Anti-Cyber Crime Law

(8 Rabi1, 1428 / 26 March 2007)

Kingdom of Saudi Arabia
Bureau of Experts at the Council of Ministers
Official Translation Department
Translation of Saudi Laws

Anti-Cyber Crime Law
Royal Decree No. M/17
8 Rabi 1 1428 / 26 March 2007
First Edition 2009

No. M/17
Date: 8/3/1428H

With the help of Almighty God,
We, Abdullah bin Abdulazlz Al-Saud,
King of the Kingdom of Saudi Arabia,

Pursuant to Article 70 of the Basic Law of Governance, issued by Royal Order No. (A/90), dated 27/8/1412 H; And pursuant to Article 20 of the Law of the Council of Ministers, issued by Royal Order No. (A/13), dated 3/3/1414 H; And pursuant to Article 18 of the Shura Council Law, issued by Royal Order No. (A/91), dated 27/8/1412 H; And upon perusal of the Shura Council's Resolutions No. (68/43), dated 16/9/1427 H; And upon perusal of the Council of Ministers' Resolution No. (79), dated 7/3/1428 H; Have decreed as follows:

Firstly: the Anti-Cyber Crime Law as per the attached form shall be approved.

Secondly: His Highness, the Vice-President of the Council of Ministers, and the Ministers, each within their jurisdiction, shall implement this decree of ours.

(Signed)

Abdullah bin Abdulaziz

Article 1:

The following terms and phrases, wherever mentioned in this Law, shall have the meanings expressed next to them, unless the context requires otherwise:

1. Person: Any natural or corporate person, whether public or private.
2. Information System: A set of programs and devices designed for managing and including computers.
3. Information Network: An interconnection of more than one computer or processing data, information system to obtain and exchange data, e. g. Local Area Network (LAN), Wide Area Network (WAN), and World Wide Web (Internet).
4. Data: Information, commands, messages, voices, or images which are prepared or have been prepared for use in computers. This includes data that can be saved, processed, transmitted, or constructed by computers, such as numbers, letters, codes, etc
5. Computer Programs: As a set of commands and data which contain guidelines or applications when run in computers or computer networks to perform required functions.
6. Computer: Any electronic device whether movable or fixed, wired or wireless, which is equipped with a system to process, store, transmit, receive or browse data and perform specific functions according to programs and commands.
7. Unauthorized Access: The deliberate, unauthorized access by any person to computers, websites, information systems, or computer networks.
8. Cyber Crime: Any action which involves the use of computers or computer networks, in violation of the provisions of this Law.
9. Web Site: A site providing data on the information network through specific Uniform Resource Locator (URL).
10. Reception: Illegal viewing or obtaining of date.

Article 2

This Law aims at combating cyber crimes by identifying such crimes and determining their punishments to ensure the following:

1. Enhancement of information security.
2. Protection of rights pertaining to the legitimate use of computers and information networks.
3. Protection of public Interest, morals, and common values.
4. Protection of national economy.

Article 3:

Any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding one year and a fine not exceeding live hundred thousand riyals or to either punishment:

1. Spying on, interception or reception of data transmitted through an information network or a computer without legitimate authorization.
2. Unlawful access to computers with the intention to threaten or blackmail any person to compel him to take or refrain from taking an action, be it lawful or unlawful.
3. Unlawful access to a web site, or hacking a web site with the intention to change its design, destroy or modify it, or occupy its URL.
4. Invasion of privacy through the misuse of camera-equipped mobile phones and the like.
5. Defamation and infliction of damage upon others through the use of various information technology devices.

Article 4

Any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding two million riyals, or to either punishment:

1. Acquisition of movable property or bonds for oneself or others or signing such bonds through fraud or use of false name or identity.
2. Illegally accessing bank or credit data, or data pertaining to ownership of securities with the intention of obtaining data, information, funds or services offered.

Article 5:

Any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding three million riyals or to either punishment:

1. Unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data
2. Causing the information network to halt or breakdown, or destroying, deleting, leaking or altering existing or stored programs or data.
3. Obstruction of access to, distortion, and causing the breakdown of services by any means.

Article 6:

Any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding five years and a fine not exceeding three million riyals or to either punishment:

1. Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers.
2. The construction or publicizing of a website on the information network or computer to promote or facilitate human trafficking.
3. The preparation, publication, and promotion of material for pornographic or gambling sites which violates public morals.

4. The construction or publicizing of a web site on the information network or computer to trade in, distribute, demonstrate method of use or facilitate dealing in narcotic and psychotropic drugs.

Article 7:

Any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding ten years, and a fine not exceeding five million riyals or to either punishment:

1. The construction or publicizing of a website on the information network or on a computer for terrorist organizations to facilitate communication with leaders or members of such organizations, finance them, promote their ideologies, publicize methods of making incendiary devices or explosives, or any other means used in terrorist activities.
2. Unlawful access to a web site or an information system directly, or through the information network or any computer with the Intention of obtaining data jeopardizing the internal or external security of the State or its national economy.

Article 8:

The imprisonment and the fine may not be less than half the maximum if the crime is coupled with one of the following:

1. The crime is perpetrated through organized crime.
2. The offender holds a public office and the crime perpetrated relates to this office, or if he perpetrates the crime using his power or influence.
3. The luring and exploiting of minors and the like.
4. The offender has been previously convicted of similar crimes within or outside the Kingdom.

Article 9:

Any person who incites, assists or collaborates with others to commit any of the crimes stipulated in this Law shall be subject to a punishment not exceeding the maximum punishment designated for such crimes, if the crime is committed as a result of said incitement, assistance or collaboration, and he shall be subject to a punishment not exceeding half the maximum punishment designated, if the intended crime is not committed.

Article 10:

Any person who attempts to commit any of the crimes stipulated in this Law shall be subject to a punishment not exceeding half the maximum punishment designated for said crimes.

Article 11:

The competent court may exempt an offender from such punishments if he informs the competent authority of the crime prior to its discovery and prior to the infliction of damage. If the culprit informs the competent authority after the occurrence of the crime, the exemption from punishment shall be granted if the information he provides eventually leads to the arrest of the other culprits

and the seizure of the means used in the perpetration of the crime.

Article 12:
Application of this Law shall not prejudice the provisions of relevant laws, especially those pertaining to intellectual property rights, nor relevant international agreements to which the Kingdom is party.

Article 13:
Without prejudice to the rights of bona fide persons, equipment, software, and means used in perpetrating any of the crimes stipulated in this Law or the proceeds generated therefrom may be confiscated. In addition, the website or the venue where the service is provided may be shut down permanently or temporarily if it is the source for perpetrating the crime and the crime is committed with the owner's knowledge.

Article 14:
The Communications and Information Technology Commission, pursuant to its powers, shall provide the assistance and technical support to competent security agencies during the Investigation stages of such crimes and during trial.

Article 15:
The Bureau of Investigation and Public Prosecution shall carry out the investigation and prosecution of crimes stipulated In this Law.

Article 16:
This Law shall be published in the Official Gazette and shall enter into force one hundred twenty days after the date of publication.