Fighting Law against IT crimes

In accordance with the Memo of H.E. Dean of Information Technology, No. 248 on: 09-07-1433 Hijri, Regarding: "Fighting Law against IT crimes"

And in accordance with the Memo of H.E. the Vice President for studies, development and community services, No. 5/1/1970 on: 07-07-1433 Hijri, Attached with Copy of (Fighting Law against IT crimes), Received from the Panel of Experts in the esteemed Council of Ministers (for information)

Copy of (Fighting Law against IT crimes), Received from the Panel of Experts in the Council of Ministers

Kingdom of Saudi Arabia

Panel of Experts in the Council of Ministers

Article I:

The following words and phrases - wherever they appear in this system- mean the meanings indicated in front of them unless otherwise mentioned in context:

1. Person is any person with a natural or legal, public or private identity

2. **Informational System**: A collection of programs and tools designed for data processing and its management and it includes computers

3. **Information Network** :Correlation between more than one computer or information system for data acquisition and exchange, such as private or public networks and the Internet

4. **Data**: information, commands, or messages, sounds, or images that are, or previously prepared for its usage in the computer and all that can be stored and processed and transported and constructed by a Computer such as numbers, letters and symbols and others.

5. **Computer Programs:** a set of commands and data that include directions or applications when running in the computer or computer networks and they perform the required function.

6. **The Computer**: any fixed or portable electronic ,wired or wireless system that contains a system for processing data ,storing , sending, receiving or browsing data and that performs specific functions and programs, according to the commands given to it.

7. **Unauthorized access**: The access of a person deliberately to a computer or a website or information system or network of computers which is not authorized for that person to access.

8. **Cyber crime** any committed act, including the use of computer or computer network in violation of the provisions of this Regulation

9. **Electronic website**: where the availability of data on the information network through a specific address is available.

10. **Capturing**: View data or obtain it without a true systematic justification.

Article 2

This law is designed to reduce the incidence of computer crimes by identifying such crimes and penalties for each and as a result will lead to the following:

1. help in achieving informationon security
2. saving the rights of legitimate use of computers and information networks
3. protection of the public interest and morality morals
4. protection of the national economy

Article 3

A person shall be punished by imprisonment for a term not exceeding one year and a fine not exceeding five hundred thousand Saudi Riyals, or either of them, if he commits any of the following informatics crimes:

1. Tapping what is sent through the Internet or a computer system-without formal justification– or capturing or intercepting.

2. Illegal entry to threaten or blackmail a person to do or abstain from doing any act, even if such an act or abstention is legitimate.

3. Illegal entry to a website, or access to the website to change the designs of this site, or destroy, modify or occupy its title.

4. Violations of privacy through the misuse of mobile phones with camera, or the like.

5. Defamation of others and harm them by means of various information technologies.

Article IV:

A person shall be punished by imprisonment for a term not exceeding three years and a fine not exceeding two million riyals, or either of them, if he commits any of the following informatics crimes:

1. Appropriation for oneself or others a movable property or bond, or signing this bond, through fraud, or take a false name, or impersonate another person.

2. access – without a true formal justification – a bank data, or credit, or data related to the ownership of securities in order to obtain data, or information, or funds, or available services

Article 5:

A person shall be punished with imprisonment for not more than four years and a fine not exceeding three million riyals, or either of them, if he commits any of the following informatics crimes:

1. Illegal entry to clear private data, delete, or destroy, or diverse, or damage, or change, or republish them.

2. Stop the Internet from work, or disable it, or destroy or erase programs, or existing or used data in them, or delete them, or diverse, or damage, or modify them.

3. Block access to the service, or disrupt or disable it by whatever means.

Article VI:

A person shall be punished by imprisonment for a term not exceeding five years and a fine not exceeding three million riyals, or either of them, if he commits any of the following informatics crimes:

1. Production of what would undermine public order or religious values or morals, or the sanctity of private life, or prepare, or send or store via the Internet or a computer.
2. Create a site on the Internet, or computer hardware or publish, for trafficking in the human race, or facilitating it.
3. Create materials and data on pornography networks or indecent gambling activities, or publish or promote them.
4. Create a site on the Internet or computers or publishing it for drug trafficking or psychotropic, or for promotion, or abuse, or easier handling of drugs.

Article VII:

A person shall be punished by imprisonment for a term not exceeding ten years and a fine not exceeding five million riyals, or either of them if he commits any of the following informatics crimes:

1. Create a site for terrorist organizations on the Internet, or a computer or publish; to facilitate communication with the leadership of these organizations, or any of its members, or promote their ideas or financing them, or post how to make incendiary devices or explosives, or any tool used in terrorist acts.
2. Illegal entry to a website, or information system directly, or through the Internet or a computer to obtain data affecting

the internal or external security of the State or its national economy.

Article VIII:

Minimum imprisonment or a fine must not be less than half of the maximum limit if the crime is coupled with any of the following cases:

1. The offender commits the crime through an organized gang.
2. The offender holds a public office and the crime is related to that office or commits the crime by abusing his powers or influence
3. Corruption of minors and the like and exploiting them.
4. The provisions of the domestic or foreign previous convictions against the offender in similar crimes.

Article IX:

Anyone who incites another or helps him or agrees with him to commit any of the crimes provided for in this law if the crime is based on such incitement, assistance or agreement his punishment shall not exceed the upper limit of the penalty and shall not exceed half the maximum penalty if there were no original crime..

Article X:

Any person engaged in carrying out any of the crimes provided for in this law shall be punished by no more than half the maximum of the prescribed penalty

Article XI

The competent court can exempt from these punishments each of the perpetrators who informs the competent authority about the crime prior knowledge of it and before the occurrence of the injury and if that was after knowing the crime, the exempt from will be made if the reporting leads to arresting the rest of the perpetrators, if they are group, or seizure of the tools used in the crime.

Article XII

The application of this Law shall be without prejudice to the provisions contained in the laws contained in related systems: and especially with regard to intellectual property rights and the relevant international conventions to which the Kingdom is a party.

Article XIII

Without prejudice to the rights of good faith may rule confiscation of hardware or software or methods used in committing any of the crimes provided for in this Law or the funds collected from them. It also may be sentenced to close the website or place of service permanently or temporarily whenever it becomes the source to commit any of these crimes and if the crime was committed with the knowledge of its owner.

Article XIV

The Bureau of Communication and Information Technology in accordance with its competence administer providing support and technical assistance to the competent security authorities through the stages of controlling these crimes and the investigation and during the trial.

Article XV:

The Bureau of Investigation and Prosecution takes over the crimes contained in this Law.

Article XVI:

This Law shall be published in the Official Gazette and shall come into effect after (one hundred and twenty) days from the date of its publication.