**Disclaimer: The official version of the law and any amendments thereto is published in Arabic in the Official Gazette. This version of the law, including amendments thereto, is provided for guidance and easy reference purposes. The Legislation & Legal Opinion Commission does not accept any liability for any discrepancy between this version and the official version as published in the Official Gazette and / or any inaccuracy or errors in the translation.**

**For any corrections, remarks, or suggestions, kindly contact us on translate@lloc.gov.bh**

**Published on the website on May 2024**

**Law No. (60) of 2014 on Information technology crimes**

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

Having reviewed the Constitution;

Penal Code promulgated by Legislative Decree No. (15) of 1976, as amended;

Legislative Decree No. (17) of 1976 regarding Juveniles, as amended by the Legislative Decree No. (23) of 2013;

Legislative Decree No. (4) of 2001 regarding the Prohibition and Combating Money Laundering as amended;

Legislative Decree No. (28) of 2002 regarding the Electronic Transactions as amended;

Criminal Procedures Law promulgated by Legislative Decree No.(46) of 2002 as amended;

Legislative Decree No. (47) of 2002 regarding the Regulation of the Press, Printing and Publishing;

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 on the involvement of children in armed conflict and on the sale of children, child prostitution and child pornography attached to the United Nations Convention on the Rights of the Child;

Law No. (22) of 2006 regarding the Protection of Copyright and Related Rights, as amended;

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

And the Law No. (64) of 2006 promulgating the Central Bank of Bahrain and Financial Institutions Law;

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

**Introductory Chapter**

**Article (1)**

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

**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 Information technology tools, in particular, writing, still images, moving images, sound, numbers, letters, symbols, signs, etc.

**Information technology tool:** any tool or instrument that is electronic, magnetic, optical, electrochemical, or any tool that integrates communication, computing or any other tool that has the ability to receive, transmit, process, store and retrieve data very quickly.

**Information technology System:** A connected or related tool or set of tools, one or more of which automatically processes the data of the Information technology instrument according to a program.

**Information technology tool data:** Representation of realities, or facts, or information or comprehension in an appropriate form enabling the Information Technology 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 Information technology 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 Information technology system;

b) any other entity that processes or stores the data of the Information technology on behalf of the entity referred to in clause (a) of this paragraph or the users of its services.

**Route data:** Information technology data produced by the Information technology system related to the communication by the Information technology system that forms part of this communication process.

**Content data:** Information technology tool data, unlike route data, is sent as part of a connection.

**Damage:** Denatures, deactivates, cancels, deletes, destroys, alters, modifies, distorts or obscures the information technology tool data, or denatures or obstruction of the information technology system.

**Encryption:** The process of converting information, systems or information technology tools, or communications into incomprehensible or scattered symbols difficult to read or know without restoring them to their original form using a specific password or encryption device.

**Chapter One**

**Penalties for Information Technology Crimes**

**Section One**

**Crimes against the information technology tool’s systems and data**

**Article (2)**

ِAny person who, without legal justification, enters the information technology system or part of it shall be subjected to imprisonment for no more than one year and a fine not exceeding thirty thousand dinars or one of these two penalties.

If the entry results in disclosure of the data stored in the information technology tool or systems or a part of it, this shall be considered as an aggravating circumstance.

**Article (3)**

Any person who causes damage to information technology tool data or to the information technology system shall be subjected to imprisonment and a fine not exceeding fifty thousand dinars, or either of these two penalties.

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) alters, denatures or deletes medical examinations, medical diagnosis or treatment of a person.

The penalty shall be life imprisonment or a determinate term of imprisonment if the crime committed involves the intentional death of a person.

**Article (4)**

Without prejudice to more severe penalties provided by any other law, anyone who eavesdrops on, intercepts or obstructs, without legal justification, by technical tools, a transmission not intended for the public of information technology tool data, whether the data is sent from, to or within the information technology system, and this transmission includes any emission of electromagnetic waves from the information technology system which transmits this data. Shall be subjected to imprisonment and a fine not exceeding one hundred thousand dinars or either of these two penalties.

And if the eavesdropping, intercepting or obstruction involves the disclosure of the transmission or part of it without legal justification, it shall be considered an aggravating circumstance.

**Article (5)**

Without prejudice to more severe penalties provided by any other law, a person who sends any data from an information technology tool containing a threat to cause damage in order to induce another person to offer him or others a present or advantage of any kind or to perform or refrain from performing any other act.  shall be subjected to imprisonment and a fine not exceeding thirty thousand dinars, or by either of these two penalties.

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 objective.

**Article (6)**

A penalty of imprisonment for not more than one year and a fine not exceeding one hundred thousand dinars, or by either of these two penalties, shall be imposed on any person with the intention of committing one of the offences provided for in Articles (2, 3, 4, 5) of this law, produces, imports, buys, sells, offers for sale or uses, distributes, circulates, possesses, publishes or freely distributes:

a) A tool, including any software, that has been designed or modified principally for the purpose of committing one of the offences referred to above.

b) any password, access code or any other pass code or similar information technology tool data, of which an information technology system or part of it can be accessed.

**Section Two**

**Crimes related to the information technology tools**

**Article (7)**

A penalty of imprisonment for not more than ten years shall be imposed on any person who inserts, denatures, deactivates, cancels, deletes, destroys, alters, modifies, distorts or obscures the information technology tool data, owned by one of the government departments or entities mentioned in Article (107) of the Penal Code. For the purpose intended, to use data in a way that would show incorrect data to be true, with the intention of using it as if it were correct data, whether that data is understood directly or indirectly.

A penalty of imprisonment shall be imposed if the offence is committed in relation to the information technology tool data that does not belong to one of the departments or entities referred to in the previous paragraph, if this is likely to cause harm.

**Article (8)**

A prison sentence shall be imposed on anyone who, without legal justification, seizes money from others, or obtains any advantage for himself or for others, or signs, cancels, destroys or modifies a deed by adopting a false name or an incorrect capacity, or by using a fraudulent method, by one of the following means:

a) inserts, denatures, deactivates, cancels, deletes, destroys, alters, modifies, distorts or obscures the information technology tool data.

b) make any interference in the work of the information technology system.

The aggravating circumstance provided for in the second paragraph of article (391) and the second paragraph of article (392) of the Penal Code applies to this crime.

**Article (9)**

A penalty of imprisonment and a fine not exceeding one hundred thousand dinars or either of these two penalties, shall be imposed on any person who uses encryption to commit or hide any of the offences provided for by this or any other law.

**Section Three**

**Crimes related to content**

**Article (10)**

Without prejudice to more severe penalties provided by any other law:

1) A penalty of imprisonment for at least one year and a fine not exceeding ten thousand dinars, or either of these two penalties, shall be imposed on any person who commits one of the following acts:

a) Producing pornographic content with the intention to distribute it via information technology system.

b) Import, sell, offer for sale or use, exchange, transfer, distribute, send, publish or make available pornographic content via information technology system. The penalty shall be imprisonment for at least two years and a fine not exceeding ten thousand dinars, or either of these two penalties, if the pornographic content is intended for children or placed within their reach.

2) A penalty of imprisonment for at least three months and a fine not exceeding three thousand dinars, or either of these two penalties, shall be imposed on any person who commits one of the following acts:

a) Obtains pornographic content for himself or for others via the information technology system.

b) Possess pornographic content on the information technology system or on any other information technology tool. The penalty shall be imprisonment for at least six months and a fine not exceeding three thousand dinars, or either of these two penalties, if the pornographic content is intended for children or placed within their reach.

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 Two**

**Procedures for Information Technology Crimes**

**Article (11)**

The provisions of this Chapter shall apply to:

a) The crimes stipulated in Chapter One of this Law.

b) Crimes provided for in any other law if they are committed via the information technology system.

c) Collecting electronic proof related to any crime.

**Article (12)**

1) The Public Prosecution shall be entitled to order any person to preserve as a matter of urgency the safety of certain information technology tool data, including route data stored in the information technology system, in his possession or under his control, and to maintain the safety of such data whenever it is considered necessary to reveal the facts of any crime and evidence the leads to believe that such data is subject to loss or alteration.

2) The Public Prosecution shall be entitled to order the person referred to in paragraph (1) of this Article to preserve and maintain the safety of the data for a period not exceeding ninety days, and the high criminal court convening in chambers may authorise the Public prosecutor, on the basis of a substantiated request submitted three days before the expiry of the period referred to above, to extend this period for a further period or successive periods, which in total shall not exceed another ninety days. The court shall - as far as possible - hear the statements of the person concerned.

3) The Public Prosecution shall be entitled to order the person referred to in paragraph (1) of this Article to maintain the confidentiality of the order issued to him 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 of successive days, the total of which shall not exceed another ninety days, and in accordance with the procedure provided for in paragraph (2) thereto.

**Article (13)**

1) The Public Prosecution shall be entitled to order any person who is in possession or in control of certain information technology tool data to transmit it without delay, including information stored in an information technology system or any information technology tool.

2) The Public Prosecution shall be entitled to order any service provider to supply any information in its possession or in its control about any subscriber or user of its services, whether that information takes the form of information technology tool data or any other form. Such information does not include the route data and content.

All this when the public Prosecution deems it necessary to reveal the truth in the crime.

**Article (14)**

The judge of the lower court shall, at the request of the Public Prosecution, and upon examination of the papers, order the following:

a) To preserve rapidly the route data relating to the crime, regardless of whether the transmission was made by one or more service providers.

b) Disclosure of a sufficient quantity of route data to enable the public prosecution to establish the provider of the service and the route by which the data was transmitted, whenever this helps to reveal the truth about any crime punishable under this or any other law. In such cases, the judge shall issue an order with a statement of justification.

**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 tool stored therein.

b) Any means of data storage of an information technology tool data on which crime-related data is likely to be stored.

2) If, during the execution of the order referred to in clause (a) of paragraph (1) of this Article, the Public Prosecution has reliable indications that the data relating to the crime is stored in another information technology system or part thereof. And this data is accessible via the first information technology system, or is legally available from it, the Public Prosecution shall be entitled to issue a substantiated order to extend the access and search to the other system.

**Article (16)**

1) The Public Prosecution shall have the authority to control and reserve the information technology tool data accessible on the basis of the provisions of Article (15) of this Law, which includes the following:

a) The control and reservation of the information technology system, or any part thereof, or any of the information technology tool data storage means.

b) Reproducing of data from the information technology tool and conservation of the copy.

c) Maintaining the safety of the information technology tool data.

d) Uploading information technology tool date from the information technology system which was accessed or makes access to it unavailable.

2) The power of control and reservation referred to in paragraph (1) of this article shall not include any information which 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 competent or knowledgeable person aware of the functions of the information technology system and the measures applied to protect the data stored in that system to provide, as far as is reasonable, the necessary information to enable the procedures provided for in Articles (15) and (16) of this law to be executed. The judge shall assess, if necessary, the fees of the person he has instructed to handle the order.

**Article (18)**

1) Subject to the controls provided for in clause (b) of article (14) of this law, the public prosecution may, after obtaining the authorisation of the judge of the lower court, proceed as follows:

a) Assign any competent person to collect and record route data and content data, or any of them, linked to specific communications that are sent by the information technology system, when these communications occur.

b) Assign any service provider to carry out the work referred to in clause (a) or provide the necessary assistance to anyone instructed by the Public Prosecution Service to carry out this work.

c) Assign any competent person to obstruct the contents of any information technology or any part of it by means of which an Information technology crime has been committed. In all cases, the authorisation must be for a period not exceeding thirty days, renewable for one or more similar periods.

2) It shall be prohibited for a person who has been instructed under the provisions of paragraph (1) of this Article to disclose, without legal justification, to any other person about that assignment or any information relating thereto, or to benefit in any way thereby.

**Article (19)**

1) A penalty of imprisonment for not more than two years and a fine not exceeding one hundred thousand dinars or either of these two penalties shall be imposed on any persons who fail to comply with this order before the expiry of the deadline set by the judge of the lower court or the public prosecution, as the case may be, with an order or assignment issued in accordance with either paragraph (1) or (2) of Article (12), or Article (13) or (14), or paragraph (1) of Article (18) of this Law.

2) A penalty of imprisonment for not more than one year and a fine not exceeding thirty thousand dinars or either of these two penalties any person who violates:

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.

If the offender is a public official or assigned to a public service. The penalty shall be imprisonment not exceeding five years.

**Chapter Three**

**Miscellaneous provisions**

**Article (20)**

Attempts to commit the crimes stipulated in this law shall be punished by half the penalty for the full crime.

**Article (21)**

Without prejudice to the criminal liability of the natural person, a legal person shall be punished by the fine provided for the crime if any of the crimes provided for by this law is committed in his name, on his behalf or for his benefit, and was the result of the approval, concealment or serious negligence of a member of the board of directors, a president, a director or any other official authorised by that legal person.

In the event of a recidivism, the court may order the dissolution of the legal person or the permanent closure of the place where the crime was committed or of the places where it carries out an activity related to the crime, or for the period estimated by the court.

**Article (22)**

1) With the exception of what is stipulated in chapter two of this law, the provisions of the Criminal Procedure law apply to the crimes covered by this law in proportion and to the extent permitted by the nature of the information technology tool system and date the storage devices for these data.

2) In the application of the provisions of this law, the meaning of the word "thing" or "things" referred to in the Criminal Procedure Law includes the terms "information technology system" or "any part of it", "information technology tool data" and "any information technology tool data storage means". contained in this law.

The meaning of the words "papers", "documents", "editorials”, “correspondence”, "letters", and "publications" in the Criminal Procedure Law includes the phrase "information technology tool data" in this law.

**Article (23)**

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

**Article (24)**

The Prime Minister and the ministers - each within his jurisdiction- shall implement the provisions of this Law and shall come into force following the lapse of one month from the date of its publication in the Official Gazette.

**King of the Kingdom of Bahrain**

**Hamad bin Isa Al Khalifa,**

Issued at Riffa Palace:

On: 6 Dhu al-Hijjah 1435 A.H.

Corresponding to: 30 September 2014