

**Decree-Law No. (10) of 2018**  
**on**  
**Cybercrimes and Crimes of Telecommunications & IT**

*The title of this Decree-Law was amended pursuant to Article (2) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

**President of the State of Palestine**  
**Chairman of PLO Executive Committee**

In accordance with the provisions of the Amended Basic Law of 2003 as amended, in particular the provisions of Article (43) thereof,

And after having reviewed:

The provisions of the Penal Law No. (74) of 1936 as amended, in force in the Governorates of Gaza Strip;

The provisions of Penal Law No. (16) of 1960 as amended, in force in the Governorates of West Bank;

The provisions of Wire & Wireless Telecommunications Law No. (3) of 1996;

The provisions of Penal Procedure Law No. (3) of 2001 as amended;

The provisions of Decree-Law No. (18) of 2015 on Combating of Narcotic Drugs and Psychotropic Substances;

The provisions of Decree-Law No. (20) of 2015 on Combating of Money Laundering and Terrorism Financing as amended;

The provisions of Decree-Law No. (6) of 2017 on Regulation of Human Organ Transplantation and Transfer;

The provisions of Decree-Law No. (15) of 2017 on Electronic Transactions,

The provisions of Decree-Law No. (16) of 2017 on Cybercrimes;

AND based on the recommendation of the Council of Ministers dated 17/04/2018;

And in accordance with the powers vested in us,

And in pursuit of the public interest,

And in the name of the Palestinian Arab People,

We hereby promulgate the following Law:

### Article (1)

The terms and expressions mentioned in this Decree-Law shall have the meanings ascribed thereto below, unless the context indicates otherwise:

<b>Ministry</b>	The Ministry of Telecommunications and Digital Economy
<b>Minister</b>	The Minister of Telecommunications and Digital Economy
<b>Data Processing</b>	Conducting or carrying out a process or set of processes on data, whether related to individuals or otherwise, including the collection, receipt, recording, storage, modification, transfer, retrieval, erasure, publication, republication, denial of access, disabling devices, or deleting or altering their contents
<b>Information Technology</b>	Any electronic, magnetic, optical, electrochemical, or any other means, whether tangible or intangible, or any set of interconnected or non-interconnected tools used for data processing and performing logic, computation, or storage functions, including any data storage or communication capacity associated with or operating in conjunction with such means
<b>Electronic Data and Information</b>	Anything that can be stored, processed, created, supplied, or transmitted using information technology, including but not limited to writing, images, sound, numbers, letters, symbols, signals, and so forth
<b>Electronic Network</b>	A connection between more than one information technology tool to access and share information, including private or public networks, or the world wide web (Internet)
<b>e-Record</b>	A set of information constituting a description of a status relating to a person or object, created, sent, received, or stored by electronic means
<b>e-Document</b>	An electronic record issued using information technology, created, stored, extracted, copied, sent, communicated, or received by means of information technology on a physical or any other electronic medium, and retrievable in a comprehensible form
<b>Electronic Website</b>	A location for providing information or services on an electronic network through a particular address
<b>Person</b>	A natural or legal person
<b>Electronic Application</b>	A software application designed to perform a specific task directly for the user or another software application, used through information technology or equivalent means
<b>Traffic Data</b>	Any electronic data or information developed by means of information technology indicating the source of transmission, its destination, its route, time, date, volume, duration, and the type of communication service
<b>Password</b>	Anything used to access information technology systems or their equivalents to verify identity, considered part of traffic data and

	includes codes, retinal, facial, or fingerprint scans, or their equivalents
<b>e-Transaction Tool</b>	An electronic card containing a magnetic strip or smart chip or any equivalent technology or electronic application that includes electronic data or information issued by authorized entities
<b>Government Data</b>	Data related to the state, public institutions, or their affiliated companies
<b>Encryption</b>	The conversion of electronic data into a form that cannot be read or comprehend without restoring it to its original form.
<b>Code</b>	A secret key or keys specific to a person or entity used to encrypt computer data using numbers, letters, symbols, fingerprints, or equivalents
<b>Reception</b>	Viewing or obtaining data or information
<b>Hacking</b>	Unauthorized or unlawful access to information technology systems or electronic network
<b>e-Signature</b>	Electronic data added to, attached to, or logically associated with an electronic transaction, which identifies the signatory and distinguishes them for the purpose of consenting to the content of the transaction
<b>Signature Device</b>	Software used to create an electronic signature on a transaction.
<b>Certificate</b>	The electronic authentication certificate issued by the Ministry or a delegated authority to confirm the relationship between the signatory and their electronic signature data
<b>Service Provider</b>	Any person who enables users of their service to connect via information technology, or who processes, stores, or hosts computer data on behalf of any electronic service or its users
<b>Damage</b>	The complete or partial destruction of electronic software or rendering it unusable
<b>Subscriber Information</b>	Information held by the service provider regarding service subscribers, including the type of telecommunication service used, technical specifications, service duration, subscriber identity, postal or geographical address, phone number, payment details based on service agreements, and any information about the installation site of communication equipment based on such agreements
<b>Employee</b>	Each person who works in the public or private sectors, or in private institutions, local or civil bodies, associations, or private companies with state participation, and the like
<b>Confinement</b>	Placing the convicted person in a state prison for a period ranging between one week and three years by a judicial ruling
<b>Imprisonment</b>	Placing the convicted person in a state prison for a period ranging between three and fifteen years by a judicial ruling
<b>Authority</b>	The Telecommunications Regulatory Authority

<b>License</b>	The certificate issued by the Authority confirming that a person has fulfilled the legal requirements to be authorized to establish, operate, or manage a public telecommunications network, provide public telecommunications services, or use radio frequencies or radio waves, in accordance with the law
<b>Licensee</b>	The person granted the license by the Authority
<b>Telecommunications</b>	The transmission, sending, receiving, broadcasting, or routing of voice, data, signals, symbols, video, or images by wired, wireless, radio, optical, electromagnetic, or any other telecommunication means.
<b>Telecommunications Service</b>	A service consisting wholly or partly of the transmission, reception, or routing of information or data over telecommunications networks using any telecommunication method
<b>Public Telecommunications Service</b>	A telecommunication service provided to subscribers and other licensees for a fee, including the trade, import, and manufacturing of wired and wireless telecommunications devices

Additional definitions were added to this Article pursuant to Article (3) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 concerning Cybercrimes as amended.

The name “Ministry of Telecommunications and Information Technology” was replaced with “Ministry of Telecommunications and Digital Economy” pursuant to Article (2) of Decree-Law No. (15) of 2024 amending the name of the Ministry of Telecommunications and Information Technology.

### **Article (2)**

1. The provisions of this Decree-Law shall apply to any of the crimes provided herein if perpetrated either wholly or partially inside or outside Palestine, or if their effects extend into Palestine, whether the perpetrator is original, accomplice, abettor, or accessory, provided that such crime are punishable under the law of the place where they were committed, and subject to the general principles set forth in the Penal Law in force.
2. Any person who perpetrates outside Palestine any of the crimes provided for in this Decree-Law may be prosecuted in any of the following cases:
  - a. If the crime was perpetrated by a Palestinian citizen.
  - b. If the crime was perpetrated against Palestinian parties or interests.
  - c. If the crime perpetrated against foreign parties or interests by a foreigner or a stateless person whose usual place of residence is within Palestine, or by a foreigner or stateless person found in the Palestinian territory, and the legal conditions for extradition are not met in his case.

### **Article (3)**

1. A specialized unit shall be established within the Police Force and Security Services from among the judicial officers, to be called the Cybercrimes and Telecommunications and Information Technology Crimes Unit. The Public Prosecution shall exercise judicial supervision over the Unit, each within its jurisdiction.
2. The regular courts and the Public Prosecution, according to their respective jurisdictions, shall hear cases involving cybercrimes and telecommunications and information technology crimes.

*This Article was amended pursuant to Article (4) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (4)**

1. Whoever unlawfully and willfully accesses, by any means, an electronic website, system, network, or information technology medium or any part thereof, or exceeds authorized access, or remains therein after learning of such unauthorized access, shall be punished by imprisonment, or a fine not less than two hundred Jordanian dinars and not exceeding one thousand Jordanian dinars or its equivalent in the legally circulated currency, or both penalties.
2. If the act described in Paragraph (1) of this Article is committed against government data, the offender shall be punished by imprisonment for a period not less than six months or a fine not less than five hundred Jordanian dinars and not exceeding two thousand Jordanian dinars or its equivalent, or both penalties.
3. If the unauthorized access results in the deletion, alteration, disclosure, damage, transmission, interception, copying, publishing, or republication of stored electronic data or information; causes harm to users or beneficiaries; alters or cancels the website or modifies its content, address, design, or usage method; or involves impersonating its owner or administrator, the offender shall be punished by imprisonment for a term not less than one year, or a fine not less than one thousand Jordanian dinars and not exceeding three thousand Jordanian dinars or its equivalent, or both penalties.
4. If the act described in Paragraph (3) of this Article is committed against government data, the offender shall be punished by imprisonment for a term not exceeding five years and a fine not less than three thousand Jordanian dinars and not exceeding five thousand Jordanian dinars or its equivalent.

#### **Article (5)**

Whoever obstructs or disrupts access to a service, devices, programs, or data or information sources by any means via the electronic network or any information technology means shall be punished by imprisonment or a fine not less than two hundred Jordanian dinars and not exceeding one thousand Jordanian dinars or its equivalent, or both penalties.

#### **Article (6)**

Whoever produces or introduces via the electronic network or any means of information technology anything that causes it to cease functioning, become disabled, or destroys, deletes, or alters programs shall be punished by imprisonment for a term not exceeding five years and a fine not less than three thousand Jordanian dinars and not exceeding five thousand Jordanian dinars or its equivalent.

#### **Article (7)**

Whoever, without legal justification and willfully, intercepts, records, or eavesdrops on transmissions sent via the network or any information technology means shall be punished by imprisonment for a term not less than one year or a fine not less than one thousand Jordanian dinars and not exceeding three thousand Jordanian dinars or its equivalent, or both penalties.

#### **Article (8)**

1. Whoever intentionally decrypts encrypted data in circumstances not permitted by law shall be punished by imprisonment or a fine not less than two hundred Jordanian dinars and not exceeding one thousand Jordanian dinars or its equivalent, or both penalties.
2. Whoever unlawfully uses personal encryption elements or an electronic signature generation tool belonging to another person shall be punished by imprisonment for a term not less than one year or a fine not less than one thousand Jordanian dinars and not exceeding three thousand Jordanian dinars or its equivalent, or both penalties.
3. Whoever commits a crime using any of the means referred to in Paragraph (2) of this Article shall be punished by imprisonment and a fine not less than three thousand Jordanian dinars and not exceeding five thousand Jordanian dinars or its equivalent.

#### **Article (9)**

1. Whoever unlawfully benefits from telecommunications services via any information technology means or the like shall be punished by imprisonment for a term not less than six months or a fine not less than five hundred Jordanian dinars and not exceeding one thousand Jordanian dinars or its equivalent, or both penalties.
2. If the benefit referred to in Paragraph (1) of this Article is for profit, the offender shall be punished by imprisonment for a term not less than one year or a fine not less than one thousand Jordanian dinars and not exceeding three thousand Jordanian dinars or its equivalent, or both penalties.

#### **Article (10)**

Whoever intentionally, through the use of the electronic network or any means of information technology, creates or publishes a false certificate or provides false information about his identity to the competent authorities under the laws governing the issuance of such certificates, with the aim of requesting the issuance, revocation, or suspension of a certificate, shall be punished by imprisonment and a fine not less than two hundred Jordanian dinars and not exceeding one thousand Jordanian dinars or its equivalent.

#### **Article (11)**

1. Any person who forges an official electronic document of the State or public authorities or institutions, recognized by law within an information system, shall be punished by imprisonment for a period of no less than five years and by a fine of no less than three thousand Jordanian Dinars and no more than five thousand Jordanian Dinars, or the equivalent in legally circulated currency.
2. If the forgery involves any other documents and causes harm, the perpetrator shall be punished by imprisonment or a fine of no less than two hundred Jordanian Dinars and no more than one thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.
3. Any person who uses a forged document with knowledge of its forgery shall be punished with the same penalty prescribed for the crime of using a forged document under the applicable Penal Law.

4. Any person who forges or tampers with an official electronic signature, device, or system — whether by fabrication, destruction, disabling, modification, alteration, or by any other means resulting in a falsification of the data or information — shall be punished by imprisonment for no less than five years and by a fine of no less than three thousand Jordanian Dinars and no more than five thousand Jordanian Dinars, or the equivalent in legally circulated currency.
5. If the forgery or tampering relates to other than the electronic signatures mentioned in Paragraph (4) of this Article, the perpetrator shall be punished by imprisonment or a fine of no less than two hundred Jordanian Dinars and no more than one thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.
6. Any person who creates signature data or an official electronic signature system or for public bodies or institutions without having the legal right to obtain it, by using false or incorrect information or data, or by conspiring with others in its creation, shall be punished by imprisonment for no less than five years and by a fine of no less than three thousand Jordanian Dinars and no more than five thousand Jordanian Dinars, or the equivalent in legally circulated currency.
7. If the creation relates to other than the electronic signatures mentioned in Paragraph (6) of this Article, the perpetrator shall be punished by imprisonment or a fine of no less than two hundred Jordanian Dinars and no more than one thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.

### **Article (12)**

1. Any person who unlawfully accesses or manipulates the numbers or data of an electronic means of payment via the electronic network or by using any means of information technology shall be punished by imprisonment for no less than six months or by a fine of no less than five hundred Jordanian Dinars and no more than one thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.
2. Any person who forges an electronic means of payment by any method or manufactures or possesses, without authorization, any devices or materials used to produce or forge an electronic payment card shall be punished with the same penalty stated in Paragraph (1) of this Article.
3. Any person who uses or facilitates the use of a forged electronic means of payment with knowledge thereof, or accepts an invalid, forged, or stolen electronic payment means with knowledge thereof, shall be punished with the same penalty stated in Paragraph (1) of this Article.
4. If the acts mentioned in this Article are committed with the intent to obtain money, data belonging to others, or any services available through such means, the perpetrator shall be punished by imprisonment for no less than one year or by a fine of no less than one thousand Jordanian Dinars and no more than three thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.
5. Any person who unlawfully appropriates for themselves or for others any property of others as per the provisions of this Article shall be punished by imprisonment for no less than two years or by a fine of no less than one thousand Jordanian Dinars and no more than three thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.

### **Article (13)**

Any person who uses the electronic network or any means of information technology to steal or embezzle money shall be punished by imprisonment or by a fine of no less than three thousand Jordanian Dinars and no more than five thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.

### **Article (14)**

Any person who, through the electronic network or any means of information technology, unlawfully appropriates for themselves or for others movable property, a bond, an electronic signature, electronic signature data, or an electronic signature creation system, by employing a fraudulent method or by using a false name or misrepresenting their identity in a way that deceives the victim, shall be punished by imprisonment for no less than one year or by a fine of no less than one thousand Jordanian Dinars and no more than three thousand Jordanian Dinars, or the equivalent in legally circulated currency, or by both penalties.

### **Article (15)**

1. Any person who uses the electronic network or any means of information technology to threaten or blackmail another person to compel them to act or refrain from acting, even if the act or omission is lawful, shall be punished by imprisonment for no less than one year and no more than two years. The offender shall also receive a suspended sentence of two years' imprisonment for five years following the completion of the actual sentence, and a fine of no less than one thousand Jordanian Dinars and no more than three thousand Jordanian Dinars, or the equivalent in legally circulated currency.
2. If the threat involves the commission of a felony or the attribution of dishonorable or defamatory matters, the offender shall be punished by imprisonment for no less than two years and no more than three years. The offender shall also receive a suspended sentence of three years' imprisonment for five years following the completion of the actual sentence, and a fine of no less than five thousand Jordanian Dinars and no more than ten thousand Jordanian Dinars, or the equivalent in legally circulated currency.

*This Article was amended pursuant to Article (2) of Decree-Law No. (28) of 2020 amending Decree-Law No. (10) of 2018 on Cybercrimes.*

### **Article (16)**

1. Any person who intentionally sends, via the electronic network or any means of information technology, any audible, readable, or visual content containing pornographic material to individuals above the age of eighteen without their consent shall be punished by imprisonment for a period not less than three months and not more than two years, or a fine of no less than two hundred Jordanian Dinars and not more than one thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.
2. Any person who intentionally sends or publishes, via the electronic network or any means of information technology, any audible, readable, or visual content containing pornographic material to individuals under the age of eighteen, or related to their sexual exploitation, shall be punished by imprisonment for a period not less than one year, or a fine of no less than one



thousand Jordanian Dinars and not more than three thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

3. Any person who intentionally uses the electronic network or any means of information technology to create, prepare, store, process, display, print, publish, or promote pornographic activities or materials for the purpose of influencing individuals under the age of eighteen or persons with disabilities shall be punished by imprisonment for a period not less than two years, or a fine of no less than one thousand Jordanian Dinars and not more than three thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

#### **Article (17)**

Without prejudice to the provisions of the applicable Decree-Law on the Regulation of Human Organ Transplantation, any person who creates a website, application, or electronic account, or publishes information via the electronic network or any means of information technology for the purpose of human trafficking or trafficking in human organs or facilitating such acts, shall be punished by imprisonment for a period not exceeding seven years, and a fine of no less than three thousand Jordanian Dinars and not more than five thousand Jordanian Dinars, or its equivalent in legally circulating currency.

#### **Article (18)**

Without prejudice to the provisions of the applicable Decree-Law on Anti-Money Laundering and Terrorism Financing, any person who creates a website, application, or electronic account, or uses any means of information technology with the intent to:

1. Commit a money laundering crime shall be punished by imprisonment for a period not less than one year, or a fine of no less than one thousand Jordanian Dinars and not more than three thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.
2. Commit a terrorism financing crime shall be punished by imprisonment or a fine of no less than three thousand Jordanian Dinars and not more than five thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

#### **Article (19)**

Without prejudice to the provisions of the applicable Decree-Law on Combating Narcotic Drugs and Psychotropic Substances, any person who creates or publishes a website on the electronic network, or uses any means of information technology with the intent to traffic, promote, or facilitate dealings in narcotic drugs or psychotropic substances, or any equivalent substances, or sells, explains, or displays methods for producing such substances, shall be punished by imprisonment for a period not less than ten years, or a fine of no less than three thousand Jordanian Dinars and not more than five thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

#### **Article (20)**

Any person who violates intellectual, literary, or industrial property rights, in accordance with the applicable legislation, through the use of the electronic network or any means of information technology, shall be punished by imprisonment for a period not exceeding six months, or a fine of

no less than five hundred Jordanian Dinars and not more than one thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

#### **Article (21)**

1. Every individual has the right to express their opinion through speech, writing, photography, or other means of expression and publication, in accordance with the law.
2. Freedom of artistic and literary creativity is guaranteed. No lawsuits may be filed or initiated to suspend or confiscate artistic, literary, or intellectual works or against their creators except by judicial order. No custodial penalty or pretrial detention shall be imposed for crimes committed due to the public disclosure of artistic, literary, or intellectual products.
3. Freedom of the press, printing, and publication in print, visual, audio, and electronic forms is guaranteed. Palestinians, whether natural or legal persons, public or private, have the right to own and publish newspapers and to establish visual, audio, and digital media in accordance with the law.
4. No restrictions may be imposed on the press, nor may it be confiscated, suspended, warned, or revoked, except in accordance with the law and pursuant to a judicial ruling.

#### **Article (22)**

1. Arbitrary or unlawful interference in the privacy of any person or in the affairs of their family, home, or correspondence is prohibited.
2. Any person who creates a website, application, or electronic account, or publishes information on the electronic network or via any means of information technology with the intent to disseminate news, images, or audio or visual recordings, whether live or recorded, related to the unlawful interference in the private or family life of individuals, even if such information is true, shall be punished by imprisonment for a period not less than one year, or a fine of no less than one thousand Jordanian Dinars and not more than three thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

#### **Article (23)**

Any person who creates a website, application, or electronic account, or publishes information on the electronic network or via any means of information technology with the intent to operate, facilitate, encourage, promote, or advertise gambling activities or games of chance shall be punished by imprisonment for a period not less than six months, or a fine of no less than five hundred Jordanian Dinars and not more than one thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

#### **Article (24)**

Any person who creates a website, application, or electronic account, or publishes information on the electronic network or via any means of information technology with the intent to display any written words or behaviors that could incite racial or religious hatred, or racial discrimination against a specific group due to their ethnic, sectarian, racial, physical, or disability-related characteristics, shall be punished by imprisonment for a period not exceeding one year, or a fine of no less than two hundred Jordanian Dinars and not more than one thousand Jordanian Dinars, or its equivalent in legally circulating currency, or by both penalties.

#### **Article (25)**

Any person who creates a website, application, or electronic account, or publishes information on the electronic network or via any means of information technology with the intent to distort or justify acts of genocide or crimes against humanity as defined by international treaties and laws, or who deliberately assists or incites the commission of crimes against humanity, shall be punished by imprisonment for a period not less than ten years.

#### **Article (26)**

Anyone who possesses, with the intent of use, a device, software, any prepared electronic data, password, or access codes, or provides, produces, distributes, imports, exports, or promotes them for the purpose of committing any of the crimes stipulated in this Decree-Law, shall be punished by imprisonment for a period not exceeding five years, and a fine of no less than three thousand Jordanian dinars and not more than five thousand Jordanian dinars, or the equivalent in legally circulated currency.

#### **Article (27)**

1. Any public employee who commits any of the crimes stipulated in this Decree-Law, by exploiting his/her powers and authority during or because of his/her work, or facilitates their commission for others, shall be subject to a penalty increased by one-third.
2. Any service provider employee who commits any of the crimes stipulated in this Decree-Law during or because of his/her work, or facilitates their commission for others, shall be subject to a penalty increased by two-thirds.

#### **Article (28)**

Anyone who incites, aids, or conspires with another to commit any of the crimes stipulated under the provisions of this Decree-Law by any electronic means, and the crime is committed as a result of such incitement, assistance, or conspiracy, shall be punished with the penalties prescribed for the principal perpetrator.

#### **Article (29)**

If any of the crimes stipulated in this Decree-Law are committed in the name or on behalf of a legal person, the legal person shall be punished with a fine of no less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars. The court may also rule to bar the legal person from conducting its activities for a maximum period of five years or to dissolve it if the crime is punishable by imprisonment of not less than one year, without prejudice to the criminal liability of the natural person affiliated with it.

#### **Article (30)**

Anyone who intentionally publishes information about a website blocked under the provisions of Article (39) of this Decree-Law using systems, websites, or electronic applications, shall be punished by imprisonment for a period not less than three months, or a fine of no less than two hundred Jordanian dinars and not more than one thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties.

### **Article (31)**

1. Anyone who publishes or disseminates the content of any communication or telephone call via a communications network or information technology means, or a phone message that he/she accessed due to his/her position or recorded without legal basis, or assisted or participated in doing so, shall be punished by imprisonment for a period not less than three months and not more than one year, or a fine of no less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties.
2. Anyone who undertakes, assists, or participates in concealing a message or call that he/she is required to transmit through communications networks to another person, or refuses to transmit messages or calls requested to be transmitted according to the law or license, or tampers with subscriber data, including unlisted phone numbers and invoices, shall be punished by imprisonment for a period not less than six months and not more than one year, or a fine of no less than seven thousand Jordanian dinars and not more than fifteen thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties.

*This Article was added pursuant to Article (5) of Decree-Law No. (38) of 2021 amending the Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (32)**

1. Anyone who deliberately commits, assists, or participates in the sabotage of telecommunications or information technology installations or causes damage to them shall be punished by imprisonment for a period not less than six months and not more than two years, and a fine of no less than two thousand Jordanian dinars and not more than four thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties.
2. Anyone who negligently causes the sabotage of telecommunications or information technology installations or causes damage to them shall be punished by a fine of no less than one hundred Jordanian dinars and not more than five hundred Jordanian dinars, or the equivalent in legally circulated currency.

*This Article was added pursuant to Article (6) of Decree-Law No. (38) of 2021 amending the Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (33)**

1. Anyone who provides, contributes to, assists, or participates in offering telecommunications services by means that would result in unfair competition between licensed telecommunications networks and foreign or unlicensed networks, shall be punished by imprisonment for a period not less than six months and not more than one year, or a fine of no less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties. In all cases, the court shall rule to confiscate the devices and tools used in the service provision.
2. Anyone who uses or assists or participates in the use of illegal means to conduct communications without paying the required fees shall be punished by imprisonment for three months, and a fine of no less than five hundred Jordanian dinars and not more than one thousand Jordanian dinars, or the equivalent in legally circulated currency.

3. Anyone who uses a private telecommunications network to provide public telecommunications services, or connects or helps to connect a private telecommunications network to a public one without the Authority's approval, shall be punished by imprisonment for a period not less than three months and not more than one year, or a fine of no less than two thousand Jordanian dinars and not more than four thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties. The offender shall bear the cost of rectifying the violation.

*This Article was added pursuant to Article (7) of Decree-Law No. (38) of 2021 amending the Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (34)**

1. Anyone who establishes, operates, or manages a public telecommunications network for the purpose of providing telecommunications services in violation of the applicable Decree-Law on Telecommunications and Information Technologies and its related regulations, or assists or participates in doing so, shall be punished by imprisonment for a period not less than six months and not more than one year, or a fine of no less than two thousand Jordanian dinars and not more than four thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties.
2. If the violator mentioned in Paragraph (1) of this Article is a legal person, it shall be punished by a fine of no less than ten thousand Jordanian dinars and not more than twenty thousand Jordanian dinars, or the equivalent in legally circulated currency. In all cases, the court shall order the confiscation of the devices used.

*This Article was added pursuant to Article (8) of Decree-Law No. (38) of 2021 amending the Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (35)**

1. Subject to the provisions of the applicable Decree-Law on Telecommunications and Information Technologies, anyone who operates a radio station or uses frequencies or numbers without a license, or assists or participates in doing so intentionally, shall be punished by imprisonment for a period not less than three months and not more than one year, or a fine of no less than one thousand Jordanian dinars and not more than two thousand Jordanian dinars, or the equivalent in legally circulated currency, or both penalties.
2. If the violator mentioned in Paragraph (1) of this Article is a legal person, it shall be punished by a fine of no less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars, or the equivalent in legally circulated currency, and the devices used shall be confiscated.
3. Anyone who, without obtaining the Authority's approval, transfers to others the license granted to him to use a frequency, number, or any rare telecommunications resource, shall be punished by a fine of no less than two thousand Jordanian dinars and not more than four thousand Jordanian dinars, or the equivalent in legally circulated currency, and the license shall be revoked and the transfer annulled.

*This Article was added pursuant to Article (9) of Decree-Law No. (38) of 2021 amending the Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (36)**

Without prejudice to any harsher penalty stipulated in any other law, any person who intercepts, obstructs, alters, or deletes the content of a message via telecommunications networks or information technology, or incites, assists, or participates in doing so, shall be punished by imprisonment for a period not less than six months and not more than one year, or by a fine not less than two thousand Jordanian Dinars and not more than four thousand Jordanian Dinars, or its equivalent in legally circulated currency, or by both penalties.

*This Article was added pursuant to Article (10) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (37)**

1. Any person who deliberately, or through assistance or participation, intercepts radio waves designated for others, or jams or interrupts them, shall be punished by imprisonment for a period not less than three months and not more than one year, or by a fine not less than one thousand Jordanian Dinars and not more than two thousand Jordanian Dinars, or its equivalent in legally circulated currency, or by both penalties. In all cases, the court shall order the confiscation of the jamming devices used.
2. If the offense referred to in Paragraph (1) of this Article is committed by a legal person, it shall be punished by a fine not less than five thousand Jordanian Dinars and not more than ten thousand Jordanian Dinars, or its equivalent in legally circulated currency, and the confiscation of the used devices shall be ordered.

*This Article was added pursuant to Article (11) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (38)**

1. Any person who imports into the territory of the State devices, systems, or telecommunications or information technology programs that are in violation of the technical specifications or standards approved by the Authority, or that contain false data or information, with the intention of marketing or selling them, or who assists or participates in that, shall be punished by imprisonment for a period not less than three months and not more than one year, or by a fine not less than one thousand Jordanian Dinars and not more than two thousand Jordanian Dinars, or its equivalent in legally circulated currency, or by both penalties. The confiscation of the seized devices shall be ordered.
2. Any person who possesses, sells, trades in, or displays surveillance devices of any kind shall be punished by imprisonment for a period not less than six months and not more than two years, or by a fine not less than two thousand Jordanian Dinars and not more than four thousand Jordanian Dinars, or its equivalent in legally circulated currency, or by both penalties. The confiscation of the seized devices shall be ordered.

*This Article was added pursuant to Article (12) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (39)**

Any person who practices, without a license, any telecommunications or information technology profession or craft that requires licensing in accordance with the provisions of the applicable Decree-Law on Telecommunications and Information Technologies and the regulations issued thereunder, shall be punished by imprisonment for a period not less than three months and not more than one year, or by a fine not less than five hundred Jordanian Dinars and not more than two thousand Jordanian Dinars, or its equivalent in legally circulated currency, or by both penalties.

*This Article was added pursuant to Article (13) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (40)**

If the licensee fails to cover the entire geographical area designated to them with the licensed service in accordance with the license, they shall be punished by a fine not less than one hundred thousand Jordanian Dinars and not more than five hundred thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (14) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (41)**

Any person whose license has been revoked and who fails to immediately cease receiving new subscribers or providing telecommunications services—except to the extent necessary to transfer their subscribers to another licensee in accordance with what is decided by the Authority for this purpose—shall be punished by a fine not less than five thousand Jordanian Dinars and not more than ten thousand Jordanian Dinars, or its equivalent in legally circulated currency, and the court shall order the confiscation of the devices and network.

*This Article was added pursuant to Article (15) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

### **Article (42)**

1. Any person whose license renewal has been denied by the Authority and who removes the telecommunications network(s) they established, or any part thereof, without the Authority's written approval, shall be punished by a fine not less than five thousand Jordanian Dinars and not more than ten thousand Jordanian Dinars, or its equivalent in legally circulated currency.
2. If the person mentioned in Paragraph (1) of this Article is licensed to provide fixed or mobile telecommunications services or telecommunications or information technology infrastructure, they shall be punished by a fine not less than ten million Jordanian Dinars and not more than fifty million Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (16) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (43)**

1. If the licensee uses frequencies, numbers, or other important resources that have not been allocated to them by the Authority, they shall be punished by a fine not less than twenty thousand Jordanian Dinars and not more than fifty thousand Jordanian Dinars, or its equivalent in legally circulated currency, and such resources shall be immediately withdrawn and returned to the Authority.
2. If the licensee uses the frequencies, numbers, or other important resources allocated to them by the Authority for purposes other than those licensed or designated, or fails to comply with any of the allocation conditions, they shall be punished by a fine not less than ten thousand Jordanian Dinars and not more than twenty thousand Jordanian Dinars, or its equivalent in legally circulated currency, and such resources shall be immediately withdrawn and returned to the Authority.

*This Article was added pursuant to Article (17) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (44)**

1. If the licensee violates any provision of Chapter Eight of the applicable Decree-Law on Telecommunications and Information Technology concerning interconnection, access, and infrastructure sharing, they shall be punished by a fine not less than thirty thousand Jordanian Dinars and not more than fifty thousand Jordanian Dinars, or its equivalent in legally circulated currency.
2. If the person mentioned in Paragraph (1) of this Article is licensed to provide fixed or mobile telecommunications services or telecommunications or information technology infrastructure, they shall be punished by a fine not less than one hundred thousand Jordanian Dinars and not more than two hundred thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (18) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (45)**

Any licensee who fails to announce the prices of telecommunications services provided to the public in the manner approved or authorized by the Authority shall be punished by a fine not less than five thousand Jordanian Dinars and not more than ten thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (19) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (46)**

1. If the licensee violates any provision of Chapter Ten of the applicable Decree-Law on Telecommunications and Information Technology concerning the relationship between the licensee and the subscriber, they shall be punished by a fine not less than five thousand



Jordanian Dinars and not more than ten thousand Jordanian Dinars, or its equivalent in legally circulated currency.

2. If the licensee mentioned in Paragraph (1) of this Article is licensed to provide fixed or mobile cellular telecommunications services or telecommunications or information technology infrastructure, they shall be punished by a fine not less than thirty thousand Jordanian Dinars and not more than fifty thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (20) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (47)**

1. Any licensee who commits fraud, deception, or misleading conduct against a subscriber by any means, or gains enrichment at their expense without legal justification, shall be punished by imprisonment for a period not less than six months and not more than two years, and by a fine not less than five thousand Jordanian Dinars and not more than ten thousand Jordanian Dinars, or its equivalent in legally circulated currency.
2. If the licensee referred to in Paragraph (1) of this Article is licensed to provide fixed or mobile telecommunications services or telecommunications or information technology infrastructure, they shall be punished by a fine not less than fifty thousand Jordanian Dinars and not more than one hundred thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (21) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (48)**

If the licensee violates any provision of the National Numbering Plan, they shall be punished by a fine not less than ten thousand Jordanian Dinars and not more than twenty thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (22) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (49)**

If the licensee commits or refrains from an act that causes damage to archaeological or tourist sites, or results in harm to the environment or public health, they shall be punished by a fine not less than fifty thousand Jordanian Dinars and not more than one hundred thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (23) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (50)**

1. Any person who prevents or obstructs in any way the work of the Authority's inspectors designated for oversight shall be punished by imprisonment for a period not less than three

months and not more than six months, and by a fine not less than one thousand Jordanian Dinars and not more than two thousand Jordanian Dinars, or its equivalent in legally circulated currency.

2. If the licensee or one of their employees commits the violation specified in Paragraph (1) of this Article, the person causing the prevention or obstruction shall be punished by imprisonment for a period not less than six months and not more than two years, and the licensee shall be punished by a fine not less than fifty thousand Jordanian Dinars and not more than one hundred thousand Jordanian Dinars, or its equivalent in legally circulated currency.
3. If the licensee refuses or delays in providing the Authority with any reports, documents, contracts, information, or data requested, they shall be punished by a fine not less than fifty thousand Jordanian Dinars and not more than one hundred thousand Jordanian Dinars, or its equivalent in legally circulated currency.

*This Article was added pursuant to Article (24) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (51)**

The service provider shall be obligated, in accordance with the prescribed legal procedures, to:

1. Provide the competent authorities with the subscriber's information that helps uncover the truth, based on a request by the Public Prosecution or the competent court.
2. Block a link, content, or application on the electronic network pursuant to orders issued by judicial authorities, while observing the procedures stipulated in Article (39) of this Decree-Law.
3. Retain subscriber information for a period of no less than three years for the purposes set forth in Paragraph (1) of this Article.
4. Cooperate with and assist the competent authorities, based on a decision from the judge of the competent court, in collecting or recording electronic information or data and temporarily retaining it.

#### **Article (52)**

1. The Public Prosecution or its delegated members of the judicial police may search persons, places, and information technology means related to the crime.
2. The search warrant must be justified and specific, and it may be renewed more than once as long as the justification for the procedure remains valid.
3. If the search referred to in Paragraph (2) of this Article results in the seizure of devices, tools, or means related to the crime, the judicial police shall prepare a record of the seizures and present them to the Public Prosecution for appropriate action.
4. The Public Prosecutor may authorize direct access by the judicial police or those they consult from experts to any information technology means and to search it for the purpose of obtaining data or information.
5. The judicial police officer must be qualified to deal with the specific nature of cybercrimes and telecommunications and information technology crimes.

*This Paragraph was amended pursuant to Article (25) of Decree-Law No. (38) of 2021 amending the Decree-Law No. (10) of 2018 on Cybercrimes as amended.*

#### **Article (53)**

1. The Public Prosecution may obtain the devices, tools, means, data, or electronic information, including traffic data or communications-related data or users' information related to the cybercrime.
2. The Public Prosecution may authorize the seizure and retention of the entire information system or part thereof or any information technology means that may help uncover the truth.
3. If seizing and retaining the information system is not necessary or is not possible, the related data or information and data readable and comprehensible shall be copied to an information technology medium.
4. If actual seizure and retention are impossible, all appropriate means shall be employed to prevent access to the data stored in the information system in order to preserve the evidence.
5. Necessary precautions shall be taken to maintain the integrity of the seized item, including the technical means to protect its content.
6. A list of the seized items shall be prepared, as much as possible, in the presence of the accused or the person in possession of the seized item, and a report shall be drafted accordingly. The seized item shall be stored, as applicable, in a sealed envelope or container, labeled with the date and time of seizure and the record and case numbers.

#### **Article (54)**

1. The Magistrate Judge may authorize the Attorney General or any of their deputies to monitor, record, and process electronic communications and conversations to search for evidence related to a felony or misdemeanor punishable by imprisonment for no less than one year. The authorization shall be for fifteen (15) days and renewable once, based on the existence of serious indications. The person conducting the search, monitoring, or recording must prepare a report to be submitted to the Public Prosecution.
2. The Attorney General or any of their deputies may order the immediate collection and provision of any data, including communication traffic or electronic information or subscriber information deemed necessary for the benefit of the investigation under Paragraph (1) of this Article, using appropriate technical means and, if necessary, in cooperation with service providers according to the type of service provided.

#### **Article (55)**

The competent authorities shall take the necessary measures to preserve the safety and confidentiality of the devices, tools, means of information technology, electronic systems, or electronic data or information under custody until a decision is issued by the competent judicial authorities concerning them.

#### **Article (56)**

1. The competent court may authorize the immediate interception of the content of communications, their recording or copying, upon a request from the Attorney General or one of their deputies. The court's decision must contain all elements necessary to identify the communications subject to interception, the acts justifying it, and its duration.

2. The duration of the interception, as per Paragraph (1) of this Article, shall not exceed three months from the actual start date of execution, and it may be extended once only.
3. The entity tasked with executing the interception order must notify the Public Prosecution of the actual start date of the interception operation and coordinate with it regarding the necessary measures for its proper execution.

#### **Article (57)**

Evidence obtained by any means of information technology, information systems, information networks, websites, or electronic data and information shall be considered admissible evidence.

#### **Article (58)**

Evidence obtained by the competent authority or investigative authorities of other states shall be admissible evidence, provided that it was obtained in accordance with the legal and judicial procedures of international cooperation.

#### **Article (59)**

1. If competent investigation and enforcement authorities detect that websites hosted inside or outside the State publish phrases, numbers, images, videos, or promotional or other materials that may threaten national security, public order, or public morals, they shall submit a report to the Attorney General or one of their deputies and request permission to block the website(s) or specific links thereof from being accessed.
2. The Attorney General or one of their deputies shall submit the request to the Magistrate Court within twenty-four (24) hours, accompanied by a memorandum of opinion. The court shall issue its decision on the request on the same day of its submission, either approving or rejecting it. The blocking period shall not exceed six months unless renewed in accordance with the procedures set forth in this Article.

#### **Article (60)**

Except for professional obligations provided for in the law, professional secrecy or its requirements may not be invoked to refuse the provision of information or documents requested in accordance with the provisions of Law.

#### **Article (61)**

State agencies, institutions, bodies, and affiliated entities and companies shall be obligated to:

1. Take the necessary preventive security measures to protect their information systems, websites, information networks, and their electronic data and information.
2. Promptly notify the competent authority of any crime provided for in this Decree-Law immediately upon its discovery or upon discovering any attempt to unlawfully intercept, access, or eavesdrop, and provide the competent authority with all information to uncover the truth.
3. Retain information technology data and subscriber information for no less than one hundred and twenty (120) days and provide such data to the competent authority.
4. Cooperate with the competent authority in the implementation of its functions.

#### **Article (62)**

1. The competent authorities shall facilitate cooperation with their counterparts in foreign countries within the framework of ratified international, regional, or bilateral agreements, or based on the principle of reciprocity, in order to expedite the exchange of information that ensures early warning of information and communication system crimes, prevents their commission, and assists in their investigation and in tracking down perpetrators.
2. The cooperation referred to in the previous paragraph shall be conditional on the concerned foreign state maintaining the confidentiality of the information transferred to it and its commitment not to transfer it to a third party or use it for purposes other than combating the crimes specified in this Decree-Law.

#### **Article (63)**

1. The competent authorities shall provide assistance to their counterparts in other countries for the purposes of mutual legal assistance and extradition of offenders in investigations and criminal proceedings related to the crimes provided for in this Decree-Law, in accordance with the provisions of the applicable Law of Penal Procedure, ratified bilateral or multilateral agreements to which the State is a party, or based on the principle of reciprocity, and without prejudice to the provisions of this Decree-Law or any other law.
2. A request for legal assistance or extradition of offenders shall not be executed under this Decree-Law unless the laws of the requesting State and the laws of the State criminalize the offense subject to the request or a similar offense. Dual criminality shall be deemed fulfilled regardless of whether the requesting State classifies the offense under the same category of crimes or uses the same terminology as the State, provided that the act subject to the request is criminalized under the laws of the requesting State.

#### **Article (64)**

Without prejudice to any harsher penalty stipulated in the applicable Penal Law or any other law, perpetrators of the offenses punishable under the provisions of this Decree-Law shall be punished with the penalties specified herein.

#### **Article (65)**

Anyone who commits an act that constitutes an offense under any applicable legislation using the electronic network or any means of information technology, or who participates, intervenes, or incites its commission, and which is not provided for in this Decree-Law, shall be punished with the same penalty prescribed for that offense in such legislation.

#### **Article (66)**

Anyone who unlawfully discloses the confidentiality of the procedures stipulated in this Decree-Law shall be punished by imprisonment or a fine not less than two hundred Jordanian dinars and not exceeding one thousand Jordanian dinars, or the equivalent thereof in legally circulating currency, or by both penalties.

#### **Article (67)**

Anyone who tampers with, destroys, conceals, alters, or erases digital forensic evidence shall be punished with imprisonment for no less than one year and a fine not less than one thousand Jordanian dinars and not exceeding three thousand Jordanian dinars, or the equivalent thereof in legally circulating currency.

#### **Article (68)**

Anyone who participates in the commission of a felony or misdemeanor punishable under the provisions of this Decree-Law by agreement, incitement, assistance, or intervention shall be punished with the same penalty prescribed for the principal offender. If the crime is not completed, they shall be punished with half of the prescribed penalty.

#### **Article (69)**

Anyone who attempts to commit a felony or misdemeanor as provided for in this Decree-Law shall be deemed to have committed the crime of attempt and shall be punished with half of the penalty prescribed for the completed crime.

#### **Article (70)**

Without prejudice to the penalties stipulated in this Decree-Law and the rights of third parties acting in good faith, the court shall issue a decision including the following:

1. The duration of closure of the establishment and the blocking of the website through which or on which the crime was committed, as applicable.
2. The confiscation of the devices, programs, or means used in the commission of any of the crimes provided for in this Decree-Law or the funds derived therefrom, with the violation to be removed at the offender's expense.

#### **Article (71)**

The penalty prescribed in this Decree-Law shall be doubled in the event that the offender repeats the commission of any of the offenses provided for herein, whether committed inside or outside Palestine. Foreign judgments shall be considered as prior offenses for the purpose of recidivism.

#### **Article (72)**

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

1. If the crime was committed against a site, information system, data, numbers, letters, codes, or images managed by the State or any public legal person or owned by or related to it, including local authorities.
2. If the offender committed the crime through an organized gang.
3. If the offender exploited or lured a person under the age of eighteen.
4. If the crime was committed against an information system, website, or information network related to money transfers, payment services, clearing or settlement services, or any banking services provided by banks or financial companies.

### **Article (73)**

Anyone who voluntarily informs the competent authorities of any information regarding the crime and the individuals involved therein, before the authorities become aware of the crime and before any damage occurs, shall be exempted from the penalties stipulated in this Decree-Law. If the notification is made after the authorities have become aware of the crime and it results in the arrest of the remaining perpetrators, the court may order a suspension of the execution of the sentence.

### **Article (74)**

1. Decree-Law No. (16) of 2017 on Cybercrimes shall be repealed.
2. Any provision that conflicts the provisions of this Decree-Law shall be repealed.

### **Article (75)**

This Decree-Law shall be presented to the Legislative Council in its first convened session for ratification.

### **Article (76)**

All competent authorities, each in its respective field, must implement the provisions of this Decree-Law, and it shall enter into force from the date of its publishing in the Official Gazette.

1. Article (54) of the original law was repealed pursuant to Article (26) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.
2. The Articles were renumbered pursuant to Article (27) of Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 on Cybercrimes as amended.

**MAHMOUD ABBAS**  
**President of the State of Palestine**  
**Chairman of PLO Executive Committee**