Translation of

Law No. 175 of 2018

Concerning Information Technology Crimes

ترجمة القانون رقم ١٧٥ لسنة ٢٠١٨

---

11 June 2025

ANDERSEN

Law No. 175 of 2018 Concerning Information Technology Crimes

In the name of the people President of the republic

The House of Representatives has enacted the following law, which we hereby promulgate:

Part One: General Provisions

Definitions:

Article (1):

For the purposes of applying the provisions of this law, the following words and expressions shall have the meanings assigned to each of them:

The Authority: The National Telecommunications Regulatory Authority.

The Competent Minister: The Minister responsible for communications and information technology.

Electronic Data and Information: Any content that can be created, stored, processed, generated, transmitted, shared, or copied using information technology, such as numbers, codes, ciphers, letters, symbols, signals, images, sounds, or similar content.

Personal Data: Any information relating to an identified or identifiable natural person, either directly or indirectly, by linking such data with other information.

Government Data: Information relating to the State, its authorities, agencies, public bodies, independent entities, oversight bodies, or any other public legal persons, whether available on information networks, IT systems, computers, or their equivalents.

Electronic Processing: Any electronic or technical operation, wholly or partially, for writing, compiling, recording, saving, storing, integrating, displaying, transmitting, receiving, circulating, publishing, deleting, altering, modifying, retrieving, or deriving electronic data and information using any medium, computer, electronic, magnetic, or optical device or any emerging technologies.

Information Technology: Any means or collection of means, whether interconnected or not, used for storing, retrieving, organizing, managing, processing, developing, or exchanging information or data, including both wired and wireless media.

Service Provider: Any natural or legal person who provides information and communication technology services to users, including those who process or store information either directly or on behalf of others.

User: Any natural or legal person who uses or benefits in any form from information technology services.

Software: A set of instructions or commands expressed in any language, symbol, or signal, in any form, that can be used directly or indirectly by a computer to perform a function or achieve a result.

Information System: A set of software and tools designed to manage and process data and information or to provide informational services.

Information Network: A group of interconnected devices or information systems capable of exchanging information and communications, including private, public, and international networks and applications.

Website: A virtual domain or location with a specific address on an information network aimed at making data and information accessible to the public or a specific audience.

Website Administrator: Any person responsible for organizing, managing, monitoring, or maintaining one or more websites, including managing user access rights, website design, content generation, and content management.

Personal Account: A set of information related to a natural or legal person that grants them exclusive access to services through a website or information system.

Email: A means of exchanging electronic messages at a specific address between multiple natural or legal persons via an information network or other electronic connection through computers or similar devices.

Interception: The act of accessing, viewing, obtaining, or manipulating data or information with the intent of eavesdropping, disrupting, storing, copying, recording, modifying content, misusing, rerouting, or redirecting it, unlawfully and without authorization.

Hacking: Unauthorized or unlawful access to an information system, computer, or information network, or any equivalent system.

Content: Any data, whether standalone or combined with other data or information, that results in forming knowledge, orientation, direction, concept, meaning, or indicates other data.

Digital Evidence: Electronic data that has probative value, stored, transmitted, extracted, or obtained from computers or information networks or their equivalents, capable of being collected and analyzed using specialized technological tools or software.

Expertise: Any activity related to providing consultancy, inspection, audit, evaluation, or analysis in the field of information technology.

Traffic Data (Communications Metadata): Data generated by an information system indicating the source and destination of communication, the route taken, date, time, size, duration, and type of service.

Computer: Any device or technological equipment capable of data storage and performing logical or arithmetic operations, used for recording, storing, transforming, generating, retrieving, organizing, processing, developing, exchanging, or analyzing data or for communications.

Electronic Medium: Any physical medium used for storing and transmitting electronic data and information, including compact discs, optical discs, electronic memory, or their equivalents.

National Security: Matters concerning the independence, stability, security, and territorial integrity of the nation, as well as issues related to the Presidency, the National Defense Council, the National Security Council, the Ministry of Defense and Military Production, the Ministry of Interior, the General Intelligence Service, the Administrative Control Authority, and their respective agencies.

National Security Agencies: The Presidency, Ministry of Defense, Ministry of Interior, General Intelligence Service, and the Administrative Control Authority.

Part One: General Provisions: Obligations and Duties of Service Providers:

Article (2):

First: Without prejudice to the provisions of this law and Law No. 10 of 2003 regulating telecommunications, service providers shall be obligated to:

Retain and store information system logs or any other information technology means for a continuous period of 180 days, including the following data:

- Data identifying the user of the service.
- Data related to the content and nature of the information system being handled, when under the control of the service provider.
- Data regarding communications traffic.
- Data related to terminal communication devices.
- Any other data as determined by the Authority's Board of Directors.

Preserve the confidentiality of stored data and not disclose or reveal it without a justified order from the competent judicial authorities. This includes users' personal data or any data related to the websites and private accounts accessed by users or persons and entities they communicate with.

Secure the data and information to ensure its confidentiality, prevent unauthorized access, and protect against damage.

Second: Without prejudice to the provisions of the Consumer Protection Law, service providers must make the following information available to their users and relevant governmental authorities in an easily accessible, direct, and continuous manner:

- The name and address of the service provider.
- Contact information for the service provider, including their electronic address.
- Licensing data identifying the provider and the supervisory authority.

- Any other information deemed essential by the Authority to protect service users, as specified by a decision from the Competent Minister.

Third: In compliance with the constitutional right to privacy, service providers and their affiliates must, upon request from national security agencies and according to their needs, provide the necessary technical capabilities to enable such agencies to perform their duties as prescribed by law.

Fourth: Service providers and their agents and distributors authorized to market such services must obtain users' data. It is prohibited for any party other than them to do so.

Part One: General Provisions: Territorial Scope of the Law:

Article (3):

Without prejudice to the provisions of Part One, Book One of the Penal Code, this law applies to any non-Egyptian who commits any of the crimes stipulated herein outside the Arab Republic of Egypt, provided the act is punishable in the country where it was committed under any legal designation, and in any of the following circumstances:

- If the crime was committed on board any air, land, or sea transport registered in Egypt or bearing its flag.
- If the victim or one of the victims is Egyptian.
- If the crime was prepared, planned, directed, supervised, or financed from Egypt.
- If the crime was committed by an organized criminal group conducting activities in more than one country, including Egypt.
- If the crime causes harm to any Egyptian citizen or resident, or to national security or any national interest, whether inside or outside the country.
- If the perpetrator is found in Egypt after committing the crime and has not been extradited.

Part One: General Provisions: International Cooperation in Combating Cybercrimes

Article (4):

Egyptian competent authorities shall facilitate cooperation with their counterparts in foreign countries within the framework of ratified international, regional, and bilateral agreements, or based on the principle of reciprocity, by exchanging information aimed at preventing the commission of cybercrimes and assisting in their investigation and the prosecution of their perpetrators.

The National Computer and Network Emergency Response Center at the Authority shall serve as the officially recognized technical contact point for such cooperation.

Part Two: Procedural Rules and Provisions: Judicial Police Officers

Article (5):

By a decision of the Minister of Justice, in coordination with the Competent Minister, the status of judicial police officer may be granted to employees of the Authority or to others designated by the National Security Authorities, with respect to offenses committed in violation of the provisions of this Law and related to the performance of their duties.

Article (6):

The competent investigating authority may, as appropriate, issue a reasoned order to the designated judicial police officers, for a period not exceeding thirty (30) days, renewable once, if such order is deemed beneficial for revealing the truth regarding the commission of a punishable offense under the provisions of this Law, including one or more of the following:

Seizing, withdrawing, collecting, or preserving data, information, or information systems, or tracing them wherever they may be—in a system, program, electronic medium, or computer—and delivering any digital evidence to the issuing authority, provided such actions do not disrupt system continuity or service provision where applicable.

Searching, inspecting, accessing, and penetrating computer programs, databases, and other information systems to carry out the seizure.

Ordering the service provider to submit any data or information related to an information system or technological device under its control or stored in its possession, as well as user data and communication logs on the relevant system or device.

In all cases, the order of the competent investigating authority must be reasoned.

Orders issued under this Article may be appealed before the competent criminal court sitting in chambers, in accordance with the deadlines and procedures set forth in the Criminal Procedure Code.

Part Two: Procedural Rules and Provisions: Procedures and Decisions on Website Blocking Requests

Article (7):

If there is evidence that a website—whether operating within or outside the country—is publishing content including phrases, numbers, images, films, promotional materials, or the like that constitute an offense under this Law and pose a threat to national security or endanger the country's safety or national economy, the competent investigating authority may issue an order to block the site or broadcasting sites, where technically feasible.

The investigating authority shall submit the blocking order to the competent court sitting in chambers within 24 hours, accompanied by a memorandum stating its opinion. The court must issue a reasoned decision accepting or rejecting the order within 72 hours of its submission.

In urgent cases involving imminent danger or harm, the competent investigative and enforcement agencies may notify the Authority, which shall then instruct the service provider to immediately implement a temporary block of the website, content, or links mentioned in the first paragraph of this Article, in accordance with its provisions. The service provider must comply immediately upon receiving the notice.

The enforcement or investigative authority that issued the notification must prepare a report of the procedures taken under the above paragraph and submit it to the investigative authority within 48 hours. This report shall follow the same procedures described in the second paragraph of this Article. The court shall then issue a decision either upholding or canceling the blocking.

Failure to submit the report within the specified time shall render the blocking null and void.

The trial court, while hearing the case, or upon request by the investigative authority, the Authority, or an interested party, may order the termination or amendment of the blocking order.

In all cases, a blocking order shall be rendered void upon issuance of a decision to dismiss the criminal case or a final judgment of acquittal.

Part Two: Procedural Rules and Provisions: Appeals Against Website Blocking Decisions

Article (8):

Any person subject to a judicial order under Article 7 of this Law, the Public Prosecution, the competent investigating authority, or any interested party may file an appeal against the decision or its execution before the competent criminal court after seven (7) days from the issuance or execution of the order, whichever is applicable. If the appeal is denied, a new appeal may be submitted after a lapse of three (3) months from the date of the ruling rejecting the previous one.

In all cases, appeals must be filed with the registry of the competent criminal court. The court president shall schedule a session for hearing the appeal, notifying the appellant, the Authority, and all concerned parties. The court must decide on the appeal within seven (7) days from the date of filing.

Part Two: Procedural Rules and Provisions: Travel Bans

Article (9):

The Public Prosecutor, or a delegated Chief Prosecutor from the Courts of Appeal, and the competent investigative authorities may, when necessary or when sufficient evidence exists to indicate the seriousness of the charges for committing or attempting to commit an offense under this Law, issue a reasoned order to prohibit the accused from traveling abroad or to place their name on the watch list, for a specified duration.

The person subject to the travel ban may appeal the order before the competent criminal court within fifteen (15) days of being notified. If the appeal is denied, a new appeal may be submitted after three (3) months from the date of the judgment rejecting the previous one.

The appeal shall be filed by a petition with the registry of the competent criminal court. The court president shall schedule a session for hearing the appeal, and the Public Prosecution and the appellant shall be duly notified. The court must issue a reasoned ruling within fifteen (15) days of the filing, after hearing the statements of both the appellant and the prosecution or investigating authority, and may take any procedures or investigations it deems necessary.

The Public Prosecution and competent investigating authorities may at any time revoke or amend the travel ban order, including lifting the name from the travel ban or watch list for a specified period, if deemed necessary.

In all cases, the travel ban shall expire upon the lapse of one year from the issuance of the order, or upon a decision to dismiss the criminal case, or a final judgment of acquittal, whichever occurs first.

Part Two: Procedural Rules and Provisions: Experts

Article (10):

The Authority shall establish two registers for recording experts. The first shall include technical and IT personnel employed by the Authority, and the second shall include external technical and IT experts not employed by the Authority.

Experts shall be subject, in the performance of their duties and in defining their rights and obligations, to the general rules and provisions governing the conduct of expert witnesses before judicial authorities.

By way of exception, experts registered in the second register shall be subject to the administrative and disciplinary accountability rules stipulated in the laws governing their profession, if applicable.

The executive regulations of this Law shall specify the rules, conditions, and procedures for registration in each of the two registers.

Part Two: Procedural Rules and Provisions: Digital Evidence

Article (11):

Evidence derived or extracted from electronic devices, equipment, media, data carriers, information systems, computer programs, or any information technology tools shall have the same value and probative force as physical criminal evidence in criminal proceedings, provided that the technical conditions set forth in the Executive Regulations of this Law are met.

Part Three: Crimes and Penalties

Article (12):

Without prejudice to any more severe penalty stipulated in the Penal Code or any other law, and taking into account the provisions of the Child Law No. 12 of 1996, the following offenses shall be punished with the penalties specified alongside each offense.

Chapter One: Offenses Against the Integrity of Networks, Information Systems, and Information Technology: Unauthorized Benefit from Telecommunication and IT Services

Article (13):

Anyone who unlawfully benefits from telecommunication services or audio/visual broadcast channels via an information network or any means of information technology shall be punished with imprisonment for a period not less than three months, and a fine not less than EGP 10,000 and not exceeding EGP 50,000, or either of these two penalties.

Unlawful Access (Unauthorized Access)

Article (14):

Anyone who intentionally accesses, or unintentionally accesses and remains unlawfully in, a restricted website, private account, or information system shall be punished with imprisonment for a period not less than one year, and a fine not less than EGP 50,000 and not exceeding EGP 100,000, or either of these two penalties.

If such access results in the destruction, deletion, alteration, copying, or republishing of data or information on the said site, account, or system, the penalty shall be imprisonment for not less than two years and a fine not less than EGP 100,000 and not exceeding EGP 200,000, or either of these two penalties.

Exceeding Authorized Access

Article (15):

Anyone who accesses a website, private account, or information system using legally granted access rights but exceeds the limits of such rights in terms of time or level of access shall be punished with imprisonment for not less than six months, and a fine not less than EGP 30,000 and not exceeding EGP 50,000, or either of these two penalties.

Unlawful Interception:

Article (16):

Anyone who unlawfully intercepts any information, data, or communication transmitted via an information network or computer device or similar shall be punished with imprisonment for not less than one year, and a fine not less than EGP 50,000 and not exceeding EGP 250,000, or either of these two penalties.

Offense Against the Integrity of Data, Information, and Information Systems

Article (17):

Anyone who intentionally and unlawfully destroys, disrupts, alters the path, or wholly or partially deletes software, data, or information stored, processed, generated, or created on any information system or the like—by any means—shall be punished with imprisonment for not less than two years and a fine not less than EGP 100,000 and not exceeding EGP 500,000, or either of these two penalties.

Offense Against Email, Websites, or Private Accounts

Article (18):

Anyone who damages, disrupts, slows, or unlawfully hacks an individual's email, website, or private account shall be punished with imprisonment for not less than one month, and a fine not less than EGP 50,000 and not exceeding EGP 100,000, or either of these two penalties.

If the offense is committed against the email, website, or account of a private legal entity, the penalty shall be imprisonment for not less than six months, and a fine not less than EGP 100,000 and not exceeding EGP 200,000, or either of these two penalties.

Offense Against Website Design

Article (19):

Anyone who unlawfully damages, disrupts, slows, distorts, hides, or alters the design of a website belonging to a company, institution, establishment, or natural person shall be punished with imprisonment for not less than three months, and a fine not less than EGP 20,000 and not exceeding EGP 100,000, or either of these two penalties.

Part Three: Crimes and Penalties

Chapter One: Offenses Against the Integrity of Information Networks, Systems, and Technology

Offense Against State Information Systems

Article (20):

Anyone who intentionally, or inadvertently and without lawful justification, accesses, remains within, or exceeds their authorized access level in terms of time or privilege—by hacking a website, email, private account, or information system managed by, on behalf of, owned by, or related to the State or any public legal entity—shall be punished with imprisonment for no less than two years, and a fine not less than EGP 50,000 and not exceeding EGP 200,000, or either of these penalties.

If the purpose of such access is to unlawfully intercept or obtain governmental data or information, the penalty shall be imprisonment and a fine not less than EGP 100,000 and not exceeding EGP 500,000.

In all cases, if the act results in the destruction, distortion, alteration, duplication, redirection, republication, or partial or complete deletion of any data, information, websites, accounts, systems, or emails—by any means—the penalty shall be imprisonment and a fine not less than EGP 1,000,000 and not exceeding EGP 5,000,000.

Offense Against Network Integrity

Article (21):

Anyone who intentionally causes an information network to shut down, be disrupted, degraded in performance, jammed, obstructed, or intercepted, or who unlawfully processes its data electronically, shall be punished with imprisonment for not less than six months, and a fine not less than EGP 100,000 and not exceeding EGP 500,000, or either of these penalties.

If the offense results from negligence, the penalty shall be imprisonment for not less than three months and a fine not less than EGP 50,000 and not exceeding EGP 200,000, or either of these penalties.

If the network in question belongs to, is owned by, or is operated on behalf of the State or a public legal entity, the penalty shall be aggravated imprisonment (السجن المشدد) and a fine not less than EGP 500,000 and not exceeding EGP 1,000,000.

Offense Concerning Tools Used to Commit Cybercrimes

Article (22):

Anyone who, without authorization from the competent authority (the "Device"), or without legal or factual justification, possesses, obtains, imports, exports, manufactures, develops, modifies, sells, offers, or circulates any device, equipment, tools, software, access codes, passwords, encryption keys, or similar data, with the intent to use any of them in committing or facilitating any of the crimes stipulated in this law—or concealing its evidence or effects—or if such use or concealment is proven, shall be punished with imprisonment for not less than two years and a fine not less than EGP 300,000 and not exceeding EGP 500,000, or either of these penalties.

Chapter Two: Crimes Committed via Information Systems and Technology

Fraud and Offenses Against Bank Cards and Electronic Payment Tools

Article (23):

Anyone who, without authorization, uses an information network or any means of information technology to access bank card numbers, data, service credentials, or other electronic payment tools shall be punished with imprisonment for not less than three months and a fine not less than EGP 30,000 and not exceeding EGP 50,000, or either of these penalties.

If the offender intended to use such data to obtain third-party funds or services, the penalty shall be imprisonment for not less than six months and a fine not less than EGP 50,000 and not exceeding EGP 100,000, or either of these penalties.

If the offender succeeds in unlawfully obtaining money or services for themselves or others, the penalty shall be imprisonment for not less than one year and a fine not less than EGP 100,000 and not exceeding EGP 200,000, or either of these penalties.

Offenses Involving Fake Websites, Accounts, and Emails

Article (24):

Anyone who creates a fake email, website, or private account and falsely attributes it to a natural or legal person shall be punished with imprisonment for not less than three months and a fine not less than EGP 10,000 and not exceeding EGP 30,000, or either of these penalties.

If the fake email, website, or account is used to harm the person falsely attributed, the penalty shall be imprisonment for not less than one year and a fine not less than EGP 50,000 and not exceeding EGP 200,000, or either of these penalties.

If the offense is committed against a public legal entity, the penalty shall be imprisonment and a fine not less than EGP 100,000 and not exceeding EGP 300,000.

Part Three: Crimes and Penalties

Chapter Three: Crimes Related to the Violation of Privacy and Unlawful Information Content

---

Article (25):

Shall be punished by imprisonment for a period not less than six months and a fine not less than fifty thousand Egyptian pounds and not exceeding one hundred thousand Egyptian pounds, or by either of these two penalties, whoever violates any of the family principles or values in Egyptian society, invades the sanctity of private life, sends a large number of electronic messages to a specific person without their consent, provides personal data to a system or website for the purpose of promoting goods or services without the data subject's consent, or publishes through the information network or by any information technology means, information, news, images, or the like that violate the privacy of any person without their consent, whether the published information is true or false.

Article (26):

Shall be punished by imprisonment for a period not less than two years and not exceeding five years and a fine not less than one hundred thousand Egyptian pounds and not exceeding three hundred thousand Egyptian pounds, or by either of these two penalties, whoever intentionally uses an information program or information technology to process another person's personal data for the purpose of linking it to content that is contrary to public morals, or displaying it in a manner that may harm their reputation or dignity.

Part Three: Crimes and Penalties

Chapter Four: Crimes Committed by the Website Administrator

Article (27):

In cases other than those stipulated in this law, shall be punished by imprisonment for a period not less than two years and a fine not less than one hundred thousand Egyptian pounds and not exceeding three hundred thousand Egyptian pounds, or by either of these two penalties, whoever creates, manages, or uses a website or private account on an information network for the purpose of committing or facilitating the commission of a crime punishable by law.

Article (28):

Shall be punished by imprisonment for a period not less than six months and a fine not less than twenty thousand Egyptian pounds and not exceeding two hundred thousand Egyptian pounds, or by either of these two penalties, any person responsible for managing a website, private account, email, or information system, if they conceal or tamper with digital evidence of any crime provided for in this law that occurred on such platform, with the intent to obstruct the work of the competent official authorities.

Article (29):

Shall be punished by imprisonment for a period not less than one year and a fine not less than twenty thousand Egyptian pounds and not exceeding two hundred thousand Egyptian pounds, or by either of these two penalties, any person responsible for managing a website, private account, email, or information system, who exposes any of them to the commission of a crime stipulated in this law.

Shall be punished by imprisonment for a period not less than six months and a fine not less than ten thousand Egyptian pounds and not exceeding one hundred thousand Egyptian pounds, or by either of these two penalties, any person responsible for managing a website, private account, email, or information system, who negligently causes the exposure of any of them to a crime stipulated in this law, as a result of failure to take the security precautions and measures stated in the executive regulations of this law.

Part Three: Crimes and Penalties

Chapter Five: Criminal Liability of Service Providers

Article (30):

Shall be punished by imprisonment for a period not less than one year and a fine not less than five hundred thousand Egyptian pounds and not exceeding one million Egyptian pounds, or by either of these two penalties, any service provider who refuses to comply with a decision issued by the competent criminal court to block a website, link, or content referred to in the first paragraph of Article (7) of this law.

If such refusal results in the death of one or more persons, or causes harm to national security, the penalty shall be aggravated imprisonment and a fine not less than three million Egyptian pounds and not exceeding twenty million Egyptian pounds. The court shall also order the revocation of the license to practice the activity.

Article (31):

Shall be punished by imprisonment for a period not less than one year and a fine not less than five thousand Egyptian pounds and not exceeding twenty thousand Egyptian pounds, or by either of these two penalties, any service provider who violates the provisions of clause (2) of paragraph (First) of Article (2) of this law. The fine shall be multiplied by the number of affected users.

Article (32):

Shall be punished by imprisonment for a period not less than six months and a fine not less than twenty thousand Egyptian pounds and not exceeding one hundred thousand Egyptian pounds, or by either of these two penalties, any service provider who refuses to comply with the decision issued by the competent investigative authority to provide the data or information referred to in Article (6) of this law.

Article (33):

Shall be punished by a fine not less than five million Egyptian pounds and not exceeding ten million Egyptian pounds, any service provider who breaches any of the obligations stipulated in clause (1) of paragraph (First) of Article (2) of this law. The fine shall be doubled in case of recurrence, and the court may order the revocation of the license.

Shall be punished by a fine not less than twenty thousand Egyptian pounds and not exceeding two hundred thousand Egyptian pounds, any service provider who violates the provisions of paragraphs (Second) and (Fourth) of Article (2) of this law.

Shall be punished by imprisonment for a period not less than three months and a fine not less than two hundred thousand Egyptian pounds and not exceeding one million Egyptian pounds, any service provider who violates the provisions of paragraph (Third) of Article (2) of this law.

Part Three: Crimes and Penalties

Chapter Six: Aggravating Circumstances in the Crime

Article (34):

If any of the crimes stipulated in this law are committed with the intent to disturb public order, endanger the safety and security of society, harm national security or the country's economic status, prevent or obstruct public authorities from performing their duties, disrupt the provisions of the Constitution, laws, or regulations, or harm national unity or social peace, the penalty shall be aggravated imprisonment.

Part Three: Crimes and Penalties

Chapter Seven: Criminal Liability of Legal Persons

Article (35):

Shall be punished by imprisonment for a period not less than three months and a fine not less than thirty thousand Egyptian pounds and not exceeding one hundred thousand Egyptian pounds, or by either of these two penalties, any person who is responsible for the actual management of a legal entity, if the entity's designated website, account, email, or information system is subjected to any crime stipulated in this law and fails to report it to the competent authorities upon becoming aware of it.

Article (36):

In cases where any of the crimes stipulated in this law are committed in the name and for the benefit of a legal person, the person responsible for actual management shall be punished with the same penalty as the principal offender if it is proven that they had knowledge of the crime or facilitated its commission for personal benefit or for the benefit of others.

The court may order the suspension of the legal entity's license to practice its activity for a period not exceeding one year. In the event of recurrence, the court may order the cancellation of the license or the dissolution of the legal entity, as the case may be. The judgment shall be published in two widely circulated daily newspapers at the expense of the legal person.

Article (37):

In the application of the provisions of this law, establishing the criminal liability of the actual management of a legal person does not preclude the criminal liability of the natural persons who are the principal offenders or accomplices in the same criminal act.

Part Three: Crimes and Penalties

Chapter Eight: Ancillary Penalties

Article (38):

Without prejudice to the rights of bona fide third parties, the court, upon conviction of any crime under this law, shall order the confiscation of tools, machines, equipment, or devices that are prohibited by law or that were used in committing, facilitating, or contributing to the commission of the crime.

If the practice of the activity requires a license from a government authority and the convicted legal entity did not obtain such license, the court shall, in addition to the prescribed penalties, order the closure of the premises.

Article (39):

The court may, upon convicting a public employee of a crime stipulated in this law committed during or because of the performance of their duties, order their temporary dismissal from office. In the cases specified in Article (34) of this law, dismissal shall be mandatory.

Part Three: Crimes and Penalties: Chapter Nine: Attempt and Exemption from Punishment

---

Article (40):

Anyone who attempts to commit a misdemeanor stipulated in this law shall be punished with a penalty not exceeding half the maximum penalty prescribed for the completed crime.

Article (41):

Anyone who initiates reporting to the judicial or public authorities about their knowledge of any crime stipulated in this law, before the crime begins or is discovered, shall be exempt from the prescribed penalties.

The court may also exempt or mitigate the penalty if the report is made after the crime is discovered but before the investigation concludes, provided that the offender or accomplice assists the authorities in arresting other perpetrators, recovering the proceeds of the crime, uncovering the truth during the investigation, or facilitating the arrest of perpetrators of a similar crime in nature and seriousness.

This article does not affect the obligation to return the proceeds obtained from crimes under this law.

Article (42):

The accused may, at any stage of the criminal proceedings and before the judgment becomes final, establish reconciliation with the victim, their legal representative, or legal successor, before the Public Prosecution or the competent court, as the case may be, in the misdemeanors set out in Articles (14, 15, 16, 17, 18, 19, 23, 26, 28, 30, 31) of this law.

The victim's acknowledgment of reconciliation shall not be effective except after being approved by the Authority with respect to the misdemeanors mentioned in Articles (14, 17, 18, 23).

Reconciliation shall only be accepted through the Authority in the misdemeanors provided in Articles (29, 35).

The right to reconciliation shall not be extinguished by referring the criminal case to the competent court if the accused pays two-thirds of the maximum fine prescribed for the crime, or the minimum fine, whichever is greater, before a final judgment is issued.

In all cases, the accused who wishes to reconcile must, prior to referring the criminal case, pay an amount equal to double the maximum fine prescribed for the crime. Payment shall be made to the treasury of the competent court or the Public Prosecution, as the case may be.

Reconciliation results in the extinction of the criminal case but does not affect the rights of the victim or the civil claim arising from the crime.

Chapter Four: Transitional and Final Provisions

Article (43):

Service providers and all parties subject to the provisions and obligations of this Law shall take the necessary measures to regularize their status within one year from the date this Law enters into force.

Article (44):

The Prime Minister shall issue the Executive Regulations of this Law within three months from the date of its entry into force.

Article (45):

This Law shall be published in the Official Gazette and shall come into force on the day following its publication.

This Law shall be sealed with the State's Seal and shall be enforced as one of its laws.