Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers

Türkiye: Law and Practice

Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, İbrahim Yıldırım and Gizem Nur Çay
YAZICIOGLU Legal

TÜRKİYE

Law and Practice

Contributed by:
Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, İbrahim Yıldırım and Gizem Nur Çay
YAZICIOGLU Legal

Contents

1. General Legal Framework p.5
1.1 General Legal Background p.5

2. Commercial Use of AI and Machine Learning p.6
2.1 Industry Use p.6
2.2 Involvement of Governments in AI Innovation p.7

3. AI-Specific Legislation and Directives p.8
3.1 General Approach to AI-Specific Legislation p.8
3.2 Jurisdictional Law p.9
3.3 Jurisdictional Directives p.9
3.4 EU Law p.9
3.5 US State Law p.9
3.6 Data, Information or Content Laws p.9
3.7 Proposed AI-Specific Legislation and Regulations p.9

4. Judicial Decisions p.10
4.1 Judicial Decisions p.10
4.2 Technology Definitions p.10

5. AI Regulatory Oversight p.10
5.1 Regulatory Agencies p.10
5.2 Technology Definitions p.10
5.3 Regulatory Objectives p.10
5.4 Enforcement Actions p.11

6. Standard-Setting Bodies p.11
6.1 National Standard-Setting Bodies p.11
6.2 International Standard-Setting Bodies p.11

7. Government Use of AI p.11
7.1 Government Use of AI p.11
7.2 Judicial Decisions p.12
7.3 National Security p.12

8. Generative AI p.13
8.1 Emerging Issues in Generative AI p.13
8.2 IP and Generative AI p.13
8.3 Data Protection and Generative AI p.14

9. Legal Tech p.15
9.1 AI in the Legal Profession and Ethical Considerations p.15

10. Liability for AI p.16
10.1 Theories of Liability p.16
10.2 Regulatory p.17

11. Legal Issues With Predictive and Generative AI p.17
11.1 Algorithmic Bias p.17
11.2 Data Protection and Privacy p.17
11.3 Facial Recognition and Biometrics p.17
11.4 Automated Decision-Making p.18
11.5 Transparency p.19
11.6 Anti-competitive Conduct p.20

12. AI Procurement p.20
12.1 Procurement of AI Technology p.20

13. AI in Employment p.20
13.1 Hiring and Termination Practices p.20
13.2 Employee Evaluation and Monitoring p.21

14. AI in Industry Sectors p.21
14.1 Digital Platform Companies p.21
14.2 Financial Services p.22
14.3 Healthcare p.22
14.4 Autonomous Vehicles p.23
14.5 Manufacturing p.23
14.6 Professional Services p.23

15. Intellectual Property p.24
15.1 Applicability of Patent and Copyright Law p.24
15.2 Applicability of Trade Secrecy and Similar Protection p.24
15.3 AI-Generated Works of Art and Works of Authorship p.24
15.4 OpenAI p.24

16. Advising Corporate Boards of Directors p.24
16.1 Advising Directors p.24

17. AI Compliance p.25
17.1 AI Best Practice Compliance Strategies p.25

YAZICIOGLU Legal is an Istanbul-based boutique technology and commerce law firm. The firm focuses on legal matters related to technology, media, telecommunications and data protection/cybersecurity. It also has solid expertise in cross-border transactions, commercial matters, intellectual property, regulatory compliance, e-commerce, consumer protection and dispute resolution. Yazıcıoğlu Legal has a dedicated team of 12 lawyers working on data protection and cybersecurity. The majority of the firm's workload involves data protection-related matters. In particular, the firm is known for successfully representing its clients in data breach investigations before the Turkish Data Protection Authority. The firm is ranked in several legal directories on TMT and is also a Bronze Corporate Member of the International Association of Privacy Professionals (IAPP).

Authors

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, Reddit, Cerus and Avalyn in Türkiye.

Kübra İslamoğlu Bayer is a senior managing associate at Yazıcıoğlu Legal. She advises clients on data protection, e-commerce and cybersecurity laws. She is an active member of the Istanbul Bar Association's IT Law Commission: Artificial Intelligence Study Group, and of the Data Protection Commission. Furthermore, Kübra manages a website dedicated to data protection law.

İbrahim Yıldırım is an associate at Yazıcıoğlu Legal. He mainly focuses on various fields of law including personal data protection, IT law, e-commerce law, contract law, international arbitration, and labour law.

Gizem Nur Çay is an associate at Yazıcıoğlu Legal. She specialises in contract law, corporate/commercial matters, IT law, e-commerce law, data protection, and consumer protection in media and telecommunications.

YAZICIOGLU Legal

NidaKule – Goztepe
Merdivenköy Mahallesi Bora
Sokak No:1
Kat:7 34732 Kadıköy
İstanbul
Türkiye

Tel: +90 216 468 88 50
Fax: +90 216 468 88 01
Email: info@yazicioglulegal.com
Web: www.yazicioglulegal.com

1. General Legal Framework

1.1 General Legal Background

At present, Türkiye lacks specific laws solely dedicated to regulating AI or machine learning (ML). However, considering AI's broad implications, laws governing general legal domains such as human rights, privacy, data protection, intellectual property, consumer protection, criminal conduct, and tort may be deemed relevant.

Constitution of the Turkish Republic (Constitution)

While many human rights enshrined in the Constitution may be relevant depending on the application of AI, current global discussions highlight the following as particularly pertinent, namely the right to (i) life, (ii) health, (iii) fair trial, (iv) respect for private and family life, (v) protection of personal data, (vi) freedom of speech, (vii) equality before the law, (viii) to own property, and (ix) prohibition of discrimination.

Turkish Civil Law (TCiC) and Turkish Code of Obligations (TCO)

AI and personality rights intersect, especially in discussions as to whether recognising AI as a legal entity and the applicable rules when a person's personality rights are harmed. These issues are primarily governed by the TCiC.

Alongside the TCiC, TCO is the primary law that governs compensation for harm, both physical and non-physical (moral damages), caused by tortious actions, whether directly or indirectly inflicted. These well-established principles will undoubtedly be applied to situations involving AI.

It is important to note that the TCO also governs the broader legal framework for enforcing all types of contracts.

Turkish Data Protection Law No 6698 (DP Law)

The DP Law regulates the obligations of both natural and legal persons in processing personal data, outlining procedures and principles to be followed, and it aims to protect the fundamental rights and freedoms of individuals in the processing of personal data.

Consequently, this protection becomes relevant when personal data is processed during an AI model's development, training, deployment, or use.

Law on Intellectual and Artistic Works (LIAW) and Industrial Property Law (IPL)

The LIAW defines and protects the moral and financial rights (ie, copyrights) of authors of intellectual and artistic works, performing artists, phonogram producers, film producers, and broadcasters.

The IPL encompasses applications linked to trademarks, geographical indications, designs, patents, utility models, and traditional product names, along with their registration, and legal procedures and sanctions for rights infringements.

Law on Product Safety and Technical Regulations (PS Law)

This law ensures the safety of products within the country, detailing compliance with safety standards and technical regulations. It defines the responsibilities of manufacturers, importers, and distributors, establishes monitoring mechanisms, and sets penalties for non-compliance, ensuring consumer access to safe products.

Turkish Criminal Law (TCrC)

Given the potential for AI to be involved in crimes, such as illegally accessing a computer system by using AI, or death or injury caused by a self-driving car, various articles of TCrC may be applicable. According to the TCrC, criminal responsibility is personal, meaning only a natural person can be held as a perpetrator of a crime. Whether the developers or users of AI technology can be held responsible for the relevant crime is assessed based on whether there was intent or neglect by these actors.

Other Laws and Regulations

Depending on AI's use, it may invoke various laws and regulations, such as consumer protection law, the Law on the Protection of Competition ("Competition Law"), regulations governing commercial advertisements, and the ban on unfair commercial practices, etc.

Furthermore, there have been some minor changes in specific by-laws related to banking, factoring and telecommunications sector, regulating the establishment of contracts in the electronic environment. These changes address issues arising from the identification of a person by virtue of AI technology during the establishment of a contract in such an environment.

Decree Law No 664 establishes the Atatürk Culture, Language, and History High Institution as a public entity to promote Atatürk's principles and explore Turkish culture, history, and language. The institution is also tasked with developing AI-based language models and making them publicly accessible.

Presidential Decree on Organisation No 1 stipulates that ministries should monitor developments in AI and big data globally, and engage in infrastructure, software, and hardware projects related to these fields. It mandates the utilisation of AI technologies across various organisational units, from education to the economy, and from health to defence.

2. Commercial Use of AI and Machine Learning

2.1 Industry Use

The Scientific and Technological Research Council of Türkiye (TÜBİTAK), universities, and research centres are conducting various projects and research on AI/ML. In addition, some companies and start-ups in Türkiye are developing various products and solutions on AI/ML technologies.

TÜBİTAK's subdivisions, such as the Public Research Support Group (KAMAG) and the Technology and Innovation Funding Programs Directorate (TEYDEB), are offering incentives for AI projects focusing on large language models, including generative AI. The Advanced Technologies Research Centre for Informatics and Information Security (BİLGEM) is developing a large Turkish language model, aiming for general use while reflecting national values. Initial applications will serve legal processes, to be planned for image processing apps.

According to a report by a Turkish NGO focusing on AI, as of January 2024, Türkiye has a total of 321 AI start-ups focusing on:

- image processing;
- machine learning;
- predictive analytics and data analytics;
- chatbots and conversational AI;
- natural language processing;
- optimisation;
- RPA (robotic process automation);
- autonomous vehicles;
- search engines and search assistants;
- internet of things; and
- smart platforms.

2.2 Involvement of Governments in AI Innovation

Türkiye is classified as a moderate innovator country by the World Intellectual Property Organization and ranked 39th out of 132 economies in the Global Innovation Index (GII) 2023 Rankings. Türkiye is in the group that has climbed the GII rankings fastest over the last decade. Türkiye's performance boost owes much to government backing for business Research and Development (R&D) and a growing population with tertiary education. According to the European Innovation Scoreboard 2023, among others, government support for business R&D is acknowledged as a strength of Türkiye.

Türkiye has quite diverse investment and ecosystem opportunities related to AI/ML. As for government involvement, TÜBİTAK is the major funder for innovation activities in Türkiye through various support programmes that enable collaboration both within industries and between industries and universities.

Beyond TÜBİTAK, the Ministry of Industry and Technology (MoIT), Small and Medium Enterprises Development Organisation of Türkiye (KOSGEB), Ministry of Finance, and Development Agencies, provide different support and funding for research and commercialisation phases which can be utilised for AI-based business activities.

R&D and innovation by small and medium-sized enterprises can be supported through TÜBİTAK's Entrepreneurship Support Programme. TEYDEB provides funding for R&D projects to improve the R&I capabilities of the private sector and enhance innovation culture, and has ten technology and support groups. TÜBİTAK also facilitates international innovation collaborations through programmes such as the Eureka Network. Türkiye is also active in the AI-Data-Robotics pillar of the EU Horizon Partnerships.

Among eight concrete TÜBİTAK R&D Centres nationwide, BİLGEM performs cutting-edge cross-industry R&I projects in the field of cybersecurity and informatics. BİLGEM AI Institute stands as a pioneering centre for AI innovation.

Another governmental actor in AI innovation is the MoIT. The MoIT Strategic Plan for 2024-2028 includes AI as one of the main goals in line with the National Technology Movement. These efforts focus on strengthening the infrastructure for AI R&D, developing a talented workforce, and accelerating entrepreneurship in AI.

Additionally, Türkiye has various technology hubs associated with both industry and universities. These special hubs for technology transfer offices and technology development zones are primarily governed by the Technology Development Zones Law.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

In 2021, the Digital Transformation Office of the Presidency of the Republic of Türkiye (DTO) received international recognition by releasing Türkiye's inaugural National Artificial Intelligence Strategy (NAIS) for the years 2021-2025. Developed in alignment with the Presidency's Annual Programmes, NAIS is structured around six strategic priorities, aligning with the vision of "Digital Türkiye" and the "National Technology Move":

- training AI experts and increasing employment in this area;
- supporting research, entrepreneurship and innovation;
- facilitating access to quality data and technical infrastructure;
- regulating to accelerate socioeconomic adaptation;
- strengthening international co-operation; and
- accelerating structural and labour transformation.

With the publication of NAIS, which is Türkiye's first national strategy document on AI, the country has positioned itself among those with a dedicated AI strategy.

To support this initiative, several commissions have been set up by the government to actively engage in efforts to ensure the reliability and accountability of applications developed with generative AI. These initiatives target the introduction of accurate regulations regarding AI advancements, the establishment of specific standards in collaboration with the International Organization for Standardization (ISO), the creation of the "trusted AI" certification, and the formation of inspection teams.

Furthermore, the tasks and responsibilities related to the measure regarding "the preparation of national data strategy to increase data-based competitiveness", as outlined in the recently released Medium-Term Programme for 2024-2026, have been assigned to DTO. This includes the preparation of the National Data Strategy and Action Plan and strengthening data governance in public institutions as specified in the 12th Development Plan for 2024-2028.

For this purpose, as a first step, the Data Governance Framework Recommendation Report for Türkiye dated 1 April 2024, has been launched in co-operation with the United Nations Development Programme (UNDP) to establish a governance framework to define data access, use, and sharing in Türkiye.

The DTO is currently preparing the National Data Strategy, taking into account Türkiye's priority needs and international trends. In this context, legislative work on open government data, data localisation, and the national data dictionary is ongoing. Additionally, a comprehensive needs analysis and recommendation report on advanced analytics and AI data governance needs are being prepared in collaboration with the National Data Governance Working Group.

3.2 Jurisdictional Law

No AI-specific legislation has been enacted in Türkiye (see **1.1 General Legal Background**).

3.3 Jurisdictional Directives

In September 2021, the Turkish Data Protection Authority (DPA) issued its Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence ("Recommendations on AI") (see **8.3 Data Protection and Generative AI**).

Recently the Turkish Council of Higher Education prepared "Ethical Guidelines on the Use of Generative Artificial Intelligence in Scientific Research and Publication Activities of Higher Education Institutions". This guide addresses the ethical dimensions of using generative AI in scientific research and publications, including its purposes, the ethical values it supports and threatens, and the risks it poses to scientific accuracy and integrity.

3.4 EU Law

3.4.1 Jurisdictional Commonalities

There is no applicable information in this jurisdiction.

3.4.2 Jurisdictional Conflicts

There is no applicable information in this jurisdiction.

3.5 US State Law

There is no applicable information in this jurisdiction.

3.6 Data, Information or Content Laws

While the DP Law does not contain any specific provisions regarding AI, it is worth noting that data subjects have the right to object to the processing of their personal data solely through automated systems only if such processing adversely affects them.

On the other hand, according to the Medium-Term Programme, further amendments to the DP Law will be made with the purpose of aligning the DP Law with EU legislation, particularly with the General Data Protection Regulation (GDPR), which is estimated to take place in the 4th quarter of 2024. It is reasonable to expect certain provisions of the GDPR, such as Article 22 (ie, the right not to be subject to a decision based solely on automated processing, including profiling) may be incorporated into the DP Law.

Additionally, the DPA has issued Recommendations on AI (see **8.3 Data Protection and Generative AI**).

3.7 Proposed AI-Specific Legislation and Regulations

Currently, there is no ongoing legislative preparation or any draft work specifically concerning AI that is publicly known in Türkiye.

However, goals regarding the establishment of a legal framework for AI have been set in the NAIS. According to this strategy:

- an agile and inclusive legal compliance process will be operated to test and discuss ethical and legal scenarios;
- international regulatory efforts aimed at mitigating AI-generated risks and applying AI values and principles will be monitored, and suggestions will be developed to align Türkiye's regulations in this area; and

- legislation will be prepared, and guidelines will be published on creating a regulatory experimental area for innovative AI applications and benefiting from this process.

On the international front, Türkiye, as one of the first countries to become a member of the Council of Europe (CoE), initially held membership in the Ad hoc Committee on Artificial Intelligence (CAHAI) between May 2019 and December 2021 and joined the Committee on Artificial Intelligence (CAI) in February 2022 following the dissolution of CAHAI.

On 17 May 2024, the CoE adopted the first international legally binding convention dedicated to upholding human rights, the rule of law, and democratic principles in deploying AI technologies. This convention, available to countries beyond Europe, establishes a legal framework covering all stages of AI system development. It aims to mitigate potential risks while promoting accountable innovation. Türkiye's stance on signing and ratifying this convention remains unclear.

4. Judicial Decisions

4.1 Judicial Decisions

No publicly available judicial decisions have been issued relating to generative AI.

4.2 Technology Definitions

Currently, there have been no landmark judicial decisions where AI is the central issue, leaving the legal definition of AI undefined by the courts.

Although it is stated on the official page of the DTO that "the definition of artificial intelligence changes with the development of technology", in the NAIS, AI is defined as "the ability of a computer or computer-controlled robot to perform various activities in a manner similar to that of intelligent creatures", which is followed by the statement that "the term AI is used for systems equipped with human cognitive abilities such as reasoning, meaning discovery, generalization or learning from past experiences in dynamic and uncertain environments". As it is the first definition of AI made in Türkiye, courts may embrace this definition in their future decisions.

5. AI Regulatory Oversight

5.1 Regulatory Agencies

There is no specific regulatory agency solely dedicated to regulating AI matters in Türkiye. However, the DPA and other sector-specific regulatory agencies such as the Banking Regulation and Supervision Agency (BRSA) the Capital Markets Board, the Turkish Republic Central Bank (TRCB), the Information and Communication Technologies Authority (ICTA), and the Competition Authority have the authority to regulate issues regarding AI and the processing of personal data within their respective sectors.

Furthermore, the Human Rights and Equality Institution of Türkiye (HRE Institution) may also become involved in certain cases. As an independent oversight body, its role is to ensure the protection and promotion of human rights, safeguard individuals' right to equal treatment and prevent discrimination in the exercise of rights and freedoms.

5.2 Technology Definitions

See **4.2 Technology Definitions**.

5.3 Regulatory Objectives

Although no specific regulatory agency is solely dedicated to regulating AI (see **5.1 Regulatory**

Agencies), certain agencies may still be relevant, given the duties entrusted to them, such as:

- the DPA: ensuring the lawful use of personal data;
- the BRSA and TRCB: potential supervision of the use of AI in applications by banking and financial institutions;
- the Capital Markets Board: preventing financial instability and market abuse, and ensuring market stability;
- the TRCB: ensuring price stability;
- the ICTA: oversight of the electronic communications sector;
- the HRE Institution of Türkiye: cases affecting human rights and equality; and
- the Competition Authority: enhancing consumer welfare and contributing to the proper functioning of market mechanisms.

5.4 Enforcement Actions

To our knowledge, there are no publicly available decisions made or pending regarding enforcement and no other regulatory actions.

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

The Turkish Standards Institute (*Türk Standartları Enstitüsü*, TSE) is the major standard-setting body and certification institution nationwide and is the sole representative of the ISO. The TSE is also a member of the International Electrotechnical Commission (IEC), the European Organization for Quality (EOQ), the European Committee for Standardization (*Comité Européen de Normalisation*, CEN), and the European Committee for Electrotechnical Standardization (CENELEC). Therefore, the national standards established by the TSE are largely in parallel with the international standards issued by the ISO and IEC.

The TSE does not have an AI-specific standard yet. However, some of the standardisation schemes on IT/software services and products may be relevant.

6.2 International Standard-Setting Bodies

In terms of international AI standards, the ISO and IEC, the Institute of Electrical and Electronics Engineers (IEEE), the Internet Research Task Force (IRTF), and the International Telecommunication Union (ITU) are the main players in standard setting. Since AI is a multi-purpose technology and sector-indifferent technology, there is also extensive standardisation work for AI within these institutions.

Although the TSE has not yet accepted AI-focused or related standards published by the ISO, companies and AI start-ups may voluntarily comply with the ISO's AI-related standards in their business life cycles as best-practice applications and manage risks appropriately.

7. Government Use of AI

7.1 Government Use of AI

The NAIS sets forth several goals for enhancing AI use across public institutions. These include:

- giving priority to AI applications in public procurements;
- fostering the effective use of big data and AI within the public sector;
- creating positions for AI specialists in public institutions;
- developing a system to facilitate secure and uninterrupted data sharing among public organisations, the private sector, universities, and research centres;

- establishing a "Public Data Space" for sharing data among public institutions; and
- increasing the deployment of AI applications in public bodies.

Despite these goals, as of the time of writing, there is no official report by the DTO on the extent to which these AI initiatives have been realised among public institutions. However, research, studies, and governmental statements reveal some progress, including:

- implementation of organisational structures in various ministries as outlined in the NAIS;
- adoption of AI-supported workflows for tax inspection;
- the submission of requests by public bodies for AI applications tailored to their specific needs, and the development of such AI solutions by TÜBİTAK;
- use of AI in the transportation and infrastructure sectors for tasks such as highway management, identifying areas with high traffic accidents, and detecting problems with the rail system and driver fatigue;
- utilisation of AI systems and applications at the Supreme Court Precedent Centre;
- integration of AI technology into the National Judiciary Informatics System (UYAP); and
- utilisation of AI and ML technology by the TRCB to detect the risk of an illegal transaction in national money transfers.

7.2 Judicial Decisions

To our knowledge, there are no publicly available decisions made or pending related to government use of AI.

7.3 National Security

Over the past decade, Türkiye has deployed AI-powered technologies in defence border operations, in both conventional and hybrid war scenarios. Automatic targeting technology products with image processing algorithms that include AI and ML techniques have been utilised by the Turkish army.

Regarding the responsible use of AI in the military, Türkiye has endorsed the Political Declaration on Responsible Military Use of AI and Autonomy, at the first global Summit on Responsible Artificial Intelligence in the Military Domain (REAIM) in the Hague.

Türkiye is also a high contracting party to the Convention on Certain Conventional Weapons (CCW) and warns against the humanitarian impact of lethal autonomous weapons.

In addition, Military Electronics Industries (largely known as ASELSAN), a company established by the Turkish Armed Forces Foundation to meet the communication needs of the Turkish Armed Forces by national means, plans to enhance military command systems using 5G and augmented reality. This upgrade will improve soldiers' decision-making by integrating AI and big data analysis into cloud infrastructure.

Current legislation related to the development of these products does not specifically address AI use, so these AI-based developments are guided more by national defence policy than by specific legal regulations.

Türkiye's intent to utilise AI in the national defence industry is also highlighted in the 12th Development Plan, with goals such as (i) designing and producing AI chips in the field of "advanced navigation support services" used in defence, aviation, and space systems, and (ii) implementing co-operation programmes between public institutions, universities, and the private sector to train a qualified workforce in strategic areas such as the defence industry.

8. Generative AI

8.1 Emerging Issues in Generative AI

Issues raised by generative AI have come to the attention of the DPA, which has published Recommendations on AI. Additionally, the Advertisement Board under the Ministry of Commerce has announced that it has begun investigating, for the first time, advertisements created using AI, along with behaviours that manipulate consumer decisions. In the same announcement, it was stated that:

- AI-generated content that directly or indirectly affects consumers' purchasing decisions, regardless of the creation method or publication medium, is now being examined; and
- administrative fines have been imposed on three cases related to promotions created by the AI application ChatGPT; these promotions contained claims of superiority over competing products or companies that were not based on objective research results.

The Advertisement Board considers such actions as unfair commercial practices and states that it will impose sanctions, including the temporary or complete cessation of advertisements and/or administrative fines.

Although Türkiye lacks any specific law governing these issues, existing laws may provide some measures to address them (see **8.2. IP and Generative AI** and **8.3. Data Protection and Generative AI**).

8.2 IP and Generative AI

From an IP rights' perspective, two main laws are relevant: the LIAW and the IPL. If the conditions set by these laws are met, it is possible to benefit from protection through either copyrights or industrial property rights for AI models, training data, input (prompts), and output.

Copyrights

For the assets in the AI process to be protected under the LIAW's copyright, they must be considered intellectual products which bear the characteristics of the author.

AI models, which are fundamentally based on computer programs, are considered intellectual products under the LIAW, therefore these models will enjoy copyright protection.

Any input or training data that meets the above criteria will benefit from copyright protection. As a result, the use of such data without proper licenses may constitute copyright infringement.

As for the outputs created by AI tools, these will lack the characteristics of the author, hence the user of an AI model (ie, a prompt writer) may not enjoy copyright protection over such output.

Patent/Utility Model

For the outputs created by an AI tool to be patentable, they must meet the following three conditions under the IPL:

- novelty in all fields of technology;
- reaching an inventive level; and
- industrial applicability.

As an AI model will not have a personality under Turkish law, we are of the view that it cannot be regarded as the inventor of an invention or owner of a patent. However, the user of an AI model (ie, a prompt writer), who has made an intention via AI, may enjoy patent protection.

A similar evaluation applies to utility models.

Industrial Design

For an industrial design to benefit from protection, it must be new and have distinctive characteristics. Designs can be protected, whether registered or unregistered.

Any input or training data meeting these criteria will be protected as industrial design under the IPL. Therefore, utilising such data without appropriate licenses could be considered a violation.

Outputs of AI tools can benefit from industrial design protection if they meet the above criteria. Similar to patent/utility models, the user of an AI model (ie, a prompt writer) who has created industrial design via AI may enjoy protection.

Trademark

The names or logos of AI models may be subject to trademark protection, and signs created with AI models may also be subject to trademark protection.

Any input or training data registered with the Turkish Patent Office as a trademark will be protected under trademark protection. The use of such data without proper licenses may constitute trademark infringement.

Unfair Competition

Finally, if a product of labour (either AI model, input/training data or products created by AI tools) does not meet the criteria for copyright protection or any other IP protection, it will enjoy protection against unfair competition under the Turkish Commercial Code.

8.3 Data Protection and Generative AI

According to the DP Law, “the data subject has the right to object to a result adversely affecting them when it arises from data processed solely through automated systems”. This right may be at stake when AI models are used in decision-making processes that inadvertently impact the data subject, including creating inaccurate factual claims about individuals. However, the DPA has not clarified the scope of this provision’s application.

Unlike the EU legislation that the DP Law is modelled after, the DP Law lacks specific obligations to inform data subjects about Automated Decision-Making (ADM). This absence can lead to data subjects not being sufficiently informed about processes involving AI. Moreover, when personal data is used in AI model training sets gathered through web scraping methods, it is often impossible to identify the data subjects involved and inform them that their data is being used.

As the training data is collected from a wide array of sources, like web scraping, user inputs, and data brokers, there is a substantial presence of personal data within these datasets. This poses various issues in terms of the data minimisation principle as well as the rights of individuals involved.

Data minimisation and purpose limitation are envisaged in a general sense among other principles outlined in DP Law, and there are no specific provisions on how to comply with these principles when utilising AI.

Regarding the right to rectification and erasure, the methods used to collect data make it impossible to trace each piece of personal data back to its data subject. In generative AI, personal data is deeply embedded within complex algorithms, making it difficult to isolate specific data. This situation could fundamentally affect the AI model's working principle and its correctness if the personal data is to be removed from the training set.

As solutions to the issues mentioned above, it would be appropriate to develop the AI model from its design phase in compliance with DP Law and in accordance with the Data Protection by Design and by Default principles. If personal data must be used, the consideration of the use of synthetic data and the utilisation of Privacy Enhancing Technologies (PETs) can help comply with these principles.

Recommendations on AI

Recommendations on AI cover general recommendations on the protection of personal data within the scope of the DP Law for developers, manufacturers, service providers, and decision-makers operating in the field of AI, and ensure human intervention in automated decision-making and specify that principles enshrined in the DP Law, such as lawfulness, proportionality, accountability, transparency remain applicable when AI engages in the personal data processing activity.

In these recommendations, in terms of data minimisation, the DPA recommended that controllers should minimise data usage by assessing the quality, nature, origin, amount, category, and content of the personal data and that the accuracy of the developed model should be constantly monitored. In the same document, regarding the rights of data subjects, the DPA recommended that:

- individuals should have the right to object to processing activities based on technologies that affect their opinions and personal development,
- considering the capability of AI systems to analyse and use personal data, the rights of the data subjects arising from national and international legislation should be protected in the processing of personal data;
- products and services should be designed to ensure that individuals are not subjected to a decision that will affect them, based on automated processing, regardless of their own opinions;
- users should have the right to stop data processing activities, and a system that allows the erasure, destruction, or anonymisation of personal data belonging to users should be designed;
- an approach that focuses on avoiding and mitigating the potential risks and considers human rights, functioning of democracy, social and ethical values, should be adopted in the processing of personal data; and
- in case a high risk is foreseen in terms of protecting personal data in AI works based on personal data processing, a privacy impact assessment should be conducted and the compliance of processing activities with laws should be evaluated within this framework.

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

There are no announced rules or regulations promulgated or pending by public institutions or organisations regulating the practical use of AI; however, Türkiye has a growing interest in the use of AI in legal issues. This interest is reflected in the 12th Development Plan, which aims to accelerate support for legal tech applications nationwide.

There is no publicly available announcement that AI is used for court decisions. However, the Supreme Court Precedent Centre utilises AI systems and applications for case management (see **7.1 Government Use of AI**).

Also, the 2023 activity report of the Ministry of Justice (MoJ) states that AI-based software has been developed for use in the criminal record information system. There are also various SaaS products specifically designed for comprehensive decision screening for law offices.

In terms of litigation, the MoJ recently announced that it is working towards AI-enabled efficient litigation processes.

Moreover, Türkiye has an active legal-tech entrepreneurship community with diverse projects in collaboration with the European Legal Tech Association (ELTA). One project aims to create a global directory of legal technology use cases where legal tech tools are used for environmental, social, and governance issues.

10. Liability for AI

10.1 Theories of Liability

If any harm is involved, damages arising from AI technologies are generally addressed under existing legal concepts such as tort liability or contractual liability (see **1.1. General Legal Background**).

Within this framework, individuals or entities may be held responsible for damages caused by AI technologies and may be required to pay compensation.

Insurance plays a crucial role in identifying and mitigating liability risks associated with AI technologies. However, insurance for damages caused by AI is not yet widely prevalent in practice. As AI-enabled technologies become more widespread, insurance offerings covering these risks may also become more prevalent in Türkiye.

As for the liability of supply chain participants:

- the Consumer Protection Law holds responsible for damages arising from the relevant product the seller, manufacturer, and importer of the product sold to consumers; and
- the PS Law, which focuses on product safety, is applicable to all products placed on the market in Türkiye, and also holds supply chain participants liable under certain conditions.

Currently, it is a matter of debate in Turkish doctrine whether an AI tool needs to take a tangible form for the PS Law to be applicable. If damage occurs in such a chain, liability may be determined based on the defects attributable to supply chain participants according to the general provisions of the TCO, as general liability is set out therein.

In terms of liability for the consequences of acts and omissions of AI systems, as stated above, the relevant AI cannot be held liable, since AI does not possess legal personality. However, the liability of the AI developer remains a contentious issue in legal doctrine. It is generally believed that under the Turkish law of obligations, the fault of the manufacturer or developer in causing damage through acts or omissions can be ascertained based on the resultant damage.

10.2 Regulatory

Currently, there are no proposed regulations regarding the imposition and allocation of liability.

11. Legal Issues With Predictive and Generative AI

11.1 Algorithmic Bias

Bias in algorithms can be technically characterised as systematic mistakes or flaws in decision-making processes that lead to unjust or discriminating outcomes for particular individuals or groups. From a legal perspective, algorithmic bias raises concerns regarding potential violations of fairness, non-discrimination and consumer protection.

The prohibition of discrimination is specifically regulated in the Constitution. Additionally, to safeguard the prohibition of discrimination, there is the HRE Institution within the administrative organisation, which holds administrative sanctioning powers in cases of behaviour contrary to this prohibition.

Furthermore, certain activities that aim to instigate hate and/or prejudice between people based on language, race, nationality, skin colour, gender, handicap, political viewpoint, philosophical belief, religion or sect, etc, are illegal under the TCrC and punishable by imprisonment. Therefore, if any AI algorithm is developed for such purpose, the developer of the algorithm shall be liable and punished by imprisonment per the TCrC.

11.2 Data Protection and Privacy

The use of systems developed with AI and the data processing activities conducted by controllers using these systems provide significant operational benefits, particularly in terms of the speed with which this new technology processes large datasets and the quality of the outcomes it produces.

Furthermore, AI and ML are expected to play a crucial role in advancing Privacy Enhancing Technologies by enabling more efficient and secure data processing techniques. However, the inclusion of personal data within the data processed through AI systems introduces certain risks.

AI systems, if trained on biased data, can reinforce existing prejudices, leading to discrimination. For example, biased hiring tools may favour certain demographics, while flawed credit scoring algorithms can unfairly deny loans or charge higher interest rates. Human oversight is vital to prevent such unfair outcomes.

Some of the risks and their mitigating recommendations are also addressed in the Recommendations on AI (see **8.3 Data Protection and Generative AI**).

11.3 Facial Recognition and Biometrics

The DP Law is also applicable to the use of facial recognition technology and the processing of biometric data. Since the processing activities carried out by these new technologies involve personal data, it is necessary to comply with the regime set out in the DP Law and secondary legislation during these processing activities. In addition, before the DP Law came into force, the Council of State decided that the activity of keeping track of working hours by processing fingerprints was against the fundamental rights enshrined in the Constitution.

Biometric data is considered special categories of personal data under the DP Law. Processing of such data must first comply with the general principles outlined in the DP Law. There are DPA decisions stating that some biometric data processing activities do not comply with the DP Law for reasons such as:

- the purpose aimed at being achieved by processing biometric data can be achieved with less intrusive means;
- the minimum level of data of the data subject must be processed in order to achieve the purpose; and
- the processing of biometric data that is not necessary for the purpose is not proportionate to the purpose.

Therefore, it is imperative to strictly comply with the principles of purpose limitation and data minimisation when processing biometric data. In addition, in case of non-compliance with these principles, it is possible for the DPA to issue administrative fines in addition to suspending data processing activity. People who suffered damage due to the non-compliance can also claim damages before civil courts.

Special categories of personal data can be processed based on more limited legal grounds compared to other personal data and must be protected with stricter security measures. With the amendment to the DP Law that entered into force on 1 June 2024, the legal grounds on which special categories of personal data can be processed will be broader, since the amendments have introduced five alternative legal bases in addition to those currently existing for processing special categories of personal data applicable to all special categories of personal data. While consent is one of the legal bases for processing biometric data, specific applications may also rely upon newly introduced legal bases, such as (i) processing is mandatory for the establishment, exercise or protection of a right, and (ii) processing is mandatory for the fulfilment of legal obligations in the fields of employment, occupational health and safety, labour, social security, social services, and social assistance. When processing this data based on consent, it is necessary to meet the requirements for valid consent, which should be informed, freely given, specific, and unambiguous.

Additionally, in 2021, the DPA published a guideline on biometric data titled “Guideline on Considerations in the Processing of Biometric Data”. The guideline provides a definition of biometric data and mentions general principles as well as technical and organisational measures in addition to those mentioned above. The DPA has not specified any issue regarding the use of AI in this document.

Apart from data protection, under Turkish banking regulations, a stringent regime governs the utilisation of biometric identification methods for accessing internet and mobile banking, ensuring rigorous adherence to both privacy and security standards (see **1.1 General Legal Background**).

11.4 Automated Decision-Making

There is no specific law governing the applicable framework for automated decision-making (ADM). However, the DP Law is worth mentioning when personal data is involved in such a process as it provides data subjects with the right, under Article 11, to object to a result adversely affecting them when it arises from data processed solely through automated systems (see **8.3 Data Protection and Generative AI**).

This right may be at stake in cases of big data analytics, ADM, profiling or microtargeting, AI (including ML), and autonomous decision-making (including autonomous vehicles). However, the scope of this provision has not yet been clarified by the DPA. Apart from the above provision, there are no specific regulations about profiling, ADM, online monitoring or tracking, big data analysis, AI, or algorithms. Therefore, the general rules would apply.

In contrast to the GDPR, data subjects can object only if their personal data has been analysed exclusively through automated systems resulting in a negative consequence for them. Per the GDPR's "right not to be subject to automated decision-making", data subjects are able to choose not to be subject to automated decision-making even if there is no negative consequence for them.

Under the DP Law, consent is regulated as one of the legal grounds for processing in a general sense. However, there is no specific consent rule for ADM that requires obtaining the consent of the data subject affected by the ADM process. This means that every processing activity should be considered in terms of the purpose and legal grounds upon which the controller relies for such an activity in which ADM is used. There has not been any classification made by the DPA as to which legal basis should be relied upon in terms of ADM. However, it can be said that the legitimate interests of the controller and the consent of the data subject are, among other lawful bases, the most common grounds for processing personal data in activities involving ADM.

If personal data in the public domain is used in the ADM process, data subjects must be informed of this use. Furthermore, data should not be used for purposes other than their initial publication purpose without the data subjects' explicit consent.

Non-compliance with the DP Law, such as insufficient provision of information or failure to accurately determine the lawful basis, may lead to administrative fines and suspension of processing. However, if personal data is not used or anonymised data is used in ADM processes, such processes will not fall within the scope of the DP Law.

Additionally, since ADM processes might be biased due to training with flawed datasets, it is crucial to bear in mind the risk of judicial and administrative sanctions stemming from discriminatory practices (see **11.1 Algorithmic Bias**).

11.5 Transparency

In Türkiye, there is currently no specific regulation that imposes transparency obligations regarding AI systems. Therefore, the general rules apply.

It is necessary to consider the lawful use of AI within the context of the general provisions of relevant existing legislation governing the specific field of application. For instance, in the case of consumer behaviour analysis using AI:

- compliance with the DP Law is required when personal data is used;
- compliance with consumer protection legislation is required when transactions involve consumers; and
- compliance with the Competition Law is required regarding the impact of such practices in the market.

From the standpoint of data protection, it is not required to fully disclose the complexities of how an AI system works or is trained. On the other hand, according to the DP law, the methods used to gather personal data must be specified (ie, whether it is wholly or partially automatic or manual) in a privacy notice. However, the level of detail required in these disclosures remains ambiguous, as the DPA has not yet made any public decisions clarifying this issue. Consequently, it could be argued that controllers are not obligated to specifically disclose whether personal data is collected via AI systems.

Nevertheless, considering the anticipated changes to the DP Law (see **3.6 Data, Information or Content Laws**), it would be prudent to expect more extensive transparency requirements concerning AI applications in the near future. Moreover, the Recommendations on AI stated that AI and data collection activities based on personal data processing should be conducted in consideration of the principle of transparency.

11.6 Anti-competitive Conduct

In Türkiye, the protection of competition is governed by the Competition Law and its secondary regulations.

Currently, there is no specific regulation in the Competition Law or clear approach adopted by the Competition Authority concerning the use of AI. However, if AI is used in practices such as price fixing or customer segmentation among major market players, such uses could fall within the scope of the Competition Law and be investigated by the Competition Authority.

12. AI Procurement

12.1 Procurement of AI Technology

AI solutions mostly raise concerns about confidentiality, data privacy and security since they mostly access large amounts of data. Therefore, transactional contracts between customers and AI suppliers should include clear provisions about confidentiality, data protection measures, strict limitations for the purposes of processing related data, access controls, data storage and encryption and compliance with the DP Law.

Intellectual property ownership of AI-generated works and/or products is a matter of debate currently (see **15.4 OpenAI**). In order to make this ambiguity clear, at least between the parties to the contract, contracts should outline ownership and license rights as well as protection of proprietary algorithms and data.

Furthermore, AI algorithms can unintentionally perpetuate biases or discrimination, resulting in liability risks (see **10.1 Theories of Liability**) for businesses. Contracts should include provisions for transparency, bias, and mitigation measures to ensure compliance with anti-discrimination regulations.

13. AI in Employment

13.1 Hiring and Termination Practices

With technological advancements, companies are increasingly automating recruitment through AI, allowing them to manage large volumes of applications more efficiently than traditional methods. While this speeds up the process and broadens the reach of job postings through platforms, it also introduces significant challenges, including potential biases (see **11.1. Algorithmic Bias**).

Additionally, the use of AI raises data protection risks, such as over-collection of data, insufficient transparency about data processing, and concerns about international data transfers per the DP Law (see **11.2 Data Protection and Privacy**).

When such technologies are used, employees, as data subjects, will have the right to object to a result adversely affecting them when it arises from data processed solely through automated systems (see **8.3 Data Protection and Generative AI**).

AI is increasingly being used in employee performance evaluations and disciplinary actions, which may lead to termination processes. Such usage necessitates strict compliance with labour laws to prevent discrimination and ensure equal treatment. To mitigate these risks, transparency and regular audits regarding how employee data is used are essential.

There are examples of using AI systems to assess the performance of employees and evaluate disciplinary issues, which may lead to termination processes. Again, due to the risks explained above that may lead to discriminatory practices and treatment that violates the principle of equal treatment, it should be ensured that AI systems are used in such applications in accordance with existing labour law rules and general principles laid down thereunder (such as the prohibition of discrimination and the principle of equal treatment).

13.2 Employee Evaluation and Monitoring

Monitoring employees and processing their behavioural data essentially creates a legal risk for the processing of employees' personal data, as it results in the processing of large amounts of personal data, including employees' behavioural data, to an intrusive extent which may violate their right to privacy.

According to decisions of the Constitutional Court and the DPA, as well as the European Court of Human Rights, an employer is entitled to monitor the work computers, work mobile phones and other electronic devices that it provides to its employees, provided that it fulfils the following conditions:

- providing information to employees in advance (eg, by way of a privacy notice addressed to the employees);
- pursuing a legitimate purpose (eg, a compliance investigation based on a reasonable doubt); and
- observing the principle of proportionality (eg, if it is clear from the subject of the email/file that it is a personal email/file, it should not be opened and reviewed).

The obligation here to provide information is more comprehensive and extensive than that of the DP Law. In this case, it is reasonable to expect that workers be informed about the system. These principles of employee monitoring apply regardless of whether AI is used in the process.

14. AI in Industry Sectors

14.1 Digital Platform Companies

AI plays a pivotal role in digital platform companies, especially in sectors like car rental and sharing services and food delivery. By automating tasks such as routing and dispatch, optimising delivery paths, and personalising customer interactions, AI significantly boosts operational efficiency and enhances customer satisfaction.

In Türkiye and around the world, large food delivery companies are notable for their use of AI in chatbot applications. Additionally, a major company that provides car-sharing and scooter rental services has implemented AI-powered optimisation applications aimed at "increasing ridership and reducing operational costs".

However, the benefits of AI also bring several challenges. Companies must navigate issues such as ensuring compliance with data protection rules, addressing algorithmic bias, and meeting labour standards. These factors require a balanced approach to AI implementation, combining innovation with ethical and legal considerations and regulatory compliance to sustainably reshape these industries. However, to the best of our knowledge, unlike in some parts of Europe, these issues have not yet been presented before the courts in Türkiye.

14.2 Financial Services

AI is extensively used in the finance sector, particularly for optimising routine tasks in banks and other financial institutions. AI is especially effective in easily identifying financial risks such as credit and market risks. However, conducting credit risk assessments directly using AI introduces various risks. These include the potential biases inherent in AI and the extensive use of personal data in these applications, which pose significant concerns for both the protection of personal data and general banking sector practices.

In Türkiye, there are no general regulations specific to AI in financial services legislation. However, regulations exist in the legislation applicable to banks and financial leasing companies allowing for the verification of customer identities through AI.

Additionally, the use of AI-supported chatbots in banking applications is quite common in Türkiye. According to banking regulations, customer data must be stored in Türkiye (ie, the data localisation requirement) and cannot be transferred out of Türkiye, unless the BRSA grants permission. Thus, considering the possibility that this data may be disclosed during a conversation, it can be argued that the information collected via chatbots must also be stored in Türkiye. In practice, this interpretation leads banks to generally secure commitments in their service contracts with providers, ensuring that the servers hosting the AI tools are located within Türkiye.

14.3 Healthcare

Türkiye lacks specific regulations governing the use of AI in healthcare. However, the Turkish Medicines and Medical Devices Agency (TITCK) sets the standards for medical devices. TITCK's Strategic Plan for 2024-2028 includes elements related to AI, such as (i) software related to the agency's area of responsibility will be developed, integrated with AI, and the information security infrastructure will be strengthened, and (ii) the infrastructure for rational drug supply management will be enhanced and supported with AI applications. However, it has not yet issued a specific standard for the use of AI in the healthcare sector.

A major concern remains the potential for bias and errors in AI systems including robotic surgery, which can arise from unrepresentative or inappropriately repurposed training data, potentially leading to unsuitable treatments.

Additionally, the centralisation of electronic health records (ie, the e-Nabız Personal Health System) in Türkiye offers prospects for streamlined healthcare services, and it is expected that AI-driven applications will be utilised to (i) promote healthy nutrition among the public, and (ii) prevent MRI exploitation by an AI-based control mechanism via this platform.

While platforms like e-Nabız in Türkiye facilitate the access and sharing of patient data, they also centralise risk, making them prime targets for security breaches. Consequently, while AI offers substantial benefits for advancing healthcare in

Türkiye, its implementation must be accompanied by rigorous oversight to protect patient privacy and ensure equitable treatment outcomes.

Also, the sharing and use of personal health information for training ML algorithms must address privacy concerns and adhere to the DP Law, ensuring data anonymisation and security. The biggest risks are the misuse of sensitive data and the possibility of cyber-attacks, especially in centralised electronic health record systems, which gather all citizens' health information on a single platform, allowing users to access and control it regardless of time and location.

Another exemplary use of AI in healthcare is natural language processing technology. Natural language processing technology helps extract key information from unstructured clinical data, but it must adhere to strict privacy rules to protect patient privacy and data integrity.

14.4 Autonomous Vehicles

According to Turkish law, autonomous vehicles (AVs) and fully autonomous vehicles are defined under separate terms, which implies different degrees of human intervention. Fully autonomous vehicles operate without any human input, while autonomous vehicles still require some human involvement. Therefore, the deployment of autonomous vehicles (with some degree of human control) on public roads is feasible. This interpretation aligns with the existing legislative framework, which distinguishes between these two types of vehicle autonomy, providing a legal basis for autonomous vehicles to be used within regulated limits. In cases where autonomous vehicles are involved in accidents, the operator of the vehicle holds strict liability.

The liability of the driver in traffic accidents is determined according to the TCO.

Since AVs may gather a lot of sensitive and personal data, they present serious privacy and security issues that need strong protections against hacking and other unwanted access. The use of AI to make decisions in critical situations raises ethical questions about algorithmic bias and the necessity for openness in the prioritisation of decisions.

In terms of regulations, no specific regulatory steps have been taken in Türkiye to promote global collaboration and consistency in regulations and standards.

14.5 Manufacturing

See **10.1 Theories of Liability**.

Furthermore, manufacturers often adhere to standards set by the TSE and/or ISO (see **6. Standard-Setting Bodies**) to ensure their products are free of defects.

14.6 Professional Services

Usage of AI in Professional Services

Since there is no specific legislation regulating AI or the use of AI in professional services, the use of AI in providing the related service does not make any difference in terms of the responsibility of the professional providing the service.

Additionally, the provider may be obligated to keep the information private related to the client. In this case, sharing this information with an AI tool without consent could create liability for the provider in terms of confidentiality.

Professional Service as AI Programmers

The Professional Competence Authority is responsible for setting national occupational standards and national qualifications in line with the needs of the labour market. In 2022, the Professional Competence Authority published the Artificial Intelligence Programmer (Level 5) National Occupational Standard, which describes the duties and processes necessary for the successful performance of an AI programmer. Consequently, in the context of AI programmers, it could be construed that employers should recruit individuals who fulfil the criteria outlined in the Standard. Failure to do so may render the employer liable under Turkish labour law for negligence in employee selection in the event of any resulting damages.

There is no specific regulation regarding the use of AI in professional services in Türkiye other than the Standard, therefore general rules apply.

15. Intellectual Property

15.1 Applicability of Patent and Copyright Law

See **8.2 IP and Generative AI**.

15.2 Applicability of Trade Secrecy and Similar Protection

Under Turkish law, trade secrets are not explicitly defined but are characterised by their confidentiality, economic value, and the measures taken to protect them. AI technologies, resulting from significant investments, are safeguarded as trade secrets through regulations aimed at preventing unfair competition and unauthorised disclosure, both of which may result in criminal sanctions under the Turkish Commercial Code and the TCrC, respectively.

It is important to prevent AI from using users' trade secrets as training data. Ideally this concern should be addressed in the agreements executed by AI developers.

15.3 AI-Generated Works of Art and Works of Authorship

See **8.2 IP and Generative AI**.

15.4 OpenAI

See **8.2 IP and Generative AI**.

16. Advising Corporate Boards of Directors

16.1 Advising Directors

As in many legal systems, under Turkish law, the board of directors (BoDs) is authorised to make decisions regarding all kinds of transactions and operations necessary for the conduct of the company's business.

When deciding to utilise AI, corporate boards face multiple challenges that require careful management. These include:

- addressing IP rights breaches and misuse of data;
- providing data privacy and security by using reliable, impartial, and high-quality data;
- maintaining transparency through strong data governance frameworks;
- negotiating important issues in contracts with AI tool producers like licensing, confidentiality (preventing the use of all information in prompts as training data) and service level agreements;
- addressing potential biases in AI outputs by promoting accountability and fairness; and
- reinforcing cybersecurity measures to protect against breaches, cyber-attacks, and any vulnerabilities.

Furthermore, there is no legal obstacle to the use of AI by BoDs under Turkish law. However, it should be noted that under Turkish law, board members can only be elected and represented by individuals who have legal "person" status. Therefore, AI cannot be a board member, nor can it make decisions representing a board member. In this context, when corporate BoDs make certain managerial decisions using AI solutions, they will be responsible for those decisions. Indeed, under the Turkish Commercial Code, in certain situations, board members are personally liable for the decisions they make. In these situations, board members should act with awareness of this fact while using AI in their decisions.

17. AI Compliance

17.1 AI Best Practice Compliance Strategies

Türkiye closely follows legislative efforts, guidelines published by regulatory authorities, and jurisprudence and decisions of competent authorities in the EU in areas that evolve alongside technological advancements, such as cybersecurity, personal data protection, and regulations on payment systems. It is highly probable that Türkiye will incorporate developments occurring in the EU's field of AI into its own legislation in the coming years. Although Türkiye does not currently have specific legislation on AI, aligning with the fundamental values adopted in EU legislation and guidelines for AI applications to be used in the Turkish market will significantly reduce the risk of sanctions by various competent authorities in Türkiye.

On the other hand, the CoE, of which Türkiye is a member, has conducted numerous works in the field of AI. Adhering to the CoE's guidance on AI, to the extent relevant depending on the specific purpose and the means by which the AI technology is to be used, will significantly reduce the risks associated with the use of AI.

The criteria and the values determined during this regulatory process are similar at the EU and CoE levels. Therefore, it is important to comply with these basic criteria, which are given below as suggestions, when utilising AI technology in the Turkish market:

- Transparency and documentation: Complete transparency in AI operations should be adopted. Maintaining comprehensive documentation on AI system's data sources, training processes, and algorithms to support audits and possible scrutiny and demonstrating accountability is crucial.
- Risk/impact assessment: Conducting risk and impact assessment before the commencement of each AI application should be considered and risk-mitigating measures should be taken.
- Ethical considerations: Ethical values including respecting human autonomy, preventing harm, ensuring fairness, and promoting explicability should be adhered to.
- Accountability measures: Clear accountability mechanisms for the use of AI systems, including defining roles and responsibilities for AI developers, deployers, and operators should be created.
- Data governance: Strict data governance practices that respect DP Law and secondary legislation and ensure data quality and data security should be followed.
- Training: It should be ensured that directors and employees are aware of and follow approved policies and procedures designed to ensure safe, transparent, fair, and ethical use of AI.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com