Digital Business 2022

Contributing editor
Samuel G Kramer

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2000
Eighteenth edition
ISBN 978-1-83862-652-5

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Digital Business
2022

Contributing editor
Samuel G Kramer
Baker & McKenzie

Lexology Getting The Deal Through is delighted to publish the eighteenth edition of *Digital Business*, formerly *e-Commerce*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Turkey and the United States.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editor, Samuel Kramer of Baker & McKenzie LLP, for his assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
August 2021

Contents

Turkey

Sinem Mermer*

Boden Law

LEGAL AND REGULATORY FRAMEWORK

Government approach

1 | How can the government's attitude and approach to internet issues best be described?

Due to its candidate status, Turkey has enacted regulations following the footsteps of the EU regarding many aspects of digital issues so far. In that regard, Turkish legislation reflects the main EU principles especially in consumer protection and personal data protection. The Human Rights Action Plan published in April 2021 states that the personal data protection legislation will be aligned with the GDPR standards in the following year. The Action Plan also indicates that the government aims to adopt digital transformation in public administration. Amendments to the Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications were introduced taking the example of Germany's Network Enforcement Act, or NetzDG. Regulation of cryptocurrencies has been a priority for the government due to increased public attention to these assets during the pandemic, the high risks these transactions pose for most users, and fraud allegations in this area. Turkey has also adopted a preservationist approach towards cross-border data transfers and relevant legislation contains provisions encouraging or obligating companies operating in digital sectors to store domestic users' data in Turkey.

Legislation

2 | What legislation governs business on the internet?

The primary legislation applicable to online business is as follows:

- Law No. 6563 on Regulating Electronic Commerce, which sets the main framework of electronic commerce containing provisions on electronic commercial communications, service providers and intermediary service providers, their obligations to inform, contracts concluded through electronic communication tools, and sanctions.
- Law No. 6502 on Consumer Protection, which mainly governs all aspects of transactions concluded online or offline with consumers on various subjects, dispute resolution mechanisms in B2C transactions and advertisements. Distance contracts in B2C relations are regulated in the secondary legislation.
- Law No. 6698 on Personal Data Protection, which regulates personal data processing principles, rights of data subjects, and obligations of data controllers and processors.
- Law No. 5651 on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications, which governs the obligations and liabilities of content providers, hosting providers, access providers and social network providers.
- Law No. 5809 on Electronic Communications, which regulates consumer rights, competition in the electronic communications sector, obligations of operators, investments and developments in communications infrastructure.
- Law No. 6493 on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions.
- Law No. 5070 on Electronic Signatures, which covers the legal and technical aspects of e-signatures.

There is various secondary legislation (regulations, communiques and guidelines) detailing the application of the primary regulations. Other main legislation on customs, intellectual property, product liability, competition and tax, inter alia, is applicable in most cases to companies doing business online. Moreover, depending on the sector such companies are operating in, specific legislation may be applicable, such as those regulating the banking, energy or insurance sectors, for example.

Regulatory bodies

3 | Which regulatory bodies are responsible for the regulation of e-commerce, data protection and internet access tariffs and charges?

The responsible regulatory bodies differ depending on the subject. The Ministry of Trade is authorised to take any measures and carry out inspections with regard to e-commerce. The Personal Data Protection Authority is responsible for the regulation of matters related to personal data protection. The Turkish Competition Authority may also conduct investigations that have both competition and data protection aspects. The Information and Communication Technologies Authority has the power to impose cost-based tariffs on operators. The Banking Regulation and Supervision Agency and the Central Bank are authorised to regulate fintech operations, crypto assets and digital coins.

Jurisdiction

4 | What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions or disputes in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Law No. 5718 on International Private and Procedure (IPPL) regulates the jurisdiction of Turkish courts in disputes with foreign elements. Accordingly, the parties have the freedom to determine the jurisdiction for internet-related transactions or disputes. In the absence of such agreement, Turkish courts have jurisdiction when the defendant has an ordinary residence in Turkey, or the contract's characteristic obligation is performed in Turkey.

The IPPL set forth mandatory rules on the jurisdiction of consumer contracts which is defined as contracts lacking a professional or commercial aim but concluded to acquire goods, services or credit without making any distinction whether the contract is concluded online or offline. At the customer's choice, Turkish courts in places where the

consumer's domicile or ordinary residence or the other party's domicile or ordinary residence is located are competent. On the other hand, Turkish courts at the consumer's residence have jurisdiction if any claims are brought against the consumer.

Establishing a business

5 What regulatory and procedural requirements govern the establishment of digital businesses in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

Generally, there are no distinctive regulatory and procedural requirements for the establishment of digital businesses; the Turkish Commercial Code relevant to brick-and-mortar businesses would apply. E-commerce rules require service providers and intermediary service providers to register with the E-commerce Information System (ETBIS) before initiating their operations.

Additionally, companies to establish an online business or to operate in Turkey should:

- register their domain names and trademarks;
- obtain any necessary permits, licences and authorisations (for instance, payment and e-money institutions, shared e-scooter operators, online media service providers);
- ensure compliance with personal data protection rules, e-commerce rules, and rules applicable to content and hosting providers (especially information obligations); and
- social media service providers located abroad with over 1 million daily Turkish user access must appoint a representative.

CONTRACTING ON THE INTERNET

Contract formation

6 Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

Electronically forming and concluding contracts is possible in Turkey and subject to the same requirements of concluding traditional contracts regulated under the Turkish Code of Obligations No. 6098. As a rule, parties may enter into contracts for any subject unless the subject matter of the contract violates the mandatory rules of laws, morality, public order, personal rights, or if the subject of the contract is impossible. Any contracts violating this rule are null and void. Not all contracts are eligible to be concluded electronically, and there are certain form requirements stipulated in different sets of laws.

To conclude a contract via electronic means, there must be an offer and a corresponding acceptance. Offers presented on websites can be categorised as either offer or an invitation to an offer depending on whether the offeror presents the price of services or goods on its website or sends electronic catalogues or price lists to the offeree. However, article 8(2) of the Turkish Code of Obligations provides that the display of merchandise with an indication of its price or sending a tariff, price list, and so forth constitute an offer unless it is understood clearly and easily otherwise. Therefore, if the seller or provider has indicated all the objective essential elements of the contract online, there is a valid offer and the contract is concluded by the consumer (usually) with a click on the acceptance button (click-wrap contracts). It should be noted here that any deviation from the offer in acceptance declaration would not be evaluated as a meeting of the minds; thus, no contract would be concluded.

Yet, there are other specific obligations for forming and concluding contracts electronically arising from regulations on electronic commerce, such as the Law on Regulating Electronic Commerce and the Consumer Protection Law. For example, service providers (ie, legal or natural persons engaged in electronic commercial activities), as well as intermediary service providers (ie, legal or natural persons providing an electronic commerce platform for third-party economic and commercial activities), are obliged to provide certain information to customers before concluding contracts electronically, as per the named regulations. Further, the Consumer Protection Law sets forth that electronic contracts concluded with consumers shall entail certain rights in favour of consumers such as the consumer's right of withdrawal from the contract within 15 days following the delivery of the goods or services. It should be emphasised that other liabilities may arise depending on the product or service presented online that would fall into the scope of other specific regulations such as financial services, timeshare vacation, and long-term holiday products, package holidays, and package tours.

Applicable laws

7 Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

At the outset, the general provisions of the Turkish Code of Obligations regarding contracts apply to contracts concluded on the internet. In addition, the Law on Regulating Electronic Commerce and the Consumer Protection Law set the framework of obligations and duties arising when contracting on the internet. The Law on Regulating Electronic Commerce and its sub-regulations impose specific duties and obligations on service providers (ie, legal or natural persons engaged in electronic commercial activities) and intermediary service providers (ie, legal or natural persons providing an electronic commerce platform for third-party economic and commercial activities). Further, depending on the product or service offered online several other regulations become applicable, such as the Regulation on Distance Contracts and the Regulation on Distance Contracts in Financial Services, both of which apply to B2C transactions. On the other hand, in B2B transactions, service providers may opt not to fulfil their obligation to inform as per article 3(3) of the Law on Regulating Electronic Commerce. Similarly, duties and obligations applicable to online orders (confirmation of order, technical means for identifying and correcting input errors before placing the order) are not mandatory in B2B sales.

Electronic signatures

8 How does the law recognise or define digital or e-signatures?

Turkey enacted the Electronic Signatures Law No. 5070 in 2004, which is heavily influenced by Directive 1999/43/EC of the EU. The relevant articles of the Turkish Code of Obligations (article 14 regarding the form requirement and article 15 regarding signature) were aligned at the time of the introduction of e-signatures to Turkish law. The Regulation on the Principles and Procedures regarding the Application of the Electronic Signatures Law and the Communiqué on Technical Criteria and Procedure regarding Electronic Signatures expand on the Electronic Signatures Law. The Information and Communication Technologies Authority (ICTA) is authorised to enforce the Electronic Signatures Law, to inspect electronic certificate service providers, and to regulate the application of the Electronic Signatures Law.

Article 3(b) of the Electronic Signatures Law defines an electronic signature as 'electronic data that is joined or linked logically to another electronic data and which is used to authenticate an identity'. The Electronic Signatures Law also elaborates on secure electronic signatures in detail. Secure electronic signatures shall have a qualified

electronic certificate as per article 4 of the Electronic Signatures Law. The ICTA determines and publishes the list of the institutions with the qualified electronic certificate on its website. On the other hand, only the definition of simple electronic signatures is included in the Law.

Following the amendment in Communiqué on Technical Criteria and Procedure regarding Electronic Signatures in 2008, mobile signatures have also been recognised as electronic signatures. A mobile signature is an electronic signature that is attached with the use of a mobile device (a SIM card). Although the Electronic Signatures Law does not specifically refer to mobile signatures, if a qualified electronic certificate service provider provides a mobile electronic signature, that mobile signature has the same legal effect as a secure electronic signature.

As per article 5 of Electronic Signatures Law and article 15 of the Turkish Code of Obligations, secure electronic signatures have the same legal effect (ie, are equal to) wet ink or handwritten signatures. However, contracts that are required to be formed officially and letters of guarantee excluding banks' letters of guarantee shall not be signed via electronic signatures. Further, the legislator differentiates the evidentiary weight of electronically signed documents. That said, documents bearing secure electronic signatures are qualified as promissory notes, and conclusive evidence as per article 205 of the Civil Procedure Law No. 6100. Other documents bearing simple electronic signatures may only qualify as prima facie evidence. Nevertheless, parties can conclude an evidential contract as per article 193 of the Civil Procedure Law and agree that the documents with a simple electronic signature will be regarded as conclusive evidence in case of a dispute.

Data retention

9 Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

Service providers and intermediary service providers shall store the electronic logs regarding electronic commerce transactions for three years following the transaction date and submit these logs to the Ministry of Trade upon request.

Breach

10 Are any special remedies available for the breach of electronic contracts?

In B2B contracts, the remedies specified in the Turkish Code of Obligations (specific performance, damages, termination) will be available. In B2C contracts, consumers have the right of withdrawal without giving any grounds and paying any fines which can be exercised within 14 days following the conclusion of the contract or delivery of the goods. If the seller fails to fulfil its obligation to provide information to consumers, the right of withdrawal can be extended to one year. In addition to the right of withdrawal, consumers have the right to terminate the contract if the seller fails to deliver the goods within 30 days following the receipt of order by the supplier or provider.

SECURITY

Security measures

11 What measures must be taken by companies or ISPs to guarantee the security of internet transactions? Is encryption mandatory?

There is no specific legislation dedicated to explaining the security measures that must be taken in internet transactions. If the transaction has an aspect of personal data processing, the Personal Data Protection Law (PDPL), which has a broad scope of application, would apply. Companies and organisations involved in personal data processing must implement appropriate technical and organisational measures to safeguard personal data. The Guidelines on Technical and Organisational Measures published by the Personal Data Protection Authority contain information on measures to be taken by data controllers if they store personal data on external cloud computing systems. Among the measures that the controllers shall take, encryption of personal data for its storage and use of different keys for each cloud computing system are mentioned.

In regulated sectors such as banking, insurance and telecommunications, inter alia, it is required to develop network security policies, train employees and maintain backup servers. Additionally, the Turkish Presidency's Digital Transformation Office published a very detailed Guide on Information and Communication Security in July 2020, although compliance with it is not mandatory. The Guide contains detailed examples and explanations on technical measures in order to determine a minimum level of security that ensures confidentiality, integrity and accessibility of data. It also refers to specific security measures to be taken by organisations operating in particular industries such as energy and financial services.

Government intervention and certification authorities

12 As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

Companies or operators do not have a specific obligation to decrypt communications or hand out private keys to the authorities. However, as per the Regulation on Detecting, Wiretapping, Evaluation of Signal Data and Recording the Communications (the Wiretapping Regulation), the National Intelligence Service or Intelligence Offices of Security General Directorate or Gendarme General Command have the authority to give written orders to wiretap communications for prosecution of specific crimes such as espionage, crimes against the constitutional integrity or national security. Upon written orders, the Information and Communications Technologies Authority's (ICTA) respective department may require communications service providers to integrate the tools, infrastructure, and other means to decrypt the concerned data.

Additionally, the Regulation on Principle and Procedures for Coded or Encrypted Communications of Public Entities and Natural or Legal Persons requires the manufacturers (or importers) to request approval from the ICTA by submitting the used cryptographic algorithms and keys as well as software or hardware enabling decryption, if need be, before making such services or products available in Turkey. Whether or not approval is mandatory will be determined based on the technical characteristics of the encryption communications. In case of violation of these rules, judicial fines may be imposed as per the Electronic Communications Law.

The Electronic Signatures Law regulates electronic certificate service providers (ECSPs). ECSPs are required to notify the ICTA prior to starting their operations. Also, they must use secure products and systems, deliver services reliably and implement any measures to prevent certification reproduction and manipulation. The Electronic Signatures Law states that ECSPs are liable to certificate holders according to general provisions and to third parties according to electronic signature regulations and they shall insure their liabilities. Any non-liability clauses against third parties and certificate holders are invalid except for the limitations of liability relating to electronic certifications' use and material scope.

Electronic payments

13 Are there any rules, restrictions or other relevant considerations regarding the use of electronic payment systems in your jurisdiction?

The Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions is the framework legislation on the use of electronic payment systems and payment service providers. The Law on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions was amended in line with the Payment Services Directive 2 of the EU in 2019. Only banks, electronic money institutions, payment institutions, and the Postal and Telegraph Corporation qualify as payment service providers. The Central Bank of the Republic of Turkey is authorised to regulate and audit payment service providers. Payment institutions must meet capital requirements stated in the Law (except for account information service providers) and obtain an operating licence from the Central Bank. In 2020, the Union of Turkish Payment Services and Electronic Money Institution was founded with Presidential Decision No. 2678. Accordingly, all relevant entities shall become a member of the Union within a month following the issuance of an operating licence.

With regard to cryptocurrencies, payment service providers are prohibited from developing business models that use crypto assets directly or indirectly for the provision of payment services and electronic money issuance, and from providing any services related to such business models as per the Regulation on Prohibiting the Use of Crypto Assets in Payments which was enacted in early 2021. According to the same Regulation, payment institutions cannot act as an intermediary for fund transfers from or to platforms that buy, sell, deposit, transfer or export crypto assets.

14 Are there any rules or restrictions on the use of digital currencies?

Crypto assets have been regulated since April 2021. The Regulation on Prohibiting the Use of Crypto Assets in Payments which was published on 16 April 2021 defines crypto assets not as a medium of exchange but as intangible assets that are formed virtually using distributed ledger technology or similar technology and distributed over digital networks. It is explicitly stated in the Regulation that crypto assets do not qualify as fiat currency, fiduciary money, electronic money, payment instruments, securities, or other capital market instruments. As per the Regulation, the direct or indirect use of crypto assets in payments or provision of payment services and electronic currency exports are prohibited as of 30 April 2021. Payment service providers are banned from developing any business model that falls within the said prohibition scope and to provide services according to such business models. Further, payment and electronic money institutions are prohibited from acting as an intermediary for transferring funds to and from platforms that buy-sell, deposit, transfer, or export crypto assets. In a press release published on the same day as the Regulation, the Central Bank listed the risks stemming from the use of crypto assets such as their volatility and their potential use in illegal activities due to its anonymous nature. It further stated that their use may result in irrecoverable damages of parties to crypto-asset transactions and may undermine the trust in methods and instruments currently used in payments. All in all, the prohibitions introduced by the Central Bank can be categorised as a payment ban rather than an overall ban on investing in crypto assets.

Additionally, the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism was amended on 1 May 2021 to hold crypto asset service providers liable for obligations as per the anti-money laundering regulations. Crypto asset service providers must abide by the measures introduced by the Financial Crimes Investigation Board (MASAK) such as customer identification (KYC) obligations and transaction limits, among others. MASAK may impose administrative fines for violations of KYC obligations, obligation to provide continuous information and notification of suspicious transactions.

Following the global trend, the Central Bank of the Republic of Turkey announced that it had initiated the development of a central bank digital currency (CBDC), and the Central Bank is expected to create a technical and regulatory framework for the CBDC by 31 December 2021 as announced in the Economic Reforms Action Plan.

DOMAIN NAMES

Registration procedures

15 What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

For an extended period of time, 'Nic.tr Administration' within Middle East Technical University had been responsible registering ccTLD '.tr'. Later, the Regulation on Internet Domain Names opened the market to different registrars, prescribed the establishment of a central '.tr network information system' (TRABIS), and authorised the Information and Communication Technologies Authority (ICTA) to enact regulations in this field. Although 'Nic.tr Administration' had transferred its domain name allocation authority to the ICTA in 2018 and 'Nic.tr' stopped accepting new applications and renewal requests as of 23 March 2020; the TRABIS system has not initiated its operations at the time of writing. The ICTA has announced that TRABIS will be fully established by December 2022. Currently, registration operators accept applications and 'Nic.tr' continues to operate as a registration operator. Once the TRABIS system starts operating, all domain name owners must select a new registration organisation operating under TRABIS and transfer their domain names. New domain name applicants will submit their requests to one of the registration organisations, and the organisation will process the request on TRABIS.

The relevant regulation adopts two methods for domain name allocations. The 'first come, first serve' rule applies to undocumented domain name applications. '.com.tr', '.net.tr' and '.org.tr' will be open to undocumented applications once the TRABIS system starts its operations. A connection between the applicant and the domain name is not required with undocumented applications; therefore, natural persons and legal entities located abroad can submit undocumented domain name applications. On the other hand, certain domain name applications require documentation and approval by the authorities. For instance, the allocation of the domain name '.av.tr' has been limited to the use of lawyers and solicitors who are registered to the Turkish Bar Union, law offices, and lawyer partnerships.

The 'Nic.tr' Rules require trademark ownership to register trademarks as domain names with '.com.tr'. The Regulation does not have such a criterion; however, the Communique on Domain Names states that trademark owners will have priority with first-time domain name registrations. Although the 'Nic.tr' Rules set an example and sector practice in this field, the ICTA is authorised to decide on the required documents and bring additional requirements. As per the Regulation, a domain name will be allocated to a natural person or a legal entity for five years at the longest. Once this period is exhausted, domain name owners can apply for a renewal.

Rights

16 | Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

Domain names do not confer any additional rights. However, the domain name owner may allege unfair competition in a dispute as per the Turkish Commercial Code where there is an identical or similar domain name or a subsequent trademark.

Trademark ownership

17 | Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

If the trademark owner does not exploit the priority granted by the Communique on Domain Names with first-time domain name allocations, the registrars are not obliged to cross-check whether the domain name infringes a registered trademark. Yet, the ownership of a trademark would assist in challenging a domain name. The complainants may allege that the disputed domain name is identical or similar to their trademark, business title, or other; the party who registered the domain name has no rights or legal connections in respect of the domain name and the domain name has been registered or used in bad faith. Particular use of domain names is assumed to be bad faith, for instance, when the domain name owner registered the trademark in order to prevent the trademark owner's registration or when the domain name is registered to harm competitors' operations or activities.

Dispute resolution

18 | How are domain name disputes resolved in your jurisdiction?

Turkey has introduced an alternative dispute resolution mechanism similar to the Uniform Domain-Name Dispute-Resolution Policy (UDRP) for '.com.tr' domains as per the Regulation on Internet Domain Names. In this regard, parties can apply to dispute resolution service providers, or they can always seek remedies in judicial courts. Considering legislation, precedents and case law, the arbitral tribunal within the service providers can render a decision on (1) the cancellation of the domain name, (2) the transfer of the domain name, or (3) the refusal of the application.

Dispute resolution service providers shall notify the ICTA, the parties, and registration organisations and publish the decisions online.

ADVERTISING

Regulation

19 | What rules govern advertising on the internet?

The Consumer Protection Law governs commercial advertising that is aimed at consumers in Turkey. The definition of commercial advertising is defined broadly in the law and covers advertising on the internet. The competent authority is the Board of Advertisement, which has the authority to investigate and monitor all advertising activities and to impose administrative fines. All advertisements shall be true and fair, and shall not violate public order, public morality, personal rights and principles issued by the Board of Advertisement. Any unfair commercial activity (eg, misleading or aggressive activities) is also prohibited and the Board of Advertisement may issue administrative fines in violation thereof. The Regulation on Commercial Advertisements and Unfair Commercial Activities provides more details on the rules established by the Consumer Protection Law. Further, the Law on the Establishment and Principles of Radio and Television Broadcasting applies to on-demand broadcasters. Any advertisement via such broadcasts would be subject to the said Law.

Relying on the Consumer Protection Law and the Regulation on Commercial Advertisements and Unfair Commercial Activities, the Ministry of Trade published the 'Guideline on Commercial Advertisements and Unfair Commercial Activities by Social Media Influencers' in May 2021. The Guideline defines social media influencers, requires advertisements made by them to be presented in a clear and comprehensible manner and forbids any surreptitious advertising activities.

The advertisement of specific products and services is also regulated. Advertising financial services is subject to the specific rules outlined in the Regulation on the Commercial Advertisements and Unfair Commercial Activities. Accordingly, such advertisements should accurately indicate the interest and dividend rates and include all conditions that would affect the total amount accrued at the maturity rate. Advertising medicines, medical devices, health services, supplements, cosmetics, cleaning products, tobacco products, and alcoholic beverages among others are further regulated in the relevant legislation.

A recent amendment made in the Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications (the Internet Law) introduced the online advertising ban on social network providers without making any distinction to the advertised product or services. Accordingly, the Information and Communication Technologies Authority may impose an advertising ban on a social network provider that has more than 1 million daily users from Turkey if said provider does not designate a representative in Turkey.

Definition

20 | How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

In the Consumer Protection Law, commercial advertising is defined as marketing announcements made by advertisers in relation to trade, business, craft or profession; made through verbal, visual or written communication tools or similar methods; with the objective of sale or lease of a good or service for the purposes of informing or persuading the target audience. Although there is no specific definition of online advertising in the relevant legislation, it falls under the scope of commercial advertising. That said, the Board of Advertisement issued decisions on advertisements published online and imposed administrative fines for online advertising in violation of the said Law.

Surreptitious advertising is not allowed under any circumstances according to the Consumer Protection Law and the Regulation on the Commercial Advertising and Unfair Commercial Practices. Surreptitious advertising is defined as the inclusion or promotion of trade names or business names within articles, news, broadcasts and programmes, by using names, trademarks, logos or other distinctive shapes or expressions of products or services without explicitly disclosing or clearly expressing that they are advertisements. In other words, the advertiser shall be identifiable by the target audience.

Misleading advertising

21 | Are there rules against misleading online advertising?

Misleading advertising is regulated in the Consumer Protection Law and the Regulation on Commercial Advertising and Unfair Commercial Activities. Accordingly, advertisers are obliged to prove that their advertised claims are true. Advertisers shall substantiate their claims with scientific documents and information. If need be, the Board of Advertisement may also request the advertiser to submit information or documents obtained from the universities or accredited research or test facilities.

Restrictions

22 | Are there any products or services that may not be advertised on the internet?

Currently, there are several products and services that cannot be advertised as per various regulations specifically applicable to them. According to the Pharmaceuticals and Medical Preparations Law, any advertisement of medicines and human medicinal products is prohibited. In addition, any advertisement of alcoholic beverages and tobacco is prohibited by the Spirits and Alcoholic Beverages Law and the Prevention and Control of Damages Arising from Tobacco Products Law. Legal services, gambling and accountancy services can be given as examples for other sectors and services that cannot be advertised. Although the above-mentioned regulations do not mention online advertising specifically, they apply due to the broad definition of advertisement found therein.

Hosting liability

23 | What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

As per the Internet Law, content providers are primarily liable for the content they publish online. Hosting providers and access providers are not obliged to monitor the content they store or transmit. That said, hosting and access providers shall, in any case, comply with judicial or administrative decisions regarding the removal or blocking access to the content.

FINANCIAL SERVICES

Regulation

24 | Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

All transactions concluded via the internet fall under the application of the Law on Regulating Electronic Commerce. Accordingly, all suppliers of financial services shall comply with their obligation to provide information to buyers regardless of being a consumer or a business.

Banks' sale of financial services products is regulated by the Regulation on Methods Utilised by Banks for Distant Identity Verification and Concluding Contracts via Electronic Mediums, which entered in force in May 2021. Accordingly, banks shall verify the customer's identification via methods specified in the Regulation on Banks' Information Systems and Electronic Banking Services. To form a binding contract, banks shall convey all terms and conditions of the contract to customers via mediums listed in the relevant regulation and the customer shall convey its declaration of intent securely. Only thereafter will contracts concluded via electronic mediums be deemed to fulfil the written form requirement. It should also be noted that not all financial services products are eligible to be sold via the internet as some services products are only to be formed officially. As a last remark, all banking regulations referenced herein are executed by the chairperson of the Banking Regulation and Supervision Agency (BDDK).

Suppliers of financial services products shall comply with more specific obligations outlined in the Regulation on the Distance Contracts of Financial Services if such product is sold to a consumer. Suppliers are required to provide certain information to consumers prior to the conclusion of the distance contract in the form explained in the Regulation. The scope of the supplier's obligation to provide information includes, among others, the main business of the supplier and contact information, a description of the main characteristics of the financial service, the total price of the financial service including all taxes or the basis for calculation, any limitations of the period for which the information provided is valid, information relevant to the right of withdrawal, the minimum duration of the distance contract in the case of financial services to be performed permanently or recurrently, information on any party's unilateral termination rights including any penalties imposed in such cases. The supplier shall communicate this information and any additional information after the conclusion of the distance contract to the consumer on paper or a durable data medium. The Regulation further elaborates on consumers' right of withdrawal, suppliers' and consumers' obligations, the legal effect of the right of withdrawal on ancillary contracts, exceptions to the right of withdrawal, the termination method of the distance contract, burden of proof, data retention obligation of the suppliers and rules on distance communication costs for consumers. Lastly, the Ministry of Trade is authorised to execute the provisions of the Regulation.

Advertisement of financial products is also regulated. Such advertisements should indicate the interest and dividend rates accurately and include all conditions that would affect the total amount accrued at the maturity rate as per the Regulation on the Commercial Advertisements and Unfair Commercial Activities.

DEFAMATION

ISP liability

25 | Are ISPs liable for content displayed on their sites? How can ISPs limit or exclude liability?

As per the Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications (the Internet Law), hosting providers and access providers are neither obliged to monitor the content they store or transmit nor to investigate actively whether there is any illegal activity. Hence, Turkish law provides a civil and criminal exemption to hosting and service providers. However, once notified according to the conditions laid out in the Internet Law, hosting providers and access providers are obliged to remove or block access to the content that constitutes the crimes set forth in the Internet Law or violates any personality rights. Failure to comply with such obligations results in administrative or judicial fines.

Notwithstanding the above, Turkey significantly amended its Internet Law in July 2020 and added the definition of a 'social network provider' in order to amplify compliance with content removal requests. The most significant amendment is the requirement for social network providers that track over 1 million daily users from Turkey to appoint a representative in Turkey. Although globally known social network providers were reluctant to comply with this requirement which took effect in October 2020, the authorities issued fines (up to 40 million Turkish lira) to several social network providers such as Facebook, Twitter and YouTube, which initially failed to appoint a representative in Turkey. In early 2021, the authorities issued an advertisement ban on Twitter as an additional sanction, one of the few social network providers that had not yet complied with the new regulation. At last, Twitter appointed its representative in Turkey before the authorities sanctioned the platform by limiting its bandwidth. Another significant amendment applicable to social network providers is the introduction of the obligation to reply to users' requests regarding personality rights or privacy violations within 48 hours. Lastly, if a social network provider does not remove the content or block access within 24 hours despite the presence of a judge or court order, it will be held liable for damages regardless of whether the injured party initially sought remedies from the content provider or not. As this amendment was adopted in 2020, how such claims can be brought against the social network providers is subject to judicial review.

Shutdown and takedown

26 | Can an ISP shut down a web page containing defamatory material without court authorisation?

The Information and Communication Technologies Authority (ICTA) issued administrative fines to an ISP in 2012 for blocking access to various websites without any judicial or administrative measures taken by the courts or the ICTA itself. The ICTA's decision regarding the ISP's blocking access to certain websites was evaluated within the scope of regulation on online content and the ISP's failure to take all necessary measures to keep all systems running. Therefore, it is ill-advised for ISPs to shut down a web page without any court order or administrative measures taken in this regard, even though such web page contains defamatory material.

INTELLECTUAL PROPERTY

Third-party links, content and licences

27 | Can a website owner link to third-party websites without permission?

A website owner can surface link (ie, direct internet users to third-party websites' homepages) without permission even when the content is under intellectual property protection. When an owner presents the work to the public online without any further technological restrictions or in other words, when it is freely available on the internet, it is assumed that the owner has given implicit consent regarding internet users' access to the work.

A deep link allows internet users to reach a particular web content instead of the homepage. Internet users do not see the advertisements on the homepage; as a result, the linked website's advertisement revenues may decrease. Deep linking may also cause unfair competition.

The mere act of linking does not violate the owner's intellectual property rights arising from the Law on Intellectual and Artistic Works. To speak of an infringement, linking itself should also violate the owner's rights to distribute, adapt, or any other right. In addition, linking does not constitute an act to publicise since the content is already made freely accessible to users by the owner.

28 | Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?

Framing allows the display of several documents on a web page without the linked websites' URL addresses. Therefore, internet users may not realise they have accessed a different web page. In contrast, inline linking allows the display of another web page's content automatically without leaving the website that has embedded the link. The inline linker does not place a copy of the content on its internet server. The internet users do not see the linked website's URL and therefore may be under the impression that the linked content belongs to the website that has integrated the inline link. Since framing and inline linking may mislead internet users about the work's owner, the owner's right to be recognised as the owner of the work may be violated as per article 15 of the Law on Intellectual and Artistic Works.

Websites cached by online search engines may sometimes contain photos or texts that are protected by the Law on Intellectual and Artistic Works. Such caching would be deemed as having the owners' implicit consent provided that the owner has not objected to the use of their work to search engine operator, the use of the work is in line with the owners' interests, the work is used to the extent that is required.

Keyword advertising and the use of metatags are considered within the framework of the Industrial Property Law. Accordingly, the owner may allege infringement of its trademark due to the use of keywords provided that (1) an identical or similar sign is used online by others, (2) this use has a commercial effect, and (3) the perpetrator has no right or legitimate connection to such use. Decisions of the Court of Appeal on keyword advertising establish that using a sign as a keyword that has a commercial effect and causing confusion are a trademark violation and constitute unfair competition.

29 | Can a website owner exploit the software used for a website by licensing the software to third parties?

Computer software is protected as a work of science and literature if it carries its owner's genuine identity according to the Law on Intellectual and Artistic Works. The owner can claim their financial rights, namely, the right to reproduce and distribute under copyright protection. The owner of computer software can exercise their right to distribute by licensing the software without transferring the ownership or allowing the internet user to download and copy the software.

30 | Are any liabilities incurred by links to third-party websites?

If the website owner links to a website where the content is not made legally available by the owner or the authorised person of the owner, the act of linking might constitute aiding or abetting intellectual property violation. As per the Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications, content providers are not liable for the content of third parties that they link to, as a rule. However, if the presentation of linking clearly indicates that the content provider adopts the content and intends to direct other users to the unlawful content, the content provider shall be responsible according to the general provisions.

Video content

31 | Is video content online regulated in the same way as TV content or is there a separate regime?

Video content online was not regulated prior to the amendments introduced in Law No. 6112 on the Establishment of Radio and Television Enterprises and Their Media Services, which regulates radio and television broadcasting services and on-demand media services. According to the new amendment, media service providers and platform operators who broadcast online shall obtain either a licence or authorisation from the Radio and Television Supreme Council (RTUK). In cases of broadcasting without a licence or authorisation, criminal courts may rule on the removal of content or blocking access. Media service providers and platform operators incorporated abroad also fall under the application of the Law provided that broadcasts are made in Turkish or a Turkish audience is targeted. RTUK and the Information and Communications Technologies Authority adopted a secondary regulation on 1 August 2019 named the Regulation on Online Broadcasting via Radio, Television, and On-demand Services detailing the licensing and authorisation process. Major on-demand streaming platforms such as Netflix and Amazon Prime Video had obtained their licences by the end of 2020.

IP rights enforcement and remedies

32 | Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

While there are civil remedies available for all IP rights, criminal remedies are granted only to registered trademarks and copyrights. However, submission of a complaint by the IP owner is required for

criminal remedies to be carried out. If the IP owner follows one of these procedures, the competent court may order a search warrant to seize evidence or an interim measure to cease the infringement.

33 | What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

An IP owner whose IP rights are infringed can request the competent court (civil courts or specialised IP courts where applicable):

- to determine whether the act constitutes an infringement;
- to prevent an imminent infringement or to cease an existing infringement;
- to order compensation for damages;
- to confiscate infringing products, manufacturing equipment and machinery;
- to transfer infringing products' ownership to the IP owner claimant;
- to implement measures against recurring infringements, including the destruction of infringing products; and
- to publish the judgment.

IP owners might also apply for an interim measure for the cessation or prevention of the infringement, including the seizure of the infringing products.

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

34 | How does the law in your jurisdiction define 'personal data'?

The Personal Data Protection Law (PDPL) defines personal data as any information relating to an identified or identifiable natural person. Legal persons are excluded from the definition of personal data and the scope of the PDPL.

The PDPL defines personal data revealing racial, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing and attire, association, foundation or trade union membership, health, sex life, criminal conviction and security measures, biometric or genetic information, as special categories of personal data. In line with the GDPR, special categories of personal data can also be defined as 'sensitive personal data'. As a rule, sensitive personal data can only be processed with the data subject's explicit consent. Exceptionally, sensitive personal data can be processed without explicit consent when authorised by law. However, personal data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by persons subject to a secrecy obligation or competent public institutions and organisations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of healthcare services as well as their financing. In its Decision No. 2018/10, the Board within the Personal Data Protection Authority (the Board) listed the adequate measures to be taken by data controllers to process sensitive personal data, which are to be followed by controllers as per article 6(4) of the PDPL. Encryption of servers and logging for any access to sensitive personal data can be given as examples to adequate measures.

Anonymisation is defined as 'rendering personal data impossible to link with an identified or identifiable natural person in any way including matching with other data'. Although processing anonymised data would fall outside the scope of the PDPL, processors shall comply with the Regulation on Erasure, Destruction or Anonymisation of Personal Data, which stipulates the methods of anonymisation of personal data.

Registration requirements

35 | Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?

Natural persons or legal entities that process personal data wholly or partly by automated means or conduct processing by unautomated means which form part of a data filing system fall into the material scope of the PDPL. Prior to data processing, natural persons or legal entities that process personal data shall register with the Data Controllers' Registry.

The Board may exempt certain controllers from the obligation to register. For instance, the Board exempted notaries, political parties and lawyers from the obligation with Decision No. 2018/32 and all controllers – either natural or legal persons – whose main field of activity is not processing sensitive personal data are exempt from the registration obligation as per Decision No. 2018/87, provided that they have less than 50 employees and their annual financial statement amounts to less than 25 million Turkish lira. The Regulation on Data Controllers' Registry requires data controllers located outside Turkey to authorise a legal entity located in Turkey or a Turkish individual for representation and registration.

The PDPL does not prescribe the appointment of an in-house data protection officer.

Cross-border issues

36 | Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?

The PDPL does not have a specific provision on its territorial application. However, the PDPL shall be interpreted in such a way that it protects individuals to the greatest extent. While establishing the rules on data breach notifications, the Board stated that data controllers located abroad shall notify the Board of data breaches provided that the results of such breaches affect persons located in Turkey and the affected persons benefit the services and products within Turkey. Accordingly, in recent years the Board issued administrative fines to companies located abroad due to data breaches that affected persons residing in Turkey. Therefore, the lack of a specific provision on the territorial application does not exclude the application of the PDPL to persons or organisations located outside Turkey.

Foreign nationals can enforce rights granted to data subjects in the PDPL. However, the application should be made in Turkish as per the Communique on Principles and Procedures for Application to Data Controller.

Cross-border data transfers

Personal data may only be transferred outside Turkey with the data subject's explicit consent, or if another lawful processing ground exists. In addition, the recipient country must have an adequate protection, or the parties requesting to transfer personal data abroad obtain approval from the Personal Data Protection Authority (DPA). The DPA has not yet issued an adequacy decision, although it was announced in 2020 that the DPA has been in collaboration with several ministries to work on a list of countries with adequate protection. Due to the lack of adequacy decisions, data controllers shall obtain approval from the DPA by filing a commitment letter or by undertaking binding corporate rules in case of cross-border data transfers. In 2021, the DPA approved several applications for cross-border data transfers.

Customer consent

37 Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?

As per the PDPL, personal data cannot be processed without the data subject's explicit consent. Personal data can be processed without the data subject's explicit consent only when:

- Processing is clearly prescribed by law.
- It is necessary for the protection of life or physical integrity of the person or of any other person who is unable to explain their consent due to physical disability or whose consent is not deemed legally valid.
- Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract.
- It is necessary for compliance with a legal obligation which the data controller is subject to.
- Personal data has been made public by the data subject.
- Processing is necessary for the establishment, exercise or protection of any rights.
- Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate fundamental rights and freedoms of the data subject.

Data controllers shall comply with the principles laid down in the PDPL even when processing occurs according to one of the grounds given above. The DPA finds relying on consent when other processing grounds are available as an abuse of rights. Therefore, controllers may rely on the performance of the contract or legitimate interests when they process personal data of the buyer in online transactions. Nevertheless, a case-by-case analysis shall be conducted to determine which processing ground can be relied upon.

Consumer consent shall be given explicitly. In a recent decision, the Board emphasised that consent shall be obtained in a method where the individuals can approve processing with their own informed choice and opt-out mechanisms shall not be used by controllers (Decision No. 2020/173). In addition, blanket consent forms are found to be invalid and explicit consent cannot be requested as a precondition for the services or products offered by the controller.

Additionally, controllers shall perform their obligation to inform in the form of a privacy notice before processing any personal data. The same obligation can be traced in the Regulation on Service Providers and Intermediary Service Providers in Electronic Commerce stipulating that service providers and intermediary service providers should make their privacy notice texts available on their websites.

Sale of data to third parties

38 May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?

Personal data might be sold to third parties within Turkey as per article 8 of the PDPL on the transfer of personal data. In this regard, data controllers may rely on the explicit consent of the data subject or other processing grounds listed in the PDPL. In either case, general principles on personal data processing must be observed. As processing shall be undertaken for specified, explicit, and legitimate purposes, data subjects must be informed regarding the transfer and recipients. If the buyer of personal data wishes to use personal data for marketing purposes, the seller should obtain explicit consent from data subjects. It is noteworthy that data subjects have the right to know the third parties to whom their personal data is transferred.

Personal data that has been made public by the data subjects themselves can be sold by a website owner provided that the transfer is consistent with the data subject's purpose for making their data public. On the other hand, sensitive personal data may be sold to third parties only with the data subject's explicit consent. In the case of a personal data transfer, the seller and the buyer are liable as data controllers exclusively for violations of the PDPL.

Customer profiling

39 If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?

Customer profiling via cookies is regulated in Turkey within the scope of personal data protection. Cookies would qualify as personal data if they can identify individuals when combined with other information. Two separate laws contain relevant provisions: (1) the Electronic Communications Law, which is heavily influenced by the EU Directive 2002/58/EC, and (2) the PDPL.

Parallel to Directive 2002/58/EC, article 51(3) of the Electronic Communications Law requires that users are informed clearly and comprehensively regarding the data processing activities and that they have provided their explicit consent when electronic communications networks store information or gain access to information stored in users' terminal equipment other than to provide services. This provision covers only authorised operators, those who provide electronic communications services or electronic communication networks and operate the infrastructure. Operators can rely on explicit consent as it is a statutory requirement.

That said, any other party that falls outside the Electronic Communications Law's scope shall conduct their processing activities via cookies as per the PDPL. Data controllers may rely on two separate exceptions to explicit consent: performance of the contract or their legitimate interests when they process cookies that are essential for the operation of the relevant website. In any case, data controllers must rely on explicit consent when they aim to use cookies for marketing or profiling activities. Controllers are advised to avoid opt-in mechanisms in this regard and provide links to the privacy notice and consent tab separately.

In 2020, the Board issued a decision concerning the use of cookies by an e-commerce website (Decision No. 2020/173). The Board assessed the cookies notice found on the website, which was of a general nature and noted that the cookies notice was not made available to first-time visitors. The Board added that the concerned data controller failed to inform data subjects on processing methods (such as cookies) and did not request the explicit consent of visitors. In sum, the Board evaluated the use of cookies from the perspective of controllers' obligation to inform and did not detail its position on which exceptions under which circumstances can be relied on by controllers if cookies are used.

Data breach and cybersecurity

40 Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?

The PDPL stipulates that data controllers must take necessary technical and organisational measures to avoid any unlawful access or processing of personal data. In the event of a security breach, controllers must notify the Board without delay and within 72 hours at the latest after they become aware of such breach. Controllers must also notify the data subjects as soon as reasonably possible after detecting

persons affected by the breach. In addition to the PDPL, the Regulation on Service Providers and Intermediary Service Providers in Electronic Commerce requires service providers and intermediary service providers to implement necessary measures to avoid personal data security breaches.

41 What precautionary measures should be taken to avoid data breaches and ensure cybersecurity?

While the PDPL states that controllers should implement all necessary technical and organisational measures, it does not shed a light on how controllers can ensure cybersecurity. The DPA published Guidelines on Technical and Organisational Measures, which contain the following measures, inter alia:

- Controllers should first determine the existing risks and threats and evaluate if they process sensitive personal data, the privacy level expected due to the characteristics of such data, and the possible outcomes of a breach.
- Controllers should train their employees and raise awareness.
- Controllers should develop a personal data security policy.
- Controllers should update their security walls and software and follow patch management. They are encouraged to limit their employees' access to personal databases and follow the instructions regarding passwords therein.
- Controllers should check software and services in operation, keep log records, develop a reporting mechanism, and report security problems officially as soon as possible.
- Devices that contain personal data should be kept physically safe. Controllers should prefer internationally recognised encryption methods.
- When controllers use cloud services for personal data storage, they should check the security measures implemented by the cloud provider. The use of multi-factor authentication, encryption, different encryption keys for different cloud services, and the destruction of encryption keys at the end of the service are encouraged technical measures.
- Controllers should have separate backup servers that are controlled only by the system manager in case of a security breach. Controllers should ensure the physical safety of these backup systems.

In 2020, the Board issued administrative fines to a bank for not taking the necessary technical and administrative measures (Decision No. 2020/744). The Board found that the data controller failed to prevent a data leak by its employee even though it had given the necessary training to employees and installed an IT system to identify and prevent leaks through external emails. Although the Board acknowledged the measures taken by the data controller, it still issued administrative fines taking into consideration the data controller's negligence in the data leak.

Insurance

42 Is cybersecurity insurance available and commonly purchased?

Although cybersecurity insurance is available and offered by most insurance companies, 75 per cent of firms in Turkey do not have a policy against cybersecurity risks. However, some stakeholders argue that cybersecurity insurance should be mandatory in Turkey.

Right to be forgotten

43 Does your jurisdiction recognise or regulate the 'right to be forgotten'?

The Supreme Court Assembly of the Civil Chambers and the Constitutional Court recognised the right to be forgotten before the PDPL was enacted. Decisions rendered by both courts include references to the *Google Spain* decision of the CJEU. Although the right to be forgotten is usually evaluated in online cases, the Supreme Court Assembly of the Civil Chambers held that the concept of the right to be forgotten would extend to personal data in a non-digital form which is stored in mediums easily accessible by the public. Having said that, the PDPL does not contain an exclusive 'right to be forgotten' per se. Yet, the Board recognised the right to be forgotten as an extension of data subjects' right to request erasure, destruction or anonymisation of personal data set forth in the PDPL as well as in the Regulation on Erasure, Destruction and Anonymisation of Personal Data. Further, the Board issued guidelines to be taken into consideration by data controllers while evaluating requests relating to the removal of persons' names and surnames from the index of search results. The said guidelines list various criteria including but not limited to whether the information is up to date or infringes the affected individual's personality rights.

Moreover, article 8(10) of the Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications contains a provision that can be interpreted as the 'right to be forgotten'. The aforementioned provision states that the Court might order the applicant's name to be delisted in online search engines if required by the applicant whose personality rights are violated by the online content.

Email marketing

44 What regulations and guidance are there for email and other distance marketing?

Any message (in the form of data, sound, or image) transmitted electronically for commercial purposes qualifies as an 'commercial electronic message' under the Law on the Regulation of Electronic Commerce (the E-Commerce Law), which is the main regulation on commercial communication in e-commerce. Commercial electronic messages are further regulated in the Regulation on Commercial Communication and Commercial Electronic Messages, which outlines how obligations under the E-Commerce Law must be fulfilled. Other than the regulations on e-commerce, the Electronic Communications Law regulates commercial electronic messages sent to subscribers and customers by operators.

First, all natural and legal persons that wish to send commercial electronic messages must register themselves on the Message Management System (abbreviated in Turkish as IYS). IYS is a national database to which all service providers shall register the consents given by persons for receiving commercial electronic messages. Commercial electronic messages shall only be sent after obtaining prior consent from recipients (ie, opt-in mechanism). Individuals can monitor all consents given by them and may revoke any consent given in the past via the IYS platform. If the service provider obtains consent in writing or electronically, it must register these to IYS within three business days, otherwise the consent becomes invalid. In addition, if consent is obtained using any other method than the IYS platform (eg, in writing or electronically by service providers), the burden of proof on the existence of consent is on the service provider. It should be noted that obtaining consent is not mandatory in B2B relations. As per the relevant legislation, the authorities may issue administrative fines to service providers and intermediary service providers for sending commercial electronic messages in violation of the above-mentioned and other mandatory rules. All in all, the ways businesses may interact with their (potential)

customers are restricted and customers have more control over what kind of marketing messages they would like to receive with the introduction of the IYS platform.

Operators need to obtain prior consent for marketing purposes as well (opt in). Exceptionally, operators do not need to obtain consent when contact details are given in the context of the sale of a product or a service, provided that subscribers and users are informed about communication and given the opportunity to object. Yet, operators are allowed to use such contact details only for the marketing of the same or similar products or services, advertising, change and maintenance services.

Consumer rights

45 | What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

As per article 11 of the PDPL, data subjects have the right to:

- learn whether their personal data is being processed or not;
- demand information as to whether their personal data has been processed;
- learn the purpose for the processing of their personal data and whether this personal data has been or is being used in compliance with the purpose;
- know the third parties to whom their personal data has been or is being transferred to in the country or abroad;
- request the rectification of incomplete or inaccurate data;
- request the erasure or destruction of their personal data under the conditions referred to in article 7;
- request reporting of the transfer operations to third parties to whom their personal data has been transferred;
- object to a detrimental decision which is based solely on automated processing; and
- claim compensation for damages arising from the unlawful processing of their personal data.

These rights would extend to foreign individuals residing in Turkey; however, the application to the data controller can only be made in Turkish.

TAXATION

Online sales

46 | Is the sale of online products subject to taxation?

All services that are performed or whose benefits are consumed in Turkey would be subject to VAT. Other than VAT, special consumption tax (otherwise known as ÖTV) may be applicable for products such as electronic appliances.

All companies incorporated in Turkey or having a residence, business place, legal centre or business centre in Turkey are liable for VAT payment. In 2018, the Revenue Administration issued a ruling on the sale of online games by a company incorporated in Turkey and stated that all sales of online games are subject to VAT except for sales to users abroad. Sales to users residing abroad would be defined as services export, thus would be exempted from VAT.

As per article 9 of the VAT Law, the sale of online products by those who do not have a residence, workplace, legal centre or business centre in Turkey is subject to VAT as long as the services are provided electronically to natural persons who are not VAT payers in Turkey. In this case, VAT will be paid by the companies providing the service. Such corporations need to register to the Revenue Administration through the Special VAT Registration for E-Service Providers, which is available at https://digitalservice.gib.gov.tr/. In the case of B2B sales, the same corporations still need to fill out the VAT declaration, yet VAT would be paid by the buyer (ie, reverse charge mechanism).

Effective from March 2020, sale of any audio, visual or digital content on digital platforms (including computer programs, applications, music, video, games, in-app purchases and other similar products) and digital services offered to listen, watch, play or record these contents in electronic media or use them in electronic devices are subject to digital services tax set at 7.5 per cent. The tax is calculated based on the revenue generated from Turkey. Digital services tax applies to all persons generating revenue from Turkey without making any distinction to a full or limited taxpayer status, save from certain exemptions listed in Law No. 7194 on Digital Services Tax.

In addition to the aforementioned taxes, stamp duty may be applicable in some instances. In accordance with the General Communique on Stamp Tax Law (Serial No: 60), any agreement concluded via an online platform would be subject stamp duty if it is concluded via electronic signature subject to certain exceptions.

Server placement

47 | What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Corporations are taxed based on whether their legal or business centre is located in Turkey or not. Those who have their legal or business centre in Turkey are defined as taxpayers with full liability, whereas those who have neither their legal nor business centre in Turkey are defined as taxpayers with limited liability. Full taxpayers are taxed based on the revenues they generate globally, whereas limited taxpayers are taxed based on the revenue they generate only from Turkey. Therefore, establishing what constitutes a business centre is the key question that will be evaluated as per the Turkish tax law and the relevant bilateral agreements for the avoidance of double taxation. In most cases, a fixed place that is assigned for commercial activities constitutes a business centre. The Turkish Revenue Administration considers the server on which the website is stored and accessed as equipment with a physical location; thereby such location may constitute a fixed place of business of the company that operates the server. As a result of this definition, placing servers in Turkey may result in foreign corporations being declared as taxpayers with limited liability. Therefore, these corporations may be liable for paying corporate taxes, which will be calculated based on the revenue generated from Turkey.

Company registration

48 | When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

VAT liability is an automatic process. Any natural or legal person conducting any sale of a product that is subject to VAT automatically becomes liable to VAT. The liable party for the payment of VAT is required to make a declaration of the accrued VAT amounts to the taxation authority to which they are registered as taxpayers. VAT payments shall be calculated monthly and VAT declarations shall be submitted until the 26th day of the following month. Electronic service providers with no residence, business place, legal centre or business centre in Turkey shall first complete their registration on https://digitalservice.gib.gov.tr/ and then submit their VAT declarations thereto. In B2B sales, the reverse charge mechanism applies, yet electronic service providers still need to submit VAT declaration for such sales for cross-checking activities of the Revenue Administration. Lastly, C2C sales are exempted from VAT.

The Law on Digital Services Tax applies regardless of the taxpayer's full or limited liability status. All sales of audio, visual or digital content on digital platforms (including computer programs, applications, music, video, games, in-app purchases and other similar products) will be subject to the digital services tax. Digital services are taxed monthly, the same as VAT, and taxpayers shall pay the said tax before the end of the month following the taxation period. Digital service providers or intermediary service providers shall complete their registration on https://digitalservice.gib.gov.tr/.

Both VAT and digital services tax apply to domestic online sales.

Returns

49 | If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

In the case of exported goods, the importer may physically return the goods and request the import duties and tax to be refunded, subject to certain conditions (eg, goods shall not be altered). If a consumer returns goods and requests to be reimbursed, all monies paid by the customer including VAT shall be returned. In such cases, suppliers shall issue an expense voucher to deduct the paid VAT. The issue of transfer pricing is also regulated in Turkey and all transfers between different affiliates shall be done at arm's length.

GAMBLING

Legality

50 | Is it permissible to operate an online betting or gaming business from the jurisdiction?

Providing a platform for gambling is strictly forbidden by the Turkish Criminal Law. However, online betting is permissible under Turkish law, subject to strict regulations. As per the Regulation on Fixed Odds and Parimutuel Betting Based on Sports Competitions (the Betting Regulation), only legal persons can operate online betting platforms (also called online platform agencies) by obtaining a licence from the Spor Toto Organisation Presidency. There are various requirements for a legal person to obtain an online platform agency licence from the Spor Toto Organisation Presidency such as being registered in Turkey as a joint-stock company whose capital meets with the threshold determined by the Presidency. Once the licence is issued, the online platform agency will enter into an agency contract with the Spor Toto Organisation Presidency for a period of up to 10 years. The agency contract will be in force as long as the licence is valid and would automatically be terminated if the corresponding licence is cancelled.

Further, online betting agencies should comply with the necessary operational requirements set forth in the Betting Regulation; including but not limited to providing a guarantee for the amount that will be determined by the Spor Toto Organisation Presidency. If a natural person were to operate an online betting platform without complying with the relevant legislation, they would be sentenced to three to six years' imprisonment and corresponding security measures would apply to any legal persons.

51 | Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Gambling is considered as a misdemeanour as per article 34 of the Misdemeanour Law. A resident or a citizen of Turkey can be fined as a result of gambling and in such case, all related earnings would be transferred to public funds.

While residents and citizens of Turkey are permitted to use online betting platforms, the regulatory age is set at 18. According to the Betting Regulation, online betting platform providers should prevent underaged persons from placing any bets and no payment shall be made if that person earns a reward. Failure to comply with the provision regarding the regulatory age would result in termination of the licence obtained from the Spor Toto Organisation Presidency.

OUTSOURCING

Key legal and tax issues

52 | What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

Outsourcing is regulated within the scope of the Labour Law, which applies to all businesses. Not all services can be outsourced by an employer. An employer can outsource auxiliary works, which are defined as works related to or dependent on the main operations. To outsource a part of main operations, the outsourced service should be an aspect of the main operations that requires technological know-how and expertise. Technological know-how and expertise are defined as works essential for undertaking the main operations and that are beyond the businesses' expertise.

The Regulation on Subcontractors also sets forth the mandatory provisions to be included to outsourcing contracts. For instance, certifications or other relevant documents regarding the outsourced service should be attached to the contract if a service is outsourced for the need of technological know-how and expertise. Other provisions that must be inserted in outsourcing contracts include but are not limited to the business name and address of the main employer and subcontractor, work assigned and main operations undertaken in the workplace.

VAT will apply to outsourced services provided by a supplier to a local customer if the services are benefited from in Turkey. Stamp duty would also arise in case of an outsourcing contract.

Employee rights

53 | What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, and do the rules apply to all employees within the jurisdiction?

As per the Labour Law, the decision to outsource a part of the company's operations does not constitute a legitimate reason for employment termination even if the work of such employee is to be outsourced. The employee whose employment has been terminated due to a decision to outsource will be able to request compensation and indemnifications. In accordance with article 21 of the Labour Law, if the court decides that the termination is unlawful, the employer would be obliged to reinstate its former employee within a month. If the employer fails to reinstate the employee, they would be obliged to indemnify the employee. The aforementioned rights for reinstation and compensation are applicable for all employees that fall under the scope of the Labour Law.

ONLINE PUBLISHING

Content liability

54 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability? Is it required or advised to post any notices in this regard?

As a rule, content providers are liable for the content they publish online, and hosting providers do not have a general obligation to monitor the content delivered by the content provider. However, hosting providers shall comply with judicial or administrative decisions on the removal of or blocking access to unlawful content; otherwise, they would be subject to administrative or judicial fines. Furthermore, civil liability may arise as per the general terms applicable to torts. For a tort liability to arise, mistakes in information published online shall cause damages to a third party and the hosting provider shall be at fault. The burden of proof would rely on the website user. Hosting providers cannot exclude themselves from the above-mentioned liabilities via posting notices or general terms and conditions.

For social network providers, the scope of liability is broader. If the content is found unlawful by a court order and the social network provider does not remove the unlawful content within 24 hours, the social network provider would be liable for all damages. It is not required that the damaged party first seeks damages from or initiates a lawsuit against the content provider. As this rule has been recently introduced in Turkey, it has not yet been subject to judicial review.

As a last remark, the spread of online disinformation is not regulated in Turkey, and hosting providers would be only liable in cases stated above.

Databases

55 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

Turkish law affords legal protection to original and non-original databases. If certain conditions are met, an original database is protected as a 'work' and website providers can enforce their rights as a rights holder. However, the protection applies to the database itself, not to the materials or data constituting the database. Non-original databases have a special protection if the website provider has essentially invested in the construction, verification or representation of the database. The website provider can cease the use or reproduction of a non-original database if the violation concerns all of the database or a significant part. The use or reproduction of data from third parties' databases may also constitute unfair competition as per the Turkish Commercial Code.

DISPUTE RESOLUTION

Venues

56 Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

To ascertain which court has the jurisdiction to decide on a dispute, first the nature of such dispute shall be identified. If a dispute arises from a transaction undertaken online, the competent court will be determined after evaluating whether the relevant transaction is concluded with a trader or a consumer. Any disputes arising from an online transaction concluded with a customer shall be first referred to consumer arbitration committees provided that the value of the dispute is lower than 11,300 Turkish lira. Decisions rendered by consumer arbitration committees can be appealed to consumer courts. Any disputes with a value higher than 11,300 Turkish lira can be brought directly before the consumer courts. If the online transaction is concluded with a trader or related to a commercial enterprise, parties first shall refer the dispute to mediators; only thereafter can the dispute be brought before the courts.

BODEN LAW

Sinem Mermer
smermer@boden-law.com

Levent Loft 1 Büyükdere Cad. No:201 D:27 Levent
Istanbul
Turkey
Tel: +90 212 251 15 00
www.boden-law.com

ADR

57 What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

There is no ADR available specifically for online or digital disputes, other than those mentioned specifically in the relevant laws. Consumer arbitration committees and arbitration committees for domain names can be given as examples. According to the Turkish Commercial Code, all commercial disputes shall first be referred to mediation before initiating a lawsuit before the competent courts.

UPDATE AND TRENDS

Key developments of the past year

58 Are there any emerging trends or hot topics in e-Commerce regulation in the jurisdiction? Is there any pending legislation that is likely to have consequences for e-Commerce and internet-related business?

During the covid-19 pandemic, various legislation has been enacted or amendments have been introduced to enable commercial life to resume in the digital world such as legalising the onboarding of new customers to banks by distant identity verification methods. Since 2020, new amendments to the law regulating online content have been the hottest topic in Turkey. Accordingly, on-demand streaming platforms need to obtain a licence from the Supreme Council of Radio and Television and social network providers having more than 1 million daily users from Turkey must appoint a representative in Turkey. Another recent development is the introduction of a digital service tax applicable to all service and intermediary service providers in e-commerce. In April 2021, the Turkish Presidency published the Human Rights Action Plan in which it stated that the Personal Data Protection Law will be revised in line with the standards of the European Union within a year.

* *The author would like to thank Utku Veznedaroglu, associate at Boden Law, and Merve Topkoru, legal intern at Boden Law, for kindly assisting in the preparation of this contribution.*

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-652-5