Legal 500
Country Comparative Guides 2024

Türkiye
TMT

Contributor

Hamzaoğlu
Hamzaoğlu Kınıkoğlu
Attorney Partnership

Yucel Hamzaoglu

Partner | yucel.hamzaoglu@hhklegal.com

Melike Hamzaoglu

Partner | melike.hamzaoglu@hhklegal.com

Batu Kinikoglu

Partner | batu.kinikoglu@hhklegal.com

This country-specific Q&A provides an overview of TMT laws and regulations applicable in Türkiye.

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

Türkiye: TMT

1. Is there a single regulatory regime that governs software?

In Türkiye, there is no single regulatory regime that exclusively governs software. Instead, software is regulated through a framework of various laws and regulations addressing aspects such as intellectual property rights, personal data protection, and sector-specific requirements. Key regulations include the Law on Intellectual and Artistic Works No. 5846 ("**IP Law**"), which provides intellectual property protection for software, and the Law on the Protection of Personal Data No. 6698 ("**LPPD**"), which governs the processing and protection of personal data. Sector-specific laws, such as the Law on the Regulation of Electronic Commerce No. 6563 ("**Law No. 6563**") and the Electronic Communications Law No. 5809 ("**Law No. 5809**"), also impact software operations in their respective fields. Additionally, in the healthcare sector, several regulations impose strict requirements on software to ensure the confidentiality, integrity, and security of health data. These regulations are enforced by various authorities, notably the Information and Communication Technologies Authority ("**ICTA**"), the Ministry of Health, and the Turkish Medicines and Medical Devices Agency ("**TMMDA**").

2. How are proprietary rights in software and associated materials protected?

As per the Turkish law, proprietary rights in software and associated materials are protected primarily under the Law on Intellectual and Artistic Works No. 5846 ("**IP Law**") which regulates intellectual property rights. Computer programs are classified as literary works under this law, affording software the protection of copyright. This classification grants software owners exclusive rights, including the rights to process, reproduce, distribute, publicly perform, and display the software. Infringement of these exclusive rights can result in civil liability. The software owner can file a lawsuit seeking remedies such as injunctions to stop the infringing activity, monetary damages for losses incurred, and compensation for any harm suffered. The IP Law also imposes criminal liability for certain types of infringement. Unauthorised reproduction, distribution, or alteration of software can result in criminal charges, leading to penalties such as fines or imprisonment.

While registration is not required for copyright to arise, software owners have the option to register their software if they wish. Additionally, the Industrial Property Law No. 6769 covers intellectual property rights beyond copyright, including patents, utility models, and industrial designs. While copyright protects the expression of software, patents may be sought for software-related inventions that meet the patentability criteria. It is important to note that a software program itself cannot be considered an invention and would be excluded from patentability if the patent or patent application is solely related to software. However, software that is part of a broader invention that meets the criteria for patentability can be protected under this law.

In practice, the use of software is typically governed by license agreements. These agreements establish guidelines and specify terms and conditions for software use, including provisions to safeguard the software's integrity and the owner's rights. Such provisions often address issues like unauthorised copying, distribution, modification, or reverse engineering. Violating these contractual obligations can result in liability for breach of contract, with potential legal consequences.

3. In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Under the Turkish intellectual property law, specifically the Law on Intellectual and Artistic Works No. 5846 ("**IP Law**"), the default position in the absence of any agreed contractual terms is that the proprietary rights in the newly created software are owned by the software developer, consultant, or the party that created the software. According to the IP Law, the author of a work, including software, is the original owner of the copyright.

However, in scenarios where the software is developed within the scope of an employment relationship, the situation is further clarified by the Regulation on Employee Inventions, Inventions Created in Higher Education Institutions and Inventions Resulting from Public Supported Projects. According to this regulation, for software created by an employee as part of their

employment duties, the employer typically holds the economic rights to the software, while the moral rights remain with the employee.

In the case of commissioned works, unless there is a specific agreement to the contrary, the copyright remains with the developer, and the customer is granted only the right to use the software as intended by the commission.

To avoid any potential disputes and ensure clarity regarding the ownership of proprietary rights in newly created software, it is essential for parties to explicitly define these terms in a written agreement. This ensures that the intended party holds the proprietary rights as per their contractual understanding.

4. Are there any specific laws that govern the harm / liability caused by Software / computer systems?

In Türkiye, there are no specific legislative measures exclusively governing the harm or liability resulting from the use of software or computer systems. However, general provisions in various laws and regulations can be applied to address such issues.

The Turkish Law of Obligations No. 6098 ("**Law No. 6098**") establishes general rules regarding liability for damages caused by acts or omissions. This framework is crucial in cases where software or computer systems cause harm, providing guidelines on determining liability and compensation for affected individuals or entities.

The Turkish Commercial Code ("**Law No. 6102**") plays a significant role, particularly in commercial transactions involving software. This code applies specifically to commercial activities related to software and computer systems.

The Law on Consumer Protection ("**Law No. 6502**") provides additional safeguards for consumers, addressing the responsibilities of manufacturers and sellers regarding defective software. Consumers have the right to repair, replacement, or refund in such cases.

The Law on the Regulation of Electronic Commerce No. 6563 ("**Law No. 6563**") imposes specific obligations on service providers and intermediaries, including those offering software. These obligations include information requirements, prohibitions on unfair commercial practices, and certain liability exemptions for intermediaries.

Sector-specific regulations may also apply, particularly in banking, finance, and healthcare, where additional rules govern the use and reliability of software systems. For instance, the Banking Regulation and Supervision Agency ("**BRSA**") regulates IT systems in financial institutions.

Lastly, the Law on the Protection of Personal Data No. 6698 ("**LPPD**") imposes obligations on entities processing personal data, including ensuring data security, with potential liabilities for breaches affecting data integrity and confidentiality.

5. To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

In addition to the extent covered by (4) above, the Turkish Penal Code No. 5237 contains specific provisions that address computer crimes and offenses. Turkish law provides criminal sanctions for unauthorised access to computer systems, tempering and destruction of data and other cybercrimes.

6. Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

In Türkiye, there are no specific technology laws governing the provision of software between vendors and customers, so general regulations typically apply. For instance, under the Law on Intellectual and Artistic Works No. 5846 ("**IP Law**"), licensing contracts must be in written form, either physical or electronic (with e-signature by licensed Turkish entities). However, in practice, clickthrough agreements are common, particularly in SaaS models. The Court of Cassation has evaluated this matter, and despite the rule under the IP Law, it has often upheld the validity of clickthrough agreements due to the nature of software provision.

Furthermore, while not specifically aimed at regulating licensing and SaaS models, two pieces of legislation significantly impact related businesses in Türkiye. First, currency protection laws require that fees for locally produced software be denominated in Turkish currency. Second, the Turkish Law of Obligations No. 6098 ("**Law No. 6098**") mandates that SaaS vendors offering specialized services requiring legal or regulatory approval cannot limit their liability.

Regarding cloud services, Türkiye does not have comprehensive, specific regulations governing cloud

services. However, the provisions of the Law on the Protection of Personal Data No. 6698 ("**LPPD**") concerning cross-border data transfers heavily impact cloud services hosted outside Türkiye. Detailed provisions of this legislation are covered in questions 17 to 20. Despite the absence of a general regulation, various sectors have their own regulations governing cloud services, imposing standards on data handling, data residency requirements, data localization, etc. For example, in the banking sector, the Regulation on the Information Systems of Banks and Electronic Banking Services permits limited use of cloud services but requires system localization. In payment systems, the Communiqué on Information Systems of Payment and Electronic Money Institutions mandates data localization and sets stringent conditions for shared cloud services, thereby limiting the involvement of conventional cloud providers. Additionally, Presidential Circular No. 2019/12 mandates that critical public sector data must be stored on systems controlled by local service providers.

These sectoral regulations illustrate the need for compliance with specific requirements depending on the industry, emphasizing data security, localization, and the usage of local service providers for critical data management.

7. Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

In Türkiye, software vendors often include clauses in contracts that limit their maximum financial liability to customers. It is uncommon to limit financial liability to foreseeable damages in Türkiye. The liability cap is typically tied to the contract's value, either as a specific amount or a percentage of the total fee. It is also common to see liability limited to the final court decision. While parties can agree on the liability cap, vendors cannot limit liability in cases of gross negligence. Additionally, as mentioned above on Q-6, under the Turkish Law of Obligations No. 6098 ("**Law No. 6098**"), if a software provider offers products/services requiring expertise and legal or regulatory approval, they cannot limit their liability.

8. Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

In practice, confidentiality breaches, data protection and data security breaches, IPR infringement claims, and regulatory fines are typically excluded from the liability cap. These issues are often subject to either unlimited liability or a separate, higher cap, depending on the negotiation power of the parties.

Loss of data is generally treated as indirect damage, and software vendors often state that they are not liable for indemnifying such damages. Given that personal data protection laws impose monetary fines of up to 9.463.213 Turkish Liras (for 2024) and considering the high risk of reputational damage (as penalty decisions and data breach notifications are published), customers often define a higher separate cap for these liabilities.

For customers in highly regulated sectors (like banking), where outsourced software use is also regulated, most of the areas of liability are typically excluded from any financial cap on the software vendor's liability.

Regarding wilful or deliberate breaches resulting from gross negligence, liability cannot be limited as per the Turkish Law of Obligations No. 6098 ("**Law No. 6098**"). Therefore, such cases are not generally subject to parties' contractual discretion.

9. Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

The escrow regime is not very common in Türkiye but is more frequently used in high-value license or SaaS relationships. Escrow arrangements provide assurance if the software vendor goes out of business, discontinues support, or breaches contractual obligations. Istanbul Technical University National Software Certification Center is the most used escrow provider in these cases.

10. Are there any export controls that apply to

software transactions?

There are certain export controls that apply to software transactions in Türkiye. These controls typically concern the export of specific software, technologies, or related goods to protect national security, prevent the proliferation of weapons of mass destruction, comply with international agreements, and adhere to trade sanctions or embargoes.

11. Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

In Türkiye, there is no specific technology law directly regulating IT outsourcing (information technology outsourcing), but various regulations may affect activities in this field. These regulations are generally considered within the framework of information security, data protection, intellectual property law, and commercial law:

- The Law on the Protection of Personal Data No. 6698 (**"LPPD"**) includes important regulations regarding the protection of personal data. Data processing and storage issues in IT outsourcing processes can be evaluated within the scope of this law.
- The Law on Intellectual and Artistic Works No. 5846 (**"IP Law"**) aims to protect software and digital content. The intellectual property rights of software and digital content developed in IT outsourcing projects can be protected by this law.
- The Turkish Commercial Code (**"Law No. 6102"**) also affects IT outsourcing activities by governing the operations of commercial entities and incorporating regulations concerning commercial contracts, liabilities, and transactions.
- The Turkish Law of Obligations No. 6098 (**"Law No. 6098"**) regulates the rights and responsibilities of the parties, the execution of obligations, liabilities, and procedures for addressing contract breaches, all of which are critical aspects of IT outsourcing agreements.

In addition to general regulations, there are also some sector-specific regulations. For example, there is a regulation concerning the procurement of support services related to the outsourcing of banks. This regulation is issued by the Banking Regulation and Supervision Agency (**"BRSA"**), and in accordance with this regulation, banks must adhere to specific rules when obtaining IT services from external sources. Another regulation is found in the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services in the Field of Payment Services by Payment Service Providers, which stipulates conditions for IT outsourcing services due to sectoral sensitivities in the management of information systems.

12. Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

In Türkiye, there are no specific legal regulations dedicated solely to the outsourcing of services to a third-party IT provider. Generally, the Labor Law No. 4857 protects the rights of individual employees. This law regulates various aspects of employment relationships and provides certain protections to employees in cases of business transfer or change of employer. In the event of transferring a service to a third-party IT outsourcing provider, the law aims to protect the rights of employees and maintain employment relationships. The acquiring party cannot terminate existing employment contracts solely based on the transfer itself. Employment contracts remain valid upon transfer of the workplace. However, after acquiring the workplace, the new employer may terminate employment contracts if there are operational reasons or restructuring needs, but such reasons must be genuine.

Additionally, for a period of two years from the date of transfer, the former employer remains jointly liable with the new employer towards the employees. Moreover, if the new employer terminates the employment without valid reason, the employee can claim job security and not only entitlement to compensation but also the right to request reinstatement under the same conditions and can also claim their rights from the former employer.

13. Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The primary legislation overseeing telecommunications networks and services is the Electronic Communications Law No. 5809 (**"Law No. 5809"**). This law encompasses the regulation of electronic communications services, the development and management of the necessary infrastructure, and the associated network systems. Additionally, it governs the production, importation, sale, construction, and operation of various electronic

communications equipment and systems.

In addition to the primary legislation, there are also several secondary regulations that support the Law No. 5809. The most notable of these secondary regulations include the following:

- Internet Domain Names Regulation,
- Regulation on Consumer Rights in the Electronic Communication Sector,
- Regulation on Quality of Service in the Electronic Communication Sector,
- Regulation on Network and Information Security in the Electronic Communications Sector,
- Regulation on the Registration of Devices with Electronic Identity Information,
- Regulation on Authorization for the Electronic Communication Sector,
- Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector,
- Regulation on the Process of Verifying the Identity of the Applicant in the Electronic Communication Sector,
- Radio Equipment Regulation,
- Regulation on Market Surveillance and Inspection of Radio and Telecommunication Terminal Equipment,
- Regulation on Security Certificate for Electronic Communication Devices,
- Regulation on Emergency Aid Call Services in the Electronic Communication Sector,
- Number Portability Regulation,
- Regulation on Electronic Communication Infrastructure and Information System,
- Information Technologies and Communication Authority Regulation on Administrative Sanctions,
- Communiqué on Procedures and Principles for Obtaining Electromagnetic Field Measurement Certificate,
- Communiqué on Obtaining Service Quality Criteria for 3N Mobile Communication Services,
- Communiqué on Notification of Devices Produced, Manufactured or Assembled in Türkiye,
- Communiqué on Obtaining Service Quality Measures for GSM Mobile Telephony Services,
- Communiqué on the Registration of Devices with Electronic Identity Information.

14. What are the principal standard development organisations governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

Although the Turkish Standards Institution ("**TSE**") was established to develop standards for various products, processes, and services in Türkiye, there is not a single main SSO that sets principles for all new connected technologies. Instead, multiple institutions govern the development of technical standards in their respective areas.

For mobile communications, the Information and Communication Technologies Authority ("**ICTA**") is the primary SSO responsible for setting principles. The ICTA was established to ensure that the regulation and supervision of the telecommunications sector are conducted by an independent administrative authority. Additionally, the ICTA mandates several standards related to connected and autonomous vehicles, focusing on mobile services, network usage, and connected services within these vehicles.

Examples of other institutions include the Ministry of Transport and Infrastructure, which serves as the main SSO for connected and autonomous vehicles, setting relevant principles and standards.

For digital health services, the Turkish Medicines and Medical Devices Agency ("**TMMDA**"), operating under the Ministry of Health, is the primary SSO responsible for setting principles and standards in this area.

15. How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

While there are no specific laws in Türkiye that exclusively regulate interoperability, various regulations and standards indirectly ensure that interoperability is maintained within the realm of electronic communications and connected technologies. Interoperability in mobile communications and connected technologies is primarily ensured through a combination of regulations and standards set by the Information and Communication Technologies Authority ("**ICTA**") and the Turkish Standards Institution ("**TSE**"). The ICTA mandates that network operators interconnect their networks and follow specific technical standards to maintain seamless communication services. Additionally, the TSE develops and publishes national standards which ensure that devices like Wi-Fi routers and Bluetooth equipment operate compatibly and without interference.

Moreover, Türkiye often aligns its regulations with the

European Union directives, which also promote interoperability. For instance, the Radio Equipment Directive and the General Data Protection Regulation ("**GDPR**") influence Turkish regulations by encouraging the development of interoperable systems.

16. When negotiating agreements which involve mobile communications or other connected technologies, are there any different considerations in respect of liabilities/warranties relating to standard essential patents (SEPs)?

At the moment, there is not a comprehensive law regulating SEPs in Türkiye. However, the need of support and regulation relating to SEPs has been recognised in the Twelfth Development Plan issued by the Strategy and Budget Presidency of Türkiye. Therefore, for the time being there are not specific nuances relating to liabilities/warranties of SEPs.

17. Which body(ies), if any, is/are responsible for data protection regulation?

The Turkish Data Protection Authority ("**TDPA**"), possessing administrative and financial autonomy as well as public legal personality, has been established to carry out the responsibilities assigned by the Law on the Protection of Personal Data No. 6698 ("**LPPD**") in Türkiye. The TDPA ensures the implementation of the LPPD and its related secondary legislation.

18. Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

The principal legislation governing data protection in Türkiye is the Law on the Protection of Personal Data No. 6698 ("**LPPD**"), dated April 7, 2016. This law, primarily based on EU Directive 95/46/EC, aims to protect the privacy of individuals by regulating the processing of personal data.

Similar to EU's the GDPR, the LPPD aims to protect personal privacy and to ensure data security by regulating the obligations and principles for individuals and organisations that process personal data. In addition to these goals, the LPPD is designed to stop the unrestricted and random gathering of personal data, prevent unauthorised access, and avoid its disclosure or misuse, which could result in violations of personal rights.

Several secondary regulations have been enacted to implement various aspects of the LPPD, including:

1. **Regulation on the Erasure, Destruction, and Anonymizing of Personal Data** (published in the Official Gazette on October 28, 2017, numbered 30224): Outlines the methods and principles for deleting, destroying, and anonymizing personal data.
2. **Regulation on the Registry of Data Controllers** (published in the Official Gazette on December 30, 2017, numbered 30286): Establishes the rules for the registration of data controllers.
3. **Communiqué on Procedures and Principles for Compliance with the Obligation to Inform** (published in the Official Gazette on March 10, 2018, numbered 30356): Sets the guidelines for data controllers to inform data subjects about data processing activities.
4. **Communiqué on the Principles and Procedures for Requests to Data Controllers** (published in the Official Gazette on March 10, 2018, numbered 30356): Outlines how data subjects can request information from data controllers.

Apart from these secondary regulations, the Turkish Data Protection Authority ("**TDPA**") regularly issues and publishes its decisions and principle decisions to clarify specific issues and provide guidance for data controllers and processors on how to implement such rules regarding data protection, including:

1. **Decision of the Data Protection Board on Adequate Measures for Processing Special Categories of Personal Data** (dated January 31, 2018, numbered 2018/10): Specifies the additional measures data controllers must take when processing special categories of personal data.
2. **Decision of the Data Protection Board on Personal Data Breach Notification Procedures and Principles** (dated January 24, 2019, numbered 2019/10): Specifies the procedure and the time period on how to notify the TDPA and data subjects in case of data breach, including the form to be used for the notification.

Alongside its decisions, the TDPA also releases various guidelines to offer guidance on different matters. The most notable ones include:

1. Guideline on Personal Data Security (Technical and Administrative Measures),
2. Guideline on Preparation of the Data Inventory,
3. Guideline on Implementation of the Obligation to Inform,

4. Guideline on Erasure, Destruction and Anonymisation of Personal Data,
5. Recommendations For Protecting Privacy in Mobile Applications,
6. Guide on Matters to Be Taken into Consideration When Processing Genetic Data,
7. Guide on Protection of Personal Data – Banking Sector Good Practices,
8. Guide on Cookie Practises,
9. Guide on the Right to be Forgotten (Evaluation of the Right to be Forgotten Specific to Search Engines).
10. Guide on the Issues to Be Considered When Processing Biometric Data,
11. Recommendations on the Protection of Personal Data in The Field of Artificial Intelligence.

The general purpose of these laws and regulations along with decisions and guidelines is to safeguard personal data, ensure data privacy, and establish clear guidelines for data processing activities within Türkiye. It is also important highlight here that one of the goals stated in Türkiye's Medium-Term Programme (2024-2026), published by the Turkish Presidential Strategy and Budget Directorate, is to ensure the alignment of data protection law with EU legislation, particularly the GDPR. In accordance with this goal, recent amendments were made to the LPPD. These amendments that are effective from June 1, 2024, address current needs, particularly in processing special categories of data and transferring personal data abroad.

In addition to those mentioned earlier, various regulations specify rules and requirements for processing personal data in sectors such as banking and finance, health, and electronic communications.

19. What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

In the event of a breach of applicable data protection laws in Türkiye, the maximum administrative fine foreseen for 2024 is 9,463,213 Turkish Liras. It is important to note that the number of administrative fines stated in the Law on the Protection of Personal Data No. 6698 (**"LPPD"**) is increased every year at the rate of revaluation.

20. Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

In Türkiye, technology contracts generally do not refer to external data protection regimes like the EU GDPR or CCPA when there is no clear international element involved. When both parties are established in Türkiye, these contracts almost exclusively refer to the Law on the Protection of Personal Data No. 6698 (**"LPPD"**). However, when one of the parties is established outside of Türkiye, references to different data protection regimes, especially EU GDPR, can be seen.

21. Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Although there is no body directly responsible for the regulation of artificial intelligence (**"AI"**) in Türkiye, it is important to note here that Türkiye's approach is currently evolving to AI governance. Following the establishment of the Department of Big Data and AI Applications within the by the Digital Transformation Office of The Presidency of The Republic of Türkiye, a crucial initiative was the formulation of a national strategy aimed at regulating interactions with AI. Therefore, it is envisioned that in the future there will be a specialized and singular authority, akin to the Turkish Data Protection Authority (**"TDPA"**), solely responsible for AI regulations. Moreover, specific governmental organizations and administrative authorities may regulate particular issues that fall within their authorization. For example, the Information and Communication Technologies Authority (**"ICTA"**) can establish rules regarding the use of AI in the telecommunications sector, while the TDPA can oversee how AI processes personal data.

22. Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

Currently, Türkiye lacks a comprehensive law specifically governing and focusing the deployment and utilization of artificial intelligence, like the EU's AI Act. Given that AI is swiftly reshaping numerous sectors worldwide, Türkiye is also witnessing significant transformations. Consequently, there is growing momentum towards regulating AI systems. This momentum has recently led to a proposal for AI regulation. This proposal's objectives include safeguarding personal data, preventing privacy infringements, and establishing a regulatory framework for the development and deployment of AI systems. However, the proposal is criticized of being quite brief and not elaborated in detail. Therefore, it is expected that

there will be other initiatives to regulate AI, like the EU's AI Act, in the future.

Additionally, some references to the use of AI technologies, such as deep fakes, can be seen in some sectoral legislations. For instance, as per the Communiqué on Remote Identification Methods to Be Used By Intermediary Institutions and Portfolio Management Companies and on the Establishment of Contractual Relationships In Electronic Environment, intermediary institutions or portfolio management companies must take additional measures to prevent risks related to deepfake technology.

Additionally, governmental organizations and administrative authorities have developed specific strategies and guidelines pertaining to AI:

- The National Artificial Intelligence Strategy 2021-2025, outlined by the Digital Transformation Office of The Presidency of The Republic of Türkiye, sets forth measures aimed at coordinating Türkiye's AI efforts and establishing governance structures for their implementation. This strategy focuses on enhancing domestic AI development, integrating AI into key sectors to boost productivity, transforming the workforce to effectively utilize AI, and utilizing AI for public service advancements. The overarching goal is to foster a dynamic and sustainable AI ecosystem that enhances Türkiye's global competitiveness. To achieve this, the AI Strategy prioritizes training AI experts, promoting employment, supporting research and innovation, ensuring access to quality data and infrastructure, and implementing regulatory frameworks for socioeconomic adaptation.
- Within the scope of processing personal data by AI systems, the Turkish Data Protection Authority ("**TDPA**") has also issued a guideline, namely the Recommendations on the Protection of Personal Data in Artificial Intelligence, which outlines its stance and provide general guidance on safeguarding personal data in the use of AI-driven technologies. These recommendations are intended for developers, manufacturers, service providers, and decision-makers in the AI sector.

23. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

In Türkiye, there are currently no specific legal provisions governing the deployment and utilization of Large Language Models ("**LLMs**") and/or generative AI ("**GenAI**"). However, the Council of Higher Education ("**CoHE**") has issued guidance regarding the use of GenAI in scientific research conducted by higher education institutions.

The Ethical Guidelines on the Productive Use of Artificial Intelligence in Scientific Research and Publication Activities of Higher Education Institutions, published by the CoHE in 2024, outline principles for the ethical and effective utilization of LLMs and GenAI in scientific research and related activities. These guidelines serve to establish standards and foundational principles for the responsible deployment of LLMs and GenAI in academic settings, ensuring their ethical use and promoting integrity in research practices.

24. Do technology contracts in your jurisdiction typically contain either mandatory (e.g mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

No, currently in Türkiye, technology contracts generally do not include mandatory or recommended provisions addressing AI risks. However, given Türkiye's developing stance on AI regulation, this may change in the future.

25. Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

No, software or technology contracts in Türkiye typically do not incorporate provisions addressing copyright or other intellectual property rights, or ownership of outputs in relation to the use of AI systems. However, although there have been no legislative initiatives or court rulings in this area so far, given the widespread use of AI applications, it is inevitable that there will be legal developments in the coming years. These developments are likely to influence and shape provisions concerning this topic.

26. What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

In Türkiye, there is currently no specific legislation

dedicated solely to regulating blockchain technology and digital assets. However, crypto assets and crypto asset service providers ("**CASPs**") are regulated through amendments to the Capital Markets Law ("**CML**"). These amendments cover the issuance of crypto assets, the establishment and commencement of operations by CASPs, and the requirement to obtain permits from the Capital Markets Board ("**CMB**"). They also specify the conditions that partners of CASPs must meet, the obligations these providers must adhere to during their operations, the activities of platforms, and the transactions Turkish residents can perform on these platforms, including trading and transferring crypto assets.

Additionally, the amendments address crypto asset custody services, the safeguarding of clients' cash assets, the prohibition of market disruptive actions, auditing, liability of CASPs for damages, seizure of customers' crypto assets, dispute resolution, administrative penalties, operational measures, fees payable to the CMB, transitional and compliance processes, and penal provisions. The CMB has been empowered to regulate CASPs, granting it authority to issue specific and general decisions, enforce measures, and impose sanctions.

CASPs are required to obtain a license from the CMB before they can be established and commence operations. The CMB is also responsible for detailing regulations concerning the organizational structures, capital adequacy, and technological infrastructures of CASPs, among other aspects. Any contractual terms that absolve CASPs from their responsibilities towards clients are deemed void. Legal frameworks have been established with the legislative amendments regarding the seizure of crypto assets owned by customers, ensuring their enforceability by CASPs. CASPs are exclusively subjected to the stipulations outlined in the legislative amendments and are not governed by the remaining provisions of the CML.

Additionally, the Regulation on Measures for the Prevention of Laundering Proceeds of Crime and Financing of Terrorism includes CASPs among the obliged parties. Consequently, CASPs are now required to fulfill fundamental obligations such as know your customer standards and reporting suspicious transactions as part of efforts to prevent money laundering and terrorism financing.

27. Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

There is no specific regulation regarding search engines in Türkiye. However, certain aspects of the Law No. 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts ("**Internet Law**"), such as the provisions regarding hosting providers, may apply.

Definition of a "hosting provider" according to the Internet Law is as follows; real persons or legal entities that provide or run systems to contain services and content, and as stated above, marketplaces are considered hosting providers.

In this regard, a hosting provider, therefore a search engine, has the following obligations:

- to remove the illegal content from broadcast, provided that it has been informed about the illegal content,
- to store the traffic information in relation to the provided hosting services for a period not less than a year and not more than two years,
- to make hosting provider notification.

In addition to this, individuals whose personal rights have been infringed by online content may ask a judge to issue an order compelling search engines not to associate their names with internet addresses. In the same direction the right to be forgotten has been recognized by the Supreme Court and the judicial decisions in Türkiye. In line with these decisions the Turkish Data Protection Authority published a public announcement and the Guide on the Right to be Forgotten (Evaluation of the Right to be Forgotten Specific to Search Engines) on the matter which referred to the Turkish Constitution, European legislation and decisions and published criteria for Turkish citizens to exercise this right. At the same time, the Advertising Board may also conduct investigations if there are complaints regarding unfair commercial practices and may impose access restrictions as well.

In terms of market places the regulations are mainly stipulated in the Law on the Regulation of Electronic Commerce No. 6563 ("**Law No. 6563**") and the Regulation on Electronic Commerce Intermediary Service Providers and Electronic Commerce Service Providers ("**E-Commerce Regulation**"):

- The Law No. 6563 regulates mainly the obligations of the marketplaces, sellers and providers, and the relations between marketplaces-sellers and providers and customers. The Law No. 6563 also defines electronic commerce intermediary service providers

("**EISPs**") and electronic commerce service providers ("**ESPs**"), economic integrity and net trading volume. There are also specific rules on unfair commercial practices, advertisement rules and commercial communication requirements regarding e-commerce in the Law No. 6563.
- E-Commerce Regulation refers to the Law No. 6563 on several obligations of the EISPs ESPs. However, the E-Commerce Regulation is more detailed since it broadens the scope of the obligations of EISPs and ESPs (some of which is depends on the net trading volume and economic volume), regulates the relation between EISPs and ESPs, regulates the supervisory authority of the Ministry of Trade.

As of, 01/01/2024 the adjustment process for EISPs to comply with the prohibitions regarding sale of goods bearing the trademark or trademark usage right of the said EISP or persons with whom it is in economic integrity with, in electronic commerce marketplaces where it provides intermediary services has ended. Therefore, any EISPs are subject to sanctions in case of non-compliance.

At the same time there are specific provisions regarding promotion and access on online search engines in the E-Commerce Regulation which is binding for EISPs and ESPs. This provision refers to E-Commerce Information Platform (in Turkish "**ETBIS**") and economic integrity concept for imposing restrictions on marketing and promotion activities carried out by EISPs and ESPs.

In addition, there are several secondary regulations governing e-commerce, including rules on distance sales, pricing, unfair terms in consumer contracts, advertising, unfair commercial practices, the E-Commerce Information Platform, trust stamps in e-commerce, and commercial communication. At the same time, the Law No. 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts, the Law on Consumer Protection, the Law on the Protection of Personal Data No. 6698, the Law on Bank Cards and Credit Cards, secondary legislation of these are laws and the decisions of the Advertisement Board are applicable to e-commerce activities to the extend where it is relevant.

28. Please summarise the principal laws (present or impending), if any, that govern social media, including a brief explanation of the general purpose of those laws?

In Türkiye, social media is mainly regulated by the Law No. 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts ("**Internet Law**") as well as some secondary legislation. The Internet Law defines social network provider as *"natural persons or legal entities that enable users to create, display or share content such as texts, image, voice, location, over the internet for purposes of social interaction"* and lay down some obligations for social network providers having more than one million daily access from Türkiye:

- Appointment of local representative for social network providers having more than one million daily access from Türkiye, and notifying the representative to Information and Communication Technologies Authority ("**ICTA**"),
- Removing content or blocking access to content, when necessary (such as violation of personal rights or privacy),
- Providing necessary information upon request of public institutions and/or judicial authorities, and
- Act in compliance with decisions of the ICTA.

Additionally, the Procedures and Principles on Social Network Providers published by the ICTA also lay down the details of aforementioned obligations such as appointment of representative, reporting, hosting of data in Türkiye, responding applications, informing the judicial authorities, protecting users' rights and procedures to ensure compliance in detail.

Additionally, in cases where the social network provider is a qualified as a hosting provider, the social network provider is obliged to act in accordance with the provisions of the Regulation on the Procedures and Principles Regarding the Regulation of Broadcasts Made on the Internet Environment and the Regulation on the Procedures and Principles Regarding the Issuance of Activity Certificate to Access Providers and Hosting Providers by The Telecommunication Authority.

29. What are your top 3 predictions for significant developments in technology law in the next 3 years?

Considering the global legal, and technological developments, following are the top 3 predictions for significant developments in technology law in Türkiye, for the next 3 years:

- **Further harmonisation of the Law on the Protection of Personal Data No. 6698** ("**LPPD**") **with the GDPR:** Ever since the publishing and entering into the force, the harmonisation of LPPD with the GDPR has been a crucial topic. As mentioned above on Question 18, a

significant amendment as part of these efforts has been made on the related provisions of the LPPD concerning transfer of personal data abroad. Within the scope of these amendments, new methods of transferring personal data abroad similar to the GDPR has been introduced, and the legal regime of transfer has been drastically changed. Following these amendments, it is expected for additional changes to be introduced on topics such as, pseudonymised data, sanctions, automated decision making and profiling, and to further harmonise LPPD with the GDPR.

- **Secondary legislation on the OTT Service Providers:** Another development concerning the technology law is establishment of the secondary legislation on the OTT Service Providers. In 2022, an amendment was introduced on the Electronic Communications Law No. 5809 (**"Law No. 5809"**), and OTT service providers were regulated within the scope of the Law No. 5809. With the amendment on the Law No. 5809, many obligations were introduced on the OTT service providers such as *authorisation* requirement under which the OTT Service providers should obtain a license to operate, and the Information and Communication Technologies Authority (**"ICTA"**) was authorised to regulate details of the obligations of OTT service providers. Nevertheless, since 2022, the ICTA has not published a secondary legislation regarding obligations of the OTT service providers. For the time being, it is expected for the ICTA to publish related secondary legislation in due time and establish the legal requirements for OTT service providers.
- **Regulation of AI:** With AI being a global phenomenon on both legal and technological landscapes, it is expected for Türkiye to introduce a local set of rules governing the complex technology of AI. As mentioned above on Question 22, there is a recent proposal regarding a draft AI regulation that aims to ensure the safe, ethical, and fair use of artificial intelligence technologies, to guarantee the protection of personal data, to prevent the violation of privacy rights, and to establish a regulatory framework for the development and use of artificial intelligence systems. The proposal is quite brief, and it is expected for the proposal to be renewed and detailed in the future. With regards to the AI Strategy, a legal framework harmonised with the EU AI Act is expected to be on the agenda in the near future.

30. Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Currently in Türkiye, it is not common for the technology contracts to include provisions regarding sustainability / net-zero obligations or other similar environmental commitments. Nevertheless, as the regulatory landscape concerning environmental sustainability / net-zero obligations deepen, it is anticipated for the technology contracts to include provisions regarding sustainability / net-zero obligations or other similar environmental commitments.

Contributors

Yucel Hamzaoglu
Partner
yucel.hamzaoglu@hhklegal.com

Melike Hamzaoglu
Partner
melike.hamzaoglu@hhklegal.com

Batu Kinikoglu
Partner
batu.kinikoglu@hhklegal.com