
CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2026

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

Türkiye: Law and Practice
Bora Yazıcıoğlu, Simge Yüce,
Yağmur Yaren Öz dabakoğlu
and Alperen Solak
YAZICIOGLU Legal





Law and Practice

Contributed by:

Bora Yazıcıoğlu, Simge Yüce, Yağmur Yaren Özdebakoglu and Alperen Solak
YAZICIOGLU Legal

Contents

1. Legal Framework p.5

1.1 General Legal Background p.5

2. Commercial Use of AI p.7

2.1 Industry Use p.7

2.2 Involvement of Governments in AI Innovation p.8

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 AI Act p.9

3.5 US State Law p.10

3.6 Data, Information or Content Laws p.10

3.7 Proposed AI-Specific Legislation and Regulations p.10

4. Case Law p.10

4.1 Precedent-Setting Judicial Decisions p.10

5. AI Regulatory Oversight p.11

5.1 Regulatory Agencies p.11

5.2 Regulatory Directives p.11

5.3 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. AI and the State p.12

7.1 Government Use of AI p.12

7.2 Judicial Decisions p.12

7.3 National Security p.12

8. Generative AI p.12

8.1 Generative AI: Key Legal Issues and Regulatory Approaches p.12

9. Legal Tech p.13

9.1 AI in the Legal Profession and Ethical Considerations p.13

10. Liability for AI p.13

10.1 General Theories of Liability p.13

10.2 Regulatory Approaches to Liability for AI p.13

11. Agentic AI Systems and Autonomous Decision-Making p.13

11.1 Agentic AI Systems: Legal Framework and Governance p.13

11.2 Liability Allocation for Autonomous AI Systems p.14

12. Specific Legal Issues With AI p.14

- 12.1 Algorithmic Bias and Fairness p.14
- 12.2 Biometric Technologies and Emotion Recognition p.14
- 12.3 Deepfakes and Synthetic Media p.15
- 12.4 Transparency and Disclosure p.15

13. AI Procurement and Supply Chain Accountability p.15

- 13.1 AI Procurement Standards and Contracting p.15
- 13.2 AI Supply Chain Accountability and Due Diligence p.16

14. Employment p.16

- 14.1 Hiring and Termination Practices p.16
- 14.2 Employee Evaluation and Monitoring p.16

15. AI in Industry Sectors p.17

- 15.1 Digital Platform Companies p.17
- 15.2 Financial Services p.17
- 15.3 Healthcare p.18
- 15.4 Autonomous Vehicles p.18
- 15.5 Retail and Consumer p.18
- 15.6 Industrial AI and Robotics p.19

16. Intellectual Property p.19

- 16.1 IP Protection for AI Assets p.19
- 16.2 AI as Inventor/Author p.20
- 16.3 Copyright and AI Training Data p.20
- 16.4 AI-Generated Works of Art and Works of Authorship p.20
- 16.5 Foundation Models and Open-Source AI: IP Considerations p.20

17. Data Protection p.20

- 17.1 AI Training and Data Protection p.20
- 17.2 AI Deployment and Data Subject Rights p.21
- 17.3 AI Data Governance and Cross-Border Transfers p.22

18. Antitrust p.22

- 18.1 Emerging Antitrust Issues in AI p.22

19. Cybersecurity p.22

- 19.1 Applicability of Cybersecurity Legislation to AI p.22

20. ESG p.22

- 20.1 ESG Dimensions of AI p.22

21. AI Governance and Compliance p.23

- 21.1 AI Governance Frameworks and Implementation p.23

YAZICIOGLU Legal is an Istanbul-based boutique technology law firm. The firm focuses on legal matters related to technology, media and telecommunications, and data protection/cybersecurity. It also has solid expertise in cross-border transactions, corporate and commercial matters, intellectual property, regulatory compliance, e-commerce, consumer protection and dispute resolution. Yazıcıoğlu Legal has a dedicated team of 17 lawyers working on data protection and cybersecurity. The majority of the firm's workload involves data protection-related mat-

ters. In particular, the firm is known for successfully representing its clients in data breach investigations before the Turkish Data Protection Authority. It also provides assistance to several clients, both local and international, including but not limited to Acer, Reddit and Workday, in ensuring compliance with data protection legislation, particularly in cross-border data transfers. 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, Cerus and Ookla in Türkiye.



Alperen Solak is an associate at Yazıcıoğlu Legal. He focuses on various areas of law, including data protection, cybersecurity, e-commerce, contracts and consumer protection.



Simge Yüce is a managing associate at Yazıcıoğlu Legal. She focuses on various areas of law, including data protection, e-commerce, cybersecurity, consumer protection and contracts. She holds a CIPP/E

certificate from the International Association of Privacy Professionals.



Yağmur Yaren Özdebakoğlu is an associate at Yazıcıoğlu Legal. She focuses on various areas of law, including data protection, cybersecurity, e-commerce, contracts and consumer protection.

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

YAZICIOGLU
— LEGAL —

1. Legal Framework

1.1 General Legal Background

Across various jurisdictions, AI regulation is transitioning from soft policy to legislation. Although Türkiye has introduced similar proposals, they have not yet been enacted. Accordingly, AI systems are governed by existing Turkish law, requiring interpretation of current provisions.

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

AI intersects with personality rights, especially in discussions as to whether AI can be recognised as a legal entity and how to address infringements of personality rights, primarily governed by the TCiC. Liability for AI-generated harm is an evolving area under the TCO, which regulates compensation for physical and moral damages arising from torts or contractual breaches. These established principles remain applicable to AI-related disputes (see **10.1 General Theories of Liability**).

Turkish Data Protection Law No 6698 (DP Law)

The DP Law regulates obligations of natural and legal persons in personal data processing, sets out procedures and principles, and aims to protect individuals' fundamental rights and freedoms. It therefore applies where AI systems process personal data.

In September 2021, the Turkish Personal Data Protection Authority (DPA) published Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence (the "Recommendations on AI") (last updated in April 2025), setting out guidance on safeguarding personal data in AI systems, with a focus on fairness, accountability, data minimisation and user rights. The DPA has also issued an informational document on chatbots, highlighting transparency requirements, potential risks associated with AI chatbot applications, and key measures to be considered in their development.

This was followed, in November 2025, by the Guide on Generative Artificial Intelligence and Personal Data Protection (the "Generative AI Guideline") (see **8. Generative AI** and **17. Data Protection**), setting out key

principles for personal data processing in generative AI.

Lastly, in March 2026, the DPA published two separate guidance documents addressing the use of generative AI tools in workplaces (the "Workplace GenAI Guidance") and Agentic AI (the "Agentic AI Guidance"). These documents mainly focus on the organisational and technical measures to be considered when using generative AI systems in workplaces, by addressing the practical reality that employees increasingly use publicly available, third-party tools in their daily workflows, often without institutional knowledge or oversight (see **17. Data Protection**), as well as the complexity of agentic AI systems involving multiple agents, evolving purposes and data uses, which may complicate compliance with DP Law requirements.

Law on Intellectual and Artistic Works (LIAW) and Industrial Property Code (IPC)

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

While Türkiye has still not adopted AI-specific intellectual property (IP) rules, the National AI Strategy 2024–2025 Action Plan identifies clarification of IP rights over AI-generated content as a policy objective; however, no concrete legislation has been enacted as of April 2026.

Law on Product Safety and Technical Regulations (PS Legislation)

While the PS Legislation establishes the general framework for ensuring product safety in Türkiye, including compliance with applicable safety standards and technical regulations, AI-enabled products (such as smart devices and autonomous systems) fall within its scope.

In addition, sector-specific regulations may apply. For instance, AI-enabled medical devices are subject to the relevant medical device legislation issued by the Ministry of Health.

Turkish Criminal Law (TCrC)

Given the potential for AI to be involved in criminal acts (eg, unauthorised access to computer systems or harm caused by autonomous vehicles), various provisions of TCrC may apply. Under the TCrC, only natural persons may be held criminally liable. Whether the developers or users of AI technology can be held responsible is assessed based on intent or negligence.

There is currently no AI-specific provision under the TCrC; however, AI-related conduct is already being addressed under existing laws in practice. In July 2025, an ex officio investigation was launched into the AI chatbot Grok (integrated into the X platform) for generating allegedly insulting content, resulting in access blocking orders.

Moreover, several AI-related legislative proposals have been submitted to the Grand National Assembly of Türkiye (TGNA), representing the most substantive movement towards AI-specific regulation (see **3.7 Proposed AI-Specific Legislation and Regulations**).

Of particular relevance to criminal law, the Bill on Amendments to the TCrC and Certain Other Laws is particularly noteworthy, as it proposes amendments to the TCrC, as well as to the Law No 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication (the “Internet Law”) (see **3.7 Proposed AI-Specific Legislation and Regulations**).

Labour Law No 4857 (Labour Law)

No legislative amendments specifically addressing the use of AI in employment relationships, including AI assisted hiring, performance evaluation, dismissal or employee monitoring, have been enacted. The general framework of the Labour Law, the DP Law and the principles established by the Constitutional Court and the DPA regarding employee monitoring continue to apply (see **14. Employment**).

Consumer Protection Law (CPL)

The CPL and its secondary legislation intersect with AI, particularly in the context of AI-powered consumer interactions, including targeted advertising, automated pricing and chatbots. For instance, the Regulation on Distance Contracts is also relevant in AI-mediated commercial environments, such as AI-driven order flows, automated recommendation systems and conversational interfaces used in customer interactions.

Moreover, the Bill on Amendments to the TCrC and Certain Other Laws legislative package (see **3.7 Proposed AI-Specific Legislation and Regulations**) also includes a proposal on labelling obligations for AI-generated content (including a requirement to display the statement “Generated by Artificial Intelligence” on deepfake content). If enacted, such obligations are likely to have direct implications for consumer protection as well.

Other

Depending on the context, the use of AI may trigger the application of various laws and regulations. In addition, due to AI’s increasing prevalence, government policy has placed significant emphasis on AI developments. Key takeaways include the following.

Cybersecurity Law (CSL)

Despite not constituting a traditional “background law”, the Cybersecurity Law, which entered into force in March 2025, has significant implications for actors operating in cyberspace, including AI developers, deployers and service providers, thereby extending regulatory oversight to AI systems from a cybersecurity perspective.

Law on the Regulation of Electronic Commerce (E-Commerce Law)

E-commerce actors increasingly use AI to remain competitive, impacting e-commerce legislation. For instance, the use of AI is increasingly scrutinised by the Advertising Board under the Ministry of Commerce, which has addressed AI-based advertising in its decisions since 2023. The board has also prepared draft amendments to the Regulation on Commercial Advertising and Unfair Commercial Practices (not yet in force), which were opened for public consultation in late 2025. These amendments mainly introduce

requirements on clear disclosure of AI use and prohibit the misleading use of AI-generated human-like characters or digital replicas of real persons in a way that suggests genuine experience, use or endorsement.

Law on the Protection of Competition (Competition Law)

Competition Law may be engaged in the context of AI, for example where practices such as large-scale data scraping distort competitive conditions. On 7 April 2026, the Turkish Competition Authority (the “Competition Authority”) launched a sector inquiry to conduct an analysis regarding the shaping of AI Ecosystem. Separately, unfair competition rules under the Turkish Commercial Code (TCC) may also address issues such as misappropriation of effort or misleading practices arising from AI use.

Sector-specific frameworks

Among others, under the regulatory frameworks of the Banking Regulation and Supervision Agency (BRSA), Information and Communication Technologies Authority (ICTA) and Financial Crimes Investigation Board (FCIB), the use of AI is commonly used for remote customer onboarding (KYC) in Türkiye’s financial and telecommunications sectors.

Policy and regulation initiatives

AI developments are also closely followed at the policy and regulatory level. The Presidential Decree on Organisation No 1 requires ministries to monitor global developments in AI and big data, and to engage in infrastructure, software and hardware projects in these fields. In addition, the Mid-Term Programme (2026–2028) (MTP) reflects the aim to closely follow emerging AI developments, including plans to harmonise Turkish legislation with the EU AI Act by Q3 2026, update the National AI Strategy (2021–2025) (NAIS) and develop a Turkish large language model.

These initiatives represent the most concrete executive commitments to date, signalling a transition from soft policy co-ordination towards binding legislative action.

2. Commercial Use of AI

2.1 Industry Use

AI is increasingly deployed across industries through different architectural models, enabling distinct applications and levels of autonomy. In Türkiye, this trend is largely driven by institutions such as the Scientific and Technological Research Council of Türkiye (TÜBİTAK), universities, research centres and AI start-ups.

TÜBİTAK supports AI development, particularly in large language models and generative AI. In May 25, TÜBİTAK also announced an “Artificial Intelligence Ecosystem” programme to support commercialisation of AI technologies. Furthermore, the AI start-up ecosystem has expanded significantly; by early 2026, there were approximately 1,188 active AI ventures (versus 379 in January 2025), according to a Turkish NGO report.

In practice, AI applications vary depending on the underlying architecture.

- Predictive Analytics and Traditional Machine Learning – used for data-driven decision-making, including fraud detection, credit scoring and demand forecasting across finance, retail and marketing sectors.
- Foundation models and LLMs – enable generative applications such as chatbots, conversational AI and content generation, used in customer service, media and software development.
- RAG systems – enhance generative models by integrating external data, improving accuracy and reliability, particularly in enterprise and knowledge-intensive sectors.
- Agentic AI systems – enable autonomous decision-making and task execution; use cases include robotics, IoT systems and process automation.
- Autonomous systems – used in areas such as autonomous vehicles, IoT and robotic process automation, enabling automated processes across industries.
- Computer vision – applied across smart platforms and image processing applications, including facial recognition, quality control and surveillance systems.

Across industries, these technologies increase efficiency, reduce costs and enable more personalised user experiences. By 2026, AI use has shifted from exploration to operational deployment. According to 2025 TURKSTAT data, the proportion of enterprises using AI rose to 7.5% (from 4.4%), with 46.5% using AI primarily for marketing and sales.

2.2 Involvement of Governments in AI Innovation

Türkiye, ranked 43rd in the 2025 Global Innovation Index, sustains a diverse AI/ML ecosystem through multi-agency funding.

The primary roadmap is established by the NAIS, the country's first strategic framework, prioritising R&D, entrepreneurship and innovation. This vision has been reinforced by the 2026 Presidential Annual Programme, which designates AI as “national power infrastructure”.

Investment and funding strategies are co-ordinated through a multi-agency structure led by the Ministry of Industry and Technology (MoIT). The Ministry's 2024–2028 Strategic Plan prioritises AI infrastructure and entrepreneurship. A key milestone is the June 2025 call for a Turkish Language Foundation Model, offering grants of up to TRY50 million.

TÜBİTAK remains the primary funder through programmes supporting domestic R&D (TEYDEB) and international collaboration (EUREKA Network). It also launched the Artificial Intelligence Ecosystem Call in 2022, continued in subsequent calls (including 2026, with a TRY15 million budget), supporting commercialisation of AI technologies through joint projects between companies, universities and research institutions.

Moreover, Türkiye facilitates innovation through fiscal incentives. Programmes such as KOSGEB support AI start-ups and SMEs through grants and entrepreneurship programmes, while Law No 4691 on Technology Development Zones provides tax incentives for private sector R&D investment. Under the Investment Incentive Programme, certain AI and high-tech investments may qualify for enhanced incentives.

Türkiye further supports AI innovation through operational support measures, including large-scale digital skills programmes (such as the “1 Million Employment Project”), industry-focused competence centres, and initiatives improving access to data through open data platforms, while institutions such as the Advanced Technologies Research Centre for Informatics and Information Security (BİLGEM) support technical capacity and cross-sectoral research.

AI deployment is also supported by regulatory innovation. For example, the BRSA, together with the Credit Bureau (KKB), has introduced a controlled testing environment (often referred to as an “AI sandbox”) allowing financial institutions to test AI models under regulatory oversight.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

Türkiye's regulatory philosophy towards AI can be characterised as hybrid, combining an innovation-enabling approach with emerging risk-based elements. In the absence of a standalone AI law, Türkiye relies on general legal frameworks, strategic policy instruments and sectoral regulation.

However, there are ongoing efforts to develop an AI regulatory framework, particularly through updates to the NAIS and plans to align Turkish legislation with EU standards as noted in the MTP. (See **1.1 General Legal Background**.)

As Türkiye's first strategic framework, the NAIS sets out key priorities including:

- developing AI/ML expertise and employment;
- supporting R&D and innovation;
- improving access to data and infrastructure; and
- regulatory adaptation.

These priorities have been operationalised through the 2024–2025 Action Plan introducing measures such as “trusted AI” certifications, specialised inspection teams, and alignment with the International Organi-

zation for Standardization (ISO) frameworks. This trajectory is further supported by broader initiatives, including the 12th Development Plan (2024–2028), which prioritises a National Data Strategy to enhance data-driven competitiveness, and the April 2024 Data Governance Framework Recommendation Report, introducing standardised approaches to data access, use and sharing, thereby supporting the data layer of the AI life cycle.

A context- and risk-sensitive approach is emerging in practice, with higher-risk uses subject to stricter requirements, particularly regarding compliance, transparency and auditability. This is reflected in sectoral initiatives such as the BRSA's controlled testing environment and may also imply human oversight.

3.2 Jurisdictional Law

As of April 2026, no AI-specific legislation has been enacted in Türkiye (see **1.1 General Legal Background**).

3.3 Jurisdictional Directives

The absence of a comprehensive AI-specific law has led to increased reliance on non-binding directives and soft-law instruments.

Strategic and Policy-Level Instruments

One influential non-binding document is the NAIS, which underlines the values and principles of “trustworthy and responsible AI” and is expected to be updated under the 2026–2028 MTP.

This is complemented by broader policy documents, including the 2026 Presidential Annual Programme, which outlines priorities and measures for AI integration in public administration (see **7.1 Government Use of AI**).

Ethical and Operational Guidelines

Several institutions have issued guidance on the ethical and operational use of AI. For instance, in May 2024, the Turkish Council of Higher Education published ethical guidelines on the use of generative AI in academic research and publication activities, focusing on ethical considerations in scientific research and publications.

In September 2025, the Ministry of National Education published recommendations on AI ethics, emphasising human oversight in student evaluation and risks of algorithmic bias in educational tools.

Similarly, in October 2025, TÜBİTAK issued guidelines on the responsible and trustworthy use of generative AI in funding processes, highlighting risks such as misinformation, data privacy violations, IP issues and ethical concerns. TÜBİTAK has also developed an internal policy addressing the ethical and strategic use of AI in institutional processes.

Regulatory and Technical Guidance

Sectoral authorities also play a significant role in shaping AI practices through soft-law instruments. In particular, the DPA has issued various recommendations and guidance on AI in personal data processing (See **1.1 General Legal Background**, **8. Generative AI** and **17. Data Protection**).

Further guidance is expected in this area. For example, the BRSA has indicated in its 2025–2028 Strategic Plan that it will develop rules and principles on AI use in digital finance and fintech.

3.4 EU AI Act

While Türkiye is not an EU member state, the 2026–2028 MTP commits to harmonising domestic legislation with the EU AI Act, targeting Q3 2026.

In the absence of comprehensive AI law, a decentralised approach involving existing authorities (eg, BRSA and ICTA) is expected (see **5.1 Regulatory Agencies**). In this regard, the Parliamentary Research Commission on Artificial Intelligence established within the TGNA recommended, in its February 2026 report (the “Commission Report”), adopting a Türkiye-specific AI law and establishing a dedicated authority.

No formal framework exists for high-risk AI conformity assessments, although initiatives such as “trusted AI” under the NAIS suggest emerging alignment with EU standards. Progress is seen in testing environments, including the BRSA's controlled testing environment.

The Commission Report further highlights prospective measures, including:

- regulatory sandboxes;
- potential labelling requirements for AI-generated content;
- sector-specific safeguards for high-risk applications; and
- broader data governance frameworks.

3.5 US State Law

There is no applicable information in this jurisdiction.

3.6 Data, Information or Content Laws

Currently, Türkiye addresses AI-related data and content issues primarily through existing legal frameworks, while legislative efforts are ongoing. (See **3.7 Proposed AI-Specific Legislation and Regulations.**)

In this context, the DPA has issued guidance imposing stricter expectations on AI-related data use. For example, in its Generative AI Guideline, the DPA refers to the possibility of relying on “legitimate interest” for web scraping, subject to strict conditions, and recommends the use of privacy-enhancing technologies (PETs) and synthetic data. (See **17.1 AI Training and Data Protection.**)

3.7 Proposed AI-Specific Legislation and Regulations

Türkiye’s legal landscape for AI is rapidly transitioning from strategic policy to legislative action. While the Commission Report sets the stage for an omnibus law, several bills are currently under review by the TGNA.

- Artificial Intelligence Bill (June 2024) – aims to establish a general framework for AI, defining stakeholder rights and obligations, setting out fundamental principles, and regulating compliance and oversight.
- Bill on Amendments to the TCrC and Certain Other Laws (November 2025) – seeks to establish a comprehensive legal framework for AI systems, addressing risks related to crime, liability, data security, disinformation and public order, notably introducing mandatory labelling of AI-generated content (including deepfakes), expanded liability for users and developers, accelerated content removal mechanisms, and obligations on data governance and AI system safety (including human oversight).

- Internet Law Amendment Bill (December 2025) – introduces a broad mandatory labelling obligation for AI-generated content, requiring all audio, visual and textual outputs created using AI tools to be clearly and visibly identified, reflecting a content-focused approach to combating disinformation and protecting public order.
- Digital Copyright Bill (December 2025) – aims to modernise the copyright framework to address violations arising from AI-generated or reused content and ensure fair remuneration mechanisms, including platform obligations and proactive enforcement tools.
- DP Law Amendment Bill (January 2026) – introduces strict liability for the unauthorised sharing of AI-generated content involving individuals, extending data protection principles to synthetic content. Notably, digital platforms may face administrative fines of up to 5% of their annual turnover per violation, indicating a stringent enforcement approach.
- Bill on Amendments to the LIAW (April 2026) – introduces a licensing regime for the use of copyrighted works in AI systems, requiring AI developers and users to obtain licences for training, development and commercial use. It also establishes a collective rights management system, including extended collective licensing.

At the international level, Türkiye, an early member of the Council of Europe (CoE), participated in the Ad hoc Committee on Artificial Intelligence (CAHAi) (2019–2021) and joined the Committee on Artificial Intelligence in 2022.

4. Case Law

4.1 Precedent-Setting Judicial Decisions

Türkiye is currently in a limited and emerging case law phase regarding AI litigation.

Among others, although not explicitly addressing AI, a decision of the 13th Civil Chamber of Istanbul Regional Court of Appeal provides a basis for evaluating AI training practices, particularly by treating large-scale data scraping and reuse as potential infringements under IP and unfair competition law.

Moreover, in 2025, marking a first in Türkiye, an ex officio investigation into an AI chatbot (Grok on X) indicates that AI-generated outputs may be treated as publishable content with legal consequences, even when produced by systems operated abroad.

5. AI Regulatory Oversight

5.1 Regulatory Agencies

In Türkiye, there is no single dedicated AI regulator; instead, a decentralised model applies, with existing authorities (eg, BRSA, ICTA, DPA) exercising sector-specific oversight.

In late 2025, Presidential Decree No 191 established the General Directorate of National Technology and Artificial Intelligence within the Ministry of Industry and Technology, responsible for policy development, ethics and legislative co-ordination.

In parallel, Presidential Decree No 192 created the General Directorate of Public Artificial Intelligence under the Cybersecurity Presidency to oversee the security and compliance of public sector AI systems.

Finally, the Human Rights and Equality Institution of Türkiye provides independent oversight by ensuring that AI systems comply with fundamental rights and non-discrimination principles.

5.2 Regulatory Directives

No AI-specific regulator has issued dedicated guidance. However, certain regulators, particularly the DPA, have issued non-binding guidance within their areas of competence addressing AI-related matters (see 1.1 General Legal Background).

5.3 Enforcement Actions

Türkiye has not yet developed AI-specific enforcement practice; however, authorities are increasingly addressing AI-related risks under existing frameworks.

In February 2026, the DPA launched investigations into Grok and Google Assistant concerning deepfake content and unintended recording of user data, while the Competition Authority initiated an inquiry into the

AI ecosystem, focusing on data access, market power and value chain dynamics.

The Advertisement Board has also taken enforcement action in multiple decisions, imposing administrative fines for misleading AI-related claims, including references to ChatGPT and unsubstantiated medical promises.

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

The Turkish Standards Institute (TSI) is the primary national standard-setting and certification body in Türkiye, aligning its standards with international frameworks developed by the ISO, International Electrotechnical Commission (IEC), European Committee for Standardization (CEN), and European Committee for Electrotechnical Standardization (CENELEC).

The TSI has adopted relevant standards such as ISO/IEC 42001 (AI management systems), while further standardisation efforts in IT and software remain ongoing.

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.

These standards are primarily adopted through the TSI and serve as technical benchmarks. In particular, ISO/IEC standards such as 42001 (AI management systems), 23894 (AI risk management) and 22989 (terminology) are increasingly used by companies, while conformity assessment is supported by the Turkish Accreditation Agency (TÜRKAK), which accredits certification bodies and offers accreditation related to ISO/IEC 42001 (since 2025).

Moreover, frameworks such as the National Institute of Standards and Technology AI Risk Management Framework and IEEE standards influence best practices, particularly for globally operating companies.

7. AI and the State

7.1 Government Use of AI

In Türkiye, the use of AI in the public sector has expanded significantly under the NAIS, promoting AI adoption through public procurement, big data use and the development of a “Public Data Space” for secure data sharing. Current applications include:

- AI-supported tax inspection;
- the use of AI/ML by the Central Bank for detecting suspicious transactions; and
- AI integration into judicial systems such as UYAP.

AI is also used in infrastructure management and projects by TÜBİTAK for public institutions. These applications typically rely on machine learning, data analytics, natural language processing and computer vision.

Recent policy documents, including the Judicial Reform Strategy (2025–2029) and the 2026 Presidential Annual Programme, indicate further expansion, including chatbots in tax administration, and AI use in citizen services (CİMER), disaster response and defence applications.

While there is no specific AI regulation, general legal frameworks apply, including data localisation requirements for public institutions under Presidential Circular No 2019/12.

7.2 Judicial Decisions

There are no publicly available decisions related to government use of AI.

7.3 National Security

In Türkiye, AI has been increasingly integrated into national security and defence operations, particularly in targeting, image processing, surveillance and cybersecurity. AI-driven systems are used in defence and border control, while defence industry actors, including ASELSAN, are modernising military command systems by integrating AI and big data to enhance tactical decision-making.

At the policy level, Türkiye has engaged with the REAIM Political Declaration and participates in the Convention on Certain Conventional Weapons (CCW),

reflecting a cautious approach to the risks of autonomous weapons. Notably, there is no specific legal framework regulating AI in defence technologies.

National strategies, including the 12th Development Plan, further emphasise the development of AI capabilities in defence, such as AI chip production and the use of AI and big data analytics for early detection and prevention of cybersecurity threats.

In June 2025, the National Intelligence Academy (NIA) published a report entitled Artificial Intelligence, Society and Security: Situation Analysis and Turkey’s Strategic Roadmap, outlining a strategic framework for integrating AI into national security governance, including initiatives such as explainability testing, red-team laboratories and secure data-sharing infrastructures.

8. Generative AI

8.1 Generative AI: Key Legal Issues and Regulatory Approaches

Generative AI systems pose legal challenges in Türkiye, which are addressed under existing legal frameworks. These systems give rise to a broad range of issues, including copyright risks in training data and outputs, as well as data protection risks such as unlawful processing, hallucinations and data leakage. They also create significant liability risks, as harmful outputs, including misinformation and deepfakes, may cause real-world damage. In addition, bias and discrimination remain key concerns, as models trained on imbalanced datasets may produce unfair outcomes.

From a regulatory perspective, authorities have begun addressing these risks through enforcement and soft law. For instance, the Advertisement Board has investigated AI-generated advertisements and manipulative practices since 2023, imposing fines for misleading claims.

The risks associated with generative AI have also been highlighted by the DPA in its Generative AI Guideline. The DPA emphasises IP risks in training on large-scale copyrighted datasets and potential infringing outputs, as well as data protection risks and the need for tech-

nical and organisational measures to ensure transparency and compliance. (See **17. Data Protection.**)

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

The use of AI in the legal profession is expanding, particularly in legal research, document review, contract analysis and case management.

AI is increasingly used in supporting functions within the legal profession. For instance, the Supreme Court Precedent Centre employs AI-based tools for case management, and the Ministry of Justice has introduced AI-based OCR systems for notice processing (see **7.1 Government Use of AI**).

In addition, SaaS tools are used by law firms for large-scale decision analysis and document review, and policy developments indicate a move towards AI-assisted litigation.

However, generative AI raises significant risks. Hallucinations may lead to inaccurate or fabricated legal information, as illustrated by a 2026 case before the Istanbul Regional Court of Appeal, 14th Civil Chamber, where a party claimed that cited case law had been generated by AI and did not reflect real decisions.

AI tools also raise concerns regarding unauthorised legal advice and client confidentiality, particularly when using cloud-based systems subject to the DP Law. Moreover, lawyers may face malpractice risks, as they remain the ultimate responsible actors under the Attorneyship Law and must ensure human-in-the-loop review of AI-generated outputs. Core obligations such as confidentiality, diligence and independence continue to apply, and failure to properly supervise AI use may result in professional liability.

10. Liability for AI

10.1 General Theories of Liability

Liability for harm caused by AI systems is assessed under existing legal frameworks. Claims are primar-

ily based on tort and contractual liability under the TCO, as well as sector-specific rules such as the CPL and the PS Legislation (see **1.1 General Legal Background**). Since AI lacks legal personality, liability is attributed to relevant actors in the value chain, including developers, deployers and users.

These frameworks cover multiple liability theories, including:

- product liability for defective AI systems (with debate on standalone software);
- fault-based liability where due care is lacking;
- strict liability in high-risk activities;
- vicarious liability within organisational use; and
- liability for AI-generated content, such as defamation and IP infringement.

However, applying these frameworks to AI raises evidentiary and causation challenges. The “black box” nature of AI complicates establishing fault and causation, while multiple actors across the AI life cycle create attribution difficulties. These challenges have led to doctrinal debates on burden of proof and the adequacy of existing liability models.

While insurance is an important tool for mitigating AI-related risks, such coverage is not yet widespread in Türkiye but is expected to develop with increased AI adoption.

10.2 Regulatory Approaches to Liability for AI

There is currently no AI-specific liability regime in Türkiye; liability continues to be governed by existing legal frameworks (see **10.1 General Theories of Liability**).

11. Agentic AI Systems and Autonomous Decision-Making

11.1 Agentic AI Systems: Legal Framework and Governance

Existing laws applied by analogy for agentic AI (see **1.1 General Legal Background**).

However, the Agentic AI Guidance provides the first dedicated assessment for these systems, highlighting

a central requirement of human oversight, which must be proportionate to the level of autonomy and ensured across the life cycle. It also emphasises transparency and explainability, requiring that system behaviour and inter-agent interactions be traceable.

In terms of accountability, the Agentic AI Guidance stresses clear allocation of responsibility among stakeholders, particularly distinguishing between developers and deployers, and promotes co-ordinated governance to manage risks. These issues become more complex in multi-agent systems, where distributed decision-making may create unpredictability and attribution challenges.

11.2 Liability Allocation for Autonomous AI Systems

In Türkiye, liability for autonomous AI is allocated under existing legal principles and contractual arrangements, but faces serious challenges in causation, attribution and systemic complexity (see **1.1 General Legal Background** and **10. Liability for AI**).

12. Specific Legal Issues With AI

12.1 Algorithmic Bias and Fairness

Algorithmic bias may be technically defined as systematic errors in decision-making processes that produce unfair or discriminatory outcomes for certain individuals or groups, often arising from imbalanced or unrepresentative training data. From a legal perspective, such bias raises concerns regarding violations of fairness, equality and non-discrimination principles.

The prohibition of discrimination is specifically regulated under the Constitution. The Human Rights and Equality Institution of Türkiye operates as the competent authority and has the power to impose administrative sanctions in cases of conduct contrary to this prohibition.

Certain discriminatory or hate-inducing acts are criminalised under the TCrC, meaning that AI systems developed or used for such purposes may trigger criminal liability.

In its guidances, the DPA identifies algorithmic bias as a key risk, noting that AI systems may reproduce inequalities due to imbalanced datasets. It recommends mitigation measures, including:

- diverse and representative datasets;
- monitoring and auditing of outputs; and
- corrective techniques such as fine-tuning.

12.2 Biometric Technologies and Emotion Recognition

Biometric data processing is primarily governed by the DP Law. While there is no explicit regulatory framework addressing technologies such as emotion recognition, the approach of the DPA can be inferred from its decisions.

In principle, biometric data processing is not prohibited but is subject to strict conditions under the DP Law. Data controllers must rely on a legal basis under Article 6, with explicit consent being the most commonly used ground for AI-based tools. Controllers are also required to inform data subjects of the processing of their data via privacy notices and to demonstrate necessity and proportionality, especially where less intrusive alternatives exist.

The 2025 DPA Guidelines on Special Categories of Personal Data clarify legal bases and emphasise enhanced safeguards, including:

- policies;
- staff training;
- access controls; and
- technical and physical security measures (eg, encryption, logging and secure data transfer).

Failure to comply may result in administrative fines of up to TRY17,092,242 for data security breaches and up to TRY1,709,200 for violations of information obligation as of 2026.

The processing of biometric data may also trigger liability under the TCrC in the following cases:

- unlawful recording;
- transfer;
- disclosure; or

- failure to delete personal data.

Criminal investigations may be initiated ex officio by public prosecutors.

Finally, sector-specific regulations also impose additional constraints. For example, in the banking sector, under the Regulation on Banks' Information Systems and Electronic Banking Services, banks must implement:

- robust identity verification;
- access controls; and
- risk-based, multi-layered security measures.

Non-compliance may result in administrative sanctions, including fines and operational restrictions.

12.3 Deepfakes and Synthetic Media

In Türkiye, deepfakes and synthetic media are not governed by a dedicated legal framework. However, recent legislative proposals introduce requirements to label AI-generated or manipulated content (see **3.7 Proposed AI-Specific Legislation and Regulations**).

Civil remedies are available under the TCiC (protection of personality rights, including injunctive relief and damages) and the TCO (tort liability). Criminal liability may arise under the TCrC for offences such as defamation, insult or threats, and the DP Law applies where deepfakes involve the unlawful processing of personal data (eg, the use of facial images to create deepfakes).

Moreover, under the Internet Law, content removal and/or access blocking decisions may be issued by a judge or, in urgent cases, by administrative authorities, for the protection of:

- the right to life;
- public order;
- national security;
- prevention of crime; or
- public health.

12.4 Transparency and Disclosure

Transparency obligations arise indirectly through existing legal frameworks. Depending on the use

case, compliance may be required under several laws, including the CPL (for consumer interactions) and Competition Law (for market effects of AI-driven practices).

The Generative AI Guideline clarifies transparency expectations and specifies key requirements, including:

- chatbot disclosure (informing users of AI interaction);
- enhanced explainability (data types, processing logic and output criteria); and
- supply chain transparency (informing downstream deployers of risks and limitations) (see **17. Data Protection**).

Additional guidance issued by the Authority, such as the Workplace GenAI and Agentic AI Guidance, also encourages organisations to adopt transparency, data governance and risk management measures.

At the policy level, alignment with the EU AI Act is expected to introduce more structured transparency obligations, particularly for high-risk systems and AI-generated content (see **3.4 EU AI Act**).

13. AI Procurement and Supply Chain Accountability

13.1 AI Procurement Standards and Contracting

AI contracting is governed by general contract law principles under the TCO. Contracts typically address risk allocation between developers, providers and users, often supported by service level agreements (SLAs) defining performance standards such as uptime, accuracy thresholds and response times.

AI procurement raises key concerns around data protection, confidentiality and security, as such systems process large volumes of data. Contracts therefore include provisions on the following:

- data use limitations;
- access controls;
- storage;

- encryption; and
- compliance with the DP Law.

With respect to IP, ownership of AI-generated outputs remains legally uncertain (see **16. Intellectual Property**). Contracts therefore typically clarify ownership and licensing, as well as protection of proprietary algorithms and datasets.

Contracts also commonly include compliance warranties and indemnities, as well as audit rights to verify performance, data handling and compliance. These obligations are often reinforced through liability caps and insurance provisions.

Finally, exit and portability provisions are increasingly used to address vendor lock-in, ensuring data access and operational continuity upon termination.

13.2 AI Supply Chain Accountability and Due Diligence

AI supply chain accountability and due diligence obligations are addressed indirectly under existing legal frameworks.

Under guidances issued by the DPA, organisations are expected to implement appropriate technical and organisational measures, effectively requiring due diligence when procuring AI systems involving personal data. The Generative AI Guideline further emphasises that transparency extends beyond data subjects to value chain stakeholders, requiring providers to inform deployers about privacy and data protection risks and mitigation measures.

From a liability perspective, the PS Law may impose liability on manufacturers and importers for defects, including those arising from third-party components such as APIs or pre-trained models. Liability for such components is further governed by tort and contractual principles under the TCO.

Turkish companies operating within the extraterritorial scope of the EU AI Act may face cascading compliance obligations across the value chain. Consequently, contractual mechanisms such as compliance warranties, audit rights and indemnities play a key role in

managing supply chain risks, particularly for high-risk AI systems.

14. Employment

14.1 Hiring and Termination Practices

Such practices are primarily assessed under constitutional, labour and data protection frameworks.

While AI-driven recruitment enhances efficiency, it introduces significant risks of algorithmic bias (see **12.1 Algorithmic Bias and Fairness**). The principle of equality and non-discrimination under the Constitution, reinforced by the Labour Law, prohibits discriminatory outcomes.

The use of AI in recruitment (eg, CV screening or candidate scoring) must comply with equal treatment and non-discrimination principles. Similarly, termination decisions must be based on “just or valid cause”; reliance solely on AI-generated outputs, without human verification, is unlikely to satisfy the requirement of a “concrete and objective” basis for dismissal.

Under the DP Law, the use of AI in HR processes raises concerns regarding excessive data collection, lack of transparency and unlawful processing. The use of AI systems in decision-making processes, makes data subject rights particularly relevant. Employees may object to decisions based solely on automated processing where such decisions produce adverse effects (see **17. Data Protection**).

Employers must ensure that AI-assisted hiring and termination practices remain fair, transparent and subject to human oversight.

14.2 Employee Evaluation and Monitoring Monitoring

Employers increasingly use AI-based tools for productivity monitoring, performance analytics and biometric systems. However, such practices raise privacy risks due to large-scale processing of personal and behavioural data.

Under DPA practice, employers may monitor work devices (eg, computers and mobile phones) subject to certain conditions:

- employees must be informed in advance;
- monitoring must pursue a legitimate purpose (eg, compliance investigations based on reasonable suspicion); and
- the principle of proportionality must be respected (eg, clearly personal communications should not be accessed).

These principles also apply to AI-based monitoring tools, including cybersecurity and insider threat detection systems.

Case law of the Constitutional Court confirms that monitoring of corporate communication may be permissible where employees are clearly informed and the interference remains proportionate.

However, intrusive practices (particularly, continuous surveillance or biometric tracking) are subject to strict scrutiny. In this regard, the Council of State has established that mandatory facial recognition for employee attendance violates the right to privacy.

Evaluation

AI-based systems are increasingly used for employee evaluation, including performance scoring affecting employment outcomes.

Under labour law, performance-based decisions must meet the requirement of a “just or valid cause” and be supported by concrete and objective criteria. In this context, AI outputs should be treated as supporting evidence with human oversight, rather than decisive factors.

From a DP Law perspective, employees have the right to object to adverse outcomes resulting from automated processing of their personal data. However, the DPA’s Generative AI Guideline seems to suggest a broader expectation of human involvement in AI-supported decision-making, not limited to detrimental outcomes.

AI-based evaluation also raises discrimination risks, particularly where models rely on historical or behavioural data that may disadvantage certain groups. In such cases, employers may bear the burden of demonstrating that evaluation criteria are objective, consistently applied and non-discriminatory.

15. AI in Industry Sectors

15.1 Digital Platform Companies

AI is widely deployed across digital platform companies in Türkiye, including e-commerce, food delivery and gig-economy platforms. These activities are governed by existing legislation. Key laws include the DP Law, particularly in relation to profiling and targeted marketing. Certain requirements under the E-Commerce Law (eg, transparency of ranking criteria) may also affect AI-related practices, while the CPL framework introduces transparency obligations for AI-powered chatbots and automated systems (see **1.1 General Legal Background**).

The increasing use of AI by large platforms is drawing regulatory attention, particularly regarding data-driven market power. The Competition Authority has signalled growing interest in the AI ecosystem, including through sectoral review.

15.2 Financial Services

AI use in Türkiye’s financial sector is expanding, primarily governed by existing banking, capital markets and data protection frameworks. Algorithmic trading falls within automated and high-frequency trading activities regulated by the Capital Markets Board. Investment firms must ensure that trading systems are tested prior to deployment, subject to risk controls, and capable of audit and, where necessary, human intervention.

In the banking sector, AI-based credit scoring and automated decision-making tools are widely used, raising considerations around bias, transparency and lawful data processing.

More broadly, financial institutions are expected to manage risks arising from internal models, including AI, within risk management and internal control

frameworks set by the BRSA, requiring model validation, monitoring and audit, and generally applied to AI-based systems.

15.3 Healthcare

AI use in healthcare in Türkiye is increasing, particularly in diagnostics, imaging, clinical decision support and hospital management systems. Institutional capacity is also developing, including through the Turkey Health Data Research and Artificial Intelligence Applications Institute (TÜYZE) under the Turkey Health Institutes Authority (TÜSEB), with recent initiatives such as AI-supported radiology tools (RADIS) indicating gradual clinical deployment.

Türkiye lacks specific regulations governing AI in healthcare; instead, existing frameworks on medical devices, healthcare services and data protection apply, with enforcement under these regimes, particularly regarding patient safety and health data processing.

AI-based software may qualify as a medical device, subject to requirements set by the Turkish Medicines and Medical Devices Agency (TITCK). The TITCK's 2024–2028 Strategic Plan signals increased focus on AI, including development of AI-integrated systems and strengthened information security.

More broadly, the use of AI in healthcare is expected to comply with general requirements on patient safety, medical ethics and service quality, with regulatory scrutiny where risks arise in relation to patient safety, data protection or medical device compliance.

The use of AI involving health data is subject to strict data protection rules, as health data is classified as a special category requiring enhanced protection (see **12.2 Biometric Technologies and Emotion Recognition**). Centralised systems such as e-Nabız Personal Health System may enable AI-driven applications while increasing compliance expectations.

15.4 Autonomous Vehicles

There is no dedicated legal framework for autonomous driving; existing road traffic, vehicle safety and product compliance rules apply, with enforcement under these regimes.

Turkish law is based on a human driver model and does not distinguish between levels of autonomy, which limits deployment of fully autonomous vehicles. Liability is generally assessed under traffic and obligations law principles, with the operator typically remaining responsible. The use of AI in vehicles also raises data protection and cybersecurity considerations due to the volume of personal data processed.

The regulatory landscape shifted in November 2025 when provisions for temporary traffic authorisations for test vehicles were repealed without replacement. Authority over vehicle testing and compliance remains with the MoIT, which has delegated aspects of testing and standard-setting to the TSI. The TSI has issued internal instructions governing public road testing, setting out application requirements and technical criteria such as type approval, safety assessments and testing documentation.

This results in a fragmented and evolving framework, with testing governed in practice through administrative and technical standards rather than a comprehensive statutory regime.

15.5 Retail and Consumer

The use of AI in Türkiye's retail and consumer sector is expanding, particularly in:

- personalised marketing;
- recommendation systems;
- dynamic pricing; and
- customer analytics.

It is primarily regulated under existing consumer protection, e-commerce, competition and data protection frameworks (see **1.1 General Legal Background**).

Marketing and profiling activities also fall within consumer and advertising rules, including restrictions on misleading practices and unfair commercial conduct. The Advertisement Board actively monitors promotional content, and enforcement has extended to AI-assisted marketing, particularly where claims are unsubstantiated or lack objective support (see **5.3 Enforcement Actions**).

Legislative developments also indicate increasing regulatory attention, including proposed transparency and labelling obligations for AI-generated content (see **3.7 Proposed AI-Specific Legislation and Regulations**).

15.6 Industrial AI and Robotics

AI and robotics are increasingly used in Türkiye's industrial sector, particularly in manufacturing and automation, and are primarily regulated under existing product safety and occupational health and safety frameworks.

In practice, industrial robots are subject to machinery and product safety requirements aligned with EU standards, including conformity assessment and CE marking where applicable. Manufacturers and operators must ensure that AI-enabled systems meet safety requirements, particularly where automated functions affect predictability and control. Deployment also engages workplace safety obligations, especially where robots interact with human workers.

Liability is assessed under existing product liability and general tort law principles. Depending on the circumstances, responsibility may arise for manufacturers, operators or employers, particularly where defects, inadequate safeguards or operational risks are involved.

Professional standards are also developing in parallel. The Vocational Qualifications Authority has introduced occupational standards for AI-related roles, which may inform expectations around competence and due care, including in employee selection.

Industrial AI adoption is also supported by public initiatives, including programmes promoting digital transformation in manufacturing SMEs (see **2.2 Involvement of Governments in AI Innovation**).

16. Intellectual Property

16.1 IP Protection for AI Assets

From an IP perspective, the primary frameworks are the LIAW and the IPC. AI-related elements, including models, training data, inputs and outputs, may be

protected under IP rights, trade secrets or contractual arrangements, depending on their characteristics.

Copyrights (Software, Data and Outputs)

AI software is protected as a computer program under the LIAW; however, protection is generally limited to the source code and its expression, not underlying ideas or algorithms. While Turkish law does not provide a sui generis database right, databases may be protected where originality requirements are met.

Training data may qualify for copyright protection where it reflects the author's personal characteristics. Unauthorised use may constitute infringement, although the legal assessment of training use remains unsettled and context-dependent. Turkish law does not currently provide a specific text and data mining (TDM) exception, which may increase legal uncertainty.

AI-generated outputs are generally considered unlikely to meet the requirement of human authorship and may therefore fall outside the scope of copyright protection. Where AI is used as a tool under human direction, authorship may be attributed to the user, depending on the level of creative contribution. Turkish courts have not yet established clear precedent on this issue.

AI systems may give rise to infringement risks, particularly in relation to the use of copyrighted material for training and the generation of outputs that reproduce or resemble protected works. These issues remain largely untested in Turkish case law.

Patent/Utility Model

AI-assisted inventions may be protected if they meet three criteria:

- novelty;
- inventive step; and
- industrial applicability.

AI systems are not currently recognised as inventors due to the absence of legal personality. Inventorship and ownership are therefore typically linked to natural persons contributing to the inventive process. Therefore, fully autonomous outputs are likely to face significant patentability challenges.

In practice, AI-related inventions may be assessed in line with approaches to computer-implemented inventions before the Turkish Patent and Trademark Office (TÜRKPATENT).

Industrial Designs/Trade Marks

AI-generated designs may be protected where novelty, distinctiveness and human contribution are present. AI-related branding elements (eg, names and logos) may be protected as trade marks, subject to general requirements.

Trade Secrets/Confidential Information

In practice, significant value in AI systems is often protected as trade secrets, including model architectures, training methodologies, datasets and model weights. Such information may be protected under general principles of confidentiality and unfair competition, provided it remains undisclosed and commercially valuable.

Contractual Allocation

Ownership and use of AI-related inputs and outputs are frequently determined by contractual arrangements. In practice, such terms may define rights over inputs and outputs, impose usage restrictions, and allocate responsibility between developers, providers and users.

Unfair Competition

AI-related products that do not meet specific IP protection criteria may nevertheless be addressed under unfair competition provisions of the TCO.

Recent legislative proposals reflect increasing attention to AI-related copyright issues, including content reuse and remuneration (see 3.7 Proposed AI-Specific Legislation and Regulations).

16.2 AI as Inventor/Author

See 16.1 IP Protection for AI Assets.

16.3 Copyright and AI Training Data

See 16.1 IP Protection for AI Assets.

16.4 AI-Generated Works of Art and Works of Authorship

See 16.1 IP Protection for AI Assets.

16.5 Foundation Models and Open-Source AI: IP Considerations

See 16.1 IP Protection for AI Assets.

17. Data Protection

17.1 AI Training and Data Protection

Where AI training involves personal data, the general requirements of the DP Law apply. The DPA has highlighted AI-specific risks in its guidance, with the Generative AI Guideline being particularly relevant as it addresses data processing across the entire AI life cycle, including collection, training and deployment.

In principle, controllers must rely on a legal basis under Article 5 of the DP Law. In practice, explicit consent and legitimate interests are the most relevant grounds for AI training, although their applicability depends on the specific use case. Among other requirements for obtaining explicit consent (ie, given freely and based on being informed, in relation to a specific matter), the DPA expects additional information on the type of system, in particular:

- the nature of the AI system;
- whether personal data will be processed for development or operational purposes;
- the nature, function and purpose of the outputs to be generated; and
- whether such outputs may allow personal data to be accessed or viewed by third parties.

The guideline further stresses that consent should be granular and specific to each processing activity; separate consent may be required for (i) the use of uploaded data for training and (ii) the reuse of outputs for further model development.

The guideline emphasises that the use of publicly available data does not eliminate the need for a legal basis; however, it may be considered in the legitimate interest balancing test, particularly in web scraping scenarios, which require careful assessment of purpose compatibility.

General principles (ie, lawfulness and fairness, accuracy, purpose limitation and data minimisation) fully

apply to AI training. The Guideline places particular emphasis on transparency and fairness, requiring that data subjects are informed in a clear, accessible and timely manner about how their data is used, including the types of data processed and the logic underlying outputs. It also highlights the need to assess the volume of data used during training, the proportionality of processing, and the effective implementation of data minimisation measures.

While the general rules on special categories of data remain applicable, the Guideline underlines that their use in training datasets increases risks of discrimination, bias and privacy violations, and therefore requires enhanced technical and organisational safeguards. In practice, the inclusion of such data in large-scale training datasets should be carefully assessed and limited to what is strictly necessary.

Data subjects retain their rights under Article 11, including access, rectification, erasure and objection. Controllers must implement effective and accessible mechanisms to enable the exercise of these rights during the training phase. However, in practice, exercising these rights may be challenging, as personal data may be embedded in model parameters and difficult to isolate or remove without affecting system performance.

The guideline recommends the use of privacy-enhancing technologies, including anonymisation and pseudonymisation. Fully anonymised data falls outside the DP Law, but the threshold is high and must be assessed in light of re-identification risks, particularly in AI systems processing large and diverse datasets. Pseudonymised data, on the other hand, remains personal data and continues to be subject to legal requirements.

The guideline adopts a life cycle-based approach and emphasises accountability throughout the development, training and deployment phases of AI systems. Controllers are expected to implement appropriate technical and organisational measures and maintain documentation demonstrating compliance, including recording data sources, applying data mapping or labelling techniques, and ensuring traceability of datasets used in training. Controllers should also imple-

ment logging mechanisms and monitoring processes to track how data is used over time.

Lastly, the Agentic AI Guideline notes that such systems may dynamically update data usage, incorporate unforeseen datasets, or reuse data across tasks, requiring continuous monitoring to ensure alignment with defined purposes.

17.2 AI Deployment and Data Subject Rights

The deployment of AI systems involving personal data is subject to the general requirements of the DP Law. Controllers must establish a legal basis under Article 5. In practice, explicit consent and legitimate interests are most commonly relied upon, although their applicability depends on the use case.

Transparency obligations apply in full, including the obligation to inform data subjects about the processing of their personal data. The Generative AI Guideline expects enhanced transparency, including informing data subjects about the potential consequences of automated decision-making, where relevant.

Data subjects retain their rights under Article 11. In particular, individuals may object to outcomes producing adverse effects where such outcomes are based exclusively on automated processing. Unlike the GDPR, this right is triggered only where a negative consequence arises. While the DP Law does not provide a standalone right to explanation, the DPA's approach suggests that controllers are expected to provide meaningful information on the logic involved and potential consequences.

Deployers should also give specific importance to data retention and deletion obligations. Personal data must be retained only as long as necessary for the processing purpose. In AI systems, particular consideration should be given to retention of input data, logs and outputs, as well as to technical challenges in deleting or anonymising data embedded within models.

The processing of children's data requires particular care, including limiting data collection to what is strictly necessary and ensuring age-appropriate design and control, reflecting the DPA's approach to enhanced protection of vulnerable data subjects.

While there is no comprehensive AI-specific regulation in this area, recent amendments to the Internet Law introduce specific obligations for social network providers, including age verification for users under 15, age-appropriate services and parental control tools. These developments indicate a broader regulatory trend towards heightened safeguards for children's data, which may also influence the deployment of AI systems involving children in the coming years.

17.3 AI Data Governance and Cross-Border Transfers

The Generative AI Guideline emphasises privacy by design and by default across the AI life cycle and highlights data protection impact assessments (DPIAs) as a key risk management tool, particularly given the complexity of AI systems.

In AI supply chains, roles are determined by factual influence over the purposes and means of processing, rather than contractual allocation. Accordingly, a model developer may act as a controller for training, while a deploying entity may be determined as a controller for its own use of the system.

Cross-border data transfers must comply with Article 9 of the DP Law and applicable secondary legislation, requiring an adequacy decision, appropriate safeguards (eg, standard contractual clauses) or reliance on limited derogations. Given the scale and continuity of AI-related data flows, transfer mechanisms should be continuously monitored.

18. Antitrust

18.1 Emerging Antitrust Issues in AI

In Türkiye, competition law is governed by the Competition Law and its secondary legislation. There is currently no AI-specific regulatory framework or established decisional practice. However, existing competition rules apply irrespective of the technology used. The use of AI in practices such as pricing, customer segmentation or strategic decision-making may fall within the scope of the Competition Law where it leads to anti-competitive effects, including co-ordination between competitors or the strengthening of market power.

AI may also raise concerns in the context of mergers, data-driven dominance and vertically integrated ecosystems, particularly where access to data, infrastructure or key technologies may affect competitive dynamics.

19. Cybersecurity

19.1 Applicability of Cybersecurity Legislation to AI

Türkiye has recently strengthened its cybersecurity framework with the entry into force of the CSL on 19 March 2025, establishing a centralised governance model under the Cybersecurity Authority. However, the CSL does not include AI-specific provisions and, in the absence of detailed secondary legislation, the framework remains at an early stage. However, general cybersecurity obligations may apply to AI systems. Organisations deploying AI should consider risks such as adversarial attacks, data poisoning, model extraction and unauthorised access, and implement appropriate technical and organisational measures across the AI life cycle.

The CSL introduces general obligations relating to system security and incident management, which may apply to AI systems depending on their use and criticality. Incident reporting and response obligations may therefore extend to AI-related security events.

20. ESG

20.1 ESG Dimensions of AI

In Türkiye, ESG considerations in the context of AI are not subject to a standalone regulatory framework but are reflected in broader policy documents emphasising sustainability and responsible technological development.

At the policy level, the 12th Development Plan (2024–2028) promotes a sustainable and competitive high-tech industry, with AI as a key driver, emphasising innovative, reliable and accountable systems aligned with sustainability goals, as well as effective use of human capital and advanced technologies.

In addition, the 2025 Annual Programme refers to the TÜBİTAK Digital Transformation Assessment Model, which supports businesses in digital maturity assessments and the development of sustainability-oriented transformation roadmaps.

21. AI Governance and Compliance

21.1 AI Governance Frameworks and Implementation

Türkiye lacks a comprehensive AI-specific governance framework, but governance is increasingly shaped through existing legal, compliance and policy structures influenced by EU and Council of Europe standards.

In practice, particularly in regulated sectors such as banking and telecommunications, organisations are embedding AI governance within existing compliance, risk and board-level oversight structures. This approach is predominantly risk-based, often aligned with international standards such as ISO/IEC 42001, which, while not legally binding, supports structured AI risk management.

Governance is applied across the AI life cycle and is typically integrated into data protection, internal audit and enterprise risk management functions. It includes controls on data quality, bias and model performance (eg, model drift), as well as the use of AI inventories and risk-based classification (eg, biometric data or high-impact use cases such as credit scoring). Documentation and accountability remain central, including records of data sources, model development processes and risk or impact assessments where appropriate. Governance also extends to third-party providers through contractual safeguards (eg, audit rights and transparency clauses) and ongoing oversight, while organisations remain responsible for compliance.

In practice, implementation is challenged by regulatory uncertainty, as organisations must navigate evolving frameworks applied in a technology-neutral manner. Technical constraints also limit transparency and explainability in complex (“black-box”) systems, particularly where legal frameworks require understandable outputs. In addition, data governance and infrastructure dependencies, especially on global AI providers, may reduce visibility over models and increase reliance on third-party systems.

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 Luke.Wilson@Chambers.com