Developments in the UAE Cyber crimes law

by Nick O'Connell - n.oconnell@tamimi.com - Riyadh

May 2013

In this article, we outline Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes. Better known as the Cyber Crimes Law 2012, the law - which came into effect in December 2012 - replaces the earlier Cyber Crimes Law 2006.

The Cyber Crimes Law 2012 provides for a range of new offences, including offences intended to address the UAE's obligations pursuant to international treaties. Additionally, the Cyber Crimes Law sets out significantly higher penalties than those found in the 2006 law.

General themes

The general themes of the provisions of the Cyber Crimes Law can be broadly categorised as follows:

- IT security
- State security and political stability
- Morality and proper conduct
- Financial and commercial issues
- "Miscellaneous"

IT security

The provisions that relate to IT security address issues like hacking IT networks to steal data, change websites, interrupt service, distribute viruses, and the like. More specifically, the provisions in this category can be summarised as follows.

- Accessing an IT System ("IT System") without authorisation. (Greater penalties are provided where the subject data was personal data, or when the perpetrator commits the offence in the course of his or her employment.)
- Unauthorised access to an IT System to obtain government or commercial information. (This provision specifically references government information, but also refers to information relating to financial, trade or economic establishments licensed in the UAE.)
- Accessing a website without permission to damage, delete or change its content.
- Disabling access to an IT System.
- Circumventing an IP address for the purpose of committing or concealing a crime. (The scope of application of this provision is – potentially – very broad. On the one hand, it could refer to masking the IP address from which a major hacking attack is launched; on the other hand, it could potentially extend to the likes of use of an off-shore VPN in order to access pirated/unlicensed content from abroad. This latter example may be of much less interest to the authorities on a day-to-day basis, although it would still appear to be captured by the prohibition.)
- Introducing virus programmes to an IT System; and spam emails. (This provision provides significant penalties for the introduction of computer viruses, being either or both of five or more years imprisonment and AED500,000 to AED3,000,000 fine, with imprisonment and a fine of up to AED500,000 being available for unsuccessful attempts.)
- Obtaining, without authorisation, passwords to an IT System. (This provision does not specify that the act of obtaining such password/code need occur via an IT System, and the language appears broad enough to cover obtaining by way of IT System, or otherwise. Additionally, this

provision includes a broad prohibition on making available (whether by making directly or procuring; and including by way of importation, sale, etc.) any means or information designed to commit/facilitate/incite others to commit crimes specified under the law.)
- Unauthorised interception of communications via an IT System. (This provision seems to mirror the prohibition on intercepting communications (ie. eavesdropping on phone calls and intercepting mail) found in the Penal Code and (in the case of phone calls) the Telecommunications Law. Additionally, the act of disclosing information so gathered is also captured by this provision.)
- Unauthorised disclosure of confidential information via an IT System. (This provision appears to be designed to capture 'Wikileaks' type situations, namely, situations where workers who obtain confidential information in the course of their employment release such confidential information without authority.)

Basically, these provisions are all targeted at the integrity of the IT System, and data held or transmitted over such IT System.

State security and political stability

A number of provisions are specifically pointed at state security and dignity, and political stability. The provisions in this category can be summarised as follows.

- Unauthorised access to an IT System to obtain government or commercial information.
- Operating a site, or posting information online, that stirs sedition, hatred, racism or sectarianism, or hurts national unity or social peace or prejudices public order or public morals.
- Operating a site, or posting information, for a terrorist group or illegal organisation.
- Operating a site, or posting information online, that exposes the State's security and interests to danger and prejudice public order.
- Publishing information/news/rumours online for the purpose of harming the status of the State.
- Operating a site, or posting information online, for overthrowing the government of the State, or undermining the Constitution.
- Publishing information online to incite non-compliance with laws.
- Using an IT System to provide others with information that harms the interests of the state or offending its dignity.

These provisions set-out a range of prohibitions designed to manage security threats, such as terrorism and organised crime, as well as to protect the system of government.

Morality and proper conduct

A number of provisions are pointed at proper conduct. These include sanctions on using the internet for conduct that is disrespectful to Islam, as well as prohibitions on the use of the internet for activities that are otherwise inconsistent with public morals and good conduct. In summary, these include using an IT System to:

- offend religious sanctities or encourage sins,
- provide pornography, gambling activities, and other materials prejudicial to public morals,
- promote prostitution/debauchery,
- slander another person, and
- breach the privacy of another (eg. by intercepting communications, taking photographs, publishing information, etc.).

Financial and commercial issues

There are a number of provisions that can broadly be understood as relating to ecommerce and online financial activity. These include:

- Forging electronic documents or knowingly using forged electronic documents,
- Using an IT System to obtain goods fraudulently and without legal right,
- Using an IT System to unlawfully access bank account details, and
- Producing credit / debit cards without legal right or knowingly using and/or dealing with such illegal cards.

Miscellaneous

There are a number of other provisions of interest that do not neatly fall into the categories outlined above.

Articles 23, 25, 33 and 36 appear to be aimed directly at addressing international obligations as specified in related treaties. These provisions relate to human trafficking and trafficking in human organs, trading in weapons, ammunition and explosives, trading in antiquities and trading or promoting narcotics.

Of the other 'miscellaneous' offences, there are prohibitions on:

- Using an IT System to blackmail someone into committing an offence or doing something that would prejudice honour,
- Operating a site, or posting information online, for the purpose of gathering donations without a licence, and
- Using an IT System to unlawfully benefit from, or facilitate the use by others of, communications services.

Mechanical provisions of note

There are a number of important 'mechanical' provisions, including provisions that provide for the extra-territorial application of the Cyber Crimes Law, and the liability of site owners for failure to remove offending content.

Penalties

Besides providing for significant financial penalties and custodial sentences, and the deportation of foreigners convicted of any offence under the law, the Cyber Crimes Law empowers the authorities to seize and destroy equipment used in the commission of the offence.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises clients on how to work within the law on the types of matters covered by the Cyber Crimes Law. We work closely with colleagues in other departments to assist clients with issues arising from apparent breaches of prohibitions found in the Cyber Crimes Law. For further information on Cyber Crimes Law matters, please contact Nick O'Connell (n.oconnell@tamimi.com).