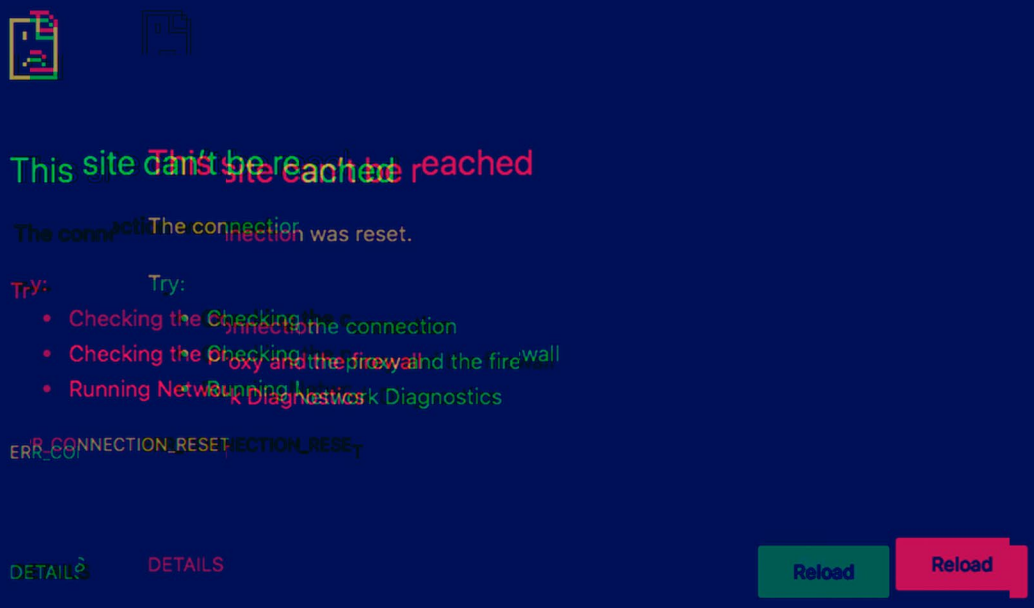
New laws .. The thick stick of the state to control the Internet



New laws.. The thick stick of the state to control the Internet

Edited by: Mohamed Nagy

Publisher:
Association o Freedom of Thought and Expression

info@afteegypt.org
www.afteegypt.org

Cover Design: **Amal Hamed**
Internal Design:

Contant

Introduction

On May 24, 2017, the Egyptian government launched a large-scale Internet monitoring campaign that resulted in the blocking of at least 500 different websites between press sites and others of civil society organizations as well as proxy sites / block-bypassing sites. However, successive Egyptian governments' attempts to control the Internet are not a recent matter; these efforts began with the increasing importance of the Internet as a tool for mobilization and political pressure.

The most prominent phase in this context was the Egyptian government's complete cut of the Internet in Egypt during the revolution of 25 January 2011. However, this quest became more urgent in the period following the ousting of former President Mohamed Morsi and the takeover by the army. This coincided with the Authority's attempts to stifle public space as a whole and the restriction of any anti-government manifestations in the new Egyptian reality, where electronic space emerged as a means - almost the only remaining one - to express free opinion.

Since the state began blocking websites, no one has claimed responsibility for the wide-ranging blocking or its causes, despite numerous human rights claims, as well as three pending cases before the Administrative Court of the State Council demanding disclosure of the legal authority behind the blocking. The only exception was a decision issued by the Committee for the Custody and Administration of the Muslim Brotherhood's funds, affecting only 33 sites.

In addition to the blocking, Egyptian authorities arrested many activists on the Internet and charged them in accordance with a number of different laws, foremost the Telecommunications Law, the Egyptian Penal Code and the Anti-Terrorism Law. Despite the vagueness of the provisions of these laws, authorities have been able to use them to charge internet activists and users of social networking sites, accusing them of misuse of social media, spreading false news and joining a terrorist group.

Because the Internet siege and repression of its users has gone beyond the jurisdiction of existing laws, the State has enacted the Anti-IT Crimes Act, which includes 45 articles divided over four sections, aiming at complete control of the Internet, suppression of

its users and the codification of state practices in controlling this space, blocking Web sites and collective monitoring of communications. The draft law has been circulated for three consecutive years, until it was passed by Parliament on 5 June 2018, ratified by the President of the Republic and published in the Official Gazette to become effective on 18 August 2018.

At the same time, the Egyptian Parliament also approved a law regulating the press and the media, which through its articles can control the Internet. Its articles give the Supreme Council for Media Regulation the authority to impose sanctions on every personal website, personal blog or personal electronic account once the number of its followers amount to 5,000 people or more, which shows Parliament's attempt to establish a system of comprehensive control of accounts, blogs and personal sites, and enable the Supreme Media Council - whose regulation does not provide for this authority - to prosecute citizens who express their views online.

The President of the Republic ratified the law and issued it under No. 180 of 2018 in the Official Gazette on 27 August, to become effective immediately.

This paper attempts to provide a reading regarding the expected Internet situation in accordance with the provisions of the new laws. The paper is divided into three small chapters. The first deals with the articles on Internet censorship, the second with the comprehensive monitoring of communications in Egypt, while the third presents the severe penalties imposed by law on users.

New laws to expand Internet censorship

The Anti-IT Crimes Act establishes the blocking of websites. According to Article 7, websites can be blocked for any published content that is considered a crime under the law, on condition that it poses a threat to national security or jeopardizes the security of the country or its national economy, all of which are vague expressions, usually used by the Egyptian legislator. A site is blocked in this case whether it is broadcasted from inside Egypt or from abroad. During previous periods, victims of violations of freedom of expression in Egypt faced similar charges, such as the investigation of nine journalists from Al-Masry Al-Youm newspaper, following the publication of an investigative report, titled "The state mobilizes voters", where they were accused of publishing false news that would with malice harm public safety and the public good.

In addition to the law of electronic crime, article 19 of the Press and Information Regulation Law was formulated in loose and vague formulations, giving the law enforcement authorities the discretion to block websites, without being bound by clear criteria. This is a repeated tendency by the Egyptian legislator, which aims at using new laws to violate citizens' rights. According to this article, a site can be blocked in case it publishes or broadcasts false news or any content that aims to encourage or instigate violation of the law, violence or hatred, discrimination between citizens, racism or intolerance, or includes defamation or slander of individuals, or an insult of divine religions or religious beliefs. Most of what is stated in this article is loose and unspecified and is used against defendants against the backdrop of expressing their views, whether through digital media or other means, as in the case of blogger and activist Wael Abbas, who was accused of publishing false news through social media networks.

Not only did the legislator order the block of websites in the law regulating the press and the media, but gave the Supreme Information Council the power to block personal accounts on social networking sites. According to article 19 of the law, if an electronic account published or broadcasted false news, or any content that instigates violation of the law, violence, hatred, discrimination against citizens, racism or intolerance, or a challenge individuals' reputation or slander, or abuse of divine religions or religious

beliefs, then the Supreme Council of Information may stop or block the personal site, blog or account, once it has 5000 or more followers.

During past years, Egyptian authorities have accused activists using laws, notably the Communications Law, the Egyptian Penal Code and the Anti-Terrorism Law, focusing on accusations of misuse of social media, spreading false news and joining a terrorist group. However, the law regulating the press and media is based on broader and more numerous possible charges. It also states for the first time that Egyptian authorities may block personal social media accounts in violation of the provisions of the Egyptian Constitution and international standards related to the protection of the right to freedom of expression.

A question arises here regarding the nature of the blocking stipulated by the law. Is it a total ban? Or is it possible to block some links only if they contain "crimes" as defined by law? It is clear that the law does not specifically distinguish between cases in which the site is completely blocked, and cases in which certain links on the site are blocked. For example, a site with millions of pages can be blocked because of the content on one page only. Since the law did not specify total and partial blockages, this would be left to the executive regulations, which would allow the executive branch to arbitrarily use the legal text. The provisions regulating censorship decisions - whether in the laws regulating the press and the media or in the law against IT crimes - contain absolute clauses on blocking (blog - site - account), which means full blocking, except for the third paragraph of Article (7) of the law Combating IT crimes, which referred to the "temporary blocking of the site, sites, links or content", which means that there is room to apply partial blocking.

The law authorizes investigation and hearing authorities (the police) the power to block sites directly, with subsequent judicial oversight. Investigating authorities can demand the block of electronic sites if they believe that these sites pose a threat to national security or the security of the country or Its national economy, provided that the block order is brought before a competent court within 24 hours, which issues its decision within 72 hours. In the event of urgency or imminent danger or damage, the police may request the block from NTRA, which in turn requests the providers

to temporarily, but immediately execute the order upon its receipt. The situation is presented to the prosecution bodies within 48 hours, which in turn present it to Court as mentioned above. On the other hand, the Supreme Council for Media Regulation has the power to block electronic sites as well as personal websites, accounts and blogs with more than 5,000 followers, according to the law governing the press and media.

The law requires telecommunications companies to implement the blocking decision immediately upon its receipt. In case of non-implementation (in accordance with Article 30), imprisonment shall be imposed for a period not less than one year and/or a fine not less than five hundred thousand pounds and not exceeding one million pounds. If failure to implement the court decision results in the death of one or more persons or harming national security, the penalty shall be up to the maximum imprisonment and a fine of not less than three million pounds and not exceeding twenty million pounds and the revocation of the license to practice the profession.

The two law regulates the process of appeal against the block decision. According to the law of "cyber crime" if the decision issuing authority is the public prosecutor or investigating magistrate or a police authority, the decision can be contested before the competent criminal court after seven days from the date of issuance or enforcement. If the appeal is rejected, a new grievance may be filed, three months after the date of rejection. The court shall decide the grievance within a period not exceeding 7 days.

In the case of the press and media regulation law, the decision of blocking can be appealed to the Supreme Council of Information, and then to the Administrative Court of Appeal in case of rejection of the grievance or lack of reply within 60 days.

Monitoring communications as a permanent practice

Article 2 of the Anti-IT-Crimes Act regulates the comprehensive monitoring of communications in Egypt, where telecommunications companies are required to keep and save customer usage data for a period of 180 days. These include user-identifiable data, data on the content of the information system, and those relating to the movement of use and devices used. This means that telecom providers will have data that illustrates all users' practices, such as phone calls and text messages, all data related to them, the sites they visit, and applications used on smart phones and computers. In addition, the law requires telecommunications companies to comply with any "other data to be determined by a decision" from the NTRA Board of Directors. This means that telecommunications service providers may be required to collect and retain data not provided for in the law, once an administrative decision has been issued by NTRA. The article gives national security authorities the right to view such data and obliges the providers of telecommunications services to provide necessary technical facilities. The law defines national security bodies as including "the Presidency, the Armed Forces, the Ministry of Interior, the General Intelligence and the Administrative Oversight Authority".

Article 2 does not address any details of the link between monitoring and a judicial measure to reveal the involvement of a legally sanctioned offense. However, the article clearly requires comprehensive monitoring of all users in Egypt. Here, the legislator of the telecommunications companies has set up a repository of information related to users and committed them to the provision of surveillance techniques, which is incompatible with Article 57 of the Egyptian Constitution, which states that: " The right to privacy may not be violated, shall be protected and may not be infringed upon.. Postal, telegraphic and electronic correspondences, telephone calls, and other means of communication are inviolable, and their confidentiality is guaranteed. They may not be confiscated, revealed or monitored except by virtue of a reasoned judicial order, for a definite period, and only in the cases defined by Law." Thus, article II of the Cybercrime Act infringed on the constitutional protection of communication data.

Although article 2 establishes permanent monitoring as a legal practice, article 6 of the law refers to the possibility of issuing a temporary conditioned injunction issued by the competent investigative bodies to the competent judicial officers for a period not exceeding 30 days, renewable for one time only, to monitor a person, once this is found to be useful in disclosing the truth on the commission of a crime punishable by virtue of the provisions of this law. This would be as follows:

- Control, withdrawal, collection or holding data, information or information systems, and tracking them anywhere, within any system, program, electronic domain or computer in which they are located. Their digital evidence shall be delivered to the issuer of the decision, provided this does not interfere with the continuity of the systems and the service provision if they are found to be necessary.
- Research, inspection, and access to computer programs, databases and other information equipment and systems for the purpose of control.

In its annual report for 2017[1], AFTE referred to the involvement of the Egyptian authorities in the purchase of devices and software to monitor the Internet from a French company, with the assistance of the Government of the United Arab Emirates, at a value of 10 million Euros. These systems and software help to monitor users, track phone calls, text messages, e-mail, and social networks. The report pointed out that this deal is only one in a long series of attempts by successive Egyptian authorities to monitor Internet users.

Despite all these years of relentless attempts to monitor the Internet, this law is a serious development in this regard. The illegal practices of successive governments in Egypt have become legal and uncontested. Given the Egyptian political climate, serious fear has emerged from the use of the law to gather information about activists, bloggers, journalists and human rights defenders.

1. Association of Freedom of Thought and Expression, Edited by Mohamed Nagy, Legalising Repression: How Authority Tightens The Control Of Freedom Of Expression, 25 march 2018 ،https://afteegypt.org/publications_org/2018/03/18/14818-afteegypt.html

Penalties .. The stick of law

A key feature of the IT Crimes Law is the intensification and expansion of sanctions in a way that reflects the government's intention to tighten an iron grip on the Internet and its users. The law monitors cynical pages and accounts and pursues those responsible for them. The IT Crimes Act describes these types of accounts as "fabrication of sites, personal accounts and emails". Penalties under Article 24 of the Law shall be as follows:

- If a mail, account or site is falsely forged or attributed to a natural or juridical person (individual or legal entity), the perpetrator shall be liable to a term of imprisonment of not less than 3 months and/or a fine of not less than 10,000 pounds and not exceeding 30,000 pounds, even if its content does not result in harm.
- In the case of harm, the penalty shall be imprisonment of not less than one year and/or a fine of not less than 50 thousand pounds and not exceeding 200,000 pounds, if the perpetrator used the mail or the site or the fake private account in a manner that harms those to which it is attributed.
- If a mail, account or website is forged or falsely attributed to a public legal person (for example, ministries, corporations and government companies), the penalty shall be imprisonment and a fine of not less than LE 100,000 and not more than LE300,000, even if this does not result in harm.

This article is an attempt to codify the attempts of security authorities and Egyptian investigative bodies to monitor this type of accounts and pages. For example, the State Security Prosecution accused Amr Mohamed (known as Amr Socrates) of the publication of false news that would disturb public peace and security, propagating them through social media networks, because of his administration of a page by the name of "Abdul Fattah al-Sisi." Amr Socrates has been held in custody pending investigations for approximately 11 months.

In its penalties, the law tends to punish individuals because of their lack of technical knowhow. For example, if an individual is subject to hacking of his/her account, personal account or an account of which he/she are the technical administrators, while

unaware of how to secure it, had a security leak in the system of is unaware of being hacked, he/she may be subject to imprisonment. This approach is not appropriate at all considering technical developments and how the Internet works and the securing of information systems.

According to Article 29 of the IT Crimes Act, those whose electronic account has been compromised can be punished for not taking the necessary insurance measures and precautions. The penalty amounts to imprisonment for a period of not less than 6 months and/or a fine of not less than 10 thousand pounds and not exceeding 100 thousand pounds for every person responsible for the administration of the site, or private account, e-mail or information system, since this ignorance resulted in the exposure of any of those spaces to one of the crimes stipulated In law. The law did not specify what measures and precautions were necessary and left the organization of the order to the executive regulations of the law. In the event of an offense on the account or website, and the person responsible for the actual management of the legal person did not report the crime, he/she shall be subject to imprisonment for a period of not less than 3 months and/or a fine of not less than 30 thousand pounds and not more than 100 thousand pounds in accordance with article (35).

These are not the only penalties for site administrators, who are defined by the IT Crimes Act as "anyone responsible for organizing, administration, following up or maintaining one or more websites, including access rights for different users on that site or its design, generation or organization of its pages or content or bearing responsibility for it." Those are subject to the following penalties:

- Article 27: A person shall be punished by imprisonment for a period of not less than two years and/or a fine of not less than LE 100,000 and not more than LE300,000 , if he/she creates, administers or uses a special site or account on a computer network aimed at committing or facilitating one of the crimes punishable by law.
- In accordance with Article (28): A penalty of not less than 6 months imprisonment and/or a fine of not less than 20 thousand and not exceeding 200 thousand or shall be imposed on anyone responsible for the administration of a site or special account, e-mail or information system if he/she withholds or manipulates digital evidence for any crime mentioned in the law, which took place on a site or electronic account

or email with the aim to impede the work of the competent official authorities.

- According to Article (29): A penalty of not less than one year imprisonment and/or a fine of not less than 20 thousand and not exceeding 200,000 pounds shall be imposed on any person responsible for the administration of a site or private account or e-mail or information system that subjects them to one of the crimes mentioned in this law.

In terms of definition of the webmaster the law equated between different responsibilities, as the management of the content of the site is a different responsibility from the responsibility of its security, design, development or programming. On the other hand, the law imposed penalties that are disproportionate to the extent of criminal offenses. In addition, there is an absence of the legal rationale behind the imposition of a penalty of deprivation of liberty due to the failure to protect the site or the electronic account, because the legislator assumes that everyone has the same level of technical knowledge and knowhow and ignores the nature of information systems regarding unknown gaps or the lack of a fully secure information system.

In addition to the punishment of those whose accounts are subjected to hacking, the law imposes some penalties on some unintentional acts on the Internet. In the case of a government employee authorized to enter an electronic system, he may face charges of assaulting the state's information systems in case of deliberate or accidental access or exceeding the limits of the right granted him in terms of time or level of entry or penetrated the site or e-mail or a special account or information system managed by or for the State. The civil servant also faces a penalty of imprisonment for a period of not less than two years and/or a fine of not less than 50,000 pounds and not exceeding 200,000 pounds, in accordance with the provisions of Article 20 of the IT Crimes Law.

The law increases the penalty in the case the entry is made to obstruct or illegally obtain governmental data or information, in which case the penalty is imprisonment and a fine of not less than 100 thousand pounds and not exceeding 500 thousand pounds. In all cases, if any of the above acts result in the destruction, distortion, alteration, changing design, copying, recording, alteration, re-publication or cancellation of such data, information, site, private account, information system or e-mail, in whole or in part, by any means, the penalty shall be imprisonment and a fine of not less than one

million pounds and not exceeding 5 million pounds.

The non-differentiation of the penalty between deliberate or accidental committing of a crime is contrary to the established legal rules. The provisions of the said articles contradict the provisions of the jurisprudential opinions regarding the necessity of the intention and will of the perpetrator. This means that the legal rule does not separate between the act constituting a crime and the result of the crime. There should be a link between an individual's intention to commit a crime and the desired result. This is the basis of an intentional crime, whereas in the crimes of error, the individual has no predisposition to achieve a result of his action.

In addition to the fines and freedom depriving penalties, the law also resorted to the penalty of travel ban. In accordance with Article 9 of the IT Crimes Law, the Attorney General or his authorized representative and the competent investigative authorities may, when necessary, prohibit travel outside the country or to put individuals' names on the "expected arrival" list, conditional on reasons and for specified duration. The Public Prosecutor's Office may, at any time, revoke the order issued by it, and may amend it by removing the name of the accused from the travel ban lists, if necessary. The travel ban ends one year from the date of issue of the order, when a decision is made that there is no basis for instituting criminal proceedings or by a final decision on acquittal, whichever comes first.

The law allows appeal against travel ban or the decision to be placed on the waiting lists before the competent criminal court, within 15 days from the date of knowledge thereof. If the appeal is rejected, the person entitled to the decision has the right to file a new complaint every 3 months from the date of the rejection. The court shall decide the grievance within a period not exceeding 15 days from the date of its approval, giving reasons for its decision after listening to the applicant and the relevant investigation authority.

Egyptian authorities have expanded the issuance of travel bans during the past three years towards activists, human rights defenders, journalists and writers. The legislator of the IT Crimes Act establishes the use of travel bans as a penalty. The Attorney General gives investigators the power to ban travel, most likely to be used later to restrict freedoms of users of social media sites, journalists and activists.

Conclusion

The issuance of the law against the crimes of information technology and the organization of the press and the media at this time in particular are only two new episodes in the authority's quest to impose full control over cyberspace as part of its persistent attempts to close public space as a whole and any space available for freedom of expression in particular. It is also an attempt by the state to legalize the illegal situation prior to the issuance of the laws of blocking and monitoring the Internet and its users.

Egyptian Parliament should review the new laws, especially with respect to Internet censorship, site blocking and user data monitoring.