Presidential Decree No. (16) for the year 2017
Regarding Cybercrime

President of the State of Palestine
Chairman of the Executive Committee of the Palestine Liberation Organization

In accordance with the provisions of the amended Basic Law of 2003, as amended, in particular the provisions of Article (43) thereof, and after reviewing the Law No. 74 for the year 1963 and its amendments in force in the Southern Governorates, and the provisions of the Jordanian Penal Code No. 16 for the year 1960 and its amendments, in force in the Northern Governorates,
Law No. (3) for the year 1996 regarding wired and wireless telecommunications,
Code of Criminal Procedure No. (3) for the year 2001 and its amendments,
Law No. 18 for the year 2015 regarding the Control of Narcotic Drugs and Psychotropic Substances,
Law No. (20) for the year 2015 regarding Combating Money Laundering and the Financing of Terrorism and its amendments,
based on the recommendation of the Council of Ministers on 20/06/2017,
and the powers vested in us,
in the interest of the public,
in the name of the Palestinian Arab people,
we have issued the following Presidential Decree

Article (1)

The words and phrases in this Presidential Decree shall have the meanings assigned to them below, unless the context indicates otherwise:
Ministry: Ministry of Telecommunications and Information Technology.
Minister: Minister of Telecommunications and Information Technology.
Data Processing: To perform or execute an operation or a series of operations on data, whether relating to individuals or otherwise, including the collection, reception, recording, storage, modification, transfer, retrieval, deletion, publication or re-publication of data, blocking access to data, as well as shutting down, cancelling or modifying the contents of devices.
Information Technology: Any means, electronic, magnetic, optical, electrochemical or other, both material and immaterial, or a group of interconnected or unconnected means, used for processing data, performing logic, arithmetic, or storage functions, and including any data storage capacity or communications related to or working in conjunction with such means.
Electronic Data: Anything that can be stored, processed, created, or transmitted using information technology, particularly written text, images, sound, numbers, letters, symbols, signs, and others.
Electronic Information: Any information that can be stored, processed, supplied, and transmitted by means of information technology, particularly by written text, images, sound, numbers, letters, symbols, signs, and others.

Electronic Network: A connection between more than one information technology means that is used to obtain and exchange information. This includes private and public networks, as well as the World Wide Web (the Internet).

Electronic Record: An accumulation of information which describes a situation involving an individual or a series of events**.** This record is generated, sent, received or stored by electronic means.

Electronic Document: An electronic record that is issued using an information technology means. This record is created, stored, extracted, copied, sent, communicated or received by means of an information technology, be it on a physical medium or any other form of electronic medium, and which is recoverable in a comprehensible form.

Website: A place on the electronic network which makes information and services available through a specific address.

Person: Natural or legal person.

Electronic Application: An electronic program designed to perform a defined task, either directly for the user or for another electronic program**.** It is utilized through means of information technology or the like.

Traffic Data: Any data or electronic information generated by information technology indicating the source and destination of a transmission, as well as the route, time, data, size, duration or type of a communication service.

Password: Encompasses anything that is used to access an information technology system in order to verify that it is part of the traffic data. These means of verification may include, but are not limited to, a string of letters and characters, fingerprint scanners, iris scanners or face scanners.

Electronic Transaction: An electronic card that contains a magnetic strip or a smart chip or the like and which uses an information technology or an electronic application. It contains electronic data issued by an authorized party.

Government Data: This includes any data belonging to the State, public bodies, public institutions as well as their corresponding subsidiaries.

Encryption: The process by which electronic data is converted into a form which is impossible to decipher without having access to the proper key.

Code: A secret private key or keys used by a person or entity to encrypt computer data into numbers, letters, symbols or the like.

Capture: To view or obtain data or information.

Breakthrough: An unauthorized or illegal access to an IT system or electronic network.

Electronic Signature: Electronic data which is added, attached or linked to an electronic transaction, and which identifies the person who made it. Every signature is unique which allows it to be used to approve the contents of a transaction.

Signature Tool: A program used to create an electronic signature for a transaction.

Certificate: Electronic certificates are issued by the Ministry or by an authorized body. They prove the relationship between a website and its electronic signature data.

Service Provider: Includes anyone who offers the service of being able to communicate via IT, or who processes, stores, or hosts computer data on behalf of any electronic service or users of the service.

Destruction: The manipulation of electronic software to render it unusable, either by destroying it completely or partially.

Subscriber Information: Any information provided by the service provider relating to the service subscribers, including:

- Type of communication service used, technical conditions and service period.
- The subscriber's identity, postal or geographic address, telephone number, as well as the payment information collected in the service agreement or during its installation.
- Any other information pertaining to the location of the installed communication equipment as specified in the service agreement.

Employee: Anyone who works in the public or private sectors, private institutions, local and civil bodies, associations, private companies supported by state contributions, or the like.

Article (2)

1. The provisions of this resolution shall be applied by law to any of the crimes provided for therein, if committed wholly or partially within or outside of Palestine. Regardless of if the actor is the perpetrator, a partner, or an instigator, the individual shall be subject to the general principles contained in the applicable Penal Code.
2. Any person who commits one of the crimes stipulated in this resolution outside of Palestine may be prosecuted in one of the following instances:
   A. If committed by a Palestinian citizen.
   B. If committed against a Palestinian party or against Palestinian interests.
   C. If committed against foreign parties or interests by a foreigner or a stateless person whose habitual residence is in Palestine, or by a foreigner or stateless person present in the Palestinian territories, for whom the conditions of legal extradition are not satisfied.

Article (3)

1. A specialized unit for cybercrime shall be established in the police and security forces, provided that it has judicial authority. The public prosecution shall supervise the judicial control officers within their jurisdiction.
2. In accordance with their mandates, the regular courts and the public prosecution shall review the cases of electronic crimes.

Article (4)

1. Any person who has intentionally and unlawfully accessed any electronic system or network, has abused any information technology or part thereof, or has exceeded the authorized entry shall be liable to either imprisonment, a fine between two hundred and one thousand Jordanian dinars, or a combination of the two.
2. If the act specified in paragraph (1) of this article is committed against any official statement by the government, the culprit shall be punished by imprisonment for a period of at least six months, or by a fine of no less than two hundred Jordanian dinars and no more than one thousand Jordanian dinars, or by a combination of both punishments.
3. If access results in the deletion, addition, disclosure, destruction, alteration, transfer, capture, copy, dissemination, reproduction or attachment of data or electronic

information stored in the information system which causes damage to users or beneficiaries, alters the website, revokes it, modifies its contents, fills its address, alters its design or method of use, impersonates its owner or manages it at their place, the responsible actor shall be punished by temporary hard labor for a period not exceeding five years and a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars, or the equivalent in other legally traded currency.

4. If the act specified in paragraph (3) of this Article is committed against governmental data, the offender shall be sentenced to a minimum of five years of temporary hard labor and will have to pay a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars or the equivalent thereof in the legally circulated currency.

Article (5)

Any person who obstructs or disrupts the access to services, devices, programs, data sources or information, by any means available to them through the Internet or an information technology, shall be punished by imprisonment or by a fine of no less than two hundred Jordanian dinars and no more than one thousand Jordanian dinars, or its equivalent in the legally circulated currency, or by a combination of both punishments.

Article (6)

Anyone who has produced or deployed through an electronic network or an information technology means anything that can stop or disrupt another information technology platform, or that can destroy, delete, or modify programs, will be sentenced to temporary hard labor and a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars, or the equivalent in the legally circulated currency.

Article (7)

Anyone who receives or intercepts data which is transmitted through a computer network or an information technology device without the explicit right to do so, shall be punished by imprisonment or by a fine of no less than one thousand Jordanian dinars and no more than three thousand Jordanian dinars or by a combination of both punishments.

Article (8)

1. Any person who deliberately decrypts encrypted data without the explicit legal authorization shall be punished by imprisonment or by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.
2. Any person who unlawfully uses personal encryption elements or the electronic signature creation tool to forge the signature of another person, shall be punished by imprisonment or by a fine of no less than two thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.

3. Any person who commits an offence mentioned in paragraph (2) of this article shall be punished by temporary hard labor and by a fine of no less than two thousand Jordanian dinars or the equivalent thereof in the legally circulated currency.

Article (9)

1. Any person who unlawfully benefits from communication services by means of an information technology shall be punished by imprisonment for a period of at least six months or by a fine of no less than five hundred Jordanian dinars and no more than three thousand Jordanian dinars or by a combination of both punishments.
2. If the unlawful use specified in paragraph (1) of this article is for the purpose of profit, the culprit shall be punished by imprisonment for a period of at least one year or by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.

Article (10)

Any person who deliberately creates or publishes an incorrect certificate or provides incorrect data of his identity to the competent authorities as specified in the laws concerning issuing a certificate, applying for a certificate, or having it revoked or suspended, shall be punished by imprisonment and a fine of no less than two hundred Jordanian dinars and no more than one thousand Jordanian dinars, or its equivalent in the legally circulated currency.

Article (11)

1. Any person who falsifies an official electronic document of the State or of a public body and its institutions that is recognized by law by using an information system shall be punished by hard labor of no less than five years and a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars or the equivalent in the legally circulated currency.
2. If the forgery is committed on documents other than those specified, this constitutes a crime punishable by imprisonment or by a fine of no less than five hundred Jordanian dinars and no more than three thousand Jordanian dinars or by a combination of both penalties.
3. Anyone who uses the forged document despite having knowledge of their forged nature shall be punished by the prescribed penalty for the offense of forgery, as deemed appropriate.
4. Anyone who falsifies or manipulates an official signature, signature tool, or electronic signature system, whether by counterfeiting, destruction, alteration, modification, or in any other manner that alters the nature of the data or information, shall be punished by imprisonment for a period of at least five years and by a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars, or the equivalent in the legally circulated currency.
5. The forgery of or tampering with the electronic signatures mentioned in paragraph (4) of this article shall be punishable by imprisonment or by a fine of no less than five hundred

Jordanian dinars and no more than three thousand Jordanian dinars or by a combination of both punishments.

6. Any person who has created signature data or an instrument of an official electronic signature system, or of a public body or institution, without authorization, using false information or data, or has colluded with others in its creation, will be punished with five years of imprisonment or by a fine of no less than five thousand Jordanian dinars and no more than three thousand Jordanian dinars or by a combination of both penalties.

Article (12)

1. Any person who uses the electronic network or any other means of information technology to unlawfully access or manipulate the numbers or data of an electronic system shall be punished by imprisonment for a period of at least six months or by a fine of no less than five hundred Jordanian dinars and no more than three thousand Jordanian dinars or by a combination of both punishments.
2. Any person who falsifies electronic transaction means or tools in any way, or creates or obtains these without the proper certificates shall be punished by the same penalty described in paragraph (1) of this article.
3. Anyone who knowingly uses or facilitates the use of counterfeit electronic transaction means or electronic transactions that are not valid, or are forged or stolen, shall be punished by the same penalty as described in paragraph (1) of this article.
4. If the intention is to use the counterfeit transaction means to obtain another person's funds, data, or any subsequent services, this shall be punished by imprisonment for a period of no less than one year or by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or by both penalties.
5. If the forgery results in the obtention of another person's money, whether for oneself or for another person, the responsible actor shall be imprisoned for a period of no less than two years or shall have to pay a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or be subjected to both punishments.

Article (13)

Anyone who uses an electronic network or any other type of information technology to steal or embezzle funds shall be punished by temporary hard labor or by a fine of no less than two thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.

Article (14)

Any person who obtains movable property, documents, or an electronic signature or the means to create one through an electronic network or by any other means of information technology, either for himself or for someone else, by fraudulent means, by using a fake name or by impersonating someone, for the purpose of deceiving the victim, shall be punished by imprisonment for a period of at least one year or by a fine of no less than two thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.

Article (15)

1. Anyone who uses the Internet or an information technology device to threaten or blackmail another person to carry out an act or to refrain from doing so, even if such an act or omission is lawful, shall be punished by imprisonment or by a fine of no less than two thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.
2. If a person threatens to commit a felony or an immoral act, they shall be punished by temporary hard labor and by a fine of no less than two thousand Jordanian dinars and no more than five thousand Jordanian dinars, or the equivalent thereof in the legally circulated currency.

Article (16)

1. Anyone who has produced any material that infringes upon public morals, or has arranged, prepared, sent or stored it for the purpose of exploiting, distributing or presenting it to others through an electronic network, an information technology platform, or an animation shall be punished by imprisonment for a period of no less than one year or by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or by both penalties.
2. Any person who creates a website, an application or an electronic account, or who publishes information on the Internet or on another information technology platform in order to facilitate programs and ideas that infringe upon public morality shall be punished by imprisonment for a period of at least one year or by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.
3. If the act specified in paragraphs (1) and (2) of this article is directed at a child, this carries a punishment of temporary hard labor for a period of no less than seven years and a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars, or the equivalent thereof in the legally circulated currency.
4. If the content of the act described in paragraph (1) of this article contains a child, a child's image, or images simulating a child, the responsible actor shall be punished by temporary hard labor for a period of no less than seven years and by a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars or the equivalent in the legally circulated currency.

Article (17)

Anyone who sets up a website, application, electronic account, or who disseminates information on the Internet or an information technology device for the purpose of participating in human trafficking or in order to facilitate it, be it of human beings or of their organs, shall be punished by hard labor of at least ten years and by a fine of no less than ten thousand Jordanian dinars

and no more than twenty thousand Jordanian dinars, or the equivalent in the legally circulated currency.

Article (18)

Without prejudice to the provisions of the law fighting money laundering and financing terrorism, anyone who creates a website, application or electronic account or who disseminates information on the Internet or on any other information technology platform with the intent to commit money laundering or to finance terrorism shall be punished by temporary hard labor of no less than ten years and by a fine of no less than ten thousand Jordanian dinars and no more than twenty thousand Jordanian dinars, or the equivalent in the legally circulated currency.

Article (19)

Anyone who creates a website or an information technology device for the purpose of trafficking or promoting narcotic drugs, psychotropic substances or the like, or in order to facilitate the dealing, selling or production of narcotic substances shall be punished by imprisonment for a period of at least ten years and by a fine of no less than ten thousand Jordanian dinars and no more than twenty thousand Jordanian dinars, or the equivalent in the legally circulated currency.

Article (20)

1. Anyone who creates or manages a website or an information technology platform that aims to publish news that would endanger the integrity of the Palestinian state, the public order or the internal or external security of the State, shall be punished by imprisonment for a period of at least one year or by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.
2. Any person who propagates the kinds of news mentioned above by any means, including broadcasting or publishing them, shall be sentenced to a maximum of one year in prison or be required to pay a fine of no less than two hundred Jordanian dinar and no more than one thousand Jordanian dinars or be subjected to both penalties.
3. If the act in paragraphs (1) or (2) of this article is committed under an emergency status, the prescribed penalty shall be doubled.

Article (21)

Anyone who creates a website, an application or an electronic account, or disseminates information on the Internet or an information technology device with the intention of offending or violating a sacred or religious rite or belief shall be punished by imprisonment for a period of at least one year or by a fine of no less than two thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.

Article (22)

Anyone who creates a website, an application, or an electronic account, or publishes information on the Internet or an information technology device with the intent to attack any family principles or values relating to the inviolability of private and family life, whether directly or

indirectly, by publishing news, photos, audio or video recordings in order to defame others and harm them, shall be punished by imprisonment for a period of at least two years or by a fine of no less than three thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.

Article (23)

Anyone who creates a website, an application, or an electronic account, or who publishes information through a computer network or any other information technology platform to manage, facilitate, encourage, promote, or advertise gambling, shall be punished by imprisonment for a period of at least six months or by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars or by a combination of both punishments.

Article (24)

Anyone who creates a website, an application or an electronic account, or who publishes information through a computer network or any other information technology platform for the purpose of publishing and disseminating information that incites racial hatred, provokes racial discrimination against a particular group, or threatens aggression against someone because of their ethnic or sectarian affiliation, skin-color, looks or disability, shall be sentenced to temporary hard labor and a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars, or the equivalent thereof in the legally circulated currency.

Article (25)

Anyone who creates a website, application, electronic account, or who publishes information through a computer network or any information technology platform that justifies or incites committing acts of genocide or crimes against humanity, as defined under the international covenants, shall be punished by temporary hard labor for a period of at least ten years.

Article (26)

Whoever acquires any device, program, electronic data, password, or entry codes, or who exports, imports or issues them in order to commit any crime defined in this law shall be punished by hard labor for a period not exceeding five years and be issued a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars or the equivalent thereof in the legally circulated currency.

Article (27)

1. Any employee who commits any of the crimes stipulated in this Presidential Decree by exploiting their position or power at their workplace, or because of their work, or who aids and abets others committing the crime, shall be punished by imprisonment for a period of no less than one year or by a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars, or by a combination of both punishments.

2. Any employee of a service provider who commits any of the offenses stipulated in this decree during the course of performing their work, because of their work, or who aids and abets others to commit a crime, shall be punished by temporary hard labor for a period of no less than three years or by a fine of no less than ten thousand Jordanian dinars and no more than twenty thousand Jordanian dinars or by a combination of both punishments.

Article (28)

Any person who creates a website, an application or an electronic account, or who disseminates information on the Internet or an information technology platform with the intention of committing or enticing someone else to commit any offense punishable under any applicable legislation is subject to twice the punishment stipulated by the relevant law.

Article (29)

1. Any person who incites, assists with or agrees to commit an offense under the provisions of this decree by any electronic means shall be punished by two thirds of the maximum applicable penalty, as long as the offense was committed on the basis of the before mentioned incitement, assistance or agreement.
2. If the victim is a child, as defined in paragraph (1) of this article, the offender shall be punished by temporary hard labor for a period of no less than five years and by a fine of no less than two thousand Jordanian dinars and no more than five thousand Jordanian dinars or the equivalent thereof in the legally circulated currency, even if the crime did not actually occur.

Article (30)

If one of the offenses stipulated in this resolution was committed in the name of or on behalf of a legal entity, either the perpetrator or the legal entity or both shall be punished by a fine of no less than five thousand Jordanian dinars and no more than ten thousand Jordanian dinars. The court may prevent the legal entity and/or the perpetrator from continuing their (online) activity for a maximum period of five years, or may decide to completely dissolve the legal entity without prejudice to the criminal liability of the natural person.

Article (31)

Anyone who uses an electronic system, a website or an electronic application to bypass the blocking of a website or any other IT platform under the order of this resolution, shall be punished by imprisonment for a period of at least three months or by a fine of no less than five hundred Jordanian dinars and no more than one thousand Jordanian dinars or by a combination of both punishments.

Article (32)

Service providers commit, as per legal procedure, to the following:

1. At the request of the prosecution or the competent court they shall provide the competent authorities with all necessary data and information that will assist in uncovering the truth.
2. Based on the orders issued by the judicial authorities, and taking into account the procedures stated in article (40) of this law, they shall block any link, content or application on the Internet.
3. Retain information about the subscriber for at least three years.
4. In accordance with the decision of the competent judge of the court, they shall assist and cooperate with the competent authorities in collecting, recording and retaining information and electronic data.

Article (33)

1. The office of the public prosecutor or the person appointed by the judicial inspectors may inspect people, places and anything else related to information technology relevant to the crime.
2. The inspection order must be specific and may be renewed more than once, as long as the justification for the procedure remains relevant.
3. If the inspection specified in paragraph (2) of this article results in the seizure of devices, tools or means related to the crime, the judicial inspectors shall prepare a record of the seizures and submit them to the public prosecution in order for them to take the necessary action.
4. The attorney general may authorize the judicial control officers or their competent personnel to have direct access to any information technology they need in order to be able to conduct their inspection.
5. The judicial ombudsman is required to be competent to deal with the specific nature of cybercrime.

Article (34)

1. The public prosecution shall have access to devices, tools, means, data, electronic information, traffic data, users and other information related to cybercrime.
2. The prosecutor has the permission to seize and retain the entire information system and to make use of any IT tools that would help to uncover the truth.
3. If the seizure and retention of the information system is not necessary or cannot be performed, the direct and indirect data relating to the crime shall be copied and made available to the prosecutor.
4. If it is impossible to physically capture or seize the relevant data pertaining to the crime, all appropriate means shall be used to prevent access to data stored in the information system in order to preserve the evidence of the crime.
5. All necessary precautions must be taken in order to maintain the integrity of the seized and retained materials. This includes using all the technical means available to protect its content.
6. A list of seized and retained materials shall be produced in the presence of the defendant, or the person in whose possession the materials were in at the time of

seizure, and a report shall be made. The seized materials shall be kept in a sealed envelope or envelopes containing the date and time of the retention as well as the number of the proceeding and of the case.

Article (35)

1. The Magistrate's Court may authorize the public prosecution to monitor, register and deal with communications and electronic conversations in order to uncover evidence relating to the crime. This authorization is valid for a period of fifteen days and is renewable once, providing the availability of new evidence.
2. The public prosecution may order the immediate collection and provision of any data, including communications, electronic information, traffic data or metadata that it deems necessary to conduct the investigations. The public prosecution shall use the appropriate technical means and may resort to consulting the service providers if necessary.

Article (36)

Pending the decision by the relevant judicial authority, the competent authorities shall take the appropriate measures and establish procedures to ensure the safety of the devices, tools, means of information technology, electronic systems, data (electronic information) and the privacy of the retained materials.

Article (37)

1. The competent court may authorize the immediate objection to the metadata and may record or copy them at the request of the attorney general or at the request of one of his or her aides. The decision of the court shall include all the elements that would define the communications which are subject to the objection.
2. The duration of the objection specified in paragraph (1) of this article shall be three months from the date of actual commencement, which may only be extended once.
3. The authority responsible for implementing the objection shall inform the public prosecution of the date of actual commencement of the objection process and coordinate the necessary measures for it to function properly.

Article (38)

Any evidence resulting from any information technology means, information system, information network, website or electronic data may not be excluded because of the nature of the evidence.

Article (39)

Any evidence obtained by the competent authority or by the investigative authorities of the State shall not be excluded, as long as the access was in accordance with the legal and judicial procedures for international cooperation.

Article (40)

1. If a website hosted within or outside the country detects any statements, numbers, images, films, propaganda or other material that may threaten the national security, civil peace, public order or public morals, the relevant investigation and control authorities shall submit a statement to the attorney general or to one of his assistants requesting permission to block the site, the websites or to block some of the links from being displayed.
2. The attorney general or one of his assistants shall apply to the Magistrates Court within 24 hours for a permission, accompanied by a memorandum of opinion, whereby the court shall issue its decision on the same date the request is made as to whether to accept or reject such request.

Article (41)

With exception of the professional obligations provided for in the law, the secrets or requirements of a profession may not be invoked to refrain from providing the information or documents required which are in accordance with the provisions of the law.

Article (42)

The organs of the State, as well as its various institutions, bodies and entities shall comply with the following:

1. Take the necessary preventive security measures to protect their information systems, websites, information networks, and electronic data and information.
2. To immediately notify the competent authority of any crime specified in this resolution. This includes the discovery of any attempt to intercept data or illegally wiretap. In addition, they must provide the competent authority with all information needed to reveal the truth.
3. Maintain information technology and subscriber information for at least 120 days and provide the competent authority with such data.
4. Cooperate with the responsible authorities to implement their mandates.

Article (43)

1. The responsible authorities shall facilitate cooperation with their counterparts in foreign countries within the framework of ratified international, regional and bilateral agreements, or in applying the principle of reciprocity, in order to expedite the exchange of information and to ensure an early warning of potential abuse and thus to prevent crimes pertaining to information and communication systems.
2. The cooperation referred to in paragraph (1) of this article shall be fostered under the condition that the foreign state preserves the confidentiality of the information relating to it, does not forward it to another party and does not exploit it for purposes other than to combat the offenses covered by this resolution.

Article (44)

1. The competent authorities shall provide assistance to counterparts in other States for the purposes of mutual legal assistance and extradition of criminal investigations and

proceedings associated with the offenses set out in this resolution, in accordance with the rules established by the Code of Criminal Procedure as well as bilateral and multilateral agreements of the State and the principle of reciprocity, and in a manner that is consistent with the provisions of this resolution or any other law.

2. The request for legal assistance or extradition based on the provisions of this resolution shall be carried out only if the offense is also illegal in the state requesting the information, or if that state criminalizes a similar crime. Double criminality can be applied irrespective of whether the laws of the requesting state are in the same category of offense or use the same designation of the offense, provided that the act in question is criminalized under the laws of the requesting state.

Article (45)

Without prejudice to the applicable penal code or any other law that may codify more severe punishments, the perpetrators found guilty of the offenses contained within the provisions of this decree shall be sentenced according to the corresponding penalties provided for therein.

Article (46)

Any person who commits, participates in, intervenes in or instigates an act using the Internet or any other means of information technology and which constitutes an offense under any applicable legislation, shall be liable to the penalty codified for the crime in question under the applicable legislation.

Article (47)

Anyone who creates a website that aims to promote committing any of the crimes stipulated in the penal code or in any of the special laws shall be punished by temporary imprisonment and by a fine of at least five thousand Jordanian dinars and no more than ten thousand Jordanian dinars, or the equivalent in the legally circulated currency.

Article (48)

Any person who discloses the confidentiality of the procedures provided for in this resolution, other than in cases authorized by law, shall be punished by imprisonment and by a fine of no less than five hundred Jordanian dinars and no more than three thousand Jordanian dinars or by one of the two punishments.

Article (49)

Any person who is found guilty of tampering with, hiding, modifying or erasing judicial evidence shall be punished by imprisonment for a period of no less than one year and by a fine of no less than one thousand Jordanian dinars and no more than five thousand Jordanian dinars, or the equivalent thereof in the legally circulated currency.

Article (50)

Any person who deliberately refrains from reporting a crime or who knowingly misrepresents or withholds information shall be punished by imprisonment for a period of no less than six months

and by a fine of no less than two hundred Jordanian dinars and no more than one thousand Jordanian dinars or alternatively they may be subjected to only one of these two penalties.

Article (51)

If any of the offenses set out in this resolution are committed for the purpose of disturbing public order, endangering the safety and security of the community, endangering the lives of the citizens, preventing or obstructing the exercise of public works by the public authorities or obstructing the provisions of the Constitution, the Basic Law, or with the intention of harming national unity, social peace, contempt of religion, or that violate the rights and freedoms guaranteed by the Constitution or the Basic Law, the penalty shall be hard labor or temporary hard labor.

Article (52)

Anyone who participates by way of agreement, incitement, assistance or interference in committing a felony or a misdemeanor punishable under the provisions of this decree shall be punished by the same penalties as the main perpetrator.

Article (53)

Any person who started to commit a felony or misdemeanor that falls within the jurisdiction of this law, but was unable to complete it, shall be deemed to have committed a crime under the law and shall be punished by half of the codified penalty.

Article (54)

1. Without compromising the penalties provided for in this resolution or the good faith of others, the court shall issue a decision to confiscate the devices, programs or means used to commit any of the offenses which fall under the jurisdiction of this resolution at the expense of the owner.
2. The court shall issue a decision on how long a business shall remain closed or how long a website shall be blocked that had been involved in a crime

Article (55)

The penalty codified for in this Presidential Decree shall be doubled in the event that the offender repeats any of the crimes stipulated therein, regardless of whether it was committed in Palestine or abroad.

Article (56)

The penalty prescribed for offenses punishable under the provisions of this Presidential Decree shall be doubled in any of the following cases:

1. If the crime was committed or facilitated by an employee of a private establishment or by a public official exploiting their authority. Additionally, the public official shall be dismissed from office in case of conviction.

2. If the crime occurred on a site or or used an information system, data, numbers, letters, codes, or images administered by or owned by the State or by a public person or entity, including local authorities.
3. The perpetrator committed the crime through an organized gang.
4. Solicitation and exploitation of juveniles.
5. If the crime is committed against an information system, website or information network related to the transfer of funds, payment services, clearance services, settlements or any other services provided by banks or financial institutions.

Article (57)

Any person who informs the competent authorities of information about the crime and the persons involved in it shall be exempted from the penalties specified in this Presidential Decree, as long as this takes place before the competent authorities are aware of the situation and before any damages occur. The court may order a suspension of execution if the notification is received after the competent authorities gain knowledge of the event in the case that the remaining perpetrators are arrested as a result.

Article (58)

The ministry shall, in accordance with its competences, provide technical support and assistance to law enforcement agencies. Ministry employees appointed by the minister shall be deemed as judicial control officers for the purpose of implementing the provisions of this Presidential Decree.

Article (59)

Any contravention of the provisions of this Presidential Decree shall be repealed.

Article (60)

This Presidential Decree shall be presented to the legislative council in its first session for approval.

Article (61)

All the competent authorities shall implement the provisions of this Presidential Decree, each according to their competence, and it shall be effective from the date that it is published in the official gazette.

Issued in the city of Ramallah on: 24/06/2017 AD
Corresponding to: 29 Ramadan 2017(sic) Hijri

Mahmoud Abbas
President of the State of Palestine
Chairman of the Executive Committee of the Palestine Liberation Organization