MOROĞLU ARSEVEN

Chambers and Partners TMT 2022 Guide – Trends and Development: Cybercrime under Turkish Law

16 Mar 2022

Cybercrime under Turkish Law

Introduction

Cybercrime is a rising trend around the world, and is one of the fastest growing transnational offences in Interpol member countries. As a consequence, damages arising from cybercrime are also rising. For 2021, the annual cost of cybercrime was predicted to be USD6 trillion, doubling since 2015 and becoming the world's third largest economy after the United States and China. The cost of cybercrime is predicted to reach USD10 trillion by 2025.

In the World Economic Forum's The Global Risks Report 2021, 39% of the respondents predicted that cybersecurity failure will become a clear and present danger within two years, while 49% saw it as a medium-term risk within three to five years. 50.2% of respondents predicted that the advance of adverse tech will become a critical threat within five to ten years.

As one of the fastest growing and most concerning threats, cybercrime has become a priority for policy makers around the world.

Cybercrime does not have a universally accepted definition. In legal documents, the key terms and concepts and specific cyber-offence types are usually defined. For example, "computer system" or "information system" are defined and specific types of acts against or by using these systems are criminalised. This approach is also adopted by Turkish Penal Code No 5237 (Penal Code) and the Budapest Convention on Cybercrimes (ETS No 185) of 2001 (Budapest Convention), which is the first international legal document regarding cybercrime and aims to pursue a common criminal policy to protect society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation.

Turkey signed the Budapest Convention on 10 November 2004, which was ratified on 22 April 2014 and finally become effective as of 1 January 2015. In respect of the substantial criminal law section of the Budapest Convention, Turkish law mostly addresses the illegal access, illegal interception, data interference, system interference, misuse of devices and IP rights offences. Although computer-related forgery and computer-related fraud are not defined as a separate type of crime but are instead regulated as a matter of aggravation, Turkish law also meets the requirements regarding these offences.

Cybercrime is not a new concept in Turkish law, with the first regulations regarding cybercrime being added to Turkish Penal Code No 765 in 1991. These amendments added the phrase "the system that automatically processes information" to Turkish Penal Code No 765, and outlawed the acquisition of data from these systems, along with damaging the system or data it contains to gain a benefit, and placing data on a system to constitute judicial evidence. Provisions on informatics have since been added to many laws.

The most comprehensive cybercrime regulation came with the enactment of the new Penal Code in 2005. Section 10 of the Penal Code, titled Crimes in Information Technologies Field, listed certain offences in the information technologies field, but cybercrime is not limited to those listed offences. In other articles of the Penal Code, offences

regarding information technology are defined as either matters of aggravation in relation to certain offences or as separate offences.

In this regard, a distinction can be made between pure cybercrimes and cyber-enabled crimes. Pure cybercrimes are dependent on a computer or information system to be committed. The offences defined under Section 10 of the Penal Code are examples of these kind of cybercrimes. On the other hand, cyber-enabled crimes are traditional offences that are facilitated by or committed through information systems, such as online fraud, money laundering or illegal online gambling.

According to 2019 data, the most commonly prosecuted type of pure cybercrime in Turkey is the misuse of debit or credit cards, with 75,852 cases - almost triple the total number of prosecution cases of other pure cybercrimes. Unlawful access accounts for 9,442 cases, and disruption, corrupting, destruction or modifying the system account for 15,161. There were no cases of using forbidden devices and programs.

In certain cases, a continuous act may constitute several offences while also constituting a cybercrime. For example, if a device or a system is damaged (either physically due to heat or by preventing it from exercising its functions) due to malware, the offences of corruption of a system and damage to property would be committed at the same time. As per the Penal Code, compound offences are offences consisting of two or more acts, one of which constitutes an element of reason of aggravation of the other. In these cases, only one offence is committed. For instance, using information systems for theft is defined as a reason of aggravation for theft. Therefore, the offender will only be prosecuted for aggravated theft, which can also be grouped as a cyber-enabled crime. On the other hand, if no such relationship exists between the two acts, then a person who causes more than one offence to occur with a single act is punished for the offence that requires the heaviest penalty. In the example above, where both damage to property and corruption of a system occur, the offender will only be prosecuted for the offence that requires the heaviest penalty.

This article will first examine the pure cybercrimes defined under Section 10 of the Penal Code and then provide some brief information on common types of cyber-enabled crimes.

Unlawful Access to an Information System

Article 243 of the Penal Code outlaws unlawful and unauthorised access to an information system. In the preamble, information systems are defined as "magnetic systems that allow automatic processing of data after collecting and placing it". However, this definition is criticised by certain scholars as magnetic compounds of an information systems can be limited or non-existing in some cases. Therefore, information systems should not be limited to those magnetic systems - those that allow automatic processing of data should also be considered to be within the scope of unlawful access.

The offence is commissioned by accessing the information system partially or fully. Once the access is achieved, the offence is completed; therefore, the offence does not actually require any harm to be done to the systems or the data integrity. However, if the data in the system is corrupted or lost as a result of the access, then the action will be sanctioned with imprisonment for six months to two years, while simple unlawful access can lead to imprisonment for up to one year.

At this point, the state of mind of the offender is important. If the offender acts with the intention to corrupt or destroy the data, then another type of offence under Article 244 may be committed: that of "blocking, corrupting, destroying or modifying the system". If the data is corrupted or destroyed as a result of the unlawful access, even if the offender did not intend such, then unlawful access will be the offence committed, with aggravated punishment. Also, it is irrelevant whether the system is accessed to obtain certain data with respect to this offence. On the other hand, if an offender fails to complete an offence they intend to commit directly with appropriate actions for reasons beyond their control, they will be held responsible for the attempt.

Unlawful monitoring of data transmissions within an information system or between information systems, without entering the system, is also included in the definition of unlawful access under Article 243, and is defined as a matter of aggravation. While simple unlawful access to an information system calls for imprisonment or a judicial fine of up to one year, the monitoring of data transmission, or traffic data, calls for imprisonment ranging from one year to three years.

On the contrary, unlawful access to paid systems is considered a matter of extenuation. In this respect, unlawful access to systems that should only be accessed through making a payment requires a lesser sanction. The sanction that will be applied for illegal access to paid systems is half the sanction that will be applied to illegal access to systems. However, it should be noted that benefitting from telephone lines and frequencies or encrypted or unencrypted broadcasts made by electromagnetic waves without the consent of the owner or the possessor is defined as a separate offence under Article 163, so will not be considered to be within the scope of Article 243.

Anyone can be a victim of this offence, including legal persons whose systems are accessed without authorisation. For instance, access to a database or traffic data belonging to a natural person's systems can constitute an offence. The victim, however, does not have to be the owner of the system - system users such as social media account users can be the victim of this offence.

The offender can also be any natural person, and no special title, skill or profession is required; anyone with simple technical knowledge and the intention to access can commit this offence. Although legal persons cannot commit an offence, specific security measures can be taken against a legal person if unlawful access is committed for the benefit of the legal person.

Unlawful access includes entering and/or staying in the information systems. According to the Turkish Court of Cassation 8th Criminal Chamber's decision no E.2013/10402 of 7 May 2014, entering an information system is accessing some or all of the data therein, physically or remotely, using another device. Access can be achieved through exploiting loose security measures and loopholes in existing security measures. It is possible to log in via the network by using viruses, trojan horses, macro viruses or worms, or by forcing open the doors of the system. This offence can be in the form of opening someone else's computer and seeing the data inside, or it can be committed by logging into the information system through a network. For unlawful access, there is no difference if the communication being wired or wireless, nor if the distance is near or far. Sending an email or a file to an information system cannot be considered to come within the scope of unlawful access, since only the data is sent, with no access to the information system. It will also constitute an offence if another internet user enters the operating system (Windows, Linux, etc) of the victim's personal computer without the victim's consent.

Disrupting, Corrupting, Destroying or Modifying the System

Article 244 of the Penal Code outlaws blocking, corrupting, destroying or modifying a system:

- blocking or disrupting the operation of an information system is prohibited by the first paragraph, requiring imprisonment from one year to five years; and
- corrupting, destroying, changing or rendering inaccessible data in an information system, or injecting data on a system, or transferring existing data to another place are all prohibited by the second paragraph, requiring imprisonment from six months to three years.

From the preamble of Article 244, it can be understood that the damaging acts directed against the systems are aimed to be defined as a specific offence separate from property damage. The physical existence of the device and all other elements that enable it to function are subject to Article 244.

Blocking, corrupting, destroying or modifying a system is usually committed via an active action; however, in some cases, it can also be committed by the negligence of the offender without a positive act, such as when the technical support person deliberately fails to install the necessary software on the system to prevent a virus attack or leaves the system vulnerable to external attack.

The acts that may result in the offence defined under the first paragraph are rather broad. Any intervention in the information system that disrupts or blocks data processing and, in this sense, actions that damage the system and its elements or prevent the system from functioning fall under the concept of preventing the operation of the system.

The first paragraph outlaws two actions against information systems: blocking and disrupting the operation of the system.

Any acts that do not disrupt the system but prevent it from performing its normal functions can constitute blocking of the information system - eg, the system may work slower, cannot exchange data, cannot run various programs at all or as required, or in any way cannot properly perform its functions that it can perform under normal conditions as a result of the unlawful acts. In this case, although the system is not disrupted fully, the offender prevents its functioning. It is irrelevant whether the act of blocking is temporary or permanent in terms of the occurrence of the offence.

The term "disrupting" means making the information system incapable of doing the job expected from it - in other words, disrupting the functioning of the information system, rendering the system partially or completely inoperable. How the disruption is accomplished is irrelevant. The functioning of the information system can be disrupted by interfering with the intangible elements of the system without harming its physical existence or by damaging its physical elements.

As explained above, Paragraph 2 sets forth certain provisions for the protection of data kept in the information systems. In this regard, a person who corrupts, destroys, changes or renders inaccessible data in an information system, places data on the system or sends existing data to another place is sentenced to imprisonment from six months to three years.

The corruption of data is damage to the usability of data - ie, damaging the data in a way that will completely or partially prevent the use of the data for its determined purpose. Examples include damaging the usability of data by changing the places of interconnected data sentences, confusing their meaning or adding additional things, or deleting individual data from data sentences.

Destroying the data is rendering the data inaccessible. The difference from corrupting the data is that destroying takes data beyond the reach of the data owner - eg, deleting keys for encrypted data may also be regarded as destroying data as encrypted data cannot be used by the data owner without keys. Whether the data must be destroyed in a way that renders it incapable of restoration through simple methods in order for the destruction to have occurred remains a controversial point. Some opinions suggest that data is not destroyed if it can be restored by the data owner, while others suggest that an act of deleting data must be regarded as destruction as the data is rendered inaccessible by the data owner until it is recovered.

Changing data means changing the content of the data sets stored in the information systems - eg, changing the content, converting it to another program language code, or changing the password and plain text.

Rendering the data inaccessible means preventing the owner or the related person from accessing the data they want at any time. In terms of accessibility, there is no difference between whether the prevention of access is temporary or permanent. In rendering data inaccessible, although the integrity of the data is preserved (not corrupted/destroyed), the data owners cannot access their data for various reasons, such as virus infection, password setting, etc. In this regard, the Turkish Court of Cassation considers the change of password of social media or email accounts as rendering data inaccessible, as in the 8th Criminal Chamber's decision no E. 2015/11993 of 17 March 2016.

Injecting data on the system is placing data on a system that was not previously there. The injecting may include actions such as uploading, saving or adding data without the consent of the system owner, which takes place directly or indirectly by any technological means.

Transferring existing data to another place is sending data from one system to another system over telecommunication paths or within the existing network.

Anyone can be a victim of this offence, including legal persons whose data is subjected to any of the acts explained above. For instance, the destruction of data in a database or social media accounts belonging to a natural person can constitute this particular type of offence. The victim, however, does not have to be the owner of the system, but can also be system users such as social media account users.

The offender can also be any natural person, and no special title, skill or profession is required: anyone with limited technical knowledge and the intention to access can commit this offence. Although legal persons cannot commit an offence, specific security measures can be taken against a legal person if unlawful access is committed for the benefit of the legal person.

According to the third paragraph, if these acts are committed on the information system of a bank or credit institution or a public institution, the penalty to be imposed is increased by half. According to the fourth paragraph, if the offender gaining an unfair advantage for themselves or someone else by committing the acts explained above does not constitute another offence, they are sentenced to imprisonment from two to six years and a judicial fine of up to 5,000 days.

Misuse of Debit or Credit Cards

The misuse of debit or credit cards is also regulated under Section 10 of the Penal Code, titled Crimes in Information Technologies Field.

As per the first paragraph of Article 245, if a person who seizes or holds a bank or credit card belonging to another person, for any reason, uses it or makes someone else use it without the consent of the cardholder or the person to whom the card is to be given, that person is sanctioned with imprisonment from three years to six years and a fine of up to 5,000 days.

As per the second paragraph, a person who produces, sells, transfers, buys or accepts fake bank or credit cards by associating with the bank accounts of others is punished with imprisonment from three to seven years and a judicial fine of up to 10,000 days.

According to the third paragraph, a person who benefits themselves or someone else by using a bank or credit card that is fraudulently created or forged is sentenced to imprisonment from four to eight years and a judicial fine of up to 5,000 days, unless the act does not constitute another offence requiring a heavier penalty.

The legal interests sought to be protected by Article 245 are the same as those that are sought to be protected against offences such as theft, fraud, abuse of trust and forgery. The following legal interests are sought to be protected in the following offences:

- theft and fraud: the right to property;
- abuse of trust: personal trust; and
- forgery: trust in the legal system and the credibility of documents.

The most dominant legal interest protected by Article 245 is the right to property.

Anyone holding a credit or debit card can be the victim of this offence. In this regard, the victims are natural or legal persons who are depositors of an account to which the bank or credit card is linked, and the banks and credit institutions are the persons affected by the offence.

The offender can also be any natural person, and no special title, skill or profession is required. Although legal persons cannot commit an offence, specific security measures can be taken against a legal person if unlawful access

is committed for the benefit of said person.

On the other hand, no sanction is imposed if the acts defined under the first paragraph are committed against the following:

- a separated spouse;
- the parent or descendant of one of the offender's in-law relatives to this degree, or the adopter or adopted of the offender; or
- a sibling living in the same residence.

Forbidden Devices or Programs

Finally, as per Article 245/A, if a device, computer program, password or other security code is made or created exclusively for the commission of offences under Section 10 of the Penal Code and other offences that can be committed by using information systems as a tool, a person who manufactures, imports, forwards, transports, stores, accepts, sells, offers for sale, buys, gives to others or keeps such is punished with imprisonment from one year to three years and a judicial fine of up to 5,000 days.

In the formation of the offence defined in the article, the person's intent to commit an offence must be taken into account. If such devices and programs are made or created to test the security of information systems, the specified offence will not occur. For instance, if the tools belonging to companies that perform penetration/vulnerability testing (pentest) are used within the framework of the contract signed with the information system owner, an offence will not be committed.

Cyber-enabled Crimes

As discussed above, cyber-enabled crimes are traditional offences committed through or facilitated by information systems. Any offence committed through information systems can be considered a cyber-enabled crime, whether it is defined under the Penal Code or other laws; therefore, it is not possible to limit those. On the other hand, certain types of cyber-enabled crimes are defined under the Penal Code, such as theft by using information systems, fraud by using information systems or by using banks or credit institutions as a vehicle, or providing space for illegal gambling through information systems.

The illegal use of information systems is regulated as an aggravation. Therefore, offenders will be prosecuted for only the aggregated offence.

Conclusion

Cybercrime is a rising trend, and it will only grow as technology is surrounding us more and more each day. Therefore, policymakers are expected to bring in new rules addressing current needs. Turkish law will also be affected by these changes.

Apart from growing technologies, the most expected change is the ratification of the Budapest Convention, which has been the subject of Commission Staff Working Document reports of the European Commission. The Turkey 2021 report states that no progress was made towards the ratification of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Also, according to the report, efforts are needed to improve the legislation on cybercrime, among other topics. In this regard, changes to the Penal Code can be expected in the future, in order for Turkey to have European-aligned legislation.

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

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.
- BURCU GÜRAY
- CEYLAN NEC?PO?LU, Ph.D, LL.M.