data Protection Law in the context of artificial intelligence]. In P. Çağlayan Aksoy & H. C. Aksoy (Eds.), Kişisel verilerin korunmasına akademik bakış. Kişisel Verileri Koruma Kurumu.

Sabherwal, R., & Grover, V. (2024). The societal impacts of generative artificial intelligence: A balanced perspective. *Journal of the Association for Information Systems, 25*(1), 13–22. https://doi.org/10.17705/1jais.00860

Schepel, H. (2005). The constitution of private governance: Product standards in the regulation of integrating markets. Hart Publishing

Singh, S., Schupbach, A., Asiala, A., & Siwecki, D. A. (2025, November 20). *AI's impact on banking: Use cases for credit scoring and fraud detection.* Supervision Newsletter. European Central Bank. https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2025/html/ssm.nl251120_1.en.html

Türkiye Büyük Millet Meclisi. (2026, Mart). *Yapay zekânın kazanımlarına yönelik atılacak adımların belirlenmesi, bu alanda hukuki altyapının oluşturulması ve yapay zekâ kullanımının barındırdığı risklerin önlenmesine ilişkin tedbirlerin belirlenmesi amacıyla kurulan meclis araştırması komisyonu raporu* [Report of the Parliamentary Research Commission Established to Determine the Steps to Be Taken Regarding the Benefits of Artificial Intelligence, to Establish the Legal Infrastructure in This Field, and to Identify Measures Aimed at Preventing the Risks Arising from the Use of Artificial Intelligence] (Sıra Sayısı: 260). https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y1/T10/DosyaKomisyonRaporunuVerdi/9f0e7abf-41f6-4133-ab3d-4879113f7f9f.pdf

Türkiye Büyük Millet Meclisi. (2024, October 5). *Yapay zekânın kazanımlarına yönelik atılacak adımların belirlenmesi, bu alanda hukuki altyapının oluşturulması ve yapay zekâ kullanımının barındırdığı risklerin önlenmesine ilişkin tedbirlerin belirlenmesi amacıyla bir meclis araştırması komisyonu kurulmasına dair karar* [Decision on the establishment of the Parliamentary Research Commission Established to Determine the Steps to Be Taken Regarding the Benefits of Artificial Intelligence, to Establish the Legal Infrastructure in This Field, and to Identify Measures Aimed at Preventing the Risks Arising from the Use of Artificial Intelligence]. Official Gazette of the Republic of Türkiye, (32683). https://www.resmigazete.gov.tr/eskiler/2024/10/20241005-1.pdf

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International, 22*(4), 97–112.

Yanamala, A. K. Y., Suryadevara, S., & Kalli, V. D. R. (2023). Evaluating the impact of data protection regulations on AI development and deployment. *International Journal of Advanced Engineering Technologies and Innovations, 1*(1), 319–353. https://ijaeti.com/index.php/Journal/article/view/393

Zhai, C., Wibowo, S., & Li, L. D. (2024). The effects of over-reliance on AI dialogue systems on students' cognitive abilities: A systematic review. *Smart Learning Environments, 11*(28). https://doi.org/10.1186/s40561-024-00316-7

About the Author

Asst. Prof. Dr. Osman Gazi GÜÇLÜTÜRK
Galatasaray University| ogucluturk[at]gmail.com
ORCID: 0000-0001-5834-6635

Dr. Osman Gazi Güçlütürk is an Assistant Professor of IT Law at Galatasaray University Faculty of Law and an Affiliated Fellow at Yale Law School's Information Society Project. He obtained his LLB, LLM, and MJur from Galatasaray University, the London School of Economics, and the University of Oxford, respectively. He also holds a PhD from Galatasaray University, where his PhD thesis was recognised with the Best Thesis of the Year Award by the Council of Higher Education of Türkiye in 2022. Dr Güçlütürk focuses on technology law and policy and actively contributes to global AI governance as an AI Expert at OECD and a member of various strategic advisory groups.