INTERNATIONAL AI IN FINANCIAL SERVICES REVIEW 2025 / 26

Beaumont Capital Markets
www.beaumont-capitalmarkets.co.uk

TURKEY

KEY DEVELOPMENTS & THE LATEST TRENDS IN TÜRKIYE – FROM A LEGAL PERSPECTIVE

YAZICIOGLU

Bora Yazıcıoğlu
Partner

bora@yazicioglulegal.com

+90 216 468 88 50

www.yazicioglulegal.com

BIO

Bora Yazıcıoğlu is the managing partner at Yazıcıoğlu Legal. He has significant experience in advising national and international clients on several aspects of data protection, cybersecurity and e-commerce law. Bora has represented several major clients on data breaches and investigations before the Turkish Data Protection Authority and Ministry of Commerce. He is one of the founding members and the current president of the Data Protection Association of Türkiye. Bora acts as the data controller representative for Zoom, Acer, Cerus and Ookla in Türkiye.

YAZICIOGLU
LEGAL

YAZICIOGLU

Nafiye Yücedağ
Senior Counsel

nafiye@yazicioglulegal.com

+90 216 468 88 50

www.yazicioglulegal.com

BIO

Nafiye Yücedağ is a senior counsel at Yazıcıoğlu Legal. She is a faculty member in the Department of Civil Law at Istanbul University Faculty of Law. Nafiye specializes in personal data protection law, e-commerce law, civil law, the law of obligations, and consumer law. She has been serving at Istanbul University since 2011.

YAZICIOGLU
LEGAL

YAZICIOGLU

Emre Öntekin
Senior Associate

emre@yazicioglulegal.com

+90 216 468 88 50

www.yazicioglulegal.com

BIO

Emre Öntekin is a senior associate at Yazıcıoğlu Legal. He focuses on various areas of law including data protection law, e-commerce law, consumer law, commercial law, administrative law, criminal law and dispute resolution. He holds a CIPP/E certificate from the International Association of Privacy Professionals.

YAZICIOGLU
LEGAL

KEY DEVELOPMENTS & THE LATEST TRENDS IN TÜRKIYE FROM A LEGAL PERSPECTIVE

YAZICIOGLU LEGAL

In this article, we will examine the current legal regulations on artificial intelligence (AI) in Türkiye's financial sector, the approaches of relevant regulatory bodies.

Firstly, in 2021, the Digital Transformation Office of the Presidency of the Republic of Türkiye (DTO), in cooperation with the Ministry of Industry and Technology (MoIT), published Türkiye's first National Artificial Intelligence Strategy (NAIS) for 2021–2025.

> “
>
> Türkiye's National Artificial Intelligence Strategy (2021–2025) prioritizes training AI experts, fostering innovation, and enhancing data access to drive socioeconomic adaptation.

This strategic roadmap outlines six key priorities:

- Training AI experts and increasing employment in the field.
- Supporting research, entrepreneurship, and innovation.
- Enhancing access to quality data and technical infrastructure.
- Enacting regulations to accelerate socioeconomic adaptation.
- Strengthening international cooperation.
- Accelerating structural and labor market transformation.

In light of recent developments and national needs in AI, the 2021–2025 Action Plan was updated in accordance with the 12th Development Plan and published as the 2024–2025 Action Plan. Moreover, the DTO and MoIT jointly issued this updated National Artificial Intelligence Strategy 2024–2025 Action Plan. However, following Presidential Decree No. 157 dated 28 March 2025, the DTO was dissolved. Its responsibilities were transferred to the newly established Cybersecurity Authority under the Cybersecurity Law.

Addition to the executive branch's efforts, the legislative body has also undertaken initiatives in field of AI. In parallel, the Grand National Assembly of Türkiye (TGNA) published the “Decision on the Establishment of a Parliamentary Investigation Commission”[1]. The Commission held its last meeting on 13 May 2025. In one of its sessions, the Commission addressed the theme of “Artificial Intelligence in Macroeconomics and Digital Finance”.

Beyond parliamentary efforts, other independent regulatory authorities have also started to address the legal implications of AI. In September 2021, the Authority issued its Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence which was updated in April 2025. In November 2024, Turkish Data Protection Authority (Authority) published an information note on chatbot technologies (e.g., ChatGPT).

Meanwhile, the adoption of AI technologies in practice -particularly within the financial sector - has rapidly gained momentum and brought significant transformation in the financial sector in recent years. They are increasingly applied in areas such as cybersecurity and fraud detection, customer interaction through chatbots, credit decision-making processes, personalization and risk management. These technologies are being rapidly integrated into the operational workflows of financial institutions, offering notable advantages such as increased efficiency, enhanced customer experience, improved risk management and cost reduction.

In Türkiye, banks and fintech companies actively deploy AI technologies to detect and prevent fraud. The financial industry has increasingly adopted innovative AI-driven strategies to manage and mitigate financial risks.

1. Decision on the Establishment of a Parliamentary Investigation Commission to Determine the Steps to be Taken for the Gains of Artificial Intelligence, to Establish the Legal Infrastructure in this Field, and to Determine the Measures to Prevent the Risks of the Use of Artificial Intelligence.

According to statements from a leading bank, the systematic integration of AI solutions has enabled a 98.7% reduction in fraud-related losses over a seven-year period. Furthermore, its systems reportedly analyze approximately 40 million transactions per day and identify nearly 500 potential fraud cases daily.

The use of AI-supported chatbots and robot advisors in banking applications are also quite common in Türkiye. Robo-advisors provide investment recommendations and portfolio management through algorithms, while chatbots are widely used in customer service to reduce workload and offer 24/7 support.

Despite the rapid adoption of these tools, the regulatory response remains fragmented and indirect. There isn't comprehensive regulatory framework specifically governing the use of AI in financial services in Türkiye. However, certain sector-specific regulations contain provisions that indirectly relate to AI applications.

The role of supervisory bodies becomes critical in interpreting and applying existing rules to emerging AI-based practices. For instance, the Banking Regulation and Supervision Agency (BRSA) is the main authority responsible for ensuring trust and stability in Türkiye's financial markets, safeguarding the rights of savers, and promoting an efficient credit system.

While the BRSA hasn't issued specific regulations on AI, existing legal frameworks already apply to AI-driven practices to some extent. For instance, amendments to the Regulation on Remote Identification Methods and Establishment of Contractual Relationships in Electronic Environment authorize the BRSA Board to set out the procedures and principles for carrying out, through AI-based methods, actions that are otherwise expected to be performed by customer representatives.

The Capital Markets Board of Türkiye, as a part of its 2022–2026 Strategic Plan aims to monitor FinTech practices such as artificial intelligence and machine learning by conducting on-site inspections of companies utilizing such technologies and preparing a recommendation report based on its findings.

On February 25, 2011, with the enactment of Law No. 6111, the Risk Center was established under the Turkish Banks Association (TBB) to collect and share risk information of customers of financial institutions. The Credit Bureau, which was established on April 11, 1995, as a partnership of nine banks and now serves approximately 200 members for credit scoring, acts as the technical and operational representative of the Risk Center and provides data collection and sharing services to 185 financial institutions.

It offers a credit score service that measures customers' credit risk based on their past payment behavior and financial information. For example, the individual credit score is a numerical indicator calculated to predict the likelihood that a consumer will fulfill repayment obligations on loans obtained or to be obtained from a member institution of the Credit Bureau, compared to other consumers. The Credit Bureau has stated that the individual credit score is a decision support product created using statistical models, and information about the factors affecting this score and their impact rates is available on the bureau's official website. While the Credit Bureau does not explicitly confirm the use of artificial intelligence, such scoring systems often rely on machine learning and advanced analytics to improve accuracy.

> “
>
> AI solutions in a leading Turkish bank have achieved a 98.7% reduction in fraud-related losses over seven years, analyzing 40 million transactions daily.

Additionally, under current banking regulations in Türkiye, financial institutions are required to store customer data within Türkiye. Since chatbot interactions in banking applications involve the collection and processing of personal data -such as identity information, financial details, or transaction history - all data exchanged through AI-driven systems must also be stored locally. To comply with these requirements, banks must adopt concrete legal and technical measures. A key step is incorporating binding contractual clauses into agreements with AI service providers, explicitly requiring that data-processing infrastructure be physically located in Türkiye. This requirement introduces additional legal and operational considerations for financial institutions deploying AI solutions.

> “
>
> In Türkiye, AI-driven banking chatbots must store customer data locally, requiring banks to adopt strict legal and technical measures to comply with regulations.

Although chatbot usage in the financial sector in Türkiye offers significant advantages in terms of digitalization and customer experience, it simultaneously gives rise to a number of legal risks. Personal data issues arise during the collection of datasets, model development, and deployment of AI systems, including challenges such as accurately identifying data subjects, establishing valid legal grounds for processing, providing sufficient information to individuals, and ensuring their ability to exercise rights under data protection laws.

The Authority, in its information note regarding chatbots, emphasized that chatbot applications must provide sufficient information about how and for what purposes the data they process is used, with whom it is shared, the duration of data retention, the identity of the data controller and, if applicable, its representative, as well as the rights of data subjects, in order to enable individuals to maintain control over their personal data. However, in AI systems, especially at the stage of data collection, providing direct information to the data subjects poses certain challenges.

Moreover, the Authority has emphasized that age verification for children must be conducted accurately and reliably. It has also underlined the necessity of adopting a proactive approach to prevent adverse experiences specifically for children. However, it remains unclear whether this requirement applies to all chatbot applications universally, regardless of whether they are specifically designed for or target children.

Unlike EU legislation, the Turkish Data Protection Law (Turkish DP Law) does not require explicit notification to data subjects about automated decision-making, which may result in the reduced transparency regarding AI-driven processes.

Moreover, human intervention plays a crucial role in mitigating unfair outcomes. Turkish DP Law grants data subjects the right to object to decisions made solely by automated systems that adversely affect them. However, as opposed to GDPR privacy notice does not need to explicitly state which processing activities are carried out solely by automated systems; therefore, this right cannot be fully enjoyed under Turkish Data Protection practice. If this right was to be fully enjoyed it would call for meaningful human intervention, aimed at ensuring fairness, accountability, and the possibility of redress.

Beyond concerns about transparency and control, another significant risk associated with AI systems is the potential for discrimination and bias. AI models, if not carefully designed and monitored, may reflect or amplify existing societal biases. In the financial sector, this could lead to certain groups being systematically disadvantaged in credit evaluations or loan approvals. Such outcomes would violate the prohibition of discrimination, which is explicitly guaranteed under the Turkish Constitution. Furthermore, the Human Rights and Equality Institution is empowered to investigate and impose sanctions in cases involving discriminatory practices.

In cases where harm arises from the use of an AI system, liability is typically assessed under the general principles of tort or contractual liability. As AI systems do not possess legal personality, they cannot be held liable. Instead, the responsibility for harm is attributed to natural or legal person involved in the design, deployment or use of the AI system. In Turkish legal doctrine, the scope and attribution of this liability among developers, deployers and users remain the subject of ongoing debate.

Under the Turkish Code of Obligations, liability is primarily fault-based, requiring proof that the harm resulted from the wrongful act or omission of a responsible party. However, the suitability of a fault-based regime for addressing harm caused by AI systems is increasingly questioned. The complexity, opacity and autonomy associated with AI decision-making raises doubts as to whether traditional notions of fault can adequately address the risks and challenges posed by these technologies.

The search for appropriate liability frameworks has led to several theoretical proposals and analogies. In the Turkish legal system, there is currently no specific liability regime applicable to damages caused by AI systems. However, some efforts have been made to fit AI-related liability within the scope of existing strict liability frameworks:

- One proposal suggests treating AI systems as auxiliary persons, thereby invoking the liability of employers for the actions of their employees. This approach requires the existence of an employment relationship and that the actor be a real person. Since AI systems do not have legal personhood, this model has not gained much traction.

- Another analogy compares AI systems to animals, based on the legal responsibility of animal keepers. Yet, AI's advanced adaptive capabilities significantly distinguish it from animals, making this comparison inadequate for capturing the nature of AI-driven harm.

- Another argument draws a parallel between damages caused by AI systems and those caused by individuals lacking mental capacity, suggesting that compensation might be justified on the basis of equity, even in the absence of fault. However, given that AI lacks legal personality, this analogy has also failed to achieve widespread acceptance.

- Some scholars propose addressing AI-related harm under the doctrine of strict liability for hazardous activities. Still, for this regime to apply, the activity must involve a significant danger. Not all uses of AI -particularly in sectors such as financial services- meet this threshold, which limits the applicability of this model.

Ultimately, none of these approaches appear to offer a fully satisfactory solution that reflects the complex and evolving structure of AI systems.

Apart from tort-based and strict liability approaches, product liability has also been proposed as a potential argument. In this sense, another key question is whether the Product Safety Law (PS Law), which imposes strict liability for damage caused by defective products, can be extended to AI systems. This question is complicated by the fact that the applicability of the PS Law traditionally presumes a tangible, physical product. It remains uncertain whether AI systems fall within the scope of "products" under the current legal definition of PS Law.

Overall, the current liability framework may need to evolve to address the unique challenges posed by AI technologies, ensuring fair and effective remedies for those harmed while providing legal clarity for developers, deployers and users.

> "
>
> The Turkish Code of Obligations' fault-based liability struggles to address AI-related harm, prompting debates on applying strict liability or product safety laws to AI systems.