The Internet and the Law in Egypt Series
(Third part: Digital Privacy)
Content

Methodology 4
Introduction 4
Preamble: Privacy in the digital context 6
First: Internet users’ surveillance and anti-cryptography 8
Second: Telecommunications service providers under the control of security 15
Third: Protection of personal data in Egyptian law 18
Conclusion and recommendations 21
Methodology

The third part of “The Internet and Law Egypt series” is based on an analysis of laws affecting users’ right to privacy on the internet, starting with the Telecommunication Regulation Law No. 10 of 2003, through the Anti-Terrorism Law No. 94 of 2015, the Combating Information Technology Crimes Law No. 175 of 2018, and the Land Transport Regulation Law No. 73 of 2019, and ending with Personal Data Protection Law No. 151 of 2020.

Introduction

The Association for Freedom of Thought and Expression (AFTE) issued the first and second parts of “The Internet and Law in Egypt series.” The first part of the series dealt with a background on the beginnings of the internet in Egypt, the laws governing the communications system, which the State centralizes its administration. While the second part of the series dealt with the laws regulating digital media, setting restrictions regarding the establishment of press websites, the possibility of blocking these websites, as well as the criminal prosecution of those responsible for these websites, and the negative consequences of these legal restrictions on the work of digital media.

In the third and final part of this series, AFTE addresses the issue of digital privacy and its importance in the context of the increasing use of technology and artificial intelligence in daily life. This part of the series also deals with laws that affect privacy, and it begins to enforce mass surveillance.

Many international and regional covenants have established the right to privacy, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. With technology development, the High Commissioner of Human Rights presented a report on “Privacy in the Digital Age” to the Human Rights Council at its thirty-ninth session in 2018. This report aimed to define and clarify
principles, standards, and best practices on the right to privacy in the digital age and the obligation of States and businesses to protect the right to digital privacy.

By the end of this series, the reader who is not specialized in law can get acquainted with the most prominent legal aspects affecting digital rights and understand the reasons why these laws are repressive and in violation of relevant international covenants and standards.

At the end of this part of the series, AFTE directs a set of recommendations to legislators in the House of Representatives and the Senate. Through this, the association aims to clarify the amendments, which, if executed, would allow the protection of digital rights in Egypt.
Article 17 of the International Covenant on Civil and Political Rights states: “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.” Egypt has ratified the International Covenant on Civil and Political Rights, as Presidential Decree No. 536 of 1981 was published in the Official Gazette, considering the provisions of Islamic Law.

The report of the United Nations High Commissioner for Human Rights, published in 2018, addressed the issue of the right to privacy in the digital age, based on several international and regional covenants, including the International Covenant on Civil and Political Rights. The report stated that: “Actors at the International and regional levels are becoming more aware of the challenges and are beginning to act accordingly. The Human Rights Council established the mandate of the Special Rapporteur on the right to privacy in July 2015. In several resolutions, the Human Rights Council and the General Assembly have expressed their concerns about risks to privacy as a result of this surveillance measures or a result of business practices.”

The report defines privacy as: “Recognizing the right of individuals to enjoy a space of self-development, based on the principles of interaction and freedom, or their right to a “private space” in which they can interact or not with others, without being subject to State interference or excessive, intrusive interference practiced by other individuals without reason.” In the digital context, the report states that information privacy includes not only available information but also metadata that, through its analysis, can provide insight into an individual’s behavior, relationships, and preferences.

“For example, the right to privacy is affected when a government monitors a public place, such as a market or a train station, and monitors the individuals in that place. When publicly available information about an individual is collected and analyzed on
social media, the right to privacy is also affected, because publishing information to the public does not mean that its content is not covered by protection”.

The right to privacy in the digital age (2018)

The right to privacy has various effects on several other rights, such as the right to freedom of expression and the right to freedom of peaceful assembly and association. Therefore, moves are increasing at the level of adopting legislation to protect the privacy and limit the practices of States and business institutions that violate privacy. At the international level, there is a special rapporteur on the right to privacy.²

In Egypt, the situation did not differ from the global context, as technology and the internet expanded. According to the summary report on information and communications technology indicators issued by the Ministry of Communications, Egypt’s number of internet users reached 62.3 million by the end of September 2020 as well as, the use of the internet had a massive impact on political participation and expression of opinion in Egypt during the past two decades.

From the other side, the Egyptian government has tended to use technology to impose surveillance on internet users, whether in violation of the law or accordance with regulations issued during the last seven years, such as the Combating Information Technology Crimes Law No. 175 of 2018, and the Anti-Terrorism Law No. 94 of 2015.

As the need for foreign investment represented an economic necessity, the Egyptian government sought to adopt a law to protect personal data. Law No. 151 of 2020, regarding the protection of personal data, was issued. The paper attempts to monitor and analyze these legal variables and how digital privacy is protected in Egypt.

² OHCHR, Special Rapporteur on the right to privacy, last visited September 2021, link: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx
First: Internet users’ surveillance and anti-cryptography

“Operators and providers of telecommunication services and their affiliates, as well as users of these services, shall be not to use any devices to encrypt telecommunication services without obtaining approval from both the National Telecommunications Regulatory Authority (NTRA), the armed forces, and the national security agencies,
and this does not apply to encryption devices for radio and television broadcasting. And with due regard to the sanctity of private life for citizens protected by law, each operator or service provider is obligated or provides at its expense within the licensed telecommunications network all technical capabilities of the equipment, systems, programs, and communications within the telecommunications network that allow the armed forces and national security agencies to exercise their jurisdiction per the law, provided that the provision of the service coincides with providing the required technical capabilities. Providers and operators of telecommunication services and their agents who are entrusted with marketing these services are obligated to obtain accurate information and data about their users from citizens and various entities in the State”.

Article 64 of Telecommunications Regulation Law No. 10 of 2003.

Legislative trends in Egypt indicate indifference to protecting privacy over the Internet. This follows many practices, through which Internet users are monitored by keeping their digital activity data and purchasing spyware. This leads to an increase in arrests of Internet users, and Internet users enforce self-censorship on themselves to avoid these risks.

The legislative structure governing the telecommunications system contributes to supporting the mass surveillance process, starting with the provision of Article (67) of the Telecommunications Regulation Law, centralizing the operation of the system, placing it under the control of the “competent authorities in the state” in emergency cases, and “any other cases related to national security,” without a clear and specific mention of these cases related to national security, through which communication networks as a whole can be subjected to the control of the authorities, particularly in light of the vague definition of national security that we have already mentioned in the first part of the series.

---


4. The previous reference.
Article (64) stipulates that telecommunications companies are obligated to provide all technical capabilities and equipment to the national security agencies and the armed forces, allowing them to exercise their jurisdiction, allowing federal security agencies to monitor internet users without judicial permission.

During the past few years, several laws were issued legalizing the surveillance of telecommunications and internet users by telecommunications companies, which are the same practices that the state has practiced for many years. The beginning was with the issuance of laws that allow direct and clear surveillance of internet users in combating terrorism.

The Anti-Terrorism Law No. 94 of 2015 was issued, which allows the Public Prosecution or the competent investigative authority in Article (46) to surveillance and record conversations and messages within thirty days. Despite the requirement of this article to obtain judicial permission from the investigating authority to carry out surveillance and recording, the broad definition of crimes related to terrorism can lead to expanding the circle of suspicion and surveillance of citizens who are not involved in criminal activities. In addition, this law did not set a time limit for the possibility of renewing surveillance, as Article (46) stipulates the option of renewing surveillance “for the same period or other similar periods.”

Successively, the Combating Information Technology Crimes Law. 175 of 2018, Article (2) of which stipulates the obligations and duties of service providers to keep and store the information system record for six months, despite the stipulation of Paragraph (2) of the same article that such data should not be disclosed, except by a reasoned judicial order, paragraph (3) of the same article obliges service providers to provide all technical capabilities to “national security agencies “to exercise their competencies. This indicates that the law may be used to enforce mass surveillance on cyberspace users by federal security agencies without judicial authorization.

5. Article (46) of the Anti-Terrorism Law: “The Public Prosecution or the competent investigation authority, as the case may be, in a terrorist crime may authorize a reasoned order for a period not exceeding thirty days, to surveillance and record conversations and messages received on wired and wireless means of communication and other modern means of communication, and to record and photograph in private places or through communication networks, information, websites and what is written therein, and the seizure of correspondence, regular or electronic messages, publications, parcels and telegrams of all kinds. The order mentioned in the first paragraph of this Article may be renewed for the same period or other similar periods.”

6. Article (2) of the Combating Information Technology Crimes Law No. 175 of 2018.
Firstly: Without prejudice to the provisions of this law and the Telecommunications Regulatory Law No. 10 of 2003, service providers are obligated to the following:

1. Saving and storing a record of the information system or any means of information technology for a period of one hundred and eighty days. The data is to be saved and stored as follows:

   A. Data that enables the identification of the service user.

   B. Data is related to the content of the dealing information system whenever it is under the service provider’s control.

   C. Data relating to traffic.

   D. Data relating to communication terminals.

   E. Any other data specified by order of the Board of Directors of the NTRA.

2. Maintaining the confidentiality of the data that has been saved and stored, and not disclose it without a reasoned order from one of the competent judicial authorities, including the personal data of its users, or any data or information related to the websites and private accounts that these users or individuals access, and who they communicate with.

3. Securing data and information in a manner that maintains its confidentiality and does not hack or damage it.

Secondly: Without prejudice to the provisions of the Consumer Protection Law, the service provider shall provide to the users of its services and any competent government agency, in the form and manner that can be accessed in an accessible, direct, and continuous way, the following data and information:

1. The name and address of the service provider.
2. Contact information related to the service provider, including IP address.
3. Licensing data to determine the service provider’s identity and to determine the competent authority under its supervision.
4. Any other information is essential to the NTRA for the protection of users, and an order is issued to determine it by the competent minister.
Thirdly: Taking into consideration the sanctity of private life guaranteed by the constitution, service providers and their affiliates are obligated to provide, at the request of the national security agencies and according to their needs, all the technical capabilities that allow authorities to exercise their competencies by the law.

Fourthly: Information technology service providers and their agents and distributors who are responsible for marketing those services are obligated to obtain user data, and others are prohibited from doing so.”

Article (2) of the Combating Information Technology Crimes Law. 175 of 2018.

As well as, Article (6) of the same law referred to the possibility of judicial officers, among whom are employees of the NTRA according to the law, to obtain a reasoned order from the investigation authorities to collect or retain data and information and access to information systems to achieve the purpose of “Seizure,” for 30 days, renewable once. In addition to their right to order service providers -telecommunications companies- to deliver what they have of data or information, as well as data of service users and telecommunications traffic, which takes place on that system.

This allows the use of this article to obtain citizens’ data under the pretext of arresting the offenders, especially in the absence of specific and clear procedural rules, which opens the door to the discretion of law enforcement authorities. As well as allows for surveillance, leading to an expansion in arrests.

The competent investigating authority may issue a reasoned order to the qualified judicial officers for a period not exceeding 30 days, renewable for one time, whenever this is beneficial in revealing the truth about the commission of a crime penalized under the provisions of this law by one or more of the following:

1. Seizure, withdraw, collect or retain data, information or information systems, and track them in any place, system, program, electronic support or computer in which they are located, and digital evidence is delivered to the authority issuing the order, provided that this does not affect the continuity of the systems and service provider if it was necessary.
2. Searching, inspecting and accessing computer programs, databases, and other devices and information systems to achieve the purpose of seizure.

3. To order the service provider to deliver what it has of data or information related to the information system or technical device that is under its control or stored with it, as well as the data of its users and the communications traffic made on that system or technological device. In all cases, the order of competent investigation authority shall be reasoned.

Appeals to orders submitted before the competent criminal court shall be held in the consulting room on the dates and accordance with the procedures established in the Criminal Procedure Code.

**Article (6) of the Combating Information Technology Crimes Law No. 175 of 2018**

As the provision of Article (9) and Article (10) of the Land Transport Regulation Law, No. 87 of 2018 intersects with the requirements of the aforementioned articles regarding the broad powers granted to national security agencies in accessing user data and information.

“Subject to the provision of Article 9 of this law, companies licensed to provide or perform the service and their affiliates are obligated to secure databases and information in a manner that maintains its confidentiality and does not hack or damage it. As well as bound to preserve it directly and easily for a period of one hundred and eighty days and make it available to national security agencies or any competent governmental body upon request. The Prime Minister shall specify the data and information to be saved.

---

7. Article (9) of the Telecommunications Regulation Law No. 10 of 2003: “Taking into consideration the sanctity of private life guaranteed by the constitution, service providers and their affiliates are obligated to provide, at the request of the national security authorities and according to their needs, all data, information and technical capabilities of equipment, systems and programs that allow these authorities to exercise its competencies in accordance with the law if requested, in the manner determined by the Prime Minister's decision based on the presentation of the national security authorities.”
Article (10) of the Land Transport Regulation Law No. 87 of 2018.

Article (64) of the Telecommunications Regulation Law No. 10 of 2003 criminalizes the use of “encryption tools”. Many internet uses to pass through encrypted data transmission techniques, including social media and e-mail apps, should be noted. This provision can be used as an excuse to block cryptographic applications, as it is so broad and general. The Egyptian authorities tried to block encrypted personal chat apps such as Signal app.

According to the above, it is clear that several Egyptian laws establish the violation of privacy in the digital context, which is contrary to international law, as the purpose of monitoring individuals shall be related to suspects and under a legitimate aim and within the frame of compliance with international standards such as “international principles for the application of human rights when monitoring telecommunications.” These principles stipulate respect for the principles of necessity and proportionality, that is, the necessity of conducting communications surveillance to achieve a legitimate purpose, especially if it is the only means to accomplish this purpose, and the act of surveillance is proportional to its purpose.

---

8. Article 64 of the Telecommunications Regulation Law No. 64 of 2003 stipulated: "Operators and providers of telecommunication services and their affiliates, as well as users of these services, are obligated not to use any devices to encrypt telecommunication services without obtaining approval from each of the NTRA, the armed forces and the national security agencies, and this does not apply to devices encoder for radio and television broadcasting.

Taking into consideration the sanctity of the private life of citizens, which is protected by law, each operator or service provider is obligated or provides at his expense in the licensed telecommunications network all technical capabilities of equipment, systems, programs and communications that allow the armed forces and national security agencies to exercise their jurisdiction according the law, provided that the service coincides with the provision of the required technical capabilities, and the providers and operators of telecommunication services and their agents entrusted with marketing these services are obligated to obtain accurate information and data about their users from citizens and from various entities in the country.

9. AFTE, "Internet without surveillance" June 2021, last visit in August 2021, link: https://afteegypt.org/en/breaking_news-2/2021/06/03/22766-afteegypt.html

10. Electronic frontier foundation. International principles on the application of human rights to communication surveillance. Available at: https://necessaryandproportionate.org/ar/principles
Second: Telecommunications service providers under the control of security

Article (81) of the Telecommunications Regulation Law penalize service providers with a fine ranging from 10,000 pounds to 100,000 pounds, in addition to imprisonment and suspension of the company’s work licenses, if Article (64) of the same law is not
applied, which stipulates that telecommunications companies are under the control of national security agencies provide accurate data about users, and provide the necessary equipment and capabilities.

“Anyone who violates any of the provisions of Article (64) of this law shall be penalized by imprisonment and a fine of not less than ten thousand pounds and not more than one hundred thousand pounds. In addition, the court shall order to suspend the license temporarily until the violator provides the equipment, systems and communications programs mentioned in this article”.

Article 81 of the Telecommunications Regulation Law No. 10 of 2003.

“Article (84) of the same law stipulates a fine ranging from ten thousand pounds to fifty thousand pounds, in the event of violating the provision of Article 19, which stipulated: “All entities and companies working in the field of telecommunications are obligated to provide the NTRA with the reports, statistics or information requested by it related to its activities except for those related to national security.”

As for the Combating Information Technology Crimes Law, penalties are enforced on service providers, as stipulated in Article (31), (32), and (33) due to failure to executing Article (2) and (6) of the law, which provide for the disclosure of data users. The penalty ranges from imprisonment for six months to a year -as a minimum- and fines ranging from five thousand pounds up to 10 million pounds.

11. Article (31) stipulated that a penalty of imprisonment for a period of not less than one year and a fine of not less than five thousand pounds and not more than twenty thousand pounds, or either of these two penalties, shall be enforced as any service provider violates the provisions of Clause (2) of First Paragraph of Article (2) of this law, and the penalty for a fine multiplies by the number of defendants who use the service. As well as, Article (32) stipulated that a penalty of imprisonment for a period of not less than 6 months and a fine of no less than 20,000 pounds and not more than 100,000 pounds, or either of these two penalties, shall be enforced as every service provider refrains from executing the order issued by the competent investigation authority to deliver what it has of data or information mentioned in Article (6) of this law.

Article (33) stipulated that a fine of no less than 5 million pounds and not more than 10 million shall be enforced as any service provider breaches any of its obligations stipulated in Clause (1) of First Paragraph of Article (2) and Second Paragraph of Clause Fourth of this law. The fine shall be doubled in the event of recurrence, and the court have the right to cancel the license. Service providers shall be penalized by imprisonment for a period of no less than 3 months and a fine of no less than 200 thousand pounds and not more than one million pounds, whoever violates the provisions of the third paragraph of Article (2) of this law.
For internet users, Article (25) of the Combating Information Technology Crimes Law stipulated: “A penalty of imprisonment for a period of no less than six months, and a fine of no less than 50,000 pounds and not more than 100,000 pounds, shall be enforced on anyone who assaults any of the family principles or values in Egyptian society, or violate the sanctity of private life or send extensively many e-mails to a specific person without his consent, or give data to a system or website to promote goods or services without his permission, or by publishing through the information network or any information technology means, information, news or picture, violates the privacy of any person without his consent, whether the information published is true or false.

Although the article is defined in the law to protect citizens’ privacy, it may be used for the opposite purpose. According to this article, any social media user can be prosecuted for its posts if it violates the Egyptian family’s principles and values. This leaves law enforcement authorities to estimate the family values, which happened in court orders in the “TikTok girls” trials.\(^\text{12}\).
Third: Protection of personal data in Egyptian law

The Personal Data Protection Law No. 151 of 2020 contained exceptions, allowing some entities to violate the privacy of citizens, as Article (3) of the law stipulates the exception to some entities from the provisions of the law, the most important of which:
“National Security Agencies” and “The Central Bank of Egypt and the entities subject to its supervision and control.” This exception is similar to what is granted to national security agencies in the Combating Information Technology Crimes Law regarding obtaining user data.

These exceptions raise the question of the purpose of the legislator from this law and negate its primary role in protecting the privacy of users’ data, especially in the absence of independence from the Personal Data Protection Center.

---

13. According to the provision of Article (1), the national security agencies are defined as (the Presidency of the Republic, the Ministry of Defense, the Ministry of Interior, the General Intelligence Service, the Administrative Control Authority).
The formation of the authority responsible for data protection14 “Personal Data Protection Center” came from representatives of (the Ministry of the Interior, Intelligence and Ministry of Defense) and representatives of (the Administrative Control Authority, the Information Technology Industry Development Authority, the National Telecommunications Regulatory Authority), in addition to three experts. This raises doubts about the center’s performance, especially with approximately one-third of the center’s members from security agencies.

This is in light of the broad powers granted to the center concerning monitoring and supervising law enforcement and “taking the necessary legal measures,” in addition to presenting it the status of a judicial officer.

Conclusion and recommendations

After presenting a summary of the legislation governing the Egyptian telecommunications system and comparing it with the Egyptian constitution and relevant international standards, we can say that the sum of those laws, in light of the centralization of infrastructure and centralization of management, creating an environment that facilitates internet censorship and mass surveillance of its users.

Based on what was previously addressed in the three parts of the Internet and Law in Egypt series, the AFTE recommends the following:

1. Amending Article (12) of the Telecommunications Regulation Law No. 10 of 2003, which regulates the formation of the Board of Directors of the NTRA, to allow the increasing representation of stakeholders and specialized experts in the membership of the Board of Directors.

2. Cancellation of the Combating Information Technology Crimes Law No. 175 of 2018, especially with the possibility of confronting online crimes by introducing some amendments to the Penal Code.

3. Amending the fifth paragraph of Article (3) of the Personal Data Protection Law, No. (151) of 2020, canceling the exception to the national security authorities, the Central Bank, and the entities subject to it from the provisions of the law.

4. Amending Article (20) of the Personal Data Protection Law, by excluding representatives of the security agencies to the formation of the center, per international standards -such as the European General Data Protection Regulation- which is legislators purposes on the fact that the personal data regulator is an independent body.

5. Expedite the issuance of the administrative regulations of the Personal Data Protection Law No. 151 of 2020.

6. Amending Article (73) of the law regulating the press and media No. 181 of 2018, in a manner that guarantees the formation of the Supreme Council
for Media Regulation outside the authority of the President of the Republic, provided that it is formed through the House of Representatives.

7. Cancellation of Article (6) of the Law Regulating the Press and Media stipulates the necessity of obtaining a license from the Supreme Council for Media Regulation to create websites, provided that websites are established upon notification.

8. Cancellation of Article (64) of the Telecommunications Regulation Law No. 10 of 2003, which places telecommunications service providers under the control of national security agencies.

9. Amending Article (67) of the Telecommunications Regulation Law No. 10 of 2003, which allows national security agencies to control and subjugate telecommunications companies, by deleting the sentence: “and any other cases related to national security,” as it is required to specify the scope of exceptions precisely in any legal text.