An emerging market perspective on the convention on cybercrime: cyber laws and Turkey's progress

Gönenç Gürkaynak
ELIG, Istanbul
gonenc.gurkaynak@elig.com

İlay Yılmaz
ELIG, Istanbul
ilay.yilmaz@elig.com

Derya Durlu
ELIG, Istanbul
derya.durlu@elig.com

The Convention on Cybercrime of the Council of Europe ('Convention')[1] serves as a valuable guidance to many nations whose national legislative framework on cybercrimes require regulatory provisions on legal issues relating to cybercrimes. The Convention's significance has increased over the years, with the internet, as a medium, becoming indispensable, and criminal acts committed online becoming more prevalent.

As of 31 January 2013, 35 member states of the Council of Europe out of the 47 have ratified the Convention, which is a clear indication of the growing need to have effective local regulatory mechanisms to combat online criminal activity. Turkey signed the Convention in 2010, but has not yet ratified it.

The proliferation of computer-related criminal activity requires a transnational, harmonised and technologically acute understanding of implementing local legal rules that are implemented correctly and effectively by local courts as well as enforcement agencies, on the one hand, and aligned with international conventions, on the other.

This article addresses the Convention as it regulates cybercrimes and highlights the current state of play in Turkey on the regulatory architecture of cybercrime.

Cybercrimes and the Convention at a glance

The term 'cybercrime' has been understood as either a computer crime or as a computer-related crime.[2] Against this backdrop, the Convention emerged from the rationale of fighting cybercrime as not only a computer crime but also a computer-related crime, and that criminal laws should be sensitive to technological developments which 'offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests'.[3] This reasoning accepts the cross-border nature of information networks and sets the ground for the Convention to provide rules on questions of substantive and procedural law, as well as matters that are closely connected with the use of information technology.

The Convention is comprised of four main chapters – 'use of terms', 'measures to be taken at domestic level – substantive law and procedural law', 'international cooperation' and 'final clauses' – under which legal rules provide for the criminalisation of action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems and networks.[4]

The four types of substantive offences regulated in the Convention and that are prevalent on the internet are:

- offences against the confidentiality, integrity and availability of computer data and systems, comprising interference and misuse of devices;
- computer related offences such as forgery and computer fraud;
- content related offences, in particular the production, dissemination and possession of child pornography; and
- offences related to infringement of copyright.

As to the procedural elements of the Convention, expedited preservation of stored computer and traffic data, search and seizure of stored computer data and real time collection of traffic data are some of the wide reaching powers that are regulated with respect to enforcement authorities that investigate cybercrime.

A final topic of relevance is international cooperation, as regulated in the Convention, between states for all crimes regulated under the Convention and for gathering data and evidence in electronic form with respect to the relevant criminal offence. Given the cross-border nature of cybercrimes, there is a high potential for more than a single state to be

involved in the commission of a cybercrime. This brings forth the issue of how and to what extent states are required to cooperate in regards to acts that may have originated in other countries but that ultimately require their judicial and even their law enforcement agencies. Article 23 of the Convention sets out the general principles of mutual legal assistance and the obligations imposed upon members states:

> 'to cooperate with each other, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.'

Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the respective states, the Convention, under Article 27, establishes mutual rules under paragraphs 2 through 9 that will be applied when the European Convention on Mutual Assistance in Criminal Matters and its Protocol or other similar international conventions do not otherwise oblige the member states with respect to matters on mutual legal assistance.

Cybercrime legislation in Turkey and Turkey's progress

Turkey has progressed significantly in the past five years in regulating internet law matters in its legislative framework. With the promulgation of Law No 5651 on Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts ('Law No 5651') in 2007, and Turkey's signature to the Convention in 2010, integration with European and international communities has gained considerable momentum. The Turkish regulatory framework on cybercrimes has been in place since 1991, and these crimes were regulated more specifically when the new Turkish Criminal Law No 5237 ('Turkish Criminal Law') was promulgated as the legal lacuna on cybercrimes was in need of an effective regulation. The regulation of cybercrime, specifically within the Turkish Criminal Law in 2005, was among the first signs of Turkey's progress in this field and efforts in combating cybercrimes.

While Law No 5651 primarily draws the framework for the principles and procedures with respect to the obligations of content, hosting and access providers and removal of content for certain crimes committed on the internet,[5] the Turkish Criminal Law remains the primary law regulating cybercrimes.[6] Needless to say, there are still gaps within the Turkish Criminal Law where the regulation falls short of addressing the four offences as stipulated in the Convention. By ratifying or acceding to the Convention, Turkey will have to ensure that its domestic law (ie, the Turkish criminal law framework) criminalises the conduct described in Article 6 of the Convention (on 'misuse of devices'), as the Turkish Criminal Law does not currently criminalise the intentional commission of illegal behaviour with respect to certain devices that are used to commit offences regulated under the Convention.[7]

Concluding remarks

As soon as Turkey ratifies the Convention and it is duly put into effect, the Convention will carry the force of law and will constitute an integral part of the Turkish legislative landscape.[8] Given the cross-border nature of the internet, and the accessibility of content that is broadcasted on the internet, local regulations, particularly in emerging market economies, may be susceptible and malleable to the volatile nature of cybercrimes. With its transnational characteristic, the Convention's aim of facilitating harmonisation amongst different jurisdictions may have already borne its fruits with respect to Turkey, as Turkey gradually adapts its cyber law architecture to be on par with international standards.

Notes

1 European Council Convention on Cybercrime (CETS No 185) (adopted on 23 November 2001 and entered into force on 1 July 2004).

2 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10–17 April 2000, 'Crimes Related to Computer Networks: Background Paper for the Workshop on Crimes Related to Computer Network', p 5, available at **www.uncjin.org/Documents/congr10/10e.pdf** (defining computer crime as 'any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them', while defining computer-related crime as 'any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network';

See also Jonathon Clough, *Principles of Cybercrime* (Cambridge, 2010), p 10 (classifying cybercrimes under three sub-categories as (i) crimes in which a computerised device or network is the target of criminal activity; (ii) crimes where the computer is used to commit a recognised offence; and (iii) crimes in which the computer is incidental to the commission of a crime).

3 Council of Europe, Explanatory Report on Convention on Cybercrime (ETS No. 185) (available at **http://conventions.coe.int/Treaty/en/Reports/Html/185.htm**) (last visited: 30.01.2013)

4 Convention, Preamble, paragraph 9.

5 Article 1 ('Scope'), Law No 5651.

6 Articles 243–246, Turkish Criminal Law.

7 See Article 6 of the Convention

8 Article 90/4, Turkish Constitution ('*International treaties duly put into effect carry the force of law* – No appeal to the Constitutional Court can be made with regard to these treaties on the ground that they are unconstitutional. In case of a conflict between international treaties in the area of fundamental rights and freedoms duly put into effect and the laws due to differences in provisions on the same matter, the provisions of international treaties shall prevail.') (emphasis added).

Labour immigration in Kazakhstan

Yulia Chumachenko
AEQUITAS Law Firm, Almaty
y.chumachenko@aequitas.kz

Kazakhstan, as a young developing country rich in natural resources and pursuing foreign investor-favourable policies, is fairly attractive for business.

According to the World Bank's report, Kazakhstan ranked 49th in the 2012 Doing Business rating, up seven points compared to 2011 and ahead of some of its neighbours, for example, Russia (112th) and Kyrgyzstan (70th). According to the World Economic Forum data, Kazakhstan is ranked 51st in the 2012–2013 Global Competitiveness Index.

Investment activities in Kazakhstan often involve engagement of foreign specialists to supervise and manage foreign investors' business. Still, the local labour immigration policy is designed to protect the domestic labour market and ensure local labour employment, which finds has gained strength (especially over the past five years) in the formation of the qualitatively new directions in the immigration administration.

What one needs to know about foreign labour engagement in Kazakhstan?

The Kazakh legislation on immigrants (foreign nationals entering Kazakhstan to temporarily or permanently reside there), which was significantly changed in 2012 and has already changed in 2013, provides for various regulations, depending on the purpose of entry. The most common is labour immigration (entry for the purpose of carrying out labour activities), therefore, we will further specifically dwell on the status of labour immigrants (there exist other categories of immigrants, including business immigrants, oralmans and others, who have a special status and may be the subject of a separate review).

In order to carry out labour activities in Kazakhstan, it is necessary to perform the following key actions:

- obtain a work permit;
- obtain a visa (working or business); and
- register with the authorised agencies upon arrival into the Kazakhstan territory.

The labour immigrant's activities in Kazakhstan (including travel inside its territory) must strictly conform to the purpose of entry stated when obtaining the visa and specified in the work permit, with no other activities being allowed. Moreover, in the period of stay in the country, it is required to observe the local legislation in order to avoid imposition of sanctions and prohibition on future entries into the country.

General requirements to labour immigrants

As a prerequisite for foreign nationals to enter Kazakhstan for independent job placement or engagement by employers, they must:

- be of age;
- present a confirmation of their solvency required to exit the territory of Kazakhstan (in the amount of at least the economy airfare to the nearest airport of the country of the expat's permanent residence plus approximately US$25 per each day of stay);
- possess education, qualifications and experience necessary to perform their contemplated work;