Legal 500
Country Comparative Guides 2026

Turkey
Artificial Intelligence

Contributor

Hamzaoğlu
Hamzaoğlu Kınıkoğlu
Attorney Partnership

Yücel Hamzaoğlu

Partner | yucel.hamzaoglu@hhklegal.com

Batu Kınıkoğlu

Partner | batu.kinikoglu@hhklegal.com

Melike Hamzaoğlu

Partner | melike.hamzaoglu@hhklegal.com

Nur Güler

Senior Associate | nur.guler@hhklegal.com

Osman Yücel

Managing Associate | osman.yucel@hhklegal.com

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in Turkey.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Turkey: Artificial Intelligence

1. What is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

As of today, Türkiye does not have a specific, standalone law regulating artificial intelligence (AI), and accordingly, there is no statutory legal definition of AI under Turkish law. References to AI are mostly found in policy-level documents rather than in binding legislative instruments.

The most prominent of these is the National Artificial Intelligence Strategy (2021–2025), jointly issued by the Ministry of Industry and Technology and the Digital Transformation Office of the Presidency of the Republic of Türkiye. This strategy provides a conceptual definition of AI as "the ability of a computer or computer-controlled robot to perform various activities in a manner similar to that of intelligent creatures." While not legally binding, the strategy reflects the national policy orientation and terminological preferences regarding AI.

There is also a draft Bill on Amendments to Certain Laws Regarding Artificial Intelligence, submitted to the Presidency of the Grand National Assembly of Türkiye, which proposes introducing a statutory definition of an "artificial intelligence system" into Internet Law No. 5651. In addition, the Turkish Personal Data Protection Authority's Guidelines on Generative AI and the Protection of Personal Data, dated 24 November 2025, define generative AI as a type of artificial intelligence system trained on large-scale datasets and capable of generating content in various formats—such as text, images, video, audio, or software code—in response to a user-entered prompt or command. The Authority's February 2026 guide on "Agentic AI" further describes agentic systems as capable of evaluating environmental conditions, adapting to changing circumstances and initiating actions with varying degrees of autonomy.

Although no statutory binding definition currently exists, it is widely expected that any future legislative efforts in Türkiye concerning artificial intelligence will adopt a definition similar to that found in the EU Artificial Intelligence Act, reflecting ongoing efforts to ensure compatibility with international regulatory trends.

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made in its implementation? Are there plans for updates or revisions?

Yes. Türkiye has recently announced a new national framework for artificial intelligence through the Türkiye Artificial Intelligence Action Plan for the 2026–2030 period, which was presented by the President on 13 June 2026.

Based on the publicly available announcement, the Action Plan is structured around four main pillars: "Be Aware", "Benefit", "Produce" and "Govern". The announced priorities include increasing AI literacy, strengthening Türkiye's AI talent pool, facilitating access to public datasets, expanding data-centre capacity, supporting domestic AI development, and establishing governance mechanisms for the responsible and trustworthy use of AI.

The announced targets include providing AI-literacy training to 5 million people within two years, training 10,000 advanced AI specialists and 100,000 applied AI professionals, making at least 2,000 public datasets available through the National Data Library, increasing Türkiye's data-centre capacity to at least 1 GW by 2030, and mobilising at least USD 10 billion—predominantly from the private sector—for AI infrastructure.

However, as of the date of this review, the full text of the 2026–2030 Action Plan does not appear to have been published as a standalone official document. Accordingly, the details currently available are limited to the publicly announced framework, targets and policy priorities. Since the Action Plan has only recently been announced, its implementation remains at an early stage. Further details and concrete progress are expected to become clearer as the relevant public institutions publish implementation measures, monitoring outputs, and sector-specific programmes under the 2026–2030 framework.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/are applied to

 © 2026 Legalease Ltd

artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

Türkiye has not yet enacted a binding, comprehensive legal framework specifically regulating artificial intelligence (AI). In the absence of AI-specific legislation, several existing legal instruments may apply depending on the specific use case to certain aspects of AI technologies. These include the Law on the Protection of Personal Data No. 6698, particularly in areas such as automated decision-making and profiling; the Law on Consumer Protection No. 6502, which may apply to AI systems interacting with consumers; and the Law on Product Safety and Technical Regulations No. 7223, which can be relevant for AI-integrated products in the context of conformity and liability requirements.

In addition, general provisions under the Turkish Code of Obligations No. 6098 and the Turkish Civil Code No. 4721 may become relevant in cases involving tort liability, contractual obligations, or personal rights, depending on the use case of the AI system. However, these laws were not designed with AI in mind and may fall short in addressing the unique features of AI, such as autonomy and adaptiveness.

Applying these general laws to AI raises considerable interpretive difficulties. The evolving and probabilistic nature of AI systems complicates assessments related to causation, foreseeability, and fault—key elements in both private and public law contexts. For example, it remains unclear how legal responsibility should be allocated when a self-learning AI system changes its behavior post-deployment in a way that leads to harm or non-compliance.

Although there is no comprehensive AI-specific law, Türkiye has adopted certain policy-level and soft-law instruments relevant to AI. In particular, the Turkish Personal Data Protection Authority's Guidelines on Generative AI and the Protection of Personal Data, dated 24 November 2025, address the use of generative AI systems from a data protection perspective and assess the related personal data processing activities under Law No. 6698. The Authority has since supplemented this guidance in February 2026 with two further documents—one on the use of generative AI tools in the workplace and another on agentic (autonomous) AI systems.

As for legislative developments, the most recent initiative is the Bill on Amendments to Certain Laws Regarding Artificial Intelligence, submitted to the Turkish Grand National Assembly on 7 November 2025, which—rather than establishing a standalone AI statute—proposes AI-specific amendments to existing laws, introducing a statutory definition of an "artificial intelligence system" together with rules on AI-generated (deepfake) content, accelerated takedown timelines and training-dataset requirements through changes to the Internet Law No. 5651 and the Turkish Penal Code No. 5237.

More recent legislative and institutional activity also indicates increasing regulatory attention to AI-related issues, including proposals concerning AI-generated content and amendments to Internet Law No. 5651. In parallel, broader digital and cybersecurity developments—such as the Cybersecurity Law No. 7545 and institutional changes introduced by Presidential Decrees dated 25 December 2025—may be relevant to AI governance, although they do not constitute a comprehensive AI-specific regulatory framework.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

Türkiye does not yet impose AI-specific transparency, explainability, or audit obligations. In the absence of dedicated legislation, the relevant requirements derive from general instruments—most importantly the Law on the Protection of Personal Data No. 6698 (PPDL). Where an AI system processes personal data, data controllers must satisfy the PPDL's transparency and disclosure duty (the obligation to inform data subjects), and Article 11 grants individuals the right to object to a result produced solely through the automated processing of their data. The Turkish Personal Data Protection Authority's November 2025 Guidelines on Generative AI reinforce that data subjects must be informed, in clear terms, where their personal data is processed by AI systems. Its February 2026 guide on agentic AI adds a risk-management dimension: recognising that the multi-layered, autonomous operation of such systems makes transparency and explainability harder to achieve, it recommends that explainability be built in by design—clearly exposing how system components interact and supporting this with mechanisms that monitor system behaviour—so that how the system works and why particular decisions are taken can be understood and meaningful human oversight maintained.

Beyond data protection, sector-specific rules can impose disclosure or explainability expectations—for example in

 © 2026 Legalease Ltd

banking and financial services, where automated decisions affecting customers are subject to regulatory oversight—and consumer-protection principles require that information provided to consumers not be misleading. There is, at present, no general legal obligation to disclose to customers that they are interacting with an AI system; however, the pending AI legislative proposals contemplate transparency duties, including the labelling of AI-generated content, which would introduce more explicit disclosure requirements if enacted. In particular, a pending bill would amend the Internet Law No. 5651 to require that AI-generated "deepfake" content be clearly labelled or otherwise marked; even if enacted, this would remain narrower than a general, customer-facing AI-disclosure regime.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

There are currently no binding, AI-specific rules mandating human oversight or a "human-in-the-loop" in Türkiye. The closest existing requirement is found in the Law on the Protection of Personal Data No. 6698, Article 11 of which entitles individuals to object to a decision producing a result against them that is based solely on automated processing—effectively encouraging meaningful human involvement in significant automated decisions. Sectoral regulators, particularly in banking and finance, likewise expect that consequential decisions are not left entirely to automated systems. In its Guidelines on Generative AI and the Protection of Personal Data, the Turkish Personal Data Protection Authority likewise recommends that the outputs of AI systems be regularly monitored and, where necessary, supported by human-oversight mechanisms. The Authority's February 2026 guide on agentic AI likewise adopts a human-centric approach, noting that the human role shifts towards setting objectives, monitoring system behaviour and intervening where necessary.

As a matter of best practice, and in anticipation of alignment with the EU AI Act, organisations deploying higher-risk AI systems are increasingly adopting human-oversight mechanisms voluntarily. The pending AI legislative proposals expressly reference human-review mechanisms for high-risk applications, which, if enacted, would place human oversight on a statutory footing for certain use cases.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

Türkiye has no AI-specific legislation addressing algorithmic bias, discrimination, or fairness. The applicable protections stem from general law. The Constitution guarantees equality before the law (Article 10), and the Law on the Human Rights and Equality Institution of Türkiye No. 6701 prohibits discrimination—including on the ground of sex—in the provision of goods and services, which may extend to outcomes produced by AI systems. In the employment context, the Labour Law No. 4857 prohibits discrimination, and in data processing the PPDL's principles of lawfulness and fairness apply to profiling and automated decision-making.

There is, however, no dedicated obligation requiring bias testing or fairness auditing of AI systems. The pending AI legislative proposals seek to address this gap: the Bill on Amendments to Certain Laws Regarding Artificial Intelligence provides that datasets used to train AI must comply with principles of non-discrimination and legitimacy, and treats the use of discriminatory datasets as a breach of data security. The Turkish Personal Data Protection Authority's Guidelines on Generative AI and the Protection of Personal Data similarly warn that biases present in training data may be reproduced and reinforced in system outputs, and that the "black-box" nature of such models complicates the detection and correction of bias. Its February 2026 guide on agentic AI adds that, in multi-step or multi-agent workflows, errors and biased outputs may propagate and be reinforced across the chain, making them harder to detect and correct. Until such measures are enacted, addressing algorithmic bias—including gender bias—remains a matter of general anti-discrimination law and voluntary best practice.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

Türkiye has not enacted a dedicated liability regime for AI, so harm caused by defective AI systems is assessed under existing instruments on a case-by-case basis, depending on how the system is used, the parties involved, and the type of harm. The Law on Product Safety and Technical Regulations No. 7223 is the

 © 2026 Legalease Ltd

principal product-safety framework: a defective AI system—such as one embedded in a smart device—may qualify as a "product", and its manufacturer or importer may be held liable where the product, when used under normal conditions and in accordance with its instructions, poses more than minimal, foreseeable risks specific to its intended use. Where AI is embedded in a regulated product (for example, a medical device), sector-specific safety regulations with their own liability provisions also apply.

Liability may be borne by different actors depending on their role. Under the product-liability rules of Law No. 7223, the manufacturer or importer is strictly liable for defects regardless of fault (importers being treated as manufacturers). Under the Turkish Code of Obligations No. 6098, providers may be liable in contract for improper performance and in tort for fault-based conduct, with liability apportioned among multiple contributors according to fault. Strict liability may also arise under the employer-liability and "dangerous enterprise" regimes, so an operator deploying AI in inherently hazardous activities—for example, autonomous vehicles or industrial automation—may be liable regardless of fault. The Law on Consumer Protection No. 6502 additionally entitles consumers to remedies (repair, replacement, refund, price reduction, and compensation) where an AI-enabled good or service is defective, and the Law on the Protection of Personal Data No. 6698 holds data controllers and processors accountable where a defective system causes a personal-data breach.

The burden of proof generally lies with the victim, and its content depends on the basis of liability. In tort, the victim must establish unlawful conduct, fault, damage, and a causal link; in contract, that the system failed to perform as agreed (the provider may escape liability by proving the absence of fault). In strict-liability cases—such as product defects or harm from dangerous activities—fault need not be shown, and the victim need only prove the damage and its causal link to the AI system.

In practice, proving causation is the central difficulty: the autonomous, adaptive, and often opaque behaviour of AI systems complicates the assessment of causation, foreseeability, and fault. As of today, there are no binding court decisions or enacted legislation specifically addressing AI liability, and the framework remains under development. Notably, the pending Bill on Amendments to Certain Laws Regarding Artificial Intelligence would begin to allocate responsibility expressly—treating a user who directs an AI system to commit an offence as the perpetrator and increasing the penalty for developers whose design or training facilitates the offence (see Q3 and Q20 for pending initiatives).

8. What cybersecurity obligations apply to AI systems?

There are no cybersecurity obligations specific to AI systems as such; instead, AI systems are subject to Türkiye's general cybersecurity and data-security framework. The most significant recent development is the Cybersecurity Law No. 7545, which entered into force on 19 March 2025 and, for the first time, established a comprehensive and centralised cybersecurity regime under the Cybersecurity Board and the Cybersecurity Directorate. The Law imposes technical and administrative obligations on a broad range of public and private actors operating in cyberspace—particularly those designated as critical infrastructure in sectors such as energy, telecommunications, health, and finance—including asset inventories, risk analyses, penetration testing, audit readiness, and incident notification, backed by significant administrative fines and criminal penalties.

In parallel, the Law on the Protection of Personal Data No. 6698 requires data controllers and processors to take appropriate technical and administrative measures to ensure data security, which is directly relevant to AI systems that process personal data during training and deployment. The pending Bill on Amendments to Certain Laws Regarding Artificial Intelligence would add AI-specific security duties—such as dataset transparency and verifiability, content-verification tools, checks against manipulative or hallucinated outputs, human-review mechanisms for high-risk applications, and routine cybersecurity testing—which, if enacted, would layer AI-specific obligations onto the existing framework.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

In Türkiye, the use of artificial intelligence (AI) is not governed by a dedicated insurance framework, and there are currently no AI-specific insurance products mandated or widely available in the market. However, AI-related risks may be insurable under existing general insurance categories, depending on the specific context and application of the technology. For example, certain incidents involving AI—such as data breaches, algorithmic errors, system malfunctions, or losses arising from automated processes—may be covered under traditional policies like professional liability, cyber risk, product liability, or general business insurance.

 © 2026 Legalease Ltd

In terms of market trends, cyber-insurance uptake is growing among larger Turkish enterprises, particularly in the finance, technology, and e-commerce sectors, and insurers are increasingly attentive to AI-related exposures when underwriting cyber and professional-liability policies. Key limitations include the absence of standardised AI-specific cover, the difficulty of quantifying algorithmic and autonomous-system risks, and the likelihood that losses stemming from unlawful data processing or wilful misconduct fall outside standard policy coverage.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

Under Article 109 of the Law on Industrial Property No. 6769, the right to obtain a patent belongs to the inventor or his/her successors in title. Under Turkish patent law, an invention is patentable only if it is novel, involves an inventive step, and is capable of industrial application. These substantive requirements apply equally to inventions developed with the assistance of artificial intelligence (AI). However, the Law does not specifically address the possibility of AI being named as an inventor. The patentability criteria concern the characteristics of the invention itself rather than the legal nature of its inventor, as the current statutory framework was drafted before AI inventorship became a practical legal issue. While Turkish patent law does not contain a specific provision addressing the inventorship of AI, there have so far been no court decisions or administrative practice concerning AI inventorship, nor have any patent applications designating an AI system as the inventor been publicly reported before the Turkish Patent and Trademark Office (TURKPATENT). Accordingly, the issue has not yet been tested in practice and remains open to future legal and judicial development.

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

Under Turkish law, images generated by or with the assistance of artificial intelligence (AI) may benefit from copyright protection only if they meet the conditions set out in the Law on Intellectual and Artistic Works No. 5846.

The law defines a "work" as an original intellectual or artistic product that reflects the individuality and creativity of its author and falls within specific categories such as literary, musical, or visual works. The Court of Cassation has emphasized that to qualify as a protected work, a creation must (i) be expressed in a concrete and perceptible form, and (ii) reflect the personal creative contribution of its author.

If a person exercises sufficient creative control over the final expression, for example, through the creative selection, arrangement, refinement or editing of AI-generated outputs—the resulting work may qualify for copyright protection, provided that the required level of originality and personal character is met.

Hence, there is no court decision in Türkiye that directly and solely addresses the copyright status of AI-assisted works, and any assessment would need to rely on existing general principles of authorship and originality.

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

Under Turkish law, the use of artificial intelligence (AI) systems in the workplace—especially in areas like hiring, performance evaluation, and employee monitoring—raises significant legal and ethical concerns. Key issues include potential violations of employee privacy, discriminatory outcomes, lack of transparency, and unlawful data processing. At present, there are no AI-specific regulations governing employment practices; instead, such use is primarily regulated under existing labor and data protection laws.

Under Turkish labor law, AI tools must not lead to discrimination or unfair treatment. This is especially important under the Labor Law No. 4857, which prohibits discrimination based on language, race, color, gender, disability, political opinion, philosophical belief, religion, or similar grounds. Employers are, therefore, expected to take proactive steps to ensure that AI systems promote equal treatment and comply with anti-discrimination obligations.

AI systems used in the workplace must comply with the Law on the Protection of Personal Data No. 6698 by ensuring that data processing is lawful, transparent, and respectful of employee privacy. Employers are required to

 © 2026 Legalease Ltd

obtain valid consent or rely on another legal basis, avoid excessive data collection, and clearly inform employees about how their personal data will be used. AI-based employee monitoring tools—such as surveillance systems, keystroke trackers, or behavior analysis software—must be proportionate, necessary, and transparent. Excessive or covert monitoring can violate not only data protection laws but also constitutional protections of privacy and personal liberty. The Turkish Constitutional Court has consistently affirmed employees' rights to privacy within the workplace. In addition, AI-driven decision-making, particularly when applied without meaningful human oversight, may raise legal concerns under both data protection and labor laws.

In February 2026, the Turkish Personal Data Protection Authority published a dedicated guide, "Use of Generative AI Tools in the Workplace," which addresses the phenomenon of "shadow AI"—the uncontrolled use of third-party generative-AI tools by employees, who may share meeting notes, internal correspondence, drafts, and customer or employee data with such tools. The guide identifies risks to auditability and accountability, decision quality, intellectual property and trade secrets, information and cyber security, and personal data protection, and recommends that organisations adopt a clear internal AI-use policy rather than an outright ban—defining which tools may be used and for what purposes, restricting the information that may be entered (favouring anonymised or generalised inputs and exercising particular caution with sensitive data), preserving meaningful human review of outputs, and implementing data-security and access controls such as limiting access to approved tools and corporate devices.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

Under Turkish law, the development and use of artificial intelligence (AI)—particularly in training models and processing personal data—raises several important privacy concerns governed primarily by the Law on the Protection of Personal Data No. 6698 (PPDL).

AI systems often require large datasets for training, which may include sensitive or personally identifiable information. Under the PPDL, any collection, use, or processing of such data must have a legal basis, such as explicit consent or another lawful ground defined by the law. Using personal data—especially special categories like health or biometric data—for AI training without meeting these conditions can result in unlawful processing.

Another concern is purpose limitation and data minimization. Personal data must be collected for specific, explicit, and legitimate purposes and not processed in ways incompatible with those purposes. AI models trained on data later used for unrelated functions—such as profiling or targeted decision-making—may breach this principle.

Automated decision-making also poses privacy risks, especially if decisions significantly affect individuals (e.g., hiring, credit scoring, or surveillance). Although the PPDL does not yet contain a specific provision banning such practices, it obliges data controllers to ensure fair processing, transparency, and the right to object, which becomes challenging when opaque AI systems are involved.

Another key issue involves cross-border data transfers, as many AI systems are developed, trained, or hosted using international infrastructure or third-party services. Under the PPDL, such transfers are strictly regulated and allowed only if appropriate safeguards are in place—for example, by signing and submitting standard contracts published by the Turkish Data Protection Authority. Without these safeguards, international transfers may be deemed unlawful.

Moreover, data security is a key issue. Developers and deployers must take adequate technical and administrative measures to protect data against breaches, leaks, or unauthorized access during both training and deployment of AI systems.

As for guidance, the Turkish Personal Data Protection Authority (TPDA) has taken several steps to address the intersection of AI and data protection. In September 2021, it issued its "Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence," outlining key principles—such as transparency and accountability—for AI developers, operators, and service providers processing personal data through AI systems; this guidance was updated in April 2025 without substantial changes to its content. On 8 November 2024, the TPDA published an "Information Note about Chatbots," highlighting privacy risks associated with AI-powered conversational tools and emphasizing obligations such as conducting risk assessments before processing personal data. Sector-specific documents, including the "Guidelines on Good Practices in the Banking Sector," also address the safeguarding of

 © 2026 Legalease Ltd

personal data in AI-driven tools and services.

Most significantly, on 24 November 2025 the TPDA published its "Guidelines on Generative AI and the Protection of Personal Data (in 15 Questions)," its first comprehensive interpretation of how the PPDL applies to generative AI. The key takeaways are that generative AI is fully subject to the PPDL; that each stage of a system's lifecycle—development and training, active use, and output generation—constitutes a distinct processing activity to be assessed on its own footing; and that personal data may be produced even at the output stage, whereas the use of genuinely anonymized data falls outside the scope of the Law. The Guidelines also address the reproduction of bias in outputs, the "black-box" problem, and data-leakage and deepfake risks, and they recommend transparency, data minimization, security measures, and human-oversight mechanisms across the AI lifecycle. The Authority has continued this work into 2026, publishing further guidance in February 2026 on the use of generative AI tools in the workplace and on agentic (autonomous) AI systems, which it describes as systems capable of evaluating environmental conditions, adapting to changing circumstances and initiating actions with varying degrees of autonomy.

In terms of enforcement, while the TPDA has recognized the growing significance of AI in personal data processing through these guidelines and publications, it has not, to date, issued publicly known binding decisions or sanctions specifically concerning artificial intelligence systems, although AI-related data processing remains subject to its general supervisory and enforcement powers.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

Data scraping activities are not directly governed by a dedicated law in Türkiye; however, such practices are assessed under several existing legal frameworks, including intellectual property and data protection, each of which may entail significant risks depending on the nature and scope of the scraping involved. Although no specific judicial precedents currently address the legality of scraping for AI training purposes, Turkish law provides a basis for evaluating such activities through applicable general rules.

From an intellectual property perspective, scraping may infringe on rights protected under the Law on Intellectual and Artistic Works No. 5846. Databases that reflect creative effort may qualify as copyrighted works. Unauthorized extraction of substantial parts of such databases can amount to infringement, with rights holders entitled to seek injunctions and damages. Turkish courts have also affirmed that certain websites and layouts may be protected as databases or graphic works if they display intellectual effort (Turkish Court of Cassation, 11th Civil Chamber, Case No. 2016/6829, Decision No. 2018/768, dated 5 February 2018).

Regarding privacy, if scraping involves personal data, it qualifies as "processing" under the Law on the Protection of Personal Data No. 6698 (PPDL), requiring a valid legal basis such as explicit consent or legitimate interest. The PPDL's "public data" exception is narrowly construed, and scraping publicly accessible data for unrelated uses like profiling or marketing could result in administrative penalties or even criminal sanctions under the Turkish Penal Code for unlawful collection or disclosure. In November 2025, the Turkish Personal Data Protection Authority published its Guidelines on Generative AI and the Protection of Personal Data, confirming that every stage of an AI system's lifecycle—including the collection and use of training data—must comply with the PPDL, which further constrains large-scale scraping of personal data for AI training The Authority's February 2026 guide on agentic AI further notes that such systems may autonomously access personal data and combine it with information obtained from other sources, so that a valid legal basis and the other requirements of the PPDL apply to these data-collection activities as well.. From a competition law angle, systematic scraping of content or commercial data may constitute unfair competition under Article 55 of the Turkish Commercial Code No. 6102. In particular, the unauthorized use of another company's commercial data to gain economic benefit, damage its reputation, or attract its customers may result in legal consequences.

15. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

Under Turkish law, data scraping prohibitions in a website's terms of use can be enforceable, particularly when users have explicitly accepted these terms before accessing the site. Such clauses are generally binding under the Turkish Code of Obligations No. 6098, provided they are clearly communicated and not contrary to principles of good faith or mandatory legal rules. If users

 © 2026 Legalease Ltd

provide affirmative consent—such as through a clickwrap agreement—violating a no-scraping provision may constitute a breach of contract, allowing the website owner to pursue remedies like access restrictions, account termination, or damages.

Even in the absence of explicit acceptance, unauthorized and systematic scraping may give rise to liability under other legal regimes. Many Turkish websites, including e-commerce and classified ad platforms, expressly prohibit automated tools (e.g., bots or scrapers) in their terms of service and reserve the right to take legal action against violations. While such terms may not be contractually binding on all users, their presence helps demonstrate that the website owner has not consented to scraping and supports potential claims under intellectual property, data protection, or unfair competition laws. As such, clearly worded and prominently displayed no-scraping clauses serve both as contractual safeguards and as evidence in broader enforcement efforts against unauthorized data extraction.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

As of today, Türkiye does not have a single, dedicated authority exclusively responsible for supervising the use and development of artificial intelligence (AI). However, oversight is distributed among various public institutions, each playing a role within its regulatory mandate.

The Digital Transformation Office of the Presidency of the Republic of Türkiye and the Ministry of Industry and Technology are the primary bodies responsible for shaping AI policy and coordinating national strategy.

The institutional framework was further strengthened by two Presidential Decrees dated 25 December 2025. Decree No. 191 renamed the National Technology General Directorate, under the Ministry of Industry and Technology, as the National Technology and Artificial Intelligence General Directorate and expanded its mandate to cover data centre and cloud infrastructure, standards and certification processes, national AI capacity, and AI-related research and regulatory work. Decree No. 192 broadened the responsibilities of the Cybersecurity Directorate and established a new Public Sector Artificial Intelligence General Directorate tasked with overseeing the use of AI within public institutions.

Regulatory and sectoral supervision of AI applications is currently handled through existing authorities:

The Turkish Personal Data Protection Authority (TPDA) oversees the processing of personal data in AI systems under the Law on the Protection of Personal Data No. 6698, ensuring privacy compliance.

The Information and Communication Technologies Authority (ICTA) monitors the telecommunications and digital services sectors, which increasingly involve AI-based applications.

Sector-specific regulators in Türkiye—such as the Banking Regulation and Supervision Agency, the Central Bank of the Republic of Türkiye, and the Ministry of Health—may oversee the use of AI within their respective domains (e.g., banks, fintech, digital health tools).

The Cybersecurity Directorate—placed on a statutory footing by the Cybersecurity Law No. 7545—coordinates cybersecurity policy and practices across public institutions and, following the establishment of the Public Sector Artificial Intelligence General Directorate under Presidential Decree No. 192 (25 December 2025), has an expanded role in overseeing AI governance within the public sector.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

In Türkiye, the use of artificial intelligence (AI) by businesses is growing steadily but remains uneven across sectors. While adoption is not yet widespread on a national scale, it is gaining momentum, particularly among large enterprises and technology-forward industries. The most rapid and advanced adoption of AI technologies has been observed in the finance, telecommunications, e-commerce, and manufacturing sectors. In these industries, AI is being deployed for applications such as fraud detection, predictive analytics, customer behavior analysis, process automation, demand forecasting, and supply chain optimization.

The finance sector, for example, has integrated AI into credit scoring, risk assessment, and chatbot-based customer services. Similarly, major e-commerce platforms utilize AI for personalized recommendations, dynamic pricing, and logistics optimization. The health sector is also showing increasing interest, particularly in diagnostic tools, medical imaging, and hospital management systems.

18. How is artificial intelligence used in the legal

 © 2026 Legalease Ltd

sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

Artificial intelligence (AI) is increasingly being adopted in the Turkish legal sector, particularly among larger law firms and in-house legal departments. Although AI tools are not yet integrated into the routine operations of courts, there is growing interest in their use for lawyers' day-to-day tasks, such as document review, bilingual contract analysis, legal research, and drafting—areas where efficiency, accuracy, and speed are increasingly prioritized. Due diligence activities, particularly in cross-border mergers and acquisitions and compliance reviews, are increasingly benefiting from AI-powered solutions that enhance efficiency, reduce review times, and minimize human error. Nonetheless, a key barrier to the development of effective domestic tools remains the limited availability of Turkish-language AI training datasets and legal-domain resources.

From a regulatory standpoint, the use of AI tools by lawyers may raise important questions under the Law on Attorneyship No. 1136, particularly with regard to strict professional confidentiality obligations, the prohibition on advertising and solicitation, and the requirement that legal services be provided personally and responsibly by licensed attorneys. It is also significant that there is currently no binding ethical framework or official guidance from the Union of Turkish Bar Associations on the use of AI in legal services, which contributes to uncertainty surrounding professional liability and the interpretation of these obligations under the Attorneyship Law in the context of AI deployment.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Artificial intelligence (AI) presents both significant challenges and promising opportunities for lawyers in Türkiye. One major challenge lies in the regulatory uncertainty surrounding AI. While certain national strategies, soft law instruments, and policy papers introduce general principles regarding the development and use of AI, Türkiye lacks a comprehensive and binding legal framework specifically tailored to AI technologies. This gap creates ambiguity in legal compliance, particularly in how lawyers should tackle, interpret, and apply existing laws—or develop new legal approaches—to address the complex issues arising from the development, deployment, or use of AI systems in practice. Lawyers also face growing concerns about data privacy and ethical risks, including bias in AI systems and the explainability of their outputs, which could impact client trust and professional responsibility. Limited familiarity with technology among some legal professionals can make it harder to assess or use AI tools effectively. Additionally, there are concerns about job displacement as AI threatens to automate routine tasks such as document review and research. Finally, unresolved questions around liability—particularly when legal outcomes are influenced by AI-generated insights—pose a serious challenge in determining accountability.

Despite these concerns, AI offers considerable opportunities for the legal profession in Türkiye—many of which reflect broader global trends. AI-powered tools can dramatically enhance the efficiency of legal research, document drafting, and contract analysis, reduce turnaround times, and improve accuracy. Predictive analytics can assist lawyers in evaluating litigation risks and outcomes based on historical court decisions, thus supporting more strategic client advice. Automation of administrative tasks—ranging from deadline tracking to compliance monitoring—frees up time for higher-value legal reasoning and client engagement. Globally, AI is also seen as a key driver in expanding access to justice, and in Türkiye, AI-driven platforms have the potential to offer cost-effective legal support and guidance to individuals in underserved or remote areas. Finally, as in many jurisdictions, early adoption of AI in Türkiye's legal sector can offer a competitive edge, as innovation and technological fluency are becoming key differentiators in delivering efficient, high-quality client service in an increasingly dynamic legal market.

20. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

In the next 12 months, Türkiye is expected to witness important legal developments in the field of artificial intelligence (AI), largely driven by domestic regulatory initiatives and an ongoing effort to align with international—particularly European Union—standards.

While the most significant progress is likely to focus on establishing a foundational framework for AI regulation, two legislative proposals are already before the Grand National Assembly—a comprehensive, risk-based Artificial Intelligence Law Bill, which would introduce mandatory registration for high-risk AI systems and a

 © 2026 Legalease Ltd

national AI registry, and a Bill on Amendments to Certain Laws Regarding Artificial Intelligence (Esas No. 2/3358), submitted on 7 November 2025, which would introduce a statutory definition of an "artificial intelligence system" together with deepfake-labelling, six-hour takedown and dataset requirements through amendments to the Turkish Penal Code, the Internet Law No. 5651 and other statutes—although the enactment of a comprehensive, standalone AI law within this timeframe remains uncertain given the complexity and length of the legislative process. Notably, Türkiye's Medium-Term Programme (2024–2026) sets completing the alignment of national data protection law with the EU acquis, particularly the GDPR, as a key objective—reflecting a broader harmonization trend that suggests the EU AI Act may likewise influence the future direction of AI regulation in Türkiye. In the meantime, regulatory efforts are likely to concentrate on articulating ethical principles, updating secondary legislation—especially in the area of data protection—and issuing institutional or sector-specific guidelines. Consistent with this, the Turkish Personal Data Protection Authority published its Guidelines on Generative AI and the Protection of Personal Data in November 2025, and in January 2026 a further bill was submitted proposing to amend the PPDL to introduce a turnover-based administrative fine on platforms that enable the sharing of AI-generated content without the data subject's consent. Parallel to these developments, growing references to AI in judicial decisions are anticipated, which may help shape legal interpretation on matters such as automated decision-making, liability, and data privacy through evolving case law. Additionally, the National Artificial Intelligence Strategy and its 2024–2025 Action Plan, prepared by the Digital Transformation Office of the Presidency of the Republic of Türkiye and the Ministry of Industry and Technology, having reached the end of their 2021–2025 cycle, are being succeeded by a National Artificial Intelligence Strategy for 2026–2030 that is expected to play a central role in shaping AI governance. The plan outlines concrete goals for the responsible development of AI and includes initiatives such as the creation of legal evaluation tools for AI systems, the preparation of guidance to clarify intellectual property rights related to AI-generated content, and standardization efforts concerning the patentability of AI products, along with the potential establishment of a "Trusted AI" certification mechanism—all of which reflect Türkiye's commitment to proactive and structured AI regulation in the near term.

Contributors

Yücel Hamzaoğlu
Partner
yucel.hamzaoglu@hhklegal.com

Batu Kınıkoğlu
Partner
batu.kinikoglu@hhklegal.com

Melike Hamzaoğlu
Partner
melike.hamzaoglu@hhklegal.com

Nur Güler
Senior Associate
nur.guler@hhklegal.com

Osman Yücel
Managing Associate
osman.yucel@hhklegal.com

© 2026 Legalease Ltd