



شعبة الترجمة الرسمية
Official Translation Department

Anti-Cyber Crime Law

Royal Decree No. M/17
March 27, 2007

Translation of Saudi Laws



NOTE:

The translation of Saudi laws takes the following into consideration:

- Words used in the singular form include the plural and vice versa.
- Words used in the masculine form include the feminine.
- Words used in the present tense include the present as well as the future.
- The word “person” or “persons” and their related pronouns (he, his, him, they, their, them) refer to a natural and legal person.



Anti-Cyber Crime Law

Article 1

In this Law, the following terms shall have the meanings assigned thereto, 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 to manage and process data, including computers.
3. **Information Network:** An interconnection of more than one computer or information system to obtain and exchange data, e. g. Local Area Network (LAN), Wide Area Network (WAN), and the 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 which can be saved, processed, transmitted, or constructed by computers, such as numbers, letters, symbols, etc.
5. **Computer Programs:** A set of commands and data which contain instructions or applications when run on computers or computer networks and 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 which performs specific functions according to programs and commands.
7. **Unauthorized Access:** The deliberate, unauthorized access of any person to computers, web sites, information systems, or computer networks.
8. **Cyber Crime:** Any act which involves the use of computers or information networks, in violation of the provisions of this Law.
9. **Web Site:** A site providing data on an information network through a specific Uniform Resource Locator (URL).
10. **Reception:** Illegally viewing or obtaining data.

Article 2

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

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



Article 3

Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding one year and a fine not exceeding 500,000 riyals, or either penalty:

1. Spying on, or interception or reception of data transmitted through an information network or a computer without legitimate authorization.
2. Unauthorized access with the intention of threatening or blackmailing any person to compel him to take or refrain from taking an action, be it lawful or unlawful.
3. Unauthorized access to a web site, or hacking a web site 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 any of the following cybercrimes shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding 2,000,000 riyals, or either penalty:

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

Article 5

Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding 3,000,000 riyals, or either penalty:

1. Unauthorized access with the intention of canceling, deleting, destroying, leaking, damaging, altering, or redistributing private data.
2. Causing an information network to halt or breakdown, or destroying, deleting, leaking, damaging, or altering existing or used programs or data.
3. Obstructing access to, distorting, or causing the breakdown of services by any means.

Article 6

Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding five years and a fine not exceeding 3,000,000 riyals, or either penalty:



1. The production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, or privacy, through an information network or computer.
2. The construction or publication of a web site on an information network or computer to promote or facilitate human trafficking.
3. The preparation, publication, or promotion of material for pornographic networks or gambling activities which violates public morals.
4. The construction or publication of a web site on an information network or computer to trade, distribute, demonstrate methods of use, or facilitate dealing in narcotic and psychotropic drugs.

Article 6

Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding five years and a fine not exceeding 3,000,000 riyals, or either penalty:

1. The production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, or privacy, through an information network or computer.
2. The construction or publication of a web site on an information network or computer to promote or facilitate human trafficking.
3. The preparation, publication, or promotion of material for pornographic networks or gambling activities which violates public morals.
4. The construction or publication of a web site on an information network or computer to trade, distribute, demonstrate methods of use, or facilitate dealing in narcotic and psychotropic drugs.

The sentence may provide for the publication of its summary at the expense of the convicted person in one or more local newspapers or in any other appropriate medium, depending on the type, gravity, and impact of the crime committed, provided that such publication is executed after the judgment becomes final.

Article 7

Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding 10 years and a fine not exceeding 5,000,000 riyals, or either penalty:

1. Establishing or publicizing a web site on an information network or computer for terrorist organizations to facilitate communication with the 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. Unauthorized access to a web site or information system directly, or through an information network or computer to obtain data that threatens 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 any of the following:

1. The crime is perpetrated through organized crime.
2. The offender holds a public office and the crime perpetrated is related to this office, or the offender perpetrates the crime using his power or influence.
3. The luring and exploitation 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 prescribed 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 prescribed punishment 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 prescribed for said crimes.

Article 11

The competent court may exempt any 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 other culprits (if any) or the seizure of the means used in the commission of the crime.

Article 12

Application of this Law shall not prejudice the provisions of relevant laws, especially those pertaining to intellectual property rights, or 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 web site or 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 assistance and technical support to competent security agencies during the investigation of such crimes and during trial.

Article 15

The Bureau of Investigation and Public Prosecution shall carry out the investigation and prosecution of the crimes stipulated in this Law.

Article 16

This Law shall be published in the Official Gazette and shall enter into force 120 days after the date of publication.