Cybercrime Legislation in Iraq

Haydar Jawad - Senior Counsel - Corporate / Mergers and Acquisitions / Commercial / Employment and Incentives

h.jawad@tamimi.com - Erbil

Aro Omar

a.omar@tamimi.com - Erbil, Iraq

September 2017

Overview of Cybercrime in Iraq

Iraq's internet sector is currently unregulated, placing it among the freest globally, but also amongst the most vulnerable. The current political and security situation in Iraq means that further work is necessary to develop the legal, technical, organisational, and capacity building fundamentals to provide comprehensive cybersecurity for its citizens, businesses, and the state.

Data on the types of cybercrime in Iraq is scarce, and rarely published by the Iraqi government. However, earlier reports released by the Iraqi government expose the most common types of cybercrime in Iraq, which have likely increased over the years.

In 2013, the Iraqi Ministry of Planning reported that, the vast majority of cybercrime is conducted via social media platforms, primarily on Facebook, and against persons rather than businesses or governments. The most common cyberattacks involve internet fraud, identity theft, child pornography, cyber-stalking, cyber-blackmail, copyright infringement, satellite piracy, and cyberterrorism.

Applicable Legislation

A draft Iraqi Information Crimes Law was proposed by the Presidential Council of Iraq in 2011. The draft law was intended to regulate the use of information networks, computers, and other electronic devices and systems. It was, however, widely argued the proposed legislation violates international standards protecting due process, freedom of speech, and freedom of association. With the result that, on 6 February 2013 following strong local and international objections, as well as a decisive letter by the Iraqi Council of Representatives' Culture and Media Committee addressed to the head of the Council, the Iraqi Council of Representatives revoked and discarded the draft law.

Iraq does not currently have any specific legislation on cybercrime in place. In the absence of specific legislation, the judiciary must apply the provisions of the Iraqi Civil Code No. 40 of 1951 (the "Civil Code") and the Iraqi Penal Code No. 111 of 1969 (the "Penal Code"), in addition to sector-specific laws (e.g. the Banking Law of 2004, and Communications and Media Commission Law CPA Order 65 of 2004), to cases involving cybercrime.

Furthermore, Iraq does not currently have any specific data protection legislation in place and privacy protection under the Civil Code remains largely undeveloped. There is reference to a "right to personal privacy" in the Iraqi Constitution of 2005, but guidance with respect to this right is unavailable, and it remains undefined in legislation.

Applying Existing Legislation

As noted above, the most common cybercrimes in Iraq are internet fraud, identity theft, child pornography,

cyber-stalking, cyber-blackmail, copyright infringement, satellite piracy, and cyberterrorism. The Penal Code broadly addresses the criminal nature of these cybercrimes, but fails to adequately incorporate their 'cyber' property.

Any person who is convicted of a cybercrime involving violence, sexual exploitation, threats, or manipulation may be penalised under Article 369 and 396 of the Penal Code:

Under Article 369 the penalty is imprisonment with a maximum term of 4 years (eighteen years if the victim is younger than eighteen years of age) on any person who assaults another using force, or threatens, manipulates or violates in any way the decency of another male or female, or initiates such violation.

Similarly, Article 396 of the Penal Code imposes a maximum term of imprisonment of 7 years on any person who sexually assaults a man or woman or attempts to do so without his or her consent and with the use of force, deception or other means. The penalty for offences against victims under 8 years of age is imprisonment for a term not exceeding 10 years.

In addition to the above, any person who is convicted of a cybercrime involving identity theft, internet fraud, blackmail or other relevant acts may be penalised by detention under Article 456 of the Penal Code.

Any person who is convicted of a cybercrime involving copyright infringement may be penalised under Article 45 of the Copyright Law. Legal relief available to the copyright owner under Article 45 includes:

- injunctions to order the infringer to cease infringing activities;
- confiscation of the original and copies and materials used to manufacture infringing copies; and
- confiscation of the proceeds of the infringement.

Any person who is convicted of cyberterrorism may be penalised under the Anti-Terrorism Law No. 13 of 2005.

The above provisions are in addition to the civil rights of harmed persons to file claims for damages caused to them by virtue of said violations, in accordance with the Civil Code.

Conclusion

The Internet is a unique domain. Laws that regulate other forms of media cannot always effectively govern this medium, and attempting to have them do so may create inconsistency and ambiguity in application. Regulatory approaches need to be tailored specifically for the internet and the criminalization of e-crimes. While the Penal Code and Civil Code, in addition to the sector-specific laws dealing with e-transactions, serve as a step towards the establishment of cybersecurity, it is hoped that the Iraqi legislature will adopt articles specifically relating to cybercrime. Specific and extensive cybercrime legislation will provide judicial consistency on the subject as well as facilitate the enforcement of the law.

Al Tamimi & Company's corporate commercial and media and telecommunications teams regularly advise on e-transactions and cyber crimes. For further information please contact Haydar Jawad (H.Jawad@tamimi.com) or Aro Omar (a.omar@tamimi.com).