Anti-Cyber and Information Technology Crimes Law "EGYPT" Law No. 175 of 2018

"Unofficial Translation"

Mohamed CHAWKI, Ph.D.

Chairman, International Association of Cybercrime Prevention (AILCC)

Paris – France

2020

This work is dedicated to my parents.

For their endless love, support and encouragement

Mohamed Chawki holds a (Ph.D.) in law from the University of Lyon III in France for a dissertation on French; British and American cybercrime legal systems. This was followed by a 3-year post-doctoral research at the Faculty of Law, University of Aix-Marseille III, France. He is senior judge at the supreme administrative court (vice president of the Egyptian Council of State) and former advisor to the Chairman of Capital Market Authority (CMA), to the Chairman of the Egyptian Financial Supervisory Authority (EFSA), to the Minister of Antiquities, at the Nuclear Power Plants Authority (NPPA) and to the Egyptian Minister of Military Production.

Dr. Chawki has extensive knowledge of High Tec criminality, cybercrime, cyber terrorism and IT, including countermeasures and prevention. As a part of his research in France, he carried out an internship at Interpol's Financial and High Tec Crime Unit. He also conducted legal analysis for the Organisation of CyberAngels in NYC and advised cybercrime victims on various issues related to countermeasures and prevention. Doctor Chawki is the co-drafter of the African Union Convention on Cybersecurity. He is also a member of the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program (ISPAC), a member of the European Society of Criminal Law, and a board member of Computer Crime Research Center (CCRC) in Ukraine. He teaches law at private and public universities in Egypt and holds a number of visiting posts abroad. His research interest covers national security, cybercrime and data protection.

Judge Chawki is recognized as a *world leading expert on cybercrime*, Cyberlaws, and Law of ICTs.

Dr. Chawki holds over 25 prizes for this academic achievement and was awarded by the Medal of Excellence by the President of the Arab Republic of Egypt in 1998 , the international prize Claire l'Heureux Dubé from Canada in 2007 and the distinguished services medal from the government of Brazil in 2009.

Email: chawki@cybercrime-fr.org

Official Journal – Issue 32 Bis (C), dated August 14, 2018

Law No. 175 of 2018
On Anti-Cyber and Information Technology Crimes

In the Name of the People,
President of the Republic,
The Assembly of Representatives passed the following Law, and we hereby promulgate it:

Part I
General Provisions
Definitions
Article (1)

In applying the provisions of the current Law, the words and expressions listed below shall have the meanings indicated next thereto:

Authority	**:** National Telecommunication Regulatory Authority
Competent Minister	**:** The Minister concerned with Communications and Information Technology Affairs.
Electronic Data and Information	: all material that can be created, stored, processed, synthesized, transferred, shared or replicated, using the information technology, such as numbers, codes, ciphers, letters, symbols, signals, images, sounds and the like.
Personal Data:	: Any data related directly or indirectly to an identified or identifiable natural person by connecting such data with other ones.
Governmental Data:	: any data related to the State, one of its agencies, bodies, or units, public or independent entities, oversight bodies or any other public legal persons, and the like, that are available on the information network, any other Information System, computer and the like.
Electronic Processing	**:** Any electronic or technological process performed, wholly or partially, for writing, collecting, recording, preserving, storing, integrating, displaying, sending, receiving, handling, publishing, erasing, changing, amending, retrieving or extracting Electronic Data and Information using any other electronic, magnetic or optical media, computers or equipment or any other new technologies or media.
Information Technology	**:** Any connected or disconnected device or range of devices used in storing, retrieving, arranging, organizing, processing, developing and exchanging information or data, including anything related to the mean or media used wirelessly or otherwise.
Service Provider	**:** Any physical or legal person providing Users with information and communication technology services, including whoever processes or stores information by itself or on behalf thereof in any of such services of Information Technology.
User	**:** All natural or legal persons using Information Technology services or benefiting therefrom by any manner whatsoever.
Information Program	: A set of orders and instructions expressed in by any language, sign or signal which take any form whatsoever and which can be used directly or indirectly in a computer for performing a function or achieving a result, whether such orders or instructions are in their original form or any other form in which the same appears in a computer or an Information System.
Information System	: A set of programs and tools prepared for the purpose of managing and processing data and information or providing information services.
Information Network	: A set of devices or information systems connected together, between which information and communication can be exchanged, inter alia, private

and public networks, international information networks and applications used therein.

Website : A domain or virtual location with a definite address on the information network aiming at providing data and information publicly or privately.

Website Administrator : All persons responsible for organizing, administering, following up or maintaining one or more website on the information network, including for access rights of various users of such website, designing or creating and organizing pages, content or administrator thereof.

Private Account : A set of information belonging to and exclusively conferred to a physical or legal person to access or use available services through a website or an Information System.

Electronic mail : a means of exchanging electronic messages through a specific address, between more than a natural or legal person, via information network or other electronic connection means through computers and the like.

Sniffing : Visualizing or obtaining data or information for the purpose of ambience listening, disabling, storing, copying, recording, content changing, misappropriating, path modifying or redirecting for illegitimate reasons and unrighteously.

Hacking : Unauthorized access or that is in violation of the license provisions or access to an Information System, Computer, information network and equivalent thereof by any illegitimate way.

Content : Any data which constitute, solely or jointly with other data or information, a piece of information, sentiment, orientation, conception, meaning or signal to other data.

Digital Evidence : Any electronic data with a probative force or value stored, transferred, extracted or taken from Computers, information network or equivalent thereof. Such information can be collected and analyzed using special devices, programs or applications.

Experience : Any work connected to delivering consultations, examination, revision, assessment or analysis in the fields of Information Technology.

Connection Traffic (Traffic Data) : Data produced by an Information System and indicate the source of connection, contact, sender, recipient, path, hour, date, size, duration and the type of service.

Computer : Each device or technological equipment capable of storing and performing logic and arithmetic operations and used in recording, storing, transferring, creating, retrieving, arranging, processing, developing, exchanging or analyzing data or information or used in connection.

Electronic Support : Any tangible medium used in preserving and handling electronic data and information, including compact disks, optical disks, electronic memory and equivalent thereof.

National Security : Anything related to the independence, stability, security, unity and safety of the country as well as to the affairs of the Presidency of the Republic, National Defense Council, National Security Council, Ministry of Defense and Military Production, Minister of Interior, General Intelligence Service, Administrative Control Authority and bodies thereof.

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

Obligations and Duties of the Service Provider
Article (2)

First: Without prejudice to the provisions of this law and Telecommunication Regulation Law as promulgated by Law No. 10 of 2003, the Service Providers shall:

1. Preserve and store the Information System Registry or any means of information technology for one hundred and eighty days on end. Data to be saved and stored shall be as follows:
   (A) Data enabling identification of the service user.

(B) Data related to the content of the Information System dealt with whenever such data are under the control of the Service Provider.
(C) Traffic-related data.
(D) Data related to communication terminals.
(E) Any other data for which a resolution is passed by the Board of the Authority.

2. Maintain the confidentiality of preserved and stored data, and shall not reveal or disclose such data without a substantiated order of a competent judicial body, including the personal data for any user of the service, or any data or information related to the websites and private accounts to which these users, or the persons and bodies with which they communicate, have an access.
3. Secure the data and information marinating its confidentiality, and shall not disclose or damage it.

Second: Without prejudice to the provisions of the Law on Consumer Protection, the Service Provider shall, in convenient, direct and ongoing manner and way, provide the users of its services and any competent governmental body with the following data and information:

1. Name and address of the Service Provider.
2. Contact information related to the Service Provider, including the email address.
3. Data of license to identify the Service Provider and the competent body by which the Service Provider is supervised.
4. Any other information whose value is deemed by the Authority as important for protecting the service users, and for its determination a resolution is passed by the Competent Minister.

Third: Subject to observing the privacy guaranteed by the Constitution, the Service Providers and their respective members shall, upon the request of National Security Agencies and according to their needs, provide all technical capabilities that permit such agencies to exercise its competences according to the Law.

Fourth: The Service Providers of Information Technology, and their agents and distributors that are entrusted with marketing such services, shall obtain the users data. It shall be prohibited for any person other than the foregoing to do the same.

Scope of applying the law in terms of place
Article (3)

Without prejudice to the provisions of Part I of Book I of the Penal Code, the provisions of this Law shall apply to each non-Egyptian who commits outside the Arab Republic of Egypt an offence as set forth in this Law, whenever the crime was criminalized, under any description, in the country in which it was committed, in any of the following cases:

1. If the offence was committed using any of the means of transportation by land, sea or air registered in the Arab Republic of Egypt or flying its flag.
2. If one or all of the victims were Egyptians.
3. If the offence was prepared, planned, directed, managed or financed in the Arab Republic of Egypt.
4. If the offence was committed by an organized criminal group, which practices its criminal activities in more than one country including the Arab Republic of Egypt.
5. If the offence is likely to cause detriment to any citizen or resident of the Arab Republic of Egypt, or to endanger the security or any interest of the Republic whether locally or abroad.
6. If the perpetrator is found in the Arab Republic of Egypt after committing the crime and was not extradited yet.

International Cooperation in the field of Anti-Cyber and Information Technology Crimes
Article (4)

In light of the ratified international, regional and bilateral agreements, or in application of the principle of reciprocity, the concerned Egyptian authorities shall cooperate with their foreign counterparts through exchanging information to avoid committing Information Technology Crimes, and to assist in the investigation and tracking down the perpetrators of those crimes.

The National Centre for Computer and Network Emergency Response at the Authority shall be the technical point accredited in this regard.

Part II
Provisions and Procedural Rules
Law enforcement Officers
Article (5)

By a resolution of the Minister of Justice in agreement with the Competent Minister, the power of law enforcement officers may be given to the personnel of the Authority or other as determined by the National Security Agencies regarding the offences committed in violation of the provisions of the present Law or related to the duties of their jobs.

Temporary Judicial Writs
Article (6)

The investigation body concerned may, as the case may be, issue a substantiated writ to the competent law enforcement officer in respect of one or more of the following matters, for a period not exceeding thirty days renewable for one time, if this will help reveal the truth about the perpetration of an offence punishable under this law:

1. Control, withdrawal, collection, or seizure of data and information or information systems, or tracking them in any place, system, program, electronic support or computer in which they are existing. Its digital evidence shall be delivered to the body issuing the order, provided that it shall not affect the continuity of the system and provision of the service, if so required.
2. Searching, inspecting, accessing and signing in the computer programs, databases and other devices and information systems in implementation of the seizure purpose.
3. The concerned investigation body may order the Service Provider to submit the data or information related to an information system or a technical device under the control of or stored by the Service Provider, as well as the data of the users of its service and the connection traffic made in that system or the technical system.

   In all circumstances, the writ issued by the investigation entity must be substantiated.

   The aforesaid writs shall be appealed before the criminal court concerned, as held in the deliberation room on the dates and according to the procedures stipulated in the criminal procedural law.

Procedures and decisions issued in respect of the site block writs
Article (7)

If there are evidences that a website broadcast, inside or outside the State, is displaying words, numbers, images, films, any publicity materials or other, that would be an offence of those stipulated in the present Law, jeopardize the national security or economy, the concerned investigation body may order to block the website(s), subject matter of broadcasting, where applicable from the technical point of view.

The investigation body shall submit the blocking order to the competent court, held at council chamber within twenty-four hours along with a memorandum of its opinion. The court shall issue its decision on the substantiated order, either by admitting or dismissing such substantiated order, in no more than seventy-two hours as of the date of submitting the substantiated order to the court. In case of summary matters due to a current risk or imminent harm, the inquiry and law enforcement bodies may notify the AUTHORITY which shall immediately notify the Service Provider of the temporary blocking of the website, content, websites, or links set out in the First Paragraph of this Article and in accordance with its provisions. Upon its receipt, the Service Provider shall implement the content of the notice.

The inquiry and law enforcement body that gave the notice shall file a report establishing the procedures made in accordance with the provisions of previous Paragraph. Such report shall be submitted to the investigation bodies within forty-eight hours as from the date of notice given to AUTHORITY. Regarding this report, the procedures set out in the Second Paragraph of this Article shall be applied. In this case, the competent court shall issue its decision, either by admitting or dismissing the procedures of blocking.

If the report set out in the previous Paragraph is not timely submitted, the blocking shall be deemed null and void.

During the consideration of the action or based upon the request of the investigation body, AUTHORITY or relevant parties, the trial court shall issue an order terminating or amending the scope of the blocking decision.

In all circumstances, nullification of the block decision shall take place by issuing a criminal lawsuit dismissal order or a final judgement of acquittal.

Grieving the Decisions Issued on Websites Blocking Applications

Article (8)

Any person against whom a judicial writ that is stipulated in Article (7) hereof was issued, the public prosecution, the concerned investigation body and all persons concerned, may lodge a complaint against such judicial decision or against the procedures of its implementations before the competent criminal court after the lapse of seven days from the date of issuing or implementing the decision, as the case may be. Should the complaint be dismissed, such person may lodge a new complaint after the lapse of three months from the date of the dismissal of his complaint.

In all circumstances, the complaint shall be reported at the registry of the competent criminal court. The head of the court shall schedule a hearing for the complaint and shall notify the complainant, AUTHORITY and all persons concerned. The court shall decide on the grievance within a maximum period of seven days from the date of reporting such complaint.

Travel Ban

Article (9)

The public prosecutor or assigned attorneys general at the appeal prosecution, and the concerned investigation bodies, may as necessary or where sufficient evidence is established as to the gravity of an accusation in committing or attempting the commission of a crime prescribed in this Law order banning the accused from traveling outside the country, or add his/her name to the arrest-on-arrival list under a fixed-term substantiated order.

Any person against whom a travel ban order was issued may lodge a complaint against such order before the competent criminal court within fifteen days from being notified of the order. Should the complaint be dismissed, such person may lodge a new complaint after the lapse of three months from the date of the dismissal of his complaint.

The complaint shall be reported at the registry of the competent criminal court. The head of the court shall schedule a hearing for the complaint and shall notify the public prosecution and complainant. The court shall decide on the complaint within a maximum period of fifteen days from the date of reporting such complaint by a substantiated judgment after hearing the statements of the complainant and public prosecution or the concerned investigation body, as the case may be, for which purpose the court may apply the procedures or investigations as it deems necessary in this regard.

The public prosecution and competent investigation bodies may at all times withdraw the writ issued thereby, and may also modify same by removing the name placed on the travel ban lists or arrival watch list for a definite period when necessary.

In all circumstances, the travel ban shall be overturned after the lapse of one year of its issuance, by issuing an order that the criminal case is to be dismissed, or issuing a final judgment for acquittal.

Experts

Article (10)

Two registers shall be founded at the Authority for entering the experts, one of which for the technical and technological staff of the Authority and the other for the technical and technological experts not working at the Authority.

For exercising their duties and determining their obligations and rights, the experts shall be subject to the rules and provisions related to the rules regulating expertise before judicial bodies.

For exception to those rules, the experts entered in the second registry shall be subject to the rules and provisions related to the administrative and disciplinary liability set forth in the law governing their work, if any.

The executive regulations of this Law shall specify the rules, conditions and procedures of entry in each registry.

Digital Evidence

Article (11)

The evidence derived or taken from devices, equipment, media, electronic supports, information system, software, or any means of information technology shall have the same value and force of criminal material evidence in criminal evidence where the technical conditions set out in the executive regulations of this Law are met.

Part III
Crimes and Penalties
Article (12)
Without prejudice to any severer penalty provided for in Penal Code or any other law, and subject to the provisions of Law No. 12 of 1996 Promulgating the Child Law, the following crimes shall be punished according to the penalty next to each crime.

(Chapter One)
Encroaching on the Security of Information Networks, Systems and Technologies
Crime of unrighteous benefit from the telecommunications and information services and the technology thereof
Article (13)
Anyone who unduly uses the network of information system or a mean of information technology in communication service or a service of audio or visual broadcasting channels shall be punishable by imprisonment for no less than three months and a fine of no less than ten thousand Egyptian Pounds and no more than fifty thousand Egyptian Pounds, or by one of these two penalties.

Unauthorised Access Offences
Article (14)
Anyone who intentionally gains access to or unintentionally and unduly continues in a website, private account or prohibited information system shall be punishable by imprisonment for no less than one year and a fine of no less than fifty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.

If such access resulted in damaging, removing, changing, copying or republishing the data or information existed in the website, private account or information system, such person shall be punishable by imprisonment for no less than two years and a fine of no less than one hundred thousand Egyptian Pounds and no more than two hundred thousand Egyptian Pounds, or by one of these two penalties.

Crime on Infringement of surpassing the Right of Access
Article (15)
A penalty of imprisonment for a period not less than 6 months and or a fine of no less than thirty thousand Egyptian pounds and no more than fifty thousand Egyptian pounds shall be inflicted on whoever accessed a site, private account or information system using authorized right of his own but exceeded the limits of this right in terms of time or access level.

Crime on Infringement of Unlawful Sniffing
Article (16)
Anyone who unduly intercepts any information, data, or whatever is published on the information network or a computer and other shall be punishable by imprisonment for no less than one year and a fine of no less than fifty thousand Egyptian Pounds and no more than two hundred and fifty thousand Egyptian Pounds, or by one of these two penalties.

Crime on Infringement of Data, Information, and Information Systems Integrity
Article (17)
Anyone who causes damage to, disrupts, modifies the path of, intentionally and dully cancels, either wholly or in part, software and data or information stored, processed, produced or created in any information system and other, whatever the method used in the crime, shall be punishable by imprisonment for no less than two years and a fine of no less than one hundred thousand Egyptian Pounds and no more than five hundred thousand Egyptian Pounds, or by one of these two penalties.

Crime of encroaching on the Email, sites or private accounts
Article (18)
Anyone who causes damage to, disrupts, slows down or hacks an email, website or private account owned by an individual shall be punishable by imprisonment for no less than one month and a fine of no less than fifty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.

If the crime is perpetrated against an email, website or private account owned by a private legal person, the penalty shall be imprisonment for no less than six months and a fine of no less than one hundred thousand Egyptian Pounds and no more than two hundred thousand Egyptian Pounds, or by one of these two penalties.

Crime on Infringement of Website Design

Article (19)

A penalty of imprisonment for a period not less than three months, and or a fine of no less than twenty thousand Egyptian pounds and no more than one hundred thousand Egyptian pounds, shall be applied on whoever without right deactivates, damages; obstructs, deforms, hides or alters the designs of a website that belongs to a company, institution; establishment or a natural person.

Crime on Infringement of State Information Systems

Article (20)

Anyone who intentionally gains access to, unintentionally and unduly continues in, excesses the authorized right as to the time or level of access, hacks a website, email, private account, or information system administrated, with the knowledge of or for, owned by or related to the State or a public legal person shall be punishable by imprisonment for no less than two years and a fine of no less than fifty thousand Egyptian Pounds and no more than two hundred thousand Egyptian Pounds, or by one of these two penalties.

If the access was with the intention of interception or unduly obtaining governmental data or information, the penalty shall be imprisonment and a fine of no less than one hundred thousand Egyptian Pounds and no more than five hundred thousand Egyptian Pounds.

In all circumstances, if any of the previous acts resulted in damaging to, destructing, distorting, changing, altering the design of, copying, recording, amending the path, republishing or cancelling, either wholly or in part, by any mean whatsoever, such data, information, website, private account, information system or email, the penalty shall be imprisonment and a fine of no less than one million Egyptian Pounds and no more than five million Egyptian Pounds.

Crime on Infringement of Information Network Integrity

Article (21)

Anyone who intentionally suspends, disrupts, impedes the efficiency of, jams, intercepts or unduly makes e-processing for the data of the information network shall be punishable by imprisonment for no less than six months and a fine of no less than one hundred thousand Egyptian Pounds and no more than five hundred thousand Egyptian Pounds, or by one of these two penalties.

Anyone whose fault caused the foregoing shall be punishable by imprisonment for no less than three months and a fine of no less than fifty thousand Egyptian Pounds and no more than two hundred thousand Egyptian Pounds, or by one of these two penalties.

If the crime is perpetrated against an information network related to, owned or administrated by the State or a public legal person, the penalty shall be imprisonment and a fine of no less than five hundred thousand Egyptian Pounds and no more than one million Egyptian Pounds, or by one of these two penalties.

Programs and Equipment Used in
Committing Information Technology Crimes

Article (22)

Anyone who possesses, acquires, procures, sells, makes available, manufactures, produces, imports, exports or trades, by any way whatsoever, any devices, equipment or tools, or designed, developed or transformed software, or passcodes, ciphers, symbols or any similar data, without obtaining the permission of AUTHORITY or holding a credential in fact or in law, and it is proved that such act was aimed at using any of the foregoing for committing or enabling the commission of any crime provided for in this Law, or for concealing the traces or evidence thereof, or that such use, enablement or concealment took place, shall be punishable by imprisonment for no less than two years and a fine of no less than three hundred thousand Egyptian Pounds and no more than five hundred thousand Egyptian Pounds, or by one of these two penalties.

(Chapter Two)

Crimes Committed by Information Systems and Technologies

Fraud and Encroachment Crimes Against Credit Cards, Services and electronic payment tools

Article (23)

Anyone who uses the information network or a mean of information technology to unduly access numbers or data of bank cards and services or other means of e-payment shall be punishable by imprisonment for no less than three months and a fine of no less than thirty thousand Egyptian Pounds and no more than fifty thousand Egyptian Pounds, or by one of these two penalties.

If the perpetrator intended from conducting the foregoing acts to obtain funds of third parties or the services provided thereby, the perpetrator shall be punishable by imprisonment for no less than six months and a fine of

no less than fifty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.
A penalty of imprisonment for a period not less than one year and or a fine of no less than one hundred thousand Egyptian pounds if the perpetrator was able to seize such services or third party funds whether for himself or for others.

Crimes on Creating Fake Websites, Private Accounts and Emails

Article (24)

Anyone who creates a fake email, website or private account, and falsely attributed the same to natural or legal person, shall be punishable by imprisonment for no less than three months and a fine of no less than ten thousand Egyptian Pounds and no more than thirty thousand Egyptian Pounds, or by one of these two penalties.
If the perpetrator used the fake email, website or private account in a matter that defiles reputation of the person to whom same is attributed, the perpetrator shall be punishable by imprisonment for no less than one year and a fine of no less than fifty thousand Egyptian Pounds and no more than two hundred thousand Egyptian Pounds, or by one of these two penalties.
If the crime is perpetrated against a public legal person, the penalty shall be imprisonment and a fine of no less than one hundred thousand Egyptian Pounds and no more than three hundred thousand Egyptian Pounds, or by one of these two penalties.

(Chapter Three)

Crimes on Infringement of Privacy and Unlawful Information Content

Article (25)

Anyone who infringes a family principle or value of the Egyptian society, encroaches on privacy, sends many emails to a certain person without obtaining his/her consent, provides personal data to an e-system or website for promoting commodities or services without getting the approval thereof, or publishes, via the information network or by any means of information technology, information, news, images or the like, which infringes the privacy of any person involuntarily, whether the published information is true or false, shall be punishable by imprisonment for no less than six months and a fine of no less than fifty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.

Article (26)

Anyone who deliberately uses an information program or information technology in processing personal data of a third party to connect such data with an abusive content or to display the same in a way detrimental to the reputation of such third party shall be punishable by imprisonment for no less than two years and a fine of no less than one hundred thousand Egyptian Pounds and no more than three hundred thousand Egyptian Pounds, or by one of these two penalties.

(Chapter Four)

Crimes Committed with the Site Administrator

Article (27)

In cases other those stipulated herein, anyone who creates, manages, uses a website or a private account on the information network for the purpose of committing or facilitating a punishable crime shall be punishable by imprisonment for no less than two years and a fine of no less than one hundred thousand Egyptian Pounds and no more than three hundred thousand Egyptian Pounds, or by one of these two penalties.

Article (28)

Anyone responsible for managing a website, private account, email or information system conceals or manipulates the digital evidence of a crime stipulated herein and committed in a website, account or email with the purpose of hindering the work of the competent official authorities shall be punishable by imprisonment for no less than six months and a fine of no less than twenty thousand Egyptian Pounds and no more than two hundred thousand Egyptian Pounds, or by one of these two penalties.

Article (29)

Anyone responsible for managing a website, private account, email or information system and exposes any of the same to a crime stipulated herein shall be punishable by imprisonment for no less than one year and a fine of no less than twenty thousand Egyptian Pounds and no more than two hundred thousand Egyptian Pounds, or by one of these two penalties.
Anyone responsible for managing a website, private account, email or information system and its negligence, which is failure to take security measures and precautions mentioned in the executive regulation hereof, causes the same to be exposed to a crime stipulated herein shall be punishable by imprisonment for no less than six

months and a fine of no less than ten thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.

(Chapter Five)
Criminal liability of the Service Providers

Article (30)

Each Service Provider refrains from implementing the judgement issued by the competent criminal court, which is blocking a website, link or content referred to in the first paragraph of Article (7) hereof shall be punishable by imprisonment for no less than one year and a fine of no less than five hundred thousand Egyptian Pounds and no more than one million Egyptian Pounds, or by one of these two penalties. If refraining from implementing such judgement results in the death of one or more person or damaging national security, such Service Provider shall be punishable by rigorous imprisonment and a fine of no less than three million Egyptian Pounds and no more than twenty million Egyptian Pounds. Further, the court revokes the license of practicing the activity.

Article (31)

A penalty of imprisonment for a period not less than one year and or a fine of no less than five thousand Egyptian pounds and no more than twenty thousand Egyptian pounds shall be applied one each service provider who violates the provisions of item 2 of Clause First of article 2 of the current law. The penalty shall be multiplied in case there are multiple victims of the service users.

Article (32)

Each Service Provider refrains from implementing the order issued by the competent investigation authority regarding delivering data and information referred to in Article (6) herein shall be punishable by imprisonment for no less than six months and a fine of no less than twenty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.

Article (33)

Each Service Provider breaches any of obligations thereof stipulated in clause (1), (first) paragraph, Article (2) herein shall be punishable by a fine of no less than five millions Egyptian Pounds and no more than ten millions Egyptian Pounds. In case of recidivism, such fine shall be doubled and the court may revoke the license.

A fine of no less than twenty thousand Egyptian pounds and no more than two hundred thousand Egyptian pounds shall be applied on every service provider who infringes the provisions of clause second and clause fourth of article 2 of this law.

Each Service Provider violates the provisions of the (third) paragraph of Article (2) herein shall be punishable by imprisonment for no less than three months a fine of no less than two hundred thousand Egyptian Pounds and no more than one million Egyptian Pounds.

(Chapter Six)
Aggravating Circumstances of the Crime

Article (34)

If any crimes stipulated herein committed for the purpose of disturbing the public order, jeopardizing the safety and security of the society, damaging the national security or economic position of the country, obstructing or hindering the works of public authorities, suspending the provisions of the constitution, laws or regulations, or prejudicing national unity or social harmony, the penalty shall be rigorous imprisonment.

(Chapter Seven)
Criminal liability of the Legal Person

Article (35)

Each person responsible for the actual management of any legal person, if the website, private account, email or information system of the entity administered by such person exposes to any crimes stipulated herein and such person does not inform the competent official authorities when it becomes aware of such crime, shall be punishable by imprisonment for no less than three months and a fine of no less than thirty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.

Article (36)

In cases where any of the crimes stipulated herein are committed in the name of and in favor of the legal person, the person responsible for the actual management, if it is proven that such person is aware of or facilitates the crime for achieving an interest for itself or a third party, shall be punishable by the same penalty imposed on the original perpetrator of the crime.

The court may suspend the license of practicing the activity relating to the legal person for no more than one year. In case of recidivism, the court may revoke such license or dissolve the legal person as the case may be. The judgement shall be published in a widely known daily newspaper at the expenses of the legal person.

Article (37)

In applying the provisions of this Law, determining the responsibility of the actual management of the legal person shall not result in the exclusion of the criminal responsibility of natural persons acting as principals or partners from the same facts of the crime.

(Chapter Eight)
Consequential Penalties

Article (38)

Without prejudice to rights of other bona fide third parties, in case of conviction in any of the crimes stipulated herein, the court shall confiscate tools, machines, equipment and devices which may not be possessed according to the law or other tools, machines, equipment and devices used in committing, participating in or facilitating the crime.

In the cases where the obtainment of a license from a governmental entity is a precondition for practicing the activity, however the legal person convicted of any of the offences mentioned in the current law didn't obtain such license, the court shall decide the closure of the legal person in addition to the prescribed penalties.

Article (39)

If the court convicts a public employee for committing a crime stipulated herein, during and because of its job, the court may temporarily dismiss such public employee except in cases referred to in Article (34) herein where dismissal shall be mandatory.

(Chapter Nine)
Attempting to Commit a Crime and Exception from Penalty

Article (40)

Whoever attempts to commit the crimes stipulated herein shall be punishable by no more than half of the maximum penalty prescribed for a crime.

Article (41)

Any perpetrators or co-perpetrator take the initiative to inform the judicial or public authorities of a crime before committing and after detection thereof shall be exempted from penalties prescribed for crimes stipulated herein.

The court may exempt or mitigate such penalty if such informing takes place after detection of the crime and before conducting investigation therein and if the perpetrator or partner, during investigation, enables the competent authorities to arrest the other perpetrators of the crime, seize funds – subject of the crime; helps in revealing the truth during research and investigation or in arresting the perpetrator of another similar crime in terms of type and seriousness thereof.

The provision of this Article shall not breach the mandatory repayment of funds collected from crimes stipulated herein.

Reconciliation

Article (42)

In any case whatsoever of the criminal proceeding and as of the date in which the judgement becomes final, the accused may prove reconciliation with the victim or attorney or general successor thereof before the public prosecution or the competent court as the case may be, in misdemeanors stipulated in Articles nos (14, 15, 16, 17, 18, 19, 23, 26, 28, 30 and 31) herein.

The victim's acknowledgement of the aforementioned reconciliation shall be effective only by certification from AUTHORITY with respect to misdemeanors stipulated in Articles nos (14, 17, 18 and 23) herein.

Compromise shall accepted only by AUTHORITY with respect to misdemeanors stipulated in Articles nos (29 and 35) herein.

The accused's right to reconciliation by filing the a criminal proceeding before the competent court shall not be forfeited if the accused pays two thirds of the maximum fine prescribed for the crime or the minimum thereof, whichever is greater, before issuing a final judgement in the subject of such criminal proceeding.

In all cases, before filing the criminal proceeding, the accused who seeks reconciliation shall pay an amount equivalent to the double maximum of the fine prescribed for the crime. Such fine shall be paid in the treasury of the competent court or the public prosecution, as the case may be.

The reconciliation shall result in the lapse of the criminal lawsuit, and shall have no impact on the rights of the person affected by the crime or on the civil lawsuit.

Part IV
Transitional and Closing Provisions

Article (43)

The Service Providers and the parties addressed with the provisions of this Law and the obligations set hereby shall take the measures required for adjusting their state of affairs within one year as of the date of enforcing the provisions hereof.

Article (44)

The Prime Minister shall issue the executive regulations of this Law within three months as of the date of enforcing it.

Article (45)

This Law shall be published in the Official journal, and shall come into force following its date of publication. This Law shall be stamped by the seal of the State, and shall be enforced as one of its Laws.

The Presidency of the Republic on:
3 Thul-Hijjah 1439 A.H.
(Corresponding to 14 August 2018 Gregorian calendar)

Abdelfattah Elsisi