MOROĞLU ARSEVEN

Chambers and Partners TMT 2022 Guide – Law and Practice: Turkey Chapter

16 Mar 2022

1. Cloud Computing

1.1 Laws and Regulations

Although there are no specific laws for regulating cloud computing in Turkey, certain rules prescribed in several laws and secondary legislation concerning cloud computing apply in most cases. These rules are mainly concentrated on the notification requirement and data localisation.

Laws and Regulations on Hosting Providers

As per Law No 5651 on the Regulation of Publications on the Internet and the Suppression of Crimes Committed by Means of Such Publications, hosting providers should notify the Information and Communication Technologies Authority (ICTA) before providing hosting services. Violation of this obligation will incur an administrative fine ranging from TRY148,608 to TRY1,486,078. The approval and licence requirements are no longer applicable to hosting services.

Law No 5651 defines hosting providers as "natural or legal persons who operate or provide systems that store services and content". As such, cloud computing providers are regarded as hosting providers under Law No 5651 and are obliged to notify ICTA before starting to provide cloud computing services.

As per Law No 5651, hosting providers are not responsible for inspecting the legality of the content, but they are required to retain the traffic data for one year and to ensure the integrity, accuracy and privacy of this data. At this point, it should be kept in mind that, as per Electronic Communication Law No 5809 (ECL), the traffic data cannot be transferred abroad without the data subject's explicit consent. This is an important challenge for cloud computing providers whose servers are located in foreign countries.

If any requests are duly made by authorised institutions for certain content, the hosting provider should discontinue broadcasting the relevant content if it is broadcasted.

According to Article 51 of the ECL, traffic and location data can be transferred abroad only if explicit consent has been obtained from the data subject. In this sense, if such data is to be kept in a cloud, the servers of this cloud must be in Turkey.

In 2013, ICTA published a report analysing the usage, advantages and disadvantages of cloud computing within the EU and Turkey, but said report is not binding and cannot count as a guideline.

Lastly, as per ICTA decision no 2019/DK-TED/053 dated 12 February 2019 (ICTA Decision), all structures, systems, storing units and software regarding remote programmable sim technologies (e-sim) must be

established in Turkey, and data must be kept in Turkey. In such cases, cloud computing is allowed but the servers of the cloud services must be kept in Turkey.

Data Protection and Transferring Personal Data Abroad

Personal Data Protection Law No 6698 (DP Law) is the main legislation governing the protection of personal data in Turkey. As per the DP Law, the following conditions must be met in order to transfer personal data:

- the data subject must give explicit consent for the data transfer;
- the country where the data is going to be transferred should be among the safe countries declared by the Turkish Data Protection Board (Board); or
- the receiver of the data should undertake to take all necessary measures to protect the data, and the Board should approve the receiver's undertaking.

The explicit consent of the data subject or an approved undertaking is currently required in order to transfer personal data abroad.

At this point, an assessment should be made in order to determine whether retaining data in a cloud system whose servers are located in foreign countries can be regarded as a cross-border data transfer. The Board has issued some decisions that indicate its opinion on this matter: for example, decision 2019/157 dated 31 May 2019 highlighted that, in the usage of Gmail services provided by Google, emails are being held at data centres all around the world, which constitutes transferring personal data abroad under Article 9 of the DP Law.

Moreover, in decision 2020/173 dated 27 February 2020 regarding commercial email services, the Board concluded that Amazon Turkey violated DP Law rules regarding cross-border data transfers due to the failure to obtain the explicit consent of the users for email services. In line with the Gmail decision, this recent Amazon decision has again underlined that the usage of email services constitutes a transferral of personal data abroad with.

Finally, in decision 2021/359 dated 13 April 2021, the Board sanctioned a data controller employer for using cloud services to store employees' personal data without first obtaining the employees' explicit consent. In the incident subject to the decision, the employee data was stored in a cloud database with servers abroad, which could only be accessed by relevant authorised persons; therefore, the Board ruled that the data was transferred abroad.

As a result of these three cases, it is important for cloud computing service providers to comply with the DP Law (especially Article 9). Currently, transferring data abroad is only possible with the explicit consent of the data subjects or the undertaking approved by the Board, as the Board has not yet published the list of "countries with adequate level of protection" for data centres under Article 9 that would allow the transferring of data abroad without explicit consent.

Financial Market Regulations

Due to the importance attached to financial data, a special regime is prescribed in banking and financial market regulations regarding cloud computing in the financial sector.

The financial sector in Turkey is regulated and supervised by the Banking Regulation and Supervision Agency (BRSA). The sector is traditionally divided into two main categories: banks and financial institutions (financial leasing, factoring and financing companies) (together, Institutions).

The Official Gazette dated 15 March 2020 contained the new regulation by the BRSA regarding the utilisation of information systems for banking services, which became fully effective on 1 January 2021. Before the new regulation, there were two communiqués in force regulating information systems of financial institutions and payment and electronic money institutions. All three of these regulations (BRSA Regulations) set forth similar provisions regarding cloud systems.

The use of cloud systems is not prohibited under the BRSA Regulations, but certain conditions should be fulfilled.

According to the BRSA Regulations, the primary and secondary systems of the Institutions should be kept in Turkey. If cloud computing services are used, the information systems of cloud computing service providers and their back-ups are also regarded as primary and secondary systems of the Institutions. In such cases, this data, hardware and software, and their back-ups, should also be kept in Turkey.

Moreover, if cloud computing services are used for primary and secondary systems, the hardware and software used should be dedicated to a single institution. However, the use of community clouds is permitted for banks and financial institutions in certain conditions. If BRSA approval is obtained, a community cloud can be used by banks and financial institutions, on the condition that the software and hardware are dedicated to BRSA-regulated institutions and logical separation is provided for each company. In addition, with BRSA approval, financial institutions may use the same dedicated software and hardware if logical separation is provided for each company.

Capital Markets Regulations

The Capital Markets Board (CMB) Communiqué on Management of Information Systems (CMB Communiqué) was published in the Official Gazette and come into force on 5 January 2018. The Communiqué contained special provisions regarding the localisation of data for those institutions to which the Communiqué is applicable.

In this scope, stock exchange markets, the Central Registry Agency, capital market institutions, public companies and several other capital markets actors are obliged to keep their primary and secondary systems in Turkey.

Primary systems are defined as all systems consisting of infrastructure, hardware and software data enabling all information required for the conduct of all activities and the fulfilment of all duties to be utilised and accessed safely and at any time electronically. Secondary systems are defined as the back-ups of primary systems.

Although there is no clear addressing of cloud systems, the definition of primary systems is very inclusive and clear enough to determine that, if cloud computing is used, the main data, software and hardware and their back-ups should be kept in Turkey, which requires the servers to be located in Turkey.

Regulation regarding Payment and Electronic Money Institutions

The use of cloud services by payment and electronic money institutions is regulated under the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services in the Field of Payment Services of Payment Service Providers (Payment IT Communiqué), according to which, payment and electronic money institutions can use cloud computing services established domestically as an outsourced service to process, store and transmit all kinds of data. However, obtaining a cloud computing service to process sensitive customer data, competitively sensitive data or personal data requires the hardware and software resources to be allocated solely to the institution doing the processing. In certain cases, logical separation in the same hardware can be used if the hardware is allocated to payment and electronic money institutions or credit/financial institutions that are regulated and supervised by an authority.

Regulations regarding Public Utilities

The Circular on Information and Communication Security Measures (Circular) was published in Official Gazette No 30823, dated 6 July 2019, and contained several rules regarding security measures to be taken by public utilities for information security.

The first provision prescribes that information such as inhabitation, health and communication data will be kept in Turkey, and the third provision clearly prescribes that data held by public institutions cannot be kept in cloud systems except the own special systems of the institutions and those of local service providers supervised by the institutions.

The localisation of government data has become concrete through the Circular. As such, cloud outsourcing is not allowed in public institutions except for local service providers supervised by the institutions. Even in that case, all systems of the cloud service providers containing the public data should be kept in Turkey.

2. Blockchain

2.1 Legal Considerations

Blockchain is currently not regulated under any specific law or regulation. It is understood, however, from publicly available data that work on draft legislation is in progress

The use of cryptocurrencies in capital markets is prohibited. In 2017, the CMB sent a general letter to intermediary institutions, pursuant to their information request, stating that Turkish legislation contains neither a regulation nor a definition of crypto-assets, and as crypto-assets are not listed among the underlying assets upon which a derivative instrument can be based, intermediary institutions should not conduct any derivatives or spot transactions based on cryptocurrencies.

Aside from this, blockchain technology is usable in the financial sector. For example, the Istanbul stock exchange Borsa Istanbul (BIST) has carried out a project to use a customer database that is based on blockchain technology. In this respect, the adding of new customers and the changing of data and documents are managed through a blockchain network. Similarly, Istanbul Takas ve Saklama Bankası A.Ş. has implemented a blockchain application to enable physical gold to be converted into a digital asset and thereby allow the transfer of gold without time limitation, from person to person.

Digital securities have structural similarities with investment instruments regulated under Capital Markets Law No 6362 (CML). In this sense, while issuing these assets it is important to make a detailed assessment

regarding whether they may fall within the scope of the CML and relevant legislation. Where the instrument has a regulated underlying asset such as equities, the issue of such asset would probably subject it to the CML and relevant legislation.

Cryptocurrency transactions are subject to extant laws on the prevention of financial crimes, anti-money laundering and combatting the financing of terrorism, and laws of taxation.

In the absence of specific blockchain regulations, existing law limits the types of assets in which a fund may invest. Since blockchain assets are not specifically approved, it is reasonable to conclude that funds may not invest in these assets. Moreover, the CMB does not allow intermediary institutions to conduct any derivative or spot transactions based on crypto-assets.

The BRSA published a public statement in November 2013 assessing cryptocurrencies' legal status with respect to Law No 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions (Payment Law). According to the BRSA, cryptocurrencies (bitcoin in the public statement) cannot be regarded as electronic money since they are not issued by any official or private institution, and their intrinsic value is not reserved by funds received by the issuer. Also, as per the Regulation on the Use of Crypto-Assets in Payments, crypto-assets cannot be used, directly or indirectly, to purchase goods and services in Turkey nor in the provision of payment services or the issuance of e-money. Intermediary financial services to crypto-asset platforms and service providers, including funds transfers, custodial, settlement and issuance services and the development of financial services business models involving crypto-assets are prohibited.

Blockchain can serve as both an advantage and a disadvantage for the protection of personal data. The data can be stored more securely in a blockchain. However, as the data in a blockchain is not kept by a central database but rather distributed through decentralised databases, it is not clear whether joint controllership exists between the ledger holders. Also, as it is difficult to delete or alter data in a blockchain, any necessary erasure, destruction or anonymisation becomes a problem. In this respect, blockchain may prevent data controllers effectively meeting their obligations.

As there is no centralised database, jurisdictional issues may also arise. The International Private and Civil Procedure Law No 5718 (PCPL) is the main legal document governing jurisdiction and conflict of law issues. As per the PCPL, domestic jurisdiction rules apply for the jurisdiction of Turkish courts internationally, but for certain specific cases the jurisdiction is addressed under the PCPL. In this regard, jurisdiction for the usage of blockchain is determined based on the purpose for which the blockchain is used and the nature of the dispute, as per Civil Procedure Law No 6100.

Intellectual property (IP) has become an important topic in relation to blockchain networks, especially after the rise of NFTs. There are different aspects of blockchain that raise IP-related issues - mainly blockchain software and the content or data embedded in the blockchain.

The software related to blockchain technology is protected under Turkish Copyright Law No 5846 (Copyright Law) as long as it bears the individuality of its author. Protection granted to software does not include algorithms and interfaces, but interfaces may be protected as designs under Copyright Law and Industrial Property Law No 6769 (IP Law) as well as unfair competition rules.

However, detecting the ownership of any IP rights or any infringement of IP rights is still problematic, based on various factors, such as: ownership of a work is hard to determine in a decentralised network, and the infringement claim can differ based on whether or not an open-source was used and then what type of licence was used, etc.

The content or data embedded in the blockchain can be transferred easily through blockchain technology. The content may include copyrighted work or trade secrets, so it is not wrong to prognosticate that blockchain may be subject to copyright infringement or other IP rights infringement claims.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

3.1 Challenges and Solutions

The main challenge regarding starting a project involving big data, machine learning or artificial intelligence (AI) is the personal data protection issues. The DP Law, which is based former EU Directive 95/46/EC on the protection of personal data, is the main legal document that governs the processing of personal data - see **6.1 Core Rules for Individual/Company Data**.

Personal data composing "big data" and the resource data for machine learning must be obtained and processed in line with the DP Law. As such, the collection and process of the personal data must be based on a valid legal ground as per the DP Law; the explicit consent of the data subjects, when necessary, must be obtained in compliance with the personal data processing principles; and the data subjects must be informed of the data processing.

AI is not specifically regulated under Turkish law, but its use may trigger certain control mechanisms under various laws and regulations.

For instance, the use of AI automatic decision making or any other processing exclusively conducted through automatic means can be challenged by data subjects if it has a negative impact on them.

Product liability and tort provisions of Turkish law also apply to damages incurred due to the use of AI. The use of AI in smart vehicles, including driverless cars, may result in product liability issues. As the driver may be the AI rather than the person who holds the driver's licence, traffic insurance issues may arise. In this specific case, as driverless cars are not actively in traffic as of yet, it is not clear how the courts and insurance companies will handle such cases.

Another aspect is the IP issues. Software is considered a science and literature work under the Copyright Law, and is protected without any registration obligation. Therefore, the outputs of machine learning processes and artificial intelligence are protected under the Copyright Law.

One issue regarding the use of artificial intelligence is whether the products created by AI are patentable, or whether AI can be regarded as an inventor. This issue is yet to be resolved officially in Turkey as there are not yet any patent applications regarding products produced by AI. Pursuant to Article 74 of the Regulation on the Implementation of the Industrial Property Law of 24 April 2017, the identity and contact information of the inventor must be included in the patent application form. Therefore, although there is no clear statement, it can be said that an inventor can only be a real person in the context of the IP Law. In other words, it is not

possible for artificial intelligence to be accepted as an inventor according to the current regulations; even legal persons are not accepted as inventors in this direction. As a matter of fact, the IP Law regulates employee inventions and states that legal entities do not have the title of inventor.

The PCPL is the main legal document governing jurisdictional and conflict of law issues. It states that domestic jurisdiction rules apply for the jurisdiction of Turkish courts internationally, but for certain specific cases the jurisdiction is addressed under the PCPL. In this regard, jurisdiction for the usage of big data, machine learning and AI is determined based on the purpose for which they are used and the nature of the dispute.

Elements of big data, machine learning and AI - such as databases, software, designs, artistic works, models and robots - may be protected based on their nature under the Copyright Law or the Commercial Law, or as long as they meet the requirements. Some people defend the protection of an algorithm as a literate work if it is unique, but there is not yet any case law on this subject. Algorithms may be protected as trade secrets in certain cases.

The ownership of a creation of an AI is still under discussion in the Turkish community and all around the world. There is no case law regarding AI in Turkey yet. However, the Copyright Law and the IP Law are based on human creativity and only determine real persons as authors or inventors. Accordingly, future challenges will revolve around determining the ownership of works and inventions created by an AI, necessitating the adaptation and evolution of the legal IP framework.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions on a Project's Scope

The internet of things (IoT) is not specifically regulated under Turkish Law. The main legal issues regarding IoT are data protection and cybersecurity. As explained in detail in **6.1 Core Rules for Individual/Company Data**, the collection and processing of personal data must follow the DP Law. In this respect, if personal data is collected and processed through IoT, such collection and processing must have a legal basis under the DP Law, the data processing principles must be followed, and the data subjects must be informed of the data processing. In this regard, the excessive collection of personal data must be avoided.

For Turkey-domiciled data subjects, the rules for cross-border transfers of personal data apply. Therefore, if the servers where the data is stored are located outside Turkey, either the explicit consent of the data subject must be obtained, or an undertaking must be approved by the Board. Also, the data controller is responsible for the protection data subjects' personal data collected through IoT. The hacking of those devices may also raise product liability claims.

Another important issue is when the products use e-sim technology to communicate. As per the ICTA Decision (see **1.1 Laws and Regulations**), if e-sim technologies are used within the borders of Turkey, the modules within this scope must be programmed exclusively to be controlled by mobile operators in Turkey, and only the profiles of Turkish operators must be set up. Also, all structures, systems, storing units and software regarding remote programmable sim technologies (e-sim) must be established in Turkey, and data must be kept in Turkey.

As per the Regulation on the Registration of Devices with Electronic Identity Information of 12 July 2014, devices that communicate without voice communication (starting a voice call, ending a voice call and initiating a short message) and with electronic identity information that receive international permanent data

roaming service and devices with electronic identity information used in the in-vehicle emergency call system (e-Call) are also subject to registration obligation. In this respect, if the IoT device receives permanent roaming service by leaving a trace on the network without voice communication (starting a voice call, ending a voice call, starting a short message) for more than 90 days cumulatively within 120 consecutive days, it will also be subject to a registration obligation.

5. Challenges with IT Service Agreements

5.1 Legal Framework Features

IT service agreements are not specifically regulated under Turkish law, and the IT service agreements are subject to general laws of obligation and commercial law, except those received by entities in regulated sectors.

The most important issue regarding IT service agreements is personal data protection. As explained under **6.1 Core Rules for Individual/Company Data**, cross-border personal data transfers are heavily restricted under the DP Law. In this regard, cloud-based IT services in particular will be subject to these cross-border personal data transfer rules if their servers are located abroad.

In regulated sectors, the outsourcing and receiving of IT services are also regulated. The principles regarding the IT service provision and the minimum content of the service agreements are regulated in the BRSA Regulations and the CMB Communiqué. As explained in **1.1 Laws and Regulations**, in any case primary and secondary systems must be kept in Turkey.

IT service agreements regarding payment services are regulated under the Payment Law and secondary legislation. As per the Payment Law, agreements between payment and settlement system providers and the participants can only be concluded with the prior approval of the Central Bank of the Republic of Turkey (CBRT). The minimum content and other requirements for framework agreements between the payment service provider and the customer are also regulated under the Payment Law.

It should be kept in mind that, as per the Circular (see **1.1 Laws and Regulations**), operators that are authorised to provide communication services are obliged to establish an internet exchange point in Turkey. Necessary measures must be taken to prevent the export of domestic communication traffic that should be exchanged domestically. Also, in those regions where critical institutions are located, operators must transmit data on fibre optic cables instead of through methods such as radio links. In critical data communication, radio link communication must not be used; however, in cases where such use is inevitable, data must be encrypted using devices that hold national encryption systems.

6. Key Data Protection Principles

6.1 Core Rules for Individual/Company Data

Personal data is defined under the DP Law as any information relating to an identified or identifiable real person. Any information that can be used to identify an individual would constitute personal data - eg, a customer's name and address, IP address, email address or a database of customer email addresses. On the other hand, the data of a company is not regarded as personal data unless it consists of any information that can be used to identify an individual.

Under the DP Law, a data controller is the responsible party and addressee of the obligations. "Data controller" is defined as a real person or entity who determines the intended purposes and means of processing personal data. Data controllers are responsible for establishing and administering data registry systems.

The following key principles need to be followed in all personal data processing activities (Article 4 of the DP Law) performed by data controllers. Personal data must be:

- processed lawfully and fairly;
- accurate and, where necessary, kept up to date;
- processed for specified, explicit and legitimate purposes;
- relevant, limited and proportionate to the purposes for which it is processed; and
- retained for the period determined by relevant legislation, or as deemed necessary for the purpose of the data processing.

In addition to these main principles, current legislation provides various legal grounds for processing personal data and special categories of personal data to ensure adequate protection under the DP Law.

Article 5 of the DP Law states the legal basis for data processing, according to which personal data can be processed in the following cases:

- if the data subject has given their explicit consent;
- if it is explicitly permitted by law;
- if it is mandatory for the protection of life or to prevent the physical injury of a person, where that person is physically or legally incapable of providing their consent;
- if the processing of personal data belonging to the parties to a contract is necessary, provided that it is directly related to the execution or performance of that contract;
- if it is mandatory in order for the data controller to fulfil its legal obligations;
- if the personal data was previously publicised by the data subjects themselves;
- if it is mandatory for the establishment, exercise or protection of certain rights; and
- if it is vital to the legitimate interests of the data controller, provided, however, that the fundamental rights and freedoms of the data subject are not compromised.

Narrow legal grounds have been introduced for the processing of special categories of personal data.

To ensure transparency, it is mandatory under Article 10 of the DP Law for a data processor to inform the data subject of the following when collecting personal data, regardless of the legal basis for data processing:

- the identity of the data controller and its representative, if any;
- the purpose of the personal data processing;
- the recipients to whom the personal data can be transferred, and the purpose of the transfer;
- the methods of and legal reasons for collecting personal data; and
- the rights of the data subject under the DP Law.

This obligation to inform is not subject to a request from the data subject and must be fulfilled no later than the time of obtaining the personal data.

The DP Law stipulates the same circumstances for processing personal data and transferring personal data inside Turkey (Article 8 of the DP Law). In this regard, one of the conditions for data processing listed above must be met in order to transfer personal data inside Turkey to a data controller or a data processor.

A cross-border transfer may take place if the data subject has given their explicit consent. If the cross-border transaction is based on one of the conditions other than explicit consent, the following applies:

- the receiving country must be accepted as a country with an adequate level of data protection by the Board; or
- if the level of data security is not adequate, then the data transferor in Turkey and the data receiver abroad (data controller or processor) must execute a written undertaking letter (the minimum content of which is already determined by the Board) and seek the approval of the Board for the data transfer.

The list of countries with an adequate level of protection has yet to be published by the Board, so explicit consent and undertaking are the available options for data transfers.

Data controllers are obliged to notify data subjects and the Board within the shortest possible timeframe if processed data is collected by parties through unlawful methods. When necessary, the Board may announce such breach on its official website or through other methods it deems appropriate.

Data controllers are also obliged to register on the data controllers registry system (VERBİS), which is an online registration system where data controllers record their data processing activities. In principle, all data controllers are required to register with VERBİS before processing personal data (Article 16 of the DP Law), but the Board may grant exemptions, at its discretion.

In this regard, the Board has issued decisions granting exemptions from the VERBİS registration requirement to certain professional groups, associations and political parties. It has also granted a general exemption to local data controllers with fewer than 50 employees annually, or whose annual balance is below TRY25 million.

A local data controller with employees or revenue in excess of these thresholds must register with VERBİS unless they fall within another exception, or unless one is granted by the Board on other grounds.

Notably, data controllers abroad processing data from Turkey must register with VERBİS without exception.

7. Monitoring and Limiting of Employee Use of Computer Resources

7.1 Key Restrictions

Monitoring and limiting the use by employees of company computer resources is mainly covered by data protection and employment laws. However, the Constitutional Court of Turkey (Court) has also published several decisions regarding the monitoring of employee computers. The Court is the final domestic destination under Turkish law for the examination of whether a person's fundamental rights arising from the constitution are being infringe; its decisions are final and binding for the case. Although the decisions are only binding for that specific case, judges usually consider the Court's decisions while delivering a verdict, as the issue may be reviewed by the Court in the end.

The Kara/Özbek decision numbered 2013/4825 was a famous decision delivered by the Court before the landmark Bărbulescu v Romania decision of the European Court of Human Rights in 2017, discussing the

surveillance of employees' communication. According to the Kara/Özbek decision, the employer's surveillance of email contents did not violate the employee's freedom of communication and the privacy of his private life on the conditions that:

- the employer has a legitimate interest in reviewing the contents of e-mail;
- the measures applied by the employer are proportionate to the employer's legitimate interest;
- the employees are bound by the rules and regulations of the workplace, which outline the employer's legitimate interest as well as the employer's email surveillance practice; and
- employees are warned by the employer that corporate emails are restricted for private communications or use.

However, in the Court's decision (Decision) dated 17 September 2020, published in Official Gazette No 31274, dated 14 October 2020, the Court aligned its approach with that of the ECHR, as can be observed in the Bărbulescu v Romania judgment. Although reaffirming the main principles set in its Kara/Özbek decision, the Court departed from its previous approach of requiring employers to exclude or prohibit the private and personal use of corporate email accounts as an element of the surveillance. According to the Decision, the following must occur in order for the monitoring to be legal:

- the employer must have a legitimate interest in monitoring communication and must consider whether this interest can be pursued by only monitoring the flow of the communication or by monitoring the content of the communication;
- the employees must be informed by the employer beforehand about the surveillance, its purposes, its legal grounds, its scope, its results and their rights;
- the invasion of the employee's privacy must be paramount to accomplishing the purpose of the surveillance;
- the invasion must be compulsory for the purpose of the surveillance and the same results must not be able to be accomplished by other means that require less personal data to be processed or mean that data will be processed less intensely;
- the data to be collected must be limited by the purpose of the surveillance - no excessive data processing must take place; and
- the legitimate interest of the employer must be balanced with the employee's fundamental rights and freedoms.

Following this Decision, in the decision numbered 2018/31036 and dated 12 January 2021, the Court decided that the employer, a private bank, had a legitimate business interest in the surveillance of employees' emails and found no violation of employee privacy or freedom of communication, because the employer had informed employees of the surveillance of their email, and because the surveillance was proportional under the circumstances, considering that the employer used only emails indicating the applicant's engagement in commercial activities to support its claim.

Considering these decisions and the DP Law, informing is an essential part of personal data processing. It is important to contain provisions in the employment contract and employment information notice regarding the monitoring of correspondences and personal data that may be processed for internal control purposes.

In this regard, web traffic monitoring and tools to detect extensive private email use can be used for the protection of company data, as long as the principles listed in the Decision and Article 4 of the DP Law are followed and the employees are informed beforehand.

There is no obstacle to or regulation of data loss prevention tool, the use of which is supported by the Board as it is considered a technical measure.

8. Scope of Telecommunications Regime

8.1 Scope of Telecommunications Rules and Approval Requirements

Telecommunications is a highly regulated sector under Turkish Law, with the ECL being the main legislative document and ICTA being the national regulatory agency for the supervision of the sector and execution of the ECL. The telecommunications sector is regulated by licensing, authorisation, notification and other control mechanisms regarding the establishment, conduct and structure of companies.

Electronic communications services could be provided and/or electronic communications networks or infrastructure could be constructed and operated upon receiving authorisation from ICTA.

It is fundamental that the electronic communications service and/or network or infrastructure is provided primarily by operators that are authorised by ICTA.

Nevertheless, the following electronic communications services and/or networks or infrastructure are not subject to authorisation:

- those that are within any natural person's or legal entity's property under their own use and do not exceed any property's borders, which are used for individual or organisational needs exclusively, which are not used to provide any electronic communications services to third parties, which are provided without any commercial intention and which are not publicly available; and
- those that are constructed pertaining solely to the services of public corporations and institutions in accordance with the specific laws thereof.

VoIP and instant messaging services fall within the scope of the authorisation obligation. Although ICTA tends to consider those services under the authorisation obligation, there is no public information regarding any sanctions imposed on instant messaging and VoIP services. RFID tags seem less likely to be regarded as electronic communication devices, but electronic communication is very widely defined under the ECL as the transmission, exchange and receiving of all kinds of signals, symbols, sounds, images and data that could be converted into electrical signals, by means of cable, radio, optic, electric, magnetic, electromagnetic, electrochemical, electromechanical and other types of transmission systems. Therefore, in a wider interpretation, they may also be regarded as electronic communication devices.

Authorisation is issued on the basis of notification or rights of use. Companies that are willing to provide electronic communications services and/or to construct and operate electronic communications networks or infrastructure must notify ICTA of their intention to do so prior to the commencement of activities. When companies that have notified ICTA do not need the assignment of resources such as number, frequency and satellite position for electronic communications services and/or electronic communications network or infrastructure that they plan to provide and/or to operate, they are authorised pursuant to the notification to ICTA.

If they do need the assignment of resources, they are authorised upon receiving the right of use from ICTA.

ICTA issues right of use within 30 days upon due application for electronic communications services for which the number of rights of use does not need to be limited. The number of rights of use could only be limited when the resources need to be operated by a limited number of operators and for the aim of ensuring the efficient and effective use of resources. In such a case, allocation is made through public tenders.

The durations of rights of use are not to exceed 25 years. The duration of authorisation is determined by taking into consideration the qualification of the service and network and the request of the applicant.

ICTA is entitled to reject applications for rights of use due to the insufficiency of resources and the non-availability of the qualification requirements specified in the tender stage, and on grounds related to national security, public order, public health and similar public interests.

The authorisation fee consists of administrative charges and fees for rights of use.

In order to contribute to the expenses arising from market analysis, the preparation and implementation of regulations, the supervision of operators, technical monitoring and supervision services, market control, international co-operation, harmonisation and standardisation studies and other activities, and all kinds of administrative expenses, ICTA receives administrative fees from the operators, not to exceed 0.35% of the net sales of the operator in the previous year. However, the annual administrative fee cannot be less than the lower limit of TRY16.547.

9. Audio-Visual Services and Video Channels

9.1 Audio-Visual Service Requirements and Applicability

The legal framework for media in Turkey is regulated by the following various acts and regulations instead of a single unified media law:

- Law No 6112 on the Establishment of Radio and Television Enterprises and Their Media Services (Media Law);
- Press Law No 5187;
- Law No 5651;
- the ECL;
- the Copyright Law;
- the IP Law;
- the Regulation on the Provision of Radio, Television and On-demand Media Services Via Internet Environment, published in the Official Gazette No 28444 (OTT Regulation);
- the Regulation on the Principles and Procedures in Relation to the Rating and Monitoring of the Viewing and Listening of Broadcast Services, published in Official Gazette No 28444;
- the Regulation on the Procedures and Principles of Media Services, published in Official Gazette No 28103;
- the Regulation on Broadcasting via Cable Networks, published in Official Gazette No 27965;
- the Regulation on Broadcasting Via Satellite, published in Official Gazette No 27965; and
- the Regulation on the Principles and Procedures Relating to the Implementation of Multiple Partnerships With Media Service Providers, published in Official Gazette No 28144.

In the broadcasting industry, the Media Law mainly provides the governing regulatory provisions. On 3 March 2018, the Media Law was amended to introduce licensing requirements for online broadcasts, and the OTT

Regulation was subsequently enacted on 1 August 2019.

Broadcasting services can only be provided with a licence obtained from the Radio and Television Supreme Council (RTÜK). Media service providers must apply to the RTÜK for a separate licence for each broadcasting technique and network in order to be able to broadcast through cable, satellite, terrestrial and similar networks. The licence document must clearly indicate which broadcasting technique and network the licence is granted for. Enterprises requesting to make simultaneous broadcasts on different networks by different techniques must apply for separate licences for each broadcasting technique and network.

The term of the broadcasting licence is ten years. The terrestrial broadcast capacity that becomes available at the end of the licence term must again be put out to tender by the RTÜK. Any enterprise to which the RTÜK has granted a terrestrial broadcasting licence cannot transfer its licence rights. An enterprise that decides to cease its broadcasting activity must return its licence to the RTÜK.

A broadcasting licence can only be granted to incorporations that are established in accordance with the provisions of Commercial Law No 6102 for the purpose of exclusively providing radio broadcasting service, television broadcasting service and on-demand media service. A single company can provide only one radio broadcasting service, one television broadcasting service and one on-demand media service. Media service providers cannot insert any provisions contrary to the principles stipulated in this article into their articles of association after the broadcasting licence has been granted. Articles of association amendments must be reported to the RTÜK within one month.

Political parties, labour unions, professional associations, co-operatives, associations, societies, foundations, local administrations and companies established by such entities or of which they are direct or indirect shareholders, stock-broker companies and real or legal persons who are direct or indirect shareholders of these companies cannot not be granted broadcasting licence, and cannot directly or indirectly be shareholders of the media service providers.

The total direct foreign capital share in a media service provider cannot exceed 50% of the paid-in capital. A foreign real or legal person can directly become a partner of no more than two media service providers. If foreign real or legal persons hold shares in companies that are shareholders of media service providers and become indirect partners of the broadcasters, the chair, the deputy chair and the majority of the board of directors and the general director of the broadcasting enterprises have to be citizens of the Republic of Turkey, and the majority of the votes in the general assemblies of broadcasting enterprises must belong to Turkish real or legal persons. The arrangements ensuring these provisions must be stated clearly in the main contracts of such corporations.

In media services, broadcasts with generalist or thematic content can be made. Whilst applying for a broadcasting licence, media service providers must submit a written notification to the RTÜK about their type of broadcast. The type of the broadcast must be clearly stated in the broadcasting licence document to be granted to these enterprises by the RTÜK.

Broadcasting services must be made in accordance with the specified type and language informed to the RTÜK. Upon request, the type of broadcast can be changed with the permission of the RTÜK. Any enterprise that broadcasts contrary to the type specified in its licence will be deemed to have violated the terms of the broadcasting licence.

If generalist and thematic television enterprises provide animated cartoons in children's programmes, at least 20% of the animated cartoons and at least 40% of the other children's programmes must be productions made in the Turkish language and reflecting the Turkish culture. Statistical data on the broadcasting hours and durations of children's programmes and details about the place of production must be reported to the RTÜK in monthly schedules.

Radio and television enterprises must provide Turkish folk music and Turkish art music in their broadcasts at specified percentages and hours. The principles regarding the percentages and broadcasting hours of these programmes must be determined by the RTÜK.

The OTT Regulation and the Media Law are the main documents that regulate online broadcasting services.

Article 29/A of the Media Law and the OTT Regulation establish the principles and procedures regarding online broadcasting licences of media service providers, and broadcasting transmission authorisations of platform operators that carry out online television, radio or on-demand services. The OTT Regulation also applies to foreign service providers and operators that broadcast in the Turkish language from abroad or, regardless of the broadcasting language, those who target audiences in Turkey in their commercial publications.

According to Article 29/A of the Media Law, media service providers wishing to provide media services solely on the internet must obtain a licence from the RTÜK. However, if a media service provider already holds a broadcasting licence, no separate licence is required to provide media services on the internet.

Media services providers wishing to engage in online broadcasting must obtain the following separate broadcast licences from the RTÜK:

- for online radio services: INTERNET-RD broadcast licence;
- for television services: INTERNET-TV broadcast licence; and
- for on-demand broadcast services: INTERNET-İBYH broadcast licence.

A single media services provider is limited to one radio, one television and one on-demand service. Online broadcast licences are granted to companies for ten years. Platform operators broadcasting on their own websites or mobile applications must be authorised by the RTÜK.

Foreign media service providers wishing to broadcast in Turkey and in a language other than Turkish must also be licensed. A foreign entity should begin the licensing process by legally establishing its business in Turkey.

With all other internet contents, online media services are also regulated under Law No 5651, which regulates the obligations of content providers, hosting providers, internet providers and social network providers, and states the following:

- content providers are required to provide information to ICTA if requested (Article 4);
- hosting providers are required to provide information to ICTA if requested, and to retain traffic data about their hosting activities (Article 5);
- access providers are required to block alternative access methods and to provide information to ICTA if requested (Article 6); and
- mass-use providers are required to take measures to prevent users accessing criminal content (Article 7).

Social Network Providers are obliged to respond to individual requests within 48 hours, complying with content removal and access prevention measures, and providing regular reports including statistical and categorical information containing the foregoing (Additional Article 4).

Social network providers abroad that have more than 1 million daily accesses from Turkey are required to appoint local representatives, who are responsible for accepting notices, notifications and requests from administrative and judicial authorities in Turkey, responding to individual applications and fulfilling other obligations under Law No 5651.

10. Encryption Requirements

10.1 Legal Requirements and Exemptions

Article 12 of the DP Law requires controllers to take all necessary technical and administrative measures to provide a sufficient level of security in order to prevent unlawful processing and unlawful access, and to ensure the retention of personal data. However, the DP Law does not detail the minimum requirements for complying with this rule. The Turkish parliament preferred, in fact, to refrain from limiting the measures to be taken by data controllers and instead required data controllers to take any and all measures required to protect the data, without limitation.

This being said, the Board has published the Guideline on Personal Data Security (Technical and Organisational Measures) (DP Guideline) to guide data controllers on the following technical measures to be taken to protect personal data:

- authority matrix;
- authority control;
- access logs;
- user account management;
- network security;
- application security;
- encryption;
- penetration test;
- intrusion detection and prevention systems;
- log records;
- data masking;
- data loss prevention software;
- backup;
- firewalls;
- current anti-virus systems;
- deletion, destruction or anonymisation; and
- key management.

The Circular governs the security measures that should be taken by public institutions and operators providing critical infrastructure services in order to mitigate and eliminate the security risks faced in information systems and to secure the critical data that could jeopardise national security or cause the destruction of public order when their privacy, integrity and accessibility are compromised.

The Circular details the following:

- at points where classified information is processed by public institutions and organisations, dissemination security (TEMPEST) or similar security measures must be taken;
- portable devices (laptops, mobile devices, external memory/discs, CD/DVDs, etc) with uncertain origins, including those personally used, must not be connected to institutional systems. Devices storing classified data must be taken outside the institution only once the data contained in terms of hardware and/or software is encrypted, and devices used for this aim must be recorded;
- the development of local and national encryption systems must be encouraged, and institutions' classified communication must be conducted on such systems; and
- the settings of public email systems must be configured to be secure; email servers must be hosted within Turkey and under the control of the institution; and communication between servers must be conducted in an encrypted form.

New information systems to be established in all public institutions and organisations as well as enterprises providing critical infrastructure services must comply with the procedures and principles set forth in the Circular and the guidelines prepared based on the Circular.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

COVID-19-related legislative acts in the TMT sector mostly concerned activities that may be conducted remotely that were previously conducted face-to-face.

The Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relations in Electronic Environment was published in Official Gazette No 31441, dated 1 April 2021. With the regulation, it became possible to perform identity verification proceedings by video calls online without the need for the customer representative and the customer to be physically present in the same environment. In addition, after identity verification was made remotely or through branches, it became possible to establish remote banking contracts.

The Regulation on Verification Process of the Applicant's Identity in the Electronic Communications Sector (RIR) was introduced in Official Gazette No 31523, dated 26 June 2021. According to the RIR, only the following channels can be used for identification verification:

- e-Government gateway;
- visual verification by AI or an authorised person, together with a document with a near field communication feature in accordance with the ICAO 9303 standard;
- creating PAdES with a Republic of Turkey ID Card; and
- taking video footage that is specific to the process with the applicant's identity document in face-to-face channels - the Regulation allows AI to compare the face in the live image with the photograph in the identity document.

On 19 August 2021, the BRSA published the Draft Regulation on the Operating Principles of Digital Banks and Service Model Banking (DBDR), and opened it for public opinion. The DBDR aims to determine the operating principles of branchless banks that serve exclusively through digital channels and the conditions for the provision of the banking as a service model to businesses and innovative enterprises (ie, start-ups).

**This content was originally published in Chambers and Partners' TMT Guide.*

Related Practices

- R&D, Licensing and Technology Transactions
- Privacy and Data Protection
- Domain Names and Internet Infringement
- IP Litigation
- IP Licensing
- Copyrights

Related Attorneys

- BURCU TUZCU ERSİN, LL.M.
- EZGİ BAKLACI GÜLKOKAR, LL.M.
- ECE BERKMAN
- CEYLAN NECİPOĞLU, Ph.D, LL.M.