19 September 2018

Client Alert: The New Egyptian Anti-Cybercrime Law Regulates Legal Responsibility for Web Pages and Their Content

By Kilian Bälz and Hussam Mujally

In mid-August 2018, Egypt enacted a new anti-cybercrime law that comprehensively regulates Internet activities for the first time. This client alert summarizes the key aspects of the new law, which may be relevant for international companies and organizations that operate web pages with a connection to Egypt, be it a web page hosted in or managed from Egypt, or one merely targeting Egyptian readers.

Introduction to the Anti-Cybercrime Law

On 15th August 2018, Law No. 175/2018 on Combating Information Technology Crimes ("**Anti-Cybercrime Law**") came into force. The Anti-Cybercrime Law regulates activities online, and, according to official statements, it aims to complement the new press and media laws, which penalize, *inter alia*, unlicensed online activity and content violations, such as fake news. According to Article 44 of the new law, the Prime Minister will issue Executive Regulations within three months of the 15th August 2018 enactment date. Under Article 43, telecommunication service providers and other addressees of the law have a one-year transitional period during which they must bring their activities in line with the Anti-Cybercrime Law.

Overview of Addressees, Offenses, and Penalties

The Anti-Cybercrime Law comprises 45 articles that address a variety of offences, which are broadly related to the Internet, and their respective penalties. It covers offences against confidentiality, the integrity and availability of computer data, computer-related offences, offences related to infringements of privacy, and content-related offences, such as immoral content, as well as such threating national security[1].

Addressees of the Anti-Cybercrime Law are: (i) users (natural and legal persons); (ii) managers of legal persons; (iii) service providers; (iv) web administrators; and (v) state officials. The law defines the term "web administrator" broadly to comprise both persons

[1] Article 1 (25) defines national security as follows:

All that is related to the independence, stability, security of the country and the unity and safety of its territory. As well as all related to the affairs of Presidency, National Defense Council, National Security Council, Ministry of Defense and Military Production, Ministry of Interior, General Intelligence Directorate, Administrative Control Authority, and of all organs thereunder.

responsible for the technical aspects of a website, such as system administrators, and persons responsible for the content of the website (Article 1[14]).

The offences included in the Anti-Cybercrime Law are listed in eight chapters under Part Three. The most relevant chapters are:

- *Chapter I: Offences Against the Integrity of Information Networks, Systems, and Technologies*, which include such offences as online piracy, illegal access, data interference, computer sabotage, email account hacking, websites hacking, and offences against state-owned information systems.
- *Chapter II: Crimes Committed by Means of Information Systems and Technologies*, which include the theft of information, including credit cards and further electronic payments system, credit card fraud, and impersonation with fake email accounts, websites, and social media accounts.
- *Chapter III: Crimes Related to Invasion of Privacy and Illegal Content*, which include selling personal data, publishing personal and private data without consent, and violating the familial values and principles of Egyptian society.
- *Chapter IV: Crimes Committed by Web Administrators*
- *Chapter V: Criminal Liability of Service Providers*
- *Chapter VII: Criminal Liability of Legal Persons*

The penalties include imprisonment of up to two years and fines of up to 10 million Egyptian pounds.

The Law's Key Trends

The Anti-Cybercrime Law deals with a broad variety of issues, stretching from combatting online crime to censoring web pages with sensitive content. For international companies and institutions active in Egypt, the most relevant sections will be those regulating web pages and their content.

For example, Article 7 grants the investigating authority the power to block Egyptian-based or foreign websites featuring content that threatens national security or the national economy, as well as any content criminalized under the Anti-Cybercrime Law. A judge must validate an order to block a website within four days. The public prosecutor is further entitled to impose a travel ban on individuals suspected of committing a crime under the Anti-Cybercrime Law (Article 9). The authorities may also access, seize, attach, or trace information, data, or information systems for a period of not more than 60 days and in any medium in order to establish facts related to the commitment of a crime punishable under the law. Service providers are obligated to turn over any information related to users' activities as required by the authorities (Article 6).

Moreover, Article 3 allows Egyptian authorities to claim criminal jurisdiction over non-Egyptian citizens for crimes punishable under the Anti-Cybercrime Law when committed outside Egypt, provided such actions are also punishable in the country in which they were perpetrated. As a result, action can be taken against web pages, and the people who operate them, even if they are hosted or located outside Egypt.

Liability of Web Administrators and Managers

Pursuant to Article 27, a web administrator who creates, manages, or uses a website or a private account with the aim of committing or facilitating a crime can face imprisonment of not less than two years and/or a fine of between 100,000 and 300,000 Egyptian pounds.

Furthermore, web administrators are criminally liable for the safety of the information systems, websites, and accounts under their management. Under Article 29, if a web administrator exposes a website, an email account, a private account, or an information system to a crime punishable under the Anti-Cybercrime Law, the penalty is imprisonment for a period of no less than one year and/or a fine of between 20,000 and 200,000 Egyptian pounds. Where the crime occurred due to the web administrator's negligence, the penalty is reduced to imprisonment of not less than six months and/or a fine of between 20,000 and 200,000 Egyptian pounds. Negligence is assumed when the safety measures and precautions stipulated in the Executive Regulations are not satisfied.

If an entity's website or email accounts become the victim of a crime punishable under the Anti-Cybercrime Law, the entity's manager is obligated to report the matter to the competent authorities. Article 35 provides for imprisonment of not less than three months and/or a fine of between 30,000 and 100,000 Egyptian pounds for managers who fail to report such incidents. Furthermore, pursuant to Article 36, a manager of a legal person who is aware of a crime committed in the name or through the account of the legal person or facilitates the same shall be punished with the penalty designated for the perpetrator.

Liability for Website Content

Illegal content is not clearly defined in the Anti-Cybercrime Law. However, Article 25 provides that content violating the familial values and principles of Egyptian society or invading privacy is illegal.

The introduction of the Anti-Cybercrime Law triggered a controversial public debate. It is questionable whether persons responsible for a website's content, admins of social media accounts, or managers of a legal entity are criminally liable for any user-generated content presented online on their respective websites or accounts (*e.g.*, through a comment or chat function). According to observers, the Anti-Cybercrime Law could be used to prosecute persons for content produced online, for instance via social media.

In our view, given that Article 27 provides for criminal sanctions, the aforementioned interpretation is too broad, and we find a narrow interpretation more convincing. According to the latter interpretation, the web administrator can only be held responsible for illegal content that was approved or solicited. Unless the aim of the website is to solicit or promote entries with illegal content, the broader interpretation would mean using Article 27 to prosecute a web administrator for a user's entry, which is not related to the webpage and beyond the administrator's control. In our view, therefore, a web administrator should not be held responsible for any illegal content that was published through a comment function and without a connection to the website's content. However, the offences in Articles 25, 27, 29, and 35 are indeed very broadly defined, and we cannot exclude a general liability for web administrators or managers of a legal entity for content-related violations.

It remains to be seen how the law will be implemented in practice. In any event, we recommend undertaking a due diligence analysis of security standards for websites, emails, and information systems of entities operating in Egypt as well as raising awareness amongst employees regarding cybersecurity and cybercrimes punishable under the Anti-Cybercrime Law.

If you would like more information about this topic, please contact us.

Kilian Bälz
Partner
Berlin / Cairo / Tripoli
kb@amereller.com

Hussam Mujally
Associate
Berlin / Cairo / Dubai
mujally@amereller.com

BERLIN | Kurfürstenhöfe | Spreeufer 5 | 10178 | Berlin | Germany | t: +49.30.609.895.660

CAIRO | MENA Associates in association with Amereller | GIC Tower | 21 Soliman Abaza St. | Mohandessin | Giza | Egypt | t: +20 2 376 26 201