UNOFFICIAL TRANSLATION
Law on Combating Cybercrime in the Kingdom of Bahrain

On information technology crimes

We are Hamad bin Isa Al Khalifa, King of the Kingdom of Bahrain.

After reviewing the Constitution,

The Penal Code promulgated by Legislative Decree No. 15 of 1976 and its amendments,

And Decree-Law No. (17) of 1976 regarding Juveniles, amended by Legislative Decree No. (23) of 2013,

And Decree-Law No. 4 of 2001 on the Prohibition and Combating of Money Laundering and its amendments,

And Decree-Law No. (28) of 2002 on electronic transactions and its amendments,

And the Code of Criminal Procedure promulgated by Legislative Decree No. 46 of 2002 and its amendments,

And Decree-Law No. (47) of 2002 regarding the organization of the press, printing and publishing,

And the Telecommunications Law promulgated by Legislative Decree No. 48 of 2002,

Law No. (19) of 2004 approving the accession of the Kingdom of Bahrain to the Optional Protocols to the Convention on the Rights of the Child on the involvement of children in armed conflict and on the sale of children, child prostitution and child pornography,

Law No. (22) for the year 2006 regarding the protection of copyright and related rights and its amendments,

Law No. (58) for the year 2006 regarding the protection of society from terrorist acts and amended by Legislative Decree No. (20) of 2013,

Law No. 64 of 2006 promulgating the Central Bank of Bahrain Law and financial institutions,

The Shura Council and the Council of Representatives approved the following law, which we have ratified and issued:

Introductory chapter

Article (1)

In the application of the provisions of this Law, the following words and expressions shall have the meanings assigned to each of them unless the context otherwise requires.

Information technology : includes all forms of technology used to create, process, store, share, use and display information in various formats.

Information : All that can be stored, processed, generated and transmitted using IT means, in particular, writing, still images, mobile, sound, numbers, letters, symbols, signs, etc.

Means any electronic, magnetic, optical, electrochemical, or any instrument that integrates communication, computing or any other device that has the ability to receive, transmit, process, store and retrieve data very quickly.

IT system : A related or related tool or set of tools, one or more of which automatically processes the IT data in accordance with a software program.

IT data : representation of facts, facts, information, or concepts in an appropriate form that allows the IT system to process them.

Program : A set of instructions expressed in words, symbols, methods or otherwise, if included in any of the machine-readable media, is capable of making an IT tool perform a particular work or produce a specific result.

Service Provider, any of the following:

A) any public or private entity providing its users with the possibility of communicating through the IT system;

B) any other entity that processes or stores the data of the IT device on behalf of the entity referred to in item (a) of this paragraph or the users of its services.

Route data: Information technology (IT) data produced by the IT system for communication through an IT system that forms part of this communication chain.

Content data : IT data, unlike route data, is sent as part of a connection.

Damage : Define, disable, cancel, delete, destroy, alter, modify, misrepresent or block the data of an IT device, or to impair or impair the IT system.

Encryption : The process of converting information, systems or means of information technology or communications into symbols that are incomprehensible or scattered so that they are difficult to read or know without being returned to their original form using a particular password or encryption tool used.

Chapter I
Penalties for IT crimes

First branch

Crimes against IT systems and data

Article (2)

A penalty of imprisonment for a period not exceeding one year and a fine not exceeding thirty thousand dinars or one of these two penalties shall be imposed without legal justification for entering into the IT system or part of it.

If the entry results in disclosure of the data stored in the means or system of the information technology or part of it is counted as an aggravating circumstance.

Article (3)

It is punishable by imprisonment and a fine not exceeding fifty thousand dinars or one of these two penalties, which is the most recent damage to the data of the means of information technology or IT system.

The penalty shall be doubled if the commission of the crime results in any of the following:

(A) Impede the conduct of any public facilities or works of public interest;

B) Threat to people's lives, security or health.

C) harming the safety of the human body.

D) alteration, adaptation or cancellation of medical examinations, medical diagnosis or treatment of a person;

The penalty shall be life or temporary imprisonment if the commission of the crime results in the deliberate death of a person.

Article (4)

Without prejudice to any more severe penalty in any other law, imprisonment with a fine not exceeding one hundred thousand Dinars or one of these penalties shall be punishable by wiretapping, intercepting or intercepting without legal justification using technical means, Transmitted from or to the IT system, including any emissions of electromagnetic waves from the IT system that carry such data.

If an eavesdropping, capture or objection results in a disclosure of the transmission or part thereof without legal justification, that is not an aggravating circumstance.

Article (5)

Without prejudice to any stricter penalty in any other law, a person who sends the data of an information technology device containing a threat of causing damage to the carrying of another shall be punished by imprisonment and a fine not exceeding thirty thousand dinars or one of the two penalties, provided that he or she gives him or any other gift of any kind Or to perform or abstain from doing so.

The penalty shall be imprisonment for a period not exceeding five years and a fine not exceeding sixty thousand dinars if the offender reaches his destination.

Article (6)

Whoever commits any of the offenses set forth in Articles 2, 3, 4 and 5 of this Law to produce, import, buy or sell, shall be punished by imprisonment for a period not exceeding one year and a fine not exceeding one hundred thousand dinars or one of these two penalties. Or offer for sale, use, distribution, circulation, acquisition, publication or availability:

(A) A tool - including any program - designed or modified primarily for the purpose of committing any of the offenses referred to;

B) any other password, access code, access code or other similar information technology medium, by which access to the IT system or any part of it is possible;

Section II
Crimes related to the means of information technology

Article (7)

Shall be liable to imprisonment for a term of not more than ten years from the introduction, adaptation, suspension, cancellation, deletion, destruction, alteration, modification, alteration or omission of the data of an IT device belonging to a governmental interest or entities mentioned in Article 107 of the Penal Code , In a manner that would show incorrect data as true, designed to be used as valid data, whether directly or indirectly understood.

The penalty shall be imprisonment if the offense is committed in respect of the data of an information technology device not belonging to one of the interests or entities referred to in the preceding paragraph if that would cause harm.

Article (8)

A person who unlawfully obtains possession of property owned by third parties or receives any benefit for himself or others or to sign, cancel, destroy or modify a bond by means of a false name or an incorrect or fraudulent form shall be punished by any of the following: :

A) the introduction, adaptation, disabling, cancellation, deletion, destruction, alteration, modification, alteration or omission of IT data;

B) make any interference in the work of the IT system;

The aggravated circumstance provided for in articles 391 and 392 of the Penal Code applies to this offense.

Article (9)

Any person who uses encryption in order to commit or conceal any of the crimes provided for in this Law or any other law shall be punished by imprisonment and a fine not exceeding one hundred thousand Dinars or by either of these two penalties.

Section III
Crimes related to content

Article (10)

Without prejudice to any more severe penalty in any other law:

1) A penalty of not less than one year imprisonment and a fine not exceeding ten thousand Dinars shall be imposed on either of the following:

A) Producing pornographic material for distribution by the IT system.

B) imported, sold, offered for sale, used, traded, transferred, distributed, sent, published or made available by the IT system.
The penalty shall be imprisonment for a period of not less than two years and a fine not exceeding ten thousand dinars or one of these two penalties if the child pornography is directed at or placed within the reach of children.

(2) A penalty of not less than three months' imprisonment shall be imposed and a fine not exceeding three thousand dinars or one of these two penalties shall be imposed on anyone who commits any of the following acts:

A) he or she has obtained pornographic material through the IT system.

B) Obtain pornographic material in the IT system or in any other means of information technology.
The penalty shall be imprisonment for a period of not less than six months and a fine of not less than three thousand dinars or one of these two penalties if the child pornography is directed at or placed at their disposal.

3. In the application of the provisions of this article, the term "child pornography" means the definition of child pornography in the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

Chapter II
Procedures for IT crimes

Article (11)

The provisions of this Chapter shall apply to:

A) The crimes stipulated in Chapter I of this Law.

(B) Offenses provided for in any other law if committed using the IT system.

C) Collection of evidence in electronic form relating to any crime.

Article (12)

(1) The Public Prosecution may order any person to expeditiously maintain the integrity of certain data for the means of information technology, including the route data stored within the IT system, in its possession or control and to maintain the integrity of such data whenever it deems necessary to demonstrate the truth In any crime and have evidence to believe that such data is liable to be lost or altered.

2. The Public Prosecution may order the person referred to in paragraph 1 of this article to maintain and maintain the data for a period not exceeding ninety days and the Grand Criminal Court in the Chamber of Counsel may authorize the Public Prosecution, at the request of justification, The period referred to by three days, extending this period for a period or consecutive periods not exceeding a total of ninety days. Where possible, the court shall hear the statements of the person referred to.

(3) The Public Prosecution may order the person referred to in paragraph (1) of this article to maintain the confidentiality of the order issued in accordance with the provisions of any of paragraphs (1) and (2) of this Article for a period not exceeding ninety days, renewable for a period or periods Shall not exceed ninety days in total and the procedure provided for in paragraph (2) referred to above.

Article (13)

(1) The Public Prosecution may order any person possessing or under its control certain data to transmit information promptly, including data stored within an information technology system or any means of information technology.

(2) The Public Prosecution may order any service provider to provide any information in its possession or control of any subscriber or user thereof, whether this information is in the form of an IT or any other form and does not include traffic and content data .

All this when the Public Prosecution sees the need for this to show the truth in the crime.

Article (14)

The judge of the lower court may, at the request of the Public Prosecution, after having examined the papers, order the following:

(A) The transmission of crime-related traffic data whether the transmissions have been transmitted through one or more service providers is expeditiously maintained;

B) the disclosure of sufficient traffic data to enable the Public Prosecution to determine the service provider and the path through which such data were transmitted, as long as it contributes to the truth in a crime punishable under this Act or any other law; In this case, the judge shall issue an order.

Article (15)

1) The Public Prosecution may issue an injunction to enter and inspect the following:

(A) The information technology system related to the crime or any part thereof and any data of the information technology stored therein;

B) any means of storing the data of an information technology device in which crime-related data may be stored.

(2) If, in the execution of the order referred to in paragraph 1 (a) of this article, the Public Prosecution has strong indications that the crime-related data is stored in another or part of the IT system and that such data could be accessed Through the IT system or through which it is legitimately available, the Public Prosecution may issue an injunction to extend access and inspection to the other system.

Article (16)

(1) The Public Prosecution Authority shall have the authority to control and preserve the data of the means of information technology accessed pursuant to the provisions of Article (15) of this law, including the following:

A) the control and reservation of the IT system, or any part thereof, or any of the IT data storage media;

B) Reproducing the information technology data and maintaining the copy.

C) Maintain the integrity of the data of the IT medium.

D) Uploading the data of the IT system from the IT system that has been accessed or made unavailable.

2. The power of control and reservation referred to in paragraph (1) of this article shall not include what the accused has placed at the disposal of the defender or the consultant to perform the task entrusted to them or the correspondence between them in the case.

Article (17)

The judge of the lower court shall, at the request of the Public Prosecution, and upon examination of the papers, order any person who is competent or familiar with the functioning of the IT system and the measures applied to protect the data stored in this system by providing it with reasonable information to enable it to carry out the prescribed procedures In Articles (15) and (16) of this Law. The judge assesses, if necessary, the fees of the commissioner.

Article (18)

(1) Subject to the provisions of section (b) of Article (14) of this Law, the Public Prosecution may, after obtaining the permission of the lower court judge:

A) Assign any person competent to collect and record traffic data and content data, or any of them, relating to specific communications transmitted by the IT system, when such communications occur.

B) Assign any service provider to carry out the acts referred to in item (a) or to provide the necessary assistance to those commissioned by the Public Prosecution.

C) Assign any person competent to block the data of the content of any information technology device or any part thereof by which any of the IT crimes were committed.
In all cases, the permit shall be for a period not exceeding thirty days renewable for another period or similar periods.

(2) Persons assigned in accordance with the provisions of paragraph (1) of this Article shall not be subjected to undue disclosure in the law to any other person of this commission or any relevant information or use in any manner.

Article (19)

(1) A person who has not complied with an order or order issued in accordance with the provisions of any of the following paragraphs shall be punished by imprisonment for a period not exceeding two years and by a fine not exceeding one hundred thousand dinars or one of these two penalties. (1) or (2) of Article (12), or any of Articles (13) or (14), or paragraph (1) of Article (18) of this Law.

2) A penalty of imprisonment for a period not exceeding one year and a fine not exceeding three thousand dinars or one of these two penalties shall be imposed on anyone who contravenes:

(A) The order referred to in paragraph (3) of Article (12) of this Law.

B) The provision of paragraph (2) of Article (18) of this law.

The penalty shall be imprisonment for a term not exceeding five years if the offender is a public official or a public service officer.

Chapter III
Miscellaneous provisions

Article (20)

The initiation of the offenses provided for in this Law shall be punishable by half of the prescribed penalty for the full offense.

Article (21)

Without prejudice to the criminal liability of the natural person, the legal person shall be liable to the fine prescribed for the offense if any of the offenses provided for in this law were committed in his name or for his account or for his benefit. This was the result of the approval or concealment or gross negligence of any member of the board of directors, Any other official authorized by such legal person.

In the event of a return, the court may decide to dissolve the legal person or close the headquarters in which the crime or the place in which the offense was committed has been closed for a final period or for the period estimated by the court.

Article (22)

(1) Except as provided in Chapter Two of this Law, the provisions of the Code of Criminal Procedure shall apply to the offenses provided for in this Law, to the extent permitted by the nature and the means of storing the data.

2. In the application of the provisions of this Act, the meaning of the word "thing" or "objects" in the Code of Criminal Procedure includes the term "information technology system" or "any part thereof", "information technology medium" and " Information technology "contained in this law.

The meaning of the words "papers", "documents", "editors", "letters", "letters" and "publications" in the Code of Criminal Procedure means "information technology means".

Article (23)

Except as provided for in this law, whoever commits an offense stipulated in any other law by means of a system or any technical means of information shall be punished by the prescribed penalty for that crime.

Article (24)

The Prime Minister and the Ministers, each within his own jurisdiction, shall implement the provisions of this Law and shall come into force one month after the date of its publication in the Official Gazette.

King of the Kingdom of Bahrain

Hamad bin Isa Al Khalifa

Issued at Riffa Palace:

Date: 6 Dhu al-Hijjah 1435 e

Corresponding to: 30 September 2014